SECURE COMMUNICATION IN COOPERATIVE NETWORKS USING COOPERATIVE JAMMING TECHNIQUES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

KEREM ERKAN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
ELECTRICAL AND ELECTRONICS ENGINEERING

JANUARY 2014

Approval of the thesis:

SECURE COMMUNICATION IN COOPERATIVE NETWORKS USING COOPERATIVE JAMMING TECHNIQUES

submitted by **KEREM ERKAN** in partial fulfillment of the requirements for the degree of **Master of Science in Electrical and Electronics Engineering Department, Middle East Technical University** by,

Prof. Dr. Canan Özgen
Dean, Graduate School of **Natural and Applied Sciences** _____

Prof. Dr. Gönül Turhan Sayan
Head of Department, **Electrical and Electronics Engineering** _____

Assoc. Prof. Dr. Ali Özgür Yılmaz
Supervisor, **Electrical and Electronics Engineering, METU** _____

Examining Committee Members:

Prof. Dr. Yalçın Tanık
Electrical and Electronics Engineering Department, METU _____

Assoc. Prof. Dr. Ali Özgür Yılmaz
Electrical and Electronics Engineering Department, METU _____

Assoc. Prof. Dr. Çağatay Candan
Electrical and Electronics Engineering Department, METU _____

Prof. Dr. Elif Uysal Bıyıkoğlu
Electrical and Electronics Engineering Department, METU _____

Çağdaş Enis Doyuran
ASELSAN Inc. _____

Date: **23.01.2014**

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: KEREM ERKAN

Signature :

ABSTRACT

SECURE COMMUNICATION IN COOPERATIVE NETWORKS USING COOPERATIVE JAMMING TECHNIQUES

Erkan, Kerem

M.S., Department of Electrical and Electronics Engineering

Supervisor : Assoc. Prof. Dr. Ali Özgür Yılmaz

January 2014, 58 pages

In cooperative communication, a source communicates with a destination over indirect links through relays. Like most wireless systems, cooperative networks seriously suffer from secrecy related issues. In this thesis, cooperative jamming method is utilized to provide secrecy for cooperative networks in which there exist adversary receivers called eavesdroppers. The main idea is to broadcast noise signals from a selected relay to corrupt the signal-to-interference-plus-noise ratio (SINR) at eavesdroppers when the transmitter communicates with the receiver through another selected relay. Throughout the study, it is assumed that channel state information (CSI) of the links between the source, relays and the destination is available at the transmit and receive sides of links. Rich scattering channels are assumed and all channel gains are taken as independent. In contrast to the past studies in the literature, CSI of eavesdroppers' channels exist at only themselves since they are accepted as passive devices in this study. The knowledge on channel gains except eavesdroppers' ones are used to adaptively select the relays to support cooperative jamming.

Cooperative jamming is investigated here from an outage probability perspective where probability of secure transmission is the parameter of interest for a fixed transmission rate. First, cooperative jamming is applied to cooperative networks with single-antenna nodes. The probability of secure communication increases to a degree for a range of the communication rate R with cooperative jamming and adaptive selection of relays. The results are generally encouraging, but may be insufficient for real-world cooperative networks. Second, cooperative jamming is implemented at cooperative networks with multiple-antenna nodes to increase the probability of secure communication benefiting from advantages of multiple antennas. Adaptive transmit precoding is applied at the source and the communicating relay to enhance the SINR at legitimate receivers. This advantage brings an edge over eavesdroppers. Moreover, adaptive noise generation is proposed at the noise emitting relays in order to minimize the effect of noise at legitimate receivers. It is shown that the probability of secure communication dramatically rises with these adaptive techniques. As a result, there is a certain transmission rate R at which the source is able to securely communicate with the destination with probability approaching one.

Keywords: Relay communication, cooperative jamming, secure cooperative communication, relay selection, adaptive transmit precoding, adaptive noise generation

ÖZ

İŞBİRLİKLİ AĞLARDA İŞBİRLİKLİ KARIŞTIRMA TEKNİKLERİ İLE GÜVENLİ HABERLEŞME

Erkan, Kerem
Yüksek Lisans, Elektrik ve Elektronik Mühendisliği Bölümü
Tez Yöneticisi : Doç. Dr. Ali Özgür Yılmaz

Ocak 2014 , 58 sayfa

İşbirlikli haberleşme yönteminde, bir göndermeç bir hedef almaç ile röleler üzerinden dolaylı yoldan iletişim kurmaktadır. Çoğu kablosuz ağlarda olduğu gibi, işbirlikli ağlarda da güvenli haberleşme konusunda ciddi sorunlar ile karşılaşılmaktadır. Bu tez çalışmasında, işbirlikli ağlarda güvenliği arttırmak amacıyla ağda bulunan düşman almaçlara karşı işbirlikli karıştırma metodundan yararlanılmaktadır. Temel fikir, göndermeç ve hedef almaç seçilmiş bir röle üzerinden haberleşirken, seçilmiş diğer bir röle tarafından düşman almaçlara gürültü sinyali yayınlanması ve bu şekilde düşman almaçtaki sinyal gürültü oranının düşürülmesidir. Bu çalışma boyunca, göndermeç, hedef almaç ve röleler arasındaki kanal kazançlarının tüm bu noktalarda bilindiği kabul edilmiştir. Kanalların yüksek saçılımlı olduğu varsayılmıştır ve tüm kanal kazançları bağımsız seçilmiştir. Geçmişte literatürde yer alan çalışmaların aksine, düşman almaçlar bu çalışma boyunca pasif kabul edildiği için, bu almaçlara ait kanal kazançlarının düşman almaçları dışındaki göndermeç, hedef almaç ve rölelerde bilinmediği

varsayılmıştır. Bu sayede, bilinen kanal kazançları gerekli rölelerin seçiminde kullanılarak, işbirlikli karıştırma yönteminin getirdiği kazanç arttırılmaya çalışılmaktadır.

Bu çalışmada, işbirlikli karıştırma, belli bir haberleşme hızındaki güvenli haberleşme olasılığı parametresi üzerinden incelenmektedir. İlk olarak, tek antenli elemanlardan oluşan işbirlikli ağlara işbirlikli karıştırma uygulanmaktadır. Ayrıca, ilgili röleler bilinen kanal kazançlarına göre seçilmektedir. Bu şekilde belli bir haberleşme hızı aralığında, güvenli haberleşme olasılığında bir seviyeye kadar artış sağlanmaktadır. Bu artış ile ulaşılan sonuç olumlu olsa da gerçek dünya dikkate alındığında yeterli olmayabilir. Bu nedenle, ikinci olarak, birden fazla anten bulunduran elemanlardan oluşan işbirlikli ağlara işbirlikli karıştırma uygulanmaktadır. Böylece çoklu anten yapısının getirmiş olduğu avantajlardan yararlanılması amaçlanmaktadır. Göndermeç ve haberleşme rölesinde uyarlamalı önkodlama uygulanıp hedef almaçlarda alınan sinyal gürültü oranı arttırılmaktadır. Buna ek olarak, gürültü sinyali yayan rölelerde, bilinen hedef almaç kanal kazancına göre uyarlamalı gürültü yayılması sağlanarak, hedef almaçta gürültü etkisinin bastırılması amaçlanmaktadır. Kanal kazançlarına göre uyarlamalı iki farklı teknik ile göndermeç ve hedef almaç arası güvenli haberleşme olasılığı önemli ölçüde iyileştirilmektedir. Sonuç olarak, göndermecin hedef almaç ile belli bir haberleşme hızında, bire yakın olasılıkla güvenli haberleşebildiği gösterilmektedir.

Anahtar Kelimeler: Röle haberleşmesi, işbirlikli karıştırma, güvenli işbirlikli haberleşme, röle seçimi, uyarlamalı göndermeç önkodlaması, uyarlamalı gürültü yayma

To my family ...

ACKNOWLEDGMENTS

I would like to thank my supervisor Assoc. Prof. Dr. Ali Özgür Yılmaz for his endless support, technical guidance and friendship during my research. Without his supervision and patience during completion of my thesis, this thesis would never have been able to be fulfilled.

I would like to thank all of my colleagues at ASELSAN Inc. and my friends at METU for their sincere recommendations and patience.

I would like to express my gratitude to The Scientific and Technological Research Council of Turkey (TÜBİTAK) for its financial support throughout my graduate studies.

Finally, I am grateful to my family for their admired support not only during my master's studies but also during my whole life.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

AF	Amplify-and-Forward
CF	Compress-and-Forward
CSI	Channel State Information
DF	Decode-and-Forward
MIMO	Multiple Input Multiple Output
SISO	Single Output Single Input
SINR	Signal-to-Interference-plus-Noise Ratio
SNR	Signal-to-Noise Ratio
SVD	Single Value Decomposition
ZMCSCG	Zero-Mean Circularly Symmetric Complex Gaussian

CHAPTER 1

INTRODUCTION

Wireless communication has experienced an amazing progress in the communications industry in the last two decades. It is totally different from wired communication due to characteristics of wireless channels. Besides providing countless benefits, wireless communication suffers from a number of distinct problems compared to wired communication. Its vulnerability to interference and other channel impediments completely change the communication performance. Moreover, unforeseen variations of these impediments over time as a result of user movement and environment dynamics result in an unpredictable nature of communication. Over relatively large distances there are fluctuations in received power owing to the effects of path loss and shadowing and this effect is called large-scale fading [1]. Furthermore, another serious problem of wireless communication is small-scale fading. Fading is caused by multipath signals which are scaled and delayed versions of the original transmitted signal at the receiver. It leads to rapid variations of signal strength over a short travel distance or time period [2]. Therefore, it hinders the reliability of communication between transmitter and receiver. The basic tool to mitigate the effects of fading is diversity. Diversity techniques benefit from opportunities in various domains. One of the important diversity techniques is space diversity where multiple copies of the same signal are transmitted or received at multiple antennas [1].

One common application of the space diversity technique is observed in Multiple Input Multiple Output (MIMO) systems. MIMO systems use multiple antennas at both transmitter and receiver to enhance the communication performance. These systems especially take advantage of diversity and multiplexing techniques. Firstly, space

diversity at transmitter or receiver reduces the effects of fading at each receiver antenna in MIMO systems. When the antennas of the transmitter or receiver are placed adequately far apart, the probability of being concurrently subjected to deep fades between different transmitter antennas and a single receiver antenna becomes very low. In other words, guaranteeing the independency between the channel gains from transmitter antennas to single receiver antenna, signal power losses due to fading at receiver are minimized. Hence, the reliability of communication is improved. Furthermore, multiplexing techniques increase the data rate that can be sent over a fixed bandwidth in MIMO systems. Different data streams can be sent through different independent channels. Therefore, a significant increase in data rate is obtained in comparison to Single Output Single Input (SISO) systems [1], [3]. Despite many advantages, some drawbacks may decrease usability of MIMO systems in some wireless equipments. Firstly, due to multiple antennas, MIMO systems require powerful processing units at transmitter and receiver. They are complex systems in terms of hardware and software. Moreover, antennas must be placed sufficiently far away from each other to ensure independence between their channels. Furthermore, this complexity may cause high power consumption and thermal problems. For these reasons, the MIMO structure may be inconvenient for power, size or hardware limited wireless devices [4].

An interesting implementation of space diversity has emerged recently through cooperative communication. This new communication technique aims to gain the advantages of MIMO systems by using the relay concept [4]. A generic cooperative network consists of three single-antenna nodes: a source node, a relay node and a destination node. The source attempts at communicating with the destination through both direct link and indirect link over the relay. Therefore, it uses the relay like an additional antenna. Hence, with this implementation, it obtains a diversity gain as can be attained from multiple antennas in MIMO systems [4]. Cooperative networks have advantages in terms of space diversity, but they are more vulnerable to secrecy related problems due to multiple-hop transmission between the source and destination. They are more susceptible to eavesdropping by adversary receivers around the relays and destination [7]. The focus of this thesis is in general to achieve relatively high probability of secure communication at reasonable rates in cooperative networks.

In Chapter 2, the background about cooperative networks and secure communication on physical layer is given. Accordingly, secure communication in cooperative networks is defined as the situation where the destination can decode the message signal transmitted by the source while the eavesdroppers cannot decode it in any of the phases of transmission as in [7]. This is accomplished by attempting at increasing SINR at the destination yet decreasing it at the eavesdroppers. Therefore, it is aimed that the channels of eavesdroppers should be always noisier than those of the destination [14]. For this reason, cooperative jamming method is utilized in cooperative networks to satisfy this necessity. In cooperative jamming, while the source cooperatively communicates with the destination through a relay, another relay in the network transmits noise signal to block the eavesdroppers in both phases.

In Chapter 3, cooperative jamming is applied to cooperative networks with single-antenna nodes. Initially, the signal model is derived for these cooperative networks when there exists cooperative jamming. Throughout the study, it is assumed that CSI of the links between the source, relays and the destination is available at the transmit and receive sides of links. Moreover, channels are assumed to be rich scattering and all channel gains are taken as independent. However, since the eavesdroppers are accepted as passive devices in this study, CSI of the links between them and the other nodes are unknown to other nodes. Therefore, secrecy to be held in this study does not rely on the knowledge about channel gains of eavesdroppers as supposed in [15], [16]. Therefore, the relays used in both message and noise transmission can be selected according to known channel gains to mitigate the negative effects of cooperative jamming on legitimate receivers as in [7]. Thus, it is shown that the probability of secure communication increases to a degree for a range of the communication rate R.

In Chapter 4, cooperative jamming is applied to cooperative networks with multiple-antenna nodes to increase the probability of secure communication to a satisfying level at a reasonable rate R. The communicating and noise emitting relays are intelligently chosen according to known channel gain matrices. It is important to note that the number of antennas is the same at all nodes for fairness including eavesdroppers unlike [16] where the number of antennas at the source and relays have more antennas than the eavesdroppers. Furthermore, adaptive transmit precoding is utilized based on

known channel gain matrices at the source and the communicating relay to improve the SINR values at the legitimate receivers. Finally, adaptive noise generation is applied to totally benefit from the multiple antennas at noise emitting relays. While this technique is used in [16] for non-cooperative networks with multiple-antenna nodes, we adapt it to our cooperative networks. Owing to this technique, the negative effects of noise signals are minimized at legitimate receivers when there is no great changes at the eavesdroppers. Therefore, the maximum probability of secure communication dramatically rises and the related communication rate improves. Moreover, if the number of antennas at all nodes increases, it is possible to accomplish secure communication with probability approaching one at a certain transmission rate R.

The thesis concludes with Chapter 5 where the results produced are summarized and discussed.

CHAPTER 2

COOPERATIVE COMMUNICATION

2.1 Cooperative Communication

A generic cooperative network consists of three single-antenna nodes; a source node, a relay node and a destination node as depicted in Fig. 2.1. In cooperative communication, signal which is generated by the source node follows two different main paths until reaching the destination node. The first path is the direct link between the source and the destination nodes. It is valid when the destination node is not far away from the source node. The second one is the indirect link from the source node to the destination node through the relay node. In this link, transmitted signal from the source node is initially received by the relay node. Then, the relay retransmits the received signal by applying various signal forwarding methods on it. Therefore, the destination node receives two distinct signals which are transmitted from the source node and the relay node. Since the source and relay nodes are placed on different locations in the network, the received signals have highly independent characteristics. In other words, these signals are independently faded versions of the original signal transmitted by the source node. In this manner, spatial diversity is generated through cooperation in the network with single-antenna nodes. Because the probability of observing deep fading on both independent links is low, reliability of communication from the source node to the destination node is reinforced compared to non-cooperative communication [4].

The roots of cooperative communication extend back to 1979 when Cover and El Gamal worked on relay channels from an information theoretic point of view where

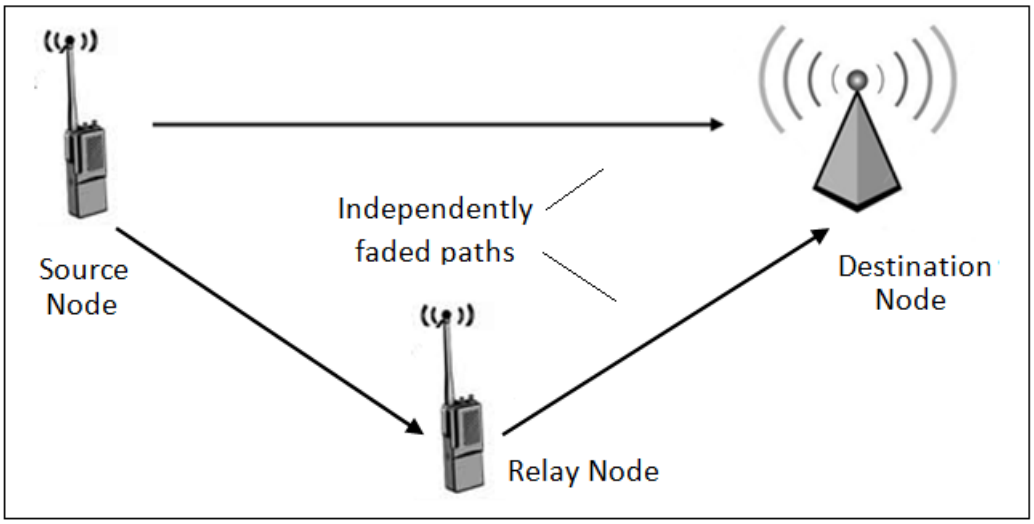

Figure 2.1: Elements of a simple cooperative network

three different types of discrete relay channels were defined. These channels were degraded, reversely degraded relay channels and arbitrary relay channels with feedback. In degraded relay channels, the signal received by the relay is better than received by the destination in terms of signal-to-noise ratio (SNR) while in reversely degraded channels, the opposite is true. As for relay channels with feedback, there are feedback links from signals received by the relay and destination to signals transmitted by the source and relay. Capacity theorems for these types of discrete memoryless relay channels were presented and achievability of these capacity expressions were also proved by Cover and El Gamal. According to the capacity theorems, in degraded relay channels, the rate of the channel from the source to the destination can be improved through cooperation. In reversely degraded channels, the rate of the channel can also be increased depending on signal forwarding technique which is applied at the relay. Furthermore, an achievable rate expression was defined for the general Gaussian relay channel without any relation of degradedness [5]. Although only discrete memoryless and additive white Gaussian relay channels were analyzed without the concept of fading in the Cover and El Gamal's study, the study became a milestone and provided a basis for new researches about the relay channels [4]. In this thesis, the effects of fading will be included in the signal model besides the additive white Gaussian noise.

2.2 Signal Model

The signal model will be derived for the simple cooperative network which is shown in Fig. 2.2. The link between the relay node and the destination node is assumed to be much better than the link between the source node and the destination node. The scenario here can be considered to correspond to a long-distance communication link which needs a relaying terminal for reliable transmission.

