Hybrid Cooperative Relaying and Jamming for Secure Two-Way Relay Networks

A Thesis

submitted by

Aman Gupta

EE08B056

for the award of the degree

of

Master of Technology

(Communication System)

and

Bachelor of Technology

(Electrical Engineering)

DEPARTMENT OF ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY MADRAS

MAY 2013

May 2013

THESIS CERTIFICATE

This is to certify that the thesis titled **Hybrid Cooperative Relaying and Jamming for Secure Two-Way Relay Networks**, submitted by **Aman Gupta**, to the Indian Institute of Technology Madras, Chennai for the award of the degree of Master of Technology and Bachelor of Technology, is a bona fide record of the research work done by him under our supervision. The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Prof. Devendra Jalihal
Project Guide
Professor
Dept. Of Electrical Engineering
IIT-Madras, 600 036

Place: Chennai

Date: 23/05/2013

ACKNOWLEDGEMENTS

It has been a great privilege to pursue my bachelors and masters at this esteemed institute. First and foremost, I would like to thank my guides Dr. Devendra Jalihal and Dr. K Giridhar for their valuable guidance and probing questions. Their approach towards research and interest in the subject kept me motivated throughout the course of my project.

My thanks are also due to Rajeshwari and Kamalakar for their insights. I would like to express my gratitude to all my professors at IITM who have imparted valuable teachings in the hope that it would be transformed into knowledge. Their enthusiasm in teaching and expertise in their subject has never failed to amaze me.

I would like to acknowledge and extend my gratitude to the super computing center IIT Madras and MAD Lab, without which I wouldn't be able to finish my simulations on
time.

My family has constantly supported me through the ups and downs in life. I am indebted to them for life and a line or two is hardly a fitting payback. Nevertheless, I would like to thank them for their love and affection they have showered on me throughout my life.

ABSTRACT

This thesis considers the design of a system with relays, an eavesdropper , a jammer and two terminal nodes with aim of achieving maximum Secrecy rate . We extend this work for two antenna case instead of one antenna case deployed only on two terminals of the system. To solve the above problem , we use Convex Optimization as the mathematical tool as one can get global maximum and minimum values if the problem can be formulated as Convex Optimization problem. SOCP (Second Order Convex-Cone Programming) is the used Convex Optimization form used in this thesis. To solve the SOCP problem, CVX toolbox is used integrated to Matlab. For each plot, thousands of Monte-Carlo simulations are done and obtained simulations agreed with the published results.

Table of Contents

Chapter 1..5
1. Introduction..5
2. Motivation..5
3. Organisation of the Thesis..6
Chapter 2..7
2.1 System with only eavesdropper..7
2.1.1 First Phase..7
2.1.2 Second Phase..8
Chapter 3..11
3.1 Optimal Security Scheme : Maximum Secrecy Rate..11
3.2 Suboptimal Security Scheme: Null-Space Beamforming with Full Eavesdropper's CSI 12
3.3 Suboptimal Security Scheme : Artificial Noise Beamforming with no Eavesdropper's CSI..14
Chapter 4..17
4.1 System with a friendly Jammer and an Eavesdropper..17
4.1.1 First Phase..17
4.1.2 Second Phase..17
4.2.1 Secrecy Scheme with Eavesdropper's CSI..18
4.2.2 Secrecy Scheme without Eavesdropper's CSI 22
Chapter 5..24
5.1 Secrecy Scheme with Two Antennas at Source Terminals while Receiving , Friendly Jammer and an Eavesdropper without its CSI..24
5.1.1 First Phase..24
5.1.2 Second Phase..24
Chapter 6..28
6.1 System with only eavesdropper and eavesdropper's CSI known..28
6.2 System with only eavesdropper and eavesdropper's CSI not known and artificial noise scheme is used..31
6.3 System with an eavesdropper and a jammer and eavesdropper's CSI known......32
6.4 System with an eavesdropper and a jammer and eavesdropper's CSI not known and Terminals with two antennas are deployed..33
Chapter 7..35
Reference..36

Chapter 1

1. Introduction

THE ISSUE of security is a fundamental problem in data communications. In wireless communications, the security issue becomes more challenging due to the fundamental characteristics of the openness of wireless medium. Any receiver located in the cover range of the transmitter can obtain the transmitted signal. In this context, physical layer security, or information-theoretic security, has attracted considerable attention recently. The information-theoretic security was first introduced by Shannon . Wyner introduced the degraded wiretap channel model in where a wire-tapper wants to access a degraded version of the intended receiver's signal, and defined the notion of secrecy capacity to measure the maximum transmission rate from source to the legitimate destination while making the amount of information leaked to the eavesdroppers negligible. Information-theoretic security of multiple-antenna systems has attracted a lot of attention recently. It is worth mention that when the channel gains are fixed and known to all the transceivers, the optimal transmission scheme for Gaussian codebook that maximizes the secrecy rate of Gaussian MISO channels is beamforming along the direction of the generalized eigenvector corresponding to the maximum generalized eigenvalue of the matrix pencil of main channel and wiretap channel matrices. On the other hand, a lot of multiuser scenarios are considered for physical layer security transmission, such as broadcast channels, multiple access channels, cooperative relay channels , and two-way channels.

2. Motivation

Wireless Security has become oer of the important issue of the modern world of Wireless system . The increase in demand of wireless device has led to various security concerns like leaking of private/confidential knowledge which is may be very damaging in case of war situation when an army is sharing strategical information through wireless network and enemy get access of the information by eavesdropping in the wireless network. Present take this point as an inspiration and try minimize the eavesdropper role in the wireless communication.

3. Organisation of the Thesis

Chapter 2: System Model

Chapter 3: Scheme discussed for the scenario when only Eavesdropper is present

Chapter 4: Scheme discussed for the scenario when Eavesdropper and Jammer are present

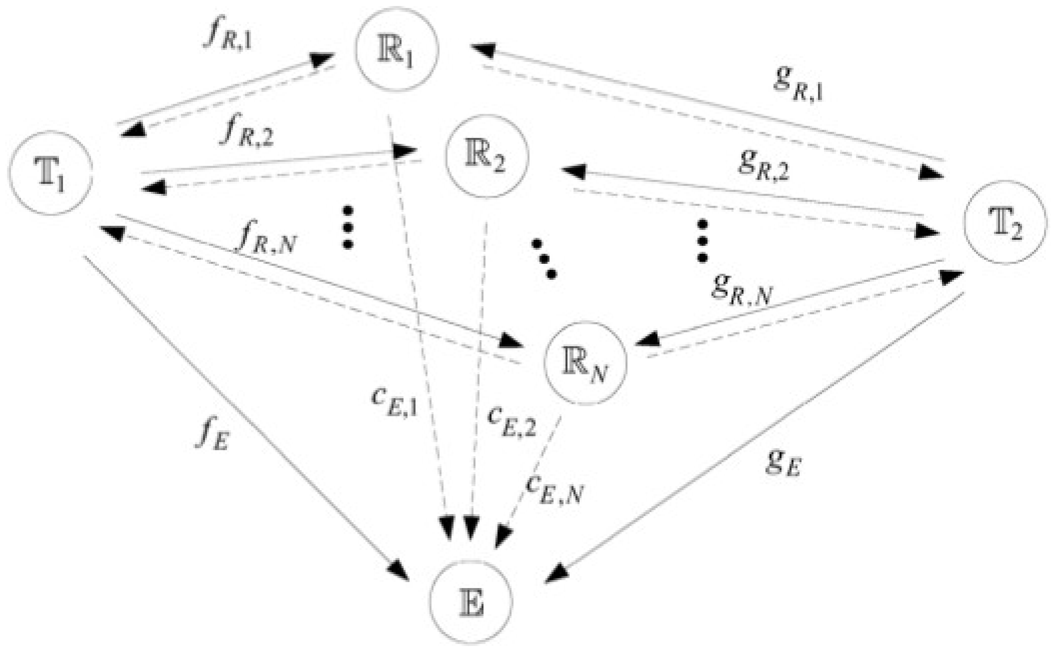
Chapter 5: Deals with the extended work for the terminal nodes with two antennas

Chapter 6: Simulation results

Chapter 7: Conclusion

Chapter 2

2.1 System with only eavesdropper



2.1.1 First Phase

A wireless network is considered in which two legitimate ter minal nodes , $T_m, m=1,2$ wish to exchange information under the existence of an eavesdropper E , with the help of distributed relay nodes , $R_n, n=1,2,...,N$ as depicted in Fig. 1. The eavesdropper is passive and the goal is to get the source information from terminal nodes T_1 and T_2 . Each node in the whole network is only equipped with a single antenna. All the terminal and relay nodes are subject to the half-duplex constraint, i.e., they cannot transmit and receive simultaneously. Denote the quasi-stationary flat-fading channel between T_1 and the n^{th} relay $f_{R,n}$ as, and the channel between R_n and the T_2 as $g_{R,n}, n=1,2,\ldots,N$. Further denote the channel between T_1 and E as f_E , the channel between T_2 and E as g_E , and the channel between relay nodes R_n and E as $c_{E,n}, n=1,2\ldots N$. We assume the channel coefficients $f_{R,n}, g_{R,n}, f_E, g_E, c_{E,n}$ are all independent complex Gaussian random variables with zero-mean and unit-variance .

