Vietnamese – German University
Department of Electrical Engineering & Information Technology

Frankfurt University of Applied Science
Faculty 2: Computer Science and Engineering

Physical-Layer Security for Cooperative Networks with Jamming and Beamforming

BY

PHAM NHAT NAM
Matriculation number: 1105331

First supervisor: Dr. Chan Dai Truyen Thai
Second supervisor: M.Sc. Nhu Quang Tran

BACHELOR THESIS

Submitted in partial fulfillment of the requirements
for the degree of Bachelor Engineering in study program
Electrical Engineering& Information Technology,
Vietnamese – German University, 2018

Binh Duong, Vietnam, July 2018

Physical-Layer Security for Cooperative Networks with Jamming and Beamforming

Approved by

____

Dr. Chan Dai Truyen Thai, First Supervisor

____

M.Sc. Nhu Quang Tran, Second Supervisor

Thesis Committee

Disclaimer

I declare that this thesis is the outcome of my own work. The used methods and schemes are well cited. I also declare that all opinions, results, conclusions and recommendations are my own and do not violate the policies of the Department of Electrical Engineering and Information Technology of the Vietnamese-German University and the Faculty 2: Computer Science and Engineering of the Frankfurt University of Applied Science.

Pham Nhat Nam

Abstract

Security for network is critical and essential aspect in modern life. Physical-layer security is a newly developed area of network security in which security methods and schemes are used to guarantee that the eavesdroppers cannot get any secured exchanged information without encryption. Therefore, the data processing time is reduced and the data transmission rate is increased. However, the techniques used in physical-layer security have a constraint in which the source-destination channel has to be better than the source-eavesdropper channel. In practice, issues such as obstacles or large distance between the source and the destination affect the quality of the source-destination channel. Therefore, the utilizations of relay communication combining with a security technique helps the source-destination channel get over these troubles and improve the capacity.

To the best of my knowledge, a single method may not guarantee a strictly secured communication, especially when the malicious agents gain higher and higher capability these days. In order to determine which combination of methods gives the best performance, studying and simulating the relationship between secrecy rate and other variables such as transmit power levels, eavesdropper's position, etc. are done several times and the average results are recorded. Nevertheless, some simulation results are recorded with the best result, not average one, because the results are not stable for some unknown causes. Among all the techniques analyzed in this thesis, beamforming is the best supportive technique for jamming signal since it gives the highest result in all the simulations. Optimal Relay Selection (ORS), Energy Harvesting (EH), etc. are the techniques that will be analyzed along with some beamforming technique applications.

Acknowledgements

I would like to express my thanks to all my friends, teachers and teacher assistant who support me to finish my bachelor thesis.

First of all, the most important person I want to express my gratitude is Dr. Thai Truyen Dai Chan for his guide and advice in my thesis process. I have learned a lot of knowledge not only in telecommunications but also in mathematics and other useful skills. Although he were busy all the time, he still had time to reply my email thoughtfully and carefully.

Second, I am also grateful to my friends: Ngo Le Quoc Bao, Nguyen Phuc Hai; who have helped me to analyze paper and to solve problems that I was stuck. Anytime I had trouble, I always discussed with my friends before contacting with Dr. Chan which help me save a lot of time.

Third, I want to say thank to lab engineer/ teacher assistant M.Sc. Tran Quang Nhu, who helped me write the thesis report and found errors in my work; and Dr. Pham Thanh Duong, my mathematical teacher in second year, who helped me with my mathematical problem, especially in matrix.

Finally, I appreciate my family and all people who encourage and run errands for me a lot when I has difficult time, especially Luong Nguyen The Minh and Nguyen Thien Tuan for helping me contact and apply documents for VGU since I have problem with my leg and could not go to the university.

Table of Contents

List of Figures

List of Abbreviations

AF: Amplify-and-Forward.

AWGN: Addiction White Gaussian Noise.

CJ: Cooperative Jamming.

DAJB: Destination Assisted Jamming and Beamforming.

DF: Decode-and-Forward.

EH: Energy Harvesting.

LP: Linear Programming.

MER: Main-to-Eavesdropper Ratio.

ORS: Optimal Relay Section.

SNR: Signal-to-Noise Ratio.

SOCP: Second-Order Convex cone Programming.

Chapter 1: Overview

Chapter 1 contains overall information about my thesis such as overview, problem declaration, the way I carried the project and some common notations that I used**.**

1.1 Introduction

In any period of time, information is very important which can provide people the capabilities to decide and change the situations in the way they want. In order to exchange information, many communication techniques appear which required appropriate security techniques to protect the confidential information. Therefore, to secure the essential information, we required security to be good, reliable and has to improve in parallel with the development of the technology, especially in network security. Nevertheless, network security is a broad field of research which includes many approaches to secure the transmitted information such as encryption, firewall or in the physical ways. In all of them, physical layer security is one of the latest technologies which has been in research recently and validated to have many advantages compared to the traditional network security techniques.

Because physical layer security is new and has a wide range for new developments, after finishing the study about how to secure a simple network communication with only jamming signal, I decided to continue my study with an upgrade version of previous project which contains more applications of jamming signal. Combining jamming signal with another technique is the choice I made to have improvement in channel capacity because it is less complicated than researching a new protection technique. After all the studies, beamforming, which is the technique with the best performance, is the main target technique in combining with jamming signal. However, in order to have a fair perspective, there are other auxiliary techniques for jamming which will be analyzed along with the beamforming.

My work in this thesis process is mainly analyzing, studying papers to understand the proposed techniques. To provide readers not only a clear view of my study but also the comparison in protection effect between differences proposed techniques, I simulated some papers on MATLAB (version R2015a) and explained the reason of changes in graph. All the contents in my thesis are deliberately selected to achieve the main objective so that any irrelevant information is fully filtered. The model and setup of some cases are also simplified and modified for the contents to be unified and easy to follow.

My thesis report is for academic and educational purposes and it contains a wide range of mathematical knowledge, especially in matrix, complex number, probability, and variety of knowledge about telecommunication and network. Consequently, only readers with good background in advanced math, telecommunication system and having interested in the network security field are recommended for reading. In addition, Internet or the cited documents are required in order to search for unclear or additive information.

1.2 Problem Statement

The most challenging problem in writing this thesis is that this topic requires a researcher-level knowledge of mathematics. In this thesis report, there are three main noteworthy mathematic issues: linear algebra, probability and matrices calculation. All necessary knowledge in these three issues for realistic applications is not always fully covered by the mathematical classes for bachelor degree so that searching for theories or formulas required a huge amount of time.