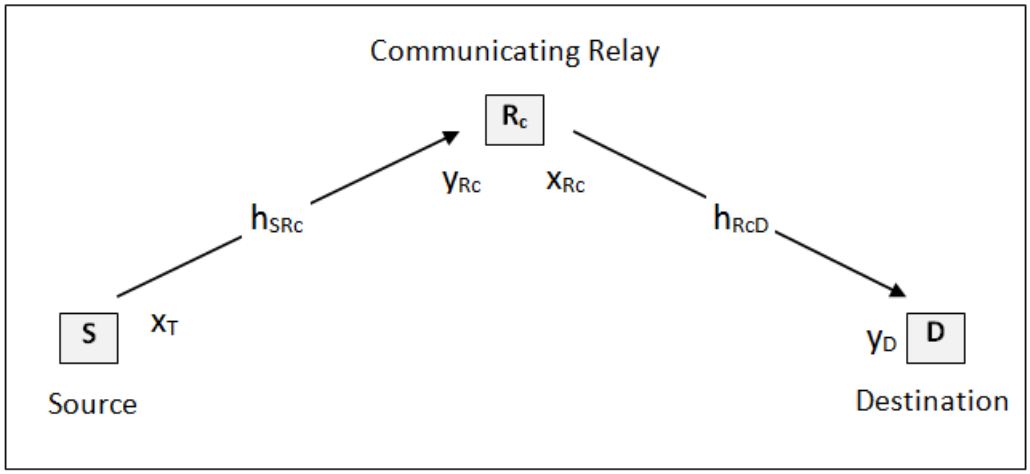

Figure 2.2: Simple cooperative network

Communication takes place in two phases. In the first phase, the signal x_T is transmitted by the source node and the signal y_{R_c} is received by the relay node. In cooperative communication, distinct signal forwarding techniques can be applied on the received signal at the relays. These signal forwarding schemes are mainly grouped in three classes: amplify-and-forward (AF), decode-and-forward (DF) and compress-and-forward (CF) methods. Based on the channel gains of the links between the source node and the relay node or the relay node and the destination node, proper selection of the signal forwarding method among these methods improves the performance of the cooperative network by increasing the transmission reliability. Firstly, in AF method, the relay simply retransmits its received signal by amplifying it with a coefficient. The destination node receives two independently faded versions of the signal. On the other hand, in the DF method, the relay decodes its received signal from the source node and transmits decoded bits by reencoding them. To apply this

method, the channel condition of the link between the source node and the relay node is required to be sufficiently good [4]. Finally, in the CF method, also known as the estimate-and-forward or quantize-and-forward method, the relay does not endeavor to decode its received signal. It only sends a quantized and compressed version of its received message to the destination node. Then, the destination node decodes the data by utilizing both compressed and original versions of signals transmitted by the relay and the source nodes [9]. In comparison of three cooperative signal processing methods, both AF and DF methods have higher block error rate than the CF method and are not powerful at low direct link SNR values. At high direct link SNR values, the difference between the AF, DF and CF methods gets smaller. The AF and DF methods obtain approximately same error rates at high direct link SNR values [4]. In this thesis, the AF method will be used due to its simplicity in analytic expressions and simulations. In the AF method, the received signal y_{R_c} is multiplied by a coefficient α_R to yield the signal x_{R_c}. In the second phase of communication, the signal x_{R_c} is sent by the relay node and the signal y_D is received by the destination node. Energy of the transmitted symbols x_T and x_{R_c} is assumed to be E. Moreover, block fading is assumed. Thus, channel gains are accepted as constant over the blocklength of the source codewords. Furthermore, independent frequency non-selective Rayleigh fading is assumed on the links between all nodes to simplify the expressions. Therefore, channel gains h_{SR_c} and h_{R_cD} are zero-mean circularly symmetric complex Gaussian (ZMCSCG) random variables. In the light of these assumptions, in the first phase of transmission, the transmitted signal x_T with energy E_b and the received signal y_{R_c} at the communicating relay are defined as

$$x_T = \sqrt{E_b} m \tag{2.1a}$$

$$y_{R_c} = \sqrt{E_b} h_{SR_c} m + z_{R_c} \tag{2.1b}$$

respectively where $\mathbb{E}\left[|m|^2\right] = 1$, h_{SR_c} is the channel gain of link from the source to the communicating relay and the white noise term z_{R_c} is a ZMCSCG random variable with variance N_0. In the second phase, the transmitted signal x_{R_c} at the communicating relay is expressed as

$$x_{R_c} = \sqrt{E_b} \alpha_R y_{R_c} \tag{2.2a}$$

$$= \sqrt{E_b} \alpha_R \left(\sqrt{E_b} h_{SR_c} m + z_{R_c} \right) \tag{2.2b}$$

from eqn. (2.1b). In order to set $\mathbb{E}\left[|x_{R_c}|^2\right] = E_b$, the coefficient α_R of the AF method is found through

$$\alpha_R = \frac{1}{\sqrt{\mathbb{E}\left[|y_{R_c}|^2\right]}} \tag{2.3a}$$

$$= \frac{1}{\sqrt{E_b|h_{SR_c}|^2 + N_0}} \tag{2.3b}$$

from eqn.(2.1b). Thus, the received signal y_D at the destination is expressed as

$$y_D = h_{R_cD}x_{R_c} + z_D \tag{2.4a}$$

$$= \sqrt{E_b}h_{R_cD}\alpha_R y_{R_c} + z_D \tag{2.4b}$$

$$= E_b h_{R_cD}h_{SR_c}\alpha_R m + \sqrt{E_b}h_{R_cD}\alpha_R z_{R_c} + z_D \tag{2.4c}$$

from eqn. (2.2b) where z_D is a ZMCSCG random variable with variance N_0. The received SNR at the destination node is expressed as

$$SNR_D = \frac{\mathbb{E}\left[|E_b h_{R_cD}h_{SR_c}\alpha_R m|^2\right]}{\mathbb{E}\left[|\sqrt{E_b}h_{R_cD}\alpha_R z_{R_c} + z_D|^2\right]} \tag{2.5a}$$

$$= \frac{E_b^2\alpha_R^2|h_{R_cD}h_{SR_c}|^2}{E_b|h_{R_cD}|^2\alpha_R^2 N_0 + N_0} \tag{2.5b}$$

from eqn. (2.4c). Thus, the capacity of the destination is defined as

$$C_D = \log_2(1 + SNR_D) \tag{2.6a}$$

$$= \log_2\left(1 + \frac{E_b^2\alpha_R^2|h_{R_cD}h_{SR_c}|^2}{E_b|h_{R_cD}|^2\alpha_R^2 N_0 + N_0}\right) \tag{2.6b}$$

from eqn. (2.5b).

The capacity of a cooperative network may dramatically change by adjusting distinct network design parameters. For example, the number of relays which help communication or the number of all relays among which cooperating relays are selected affect the performance of communication directly. Moreover, existence of two or more hops of communication and the signal forwarding method at the relays alter the signal model of the cooperative network and thus capacity is influenced. Additionally, whether the communication is secure or not when eavesdropping nodes exist is another critical issue and totally changes the network design. In the remaining of this chapter, the security issue will be studied.

2.3 Secure Communication

The broadcast nature of wireless communication constitutes severe problems. While broadcasting helps cooperation techniques in cooperative networks, it may also result in unintended leakage of data through the overheard signals at eavesdropper nodes acting as adversaries. An eavesdropper is able to exploit the communication link between the transmitter and the intended receiver and extract data from the overheard signal unless sufficient security precautions are taken. In secrecy systems, the primary goal is to minimize the information which is captured by an eavesdropper when the capacity of the intended communication link is kept as high as possible.

In wireless communication, security schemes can be grouped into two categories based on eavesdropper's abilities in a network: computational security and information theoretic security. Computational security is a standard form of security which relies on assumptions about the limited computing power of eavesdroppers. Conventional cryptographic security can be included in this type of security. It takes place at the upper layers of the protocol stack [13]. In cryptography, a message is encrypted with a selected key generated by a key source and transmitted to the intended receiver as depicted in Fig. 2.3. The receiver is able to decode the encrypted message as long as it owns the related key information [10]. Security is accomplished if an eavesdropper without the key cannot solve the difficult decoding problem. On the other hand, the eavesdropper can record the received signal and process it to break the cryptography on it in an extended time after recording. When the last developments in computation technologies, such as quantum computing are considered, decoding by breaking the crypto is not impossible even if nothing about the key is known. Therefore, in standard cryptographic methods, providing long-lasting security which may be significant especially in military networks becomes gradually hard [7].

In information-theoretic security, which is also called unconditional security, it is assumed that the eavesdropper in the network has infinite computational power for the analysis of encrypted messages although it may take unrealistic time. It is highly stronger than the computational security due to its ability to provide secret transmission without being based on computational limitations at eavesdroppers [15]. Unlike the computational security methods, information-theoretic security intends secret

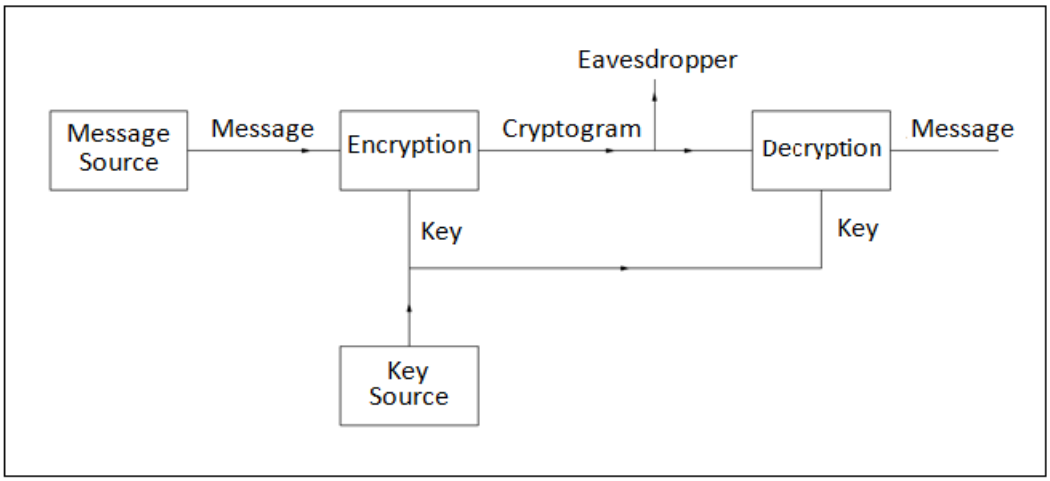

Figure 2.3: General secrecy system

communication without using an encryption key and it is characteristically handled at the physical layer.

The theoretical basis for information-theoretic security was established by Shannon [10]. According to Shannon, a secrecy system is a group of uniquely reversible transformations that convert a set of various messages into a set of cryptograms. Each message and each key corresponding to related transformation have a probability associated with them. This is called a priori probability which is the probability of selecting that key and message. These probabilities for different keys and messages constitute a priori knowledge at eavesdroppers. In secure transmission, firstly, a key is selected and sent to the destination assuming that there is no interception. Then, a message is chosen and encrypted with the selected key to obtain a cryptogram. The cryptogram is sent to the destination through insecure channel and probably captured by eavesdroppers in this insecure network. At the destination, the source message is extracted by implementing the inverse of the transformation which is applied at the source. In Shannon's work, the worst case is assumed in which eavesdroppers know the group of keys and their a priori probabilities. If an eavesdropper captures the cryptogram, from these probabilities and received cryptogram it can figure out new probabilities of different possible messages and keys, called a posteriori probabilities. In the light of these probabilities, "perfect secrecy" is obtained if a posteriori probabilities of various messages after the interception of the cryptogram are equal to the

a priori probabilities of the same messages before the interception. In other words, for perfect secrecy, intercepted cryptogram must not give eavesdroppers any information to calculate a posteriori probabilities. According to Shannon, it is possible if the system has finite number of messages and the same number of possible keys [10].

Based on Shannon's seminal work, the information theoretic security was analyzed in Wyner's paper [11] through a special wiretap channel, called the degraded wiretap channel, which is a degraded version of the receiver's main channel as depicted in Fig. 2.4. That is, the eavesdropper receives a degraded version of the signal which is obtained at the intended receiver. In this paper, secrecy of the wiretap channel was measured by the equivocation rate R_e, which is the conditional entropy of a message given the observation of the eavesdropper, and the transmission rate R. These are defined by

$$R_e = \frac{1}{n} H(W^k|Z^n) \tag{2.7a}$$

$$R = \frac{H(W^k)}{n}. \tag{2.7b}$$

The equivocation rate represents the uncertainty corresponding to a message W given the captured information Z about it at the eavesdropper. Thus, the degree of secrecy improves when the equivocation rate rises. The set of all achievable (R, R_e) pairs constitutes the rate equivocation rate region. Acccording to Wyner's study, perfect secrecy exists when the rate of equivocation is equal to the rate of transmission in this region. That is, the observation of the eavesdropper never provides any information which decreases the uncertainty of the source message at the eavesdropper in case of perfect secrecy. In a parallel manner, secrecy capacity is defined as the maximum achievable rate R such that $R = R_e$. Moreover, secrecy capacity is also defined as

$$C_s = \max_{p(x)} I(X;Y|Z) = \max_{p(x)} [I(X;Y) - I(X;Z)], \tag{2.8}$$

where X, Y, Z are random variables forming a Markov chain $X \rightarrow Y \rightarrow Z$ due to the degraded wiretap channel as shown in Fig. 2.4. Therefore, secrecy capacity is the maximum difference between the main and wiretap channels' achievable rates [11], [12].

Following Wyner's work [11], Csiszar and Körner extended the Wyner's wiretap channel concept to the Gaussian broadcast channels [14]. In this generalized work,

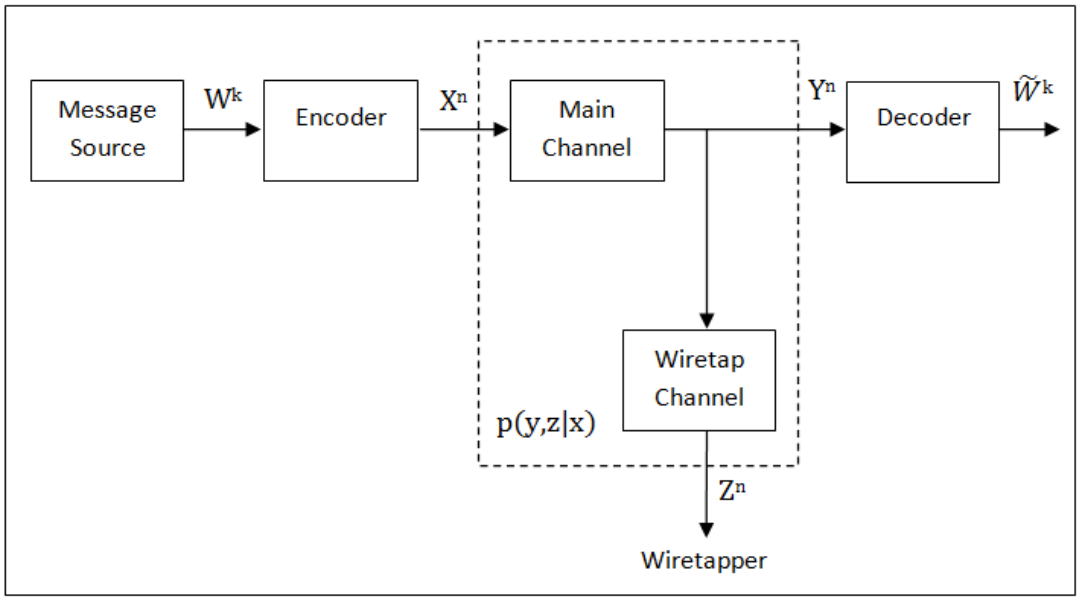

Figure 2.4: Degraded wiretap channel

while the source transmits a common message to two receivers, it also sends a private message one of the receivers by establishing secrecy against the other receiver. Unlike [11], the receivers have separate channels and there is no any degradedness condition. Perfect secrecy is provided when the private receiver's channel is not worse than the other's receiver channel. In other words, the secrecy capacity is always positive when the channel in which the private message is sent is not noisier than the other channel [14].

CHAPTER 3

COOPERATIVE JAMMING METHOD WITH SINGLE-ANTENNA NODES

3.1 Cooperative Jamming Method

In a two-hop cooperative communication where the eavesdroppers may wiretap the transmission in both hops, secrecy has to be held in both phases of the transmission to attain perfect secrecy from the source to the destination. Therefore, in the first phase, the signal transmitted by the source has to be prevented from being overheard by the eavesdroppers in the network. Moreover, in the second phase, the signal transmitted by the relay has to be blocked at the eavesdroppers. Thus, as defined in [14], it is required to make the channel between the source and the eavesdropper noisier than the channel between the source and the relay for the secrecy of the first phase of the transmission. In a similar manner, it is essential to make the channel between the relay and the eavesdropper noisier than the channel between the relay and the destination for the secure second phase of the transmission. For these reasons, the cooperative jamming method is applied at cooperative networks with eavesdroppers to yield end-to-end secrecy [7]. The cooperative jamming method is simply noise generation from a group of relays in the network. In this method, while a group of relay nodes called communicating relays helps the communication, another group of relay nodes called noise emitting relays attempts at jamming the eavesdroppers by emitting noise in both phases as depicted in Fig. 3.1. For instance, as the relays R_3 and R_4 help the source transmit its message to the destination, the relays R_1 and R_6 forward the noise signal to jam the eavesdroppers in the first phase of the communication and

the relays R_2 and R_5 emit the noise signal in the second phase. Therefore, SINR at eavesdroppers is lowered. Below a certain value of SINR, it is guaranteed that recovering the original message becomes impossible regardless of the processing of the signal at eavesdroppers. In fact, the emitted noise negatively affects not only the eavesdroppers, but also the communicating relays and the destination in the first and second phases respectively. Thus, the fundamental aim of the cooperative jamming method is to corrupt the eavesdroppers' channels more than the intended receivers' channels. It is critical to always keep the received SINR at the eavesdroppers below a certain value while keeping the received SINR at the destination above a certain value [7].

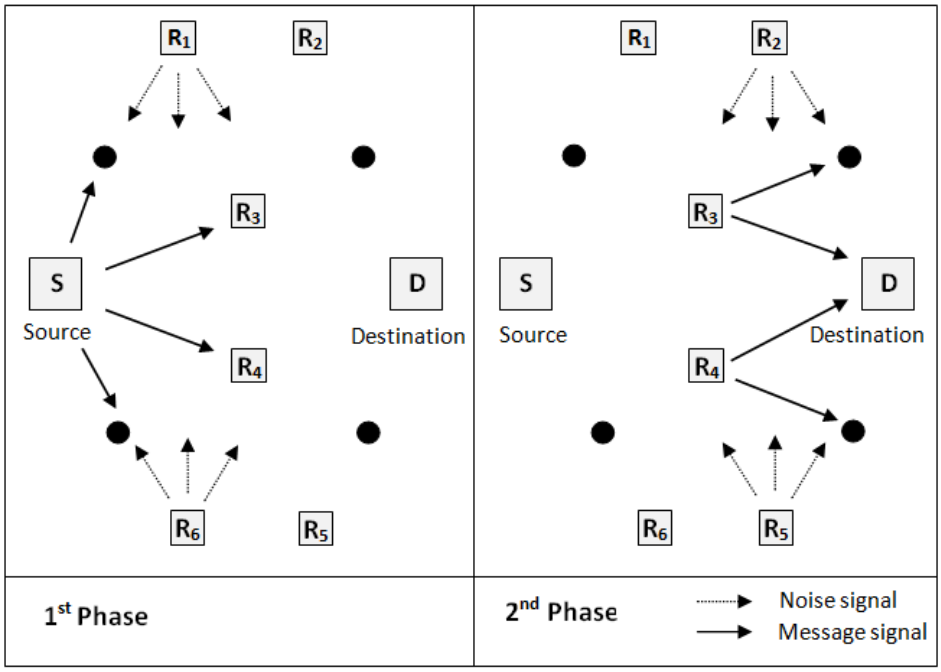

Figure 3.1: Fundamental cooperative communication with cooperative jamming

In this chapter, the cooperative jamming method will be examined for cooperative networks with single-antenna nodes. To begin with, a new signal model will be derived for these networks when there exists cooperative jamming in the network. Afterwards, numerical results will be presented to observe the effects of cooperative jamming and methods in selecting the communicating and noise emitting relays by using the derived signal model.

