# Secrecy Capacity of a Rayleigh Fading Channel under Jamming Signal

# EAST WEST UNIVERSITY

M.Sc. Research Project on

# Secrecy Capacity of a Rayleigh Fading Channel under Jamming Signal

**Supervisor**

**Dr. M. Ruhul Amin**

Professor<br>
Department of Electronics and Communication Engineering
East West University

And

**Dr. Md. Imdadul Islam**

Professor (Adjunct)
Department of Electronics and Communication Engineering
East West University

**Submitted by**

Habiba Akter
ID: 2016-1-98-002
And
Md. Mojammel Islam
ID: 2016-1-98-005

# Declaration

Hereby we declare that this research project report is an original piece of work carried out by us under the guidance and supervision of **Prof. Dr. M. Ruhul Amin** and **Prof. Dr. Md. Imdadul Islam**. This report is the requirement for the successive completion of M.Sc. in Telecommunication Engineering under the department of  Electronics and Communication engineering.

We state that the report along with its literature that has been demonstrated in this report papers, is our own work with the masterly guidance and fruitful assistance of our supervisor for the finalization of our report successfully.

| | |
|---|---|
| **Signature:** | **Signature:** |
| **-------------------------------** | **------------------------- --** |
| **Habiba  Akter** | **Md. Mojammel Islam** |
| **ID: 2016-1-98-002** | **ID: 2016-1-98-005** |

| | |
|---|---|
| **Signature of Supervisor:**<br><br>**-------------------------------------------------**<br>**Dr. M. Ruhul Amin**<br>**Professor,**<br>Department of Electronics and Communications Engineering,<br>East West university.<br>Dhaka, Bangladesh. | **Signature of Co-Supervisor:**<br><br>**-------------------------------------------------**<br>**Dr. Md. Imdadul Islam** (Adjunct Faculty)<br>**Professor,**<br>Department of Electronics and Communications Engineering,<br>East West university.<br>Dhaka, Bangladesh |

# Approval

This Research Project report on “Secrecy Capacity of a Rayleigh Fading Channel under Jamming Signal” has been submitted to the following board of examiners as a partial fulfillment of the requirements for the award degree Masters of Science in Telecommunication Engineering under the department of Electronics and Communication Engineering on December 2016 by the following students has been accepted as satisfactory.

Habiba Akter  
ID: 2016-1-98-00  
And  
Md. Mojammel Islam  
ID: 2016-1-98-005

| **Signature of supervisor:** | **Signature Co-supervisor:** |
|---|---|
| ------------------------------------------------<br>Dr. M. Ruhul Amin<br>Professor,<br>Department of Electronics and Communications Engineering,<br>East West university.<br>Dhaka, Bangladesh. | ------------------------------------------------<br>Dr. Md. Imdadul Islam (Adjunct Faculty)<br>Professor,<br>Department of Electronics and Communications Engineering,<br>East West university.<br>Dhaka, Bangladesh. |

## Approved By:

**(Dr. M. Mofazzal Hossain)**

Professor & chairperson  
Department of Electronics and Communication Engineering  
East West University, Dhaka, Bangladesh.

# Acknowledgement

We would like to express our gratitude and appreciation to all those who gave us the possibility to complete this research work. A special thanks to our Supervisor **Prof. Dr. M. Ruhul Amin** whose help, suggestions and encouragements helped us to take our thesis especially on Secrecy Capacity.

We express our deepest thanks to our research work Co-Supervisor **Prof. Dr. Md. Imdadul Islam** for his cooperative guidance and support. He supported us by showing different method of information collection while doing this work. He always helped us when required and he gave us right direction towards completion of this work.

We also want to thanks all faculty and staff of Department of Electronics and Communication Engineering of East West University for their full cooperation during the period of the report completion, from the beginning till end. Also thanks to all of our family members, friends and everyone who contributed by supporting our research work and helped us during the research progress till it is fully completed.

# Abstract

In this project work, we deal with physical layer security of a wireless network where the secrecy capacity of the link is considered as the parameter. The impact of received signal to noise ratio (SNR) of legitimate/authorized user, the number of transmitting/receiving antenna elements of multiple input multiple output (MIMO) along with antenna elements of eavesdropper, selection of transmitting antenna element under transmit antenna selection (TAS) scheme are also contemplated. Next the outage probability of the network is determined taking SNR of valid user, number of antenna elements of both transmitter of eavesdropper and threshold value of different of channel capacity as the parameters. Finally, the impact of jammer on normalized channel capacity and outage probability of eavesdropper are analyzed taking signal-to-interference ratio (SIR) of the channel as the ratio of two random variables of fading channel.

## Table of Contents

Chapter 1

Chapter 2

System Model

Chapter 3

Chapter 4

## List of figures

# Chapter 1

## Introduction

# Chapter 1

## 1. Introduction

The wireless network is totally unguided in the communication system; hence any user can intercept signal in-between the transmission of two allowable users. Thus, it is very important to ensure security in wireless network. Traditionally, by applying cryptographic approach at higher layers of protocol stack, security measure is taken [20]. In cryptography-based security system a protocol is designed such that the eavesdropper could not decode the information while the computational power of eavesdropper is considered as limited [14]. However, with the advent of technological advancement the eavesdropper is more powerful now and the mostly implemented security technique used in communication network is at application layer (7th layer of OSI model). There is a relation between throughput and security level of the communication system. Therefore, the network designer has to set the network in optimum position. Data secrecy capacity and outage probability are the main parameters regarding the security of physical layer in MIMO system [1-5]. This paper will discuss the secrecy at the physical layer based on received SNR while using MIMO. We denote the term 'data secrecy capacity' (the maximum transmission rate at which the eavesdropper is unable to decode any information) is equal to the difference between the two channel capacities of legitimate user and eavesdropper [6, 7]. Here outage probability is the probability that the secrecy capacity is less than a threshold. The outage probability of Rician channel are discussed in [8]. A common phenomenon in communication network is the primary user emulator (PUE) attack [9-11] which is also act as eavesdropper. The security model is proposed to combat such attack in [12]. In our paper, we have derived the close form expression of outage probability under secrecy capacity based on Rayleigh and Nakagami-m fading channel [12].

In SDM (space-division multiplexed) fiber optic transmission systems not only the system capacity is increased but also physical layer security against tapping is achieved. In [13] researchers have deal with the information-theoretic security of optical MIMO SDM by evaluating the relation between the maximum information rate and the confidentiality for different channel dynamics. In [14] the passive eavesdropper has increased the data secrecy rate and is able to self-interference suppression (SIS). Friendly jamming is produced by MIMO preceding system. It is the easiest way to remove interference by zero-forcing technique. Transmitter and receiver side power constraints are considered under the MIMO wire trap channel in the exact secrecy capacity. Double side correlation metrics is used in channel input. In the receiver side the artificial noise (cooperative jamming) is produced to transfer energy without sacrificing from the secure rate. Therefore, in MIMO wiretap channel artificial noise is very essential [15]. In [16] a new transmit antenna selection (TAS) scheme is proposed which examines the relationship between feedback overhead and secrecy performance in MIMO wiretap channel. The transmitter selects the two strongest antennas to maximize the instantaneous SNR of the channel. For secure data transmission alamouti coding is applied. The secrecy performance metrics is used to provide valuable insights into TAS-Alamouti. In [17] a broadcast channel sending two independent highly secured data streams to two allowable users with a multi-antenna transmitter in the presence of passive eavesdropper. To improve data secrecy the allowable users are assumed to be capable of self-interference suppression (SIS). Friendly jamming is produced by MIMO precoding system and the interfering signals of two allowable users are removed by employing the zero-forcing technique.  To construct the signals of the allowable users a secrecy encoding scheme is developed. In [18], the secrecy outage in multiple-input-single-output(MISO) systems is analyzed while considering that the transmitter has partial information about the channel and also the eavesdropper. Here, the outage probability of secure transmission is minimized under single-stream beamforming. In [22] Robust beamforming methods are proposed to resist the imperfect channel estimates.

The project work is organized as: chapter 2 provides system model, chapter 3 provides results with explanation and chapter 4 concludes the entire analysis with some recommendation of future works.

# Chapter 2

## System Model

# Chapter 2

# System Model

## 2.1 Overview

Small scale fading is used to describe rapid fluctuation of the signal over a short period of time or short travel distance. Fading is caused by constructive/destructive interference between two or more versions of the transmitted signal (e.g. reflected/diffracted/scattered waves) being slightly out of phase due to the different propagation time. It is a characteristic of radio propagation which is the result of the radio waves generated by the same transmitted signal but arrived at receiver from different direction. They may have different propagation delays/different amplitudes/different phases. The multipath components combine vectorially at the receiver and produce a fade or distortion. The most important effects of small scale fading are rapid changes in signal strength over a small travel distance or time interval, random frequency modulation and time dispersion. There are many factors which influences small scale fading such as- multipath propagation, speed of the mobile, speed of the surrounding objects and transmission bandwidth of the signal. Small scale fading is classified into different types based on different signal and channel parameters. Based on multipath time delay it classified into flat fading and frequency selective fading. Also, based on Doppler spread it is divided into fast fading and slow fading.