The second problem I has during the process is working with MATLAB. The most annoying problem related to MATLAB is using the CVX tool to solve convex optimization, second-order convex cone programming (SOCP), linear programming (LP), etc. which required complicated syntaxes and rules which make me fail to apply it after months of trying. Common errors with CVX tool appearing in simulation process are: “Invalid constraint” and “Invalid quadratic form”. “Invalid constraint” happens when two convex functions interact with each other. To solve this error, simplifying or reformulating the formula to other form is compulsory which is out of my ability. “Invalid quadratic form” error occurs when the input form of variables or functions do not match the requirements of the program. For example, $w^{\dagger}Qw$ cannot be entered normally but must be in specified form as quad_form(w,Q). The other minor problems relate to syntaxes or function usage which can be rapidly solved by searching information on MATLAB official website.

The third problem is a very common issue that everyone who used to study paper have to meet: the notations are not consistent among the papers. Therefore, comparing essential articles together with many sub-articles is mandatory to ensure the accuracy of notations' usage. For example, $[\bullet]^{\dagger}$ denotes for conjugate transpose which has the same meaning as $[\bullet]^{H}$ denotes for Hermitian transpose; or $\log(\bullet)$ is normally $\log_{10}(\bullet)$ in mathematic because decimal is more commonly used but in telecommunication network field, it is $\log_{2}(\bullet)$ since binary is more popular.

1.3 Techniques Approach

This section presents explanation of some remarkable definitions and the overview of jamming and beamforming techniques appearing in the report to make the readers easier to follow.

First of all, jamming and beamforming are two main techniques in the report that need to be emphasized:

- Jamming technique is the technique that generates an artificial signal intentionally to interfere to a communication channel such that the eavesdroppers cannot decode their intended signals.

- Beamforming is a signal processing technique to adjust the transmitting direction such that receivers in certain directions get the largest gains and/or receivers in other certain directions get the smallest gains. By combining elements in an antenna array, we can control the signal to converge in a desired direction which helps us to improve the quality of the transmission channel and deteriorate that of the eavesdropper channel.

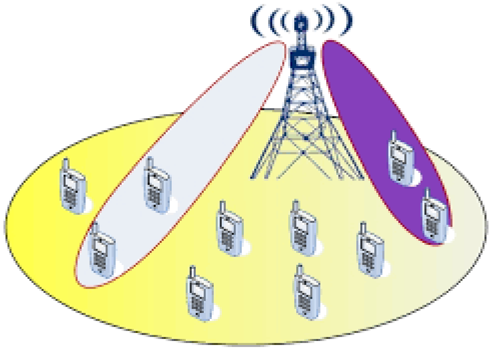

Figure 1.1: Beamforming.

Second, a system cannot work if its elements are disjointed and a scheme is the solution for that problem. Normally, the system in telecommunication has three main elements: the source, the relays, and the destination; and a scheme (or an operation mode, a relaying mode) is vital to link all of them together. [1] introduces to us some schemes which are commonly used:

- Direct Transmission (DT): the source transmits the signal to the destination directly without intermediaries (relays).
- Amplify-and-Forward (AF): the source encodes the signal and transmits it to the relays. Then the relays amplify the signal and continue to transmit it to the destination.
- Decode-and-Forward (DF): the source encodes the signal and transmits it to the relays. Then the relays receive the encoded signal and decode it before transmitting to the destination.

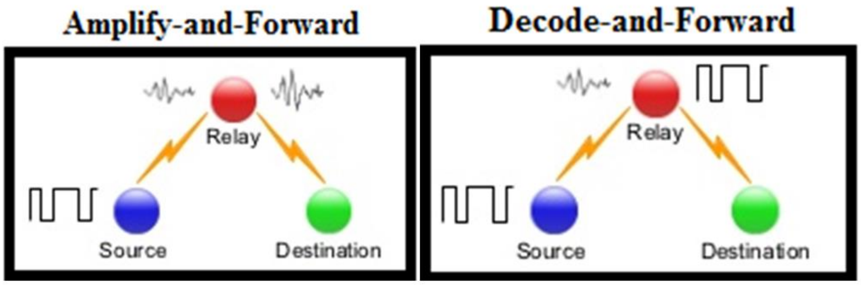

Figure 1.2: Description of AF and DF

In the next chapters, my demonstration is divided into 2 main parts:

- Chapter 2 focuses on the jamming techniques with the following schemes:
  - Review the cooperative jamming scheme in [1].
  - Relay selection technique mixes with cooperative jamming scheme in [2].
  - Energy harvesting technique combines with cooperative jamming scheme in [3].
  - In this section, the optimal relay selection technique in [4] is analyzed and simulated in addition with the result from author in [1] and my simulation's result in energy harvesting combined cooperative jamming case to choose the main scheme to work with in chapter 3 between AF or DF.
- Chapter 3 concentrates on the combination of jamming and beamforming techniques:
  - Beamforming, jamming and power allocation combination in order to protect joint cooperative network system [5].
  - The beamforming, jamming and multiple relays, jammers selection to increase physical layer secrecy in two-phase cooperative network [6].
  - Paper [10] presents "Beamforming and Jamming supporting form destination" which is a good example of combination of jamming and beamforming. However, this section doesn't have simulation because it requires CVX tool.

1.4 Common Notations

$(.)^*$: conjugate.

$(.)^T$: transpose.

$(.)^\dagger$: conjugate transpose or Hermitian transpose.

Lower case letter (x, t, y, etc.): normal variable, number.

Bold lower case letters (**w**, **h**, etc.**)**: a column vector (nx1). (can be a row vector in some cases)

Bold uppercase letters (**R**, etc.): a matrix.

$\|\boldsymbol{h}\|$**:** 2-norm of vector h.

$|h|$: the magnitude of complex number h.

$\mathbf{I}_i$: identity matrix $(i \times i)$.

$diag(\bullet)$: diagonal matrix.

$[\bullet]_{(i)}$: i-th element of a vector.

$[\bullet]^{(i)}$: i-th row of a matrix.

$[\bullet]_{(m,n)}$: the (m, n)-th component of a matrix.

$\boldsymbol{i}^o$: optimal variable i .

Chapter 2: Jamming.

In chapter 2, the order of three main schemes follows the sequence as: cooperative jamming (CJ), relays selection and energy harvesting. The optimal relay selection (ORS) is a sub scheme analyzed to choose the main relaying mode between AF and DF for chapter 3.