There is no direct connection between T_1 and T_2 . Therefore, the relay nodes play two roles:

1) help to exchange information of two terminals and to guarantee reliable communications;
2) help to prevent the information leakage to the eavesdropper to enhance security.

A two-phase complex-weighted-and-forward protocol for the bidirectional transmission is used. During the first phase, both terminals simultaneously transmit their data to the relays. The signals received at the relays can be represented, in vector form, as

$$y_R=\sqrt{(P_1)}f_R s_1+\sqrt{(P_2)}g_R s_2+n_R$$

where y_R is the *Nx1* received signal vector with the *n*th element $y_{R,n}$, $P_1(P_2)$ and $s_1(s_2)$ are the transmit power and information symbol of $T_1(T_2)$, respectively, n_R is the additive noise at the relay nodes, and

$$f_R=[f_{R,1} f_{R,2} \dots f_{R,N}]^T, g_R=[g_{R,1} g_{R,2} \dots g_{R,N}]^T$$

are the channel coefficients vectors between the relay nodes and the corresponding terminals. Concurrently, the transmitted signals will also be received by the eavesdropper, if the eavesdropper lies in the cover range of both the terminals, which can be written as

$$y_E^{(1)}=\sqrt{(P_1)}f_E s_1+\sqrt{(P_2)}g_E s_2+n_E^{(1)}$$

where $n_E^{(1)}$ is the additive noise at the eavesdropper.

2.1.2 Second Phase

In the second phase, the *n*th relay multiplies its received signal by a complex weight w_n^* and then retransmit the so-obtained signal $x_{R,n}$. Stack the transmitted signals into a column vector , which can be written as

$$x_R=Wy_R$$

where W is the weight matrix in the form of $W=diag([w_1 w_2 ... w_N])$. Denote the received signal at T_1 and T_2 as y_{T1}, y_{T2} which can be easily obtained as

$$y_{T1}=f_R^T x_R+n_{T1}$$
$$= \sqrt{(P_1)} f_R^T W f_R s_1+\sqrt{(P_2)} f_R^T W g_R s_2+f_R^T W n_R+n_{T1}$$
$$y_{T2}=g_R^T x_R+n_{T2}$$
$$= \sqrt{(P_1)} g_R^T W f_R s_1+\sqrt{(P_2)} g_R^T W g_R s_2+g_R^T W n_R+n_{T2}$$

and similarly, the received signal at the eavesdropper during the second phase is

$$y_E^{(2)}=c_E^T x_R+n_E^{(2)}$$
$$= \sqrt{(P_1)} c_E^T W f_R s_1+\sqrt{(P_2)} c_E^T W g_R s_2+c_E^T W n_R+n_E^{(2)}$$

where $c_E=[c_{E,1} c_{E,2} ... c_{E,N}]^T$ and $n_{T1}, n_{T2}, n_E^{(2)}$ are additive noise at T_1, T_2, E and during the second phase, respectively. Each terminal knows both the channels associated itself with the relay nodes and the weighted coefficients matrix W , hence, it can subtract the backward self-interference from itself and only obtain the desired information from the other one. After this operation,

$$y_{T1}=\sqrt{(P_2)} w^H F_R g_R s_2+f_R^T W n_R+n_{T1}$$
$$y_{T2}=\sqrt{(P_1)} w^H F_R g_R s_1+g_R^T W n_R+n_{T2}$$
$$y_E^{(2)}=\sqrt{(P_1)} w^H C_E f_R s_1+\sqrt{(P_2)} w^H C_E g_R s_2+c_E^T W n_R+n_E^{(2)}$$

by using the equation , $a^H diag(b)=b^H diag(a)$, where $w=[w_1, w_2, ..., w_N]^T$, $F_R=diag(f_R), G_R=diag(g_R), C_E=diag(c_E), a_{fg}=F_R g_R=G_R f_R, a_{cf}=C_E f_R, a_{cg}=C_E g_{R.}$
Combining signals of eavesdropper for phase 1 and phase 2 we get,

$$y_E=H_E s+n$$
$$y_E = \begin{bmatrix} y_E^{(1)} \\ y_E^{(2)} \end{bmatrix}$$
$$H_E = \begin{bmatrix} \sqrt{(P_1)} f_E & \sqrt{(P_2)} g_E \\ \sqrt{(P_1)} w^H a_{cf} & \sqrt{(P_1)} w^H a_{cg} \end{bmatrix}$$

$$n = \begin{bmatrix} n_E^{(1)} \\ w^H C_E n_R + n_E^{(2)} \end{bmatrix}$$

$$s = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$$

All the noise terms $n_{T1}, n_{T2}, n_E^{(1)}, n_E^{(2)}$ and n_R are zero-mean and time-spatially white independent complex Gaussian random variables with variance σ^2 . Then, eavesdroppr's noise covariance matrix can be written as

$$Q_E = \begin{bmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 (1 + w^H R_{cc} w) \end{bmatrix}$$

where, $R_{ff} = F_R F_R^H, R_{qq} = G_R G_R^H, R_{cc} = C_E C_E^H$

We have the following observations:

1) For the legitimate terminals T_1 and T_2 , the equivalent models are two SISO systems
2) For the eavesdropper E , each transmission phase grants it an opportunity to get the information. This implies the optimal strategy the eavesdropper should take is to combine the information received over the two phases to create an equivalent MIMO system.

Chapter 3

3.1 Optimal Security Scheme : Maximum Secrecy Rate

Secrecy Rate is defined as difference in rate of sum of rate of two terminals and rate of the eavesdropper. In this scheme, we maximise the Secrecy Rate.
The information rate of two legitimate terminals is defined as:

$$R_{T1} = \frac{1}{2}\log\left(1 + \frac{P_2}{\sigma^2}\frac{w^H R_{fg} w}{1 + w^H R_{ff} w}\right)$$

$$R_{T2} = \frac{1}{2}\log\left(1 + \frac{P_1}{\sigma^2}\frac{w^H R_{fg} w}{1 + w^H R_{qq} w}\right)$$

$$R_E = \frac{1}{2}\log\left(\left|I + H_E H_E^H Q_E^{-1}\right|\right)$$

$$R_{sun} = R_{T1} + R_{T2} - R_E$$

where, $R_{fg} = a_{fg} a_{fg}^H$

Therefore, objective function can be defined as

$$\max_{P_1, P_2, \mathbf{w}} \quad R^{sun}$$

$$s.t. \qquad P_S + P_R \leq P_M$$

We can see the objective function is a product of three correlated generalized Rayleigh quotients problem, which is in general difficult to solve. Actually, we observe that the objective function is a difference between the sum of two concave functions and a third concave function, which therefore is neither convex nor concave. As a result, it is a constraint nonconvex optimization problem, for which a numerical solution method, such as gradient descent method or Newton's method, should be adopted to iteratively search for a local optimum. However, a global optimum cannot be guaranteed. Hence, we will use suboptimal schemes as defined subsequently.

3.2 Suboptimal Security Scheme: Null-Space Beamforming with Full Eavesdropper's CSI

From the system model, we can see that information leakage happens in both two phases. In the first phase, relay nodes can hardly do anything to help improving the security since they have to receive the signal. In the second phase, the relays actually do the distributed beamforming. If the relay nodes choose the beamforming vector lying in the null space of the eavesdropper's equivalent channel vectors, then the eavesdropper get nothing in the second phase. As such, the information leakage happens only in the first phase, which greatly improves the security of the information exchange. Mathematically, it implies that $w^H a_{cf} = 0$ and $w^H a_{cg} = 0$. Denote $H = [a_{cf}\, a_{cg}]$, we have,

$$w^H H = 0 \quad => \quad w = H_{\perp} v$$

where, v is any vector, and $H_{\perp}$ is the projection matrix onto the null space of H **.** Design w to make the information exchange between legitimate terminals as much as possible .

$$R_T^{sun} = R_{T1} + R_{T2} = \frac{1}{2} \log(1 + SNR_1)(1 + SNR_2)$$

where,

$$SNR_1 = \frac{P_2}{\sigma^2} \frac{w^H R_{fg} w}{1 + w^H R_{ff} w} \qquad SNR_2 = \frac{P_1}{\sigma^2} \frac{w^H R_{fg} w}{1 + w^H R_{qq} w}$$

Optimization criteria can be described as: to find the beamforming weight vector w and transmit powers P_1, P_2 , such that

1) the information leaked to the eavesdropper is zero in the second phase;

2) the information exchanged between legitimate terminals is as much as possible, subject to the total transmit power constraint consumed by both terminals and

relays.