## 2.2 MIMO Wiretap Channel

We employ a MIMO wiretap channel where eavesdropper Eve hears the transmitted signal which is transmitted by Alice to communicate with an allowable receiver Bob. During communication, we use a friendly jammer which increases interference at Eve and has full secure cooperation with Bob. This is shown in fig. 1. Bob sends jamming signal to eavesdropper when Bob himself is a full duplex node. In this fig. 1 Eve is working in an interference-limited environment, where we assumed a general model with M random power distributed jamming signals. Multiple antennas are used in all terminals and $N_A$, $N_B$ and $N_E$ are indicating the number of antennas at Alice, Bob, and Eve consequently. There is no effect in the main channel due to the eavesdropper’s channel. The eavesdropper’s channel and the main channel both face slow fading with the same fading block length. Applying the TAS scheme Alice utilizes the CSI of Bob to maximize the received signal to noise ratio (SNR) of Bob. However, Bob considers two receiver combining schemes such as- maximal ratio combining (MRC) and selection combiner (SC). Here, Bob uses MRC to get higher secrecy performance gain but it has higher complexity. Also, Bob uses SC to get low complexity with slightly less secrecy performance gain. On the other hand, Eve uses only MRC scheme as this is the worst case.

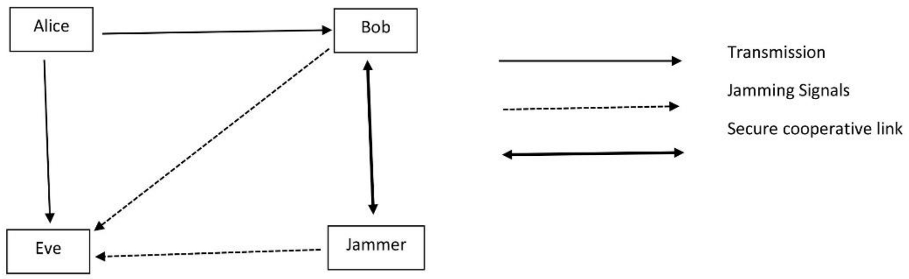

Fig. 2.1 System model.

In fig. 2.2, a MIMO system is shown to transmit signal from Alice to Bob.

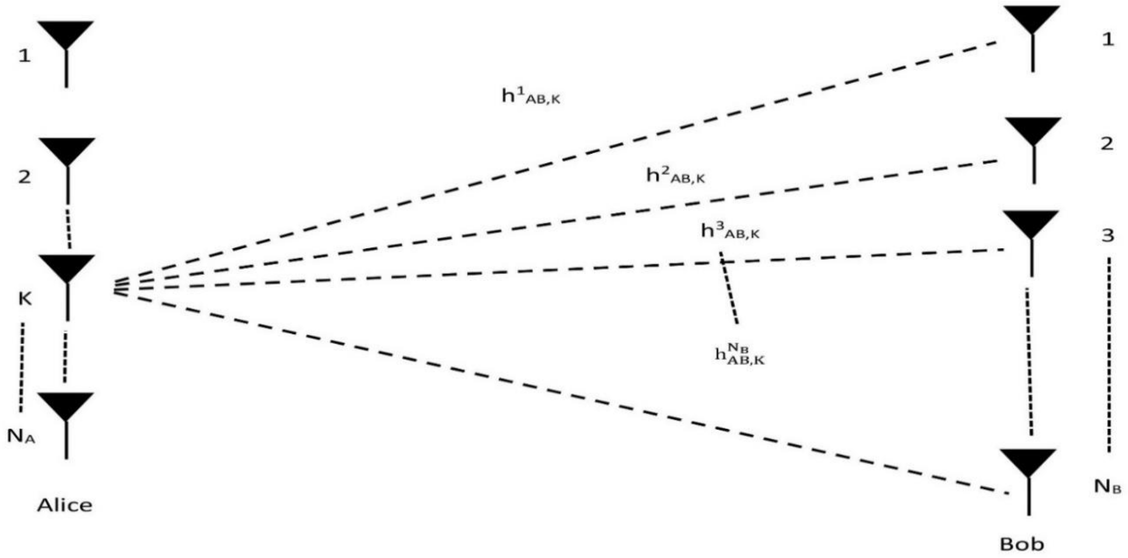

Fig. 2.2 Signal transmission from Alice to Bob.

In fig. 3 a MIMO system is shown where Eve receives the signal transmitted by Alice.

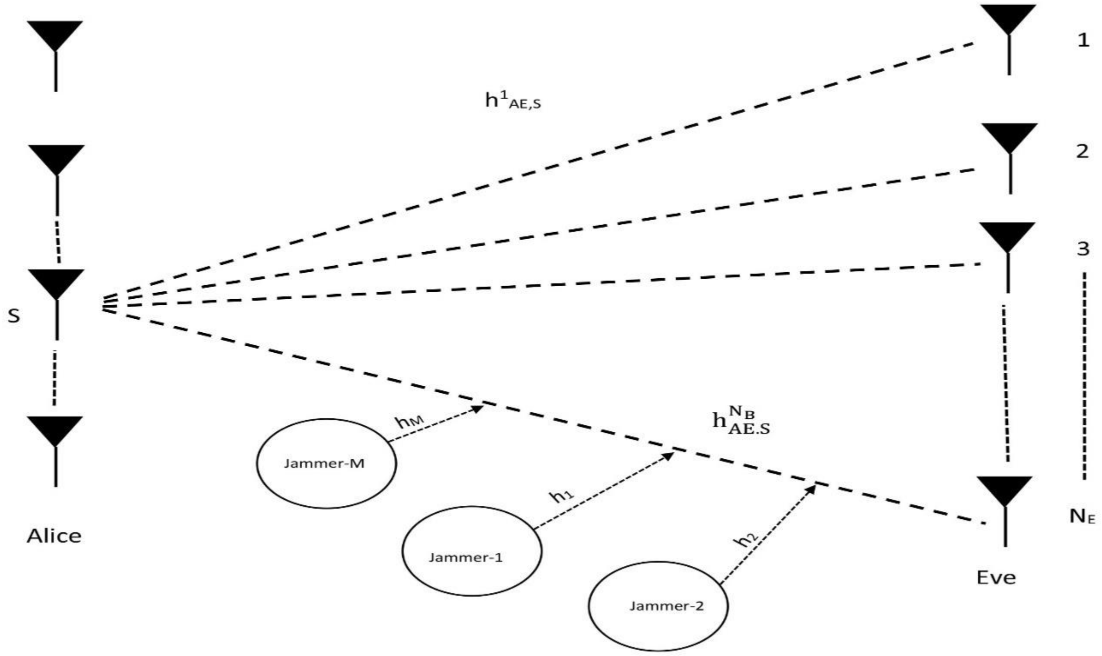

Fig. 2.3 Signal transmission to Eve.

Alice selects the transmit antennas according to the rule

$$S = \mathbf{arg}\max_{k\in\{1,\dots\ \dots\ \dots N_A\}} \ \| \ \mathbf{h}_{AB,k} \ \|, \tag{1}$$

where ‖. ‖ denotes the Frobenius norm and

$$\mathbf{h}_{AB,k} = [h^1_{AB,k}\ \ h^2_{AB,k}\ \ h^3_{AB,k} \dots\ \dots\ \dots h^{N_B}_{AB,k}].$$

Therefore,

$$\| \boldsymbol{h}_{AB,k} \| = \sqrt{\left(h^1_{AB,K}{}^2\right) + \left(h^2_{AB,K}{}^2\right) + \left(h^3_{AB,K}{}^2\right) + \dots \dots \dots + \left(h^{N_B}_{AB,K}{}^2\right)}$$

After selecting 1st antenna Alice evaluates $\| \ h_{AB,1} \|$ then it selects 2nd antenna and evaluate $\| h_{AB,2} \|$. Similarly, Alice selects all antenna and evaluate all corresponding values for

$\| \, h_{AB,S} \|$ and found that the value of $\| h_{AB,S} \|$ is maximum. Here in TAS scheme Alice selects S antenna which is shown in equation 1.