2.1 Cooperative Jamming.

Chapter 2.1 presents the analysis for paper [1] which referred to cooperative jamming technique. There are three main part in this chapter: System model, analytical result and simulation. The other chapters have the same format as this chapter also.

2.1.1 System Model.

The cooperative jamming scheme analyzed in this project is simple: while the source transmits symbol x (encoded signal $\sqrt{P_S}x$) direct to the destination, the relays transmit a separated weighted jamming signal z to disturb the eavesdropper.

To simplify the analysis and simulation, one-dimensional model is used with 1 source, 3 relays, 1 eavesdropper and 1 destination point as in the Figure 2.1. The source placed at (0, 0) will transmit symbol x to the destination at (50, 0) through 3 relays installed half way at (25, 0) and the eavesdropper will move from (30, 0) to (90, 0). The number of relays can varies without changing the test so much (a small fix in formula is required).

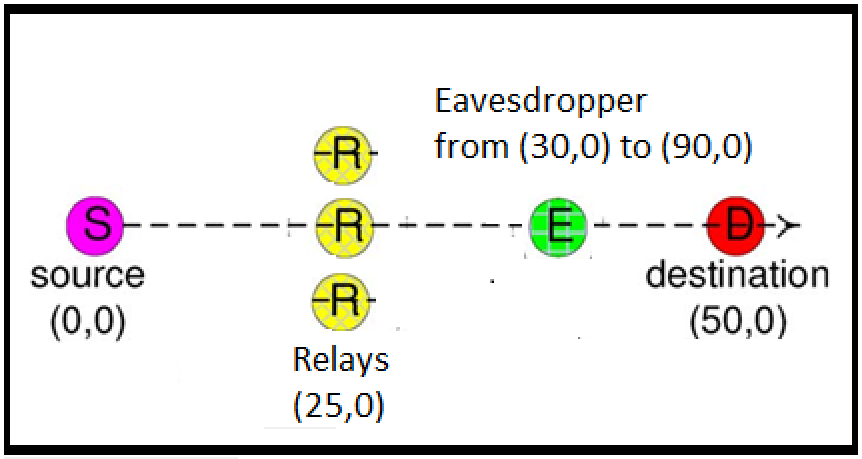

Figure 2.1: System model of cooperative jamming.

The number eavesdropper in this model can also be changed with some small fixes in formula and MATLAB program which can provide more kind of tests to provide a transparent and effective way to increase secrecy rate. However, I consider to use it for another project because I will analyze only the case of one eavesdropper appears in every part of this thesis.

2.1.2 Analytical Results.

In this report, we have some following notation: (.)*: conjugate, $(.)^T$: transpose, $(.)^\dagger$: conjugate transpose, bold lower case letters (**w**, **h**, etc.**)** denote column vector (nx1), bold uppercase letters (**R**, etc.) denote matrices, ||***h***|| denotes 2-norm of vector h, |h| denotes the magnitude of complex number h.

Received signal at destination is given by:

$$y_d = \sqrt{P_S} h_{SD}^* x + \mathbf{h}_{RD}^\dagger \mathbf{w} z + n_d . \tag{1}$$

Received signals at eavesdropper is given by:

$$y_e = \sqrt{P_S} h_{SE}^* x + \mathbf{h}_{RE}^\dagger \mathbf{w} z + n_e . \tag{2}$$

Vector **w** (3x1) is weight vector of all relays; n_d ,n_e are complex Gaussian white noise at destination and eavesdropper, respectively; h_{SD}^*, h_{SE}^* are source-destination and source-eavesdropper channels respectively; $\mathbf{h}_{\mathrm{RD}}^{*\mathrm{T}}$, $\mathbf{h}_{\mathrm{RE}}^{*\mathrm{T}}$ are channel vectors (1x3) between 3 relays and destination and eavesdropper, respectively.

In order to evaluate the secrecy of the communication channel, we use the capacity of channel definition. It is the maximum rate of communication which the transmission is possible with arbitrarily small errors. In this project, we will use the term rate of transmission in replace.

As shown in [7], the rate of communication is defined:

$$R = \log_2\left(1+\mathrm{SNR}\right) \text{ (bits/s/Hz)}, \tag{3}$$

where SNR = $\frac{\mathrm{P}}{\mathrm{N}}$ with P is power of transmitting signal and N is noise power.

From (1) and (2), we have the interference power which is the power of jamming signal in relay-destination channel and relays-eavesdropper channel, respectively:

$$n_{\mathrm{RD}} = \left(\mathbf{h}_{\mathrm{RD}}^{\dagger}\mathbf{w}\right)^{\dagger}\mathbf{h}_{\mathrm{RD}}^{\dagger}\mathbf{w} = \mathbf{w}^{\dagger}\left(\mathbf{h}_{\mathrm{RD}}^{\dagger}\right)^{\dagger}\mathbf{h}_{\mathrm{RD}}^{\dagger}\mathbf{w} = \mathbf{w}^{\dagger}\mathbf{h}_{\mathrm{RD}}\mathbf{h}_{\mathrm{RD}}^{\dagger}\mathbf{w} = \mathbf{w}^{\dagger}\mathbf{R}_{\mathrm{RD}}\mathbf{w} \;, \tag{4}$$

$$n_{\mathrm{RE}} = \left(\mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{w}\right)^{\dagger}\mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{w} = \mathbf{w}^{\dagger}\left(\mathbf{h}_{\mathrm{RE}}^{\dagger}\right)^{\dagger}\mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{w} = \mathbf{w}^{\dagger}\mathbf{h}_{\mathrm{RE}}\mathbf{h}_{\mathrm{RE}}^{\dagger}\mathbf{w} = \mathbf{w}^{\dagger}\mathbf{R}_{\mathrm{RE}}\mathbf{w} \;, \tag{5}$$

with $\mathbf{R}_{RE} = \mathbf{h}_{RE}\mathbf{h}_{RE}^{\dagger}$ and $\mathbf{R}_{RD} = \mathbf{h}_{RD}\mathbf{h}_{RD}^{\dagger}$.