3.2 Signal Model

In this section, the signal model is very similar to the model given in Section 2.2. The assumptions are the same. Distinctly, the cooperative network is composed of a source, a destination, a communicating relay, a noise emitting relay and an eavesdropper as depicted in Fig. 3.2 and 3.3. Moreover, additional noise signal is generated by the noise emitting relay in each communication phase. The noise emitting relay's function is to increase the noise at the eavesdropper and the selected communicating relay is used to help the communication.

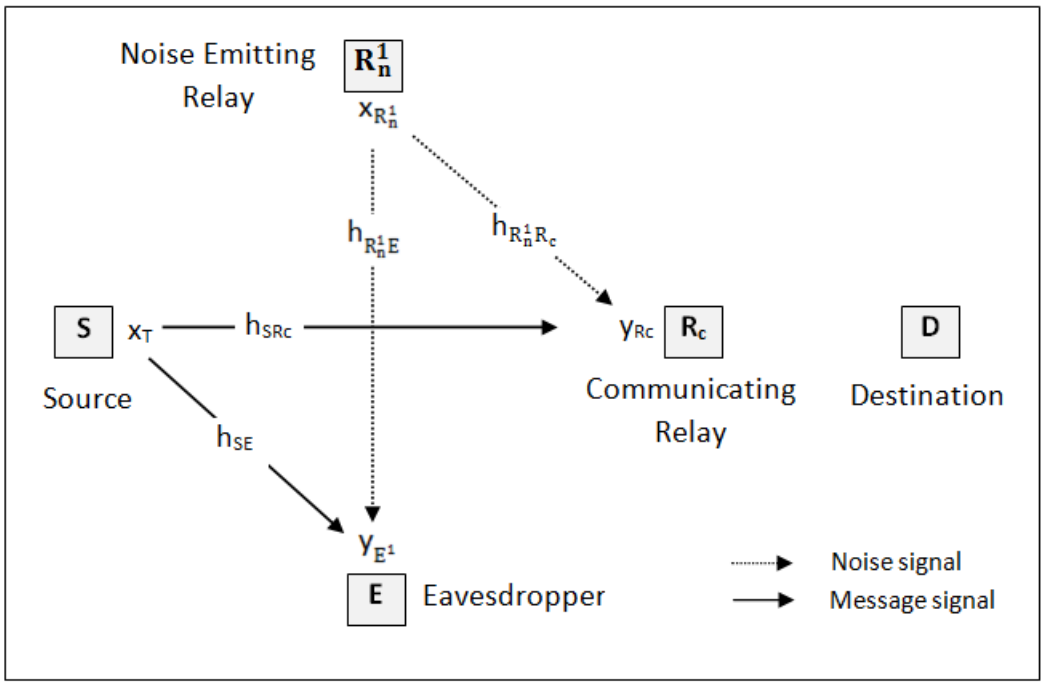

Figure 3.2: The cooperative network with single-antenna nodes in the first phase

In the first phase which is displayed in Fig. 3.2, the information signal x_T and the noise signal $x_{R_n^1}$ are transmitted by the source and the selected noise emitting relay respectively. These transmitted signals with energy E_b are defined as

$$x_T = \sqrt{E_b} m \tag{3.1a}$$

$$x_{R_n^1} = \sqrt{E_b} w_{R_n^1} \tag{3.1b}$$

where $\mathbb{E}\left[|m|^2\right] = 1$ and $\mathbb{E}\left[|w_{R_n^1}|^2\right] = 1$ [*]. The signals y_{R_c} and y_{E^1} are received by the selected communicating relay and the eavesdropper respectively. These signals are expressed as

$$y_{R_c} = h_{SR_c}x_T + h_{R_n^1R_c}x_{R_n^1} + z_{R_c} \tag{3.2a}$$

$$y_{E^1} = h_{SE}x_T + h_{R_n^1E}x_{R_n^1} + z_{E^1}. \tag{3.2b}$$

From equations (3.1a), (3.1b), (3.2a) and (3.2b)

$$y_{R_c} = \sqrt{E_b}h_{SR_c}m + \sqrt{E_b}h_{R_n^1R_c}w_{R_n^1} + z_{R_c} \tag{3.3a}$$

$$y_{E^1} = \sqrt{E_b}h_{SE}m + \sqrt{E_b}h_{R_n^1E}w_{R_n^1} + z_{E^1} \tag{3.3b}$$

where h_{SR_c} and h_{SE} are the channel gains of the links from the source to the communicating relay and the eavesdropper respectively, $h_{R_n^1R_c}$ and $h_{R_n^1E}$ are the channel gains of the links from the first phase's noise emitting relay to the communicating relay and the eavesdropper respectively, the white noise terms z_{R_c} and z_{E^1} are ZMCSCG random variables with variance N_0. Thus, the SINR observed at the eavesdropper is given as

$$SINR_{E^1} = \frac{\mathbb{E}\left[|\sqrt{E_b}h_{SE}m|^2\right]}{\mathbb{E}\left[|\sqrt{E_b}h_{R_n^1E}w_{R_n^1} + z_{E^1}|^2\right]} \tag{3.4a}$$

$$= \frac{E_b|h_{SE}|^2}{E_b|h_{R_n^1E}|^2 + N_0} \tag{3.4b}$$

from equation (3.3a). Accordingly, the capacity of the eavesdropper's channel is expressed as

$$C_{E^1} = log_2(1 + SINR_{E^1}) \tag{3.5a}$$

$$= log_2\left(1 + \frac{E_b|h_{SE}|^2}{E_b|h_{R_n^1E}|^2 + N_0}\right) \tag{3.5b}$$

from equation (3.4b).

In the second phase which is shown in Fig. 3.3, the signal transmitted by the communicating relay is

$$x_{R_c} = \sqrt{E_b}\alpha_R y_{R_c} \tag{3.6a}$$

$$= \sqrt{E_b}\alpha_R(\sqrt{E_b}h_{SR_c}m + \sqrt{E_b}h_{R_n^1R_c}w_{R_n^1} + z_{R_c}) \tag{3.6b}$$

[*] The numbers 1 and 2 in superscripts of the parameters R_n and E indicate which phase of the communication must be considered.

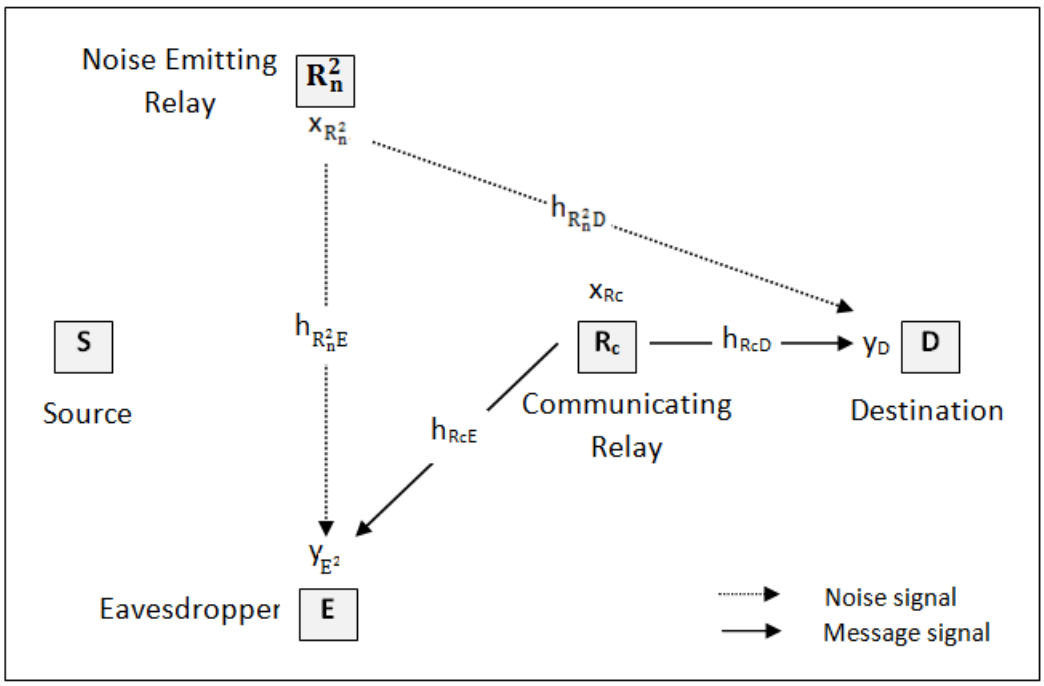

Figure 3.3: The cooperative network with single-antenna nodes in the second phase

from equation (3.3a). In order to set $\mathbb{E}\left[|x_{R_c}|^2\right] = E_b$, the coefficient α_R of the AF method is found through

$$\alpha_R = \frac{1}{\sqrt{\mathbb{E}\left[|y_{R_c}|^2\right]}} \tag{3.7a}$$

$$= \frac{1}{\sqrt{E_b|h_{SR_c}|^2 + E_b|h_{R_n^1 R_c}|^2 + N_0}}. \tag{3.7b}$$

Furthermore, the noise emitting relay may change in the second phase. Therefore, the noise signal broadcasted by the second phase's noise emitting relay is expressed as

$$x_{R_n^2} = \sqrt{E_b} w_{R_n^2} \tag{3.8}$$

where $\mathbb{E}\left[|w_{R_n^2}|^2\right]$=1. As a result, the signal y_D which is received by the destination is defined as

$$y_D = h_{R_c D} x_{R_c} + h_{R_n^2 D} x_{R_n^2} + z_D. \tag{3.9a}$$

From equations (3.6b), (3.8) and (3.9a),

$$y_D = h_{R_cD}(\sqrt{E_b}\alpha_R y_{R_c}) + \sqrt{E_b}h_{R_n^2D}w_{R_n^2} + z_D \tag{3.10a}$$

$$= \sqrt{E_b}\alpha_R h_{R_cD}(\sqrt{E_b}h_{SR_c}m + \sqrt{E_b}h_{R_n^1R_c}w_{R_n^1} + z_{R_c}) + \sqrt{E_b}h_{R_n^2D}w_{R_n^2} + z_D \tag{3.10b}$$

$$= E_b\alpha_R h_{R_cD}h_{SR_c}m + E_b\alpha_R h_{R_cD}h_{R_n^1R_c}w_{R_n^1} + \sqrt{E_b}\alpha_R h_{R_cD}z_{R_c} + \sqrt{E_b}h_{R_n^2D}w_{R_n^2} + z_D \tag{3.10c}$$

where h_{R_cD} is the channel gain of the link from the communicating relay to the destination, $h_{R_n^2D}$ is the channel gain of the link from the second phase's noise emitting relay to the destination, the white noise term z_D is a ZMCSCG random variable with variance N_0. In equation (3.10c), only the first term includes the source message m and other terms consists of the noise signals broadcasted by the noise emitting relays in the first and second phases of transmission and white noises of the related channels. Therefore, the SINR value received by the destination is

$$SINR_D = \frac{\mathbb{E}\left[|E_b\alpha_R h_{R_cD}h_{SR_c}m|^2\right]}{\mathbb{E}\left[|E_b\alpha_R h_{R_cD}h_{R_n^1R_c}w_{R_n^1} + \sqrt{E_b}\alpha_R h_{R_cD}z_{R_c} + \sqrt{E_b}h_{R_n^2D}w_{R_n^2} + z_D|^2\right]} \tag{3.11a}$$

$$= \frac{E_b^2\alpha_R^2|h_{R_cD}h_{SR_c}|^2}{E_b^2\alpha_R^2|h_{R_cD}h_{R_n^1R_c}|^2 + E_b\alpha_R^2|h_{R_cD}|^2N_0 + E_b|h_{R_n^2D}|^2 + N_0}. \tag{3.11b}$$

from equation (3.10c). Similarly, the signal y_{E^2} which is received by the eavesdropper in the second phase is defined as

$$y_{E^2} = h_{R_cE}x_{R_c} + h_{R_n^2E}x_{R_n^2} + z_{E^2}. \tag{3.12a}$$

From equations (3.6b), (3.8) and (3.12a),

$$y_{E^2} = h_{R_cE}(\sqrt{E_b}\alpha_R y_{R_c}) + \sqrt{E_b}h_{R_n^2E}w_{R_n^2} + z_{E^2} \tag{3.13a}$$

$$= \sqrt{E_b}\alpha_R h_{R_cE}(\sqrt{E_b}h_{SR_c}m + \sqrt{E_b}h_{R_n^1R_c}w_{R_n^1} + z_{R_c}) + \sqrt{E_b}h_{R_n^2E}w_{R_n^2} + z_{E^2} \tag{3.13b}$$

$$= E_b\alpha_R h_{R_cE}h_{SR_c}m + E_b\alpha_R h_{R_cE}h_{R_n^1R_c}w_{R_n^1} + \sqrt{E_b}\alpha_R h_{R_cE}z_{R_c} + \sqrt{E_b}h_{R_n^2E}w_{R_n^2} + z_{E^2} \tag{3.13c}$$

where h_{R_cE} is the channel gain of the link from the communicating relay to the eavesdropper, $h_{R_n^2E}$ are the channel gain of the link from the second phase's noise emitting relay to the eavesdropper, the white noise term z_{E^2} is a ZMCSCG random variable with variance N_0. In a similar manner, in equation (3.13c), only the first term comprises the source message m and other terms represent noise. Thus, the SINR value

at the eavesdropper in the second phase is

$$SINR_{E^2} = \frac{\mathbb{E}\left[|E_b\alpha_R h_{R_cE} h_{SR_c} m|^2\right]}{\mathbb{E}\left[|E_b\alpha_R h_{R_cE} h_{R_n^1R_c} w_{R_n^1} + \sqrt{E_b}\alpha_R h_{R_cE} z_{R_c} + \sqrt{E_b} h_{R_n^2E} w_{R_n^2} + z_{E^2}|^2\right]} \tag{3.14a}$$

$$= \frac{E_b^2\alpha_R^2 |h_{R_cE} h_{SR_c}|^2}{E_b^2\alpha_R^2 |h_{R_cE} h_{R_n^1R_c}|^2 + E_b\alpha_R^2 |h_{R_cE}|^2 N_0 + E_b |h_{R_n^2E}|^2 + N_0}. \tag{3.14b}$$

from equation (3.13c). Finally, for the second phase, the capacity expressions of the destination and eavesdropper's channels are expressed as

$$C_D = log_2\left(1 + \frac{E_b^2\alpha_R^2 |h_{R_cD} h_{SR_c}|^2}{E_b^2\alpha_R^2 |h_{R_cD} h_{R_n^1R_c}|^2 + E_b\alpha_R^2 |h_{R_cD}|^2 N_0 + E_b |h_{R_n^2D}|^2 + N_0}\right) \tag{3.15a}$$

$$C_E^2 = log_2\left(1 + \frac{E_b^2\alpha_R^2 |h_{R_cE} h_{SR_c}|^2}{E_b^2\alpha_R^2 |h_{R_cE} h_{R_n^1R_c}|^2 + E_b\alpha_R^2 |h_{R_cE}|^2 N_0 + E_b |h_{R_n^2E}|^2 + N_0}\right) \tag{3.15b}$$

respectively from equations (3.11b) and (3.14b).

3.3 Defining an Event for Secrecy

To accomplish perfect secrecy in our setting, while the destination is able to decode the source message, the eavesdropper should not be able to decode it in any of the phases. Therefore, to securely communicate with rate R, the destination's channel capacity C_D must be greater than the rate R while the eavesdropper's channel capacities C_{E^1} and C_{E^2} have to be smaller than the rate R in the first and second phases of communication respectively. In other words, our goal for secure cooperative communication is to make the events $\{C_D > R\}$, $\{C_{E^1} < R\}$ and $\{C_{E^2} < R\}$ occur together. Therefore, a new event A_{sec} may be defined as

$$A_{sec} = \{C_D > R, C_{E^1} < R, C_{E^2} < R\} \tag{3.16}$$

for simplicity. Throughout this script, it is assumed that the input alphabet is Gaussian. In the following section, the probability of secure communication $P_{sec}(R)$ is evaluated at fixed transmission rate R by using the Monte Carlo method. Therefore, the occurrence of the event A_{sec} is checked at sufficiently many different set of channel gains for fixed rate R. The frequency of occurrences of the event A_{sec} determines the probability of secure communication $P_{sec}(R)$. Hence, $P_{sec}(R)$ may be expressed as

$$P_{sec}(R) \approx \frac{1}{N}\sum_{k=1}^{N} I_k(A_{sec}) \tag{3.17}$$

where the indicator function I is

$$I_k(A_{sec}) = \begin{cases} 1 & \text{If } A_{sec} \text{ occurs,} \\ 0 & \text{otherwise.} \end{cases} \tag{3.18}$$

Similarly, to observe the distinct outcomes of the simulations, events A_D and A_E may be defined as

$$A_D = \{C_D > R\} \tag{3.19a}$$

$$A_E = \{C_{E^1} < R, C_{E^2} < R\}. \tag{3.19b}$$

It is important to note that the event A_D includes the cases where eavesdropper is able to decode its received message signal in the first or the second phase or both phases of the communication. Hence, it is not always secure. Moreover, the event A_E is composed of the cases in which the destination cannot decode its received message signal. Thus, the communication between the source and the destination cannot be accomplished in each event A_E.

In a similar manner, the frequency of occurrences of the event A_D reveals the probability $P_D(R)$ of the decoding the received message signal at the destination. Furthermore, the frequency of occurrences of the event A_E gives the probability $P_E(R)$ of the case where the eavesdropper is not able to decode its received message signal in any of the phases of communication. Thus, $P_D(R)$ and $P_E(R)$ may be expressed as

$$P_D(R) \approx \frac{1}{N} \sum_{k=1}^{N} I_k(A_D) \tag{3.20a}$$

$$P_E(R) \approx \frac{1}{N} \sum_{k=1}^{N} I_k(A_E). \tag{3.20b}$$

The probabilities $P_{sec}(R)$, $P_D(R)$ and $P_E(R)$ will be repeatedly calculated for a range of the rate R according to equations (3.17), (3.20a) and (3.20b) respectively. Finally, the plots of the probabilities $P_{sec}(R)$, $P_D(R)$ and $P_E(R)$ versus the transmission rate R will be drawn.