Then, Alice transmit its signal x using the selected antennas and the received signal at BOB is

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_B \end{bmatrix} = \begin{bmatrix} h^1_{AB,S} \\ h^2_{AB,S} \\ h^3_{AB,S} \\ \vdots \\ h^{N_B}_{AB,S} \end{bmatrix} \mathrm{x} + \begin{bmatrix} n_1 \\ n_2 \\ n_3 \\ \vdots \\ n_B \end{bmatrix}$$

$$\Rightarrow \; \boldsymbol{y_B} = \sqrt{P}\, \boldsymbol{h}_{AB,S}\, \mathrm{X} \; + \; \mathbf{n}_B \; . \qquad (2)$$

If BOB uses selection combiner it will use the antenna at which it receives the maximum SNR. If it gets max. SNR at 7th antenna then,

$$\Rightarrow \; y_B = \sqrt{P} \; | \, \mathrm{h}^7_{AB,S} \, | \; \mathrm{X} \; + \mathrm{n}_B \; . \qquad (3)$$

Here,

$$\mathrm{h}^7_{AB,S} \;\; = \; \max \, (h^1_{AB,S} \;\; h^2_{AB,S} \; h^3_{AB,S} \, \ldots \; \ldots \; \ldots h^{N_B}_{AB,S}) \qquad (4)$$

If BOB uses MRC, then the weight vector will be as follows

$$\mathrm{W_B} = \frac{[(\mathrm{h}^1_{\mathrm{AB,S}})^* (\mathrm{h}^2_{\mathrm{AB,S}})^* \; (\mathrm{h}^3_{\mathrm{AB,S}})^* \ldots \ldots \ldots (\mathrm{h}^{\mathrm{N_B}}_{\mathrm{AB,S}})^* \;]}{\sqrt{|\mathrm{h}^1_{\mathrm{AB,S}}\,|^2 + |\mathrm{h}^2_{\mathrm{AB,S}}\,|^2 + \; |\mathrm{h}^3_{\mathrm{AB,S}}\,|^2 + \ldots \; \ldots \ldots + |\mathrm{h}^{\mathrm{N_B}}_{\mathrm{AB,S}}\,|^2}}$$

$$= \frac{\mathbf{h}^{\mathrm{H}}_{\mathrm{AB,S}}}{\| \mathbf{h}_{\mathrm{AB,S}} \|}$$

$$= \; [\mathrm{W_{B1}} \; \mathrm{W_{B2}} \; \mathrm{W_{B3}} \, \ldots \; \ldots \; \ldots \, \mathrm{W_{BN_B}} \; ]. \qquad (5)$$

Hence, the output of the MRC will be

$$\Rightarrow \; \mathbf{y_B} = \sqrt{\mathrm{P}} \, \| \, \mathbf{h}_{\mathrm{AB,S}} \;\; \| \, \mathrm{X} \; + [\mathrm{W_{B1}} \; \mathrm{W_{B2}} \; \mathrm{W_{B3}} \ldots \; \ldots \; \ldots \, \mathrm{W_{BN_B}} \; ] \begin{bmatrix} \mathrm{n_1} \\ \mathrm{n_2} \\ \mathrm{n_3} \\ \vdots \\ \mathrm{n_B} \end{bmatrix}$$

$$= \sqrt{P} \parallel \boldsymbol{h}_{AB,S} \parallel X + \boldsymbol{W}_B\, \boldsymbol{n}_B$$

$$= \sqrt{P}\ \{\textstyle\sum_{i=1}^{N_B} |h_{AB,S}^{i}|^2\}^{\frac{1}{2}}\ x + \sum_{i=1}^{N_B} \boldsymbol{W}_{Bi}\, \boldsymbol{n}_i\ . \qquad (6)$$

The received SNR of BOB will be

$$\gamma_{B,S}^{mrc} = \bar{\gamma}_B \parallel \boldsymbol{h}_{AB,S} \parallel^2. \qquad (7)$$

Here, let us assume $n_b$ is the variance of the elements of $\boldsymbol{n_B}$ .

$$n_B = \frac{\sum_{i=1}^{N_B} (n_i - \bar{n})^2}{\mathrm{N}}$$

$$= \frac{\sum\ (n_i)^2}{\mathrm{N}}\ . \qquad (8)$$

Therefore, average SNR of Bob will be

$$\bar{\gamma}_B = \frac{P}{n_b}\ . \qquad (9)$$

Now we know that friendly jammer means sender willingly sends extra interference to the eavesdropper. The received signal at Eve will be

$$\begin{bmatrix} y_{e1} \\ y_{e2} \\ y_{e3} \\ \vdots \\ y_{N_E} \end{bmatrix} = \sqrt{P} \begin{bmatrix} h_{AE,S}^{1} \\ h_{AE,S}^{2} \\ h_{AE,S}^{3} \\ \vdots \\ h_{AE,S}^{N_E} \end{bmatrix} \mathrm{x} + \begin{bmatrix} \sqrt{\bar{\gamma}}_1 \\ \sqrt{\bar{\gamma}}_2 \\ \sqrt{\bar{\gamma}}_3 \\ \vdots \\ \sqrt{\bar{\gamma}}_M \end{bmatrix}^T \begin{bmatrix} h_1^i \\ h_2^i \\ h_3^i \\ \vdots \\ h_{NE}^i \end{bmatrix} \mathrm{i}$$

$$\Rightarrow \boldsymbol{y_E} = \sqrt{P}\, \boldsymbol{h}_{AE,S}\ \mathrm{X} + \sum_{i=1}^{M} \sqrt{\bar{\gamma}}_i\, \boldsymbol{h}_i, \qquad (10)$$

where $\boldsymbol{h}_{AE,S}$ is the channel component from the selected antenna at Alice to Eve, $\boldsymbol{h}_i$ denotes the $N_B$ ×1 Channel vector between the $i^{th}$ jamming signal and Eve, and $\bar{\gamma}_i$ represents the interference power of the $i^{th}$ jamming signal.

If EVE uses MRC scheme, then

$$y_E = \sqrt{P}\ \frac{\mathbf{h}_{AE,S}^{H}}{\Vert\mathbf{h}_{AE,S}\Vert}\ \boldsymbol{h}_{AE,S}\ .\ \mathrm{x}\ + \textstyle\sum_{i=1}^{M}\ \sqrt{\bar{\gamma}}_i\ \frac{\boldsymbol{h}_{AE,S}^{H}}{\Vert\boldsymbol{h}_{AE,S}\Vert}\ \boldsymbol{h}_i$$

$$\Rightarrow y_E\ = \sqrt{P}\ \frac{[(\boldsymbol{h}_{AB,S}^{1})^{2}(\boldsymbol{h}_{AB,S}^{2})^{2}\ (\boldsymbol{h}_{AB,S}^{3})^{2} \ldots\ldots\ldots (\boldsymbol{h}_{AB,S}^{N_B})^{2}\ ]}{\sqrt{|\boldsymbol{h}_{AB,S}^{1}\,|^2 + |\boldsymbol{h}_{AB,S}^{2}\,|^2 +\ |\boldsymbol{h}_{AB,S}^{3}\,|^2 + \ldots\ldots\ldots + |\boldsymbol{h}_{AB,S}^{N_B}\,|^2}}\ \mathrm{x}\ + \textstyle\sum_{\boldsymbol{i=1}}^{\boldsymbol{M}}\ \sqrt{\bar{\boldsymbol{\gamma}}}_{\boldsymbol{i}}\quad \mathrm{h}_{\mathrm{i}}^{\frown}, \qquad (11)$$

where

$\mathrm{h}_{\mathrm{i}}^{\frown}$ = single element

$$= \frac{\mathbf{h}_{AE,S}^{H}}{\Vert\mathbf{h}_{AE,S}\Vert}\,\boldsymbol{h}_{\boldsymbol{i}}$$

$$= \ \frac{\mathbf{1}}{\Vert\mathbf{h}_{\mathbf{AE,S}}\Vert}\ [(\boldsymbol{h}_{\boldsymbol{AE,S}}^{\mathbf{1}})^{*}(\boldsymbol{h}_{\boldsymbol{AE,S}}^{\mathbf{2}})^{*}\ (\boldsymbol{h}_{\boldsymbol{AE,S}}^{\mathbf{3}})^{*}\ \ldots\ \ldots\ \ldots\ (\boldsymbol{h}_{\boldsymbol{AE,S}}^{\boldsymbol{N_B}})^{*}\ ] \begin{bmatrix} \boldsymbol{h}_{\boldsymbol{i}}^{\mathbf{1}} \\ \boldsymbol{h}_{\boldsymbol{i}}^{\mathbf{2}} \\ \boldsymbol{h}_{\boldsymbol{i}}^{\mathbf{3}} \\ \vdots \\ \boldsymbol{h}_{\boldsymbol{i}}^{\boldsymbol{N_E}} \end{bmatrix}.$$

Here, Eve receives the interference from jammer with its $\mathrm{N}_{\mathrm{E}}$ antenna.

Therefore,

$$\boldsymbol{h}_{\boldsymbol{i}}\ = [\boldsymbol{h}_{\boldsymbol{i}}^{\mathbf{1}}\ \ \boldsymbol{h}_{\boldsymbol{i}}^{\mathbf{2}}\ \ \boldsymbol{h}_{\boldsymbol{i}}^{\mathbf{3}}\ \ldots\ \ldots\ \ldots\ \boldsymbol{h}_{\boldsymbol{i}}^{\boldsymbol{N_E}}\ ]^{\boldsymbol{T}}$$

$$\Rightarrow\ \mathrm{h}_{\mathrm{i}}^{\frown}\ =\ \frac{[(\boldsymbol{h}_{AE,S}^{1})^{*}\ \boldsymbol{h}_{i}^{1}\ (\boldsymbol{h}_{AE,S}^{2})^{*}\boldsymbol{h}_{i}^{2}\ \ (\boldsymbol{h}_{AE,S}^{3})^{*}\boldsymbol{h}_{i}^{3} \ldots\ldots\ldots (\boldsymbol{h}_{AE,S}^{N_B})^{*}\boldsymbol{h}_{i}^{N_E}\ ]}{\sqrt{|\boldsymbol{h}_{AB,S}^{1}\,|^2 + |\boldsymbol{h}_{AB,S}^{2}\,|^2 +\ |\boldsymbol{h}_{AB,S}^{3}\,|^2 + \ldots\ldots\ldots + |\boldsymbol{h}_{AB,S}^{N_B}\,|^2}}, \qquad (12)$$

which is a single element.