Power of useful signal received at the destination and eavesdropper from (1) and (2) are: $\left(\sqrt{\mathrm{P_S}}\mathrm{h}_{\mathrm{SD}}^{*}\right)^2$ and $\left(\sqrt{\mathrm{P_S}}\mathrm{h}_{\mathrm{SE}}^{*}\right)^2$, respectively. $\left(\sqrt{\mathrm{P_S}}\mathrm{h}^{*}\right)^2$ (6)

From (1), (3), (4), (6), the secrecy rate at destination is given by:

$$R_d = log_2\left(1+\frac{P_s\left|h_{SD}\right|^2}{n_{RD}+\sigma^2}\right) \text{ (bits/s/Hz)}. \tag{7}$$

From (2), (3), (5), (6), the secrecy rate at eavesdropper is given by:

$$R_e = log_2\left(1+\frac{P_s\left|h_{SE}\right|^2}{n_{RE}+\sigma^2}\right) . \tag{8}$$

From (7), (8) the secrecy rate of the whole connection is given by:

$$R_S(\mathbf{w}, \mathrm{P}_S) = \max\{R_d - R_e, 0\} = log_2\left(1 + \frac{P_S\left\|h_{SD}\right\|^2}{n_{RD} + \sigma^2}\right) - log_2\left(1 + \frac{P_S\left\|h_{SE}\right\|^2}{n_{RE} + \sigma^2}\right) \text{ ,} \qquad (9)$$

where $\boldsymbol{w} = \mu\left\|\boldsymbol{h}_{RD}\right\|^2 \boldsymbol{h}_{RE} - \mu\boldsymbol{h}_{RD}^{\dagger}\boldsymbol{h}_{RE}\boldsymbol{h}_{RD}$, (10)

and the scalar coefficient $\mu = \sqrt{\frac{P_0 - P_S}{\left\|\boldsymbol{h}_{RD}\right\|^4\left\|\boldsymbol{h}_{RE}\right\|^2 - \left\|\boldsymbol{h}_{RD}\right\|^2\left|\boldsymbol{h}_{RD}^{\dagger}\boldsymbol{h}_{RE}\right|^2}}$. (11)

However, when testing μ in (11) as in [7], I assume there is mistake in the formula because the trend of the graph in simulation result is opposite to [1] so I decided to use the formula of secrecy rate maximization from [1] to calculate μ:

$$arg\max_{\boldsymbol{w}}\left|\mathbf{w}^{\dagger}\mathbf{h}_{\mathrm{RE}}\right|^2,$$

$$\text{s.t.} \quad \begin{cases} \mathbf{w}^{\dagger}\mathbf{h}_{RD} = 0. \\ \mathbf{w}^{\dagger}\mathbf{w} = P_0 - P_s. \end{cases} \qquad (12)$$

From (10) and (12), we have:

$$\mathbf{w}^{\dagger}\mathbf{w} = \left\|\mathbf{w}\right\|^2 = P_0 - P_S = \mu^2\left\|\left\|\mathbf{h}_{RD}\right\|^2\mathbf{h}_{RE} - \mathbf{h}_{RD}^{\dagger}\mathbf{h}_{RE}\mathbf{h}_{RD}\right\|^2 \text{ .} \qquad (13)$$

From (13), we can account scalar coefficient μ as:

$$\mu = \frac{\sqrt{P_0 - P_S}}{\left\|\left\|\mathbf{h}_{RD}\right\|^2\mathbf{h}_{RE} - \mathbf{h}_{RD}^{\dagger}\mathbf{h}_{RE}\mathbf{h}_{RD}\right\|} \text{ .} \qquad (14)$$

2.1.3 Numerical and Simulation Results.

2.1.3.1 Setup for simulation.

The channels between the relays and the eavesdropper are given in form of:

$$\mathbf{h}_{RE} = \left(d_{RE}\right)^{\frac{-c}{2}} \mathbf{e}, \tag{15}$$

where $\mathbf{e} = \begin{pmatrix} a_1 + b_1 i \\ a_2 + b_2 i \\ a_3 + b_3 i \end{pmatrix}$, a_n, b_n are normally distributed random numbers, number of complex numbers in $\mathbf{e}$ equals to number of relays in use; c=3.5 is the path loss exponent, d_{RE} is the distance between relays and eavesdropper. Other channels are also defined in a similar function of the distance between the corresponding transmitter and receiver.

I set noise power $\sigma^2 = -60$ dBm, source power $P_S = -1$, total transmit power constraint $P_0 =$ 0 dBm.

In this simulation, the program calculates the secrecy rate at each position from 30 to 90 meters, 1 meter each step, for 100,000 times and takes the average results. 100,000 loops is the efficient number for the simulation as I test it from 1 to 1,000,000 and find out that if it is lower than 100,000, the graph varies wildly (the smaller the loop number, the more the graph varies) and if it is higher than 100,000, the time required to process the simulation is too long but the results does not change clearly. Additionally, I observe there are always approximate 10% of results has NaN value and some unpredictable results which are too high or too low compared to the others at same distance which make the simulation error due to the uncontrollable random complex numbers $\mathbf{r}$. Then, I decide to discard these NaN values. Figure 2.2 is the final result of the simulation.

2.1.3.2 Simulation Result.

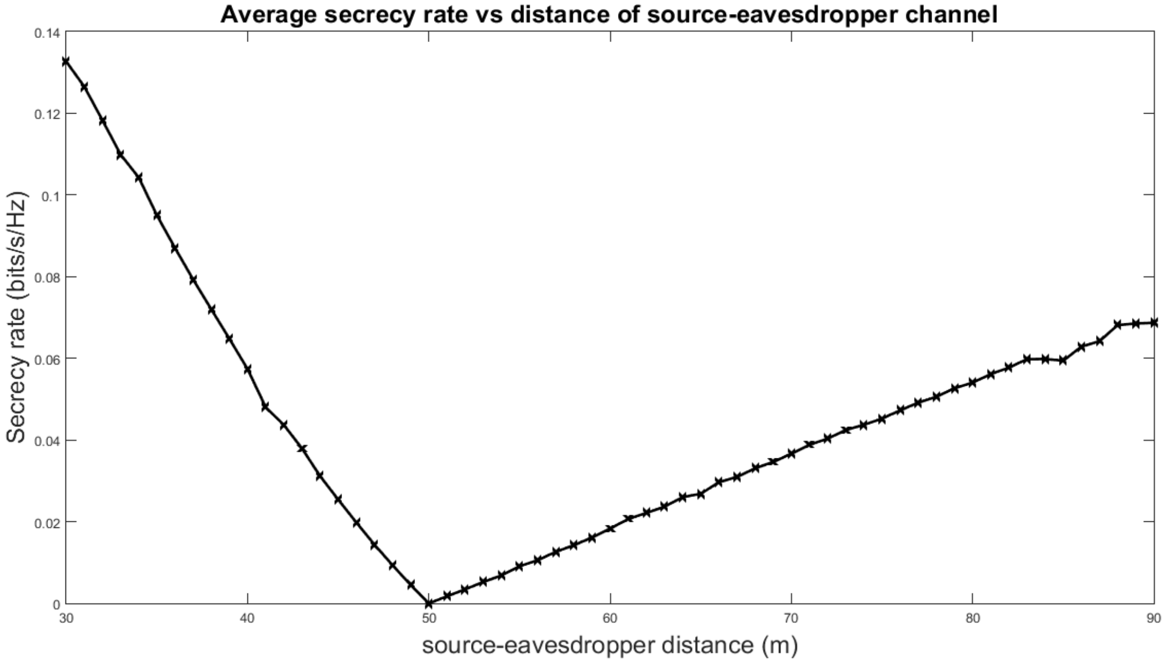

Figure 2.2: Average secrecy rate versus distance of source-eavesdropper channel (CJ).