Define $P_T = P_1 + P_2 + P_R$ .We can formulate the security criteria as the following optimization problem:

$$\max_{P_1, P_2, \mathbf{w}} \quad R_T^{sun}$$

$$s.t. \qquad w = H_{\perp} v$$

$$P_1 (1 + w^H R_{ff} w) + P_2 (1 + w^H R_{qq} w) + \sigma^2 w^H w \le P_M$$

To solve above , we firstly do the following simplifications:

1) since logarithm is an increasing function, the objective function can be written as $(1+SNR_1)(1+SNR_2)$, which will not impact the optimal values;

2) at the optimum, we will have $P_T = P_M$

3) at the optimum, we have $SNR_1 = SNR_2$.

The final expression for optimization problem can be written as:

$$\max_{P_1, \mathbf{v}} \quad \frac{P_1}{\sigma^2} \quad \frac{v^H H_{\perp}^H R_{fg} H_{\perp} v}{1 + v^H H_{\perp}^H R_g H_{\perp} v} \qquad \textbf{...(1)}$$

$$s.t. \qquad v^H A(P_1) v = K$$

where, $K = P_M - 2\mathrm{P}_1$ $\quad A(P_1) = H_{\perp}^H (2\mathrm{P}_1 R_{ff} + \sigma^2 I) H_{\perp}$

It is a Rayleigh Quotient Problem and has a well known solution.

Define, $\hbar = H_p^H a_{fg}$. The above problem can be formulated as:

$$\max_{P_1 \ge 0} \quad \frac{P_1}{\sigma^2} \quad K \hbar^H (A(P_1) + K H_{\perp}^H R_{qq} H_{\perp})^{-1} \hbar \qquad \textbf{...(2)}$$

$$s.t. \quad 0 \le P_1 \le \frac{P_M}{2}$$

The above function is a polynimial in P_1 and a concave function and hence has a unique optimal value. The optimal weight vector is given by

$$w^o = H_{\perp} v(P_1^o)$$

$$P_2^o = P_1^o \quad \frac{1 + w^{oH} R_{ff} w^o}{1 + w^{oH} R_{qq} w^o}$$

$$Secrecy\ Rate = R_1 + R_2 - R_E$$

$$= \quad \frac{1}{2} \quad \left[\log \left(\frac{\left(1 + \frac{w^{oH} R_{fg} w^o}{1 + w^{oH} R_{ff} w^o}\right)\left(1 + \frac{w^{oH} R_{fg} w^o}{1 + w^{oH} R_{qq} w^o}\right)}{1 + \frac{1}{\sigma^2}\left(P_1 |f_E|^2 + P_2 |g_E|^2\right)} \right) \right]$$

3.3 Suboptimal Security Scheme : Artificial Noise Beamforming with no Eavesdropper's CSI

In many applications, it may not be practical to know the eavesdropper’s channel. In this section, we consider the scenario when the terminals and relay nodes are not aware there is an eavesdropper, i.e., without eavesdropper’s CSI. In the second phase, the so-called artificial noise scheme for the relay nodes. In this scheme the relay nodes transmit artificial noise (interference) to mask the concurrent transmission of information bearing signal to the legitimate receivers. The signal transmitted by the relay nodes in the second phase is

$$x_R = W\, y_R + n_a$$

After the backward self-interference cancelation, the obtained signals are

$$y_{T1} = \sqrt{(P_2)}\, w^H F_R\, g_R s_2 + f_R^T n_a + f_R^T W n_R + n_{T1}$$
$$y_{T2} = \sqrt{(P_1)}\, w^H F_R\, g_R s_1 + g_R^T n_a + g_R^T W n_R + n_{T2}$$
$$y_E^{(2)} = \sqrt{(P_1)}\, w^H C_E f_R s_1 + \sqrt{(P_2)}\, w^H C_E g_R s_2 + c_E^T W n_R + n_E^{'}(2)$$

where,

$$n_E^{'(2)} = c_E^T n_a + c_E^T W n_R + n_E^{(2)}$$

To avoid interfering the legitimate users, we should require $f_R^T n_a = g_R^T n_a = 0\,,$ i.e., the artificial noise should be broadcasted in the null space of the terminals’s channels.

On the other hand, due to the lack of eavesdropper's channel information, the relay nodes can only transmit artificial noise isotropically instead of concentrating the inference power in some direction. As a result, n_a is in the form of $n_a = U_{\perp} z$ where $U_{\perp}$ is the projection matrix onto the null space of $U = [f_R g_R]$, and the component of z are i.i.d. Gaussian variables with zero mean and variance σ_z^2 . Therefore, the power consumed by all the relays P_R can be written as $P_R = P_i + P_n$, where $P_i = w^H (P_1 R_{ff} + P_2 R_{qq} + \sigma^2 I) w$ is allocated for information transmission and $P_n = E n_a^H n_a = \sigma_z^2 (N-2)$ is allocated for artificial noise. As P_R is limited, we hope that under the constraint that the two terminals has the required quality of service (QoS), the power used for information transmission is minimized (decrease P_i) so that as much as power can be used to transmit artificial noise to confuse the potential eavesdropper (increase P_n) and improve security.

In summary, we adopt the following optimization criteria for the security issue: to find the beamforming weight vector , such that:

1) the two terminals has the required QoS , or, the received $SNRs$ for the information bits are required to be above certain predefined thresholds;

2) the power occupied to transmit desired information is minimized so that the power available for transmitting artificial noise is maximized, under the constraint of total transmit power available by relays.

Therefore, the optimization problem can be expressed as:

$$\min_{w} \quad w^H R w$$

$$\frac{w^H R_{fg} w}{1 + w^H R_{ff} w} \geq \gamma_1 \quad , \quad \frac{w^H R_{fg} w}{1 + w^H R_{qq} w} \geq \gamma_2$$

where γ_1 and γ_2 are two required receive SNR thresholds. It can be further expressed as,

$$\min_{w} \quad w^H R w \qquad \textbf{...(3)}$$

$$\text{s.t.} \quad \left|w^H a_{fg}\right|^2 \geq \Gamma_1 \left\| \begin{matrix} \sqrt{(R_{ff})}\, w \\ 1 \end{matrix} \right\|^2$$

$$\left|w^H a_{fg}\right|^2 \geq \Gamma_2 \left\| \begin{matrix} \sqrt{(R_{qq})}\, w \\ 1 \end{matrix} \right\|^2$$

where, $R = P_1 R_{ff} + P_2 R_{qq} + \sigma^2 I$, $\quad \Gamma_1 = \dfrac{\sigma^2 \gamma_1}{P_2}$, $\quad \Gamma_2 = \dfrac{\sigma^2 \gamma_2}{P_1}$

Multiplying the optimal w^o by an arbitrary phase shift will not affect the objective function or the constraints. Therefore, we can assume, without loss of generality, that $w^H a_{fg}$ is a real number The above optimization criteria can be written in the form of Second Order Convex Optimization(SOCP) as :

$$\min_{w} \quad t$$

$$s.t. \quad \|\sqrt{(\acute{R})}\, \hat{w}\| \leqslant t$$

$$\|\sqrt{(\acute{R}_{ff})}\, \hat{w}\| \leqslant \frac{1}{\sqrt{(\Gamma_1)}} real\left(\bar{a}_{fg}^H \hat{w}\right) \qquad \|\sqrt{(\acute{R}_{qq})}\, \hat{w}\| \leqslant \frac{1}{\sqrt{(\Gamma_2)}} real\left(\bar{a}_{fg}^H \hat{w}\right)$$

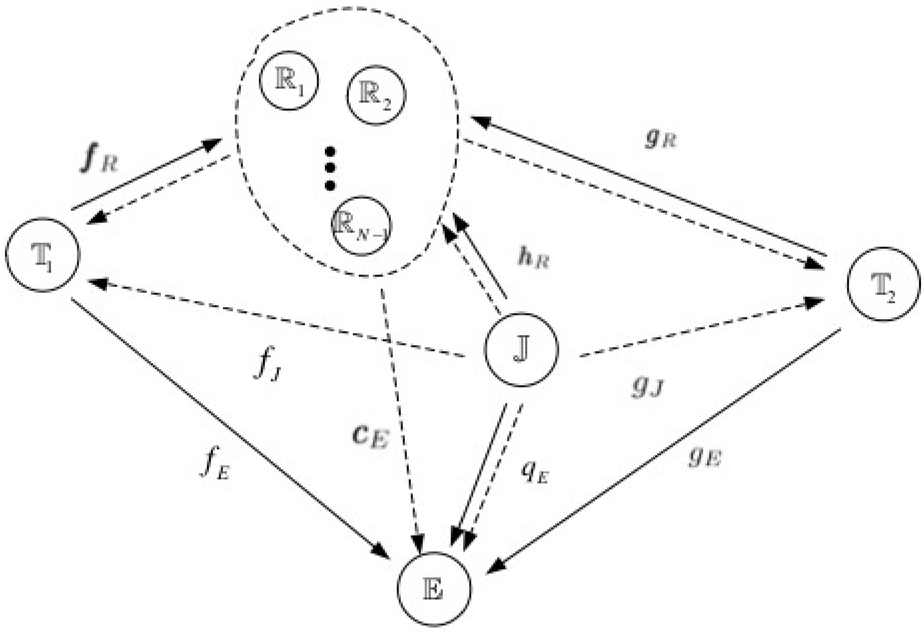
$$[\hat{w}]_{N+2} = 1$$

where, $\hat{w} = [w^T, t, 1]^T \qquad \bar{a}_{fg}^H = [a_{fg}^H 0\, 0]$

$$\boldsymbol{\acute{R}} = \begin{bmatrix} R & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} , \quad \boldsymbol{\acute{R}_{ff}} = \begin{bmatrix} R_{ff} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} , \quad \boldsymbol{\acute{R}_{qq}} = \begin{bmatrix} R_{qq} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Chapter 4