3.4 Relay Selection Mechanism

One of the most critical issues about cooperative transmission with cooperative jamming is the relay selection. Proper selection of the communicating and noise emitting relays among a group of relays minimizes the negative effects of the noise emitted by relays on legitimate receivers. Therefore, the probability of secure communication $P_{sec}(R)$ is improved. The relay selection rules are primarily based on channel gains. Hence, whether CSI exists at the nodes in the network is significant in the relay selection algorithms. Firstly, it is assumed that all of the channel gains between the nodes in the network except the eavesdropper's channel gains are known to all nodes, probably even to the eavesdropper. Thus, the secrecy to be established does not depend on secrecy of channel gains. These channel gains are used in the relay selection algorithm. Since the eavesdropper is assumed to be a passive node in this work, it is not realistic to know the gains of the eavesdropper's channels at other nodes in the network. In the first set of simulations, the relay selection algorithm proposed in [7] will be used. In that algorithm, the communicating relay R_c is selected at the beginning and then, the noise emitting relays R_n^1 and R_n^2 are chosen according to the channel gains of the selected communicating relay R_c and the destination. The number of the relays in the relay set is 5 in our simulations. Hence, the communicating and noise emitting relays are selected among 5 relays in the network. The relay R_i with the largest $\min\{|h_{SR_i}|^2, |h_{R_iD}|^2\}$ is chosen as the communicating relay R_c

$$R_c = \underset{R_i}{\operatorname{argmax}} \ \min\{|h_{SR_i}|^2, |h_{R_iD}|^2\} \tag{3.21}$$

where h_{SR_i} and h_{R_iD} are the channel gains of the links from the source and the destination to the relay R_i. For this reason, the algorithm is called largest minimum selection in this section. Moreover, the relay which has the weakest link to the communicating relay R_c is selected among the remaining 4 relays as the noise emitting relay R_n^1 in the first phase. Therefore,

$$R_n^1 = \underset{R_i \neq R_c}{\arg\min} \ |h_{R_iR_c}|^2 \tag{3.22}$$

where $h_{R_iR_c}$ is the channel gain of the link from the relay R_i to the communicating relay R_c. Hence, the unfavorable effects of the noise emitting relay on the communicating relay is minimized and the received SINR at the communicating relay is maximized

as much as possible. Similarly, the second phase's noise emitting relay is selected as

$$R_n^2 = \arg\min_{R_i \neq R_c} |h_{R_i D}|^2 \tag{3.23}$$

where $h_{R_i D}$ is the channel gain of the link from the relay R_i to the destination. Thus, the noise emitting relay minimally decreases the received SINR at the destination [7]. Note that this is not optimal strategy but just a good strategy that does not require exhaustive search.

3.5 Numerical Results

There are several parameters which must be set before presenting the simulations. Firstly, the value of average SNR E_b/N_0 must be adjusted. As indicated in the previous Section 3.2, the average SNR values at the source, the communicating relay R_c and the noise emitting relays R_n^1 and R_n^2 are the same. In all simulations in this section, the value of average SNR E_b/N_0 will be taken as 10 dB. Furthermore, the number of the trials which is used in the calculations of the probabilities $P_{sec}(R)$, $P_D(R)$ and $P_E(R)$ will be taken as $N = 10000$ for convenience. The number of trials $N = 10000$ is sufficiently large for our purposes here as observed from the smoothness of the produced curves. In each trial, different independent set of channel gains will be used. The channel gains are assumed to be ZMCSCG random variables with variance 1.

In the following sections, the simulation results will be examined by observing the effects of cooperative jamming and the relay selection method on the probability of secure communication $P_{sec}(R)$.

3.5.1 The Effect of Cooperative Jamming

In this section, the probabilities $P_{sec}(R)$, $P_D(R)$ and $P_E(R)$ for a range of rate R are compared in the scenarios with and without cooperative jamming. The largest minimum selection method is used as the relay selection method. In the first simulation which is shown in Fig. 3.4, the probability $P_{sec}(R)$ is displayed against rate R for two cases. As observed in this graph, the source can securely transmits its message to the destination most probably at the rate $R = 2.8$ bps when there is no cooperative

jamming. Its probability of secure communication $P_{sec}(R)$ at this rate is 0.15. On the other hand, the maximum value of the probability $P_{sec}(R)$ rises to approximately 0.34 when cooperative jamming is taken into account. Moreover, the communication rate at which secure communication is most probably accomplished decreases to approximately $R = 1.2$ bps. Nevertheless, the source is able to more probably establish secure communication with the destination until the rate $R = 2.3$ bps when there exists cooperative jamming. At rates greater than this rate, negative effects of cooperative jamming harm the destination as well as the eavesdropper and so the advantage of the cooperative jamming dissappears.

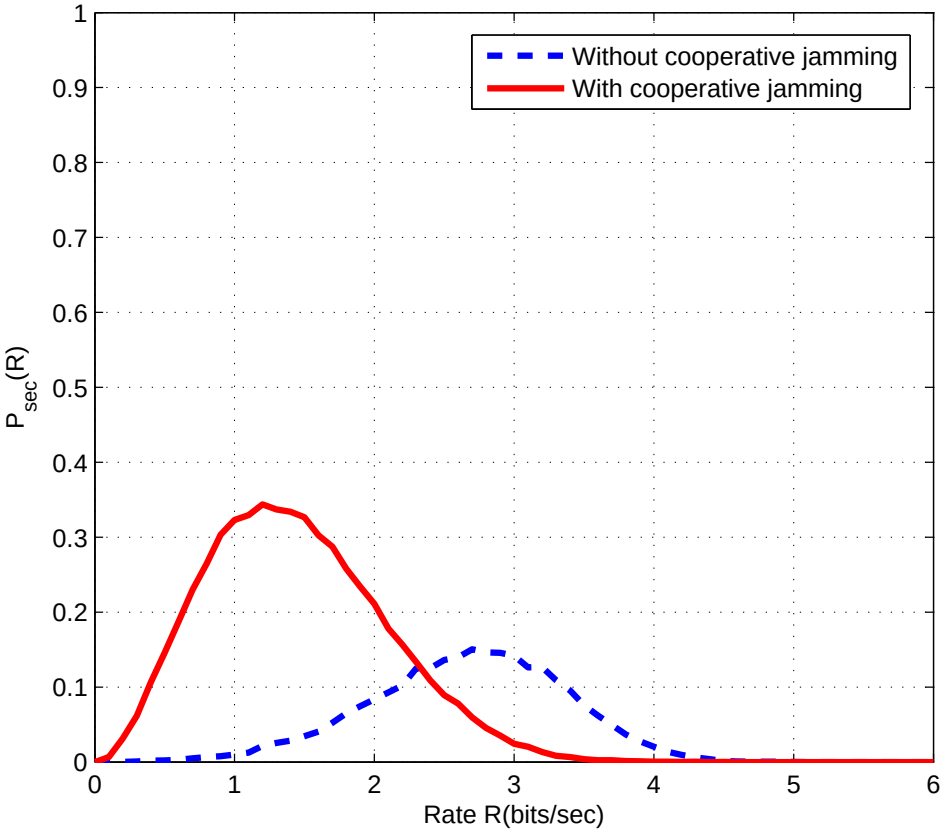

Figure 3.4: The effect of the cooperative jamming with largest minimum selection on $P_{sec}(R)$

The other simulation which is depicted in Fig. 3.5 investigates the effect of cooperative jamming on the probabilities $P_D(R)$ and $P_E(R)$. As observed, while the prob-

ability $P_D(R)$ of the event A_D without cooperative jamming begins to decline at the rate $R = 1.1\ bps$, it begins to decrease at the rate $R = 0.3\ bps$ when there is cooperative jamming. As expected, the cooperative jamming inhibits the destination as well as the eavesdropper. Hence, the probability $P_D(R)$ of the event A_D with cooperative jamming is always smaller than the probability $P_D(R)$ without cooperative jamming. Futhermore, the other outcome of the simulation in Fig. 3.5 is the comparison of the probabilities $P_E(R)$ of the combined event A_E with and without the cooperative jamming. As shown in the graph, in the scenario with cooperative jamming, the probability $P_E(R)$ increases faster compared to the scenario without cooperative jamming. Since there exists a noise signal applied on the eavesdropper in both phases of the communication, the received SINR values at the eavesdropper are corrupted and even at small rates R, the probability $P_E(R)$ with cooperative jamming is always higher than that without cooperative jamming.

It is significant to note that the event A_D encloses the trials in which the eavesdropper is able to decode the source message signal in any phase or in both phases as defined in Section 3.2. Therefore, attempting to infer any knowledge about the secrecy from the probability $P_D(R)$ is not very meaningful. Nonetheless, the behavior of $P_D(R)$ is helpful to examine the damaging effects of cooperative jamming on the destination. Moreover, the event A_E includes the cases where the destination cannot decode the source message signal. Hence, a high $P_E(R)$ does not give any information about whether the communication between the source and the destination is achieved. On the other hand, it presents at least how much the message signals transmitted by the source and the communicating relay are blocked at the eavesdropper regardless of the situation of the communication between the source and the destination.

3.5.2 The Effect of Relay Selection

In the previous Section 3.5.1, the maximum value of $P_{sec}(R)$ of the source is 0.34, which is smaller than even 0.5. Especially, for tactical networks, this value of $P_{sec}(R)$ is fairly low. We will check the best possible performance by a non-realistic method. In this new method which is called the genie-aided selection, it assumed that all the channel gains including the eavesdroper's ones are known by all the nodes in the

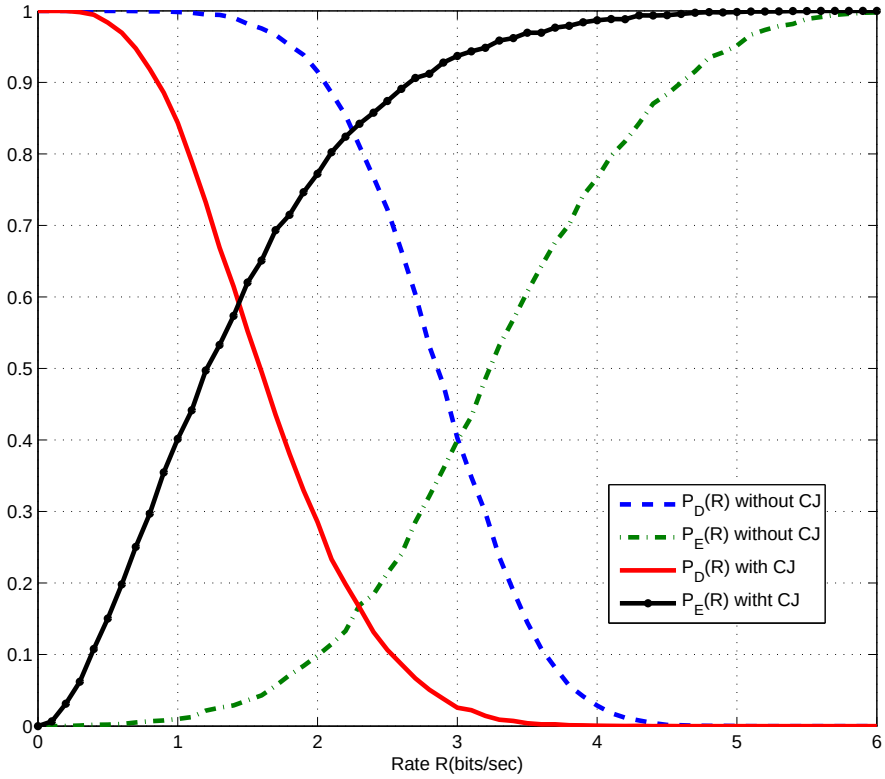

Figure 3.5: The effect of the cooperative jamming (CJ) with largest minimum selection on $P_D(R)$ and $P_E(R)$

network. In the genie-aided selection, the algorithm controls whether the event A_{sec} occurs or not at a fixed rate R for different relay configurations which consist of a communicating relay and two noise emitting relays. One of the emitting relays is for the first phase of the transmission and the other is for the second phase. Similarly, the relay configuration is constituted from 5 relays. At a fixed rate R, the relay configuration which makes the indicator function $I(A_{sec}) = 1$ is selected in each independent trial if it exists. Moreover, a different set of channel gains are used in each trial. The process is repeated for $N = 10000$ trials at a fixed rate R. At the end of the trials, $P_{sec}(R)$ is evaluated by using equation (3.17). For a required range of rate R, the calculation of $P_{sec}(R)$ is recurred and at the end, the probability $P_{sec}(R)$ vs rate R is drawn.

First of all, $P_{sec}(R)$ with genie-aided selection is contrasted according to the existence

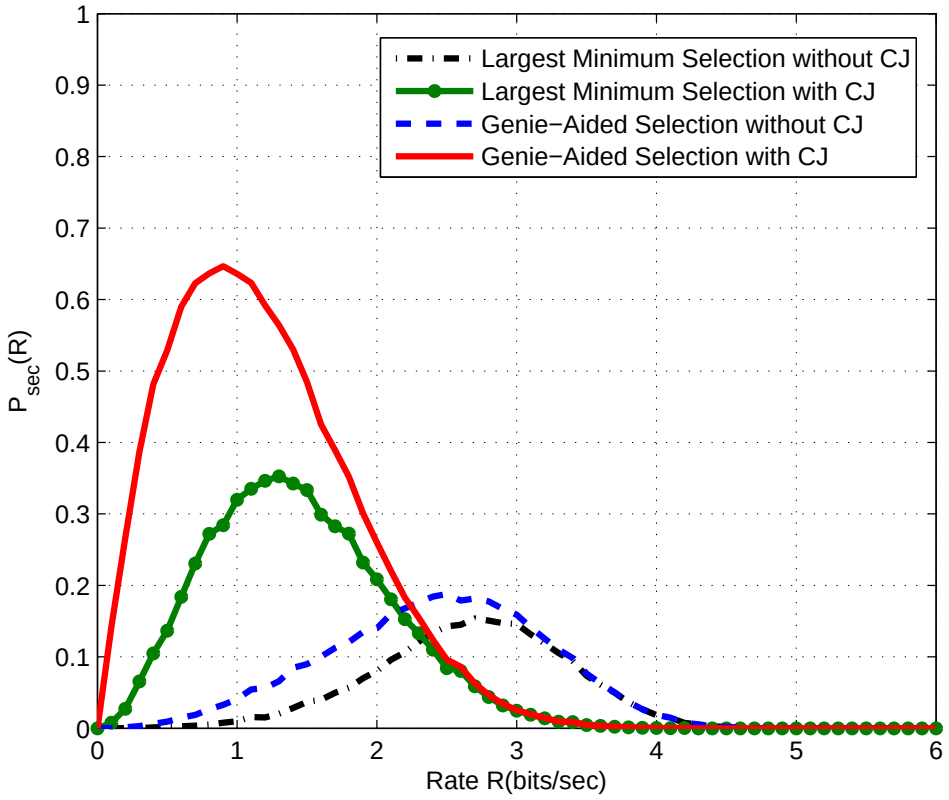

Figure 3.6: The effect of the relay selection method on the probability $P_{sec}(R)$

of the cooperative jamming in the simulation which is depicted in Fig. 3.6. Similar to the largest minimum selection, when the cooperative jamming is taken into account, the maximum value of $P_{sec}(R)$ rises in genie-aided selection. Hence, it is significant to state that the source can securely communicate with the destination more probably at lower rates compared to the case without cooperative jamming. Furthermore, the largest minimum selection and the genie-aided selection algorithms are compared in terms of the $P_{sec}(R)$ in Fig. 3.6. The genie-aided selection outperforms the largest minimum selection regardless of the existence of cooperative jamming at each rate R. In the case with cooperative jamming, while the maximum probability $P_{sec}(R)$ is just 0.34 for the largest minimum selection, it is 0.65 for the genie-aided selection. In fact, the knowledge about the eavesdropper's channel gains in the latter selection results in this probability difference. Since it is assumed that the eavesdropper's channels h_{SE}, h_{R_cE} and h_{R_iE} are known by all the nodes, they are used in the selection of the

communicating and noise emitting relays. For this reason, the most convenient relay configuration which makes the event A_{sec} occur can be chosen in the genie-aided selection algorithm. This results in an increment in the number of occurrence of the event A_{sec} and so in the probability $P_{sec}(R)$.

The genie-aided selection effectively improved the probability of secure communication $P_{sec}(R)$ between the source and the destination compared to the largest minimum selection. However, it is not very practical to be used since it is not realistic to always know the gains of the eavesdropper's channels. The eavesdroppers in the network may be passive. In other words, they do not have to emit any signal. They may only listen. Thus, their locations and channel gains may be unknown. In fact, even if the eavesdroppers are active nodes, their channel gains may not be determined by the other nodes in the network. Moreover, the maximum value of the probability $P_{sec}(R)$ and the related communication rate R with genie-aided selection are still low especially for the tactical cooperative networks. For these reasons, multiple antennas will be utilized to enhance secrecy.

CHAPTER 4

COOPERATIVE JAMMING METHOD WITH MULTIPLE-ANTENNA NODES

4.1 Cooperative Jamming Method with Multiple-Antennas

In concept of secret cooperative communication for cooperative networks, the source requires to communicate with the intended destination without the eavesdroppers' being able to decode the secret source message signal. To obtain the secrecy in cooperative networks, it is demanded to make the eavesdroppers' channels noisier than the channel of the destination. For this reason, the cooperative jamming method was presented for the cooperative networks with single-antenna nodes to achieve this statement in Chapter 3. However, the noise signals transmitted by the noise emitting relays corrupted the received signals at not only the eavesdropper but also the intended receivers: the communicating relay and the destination. By intelligently selecting the relays in different relay selection algorithms, the probability $P_{sec}(R)$ was inclined at low rates R. Nonetheless, the results were not very fulfilling in terms of both $P_{sec}(R)$ and related rates R. For these reasons, utilization of the multiple antennas is recommended for the nodes in the cooperative network to develop both the probability $P_{sec}(R)$ and the communication rate R. It is aimed to improve the rate R benefiting from the space diversity created by the multiple antennas. Moreover, it is intended to increase $P_{sec}(R)$ to satisfactory levels by minimizing, even nullifying the destroying effects of the emitted noise signals on the legitimate receivers with the help of adaptive noise generation. In this chapter, firstly the signal model will be presented for the cooperative networks with multiple-antenna nodes when there exists

cooperative jamming. Furthermore, numerical results will be examined to display the effects of adaptive transmit precoding at the source and communicating relay, number of antennas and adaptive noise generation on $P_{sec}(R)$ and the communication rate R.

4.2 Signal Model

In this section, the signal model is very similar to the model given in Section 3.2. The assumptions are the same. Similarly, the noise emitting relay is used to broadcast the noise to the eavesdropper and the selected communicating relay is used to help the communication. Distinctly, the nodes of the cooperative network (a source, a destination, a communicating relay, a noise emitting relay and an eavesdropper) have L antennas as in Fig. 4.1 and 4.2 where $L > 1$.