Therefore,

$$\mathrm{y}_{\mathrm{E}}\ =\ \sqrt{P}\ \ (\sqrt{|\boldsymbol{h}_{\boldsymbol{AE,S}}^{\mathbf{1}}\,|^{\mathbf{2}}\ +\ |\boldsymbol{h}_{\boldsymbol{AE,S}}^{\mathbf{2}}\,|^{\mathbf{2}}\ +\ \ |\boldsymbol{h}_{\boldsymbol{AE,S}}^{\mathbf{3}}\,|^{\mathbf{2}}\ +\ \ \ldots\ \ldots\ \ldots +\ |\boldsymbol{h}_{\boldsymbol{AE,S}}^{\boldsymbol{N_E}}\,|^{\mathbf{2}}}\ \ )\ \mathrm{x}\ +$$

$$\textstyle\sum_{\boldsymbol{i=1}}^{\boldsymbol{M}}\ \sqrt{\bar{\boldsymbol{\gamma}}}_{\boldsymbol{i}}\quad \mathrm{h}_{\mathrm{i}}^{\frown}$$

$$= \sqrt{P}\ \ \Vert\boldsymbol{h}_{\boldsymbol{AE,S}}\Vert\ \ \mathrm{x}\ \ + \textstyle\sum_{\boldsymbol{i=1}}^{\boldsymbol{M}}\ \sqrt{\bar{\boldsymbol{\gamma}}}_{\boldsymbol{i}}\quad \mathrm{h}_{\mathrm{i}}^{\frown}, \qquad (13)$$

where $\bar{\gamma}_i$ is the average interference power of the $i^{th}$ jammer.

Now SNR at Eve will be

$$\gamma_{\mathrm{E,S}} = \bar{\gamma}_E \, \|\boldsymbol{h}_{\boldsymbol{AE,S}}\|^2 \tag{14}$$

And SIR (signal to interference ratio) of Eve will be

$$\gamma_{\mathrm{E}} = \frac{\gamma_{E,S}}{\gamma_I}\,, \tag{15}$$

where $\gamma_I$ is the interference power of Eve and it will be

$$\gamma_I = \sum_{\boldsymbol{i=1}}^{\boldsymbol{M}} \left(\sqrt{\bar{\boldsymbol{\gamma}}}_{\boldsymbol{i}}\, \tilde{\mathrm{h}}_{\mathrm{i}}\right)^2$$

$$= \sum_{\boldsymbol{i=1}}^{\boldsymbol{M}} \bar{\gamma}_i \,|\, \tilde{\mathrm{h}}_{\mathrm{i}}| \,.$$

## 2.3 Secrecy Capacity of Wireless Link:

Since SIR is the ratio of two random variables *x* and *y* hence SIR becomes another random variable,

$$\mathrm{Z} = \frac{x}{y}\,.$$

Then the cumulative distribution function (CDF) of z will be

$$\mathrm{R_z}\,(\tau) = \int_0^\infty \mathrm{p}\{\, \frac{\mathrm{x}}{\mathrm{y}} \le \tau \mid \mathrm{y}\,\}\, \mathrm{g_y(y)\, dy}$$

$$= \int_0^\infty \mathrm{p}\{\, \mathrm{x} \le \tau\mathrm{y} \mid \mathrm{y}\,\}\, \mathrm{g_y(y)\, dy}$$

$$= \int_0^\infty \mathrm{F_x}(\tau\mathrm{y})\, \mathrm{g_y(y)\, dy}\,. \tag{16}$$

For Rayleigh fading,

$$g_y\,(\mathrm{y}) = \frac{1}{y_{av}}\, e^{-\frac{y}{y_{av}}} \tag{17}$$

$$F_x\,(X) = 1 - e^{-\frac{X}{X_{av}}}$$

$$\Rightarrow\; F_X(\tau Y) = 1 - e^{-\frac{\tau y}{X_{av}}}\,. \tag{18}$$

Therefore,

$$R_z\ (\tau) = \int_0^\infty \left(\frac{1- e^{-\frac{\tau y}{X_{av}}}}{y_{av}}\ e^{-\frac{y}{y_{av}}}\right)\mathrm{dy}\ , \tag{19}$$

and

$$R_z\ (\tau) = \frac{1}{y_{av}}\int_0^\infty \mathrm{e}^{-\frac{\mathrm{y}}{\mathrm{y_{av}}}}\ \mathrm{dy}\ -\ \frac{1}{y_{av}}\int_0^\infty e^{-y\ \left(\frac{\tau}{x_{av}}+\frac{1}{y_{av}}\right)}\ \mathrm{dy}$$

$$=\ \frac{y_{av}}{y_{av}}[\mathrm{e}^{-\frac{\mathrm{y}}{\mathrm{y_{av}}}}]_0^\infty +\ \frac{1}{y_{av}}\ [\frac{e^{-y\ \left(\frac{\tau}{x_{av}}+\frac{1}{y_{av}}\right)}}{\left(\frac{\tau}{x_{av}}+\frac{1}{y_{av}}\right)}]_0^\infty$$

$$= [\ 0 - \ 1\ ]\ +\ \frac{1}{y_{av}}\left[0 - \frac{1}{\left(\frac{\tau}{x_{av}}+\frac{1}{y_{av}}\right)}\right]$$

$$= 1 - \frac{1}{\left(\frac{\tau y_{av}}{x_{av}}+1\right)}$$

$$\Rightarrow R_z\ (\tau) = 1 - \frac{x_{av}}{\tau y_{av}\ + x_{av}}\ \ . \tag{20}$$

Now the probability density function (PDF) of $\tau$ will be,

$$\frac{dR_Z(\tau)}{d\tau} = -\ \mathrm{x_{av}}\ \{\ -\ \frac{y_{av}}{(\ \tau y_{av}\ + x_{av}\ )^2}\}$$

$$=\ \frac{y_{av}\ x_{av}}{(\ \tau y_{av}\ + x_{av}\ )^2}$$

$$= f_Z(\tau). \tag{21}$$

If the received SNR of Bob is $\gamma_B$ and that of Eve is $\gamma_E$ then the PDFs of the above random variables are:

Rayleigh Fading case [23-25] of Bob:

$$f_{\Gamma_B}(\gamma_B) = \frac{1}{\gamma_{B\_av}} e^{-\frac{\gamma_B}{\gamma_{B\_av}}}\ . \tag{22}$$

Eve’s under Rayleigh Fading case,

$$f_{\Gamma_E}(\gamma_E) = \frac{1}{\gamma_{E\_av}} e^{-\frac{\gamma_E}{\gamma_{E\_av}}} \quad . \tag{23}$$

The normalized secrecy capacity will be [26],

$$C_S = \int_0^\infty \int_0^\infty \{ \, log\,(1-\gamma_B) - log\,(1-\gamma_B) \} f_{\Gamma_B}(\gamma_B) . f_{\Gamma_E}(\gamma_E)\, d\gamma_B\, d\gamma_E \, , \tag{24}$$

where the normalized channel capacity of Bob and Eve are $C_B = \log_2(1+\gamma_B)$ and $C_E = \log_2(1+\gamma_E)$ respectively.