4.1 System with a friendly Jammer and an Eavesdropper



4.1.1 First Phase

The first phase is same as one in case with only eavesdropper except an additional signal from jammer.

$$y_R=\sqrt{(P_1)}f_R s_1+\sqrt{(P_2)}g_R s_2+\sqrt{(P_J^{(1)})}h_R z^{(1)}+n_R$$

where, $h_R=[h_{R,1}h_{R,2}...h_{R,N-1}]^T$

Similarly, signal received by the eavesdropper will have an additional signal from the jammer.

$$y_E^{(1)}=\sqrt{(P_1)}f_E s_1+\sqrt{(P_2)}g_E s_2+\sqrt{(P_J^{(1)})}q_E s_2+n_E^{(1)}$$

4.1.2 Second Phase

In the second phase, the $N-1$ relay do a distributed beamforming, and transmit the signal $x_R=Wy_R$

where, $W = diag([w_1 w_2 ... w_{N-1}])$

Concurrently, the jammer transmits interference signal again as $z^{(2)}$ with power $P_J^{(2)}$. The received signal at T_1, T_2 and E after self-interference cancel can be obtained as:

$$y_{T1} = \sqrt{(P_2)} w^H F_R g_R s_2 + \sqrt{(P_J^{(2)})} f_J z^{(2)} + f_R^T W n_R + n_{T1}$$

$$y_{T2} = \sqrt{(P_1)} w^H F_R g_R s_1 + \sqrt{(P_J^{(2)})} g_J z^{(2)} + g_R^T W n_R + n_{T2}$$

$$y_E^{(2)} = \sqrt{(P_1)} w^H C_E f_R s_1 + \sqrt{(P_2)} w^H C_E g_R s_2 + \sqrt{(P_J^{(2)})} q_E z^{(2)} + c_E^T W n_R + n_E^{(2)}$$

Receive model for the eavesdropper in the whole procedure is:

$$y_E = H_E s + n$$

$$y_E = \begin{bmatrix} y_E^{(1)} \\ y_E^{(2)} \end{bmatrix}$$

$$H_E = \begin{bmatrix} \sqrt{(P_1)} f_E & \sqrt{(P_2)} g_E \\ \sqrt{(P_1)} w^H a_{cf} & \sqrt{(P_1)} w^H a_{cg} \end{bmatrix}$$

All the noise terms $n_{T1}, n_{T2}, n_E^{(1)}, n_E^{(2)}$ and n_R are zero-mean and time-spatially white independent complex Gaussian random variables with variance σ^2. Then, eavesdroppr's noise covariance matrix can be written as

¿

$$Q_E = \begin{bmatrix} \sigma^2 + P_J^{(1)} |q_E|^2 & 0 \\ 0 & w^H (P_J^{(1)} R_{ch} + \sigma^2 R_{cc}) w + \sigma_z^2 c_E^H U_\perp U_\perp^H c_E + \sigma^2 \end{bmatrix}$$

4.2.1 Secrecy Scheme with Eavesdropper's CSI

For this case we can choose the complex weights as follow:

1) design w in the null space of a_{cf} and a_{cg} to completely eliminate the information leakage in the second phase, i.e., let $w^H a_{cf} = w^H a_{cg} = 0$ so that the second row of H_E can be eliminated;

2) design w in the null space of a_{fh} and a_{gh} to eliminate the interference to the terminals by the jamming signal in the first phase (it has been forwarded by the relay nodes in the second phase);

3) since no information leakage happens in the second phase (by 1)), the jammer should stop send interference so that the terminals will not be jammed (2) when receiving, i.e., $P_J^{(2)}=0$.

We want to make information leakage as less as possible, therefore, $P_J^{(1)}=P_\perp$ where $P_\perp$ is the maximum power allocated for the jammer. Subject to the total power constraint P_M of the intermediate nodes including both relay and jammer, optimization criteria can be mathematically expressed as

$$\max_{w} \quad R_T^{sun}=R_{T1}+R_{T2} = \frac{1}{2} \log(1+SNR_1)(1+SNR_2)$$
$$s.t.\ w=H_\perp v$$
$$P_R+P_\perp \leqslant P_M$$

where, $\frac{w^H R_{fg} w}{1+w^H R_{qq} w} \geq \gamma_2$

$$SNR_1 = \frac{P_2}{\sigma^2} \quad \frac{w^H R_{fg} w}{1+w^H R_{ff} w} \qquad SNR_2 = \frac{P_1}{\sigma^2} \quad \frac{w^H R_{fg} w}{1+w^H R_{qq} w}$$

$H=[a_{cf}, a_{cg}, a_{fh}, a_{gh}], H_\perp$ is the projection matrix onto the null space of H , v is any vector, $P_R=E(x^H x_R) = w^H T w$ is the transmit power of relay nodes with $T=P_1 R_{ff}+P_2 R_{qq}+P_R R_{hh}+\sigma^2 I$.

However, the above problem is non-convex since the objective function is not a concave function. To address this issue,an alternative method called the rate- split method is used , formulated as

$$\max_{w} \quad R_T^{sun} \qquad \textbf{...(5)}$$

$$s.t. \quad \frac{1}{2}\log(1+SNR_1) \geqslant \eta R_{sun}^T$$

$$\frac{1}{2}\log\left(1+SNR_2\right)\geqslant\left(1-\eta\right)R_{sun}^T$$

$$w=H_{\perp}v$$

$$w^H T w\leqslant P_M b$$

where, $P_{M\perp}=P_M-P_{\perp}$, and $\eta\in[0,1]$. For any given η , the first two constraints impose a rate-split between two terminals . An one-dimension search is done on η to find the maximum $R_{sun}(\eta^o)$ under optimal rate split scheme η^o .

To solve the above problem first we consider relay power minimization problem as follows:

$$\min_{w} \quad w^H Tw$$

$$s.t. \quad \frac{1}{2}\log\left(1+SNR_1\right)\geqslant\eta R_{sun}^T$$

$$\frac{1}{2}\log\left(1+SNR_2\right)\geqslant\left(1-\eta\right)R_{sun}^T$$

$$w=H_{\perp}v$$

By solving above problem the minimum power required to achieve sum rate r under the rate split scheme η is achieved. If the minimum power required is less than the power constraint P_M , then we can increase the value of r , otherwise decrease the value of r , and again find the minimum power required to achieve that rate. Through this iteration, we can converge on the optimal value of r that satisfies the power constraint.

The iterative algorithm is as follows:

- Set $\eta(0) = 0$.
- At step k, set $\eta(k) = \eta(k-1) + \delta$, where δ is the step size.
  - Initialize $r_{low} = 0$, $r_{up} = r_{max}$.
  - Repeat the following Until $r_{up} - r_{low} < \varepsilon$.

1) Set $r \leftarrow \frac{1}{2}(r_{low} + r_{up})$, and calculate γ_1, γ_2.

2) Solve SOCP problem (23) with r using interior point method.

3) Update r: If $\boldsymbol{v}^H \boldsymbol{R} \boldsymbol{v} \leq \bar{P}_M$, set $r_{low} = r$; otherwise, $r_{up} = r$.

- Obtain $R^T_{sum}(\eta^o)$ by comparing all $R^T_{sum}(\eta(k))$, $k = 1, \cdots, K$.