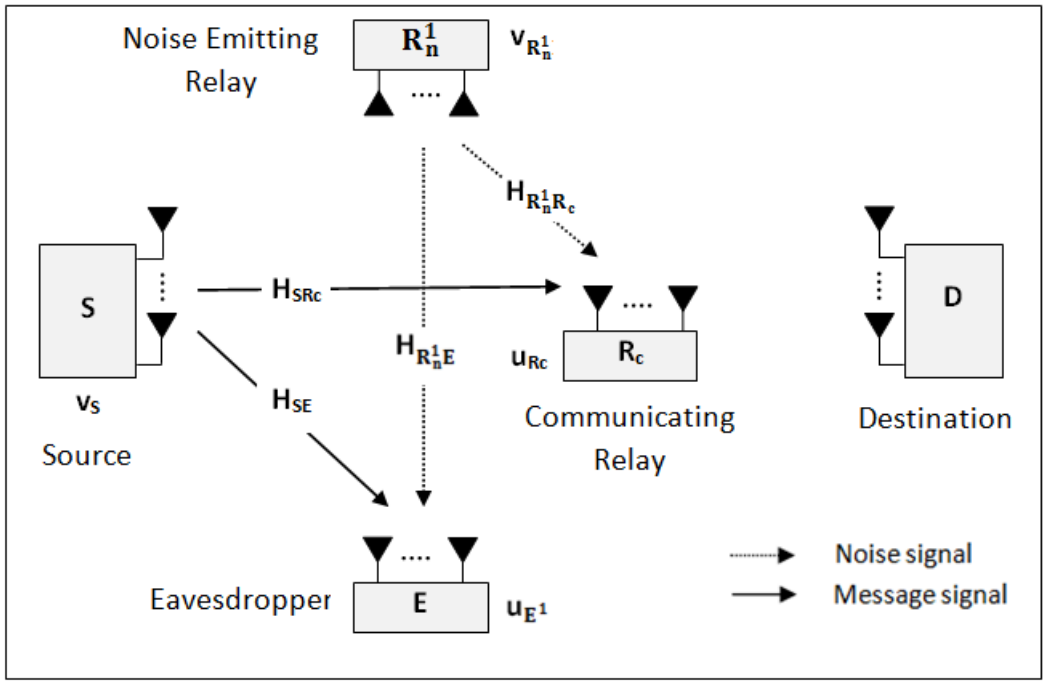

Figure 4.1: The cooperative network with multiple-antenna nodes in the first phase

In the first phase of communication which is displayed in Fig. 4.1, the L-dimensional message and noise signal vectors $\mathbf{x_T}$ and $\mathbf{x_{R_n^1}}$ are transmitted by the source and the selected noise emitting relay R_n^1 respectively. These transmitted signal vectors with

energy E_b are defined as

$$\mathbf{x_T} = \sqrt{E_b}\mathbf{v_S} \cdot m \tag{4.1a}$$

$$\mathbf{x_{R_n^1}} = \sqrt{E_b}\mathbf{v_{R_n^1}} \cdot w_{R_n^1} \tag{4.1b}$$

where $\mathbf{v_S}$ and $\mathbf{v_{R_n^1}}$ are the L-dimensional transmit precoding vectors with unit energy at the source and the noise emitting relay R_n^1 respectively, m and $w_{R_n^1}$ are the message and noise signals with unit energy. In the following section, all the transmit precoding vectors will be appropriately adjusted for the best communication performance.

The signals y_{R_c} and y_{E^1} are received by the selected communicating relay and the eavesdropper respectively. These signals are expressed as

$$y_{R_c} = \mathbf{u_{R_c}^H}\left(\mathbf{H_{SR_c}x_T} + \mathbf{H_{R_n^1R_c}x_{R_n^1}} + \mathbf{z_{R_c}}\right) \tag{4.2a}$$

$$y_{E^1} = \mathbf{u_{E^1}^H}\left(\mathbf{H_{SE}x_T} + \mathbf{H_{R_n^1E}x_{R_n^1}} + \mathbf{z_{E^1}}\right) \tag{4.2b}$$

where $\mathbf{u_{R_c}}$ and $\mathbf{u_{E^1}}$ are the L-dimensional receiver shaping vectors with unit energy at the communicating relay and eavesdropper respectively, $\mathbf{H_{SR_c}}$ and $\mathbf{H_{SE}}$ are $L \times L$ channel gain matrices of the links from the source to the communicating relay and eavesdropper respectively, $\mathbf{H_{R_n^1R_c}}$ and $\mathbf{H_{R_n^1E}}$ are $L \times L$ channel gain matrices of the links from the noise emitting relay to the communicating relay and eavesdropper respectively, the white noise terms $\mathbf{z_{R_c}}$ and $\mathbf{z_{E^1}}$ have elements which are ZMCSCG random variables with variance N_0 [*]. In the following section, all the receiver shaping vectors will be set for the best communication performance. From (4.1a), (4.1b), (4.2a) and (4.2b),

$$y_{R_c} = \sqrt{E_b}\mathbf{u_{R_c}^H H_{SR_c} v_S} \cdot m + \sqrt{E_b}\mathbf{u_{R_c}^H H_{R_n^1R_c} v_{R_n^1}} \cdot w_{R_n^1} + \mathbf{u_{R_c}^H z_{R_c}} \tag{4.3a}$$

$$y_{E^1} = \sqrt{E_b}\mathbf{u_{E^1}^H H_{SE} v_S} \cdot m + \sqrt{E_b}\mathbf{u_{E^1}^H H_{R_{n_1}E} v_{R_n^1}} \cdot w_{R_n^1} + \mathbf{u_{E^1}^H z_{E^1}}. \tag{4.3b}$$

In eqn. (4.3a) and eqn. (4.3b), while the first terms include the source message, the other terms represent the noise. Thus, the SINR received by the communicating relay

[*] The superscript H parameter indicates Hermitian.

is expressed as

$$SINR_{R_c} = \frac{\mathbb{E}\left[|\sqrt{E_b}\mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{H}_{\mathbf{SR_c}}\mathbf{v}_{\mathbf{S}}\cdot m|^2\right]}{\mathbb{E}\left[|\sqrt{E_b}\mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R_n^1R_c}}\mathbf{v}_{\mathbf{R_n^1}}\cdot w_{R_n^1} + \mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{z}_{\mathbf{R_c}}|^2\right]} \tag{4.4a}$$

$$= \frac{E_b\left|\mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{H}_{\mathbf{SR_c}}\mathbf{v}_{\mathbf{S}}\right|^2}{E_b\left|\mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R_n^1R_c}}\mathbf{v}_{\mathbf{R_n^1}}\right|^2 + N_0} \tag{4.4b}$$

and the SINR received by the eavesdropper is given as

$$SINR_{E^1} = \frac{\mathbb{E}\left[|\sqrt{E_b}\mathbf{u}_{\mathbf{E^1}}^{\mathbf{H}}\mathbf{H}_{\mathbf{SE}}\mathbf{v}_{\mathbf{S}}\cdot m|^2\right]}{\mathbb{E}\left[|\sqrt{E_b}\mathbf{u}_{\mathbf{E^1}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R_{n_1}E}}\mathbf{v}_{\mathbf{R_n^1}}\cdot w_{R_n^1} + \mathbf{u}_{\mathbf{E^1}}^{\mathbf{H}}\mathbf{z}_{\mathbf{E^1}}|^2\right]} \tag{4.5a}$$

$$= \frac{E_b|\mathbf{u}_{\mathbf{E^1}}^{\mathbf{H}}\mathbf{H}_{\mathbf{SE}}\mathbf{v}_{\mathbf{S}}|^2}{E_b|\mathbf{u}_{\mathbf{E^1}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R_n^1E}}\mathbf{v}_{\mathbf{R_n^1}}|^2 + N_0}. \tag{4.5b}$$

Accordingly, the capacity of the eavesdropper's channel is expressed as

$$C_{R_c} = log_2(1 + SINR_{R_c}) \tag{4.6a}$$

$$= log_2\left(1 + \frac{E_b|\mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{H}_{\mathbf{SR_c}}\mathbf{v}_{\mathbf{S}}|^2}{E_b|\mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R_n^1R_c}}\mathbf{v}_{\mathbf{R_n^1}}|^2 + N_0}\right) \tag{4.6b}$$

from eqn. (4.4b) and the capacity of the eavesdropper's channel is expressed as

$$C_{E^1} = log_2(1 + SINR_{E^1}) \tag{4.7a}$$

$$= log_2\left(1 + \frac{E_b|\mathbf{u}_{\mathbf{E^1}}^{\mathbf{H}}\mathbf{H}_{\mathbf{SE}}\mathbf{v}_{\mathbf{S}}|^2}{E_b|\mathbf{u}_{\mathbf{E^1}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R_n^1E}}\mathbf{v}_{\mathbf{R_n^1}}|^2 + N_0}\right) \tag{4.7b}$$

from eqn. (4.5b).

In the second phase which is shown in Fig. 4.2, the signal transmitted by the communicating relay is

$$\mathbf{x}_{\mathbf{R_c}} = \sqrt{E_b}\mathbf{v}_{\mathbf{R_c}}\alpha_R y_{R_c} \tag{4.8a}$$

$$= \sqrt{E_b}\alpha_R\mathbf{v}_{\mathbf{R_c}}\left(\sqrt{E_b}\mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{H}_{\mathbf{SR_c}}\mathbf{v}_{\mathbf{S}}\cdot m + \sqrt{E_b}\mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R_n^1R_c}}\mathbf{v}_{\mathbf{R_n^1}}\cdot w_{R_n^1} + \mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{z}_{\mathbf{R_c}}\right) \tag{4.8b}$$

from eqn. (4.3a) where $\mathbf{v}_{\mathbf{R_c}}$ is the L-dimensional transmit precoding vector with unit energy at the communicating relay. In order to set $\mathbb{E}\left[|\mathbf{x}_{\mathbf{R_c}}|^2\right] = E_b$, the coefficient α_R of the AF method is described as

$$\alpha_R = \frac{1}{\sqrt{\mathbb{E}\left[|y_{R_c}|^2\right]}} \tag{4.9}$$

$$= \frac{1}{\sqrt{E_b|\mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{H}_{\mathbf{SR_c}}\mathbf{v}_{\mathbf{S}}|^2 + E_b|\mathbf{u}_{\mathbf{R_c}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R_n^1R_c}}\mathbf{v}_{\mathbf{R_n^1}}|^2 + N_0}}. \tag{4.10}$$

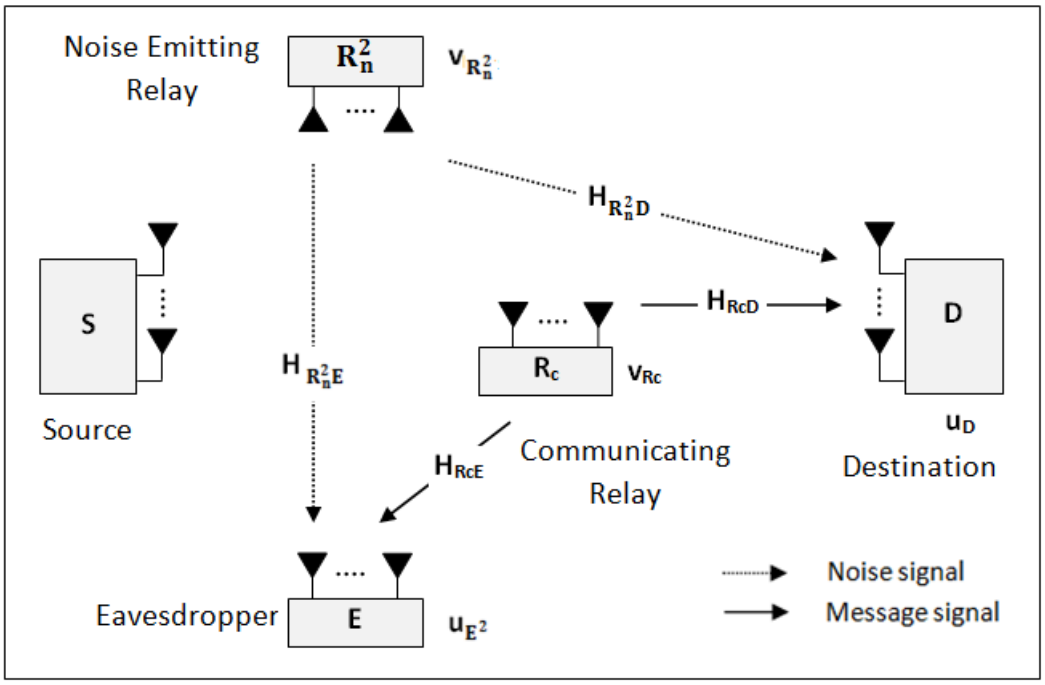

Figure 4.2: The cooperative network with multiple-antenna nodes in the second phase

from eqn. (4.3a). The noise signal broadcasted by the second phase's noise emitting relay is also expressed as

$$\mathbf{x}_{\mathbf{R_n^2}} = \sqrt{E_b}\mathbf{v}_{\mathbf{R_n^2}} w_{R_n^2} \tag{4.11}$$

where $\mathbf{v}_{\mathbf{R_n^2}}$ is the L-dimensional transmit precoding vector with unit energy at the noise communicating relay, $w_{R_n^2}$ is the noise signal with unit energy. Furthermore, the signals y_D and y_{E^2} which are received by the destination and the eavesdropper in the second phase respectively are defined as

$$y_D = \mathbf{u_D^H}(\mathbf{H}_{\mathbf{R_c D}}\mathbf{x}_{\mathbf{R_C}} + \mathbf{H}_{\mathbf{R_n^2 D}}\mathbf{x}_{\mathbf{R_n^2}} + \mathbf{z_D}) \tag{4.12a}$$

$$y_{E^2} = \mathbf{u_{E^2}^H}(\mathbf{H}_{\mathbf{R_c E}}\mathbf{x}_{\mathbf{R_C}} + \mathbf{H}_{\mathbf{R_n^2 E}}\mathbf{x}_{\mathbf{R_n^2}} + \mathbf{z}_{\mathbf{E^2}}) \tag{4.12b}$$

where $\mathbf{u_D}$ and $\mathbf{u}_{\mathbf{E^2}}$ are the L-dimensional receiver shaping vectors with unit energy at the destination and eavesdropper respectively, $\mathbf{H}_{\mathbf{R_c D}}$ and $\mathbf{H}_{\mathbf{R_c E}}$ are the $L \times L$ channel gain matrices of the links from the communicating relay to the destination and eavesdropper respectively, $\mathbf{H}_{\mathbf{R_n^2 D}}$ and $\mathbf{H}_{\mathbf{R_n^2 E}}$ are the $L \times L$ channel gain matrices of the links from the noise emitting relay to the destination and eavesdropper respectively, the white noise terms $\mathbf{z_D}$ and $\mathbf{z}_{\mathbf{E^2}}$ have elements which are ZMCSCG random variables

with variance N_0. From (4.8b),(4.11) and (4.12a),

$$\begin{aligned} y_D =& E_b\alpha_R \mathbf{u_D^H H_{R_cD} v_{R_c} u_{R_c}^H H_{SR_c} v_S} \cdot m + E_b\alpha_R \mathbf{u_D^H H_{R_cD} v_{R_c} u_{R_c}^H H_{R_n^1R_c} v_{R_n^1}} \cdot w_{R_n^1} \\ &+ \sqrt{E_b}\alpha_R \mathbf{u_D^H H_{R_cD} v_{R_c} u_{R_c}^H z_{R_c}} + \sqrt{E_b}\mathbf{u_D^H H_{R_n^2D} v_{R_n^2}} w_{R_n^2} + \mathbf{u_D^H z_D} \end{aligned} \tag{4.13}$$

In eqn. (4.13) the only first term includes the source message and the other terms is composed of the noise. Therefore, the SINR received by the destination is

$$SINR_D = \frac{E_b^2\alpha_R^2 |\mathbf{u_D^H H_{R_cD} v_{R_c} u_{R_c}^H H_{SR_c} v_S}|^2}{E_b^2\alpha_R^2 |\mathbf{u_D^H H_{R_cD} v_{R_c} u_{R_c}^H H_{R_n^1R_c} v_{R_n^1}}|^2 + E_b\alpha_R^2 \|\mathbf{u_D^H H_{R_cD} v_{R_c} u_{R_c}^H}\|^2 N_0 + E_b |\mathbf{u_D^H H_{R_n^2D} v_{R_n^2}}|^2 + N_0}. \tag{4.14}$$

Moreover, from (4.8b),(4.11) and (4.12b),

$$\begin{aligned} y_{E^2} =& E_b\alpha_R \mathbf{u_{E^2}^H H_{R_cE} v_{R_c} u_{R_c}^H H_{SR_c} v_S} \cdot m + E_b\alpha_R \mathbf{u_{E^2}^H H_{R_cE} v_{R_c} u_{R_c}^H H_{R_{n1}R_c} v_{R_n^1}} \cdot w_{R_n^1} \\ &+ \sqrt{E_b}\alpha_R \mathbf{u_{E^2}^H H_{R_cE} v_{R_c} u_{R_c}^H z_{R_c}} + \sqrt{E_b}\mathbf{u_{E^2}^H H_{R_n^2E} v_{R_n^2}} w_{R_n^2} + \mathbf{u_{E^2}^H z_{E^2}}. \end{aligned} \tag{4.15}$$

In eqn. (4.15), the only first term includes the source message and the other terms consists of only the noise. Therefore, the SINR received by the eavesdropper is

$$SINR_{E^2} = \frac{E_b^2\alpha_R^2 |\mathbf{u_{E^2}^H H_{R_cE} v_{R_c} u_{R_c}^H H_{SR_c} v_S}|^2}{E_b^2\alpha_R^2 |\mathbf{u_{E^2}^H H_{R_cE} v_{R_c} u_{R_c}^H H_{R_{n1}R_c} v_{R_n^1}}|^2 + E_b\alpha_R^2 \|\mathbf{u_{E^2}^H H_{R_cE} v_{R_c} u_{R_c}^H}\|^2 N_0 + E_b |\mathbf{u_{E^2}^H H_{R_n^2E} v_{R_n^2}}|^2 + N_0}. \tag{4.16}$$

Thus, in the second phase, the capacity expressions for the destination and eavesdropper's channels are expressed as

$$C_D = log_2(1 + SINR_D) \tag{4.17a}$$

$$C_{E^2} = log_2(1 + SINR_{E^2}) \tag{4.17b}$$

respectively.

4.3 Transmit Precoding and Receiver Shaping

Transmit precoding and receiver shaping vectors introduce a transformation on the input and output of channels between multiple-antenna nodes as shown in Fig 4.3.