As shown on the graph, the secrecy rate has two opposite trends in 2 parts: decreasing from 30 to 50 meters and increasing from 50 to 90 meters. The trend of the graph is predicted as in [1].

In the first part (30, 50), the eavesdropper shifts not only far away to the source but also near to the destination. Therefore, the source has to increase power to transmit jamming signal and decrease power for the message signal. It makes the source-destination channel capacity lower and source-eavesdropper channel capacity higher so that the secrecy rate decreases.

In the second part (50, 90), when the eavesdropper goes out of the source-destination distance (from 51 to 90 meters), the source can allocate more power to the message signal and lower power to the jamming signal. Then, the secrecy rate increases because the source-destination channel become better than of the source-eavesdropper channel.

Although the secrecy rate goes up in the second part, the going up speed is not as fast as the first part (same in [1]). This phenomena can be explained that although the eavesdropper goes outside the source-destination range, the source still has to allocate power to interfere it and the further the eavesdropper, the higher the shared power.

2.1.3.3 Conclusion.

The numerical result of the simulation is not acceptable as long as the secrecy rate is significantly low (the maximum R_s in my simulation is about 0.13 when the lowest R_s in [1] is approximate 0.6). The cause of this error can be the fault when typing and checking the paper makes the formulas wrong since I found out a small clearly error in formula 42 in [1]. I also suspected formula (45) in paper [1] as the result when using it makes the trend of graph rise up the same as graph of log function. As long as the paper is not fixed and confirmed again, I can assume there are more typo errors that leads to the huge difference between two results.

2.2 Relay selection and jamming.

Chapter 2.2 presents the combination technique of jamming and relay selecting. The main objective in this chapter is to find the best relay selection policy among three referred cases based on secrecy rate.

2.2.1 System Model.

This model will work in DF mode, in a slow, flat, block Rayleigh fading environment and be splitted into two phases: the source transfers signal to 4 (as in [2]) or more intermediate relays in first phase; then, 2 relays will be chosen due to the formulas: one acts as a relay and transfer the signal to destination, the other will act as a jammer and broadcast interference signal to protect the transmission. In addition, because this model is in DF scheme, I also assume all the relays can successfully decode the encoded source signal to make the theory simple. Moreover, the main objective of this case focus on criteria to choose relay and jammer for cooperative system so that I should assume that the direct link source-destination and source-eavesdropper is not available so that all the transfers have to go through the relays to express clearly the impact of chosen relay/jammer to the secrecy rate. This assumption bases on the following conditions:

- The direct link source-destination and source-eavesdropper are both deep fading because between source, destination and eavesdropper, there are obstacles that block the path and interrupt the signal transfer. Otherwise, the relays can work since they are placed at the corner of obstacles and they have sight of line to both destination and the source.
- The cooperative protocol works as two different orthogonal channels (in frequencies or time slots, etc.) and the eavesdropper can only overhear cooperative channel (chosen relay-destination) but not broadcast channel (source-relays).

There is another very important assumption [2] mentioned: the destination node cannot mitigate jamming signal to prevent eavesdropper to track jamming signal and also know how to mitigate the interference as the destination.

The setup for simulation in this case I use the same as in cooperative jamming case and let the number of relays varies (the paper fixes at 4) since it does not affect the result: one-dimensional model is used with 1 source, N relays, 1 eavesdropper and 1 destination point. The source placed at (0, 0) will transmit symbol x to N relays installed randomly from (1, 0) to (49, 0), two relays will be chose as jammer and broadcaster to continue transferring the signal to the destination at (50, 0), the eavesdropper will stay in half way (25, 0).

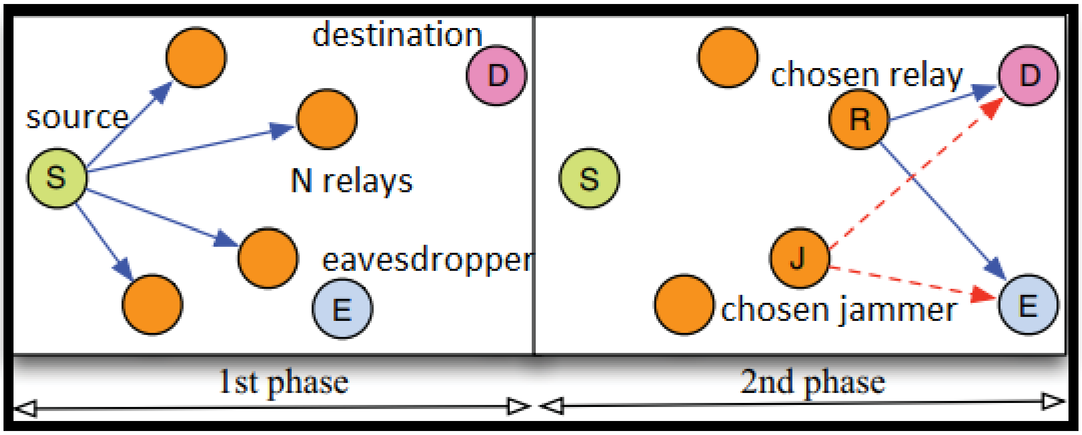

Figure 2.3: Model of relay selection and jamming.

2.2.2 Analytical Results.

As [2] shows that the secrecy rate at the destination node and the eavesdropper node respectively:

$$R_d = \frac{1}{2}\log_2\left(1+\frac{P*|h_{RD}|^2}{1+P*|h_{JD}|^2}\right), \tag{16}$$

$$R_e = \frac{1}{2}\log_2\left(1+\frac{P*|h_{RE}|^2}{1+P*|h_{JE}|^2}\right), \tag{17}$$

where P is transmitted/jammed power at the chosen relay/jammer, $h_{RD}, h_{JD}, h_{RE}, h_{JE}$ are channel coefficient for the relay-destination, jammer-destination, relay-eavesdropper, jammer-eavesdropper respectively.