The optimization problem can be reformulated as:

$$\min_{w} \quad w^H T w \qquad \textbf{...(7)}$$

$$s.t. \quad |w^H a_{fg}|^2 \geq \gamma_1 \left\| \frac{\sqrt{(R_{ff})}\, w}{1} \right\|^2$$

$$|w^H a_{fg}|^2 \geq \gamma_2 \left\| \frac{\sqrt{(R_{qq})}\, w}{1} \right\|^2$$

where, $\gamma_1 = \frac{\sigma^2 (2^{2\eta r} - 1)}{P_2}$, $\gamma_2 = \frac{\sigma^2 (2^{2(1-\eta) r} - 1)}{P_1}$

Multiplying the optimal w^o by an arbitrary phase shift will not affect the objective function or the constraints. Therefore, we can assume, without loss of generality, that $w^H a_{fg}$ is a real number The above optimization criteria can be written in the form of Second Order Convex Optimization(SOCP) as :

$$\min_{w} \quad t \qquad \textbf{...(8)}$$

$$s.t. \quad \|\sqrt{(\check{T})}\, \hat{w}\| \leqslant t$$

$$\|\sqrt{(\acute{R}_{ff})}\, \hat{w}\| \leqslant \frac{1}{\sqrt{(\gamma_1)}} real(\bar{a}^H_{fg} \hat{w}) \qquad \|\sqrt{(\acute{R}_{qq})}\, \hat{w}\| \leqslant \frac{1}{\sqrt{(\gamma_2)}} real(\bar{a}^H_{fg} \hat{w})$$

$$[\hat{w}]_{N+2}=1$$

where, $\hat{w}=[w^T,t,1]^T$ $\bar{a}_{fg}^H=[a_{fg}^H 0 0]$

$$\check{T}=\begin{bmatrix} T & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \acute{R}_{ff}=\begin{bmatrix} R_{ff} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \acute{R}_{qq}=\begin{bmatrix} R_{qq} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

4.2.2 Secrecy Scheme without Eavesdropper's CSI

In the first phase, the procedures are the same as the previous scheme. Both terminals broadcast their data and the jammer transmits interference $z^{(1)}$. Since the eavesdropper's CSI is not known, the relay nodes transmit artificial noise (interference) to mask the concurrent forward of the information bearing signal to the legitimate receivers. As such, the signal transmitted by the relay nodes in the second phase is

$$x_R=Wy_R+n_a$$

where n_a is the artificial noise in the form of $n_a=U_\perp z$, with $U_\perp$ the projection matrix into the null space of $U=[f,g]$ to avoid interfering the legitimate users, i.e., $f^T n_a=g^T n_a=0$, and the component of z are i.i.d. Gaussian variables with zero mean and variance σ_z^2. After the backward self-interference cancelation, the obtained signal by T_1, T_2 and E are

$$y_{T1}=\sqrt{(P_2)}w^H F_R g_R s_2+\sqrt{(P_\perp)}f_R^T W h_R z^{(1)}+f_R^T W n_R+n_{T1}$$

$$y_{T2}=\sqrt{(P_1)}w^H F_R g_R s_1+\sqrt{(P_\perp)}g_R^T W h_R z^{(1)}+g_R^T W n_R+n_{T2}$$

$$y_E^{(2)}=\sqrt{(P_1)}w^H C_E f_R s_1+\sqrt{(P_2)}w^H C_E g_R s_2+c_E^T n_a+c_E^T W n_R+n_E^{'(2)}$$

The total power consumed by all the relays P_R can be written as $P_R=P_i+P_n$, where $P_i=w^H(P_1 R_{ff}+P_2 R_{¿}+P_\perp R_{hh}+\sigma^2 I)w$ is allocated for information transmission and $P_n=E n_a^H n_a$ = $\sigma_z^2(N-3)$ is allocated for artificial noise. As P_R is limited, we hope that under the constraint that the two terminals has the required QoS, the power used for information transmission is minimized (decrease P_i) so that as much as power can be used to transmit artificial noise to confuse the potential eavesdropper (increase P_n) and improve security. In summary, we hope to find the beamforming weight vector w , such that

1) the received $SNRs$ for the information bits are required to be above certain predefined thresholds, and

2) the power occupied to transmit desired information P_i is minimized so that the power available for transmitting artificial noise is maximized.

The optimization problem is:

$$\min_{w} \quad w^H T w$$

$$s.t. \quad w = F_{\perp} v \quad ,$$

$$SNR_1 = \frac{P_2}{\sigma^2} \quad \frac{w^H R_{fg} w}{1 + w^H R_{ff} w} \geqslant \beta_1$$

$$SNR_2 = \frac{P_1}{\sigma^2} \quad \frac{w^H R_{fg} w}{1 + w^H R_{qq} w} \geqslant \beta_2$$

where $F = [a_{fh}, a_{gh}], F_{\perp}$ is the projection matrix onto the null space of F , $\beta_1 > 0$ and $\beta_2 > 0$ are two required receive SNR thresholds. The above problem is the $SOCP$ problem which has a standard solution.

Chapter 5

5.1 Secrecy Scheme with Two Antennas at Source Terminals while Receiving , Friendly Jammer and an Eavesdropper without its CSI

5.1.1 First Phase

The first phase is same as one in case with only eavesdropper except an additional signal from jammer.

$$y_R = \sqrt{(P_1)} f_R s_1 + \sqrt{(P_2)} g_R s_2 + \sqrt{(P_J^{(1)})} h_R z^{(1)} + n_R$$

where, $h_R = [h_{R,1} h_{R,2} \dots h_{R,N-1}]^T$

Similarly, signal received by the eavesdropper will have an additional signal from the jammer.

$$y_E^{(1)} = \sqrt{(P_1)} f_E s_1 + \sqrt{(P_2)} g_E s_2 + \sqrt{(P_J^{(1)})} q_E s_2 + n_E^{(1)}$$

5.1.2 Second Phase

In the second phase, the terminal nodes T_1 and T_2 uses two antenna to receive signal. Denote the channel between the first antenna and relays as $f_1 = [f_{1,1} f_{1,2} \dots f_{1,N}]^T$ and channel between the second antenna and relays as $f_2 = [f_{2,1} f_{2,2} \dots f_{2,N}]^T$. Similarly, the channel between two antennas can be defined as $f_J^{(1)}$ and $f_J^{(2)}$

After the removal of self-interference terms the recieved signal for T_1 can be written as

$$y_{T1}^{(1)} = \sqrt{(P_2)} w^H a_{f1gR} s_2 + \sqrt{(P_J^{(1)})} w^H a_{f1hR} z^{(1)} + \sqrt{(P_J^{(2)})} F_J^{(1)} z^{(2)} + w^H F_1 n_R + n_{T1}^{(1)}$$

$$y_{T1}^{(2)} = \sqrt{(P_2)} w^H a_{f2gR} s_2 + \sqrt{(P_J^{(2)})} w^H a_{f2hR} z^{(1)} + \sqrt{(P_J^{(2)})} F_J^{(2)} z^{(2)} + w^H F_2 n_R + n_{T1}^{(2)}$$

Similarly, for T_2 ,

$$y_{T2}^{(1)} = \sqrt{(P_1)} w^H a_{g1fR} s_1 + \sqrt{(P_J^{(1)})} w^H a_{g1hR} z^{(1)} + \sqrt{(P_J^{(2)})} G_J^{(1)} z^{(2)} + w^H G_1 n_R + n_{T2}^{(1)}$$

$$y_{T2}^{(2)}=\sqrt{(P_1)}w^H a_{g2fR}s_1+\sqrt{(P_J^{(2)})}w^H a_{g2hR}z^{(1)}+\sqrt{(P_J^{(2)})}G_J^{(2)}z^{(2)}+w^H G_2 n_R+n_{T2}^{(2)}$$

Choose, $w=H_{\perp} v$ where, $H=[a_{f1hR}\, a_{f2hR}\, a_{g1hR}\, a_{g2hR}]$ and also choose $z^{(2)}$ such that $z^{(2)}U=0$ where, $U=[F_J^{(1)} F_J^{(2)}]$

Hence,

$$y_{T1}=H_{T1}s_2+n_{T1}$$

$$H_{T1}=\begin{bmatrix}\sqrt{(P_2)}w^H a_{f_1 g_R}\\ \sqrt{(P_2)}w^H a_{f_2 g_R}\end{bmatrix}$$

$$n_{T1}=\begin{bmatrix}w^H F_1 n_R+n_{T1}^{(1)}\\ w^H F_2 n_R+n_{T1}^{(2)}\end{bmatrix}$$

$$H_{n1}=\begin{bmatrix}\sigma^2+\sigma^2(w^H R_{f1f1}w) & 0\\ 0 & \sigma^2+\sigma^2(w^H R_{f2f2}w)\end{bmatrix}$$

where, $R_{f1f1}=F_1 F_1^H, R_{f2f2}=F_2 F_2^H$

Hence,

$$y_{T2}=H_{T2}s_1+n_{T2}$$

$$H_{T2}=\begin{bmatrix}\sqrt{(P_1)}w^H a_{g_1 f_R}\\ \sqrt{(P_1)}w^H a_{g_2 f_R}\end{bmatrix}$$

$$n_{T2}=\begin{bmatrix}w^H G_1 n_R+n_{T2}^{(1)}\\ w^H G_2 n_R+n_{T2}^{(2)}\end{bmatrix}$$

$$H_{n2}=\begin{bmatrix}\sigma^2+\sigma^2(w^H R_{g1g1}w) & 0\\ 0 & \sigma^2+\sigma^2(w^H R_{g2g2}w)\end{bmatrix}$$

where, $R_{g1g1}=G_1 G_1^H, R_{g2g2}=G_2 G_2^H$

Using Rate split Algorithm as used in 4.1.1 , we have the following optimization problem,

$$\min_{w} \quad w^H T w \qquad \textbf{...(9)}$$

$$s.t. \quad w=H_{\perp} v$$

$$|I+H_{T1}H_{T1}^H H_{n1}^{-1}|\geq \eta r$$

$$|I+H_{T2}H_{T2}^H H_{n2}^{-1}|\geq (1-\eta) r$$

where, $T = P_1 R_{ff} + P_2 R_{qq} + P_J^{(1)} R_{hh} + \sigma^2 I$

The above can be rewritten as:

$$\frac{|w^H a_{f1gR}|^2}{\left\|\begin{matrix}\sqrt{(R_{f2f2})}\,w\\ 1\end{matrix}\right\|^2} + \frac{|w^H a_{f2gR}|^2}{\left\|\begin{matrix}\sqrt{(R_{f1f1})}\,w\\ 1\end{matrix}\right\|^2} \geq \gamma_1$$

$$\frac{|w^H a_{g1fR}|^2}{\left\|\begin{matrix}\sqrt{(R_{g2g2})}\,w\\ 1\end{matrix}\right\|^2} + \frac{|w^H a_{g2fR}|^2}{\left\|\begin{matrix}\sqrt{(R_{g1g1})}\,w\\ 1\end{matrix}\right\|^2} \geq \gamma_2$$