Let us consider the following hypothesis [8]:

$$\mathrm{H} = \begin{cases} \mathrm{C_B - C_E} \; ; & \mathrm{C_B > C_E} \quad . \\ 0 \; ; & \mathrm{C_B < C_E} \end{cases} \tag{25}$$

Now, the probability of successful detection,

$$\begin{aligned} P_\tau &= P_r\{H > \tau\} \\ &= P_r\{C_B\text{-}C_E > \tau\}, \end{aligned}$$

which can be written as

$$P_\tau = \int_0^\infty f_{\Gamma_E}(\gamma_E) \left\{ \int_{(1+\gamma_E)e^h - 1}^{\infty} f_{\Gamma_B}(\gamma_B) . d\gamma_B \right\} d\gamma_E \, . \tag{26}$$

The outage probability is

$$P_{out} = 1\text{-}\, P_\tau \, . \tag{27}$$

For Rayleigh fading case, we have

$$P_\tau = \int_0^\infty \frac{1}{\gamma_{E\_av}} e^{-\frac{\gamma_E}{\gamma_{E\_av}}} \left\{ \int_{(1+\gamma_E)e^h - 1}^{\infty} \frac{1}{\gamma_{B\_av}} e^{-\frac{\gamma_B}{\gamma_{B\_av}}} . d\gamma_B \right\} d\gamma_E \, .$$

By simplifying the above equation, we get the closed form solution of probability of successful detection as,

$$P_\tau = \frac{e^{-\frac{e^h - 1}{\gamma_{B\_av}}}}{\gamma_{B\_av}^2 \gamma_{E\_av} \left( \frac{1}{\gamma_{E\_av}} + \frac{e^h}{\gamma_{B\_av}} \right)} \quad . \tag{28}$$

# Chapter 3

## Results

# Chapter 3

## 3. Results

This section provides results using MRC scheme at receiving end of legitimate user under Rayleigh fading environment. Fig. 3.1 shows the variation of average secrecy capacity against the received SNR (in dB) of legitimate user. Here the received SNR of eavesdropper (in dB) and number of received antennas $N_B$ of legitimate user (Bob) is taken as a parameter. The secrecy capacity increases with increase in SNR of Bob and the number of received antenna of Bob. The secrecy capacity only decreases with increase in SNR of eavesdropper visualized from fig. 3.1 to 3.3. The fig.3.1 shows the profile of average secrecy capacity under TAS (transmit antenna selection) scheme, fig. 3.2 shows the same profile taking two antennas of Alice i.e. $N_A$ = 2 and the fig.3 for $N_A$ = 4. The secrecy capacity increases very small amount with increase in $N_A$ visualized from fig. 3.1 to 3.3. All the curves of fig. 3.1 to 3.3 have 3 parts: linearly rising part, saturation or non-linear part and linearly falling portion. All the curves are also drowned for $N_B$ = $N_E$. For larger value of $N_B$ = $N_E$ the secrecy capacity attains at is saturated level earlier i.e. the peak value of secrecy capacity is found at lower level of received SNR. The phenomenon becomes more severe for larger number of antenna elements $N_A$ of Alice visualized from the fig.3.1 to 3.3 together since received SNR of Eve will be higher for larger number of $N_A$. The secrecy capacity falls sharply after its peak amplitude. For larger number antenna elements of Eve, the secrecy capacity of Bob will fall for smaller value of his received SNR. Actually, the theory of secrecy capacity was developed using the concept like: the secrecy capacity will be higher when the difference between SNR of Bob and Eve is larger. When the SNR of Bob is increased to keep the 'difference between SNR of Bob and Eve' far larger, then the SNR of Eve rose above the threshold to detect the signal of Alice. Therefore, the SNR of Bob can be increased beyond a threshold SNR so that SNR of Eve is always below the threshold of signal detection. The peak amplitude of the curves of fig.3.1-3.3 indicates the threshold SNR of Bob. Above dilemma can be avoided applying jammer towards Eve hence SNR of Bob can be increased beyond the threshold NSR of above case. The profile of secrecy capacity before attaining saturation is shown in fig.4 taking the number of antennal elements of Alice and Eve as: $N_A$ = 4 and $N_E$ = 2.

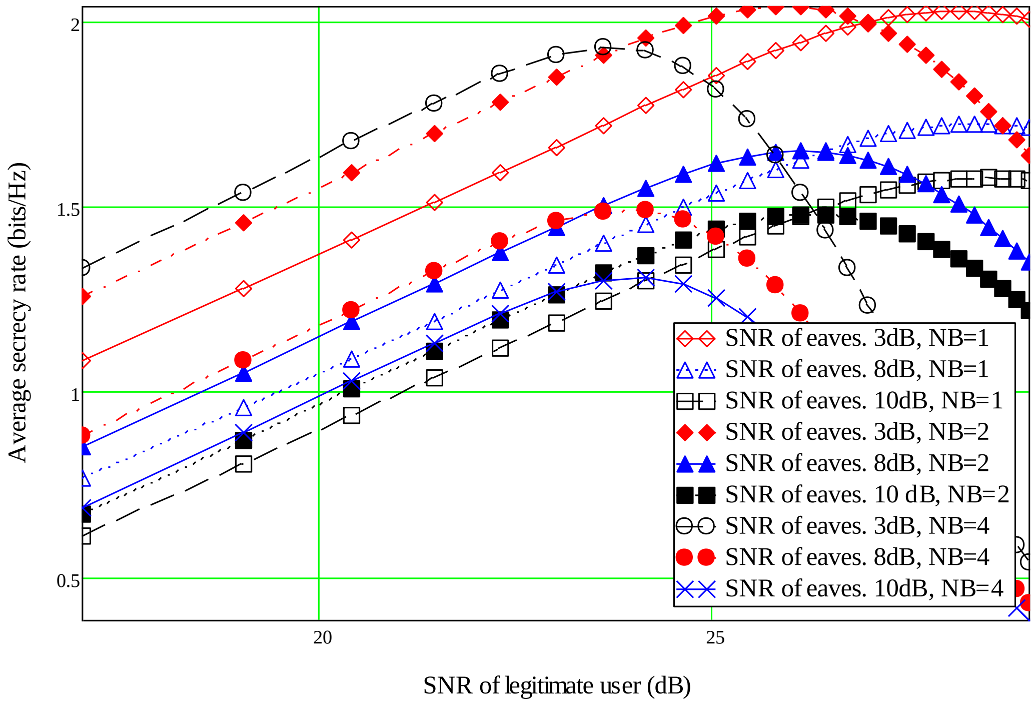

Fig.3.1 Variation of average secrecy capacity against received SNR under TAS scheme.

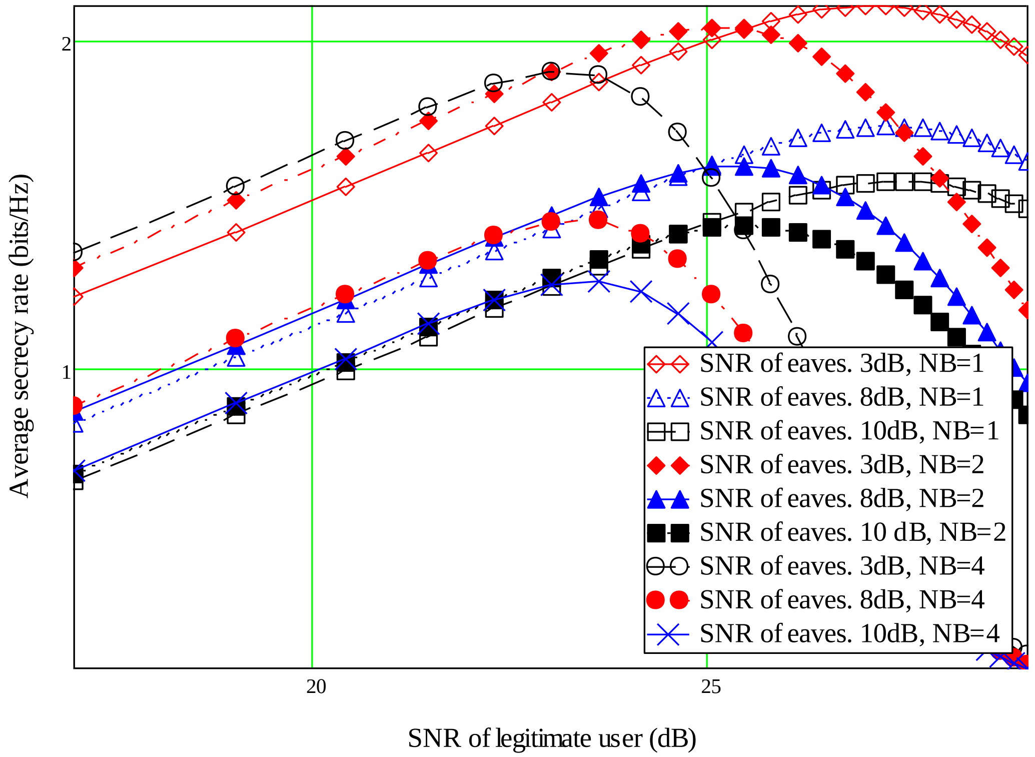

Fig.3.2 Variation of average secrecy capacity against received SNR taking $N_A = 2$.