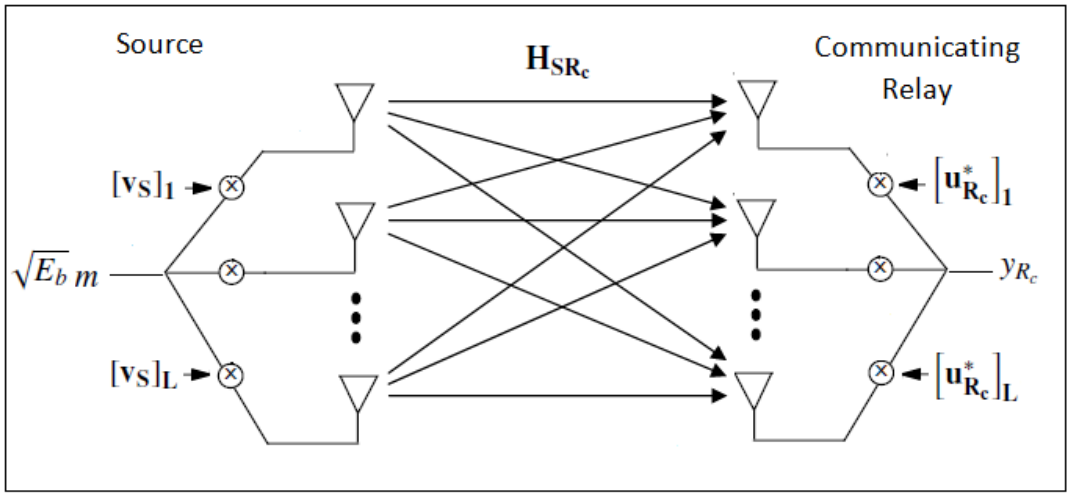

Figure 4.3: Transmit precoding and receiver shaping vectors on multiple-antenna nodes

The proper adjustment of transmit precoding and receiver shaping vectors has a significant role improving the communication performance of these nodes since these vectors can provide diversity and array gain through coherent combining of multiple signal paths [1]. In the first phase of communication, the transmit precoding vector $\mathbf{v_S}$ at the source and the receiver shaping vector $\mathbf{u_{R_c}}$ at the communicating relay should be properly defined to maximize the SINR at the communicating relay. While $\mathbf{v_S}$ determines transmitted signal power allocation at the multiple antennas of the source, $\mathbf{u_{R_c}}$ is significant for coherent combining of multiple signal paths at the communicating relay. As displayed in Fig. 4.3, the message signal m is sent over the ith antenna of the source with weight $[\mathbf{v_S}]_\mathbf{i}$. Similarly, the signal received by the ith antenna of the communicating relay is weighted by $\left[\mathbf{u}^*_{\mathbf{R_c}}\right]_\mathbf{i}$. Since it is assumed that the channel gain matrices except the eavesdropper's ones are known by the source, destination and all relays in the network, they can be used to assign the best $\mathbf{v_S}$ and $\mathbf{u_{R_c}}$ vectors. The received SINR at the communicating relay is maximized by selecting $\mathbf{v_S}$ and $\mathbf{u_{R_c}}$ as the principal right and left singular vectors of the channel gain matrix $\mathbf{H_{SR_c}}$ respectively. The principal right and left singular vectors are extracted from the singular value decomposition (SVD) of channel gain matrix $\mathbf{H_{SR_c}}$ which is expressed as

$$\mathbf{H_{SR_c}} = \mathbf{U_{R_c}} \mathbf{\Sigma_{SR_c}} \mathbf{V_S^H} \tag{4.18}$$

where $\mathbf{U_{R_c}}$ and $\mathbf{V_S}$ are $L \times L$ unitary matrices and $\mathbf{\Sigma_{SR_c}}$ is an $L \times L$ diagonal matrix of singular values of $\mathbf{H_{SR_c}}$ in decreasing order. Accordingly, the principal right and left singular vectors of the channel gain matrix $\mathbf{H_{SR_c}}$ are defined as the first columns of the unitary matrices $\mathbf{V_S}$ and $\mathbf{U_{R_c}}$ respectively. Thus, the vectors $\mathbf{v_S}$ and $\mathbf{u_{R_c}}$ should be the first columns of $\mathbf{V_S}$ and $\mathbf{U_{R_c}}$ respectively to generate the largest numerator of $SINR_{R_c}$ which is defined in eqn. (4.4b). Hence, the expression of the numerator of $SINR_{R_c}$ becomes

$$SINR_{R_c} = \frac{E_b \left| \mathbf{u_{R_c}^H U_{R_c} \Sigma_{SR_c} V_S^H v_S} \right|^2}{E_b \left| \mathbf{u_{R_c}^H H_{R_n^1 R_c} v_{R_n^1}} \right|^2 + N_0} \tag{4.19}$$

from eqns. (4.4b) and (4.18).

Furthermore, the transmit precoding vector $\mathbf{v_{R_n^1}}$ at the noise emitting relay and the receiver shaping vector $\mathbf{u_{E^1}}$ should be defined to complete the calculation of received SINR values at the eavesdropper and communicating relay in the first phase. As for $\mathbf{v_{R_n^1}}$, $\mathbf{v_{R_n^1}}$ must be chosen as the principal right singular vector of the channel gain matrix $\mathbf{H_{R_n^1 E}}$ to maximally reduce the SINR at the eavesdropper. However, since it is assumed that the eavesdropper is a passive node, $\mathbf{H_{R_n^1 E}}$ is not known by the noise emitting relay. Therefore, $\mathbf{v_{R_n^1}}$ cannot be adjusted according to $\mathbf{H_{R_n^1 E}}$ and will be taken as

$$\mathbf{v_{R_n^1}} = \frac{\mathbf{1}}{\sqrt{L}} [\mathbf{1} \cdots \mathbf{1}]^{\mathbf{T}} \tag{4.20}$$

for simplicity in the simulations. However, the eavesdropper itself may have knowledge about its channel gain matrices $\mathbf{H_{SE}}$ and $\mathbf{H_{R_n^1 E}}$ in the first phase. Since it requires to maximize the reception of message signal transmitted by the source, it can calculate its receiver shaping vector $\mathbf{u_{E^1}}$ from the SVD of $\mathbf{H_{SE}}$. This improves $SINR_{E^1}$ which is expressed in eqn. (4.5b) to a degree. On the other hand, since the transmit precoding vector $\mathbf{v_S}$ at the source is calculated according to the channel gain matrix $\mathbf{H_{SR_c}}$, $SINR_{E^1}$ cannot be maximized by the eavesdropper. Hence, this is an advantage of the communicating relay against the eavesdropper in the first phase.

Similar to the first phase, the transmit precoding vector $\mathbf{v_{R_c}}$ at the communicating relay and the receiver shaping vector $\mathbf{u_D}$ at the destination should be appropriately assigned to maximize the SINR at the destination as for the second phase of communication. Similarly, the signal is sent over the ith antenna of the communicating

relay with weight $[\mathbf{v_{R_c}}]_\mathbf{i}$ and the signal received by the ith antenna of the destination is weighted by $\left[\mathbf{u_D^*}\right]_\mathbf{i}$. Since the knowledge about the channel gain matrix $\mathbf{H_{R_cD}}$ is assumed to exist at both communicating relay and destination, $\mathbf{v_{R_c}}$ and $\mathbf{u_D}$ can be calculated based on $\mathbf{H_{R_cD}}$. The numerator of $SINR_D$ is maximized by choosing $\mathbf{v_{R_c}}$ and $\mathbf{u_D}$ as the principal right and left singular vectors of $\mathbf{H_{R_cD}}$ respectively. Hence, the singular value decomposition (SVD) of $\mathbf{H_{R_cD}}$ which is defined as

$$\mathbf{H_{R_cD}} = \mathbf{U_D}\mathbf{\Sigma_{R_cD}}\mathbf{V_{R_c}^H} \tag{4.21}$$

is applied to determine the $L \times L$ unitary matrices $\mathbf{V_{R_c}}$ and $\mathbf{U_D}$ and the diagonal matrix $\mathbf{\Sigma_{R_cD}}$ of singular values of $\mathbf{H_{R_cD}}$. Therefore, $\mathbf{v_{R_c}}$ and $\mathbf{u_D}$ are chosen as the first columns of $\mathbf{V_{R_c}}$ and $\mathbf{U_D}$ respectively to maximize the numerator of $SINR_D$ which is defined in eqn. (4.14). Thus, the numerator of $SINR_D$ changes into

$$SINR_D = \frac{E_b^2\alpha_R^2|\mathbf{u_D^H}\mathbf{U_D}\mathbf{\Sigma_{R_cD}}\mathbf{V_{R_c}^H}\mathbf{v_{R_c}}\mathbf{u_{R_c}^H}\mathbf{U_{R_c}}\mathbf{\Sigma_{SR_c}}\mathbf{V_S^H}\mathbf{v_S}|^2}{E_b^2\alpha_R^2|\mathbf{u_D^H}\mathbf{H_{R_cD}}\mathbf{v_{R_c}}\mathbf{u_{R_c}^H}\mathbf{H_{R_n^1R_c}}\mathbf{v_{R_n^1}}|^2 + E_b\alpha_R^2\|\mathbf{u_D^H}\mathbf{H_{R_cD}}\mathbf{v_{R_c}}\mathbf{u_{R_c}^H}\|^2N_0 + E_b|\mathbf{u_D^H}\mathbf{H_{R_n^2D}}\mathbf{v_{R_n^2}}|^2 + N_0} \tag{4.22}$$

from eqns. (4.14), (4.18) and (4.21).

Finally, the transmit precoding vector $\mathbf{v_{R_n^2}}$ at the noise emitting relay and the receiver shaping vector $\mathbf{u_{E^2}}$ should be determined to implement the calculations of received SINR values at the eavesdropper and destination in the second phase. It is assumed that the eavesdropper is a passive node, the knowledge about $\mathbf{H_{R_n^2E}}$ does not exist at the noise emitting relay. Therefore, $\mathbf{v_{R_n^2}}$ cannot be calculated according to $\mathbf{H_{R_n^2E}}$ and will be taken as

$$\mathbf{v_{R_n^2}} = \frac{\mathbf{1}}{\sqrt{L}}[\mathbf{1}\cdots\mathbf{1}]^\mathbf{T} \tag{4.23}$$

for simplicity in the simulations. In addition, the receiver shaping vector $\mathbf{u_{E^2}}$ is found from SVD of $\mathbf{H_{R_cE}}$ similar to $\mathbf{u_{E^1}}$ in the first phase.

4.4 Relay Selection Mechanism

The selection of relays constitute a significant step as in the simulations of the cooperative networks with single-antenna nodes in Section 3.5. The rules for the selection

of the communicating relay and the noise emitting relays are mainly based on channel gains. Therefore, the first assumption is that all of the channel gains except the eavesdropper's channel gains are known by the source and relays. Since the eavesdroppers are accepted as the passive nodes in this thesis, it is not realistic to know their channel state information, but they may have their own CSI. Like the largest minimum selection in Section 3.5, the communicating relay R_c is chosen at the beginning among five different relays in the network. For simplicity, the communicating relay is chosen according to the capacity of the destination C_D when there is no cooperative jamming. Hence, the terms of the noise signals from the noise emitting relays in the denominator of $SINR_D$ disappear. Therefore, the new SINR expressions are defined as

$$\overline{SINR_D} = \frac{E_b^2 \alpha_R^2 \left| \mathbf{u_D^H H_{R_cD} v_{R_c} u_{R_c}^H H_{SR_c} v_S} \right|^2}{E_b \alpha_R^2 \| \mathbf{u_D^H H_{R_cD} v_{R_c} u_{R_c}^H} \|^2 N_0 + N_0} \tag{4.24a}$$

$$\overline{C_D} = log_2 \left(1 + \frac{E_b^2 \alpha_R^2 \left| \mathbf{u_D^H H_{R_cD} v_{R_c} u_{R_c}^H H_{SR_c} v_S} \right|^2}{E_b \alpha_R^2 \| \mathbf{u_D^H H_{R_cD} v_{R_c} u_{R_c}^H} \|^2 N_0 + N_0} \right) \tag{4.24b}$$

from eqn. (4.14) and eqn.(4.17a) respectively. The relay which satisfies

$$R_c = \underset{R_i}{\operatorname{argmax}} \, \overline{C_D} \tag{4.25}$$

is selected as the communicating relay. Therefore, the relays which have worse channel gains are eliminated. Afterwards, the noise emitting relays R_n^1 and R_n^2 which broadcast the noise signals in the first and the second phases of communication respectively are selected. In the first phase, the communicating relay is required to be minimally affected by the noise emitting relay. This is achieved by keeping the denominator of the $SINR_{R_c}$ minimum. For this reason, the interference term $\left| \mathbf{u_{R_c}^H H_{R_iR_c} v_{R_i}} \right|^2$ from the denominator of eqn. (4.4b) is calculated. Hence, the noise emitting relay R_n^1 is selected as

$$R_n^1 = \underset{R_i \neq R_c}{\arg\min} \left| \mathbf{u_{R_c}^H H_{R_iR_c} v_{R_i}} \right|^2 . \tag{4.26}$$

Hence, the negative effect of the noise signal on the communicating relay R_c decreases in the first phase of communication. Furthermore, the destination is required to be least influenced by the noise emitting relay in the second phase. Thus, the denominator of the $SINR_D$ should be kept as small as possible. For this reason, the

interference term $\left|\mathbf{u_D^H H_{R_iD} v_{R_i}}\right|^2$ from the denominator of eqn. (4.14) is calculated. Hence, the noise emitting relay R_n^2 is selected as

$$R_n^2 = \arg\min_{R_i \neq R_c} \left|\mathbf{u_D^H H_{R_iD} v_{R_i}}\right|^2 . \tag{4.27}$$

Therefore, the loss of the SINR at the destination due to the noise signal of the noise emitting relay is minimized in the second phase of communication.

4.5 Numerical Results

There are several critical decisions and selections which directly affect the probability of secure communication $P_{sec}(R)$ in the cooperative networks with multiple-antenna nodes. In the simulations, the adaptive selections and appropriate decisions may dramatically improve the communication performance. The important ones of them were explained in Sections 4.3 and 4.4.

There are several parameters which must be adjusted to implement the simulations similar to the simulations of cooperative networks with single-antenna nodes in Section 3.5. Firstly, the value of average SNR= E_b/N_0 must be assigned. Similarly, the average SNR values at the source, the communicating relay R_c and the noise emitting relays R_n^1 and R_n^2 are the same and in all simulations in this chapter will be taken as 10 dB. Moreover, the behaviors of probabilities $P_{sec}(R)$, $P_D(R)$ and $P_E(R)$ which are expressed in eqns. (3.17), (3.20a) and (3.20b) respectively will be examined under different situations in the following simulations. The number of trials N which is used in the calculations of these probabilities will be taken as 10000 for convenience. The number of trials $N = 10000$ is sufficiently large for our purposes here as observed from the smoothness of the produced curves. In each trial, different independent set of channel gain matrices will be used. The channel gains are assumed to be ZMCSCG random variables with variance 1.

4.5.1 The Effect of Adaptive Transmit Precoding

In this section, it is aimed to compare two cases in which the transmit precoding vectors at the source and communicating relay are selected in different ways and to

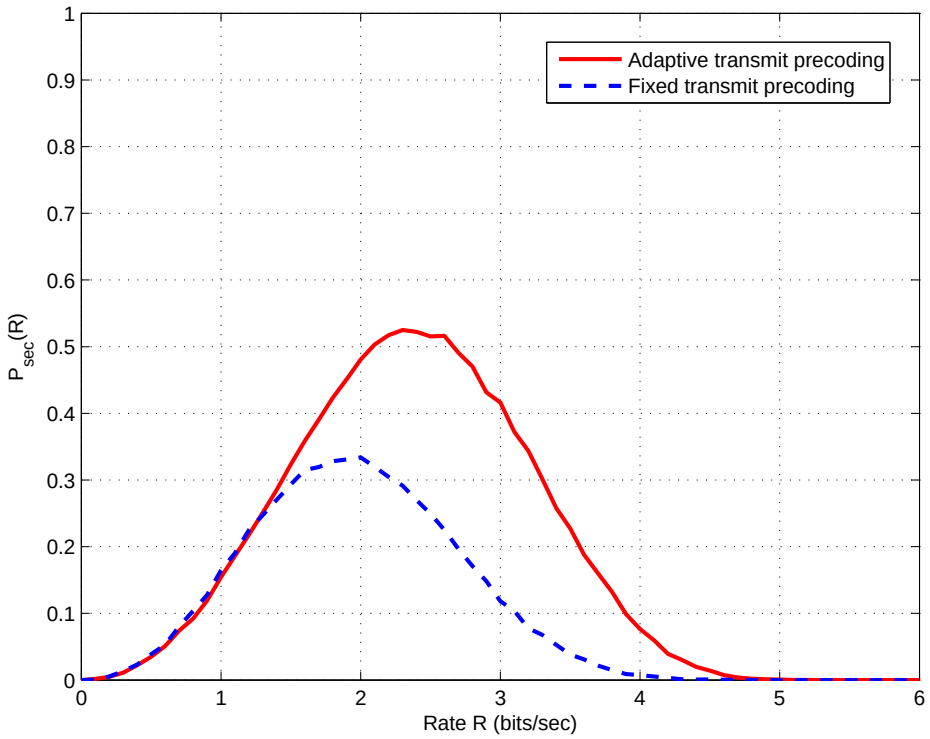

Figure 4.4: The effect of adaptive transmit precoding at source and communicating relay ($E_b/N_0 = 10$ dB,$L = 2$)

observe their effects on the probability $P_{sec}(R)$ and rate R when there exists cooperative jamming. The first one is the case where the transmit precoding vectors are adaptively adjusted according to the related channel gain matrices. As indicated in Section 4.3, the vector $\mathbf{v_S}$ at the source is calculated based on the channel gain matrix $\mathbf{H_{SR_c}}$ between the source and communicating relay in the first phase of transmission. Moreover, the vector $\mathbf{v_{R_c}}$ at the source is found according to the channel gain matrix $\mathbf{H_{R_cD}}$ between the communicating relay and the destination in the second phase. As for the other case, these transmit precoding vectors are not adaptively assigned. They are assumed to be fixed and defined as

$$\mathbf{v_S} = \frac{\mathbf{1}}{\sqrt{L}}[\mathbf{1}\cdots\mathbf{1}]^{\mathbf{T}} \tag{4.28a}$$

$$\mathbf{v_{R_c}} = \frac{\mathbf{1}}{\sqrt{L}}[\mathbf{1}\cdots\mathbf{1}]^{\mathbf{T}}. \tag{4.28b}$$

The comparison between these two different cases is displayed in Fig. 4.4 when the number antennas L equals 2. As observed in the graph, the case with adaptively ad-

justed transmit precoding vectors evidently outperforms the case with fixed transmit precoding vectors at all rates R in terms of the probability of secure communication $P_{sec}(R)$. It is important to indicate that adaptive selection of these vectors improves both maximum value of $P_{sec}(R)$ and the related rate R. Since the calculation of these vectors from the SVD of related channel gain matrices results in coherent combining of multiple signal components at the communicating relay and the destination, the received SINR values at these nodes ascend. For this reason, the maximum value of $P_{sec}(R)$ rises from 0.33 to 0.52 and the most probable rate R increases from 1.9 bps to 2.4 bps. Therefore, adaptive transmit precoding vectors will be used in all the following simulations.