Here, on LHS of equation we have sum of two SNRs where each each corresponds to SNR of one antenna instead of one term as in previous case. Hence, to convert it to a standard form, we take one of the SNR of an antenna as a constant equal to some fractional value of γ_1 and γ_2 respectively. Let k_1 and k_2 be that fractional value respectively then above function can be written as

$$\frac{|w^H a_{f1gR}|^2}{\left\|\begin{matrix}\sqrt{(R_{f2f2})}\,w\\ 1\end{matrix}\right\|^2} \geq (1-k_1)\,\gamma_1$$

$$\frac{|w^H a_{g1fR}|^2}{\left\|\begin{matrix}\sqrt{(R_{g2g2})}\,w\\ 1\end{matrix}\right\|^2} \geq (1-k_2)\,\gamma_2$$

where, $0 \leq k_1 \leq 1$ and $0 \leq k_2 \leq 1$. Hence, we can find an ensemble of values of rate for different fractional values for the same channel realisation. Then we can take average for different channel realisation as done in previous scenarios.

The optimization problem can be reformulated as:

$$\min_{w} \quad w^H T w \qquad \textbf{...(10)}$$

$$s.t. \quad |w^H a_{fg}|^2 \geq (1-k_1)\,\gamma_1 \left\|\begin{matrix}\sqrt{(R_{ff})}\,w\\ 1\end{matrix}\right\|^2$$

$$|w^H a_{fg}|^2 \geq (1-k_2)\,\Upsilon_2 \left\| \begin{matrix} \sqrt{(R_{qq})}\,w \\ 1 \end{matrix} \right\|^2$$

where, $\Upsilon_1 = \dfrac{\sigma^2(2^{2\eta r}-1)}{P_2}$, $\Upsilon_2 = \dfrac{\sigma^2(2^{2(1-\eta)r}-1)}{P_1}$

Multiplying the optimal w^o by an arbitrary phase shift will not affect the objective function or the constraints. Therefore, we can assume, without loss of generality, that $w^H a_{fg}$ is a real number The above optimization criteria can be written in the form of Second Order Convex Optimization(SOCP) as :

$$\min_{w} \quad t \qquad \textbf{...(11)}$$

$$s.t. \quad \|\sqrt{(\check{T})}\,\hat{w}\| \leqslant t$$

$$\|\sqrt{(\acute{R}_{ff})}\,\hat{w}\| \leqslant \frac{1}{\sqrt{((1-k_1)\,\Upsilon_1)}}\, real(\bar{a}_{fg}^H \hat{w})$$

$$\|\sqrt{(\acute{R}_{qq})}\,\hat{w}\| \leqslant \frac{1}{\sqrt{((1-k_2)\,\Upsilon_2)}}\, real(\bar{a}_{fg}^H \hat{w})$$

$$[\hat{w}]_{N+2} = 1$$

where, $\hat{w} = [w^T, t, 1]^T$ $\bar{a}_{fg}^H = [a_{fg}^H\, 0\, 0]$

$$\check{\boldsymbol{T}} = \begin{bmatrix} T & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} , \quad \acute{\boldsymbol{R}}_{ff} = \begin{bmatrix} R_{ff} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} , \quad \acute{\boldsymbol{R}}_{qq} = \begin{bmatrix} R_{qq} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

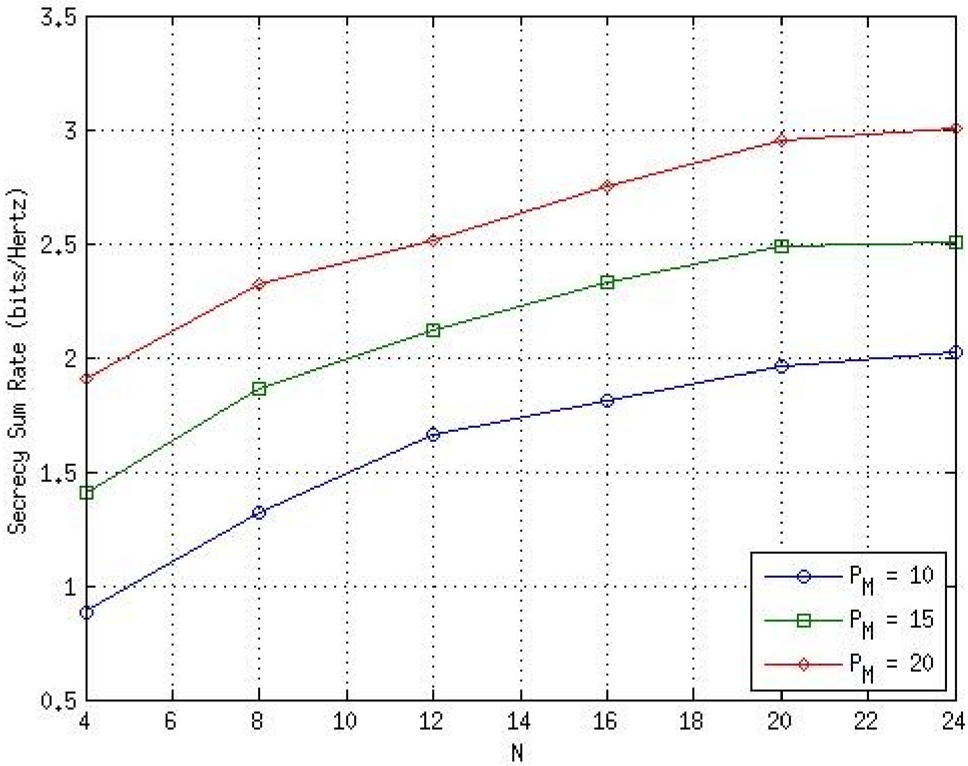
Chapter 6
Simulation Results

In this section, computer simulation results are presented to evaluate the performances of the proposed security schemes. In all the simulation cases, all the channel coefficients , $f_{R,n}, g_{R,n}, c_{E,n}, f_E, g_E$, $n=1,2\ldots N$, are randomly generated in each simulation run, as complex zero-mean Gaussian random vectors with unit covariance. The noise power is normalized to be at $0\,dBW$. We use CVX toolbox to solve the $SOCP$ problem with $Sedumi$ as the solver . Secrecy sum rate is used as the metric of security, which is obtained by averaging $1{,}000$ to $10{,}000$ $Monte\,Carlo$ simulations, unless otherwise stated. Also, to run various simulations all the codes were converted to run in parallel by using $parfor$ loop instead of for loop in $Matlab$. To obtain all the results in less time codes were ran on four different computers in $MAD\,Lab$.