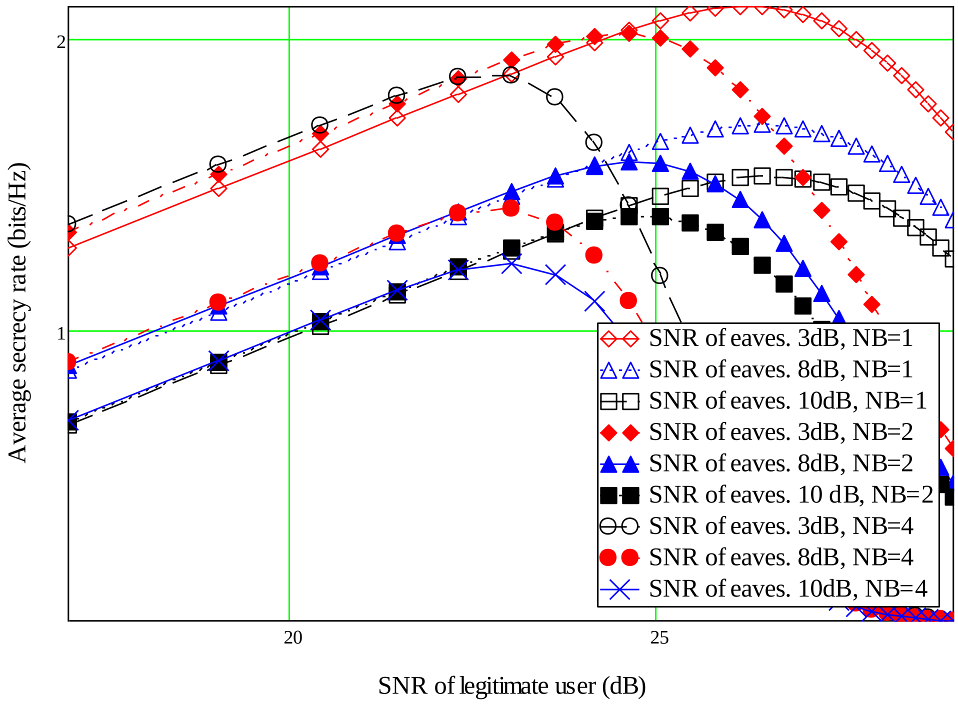

Fig.3.3 Variation of average secrecy capacity against received SNR taking $N_A = 4$.

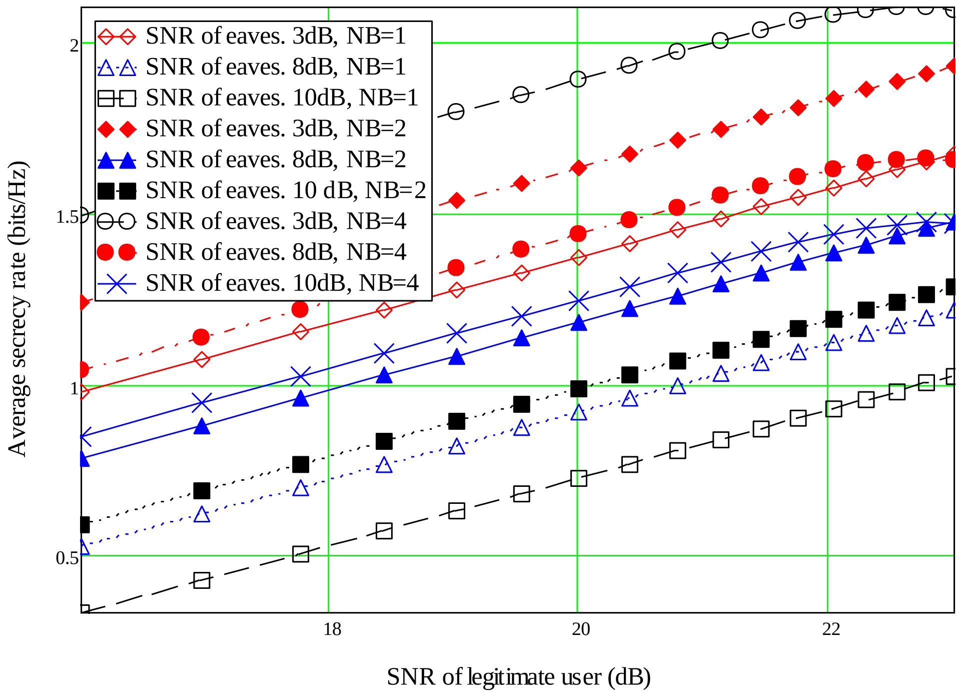

Fig.3.4 Variation of average secrecy capacity against received SNR before attaining saturation taking $N_A = 4$ and $N_E$=2.

Next, we plot the outage probability of Bob against the received average SNR taking the number of antenna element $N_B$ and threshold value of the difference $h = C_B\text{-}C_E$ as the parameter. The outage probability decreases with increase in average SNR of Bob and the number of antenna elements $N_B$. The outage probability increases with increase in threshold value h while other parameters are kept fixed. Above profiles are shown in fig 3.5 to fig.3.6 taking the number of antenna elements of Alice, $N_A$=1, 2 and 3. The outage probability also decreases with increase in $N_A$ are visualized from combination of fig. 3.5 to 3.7 since outage probability solely depends on received SNR.

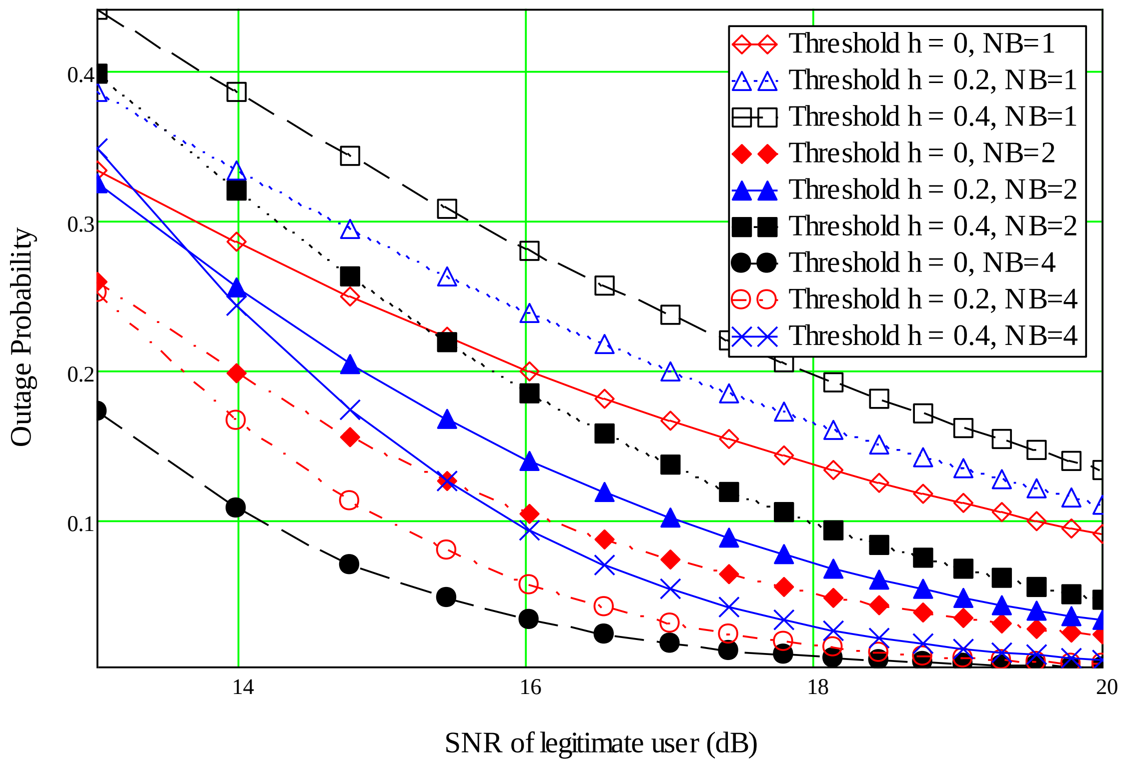

Fig. 3.5 Profile of outage probability against received SNR under TAS scheme.

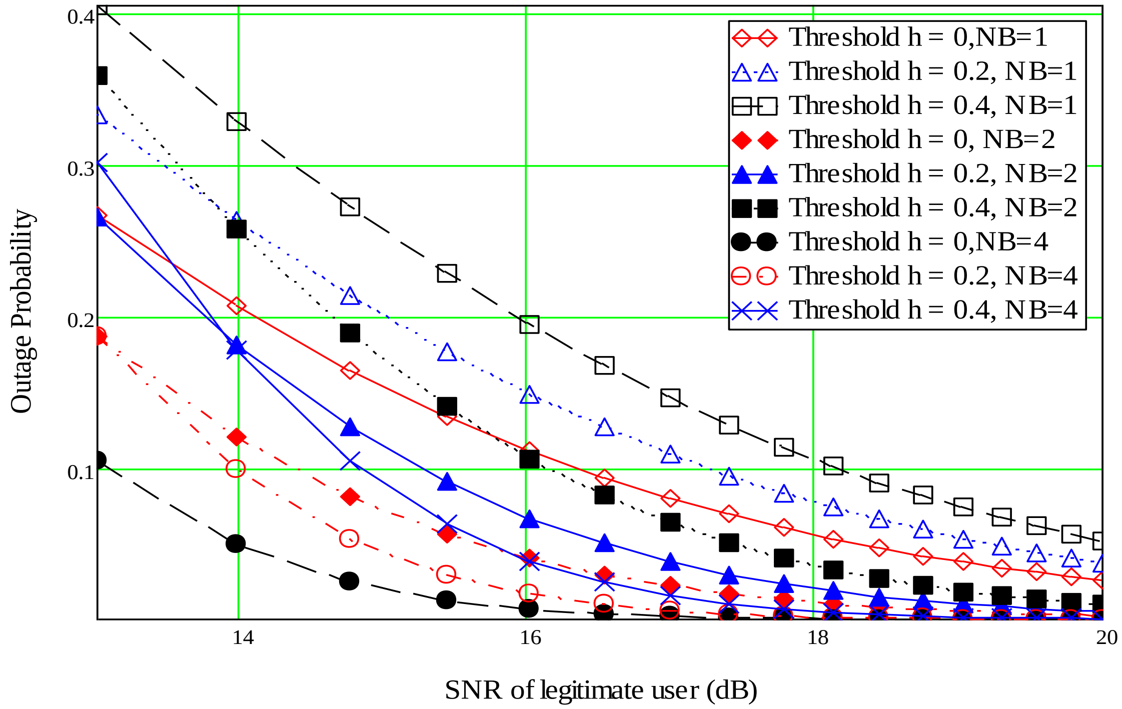

Fig. 3.6 Profile of outage probability against received SNR taking $N_A = 2$.