4.5.2 The Effect of Number of Antennas

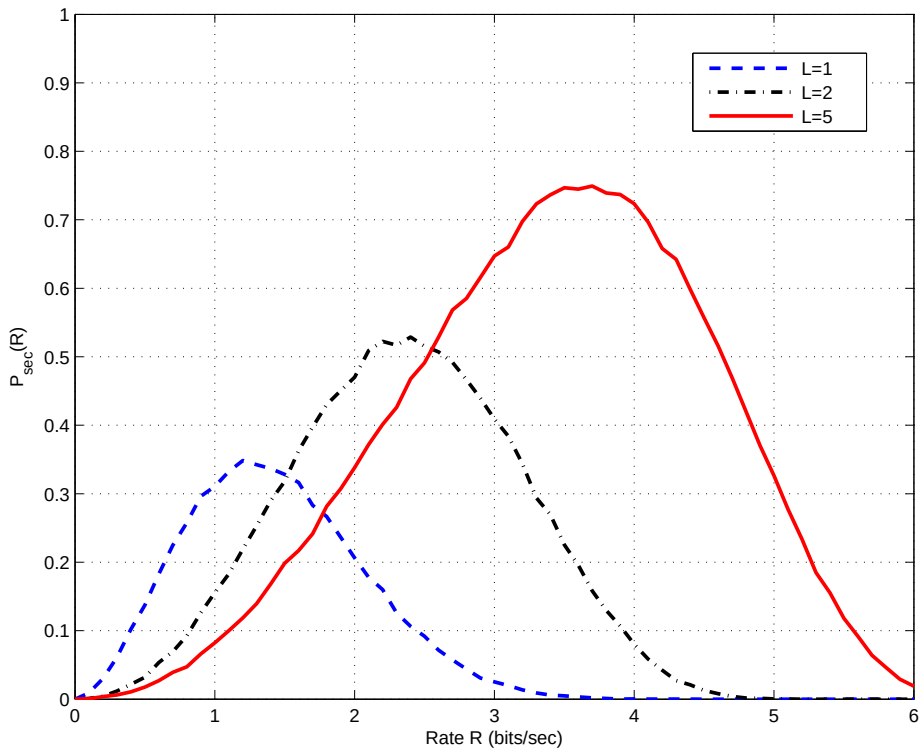

Figure 4.5: The effect of the number of antennas L (E_b/N_0 = 10 dB)

In this section, the issue is the number of antennas L at the source, destination, relays

and eavesdropper. The impact of increasing the number of antennas on the probability of secure communication $P_{sec}(R)$ is observed for $L = 1$, $L = 2$ and $L = 5$. As indicated in previous sections, L is accepted as the same at all these nodes for fairness. In the simulation which is depicted in Fig. 4.5, increasing the number of antennas L effectively develops the value of most probable rate R as expected. From $L = 1$ to $L = 5$, the rate with maximum $P_{sec}(R)$ rises from 1.2 bps to 3.7 bps. An increase in the number of the antennas results in a rise in the space diversity: the larger the number of antennas is, the higher the channel capacities become. Moreover, it is significant to note that while the most probable rate increases, the maximum value of $P_{sec}(R)$ also rises from 0.35 to 0.75 although the eavesdropper has the same number of antennas L. As the eavesdropper cannot coherently combine the multiple signal components from the source and the communicating relay, it cannot totally benefit from increasing the number of antennas. Therefore, an increase in L enhances the received SINR at the source and destination although the received SINR at the eavesdropper stays the same.

4.5.3 The Effect of Adaptive Noise Generation

In cooperative jamming, the noise signals broadcasted by the noise emitting relays inhibit not only the eavesdropper but also the legitimate receivers: the communicating relay and destination. Cooperative jamming which is used to decrease the SINR at the eavesdropper in both phases unintentionally results in an impairment at the SINR at legitimate receivers. In previous sections, this negative effect on them is reduced by intelligently selecting the noise emitting relay in both phases. However, this selection brings a restricted gain on the probability of secure communication $P_{sec}(R)$. For this reason, adaptive noise generation is recommended to nullify the effect of noise signals on the legitimate receivers while not nullifying the negative effect on eavesdropper in both phases. Since it is assumed that the channel gain matrices of the noise emitting relays are known, they can be utilized for this recommended technique. It is required to set the transmit precoding vectors $v_{R_n^1}$ and $v_{R_n^2}$ at the first and second phase's noise emitting relays respectively such that the interference terms $IT_1(\mathbf{v_{R_n^1}})$ and $IT_2(\mathbf{v_{R_n^1}}, \mathbf{v_{R_n^2}})$ are equal to zero in the denominators of the $SINR_{R_c}$ and $SINR_D$

respectively. They are defined as

$$IT_1\left(\mathbf{v}_{\mathbf{R}_n^1}\right) = E_b\left|\mathbf{u}_{\mathbf{R}_c}^{\mathbf{H}}\mathbf{H}_{\mathbf{R}_n^1\mathbf{R}_c}\mathbf{v}_{\mathbf{R}_n^1}\right|^2 \tag{4.29a}$$

$$IT_2\left(\mathbf{v}_{\mathbf{R}_n^1}, \mathbf{v}_{\mathbf{R}_n^2}\right) = E_b^2\alpha_R^2\left|\mathbf{u}_{\mathbf{D}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R}_c\mathbf{D}}\mathbf{v}_{\mathbf{R}_c}\mathbf{u}_{\mathbf{R}_c}^{\mathbf{H}}\mathbf{H}_{\mathbf{R}_n^1\mathbf{R}_c}\mathbf{v}_{\mathbf{R}_n^1}\right|^2 + E_b\left|\mathbf{u}_{\mathbf{D}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R}_n^2\mathbf{D}}\mathbf{v}_{\mathbf{R}_n^2}\right|^2 \tag{4.29b}$$

from eqns. (4.4b) and (4.14) respectively. Thus, $\mathbf{v}_{\mathbf{R}_n^1}$ is chosen in the first phase such that $IT_1\left(\mathbf{v}_{\mathbf{R}_n^1}\right) = 0$. Hence, $\mathbf{v}_{\mathbf{R}_n^1}$ must lie in the null space of product $\mathbf{u}_{\mathbf{R}_c}^{\mathbf{H}}\mathbf{H}_{\mathbf{R}_n^1\mathbf{R}_c}$. In other words, $\mathbf{v}_{\mathbf{R}_n^1}$ must be orthogonal to $\mathbf{u}_{\mathbf{R}_c}^{\mathbf{H}}\mathbf{H}_{\mathbf{R}_n^1\mathbf{R}_c}$. Accordingly, the first term of $IT_2\left(\mathbf{v}_{\mathbf{R}_n^1}, \mathbf{v}_{\mathbf{R}_n^2}\right)$ in eqn. (4.29b) also becomes zero. Similarly, $\mathbf{v}_{\mathbf{R}_n^2}$ is chosen in the second phase such that $IT_2\left(\mathbf{v}_{\mathbf{R}_n^1}, \mathbf{v}_{\mathbf{R}_n^2}\right) = 0$. Therefore, the second term of $IT_2\left(\mathbf{v}_{\mathbf{R}_n^1}, \mathbf{v}_{\mathbf{R}_n^2}\right)$ must also be zero. As a result, the new SINR expressions are defined as

$$\overline{SINR_{R_c}} = \frac{E_b\left|\mathbf{u}_{\mathbf{R}_c}^{\mathbf{H}}\mathbf{H}_{\mathbf{SR}_c}\mathbf{v}_{\mathbf{S}}\right|^2}{N_0} \tag{4.30a}$$

$$\overline{SINR_D} = \frac{E_b^2\alpha_R^2|\mathbf{u}_{\mathbf{D}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R}_c\mathbf{D}}\mathbf{v}_{\mathbf{R}_c}\mathbf{u}_{\mathbf{R}_c}^{\mathbf{H}}\mathbf{H}_{\mathbf{SR}_c}\mathbf{v}_{\mathbf{S}}|^2}{E_b\alpha_R^2||\mathbf{u}_{\mathbf{D}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R}_c\mathbf{D}}\mathbf{v}_{\mathbf{R}_c}\mathbf{u}_{\mathbf{R}_c}^{\mathbf{H}}||^2N_0 + N_0}. \tag{4.30b}$$

from eqns. (4.4b) and (4.14) respectively. As for eavesdropper, while the interference term in the denominator of $SINR_{E^1}$ in eqn. (4.5b) is preserved, the first interference term caused by R_n^1 in the denominator of $SINR_{E^2}$ in eqn. (4.16) also becomes zero due to $IT_1\left(\mathbf{v}_{\mathbf{R}_n^1}\right) = 0$. Therefore, the expression of $SINR_{E^2}$ becomes

$$\overline{SINR_{E^2}} = \frac{E_b^2\alpha_R^2|\mathbf{u}_{\mathbf{E^2}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R}_c\mathbf{E}}\mathbf{v}_{\mathbf{R}_c}\mathbf{u}_{\mathbf{R}_c}^{\mathbf{H}}\mathbf{H}_{\mathbf{SR}_c}\mathbf{v}_{\mathbf{S}}|^2}{E_b\alpha_R^2||\mathbf{u}_{\mathbf{E^2}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R}_c\mathbf{E}}\mathbf{v}_{\mathbf{R}_c}\mathbf{u}_{\mathbf{R}_c}^{\mathbf{H}}||^2N_0 + E_b|\mathbf{u}_{\mathbf{E^2}}^{\mathbf{H}}\mathbf{H}_{\mathbf{R}_n^2\mathbf{E}}\mathbf{v}_{\mathbf{R}_n^2}|^2 + N_0} \tag{4.31}$$

from eqn. (4.16). However, the second interference term caused by R_n^2 is still present. Hence, $SINR_{E^2}$ also improves but not as much as $SINR_D$.

In the first simulation which is depicted in Fig. 4.6, the effect of adaptive noise generation on the probability $P_{sec}(R)$ is examined when the number of antennas equals 2. It is obvious that the maximum value of the probability $P_{sec}(R)$ dramatically improves from 0.53 to 0.92 with this recommended technique. Moreover, the most probable rate increases from 2.4 bps to 3.8 bps. Therefore, the source is able to securely communicate with the destination at $R = 3.8$ bps with probability 0.92. Furthermore, it is important to note that at relatively low rates, $P_{sec}(R)$ is a little bit greater interestingly in the case without adaptive noise. This is totally caused by a little increase in $SINR_{E^2}$ in the case with adaptive noise. However, after a certain rate, this becomes ineffective in enhancing $P_{sec}(R)$ since the $SINR_D$ at destination is insufficient to achieve high

rates. Thus $P_{sec}(R)$ begins decreasing in the case with nonadaptive noise as observed in the plot.

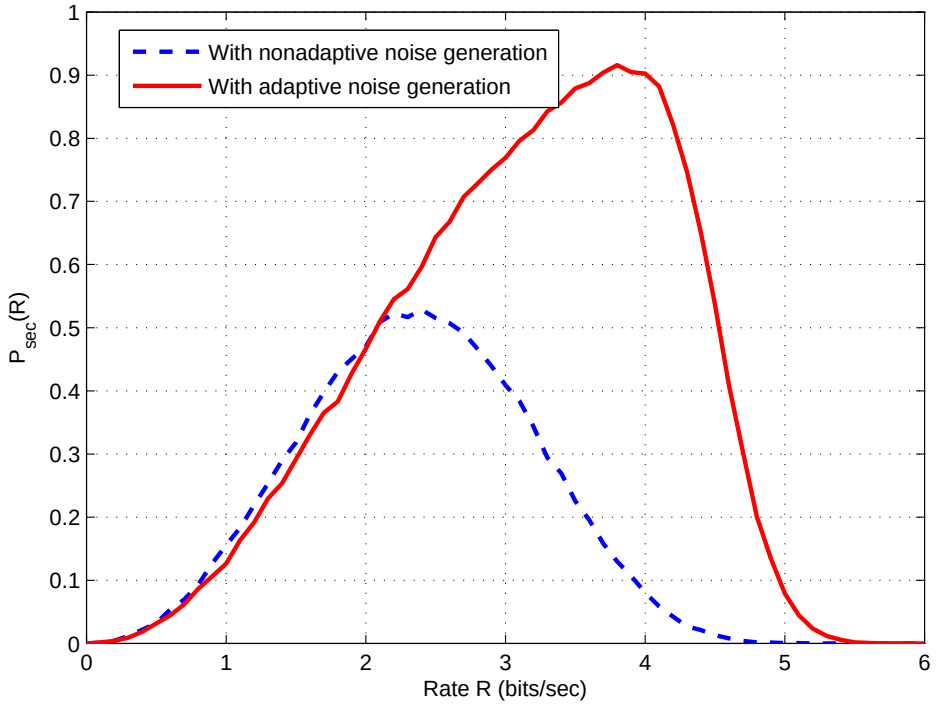

Figure 4.6: The effect of adaptive noise generation (E_b/N_0 = 10 dB, L = 2)

The effect of adaptive noise generation on the probability $P_{sec}(R)$ is shown in Fig. 4.7 when the number of antennas is equal to 5. As expected, the maximum value of the probability $P_{sec}(R)$ and the related rate R significantly improve with adaptive noise generation. It is important to note that the maximum value of $P_{sec}(R)$ increases from 0.75 to approximately 1 and the corresponding rate R rises from 3.6 bps to 5.8 bps. Therefore, the source has accomplished secure communication with the destination with probability approaching 1 among all the simulations so far. This is due to the use of multiple antennas and adaptive noise generation. Furthermore, the little superiority of the case without adaptive noise is also observed in this plot at relatively low rates similar to the plot in Fig. 4.6. The reason is the same.

Finally, we will check the influences of adaptive noise generation on the probabilities $P_D(R)$ and $P_E(R)$ in Fig. 4.8. The plot is useful to better understand the effects of this technique on the destination and eavesdropper separately. Adaptive noise generation

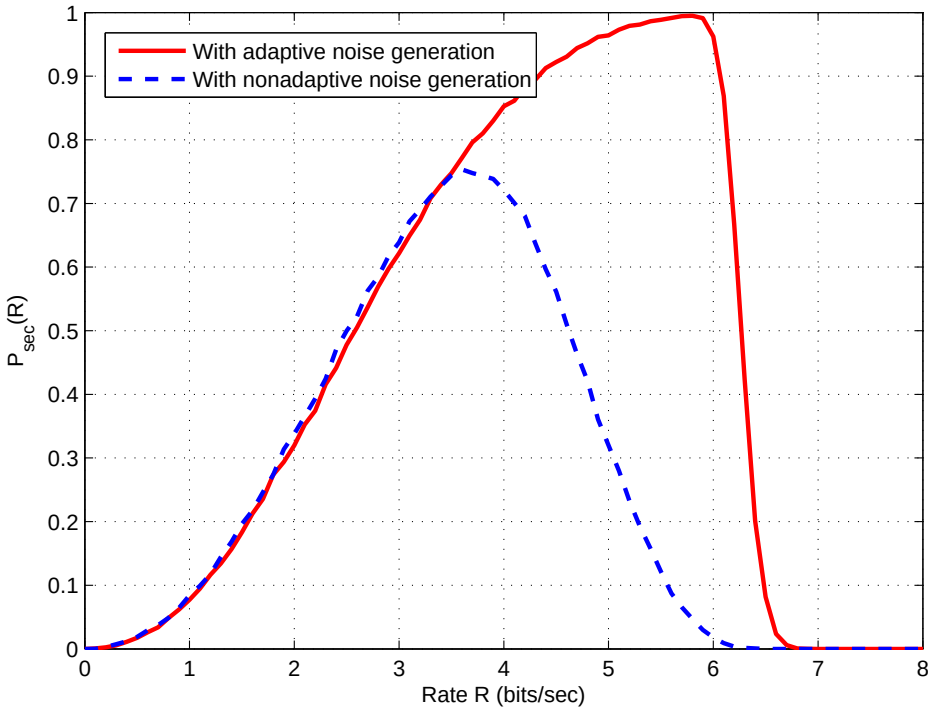

Figure 4.7: The effect of adaptive noise generation ($E_b/N_0 = 10$ dB, $L = 5$)

increases the range of rate R in which the probability $P_D(R)$ is equal to 1 since there is no interference at the destination anymore with this technique. As for $P_E(R)$, adaptive noise decreases $P_E(R)$ throughout all the rates as in the plot although the difference is very small. It is an expected result since $\overline{SINR_{E^2}}$ with adaptive noise increases a little bit while the interference term of $SINR_{E^1}$ is preserved. This obviously explains the small difference between two cases. Therefore, the improvement in the probability $P_D(R)$ determines the increase in the maximum value of probability $P_{sec}(R)$ and corresponding rate R. Furthermore, it is important to note that the probability $P_{sec}(R)$ shows a much sharper characteristic while decreasing in the case of adaptive noise generation. This is caused by the probability $P_D(R)$ which is displayed in Fig. 4.8. When there is adaptive noise, the SINR at the destination becomes $\overline{SINR_D}$ in eqn. (4.30b) and the interference terms in its denominator disappear as mentioned. The denominator of $\overline{SINR_D}$ consists of only channel noise terms and gives almost the same values in each trial. The numerator takes varying values. However, when multiple antennas exist, the variation of the numerator of $\overline{SINR_D}$ drops by the weak law of

large numbers. For these reasons, the maximum achievable rate C_D is approximately constant. Therefore, after the rate is equal to C_D, the probability $P_D(R)$ decreases with very sharp slope. On the other hand, when there is nonadaptive noise generation, the interference terms in the denominator of $SINR_D$ in eqn. (4.14) causes a larger variation in $SINR_D$. Hence, the probability $P_D(R)$ and $P_{sec}(R)$ with nonadaptive noise generation exhibit a less sharper slope in downfall.

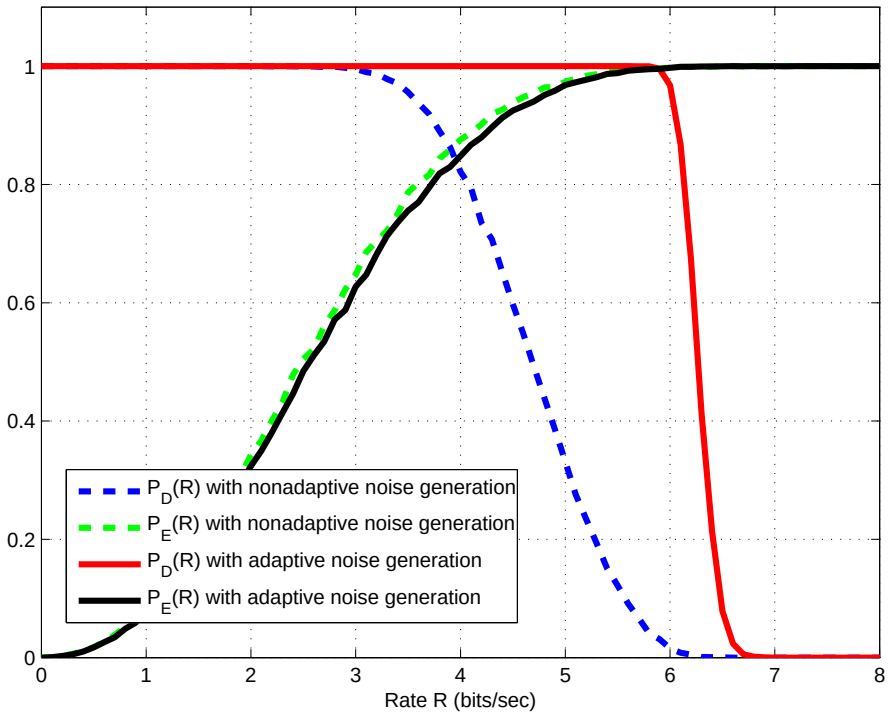

Figure 4.8: The effect of adaptive noise generation (E_b/N_0 = 10 dB, L = 5)

4.5.4 The Effect of Adaptive Receiver Shaping at Eavesdropper

In this section, it is assumed that the eavesdropper can also select its receiver shaping vectors $\mathbf{u}_{E^1}$ and $\mathbf{u}_{E^2}$ adaptively in the first and second phases respectively. For this reason, $\mathbf{u}_{E^1}$ and $\mathbf{u}_{E^2}$ are expressed as

$$\mathbf{u}_{E^1} = \frac{\mathbf{H}_{SE}\mathbf{v}_S}{\|\mathbf{H}_{SE}\mathbf{v}_S\|} \tag{4.32a}$$

$$\mathbf{u}_{E^2} = \frac{\mathbf{H}_{R_cE}\mathbf{v}_{R_c}}{\|\mathbf{H}_{R_cE}\mathbf{v}_{R_c}\|} \tag{4.32b}$$

to maximize the numerators of SINR expressions (4.5b) and (4.16). In the simulation, only the receiver shaping vectors at eavesdropper change and other parameters are the same. In Fig 4.9, the effect of adaptive receiver shaping at eavesdropper is observed in the cases with adaptive and nonadaptive noise generation. As expected, the maximization of the numerators of SINR at eavesdropper degrades the probability $P_{sec}(R)$. When there is adaptive receiver shaping at the eavesdropper, the maximum value of $P_{sec}(R)$ considerably decreases in the case with nonadaptive noise generation. However, there is almost no change in the maximum value of $P_{sec}(R)$ in the case with adaptive noise generation. Therefore, at relatively high rates, the gain extracted from adaptive noise generation tolerates the loss due to adaptive receiver shaping at the eavesdropper.