Therefore, if assume that all the relays decode the source signal successfully, the secrecy rate of the whole connection is:

$$R_s = R_d - R_e = \frac{1}{2}\log_2\left(1+\frac{P*\left|h_{RD}\right|^2}{1+P*\left|h_{JD}\right|^2}\right)-\frac{1}{2}\log_2\left(1+\frac{P*\left|h_{RE}\right|^2}{1+P*\left|h_{JE}\right|^2}\right). \tag{18}$$

In order to choose the appropriate relay and jammer to maximize the secrecy rate of different techniques. Below I will analyze the relay and jammer selection techniques for jamming in part III of [2].

a) Optimal selection with jamming (OSJ)

The selection policy in this technique is quite straight forward: choose the best relay and jammer in the relays set in order to get the secrecy rate maximum:

$$\left(R,J\right) = \underset{R\neq J}{\operatorname{argmax}}\left\{R_s\left(R,J\right)\right\} = \underset{R\neq J}{\operatorname{argmax}}\left\{\frac{1+\dfrac{P*\left|h_{RD}\right|^2}{1+P*\left|h_{JD}\right|^2}}{1+\dfrac{P*\left|h_{RE}\right|^2}{1+P*\left|h_{JE}\right|^2}}\right\}. \tag{19}$$

However, this policy requires many comparisons which can make the calculated time increase significantly if the quantity of relays increase so high. For that reason, the selection policy is proposed with a simpler approximation form as below:

$$\left(R,J\right) \simeq \underset{R\neq J}{\operatorname{argmax}}\left\{R_s\left(R,J\right)\right\} = \underset{R\neq J}{\operatorname{argmax}}\left\{\frac{\dfrac{P*\left|h_{RD}\right|^2}{P*\left|h_{JD}\right|^2}}{\dfrac{P*\left|h_{RE}\right|^2}{P*\left|h_{JE}\right|^2}}\right\} = \underset{R\neq J}{\operatorname{argmax}}\left\{\frac{P*\left|h_{RD}\right|^2}{\dfrac{P*\left|h_{RE}\right|^2*P*\left|h_{JD}\right|^2}{P*\left|h_{JE}\right|^2}}\right\}$$

$$. \tag{20}$$

We can easily see that this simple policy form can be expressed as:

$$\begin{cases} R = \arg\max \left\{ \dfrac{P*|h_{RD}|^2}{P*|h_{RE}|^2} \right\}. \\ J = \arg\min\limits_{J \neq R} \left\{ \dfrac{P*|h_{JD}|^2}{P*|h_{JE}|^2} \right\}. \end{cases} \tag{21}$$

b) Optimal switching (OS)

As in system model mentioned, the destination cannot neutralize jamming signal so that continuously broadcast jamming signal is not always positive for the system. For some operational scenarios like jammer is close to destination, using interference steadily give negative effect for the system and decrease secrecy rate. To overcome this disadvantage, the paper propose the intelligent switching for optimal selection with jamming (and also without jamming). The intelligent switching theory can be expressed as inequality between secrecy rate with and without jamming signal:

$$R_S(R,J) > R_S(R) \ . \tag{22}$$

Using simplified form in OSJ case, we have:

$$\frac{1}{2}\log_2\left(\frac{P*|h_{RD}|^2 * P*|h_{JE}|^2}{P*|h_{RE}|^2 * P*|h_{JD}|^2} \right) > \frac{1}{2}\log_2\left(\frac{P*|h_{RD}|^2}{P*|h_{RE}|^2} \right)$$

$$\Rightarrow P*|h_{JE}|^2 > P*|h_{JD}|^2$$

$$\Rightarrow \frac{|h_{JD}|^2}{|h_{JE}|^2} < 1. \tag{23}$$

The above condition guarantees jamming signal interfere the destination less than the eavesdropper so that the disadvantage we mentioned cannot happen.

c) Optimal Selection with “controlled” Jamming (OSCJ)

For this OSCJ case, the paper assumes that jamming signal can be decoded at destination but the eavesdropper cannot do that. Follow that assumption, the secrecy rate formula at the beginning can be changed as:

$$R_s = R_d - R_e = \frac{1}{2}\log_2\left(1+P*\left|h_{RD}\right|^2\right) - \frac{1}{2}\log_2\left(1+\frac{P*\left|h_{RE}\right|^2}{1+P*\left|h_{JE}\right|^2}\right). \tag{24}$$

The choice conditions for jammer and relay is expressed as:

$$\begin{cases} R = \arg\max\left\{\dfrac{P*\left|h_{RD}\right|^2}{P*\left|h_{RE}\right|^2}\right\}. \\ J = \arg\max\limits_{J\neq R}\left\{P*\left|h_{JE}\right|^2\right\}. \end{cases} \tag{25}$$

2.2.3 Numerical and Simulation Results.

2.2.3.1 Setup for simulation.

The channel coefficients are set the same as in cooperative jamming scene:

$$h = \left(d\right)^{\frac{-c}{2}} e, \tag{26}$$

where d is the distance between two nodes, e is a uniformly distributed random complex number (a+bi), c is the path loss exponent

The objective of this simulation is to show the relation between secrecy rate and the transmitted power P. I set transmitted power runs from 0 to 50 dBm, c=3.5.

There are two simulations that I do in this part: average secrecy rate versus transmitted power, and average secrecy rate versus eavesdropper position. The first one follows the simulation in the paper and the second one I do on my own to have a broader perspective on the studied issue.

The simulation has the position of relays random so the result is very unstable so that I will test the simulation by hand and then, choose the result that I satisfy and fix the set of relays. After fixing the appropriate set of relays, I run the test 10,000 times and take the average secrecy rate.

2.2.3.2 Simulation result.

The annotation can be seen on the image: red line, blue line and orange line show secrecy rate of optimal switching, optimal selection with jamming, and optimal selection with “controlled” jamming respectively. After many tries, I find out the acceptable relay set (3; 30; 35; 37) that make the secrecy rate high enough, the chosen jammer and chosen relay depend on the selection policy.