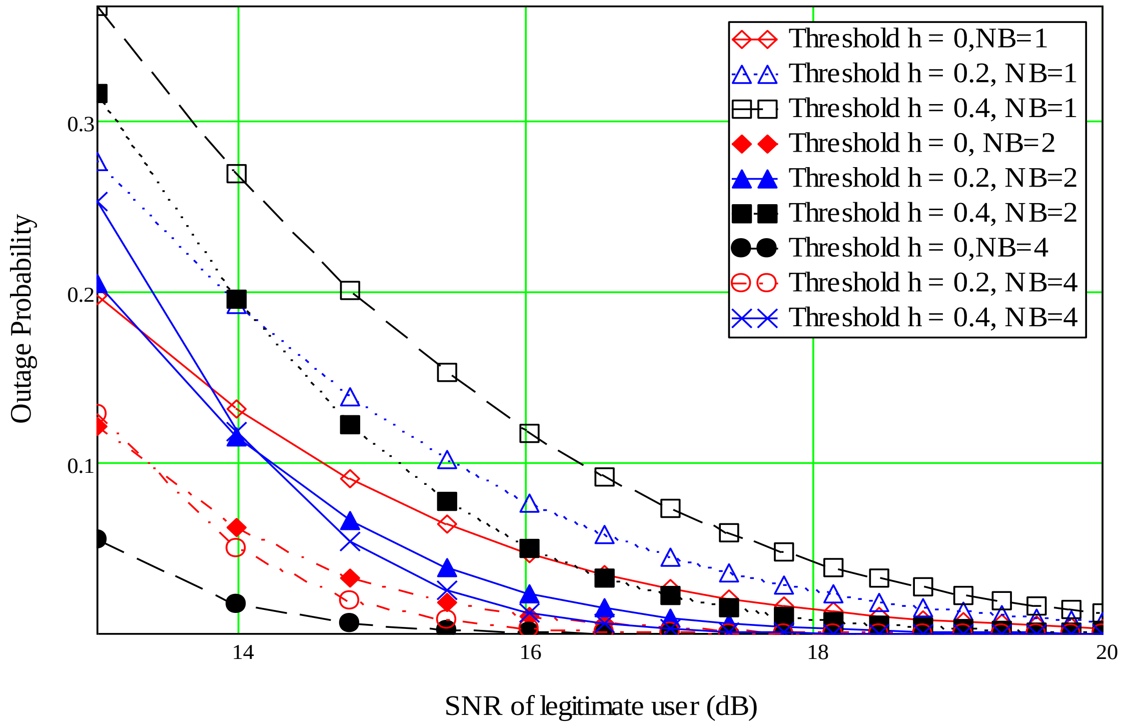

Fig. 3.7 Profile of outage probability against received SNR taking $N_A = 4$.

The next part of the results will deal with impact of jamming signal on secrecy capacity of eavesdropper. Fig. 3.8 shows the variation of secrecy capacity of Eve against interference level (in dB) of jammer taking SNR of Eve as a parameter. The secrecy capacity of Eve decreases exponentially with increase in signal level of jammer. The secrecy capacity of Eve is only comparable with Bob when Eve can maintain her SNR above 25 dB which is very difficult for practical wireless network.

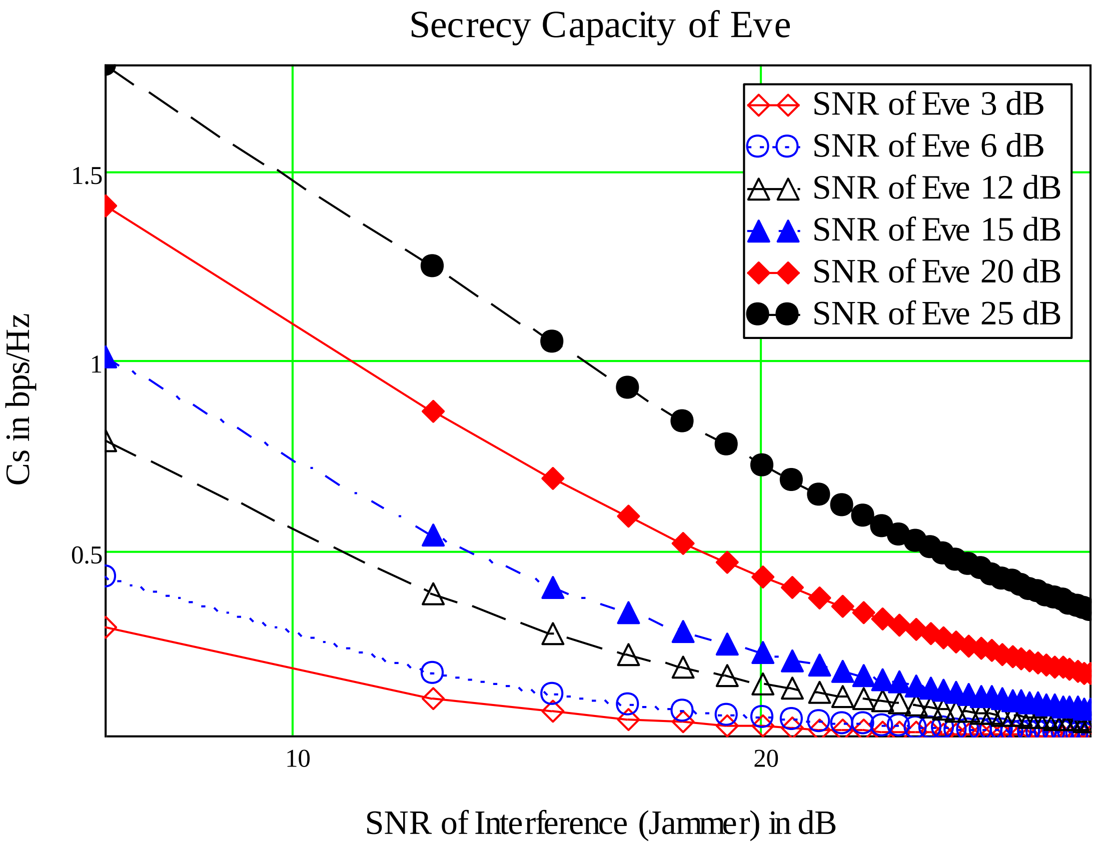

Fig. 3.8 Variation secrecy capacity of Eve against SNR of jammer at receiving end of Eve.