6.1 System with only eavesdropper and eavesdropper's CSI known

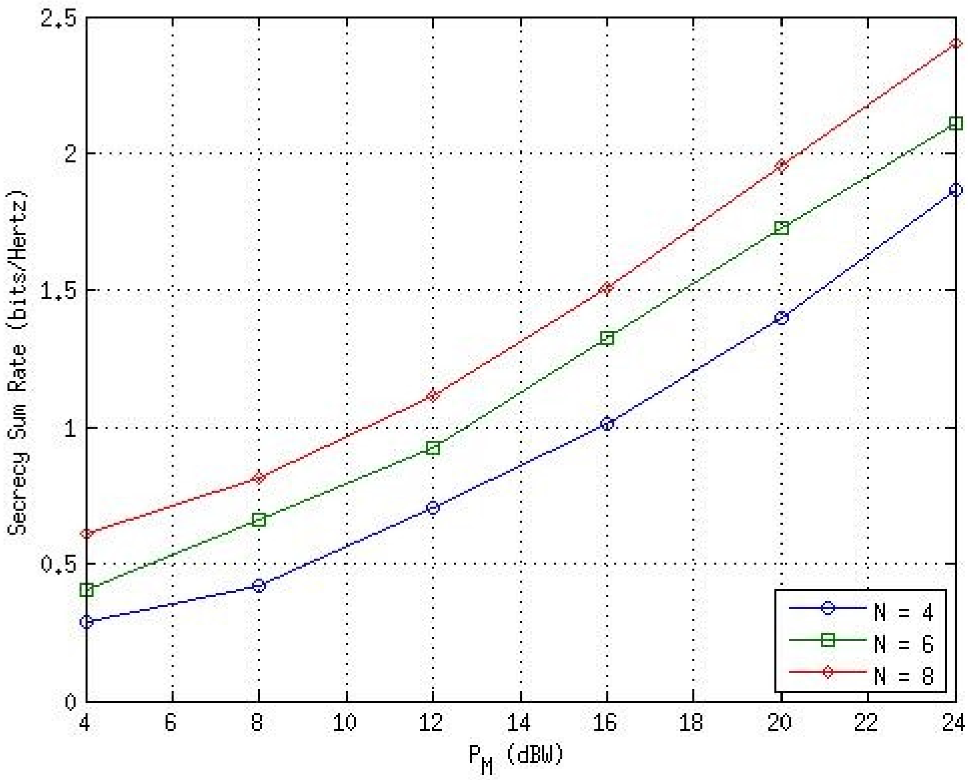
To get the following results, eq **(1)** is maximised which is a concave function with constraint $0 \le P_1 \le \frac{P_M}{2}$ and Matlab function **fminbnd()** can be used to do so. 10,000 Monte-Carlo simulations are performed to get the results.

The following result can be obtained by keeping P_M constant for various values of n as in this case n varies from $(4:4:24)$ and then varying P_M from $(10:5:20)$. Power used by nodes by T_1 and T_2 is $10\,dBW$



As the total available power increases, the secrecy sum rate increase monotonically. Also, for a fixed P_M, increasing the number of relay nodes can enhance the security performance. This is because more relay nodes provide larger array gain to increase the average amount of information exchange in each round between legitimate terminals.

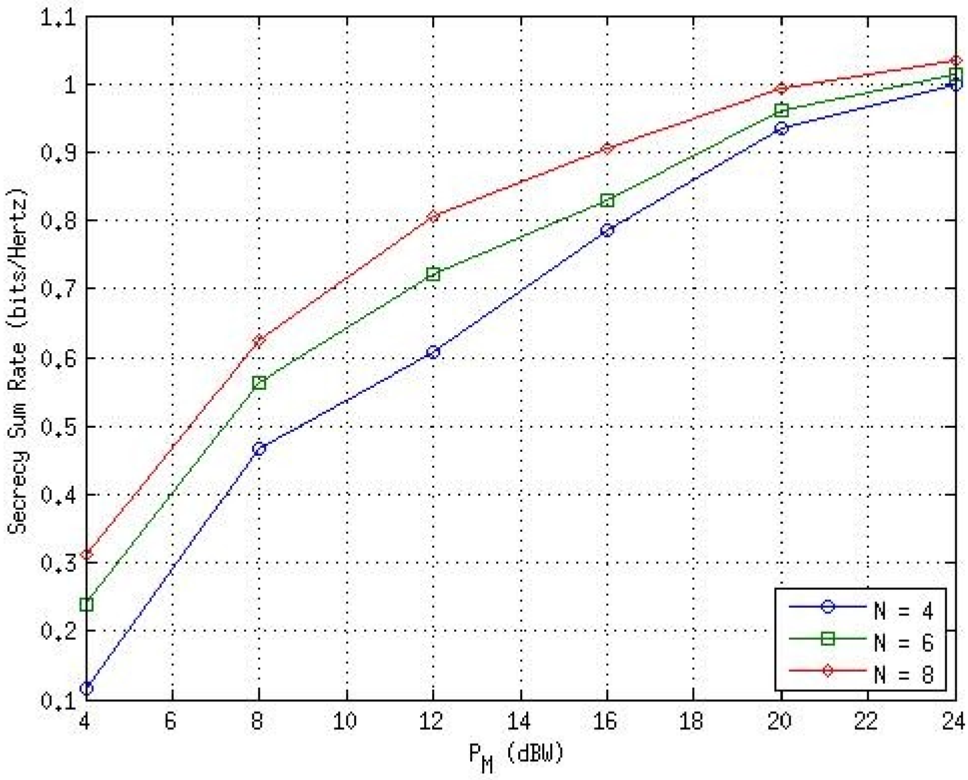
The following result can be obtained by keeping n constant for various values of P_M as in this case P_M varies from (4:4:24) and then varying n from $(4:2:8)$ Power used by nodes by T_1 and T_2 is $10\,dBW$



We can see the secrecy sum rate enhancement per relay nodes goes down as N goes up for any fixed P_M . This is due to the reason that the increase of array gain goes down as the number of antennas (relay nodes) increases.

6.2 System with only eavesdropper and eavesdropper's CSI not known and artificial noise scheme is used

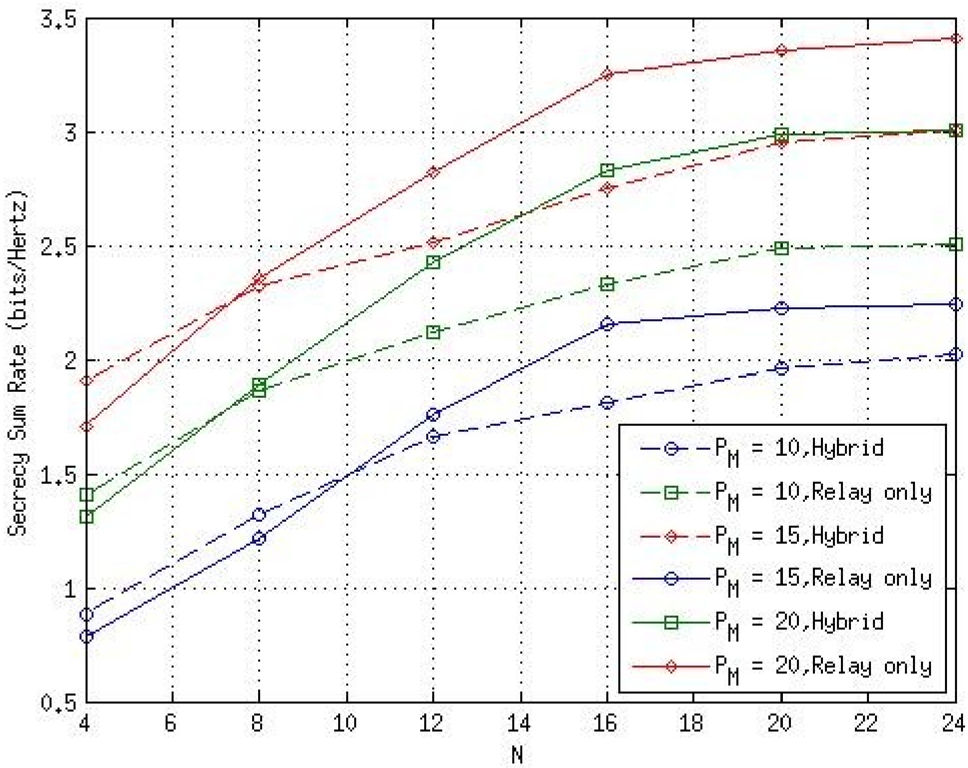
The following result can be obtained by using eq **(4).** To solve this equation CVX toolbox is used with Sedumi as the solver. 10,000 Monte Carlo simulations are performed to get the result. Power used by nodes by T_1 and T_2 is $10\,dBW$.



Although increasing the relay power P_R will enhance secrecy rate, there is a limit of maximum achievable secrecy sum rate even we have unlimited . The limit exists because even with enough relay power, the required receive $SNRs\,\gamma$ are fixed so the information exchange between legitimate terminals do not increase much, while most relay power is used to jam the potential eavesdropper. For any fixed P_R , more relay nodes also increase the secrecy sum rate since more relay nodes provide larger array gain thus decrease the power P_i consumed by information exchange to fulfill the receive SNR requirement, and consequently increase the artificial noise power to jam the eavesdropper.