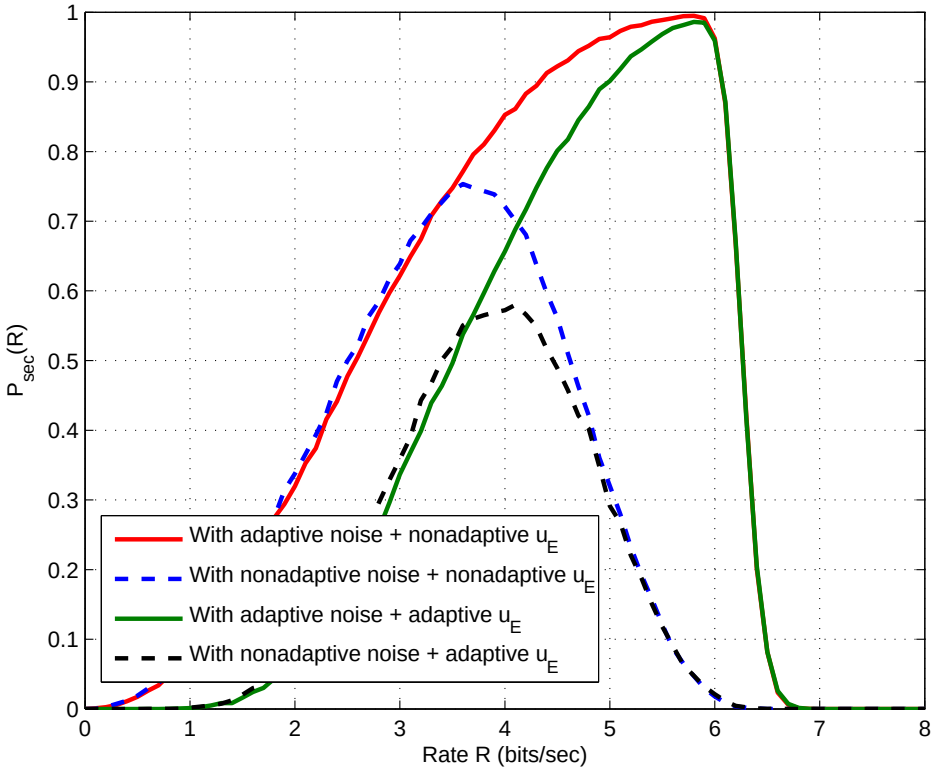

Figure 4.9: The effect of adaptive receiver shaping at eavesdropper (E_b/N_0 = 10 dB, L = 5)

The result in plot in Fig. 4.9 can be better understood by examining Fig 4.10. Similar to the plot in Fig. 4.9, the effect of adaptive receiver shaping on the probabilities

$P_D(R)$ and $P_E(R)$ is observed in both cases with adaptive and nonadaptive noise generation in Fig 4.10. Firstly, $P_D(R)$ expectedly does not change in both cases according to the adaptiveness of receiver shaping at the eavesdropper. Hence, change in $P_E(R)$ determines the difference in $P_{sec}(R)$ in Fig. 4.9. $P_E(R)$ drops almost the same amount in both cases due to adaptive receiver shaping at the eavesdropper. Therefore, this drop causes a decrease in $P_{sec}(R)$. However, since when adaptive receiver shaping exists, there is a range where both $P_E(R)$ and $P_D(R)$ are almost 1 in the case with adaptive noise generation. Thus, the maximum value of $P_{sec}(R)$ almost does not change as in Fig. 4.9. On the other hand, the intersection values of $P_D(R)$ and $P_E(R)$ which constitute the maximum value of $P_{sec}(R)$ decrease due to adaptive receiver shaping at eavesdropper in the case of nonadaptive noise generation. Thus, the maximum value of $P_{sec}(R)$ declines in that case.

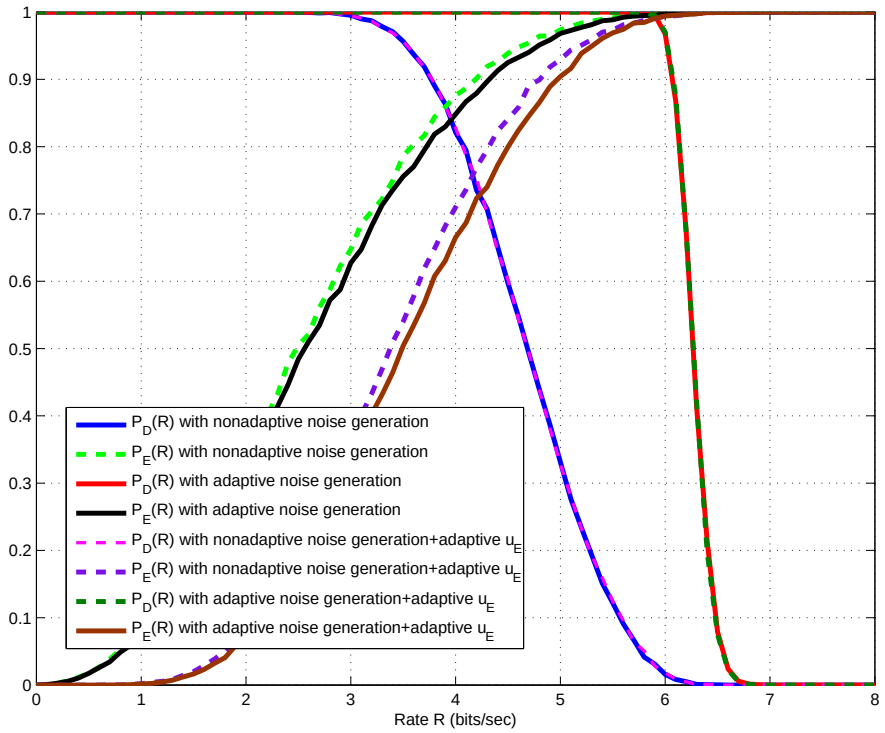

Figure 4.10: The effect of adaptive receiver shaping at eavesdropper ($E_b/N_0 = 10$ dB, $L = 5$)

4.5.5 The Comparison of the Cases with and without Cooperative Jamming

To observe the effect of cooperative jamming with multiple antennas on $P_{sec}(R)$, the plots of $P_{sec}(R)$ with adaptive noise generation, nonadaptive noise generation and without any noise generation are drawn in Figs. 4.11 and 4.12 for $L = 2$ and $L = 5$ respectively. Similar simulation exists for the single antenna case in Section 3.5.1. As observed in Fig. 4.11, when the number of antennas is 2, the case with adaptive noise generation considerably outperforms the case without any noise generation for all rates. Moreover, although $P_{sec}(R)$ in the case with nonadaptive noise generation is not always higher than that in the case without noise generation, it is more advantageous up to a rate and its maximum value is higher.

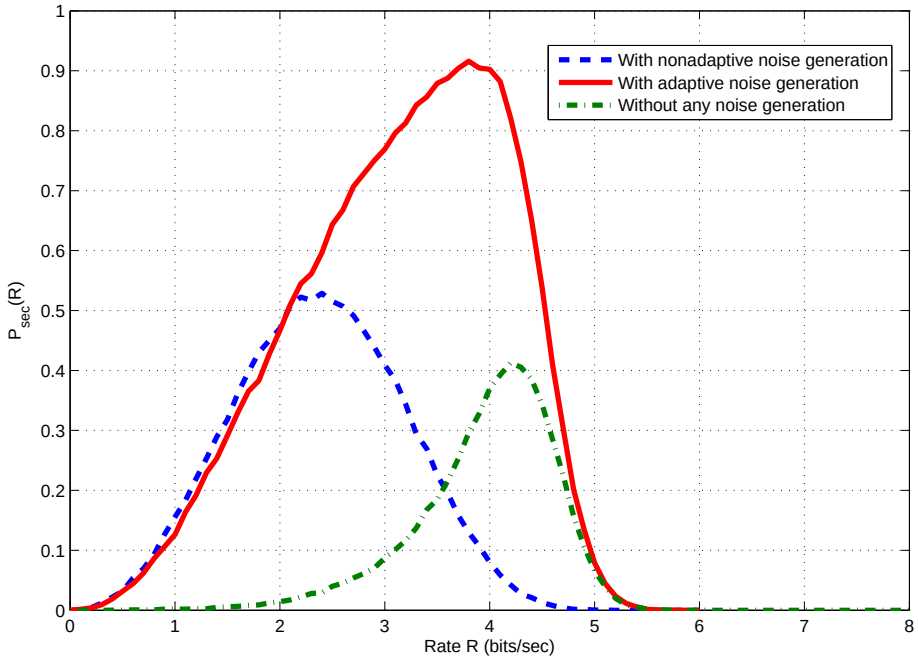

Figure 4.11: The comparison of the cases with adaptive, nonadaptive noise generation and without noise generation ($E_b/N_0 = 10$ dB, $L = 2$)

When the number of the antennas increases, the differences between the cases with and without noise generation significantly change. As displayed in Fig. 4.12, while L rises to 5, the improvement in $P_{sec}(R)$ without noise generation is much higher than the other cases. Nevertheless the difference between the maximum values of $P_{sec}(R)$ with adaptive noise generation and without noise generation reduces, the former is

always greater than the latter for all rates. However, $P_{sec}(R)$ without noise generation becomes more advantageous compared to with nonadaptive noise generation while L increases. The maximum value of the former is greater than that of the latter. As we observed that the number of antennas changes characteristics of performance, one has to be careful about the use of noise generation and should make decisions based on the number of antennas, the needed $P_{sec}(R)$ etc.

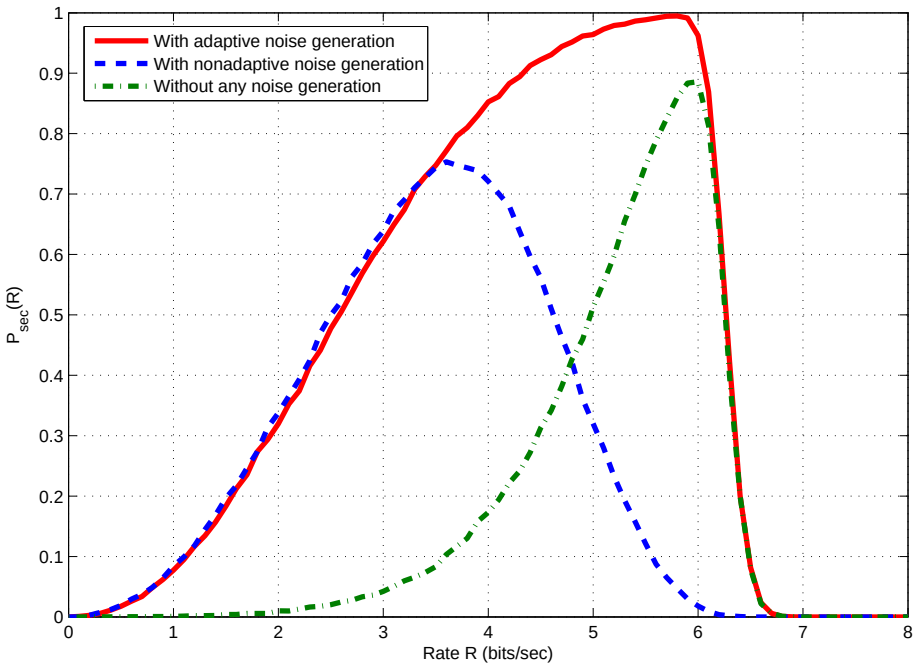

Figure 4.12: The comparison of the cases with adaptive, nonadaptive noise generation and without noise generation ($E_b/N_0 = 10$ dB, $L = 5$)

CHAPTER 5

CONCLUSION

Security is one of the most serious problems that cooperative networks encounter at large due to multiple hop transmission from the source to the destination. The source generally improves its transmission rate and reliability by utilizing relays. On the other hand, communication becomes more susceptible to be overheard by adversary receivers around the source and relays.

The event of secure communication is defined as the situation where the destination can decode the message signal while no eavesdropper can decode it in any of the hops. In this thesis work, the cooperative jamming method is implemented to accomplish high levels of probability of secure communication $P_{sec}(R)$ at reasonable communication rates in cooperative networks involving eavesdroppers. In this technique, as the source communicates with the destination over a relay, another relay attempts at making the channels of eavesdroppers noisier than that of the destination. However, it is significant to note that the legitimate receivers: the communicating relay and destination are also negatively influenced by jamming as well as eavesdroppers. Therefore, the communicating and noise emitting relays are intelligently selected among possible relays to overcome this issue at these receivers. Since channel gains of the links between the source, destination and relays are assumed to be known, the relay selection mechanism can totally benefit from them. However, since the channel gains of eavesdroppers and even existence of them are supposed to be unknown, there is no impact of their channel gains on relay selection. Moreover, rich scattering channels are assumed and all channel gains are taken as independent.

In Chapter 3, cooperative jamming is applied to cooperative networks with single-

antenna nodes to observe its effect on $P_{sec}(R)$ when the largest minimum relay selection is utilized. The relay which has channels of better quality is chosen as the communicating relay while the relays which least inhibit the legitimate receivers are labeled as the noise emitting relays. Therefore, it is shown that the source and destination can achieve more probable secure communication until a certain rate with cooperative jamming. Moreover, we check the best level we can improve $P_{sec}(R)$ with proper relay selection by utilizing an unrealistic method called the genie-aided selection. In that selection, CSI of eavesdropper's channels are assumed to be totally known. Hence, the maximum value of $P_{sec}(R)$ rises to a promising level, but it may be still unsatisfactory for especially tactical cooperative networks. For this reason, in Chapter 4, cooperation is accompanied by multiple antennas to reach higher probabilities of security.

In Chapter 4, cooperative jamming is implemented in cooperative networks with multiple-antenna nodes. It is imperative to indicate that eavesdroppers also benefit from the same number of antennas with other nodes for fairness. In this case, the legitimate nodes can take advantage of both multiple antennas and knowledge about channel gain matrices at the same time. Hence, this knowledge fortunately helps applying distinct adaptive techniques in addition to relay selection. Firstly, the implementation of adaptive transmit precoding is examined in which the transmit precoding vectors at the source and communicating relay are adjusted according to the related channel gain matrices. Therefore, there forms an advantage over the eavesdropper in terms of the received SINR and this outperforms the case with fixed transmit precoding at all the rates R.

In addition, it is benefited from the multiple antennas of the noise emitting relays to mitigate the corruptive effects of them on the communicating relay and the destination. Thus, adaptive noise generation is used to nullify the interference at these legitimate receivers by selecting transmit precoding vectors of the noise emitting relays based on the related channel gain matrices. The method with adaptive noise performs very well and the maximum value of $P_{sec}(R)$ and its related rate dramatically enhance. Thus, it is shown through simulations that it is possible to find a certain rate R at which $P_{sec}(R)$ is approaching 1 by increasing the number of antennas. Moreover, it is important to note that the method is always more advantageous

for all rates compared to the case without noise generation.

To sum up, the cooperative jamming method supported by adaptive techniques and multiple antennas significantly improves cooperative networks' resistance to illegal eavesdropping by adversary receivers and enables them to achieve reasonable communication rates with relatively high probability of secure communication.

In this thesis, all channels of the links between the nodes are rich scattering and taken as independent. For future studies, the effect of cooperative jamming method may be examined with channel gains which have different distributions. Furthermore, the direct link between the source and the destination may be added into calculations by assuming short-distance communication. In this study, the amplify-and-forward method is utilized as a signal forwarding technique at relays. Other forwarding techniques, such as decode-and-forward and compress-and-forward methods, can be applied at the relays to show the differences between them in the following studies. Moreover, the locations of the nodes, especially eavesdroppers, may be taken into account to observe the effects of the distances between the nodes on the probability $P_{sec}(R)$.

REFERENCES

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

[2] T. S. Rappaport. *Wireless Communications Principles and Practices*. Prentice Hall Press, 2002.

[3] D. Tse, P. Viswanath. *Fundamentals of Wireless Communications*. Cambridge University Press, 2005.

[4] A. Nosratinia, T.E. Hunter, and A. Hedayat. Cooperative Communication in Wireless Networks. *IEEE Communications Magazine*, Oct. 2004.

[5] T.M. Cover, A.A.El Gamal. Capacity Theorems for the Relay Channel. *IEEE Transactions on Information Theory,* vol.IT-25, no.5, pp.572-584, Sept. 1979.

[6] S.Y. Kim and J.W. Lee. To Cooperate or Not to Cooperate: System Throughput and Fairness Perspective. *IEEE Journal on Selected Areas in Communications,* vol.30, no.9, pp.1649-1657, Oct. 2012.

[7] D.Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung. Artificial Noise Generation from Cooperative Relays for Everlasting Secrecy in Two-Hop Wireless Networks. *IEEE Journal on Selected Areas in Communications,* vol.29, no.10, pp.2067-2076, Dec. 2011.

[8] W. Su, A.K.Sadek, K.J. Ray Liu. Cooperative Communication Protocols in Wireless Networks: Performance Analysis and Optimum Power Allocation. *Wireless Pers Commun.,* pp.181-217, 2008.

[9] G. Kramer, M. Gastpar, P. Gupta. Cooperative Strategies and Capacity Theorems for Relay Networks. *IEEE Transactions on Information Theory,* vol.51, no.9, Sept. 2005.

[10] C.E. Shannon. Communication Theory of Secrecy. *BellSystem Technical Journal,* vol.128-4, pp.656-715, Oct. 1949.

[11] A.D. Wyner. The Wire-Tap Channel. *BellSystem Technical Journal,* vol.54., pp.1355-1387, Oct. 1975.

[12] E.Ekrem, S. Ulukus. Secrecy in Cooperative Relay Broadcast Channels. *IEEE Transactions on Information Theory,* vol. 57, no. 1, Jan. 2011.

[13] M. Bloch, J. Barros, M.R.D. Rodrigues, S.W.McLaughin. Wireless Information-Theoretic Security. *IEEE Transactions on Information Theory,* vol. 54, no. 6, June 2008.

[14] I. Csiszar, J. Körner. Broadcast Channel with Confidential Messages. *IEEE Transactions on Information Theory,* vol. IT-24, no. 3, May 1978.

[15] Z. Ding, K.K. Leung, D. Goeckel, D. Towsley. Opportunistic Relaying for Secrecy Communications: Cooperative Jamming vs. Relay Chatting. *IEEE Transactions on Wireless Communications,* vol. 10, no. 6, June 2011.

[16] S. Goel, R. Negi. Guaranteeing Secrecy Using Artificial Noise. *IEEE Transactions on Wireless Communications,* vol. 7, no. 6, June 2008.