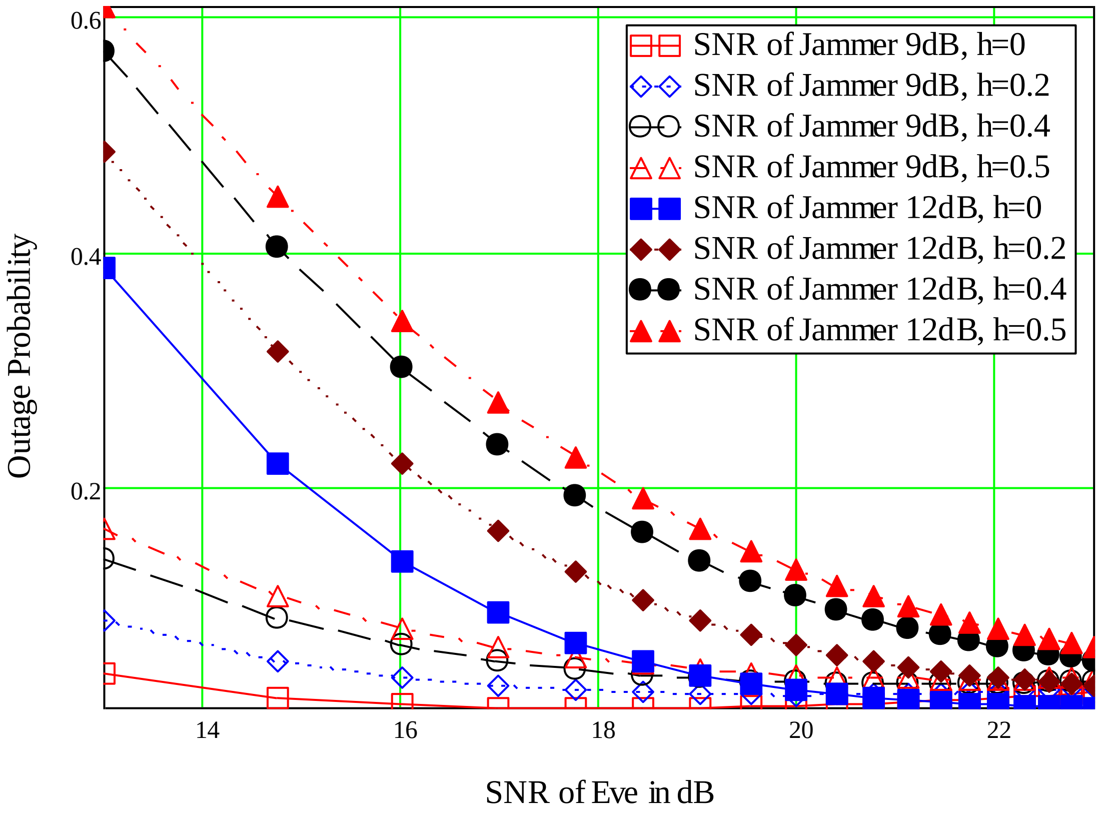

Fig.3.9 Profile of outage probability of Eve against received SNR, taking SNR of jammer and *h* as a parameter.

Fig.3.9 shows the variation of outage probability of Eve against her received SNR taking level of jammer and h as parameters. The outage probability increases with increase in jammer level and h. The outage probability is found above 40% with SNR of Eve at the level of 15dB hence Eve will loss with loss huge number of frame segments of encrypted data.  In this case message digest function is SHA-1 (Secure Hash Algorithm-1) will ensure the security of the network.

# Chapter 4

## Conclusions and Future Works

# Chapter 4

## 4. Conclusions and Future Works

In this research project the performance of a Rayleigh Fading channel in circumstances of 'secrecy capacity' and 'outage probability' of allowable users are described. We introduced a friendly jammer and assuming MRC scheme at receiving end of legitimate user, closed-form expressions for the average secrecy rate and secrecy outage probability were derived. The analytical results corroborate our analytical approach. Here we consider only Rayleigh Fading environment but we can use other fading environments like: Nakagami-m, Rician, Weisul and k-fading. For a network of short link, we can use simple pathloss model to observe the impact of distance on performance of the network. We have the scope to use 2-hop wireless link and observe the improvement of the system. Entire work is analytical but we can use simulations to verify the analysis.

## REFERENCES

**[1]** Bibhash R., Gautam R. and Ritwik C., “Enhanced key Generation Scheme based Cryptography with DNA Logic,” International Journal of Information and Communication Technology Research, vol. 1, no. 8, pp.370-374, 2011.

**[2]** Diaa S., Hatem A. and Mohiy H., “Studying the Effects of Most Common Encryption Algorithms,” International Arab Journal of e-Technology, vol. 2, no. 1, pp.1-10, 2011.

**[3]** Poonam J. and Brahmjit S., “Study and Performance Evaluation of Security-Throughput Tradeoff with Link Adaptive Encryption Scheme,’ International Journal of Security,” Privacy and Trust Management (IJSPTM), vol. 1, no. 5, pp.13-26, October 2012.

**[4]** Mohamed E., Mostafa A. and Abdelmalek A., “Improving TLS Security by Quantum Cryptography,” International Journal of Network Security & Its Applications (IJNSA), vol.2, no.3, pp.87-100, 2010.

**[5]** Mohamed H., Chetan N., Chandramouli R., and Subbalakshmi K., “Opportunistic Encryption: A Trade-Off between Security and Throughput in Wireless Networks,”’ IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 4, pp.313-324, 2007.

**[6]** Hyoungsuk J., Namshik K., Minki K. Hyuckjae L. and Jeongseok H., “Secrecy Capacity over Correlated Ergodic Fading Channel,” IEEE Transaction on Information Theory, vol. 1, no.30, pp. 1-18, 2008.

**[7]** Praveen K., Lifeng L. and Hesham G., “On the Secrecy Capacity of Fading Channels,” IEEE Transactions on Information Theory, vol. 54, no. 10, pp. 4687 – 4698, 2008.

**[8]** Xian L., “Probability of Strictly Positive Secrecy Capacity of the Rician-Rician Fading Channel” IEEE Wireless Communications Letters, vol. 2, no. 1, pp.50-53, 2013.

**[9]** Dac-Binh H., Phu-Tuan V. and Truong T., “Physical Layer Secrecy Performance Analysis over Rayleigh/Nakagami Fading Channels,” Proceedings of the World Congress on Engineering and Computer Science, vo. II, pp. 22-24, San Francisco, USA October, 2014.

**[10]** Fatty M., Maged H. and Ibrahim I., “Energy Detection Based Sensing for Secure Cognitive Spectrum Sharing in the Presence of Primary User Emulation Attack,” IEEK Transactions on Smart Processing and Computing, vol. 2, no. 6, pp.357-366, 2013.

**[11]** Jianwu L, Zebing F., Zhiqing W., Zhiyong F. and Ping Z., “Security management based on trust determination in cognitive radio networks,” EURASIP Journal on Advances in Signal Processing, vol. 2014 /1/48 pp.1-16, 2014.

**[12]** Zou, X. and Shen W., “Physical-Layer Security Against Eavesdropping Attack with Multiuser Scheduling in Cognitive Radio Networks,” IEEE Trans. Commun., vol.61, no.12, pp.5103-5113, 2013.

**[13]** Kyle Guan, Peter J. Winzer,Antonia M.Tulino, Emina Soljanin,"Physical Layer Security of space Division Multiplexed Fiber-Optic Communication Systems in the Presence of Multiple Eavesdroppers", Global Communications Conference (GLOBECOM) 2015 IEEE, pp. 1-6, 2015.

**[14]** Akgun, Berk, O. Ozan Koyluoglu, and Marwan Krunz. "Receiver-Based Friendly Jamming With Single-antenna Full-duplex Receivers in a Multiuser Broadcast Channel." 2015 IEEE Global Communications Conference (GLOBECOM). IEEE, 2015.

**[15]** Banawan, Karim, and Sennur Ulukus. "MIMO Wiretap Channel Under Receiver-Side Power Constraints with Applications to Wireless Power Transfer and Cognitive Radio." IEEE Transactions on Communications 64.9 (2016): 3872-3885

**[16]** Yan, Shihao, et al. "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels." IEEE Transactions on Wireless Communications 13.3 (2014): 1656-1667.

**[17]** B.Schneier,“Cryptographic design vulnerabilities,” Computer,vol.31,no.9,pp.29–33, 1998, doi:10.1109/2.708447.

**[18]** S.Gerbracht,C.Scheunert,and E.Jorswieck,“Secrecy outage in MISO Systems with partial channel information,” IEEE Trans.Inf.Forens.Secur., vol.7, no.2, pp.704–716,2012, doi: 10.1109 /TIFS. 2011.2181946.

**[19]** Pei, Minyan, et al. "Adaptive limited feedback for MISO wiretap channels with cooperative jamming." IEEE Transactions on Signal Processing 62.4 (2014): 993-1004.

**[20]** C.Shannon,“Communication theory of secrecy systems,” Bell System Technical Journal, vol.28, pp.656–715,Oct.1949.

**[21]** Daniel B. da Costa,Nuwan S. Ferdinand, Ugo S. Dias, Rafael T. de Sousa Jr.,and Matti Latva-aho, “Secrecy Outage Performance of MIMO Wiretap Channels with Multiple Jamming Signals,” in journal of communications and information systems,vol, 31. NO, 1, 2016.

**[22]** A.Mukherjee andA.Swindlehurst,“Robust beam forming for security in MIMO wiretap channels with imperfect CSI,” IEEE Trans.Signal Process., vol.59, no.1, pp.351–361, 2011, doi:10.1109/TSP. 2010.2078810.

**[23]** Andreas F., *Wireless Communications*, Second Edition, A John Wiley and Sons, Ltd., Publication, 2010.

**[24]** Caijun Z., Tharm R. and Kai-Kit W., “Outage Analysis of Decode-and-Forward Cognitive Dual-Hop Systems with the Interference Constraint in Nakagami-*m*Fading Channels,” *IEEE Transactions on Vehicular Technology*, vol. 60, no. 6, pp.2875-2879, 2011.

**[25]** Marco C. and Mounir G., “Spectrum Sensing and Throughput Trade-off in Cognitive radio under Outage constraint over Nakagami Fading,” *IEEE Commun. Lett.*, vol. 15, no. 10, pp. 1110-1113, 2011.

**[26]** Wang L., Elkashlan M., Huang J., Schober R. and Mallik K., “Secure Transmission with Antenna Selection in MIMO Nakagami-m Fading Channels,” *IEEE Communication on Wireless Communications*, vol.pp, issue. 99, pp. 1-14, 2014.