6.3 System with an eavesdropper and a jammer and eavesdropper's CSI known

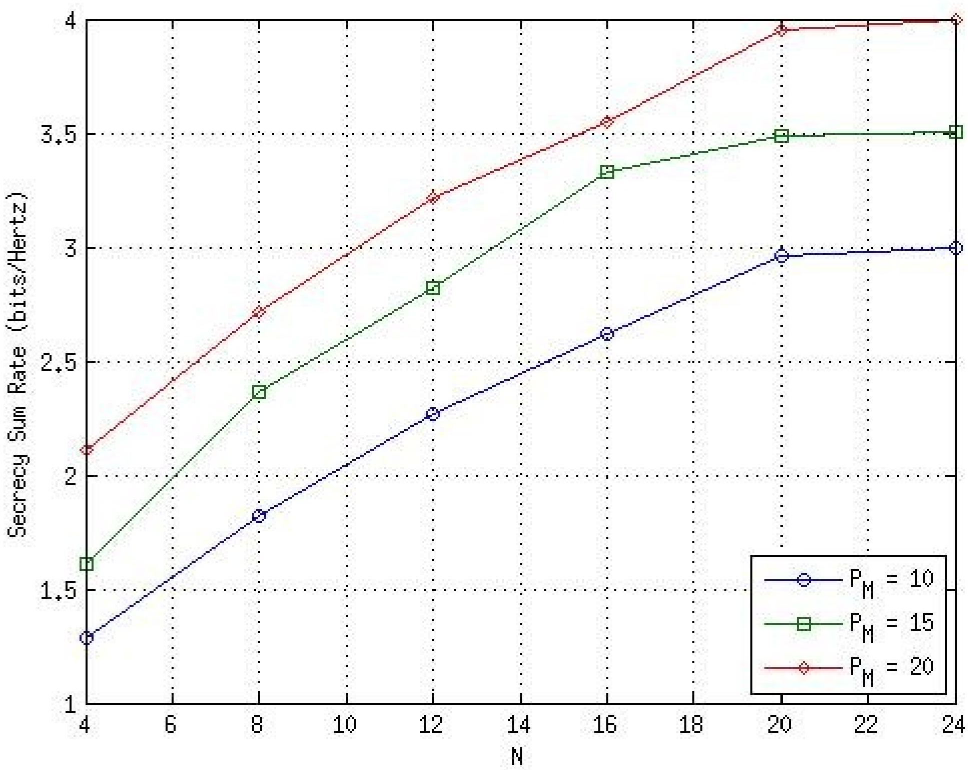
The following result can be obtained by using eq **(8).** To solve this equation CVX toolbox is used with Sedumi as the solver. 10,000 Monte Carlo simulations are performed to get the result. Power used by nodes by T_1 and T_2 is $10\,dBW$



As can be seen by above plot, the scheme with jammer performs better than the scheme without the jammer.

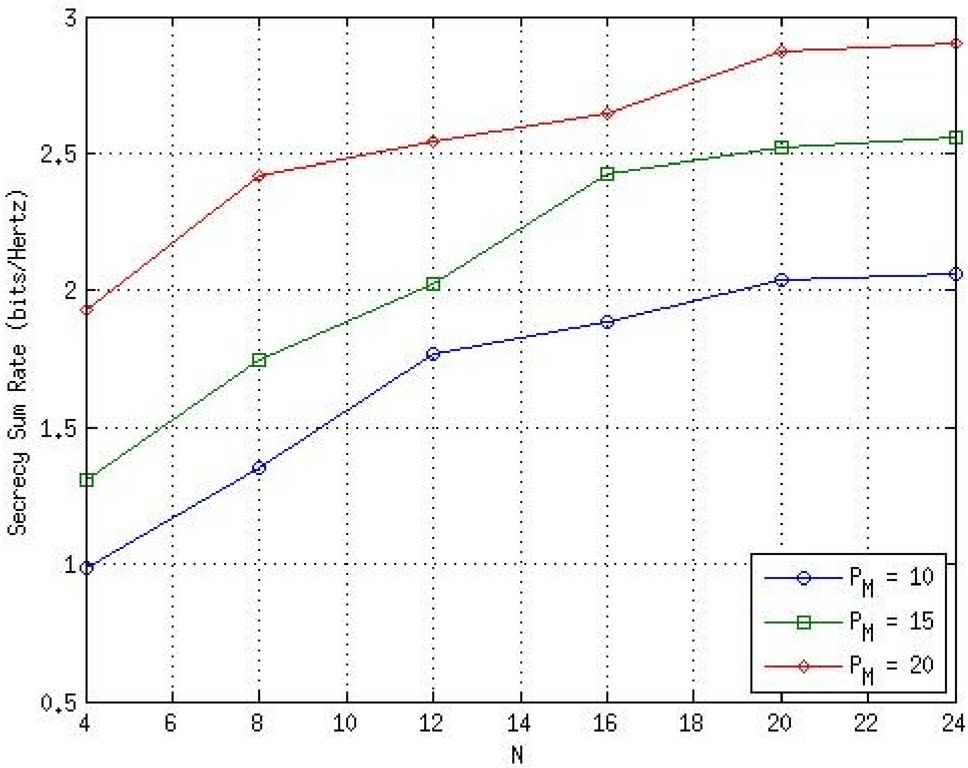
6.4 System with an eavesdropper and a jammer and eavesdropper's CSI not known and Terminals with two antennas are deployed

The following result can be obtained by using eq **(11).** To solve this equation CVX toolbox is used with Sedumi as the solver. 10,000 Monte Carlo simulations are performed to get the result. Power used by nodes by T_1 and T_2 is $10\,dBW$ and power used by jammer in both phase is $5\,dBW$



Clearly, this scheme has higher secrecy rate compared to case with single antenna which shows that using two antennas give advantage over one antenna by increasing the Secrecy Rate.

The following result can be obtained by using eq **(8).** To solve this equation CVX toolbox is used with Sedumi as the solver. 10,000 Monte Carlo simulations are performed to get the result. Power used by nodes by T_1 and T_2 is $5\,dBW$ and power used by jammer in both phase is $5\,dBW$



In the above plot, the terminals T_1 and T_2 use less power compared to the previous case and we the Secrecy Rate almost same as for the single antenna case

Chapter 7
Conclusion

In this work , we have extended the Hybrid Cooperative Relaying and Jamming for Secure Two-Way Relay Networks with terminal nodes having two antennas . As it can observed from the simulation result that for the same scenario as in the single antenna case we observed that secrecy rate has higher value than that of of single antenna case and therefore, we can conclude that for obtaining the same Secrecy rate as for the single antenna scenario , we can use less power from source nodes reducing the total power requirement for the system as a whole. The simulation results so obtained agree with the published results.

Reference

1. **Hui-Ming Wang, Member, IEEE, Qinye Yin, and Xiang-Gen Xia,** Distributed Beamforming for Physical-Layer Security of Two-Way Relay Networks , IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 60, NO. 7, JULY 2012

2. **Hui-Ming Wang, Miao Luo, and Qinye Yin ,** Hybrid Cooperative Relaying and Jamming for Secure Two-Way Relay Networks , Global Communication Conference (GLOBECOM) ,Dec 2012

3. **A. Khisti and G. Wornell,** "Secure transmission with multiple antennas I: The MISOME wiretap channel," IEEE Trans. Inf. Theory, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

4. **E. Tekin and A. Yener,** "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jam-ming," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

5. **V. Havary-Nassab, S. Shahbazpanahi, A. Grami, and Z.-Q. Luo,** "Distributed beamforming for relay networks based on second-order sta-tistics of the channel state information," IEEE Trans. Signal Process., vol. 56, pp. 4306–4316, Sep. 2008.

6. **S. Boyd and L. Vandenberghe**, Convex Optimization. Cambridge, U.K.: Cambridge Univ. Press, 2004.

7. **J. F. Sturm**, "Using SeDuMi 1.02, a Matlab toolbox for optimization over symmetric cones," Optimiz. Methods Softw., vol. 11–12, pp. 625–653, 1999.

8. **A. Mukherjee and A. L. Swindlehurst**, "Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers," in Proc. 11th IEEE SPAWC, Jun. 2010.

9. **R. Zhang, L. Song, Z. Han, B. Jiaa, and M. Debbah,** "Physical layer security for two way relay communications with friendly jammers," in Proc. IEEE GLOBECOM, Miami, FL, 2010.

10. **R. Zhang, Y.-C. Liang, C. C. Chai, and S. Cui,** "Optimal beamforming for two-way multi-antenna relay channel with analogue network coding," IEEE J. Sel. Areas Commun., vol. 27, no. 5, pp. 699–712, Jun. 2009.

11. **F. Oggier and B. Hassibi,** "The secrecy capacity of the MIMO wiretap channel," in Proc. IEEE Int. Symp. Inform. Theory, Toronto, ON, Canada, Jul. 2008, pp. 524–528.

12. **C. E. Shannon**, "Communication theory of secrecy systems," Bell Syst.
Tech. J., vol. 28, pp. 656–715, Oct. 1949.

13. **J. Chen, L. Song, Z. Han,** et al, "Joint relay and jammer selection for secure decode-and-forward two-way relay communications," in Proc. GLOBECOM, Houston, TX, Dec. 2011

14. **A. Khisti and G. Wornell,** "Secure transmission with multiple antennas I: the MISOME wiretap channel", IEEE Trans. Inform. Theory, vol. 56, no. 7, pp. 3088-3104, July 2010.

15. **R. Negi and S. Goel,** "Secret communication using artificial noise," in Proc. IEEE Veh. Tech. Conf., Dallas, TX, Sep. 2005, vol. 3, pp. 1906–1910.

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

17. **A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar,** "On the Gaussian MIMO wiretap channel," in Proc. IEEE Int Symp. Inform. Theory, Nice, France, Jun. 2007, pp. 2471–2475.

18. **S. Shafiee, N. Liu, and S. Ulukus,** “Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel,” IEEE Trans. Inf. Theory, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.