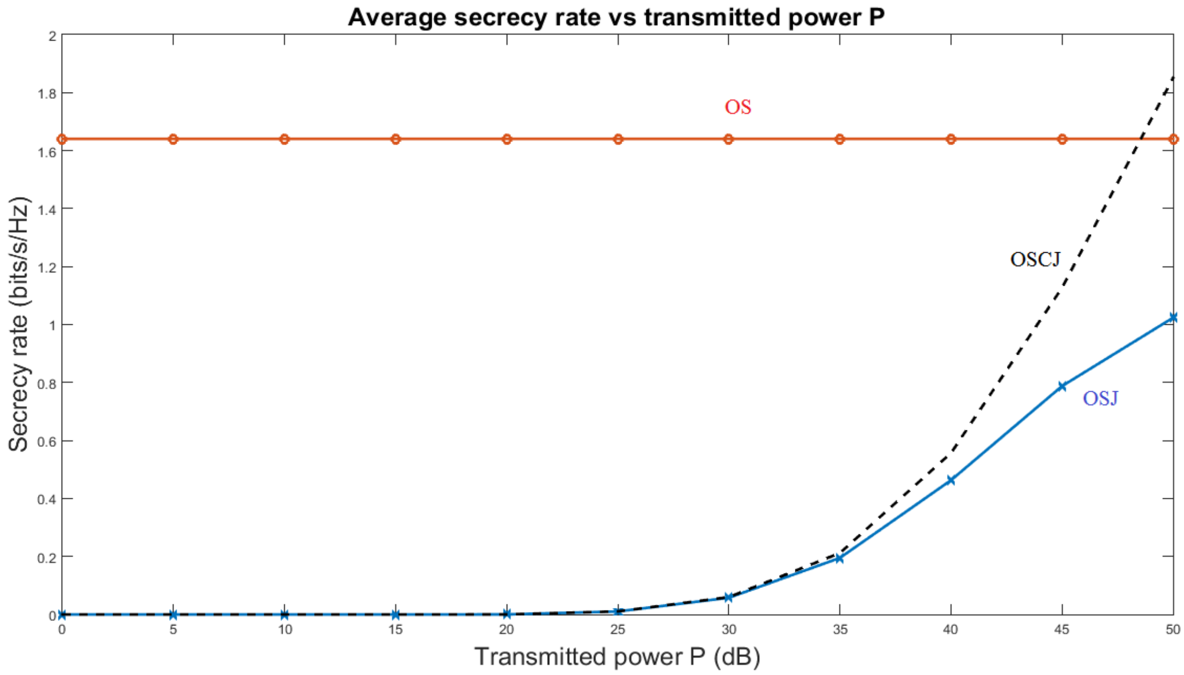

Figure 2.4: Average secrecy rate versus transmitted power P (relay select).

In the first simulation, I test the relationship between average secrecy rate R_S and the transmitted power P. Chosen jammer in OS case is (3; 0), when in OSCJ and OSJ cases are the same (30; 0). The chosen relays of all policy are (37; 0). As we can observed, the secrecy rates increase when the transmitted power increase (not in OS case when the simplified form make the formula undependable of transmitted power P), especially after P=25 dBm (before this milestone, the increasing still happen but the gain is too low to show clearly). The OSCJ and OSJ have nearly same results before P=35 dBm but after that, the secrecy rate of OSCJ increase dramatically compare to the increasing of the OSJ secrecy rate.

The second simulation I make to test the relationship between average secrecy rate R_S and the eavesdropper position. Chosen jammers of all policy in this test are (37; 0) when the chosen relays are different in each policy: (30; 0) for OSJ, (33; 0) for OS, and (35; 0) for OSCJ. To understand the result, we must remember the assumption that the eavesdropper cannot receive signal directly from source in phase 1 but have to wait until phase 2 when the chosen relay broadcast the decoded signal to destination. Because the chosen relay in all policy gather in middle from (30; 0) to (35; 0), the secrecy rates when eavesdropper near the source (from (0; 0) to (15; 0)) are high and decrease when the eavesdropper goes forward to the chosen relay. In the range around chosen relay, the secrecy rates of all policy are stable before dropping heavily when the eavesdropper go near to chosen jammer and destination.

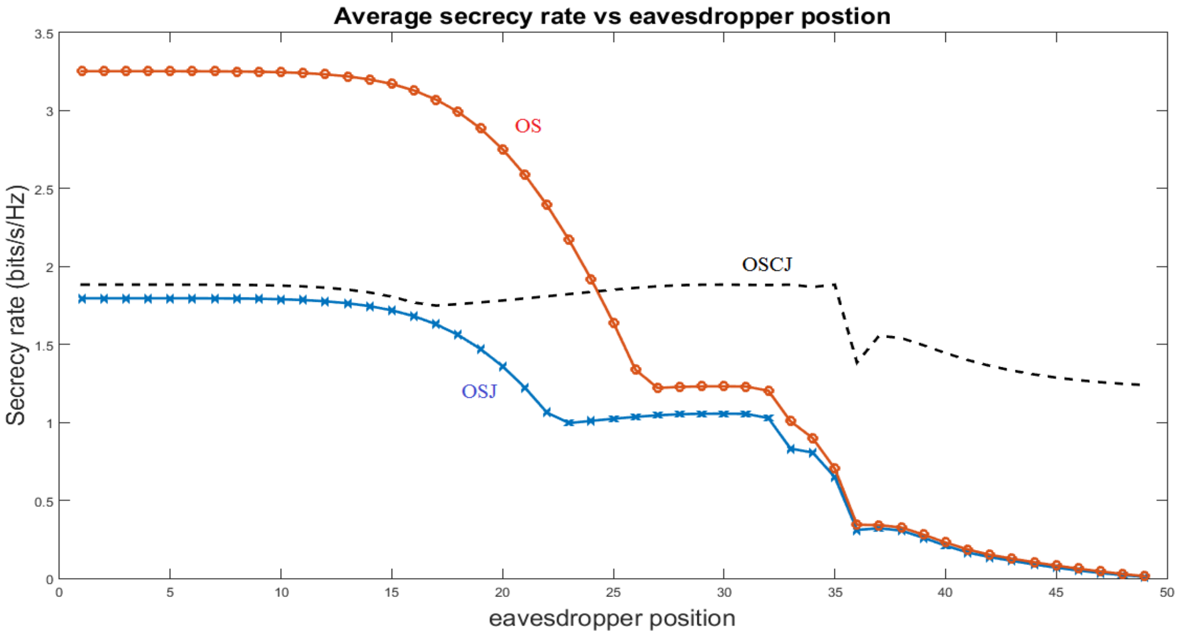

Figure 2.5: Average secrecy rate versus eavesdropper position (relay select).

2.2.3.3 Conclusion.

Compared to the paper result, the first simulation result is not so good but we can still see a large increase in secrecy rate compared to the cooperative jamming case that make these model applicable in real life. The second simulation I decided to do by myself so there is no other result to compare with but the result is also acceptable and can be referred in future work.

The difference between the first simulation result and the paper result might be related to many reason: the way they simulate (in real field, not on MATLAB), the simulation scheme setup, etc. The most obvious reason I can notice is the difference in distance setup since I simulate in a huge distance up to 50m when the paper only considers the distance 1m.

2.3 Energy Harvesting in Single Hop Relay with Jamming Technique.

Chapter 2.3 presents the combination of jamming technique and energy harvesting technique. The analysis will focus on comparing the performance of secrecy rate between AF and DF relaying mode when applying the technique.

2.3.1 System Model.

This case concentrates on investigating single hop relaying network with energy harvesting combined with jamming signal to increase secrecy rate and make the usage energy of the system efficiently.

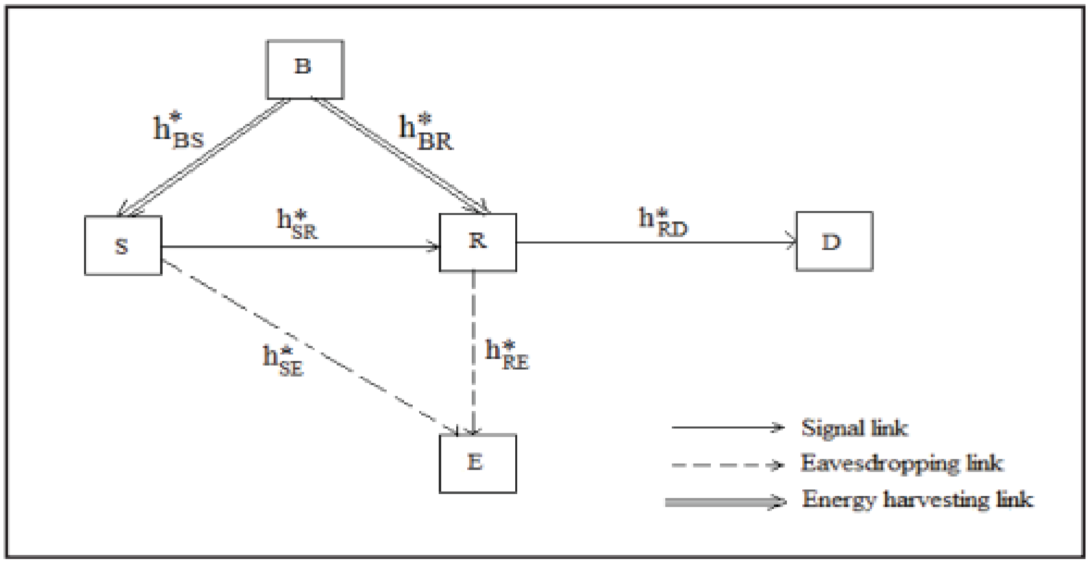

Figure 2.6: Proposed relaying system utilizing Energy Harvesting.

As shown in figure 2.6, the system has common nodes like the other cases: a source, a relay, a destination, an eavesdropper; and especially only in this case, a power beacon which provides power to source and relay. At each node, the noise is generated randomly as complex additive white Gaussian noise (AWGN). This system is studied in two most commonly used schemes: DF and AF which give me a comparison to decide the main scheme I will analyze in chapter 3. A point that need to emphasize is the system's relay in this case operates in both full and half duplex depends on the time slot it is in. This issue will be realized more clearly later.

2.3.2 Analytical Results.

a) Energy Harvesting Technique.

Energy harvesting (or power harvesting or ambient power) is the process by which energy provided by external source (power beacon in this system) is captured and stored.

As [3] mentioned, the EH technique used in this system is the time switching based EH protocol (Figure 2.7) because of its high throughput. In figure 2.7, T represents time duration to transmit a particular signal block from source to destination, 0< α <1 is time coefficient of T. The period of time T is divided into three time slots: the first time slot, when source and relay harvest energy from power beacon, lasts αT second; the second and the third time slot are the periods to transfer signal from source to relay and from relay to destination respectively and they last $(1-\alpha)\frac{T}{2}$ equally.

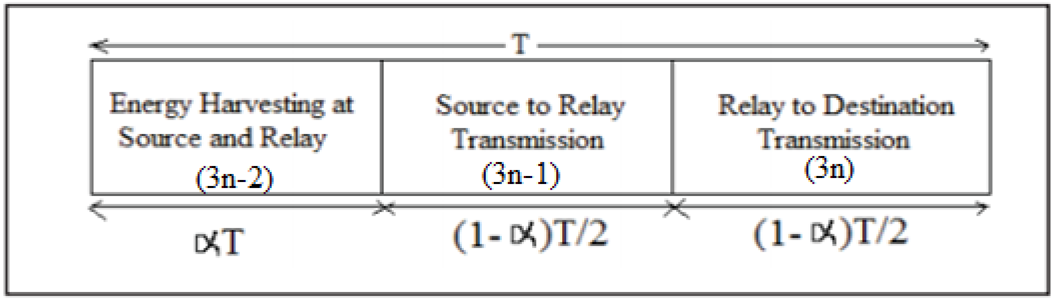
T
Energy Harvesting at Source and Relay
(3n-2)
Source to Relay Transmission
(3n-1)
Relay to Destination Transmission
(3n)
∝T
(1- ∝)T/2
(1- ∝)T/2

Figure 2.7: Time switching based EH protocol.

The harvesting energy at source and relay are expressed as below formulas respectively:

$$E_S = \eta P_B \alpha T \left| h_{BS}^* \right|^2, \tag{27}$$

$$E_R = \eta P_B \alpha T \left| h_{BR}^* \right|^2, \tag{28}$$

where 0<η<1 is the technique's energy conversion efficiency, P_B is the power provided by beacon, $\left|h_{BS}^*\right|$ and $\left|h_{BR}^*\right|$ are channel coefficients of beacon-source and beacon-relay links correspondingly.

Power transmitted by source and relay in this system are shown by:

$$P_S = \frac{2\eta P_B \alpha \left|h_{BS}^*\right|^2}{1-\alpha}, \tag{29}$$

$$P_R = \frac{2\eta P_B \alpha \left|h_{BR}^*\right|^2}{1-\alpha}. \tag{30}$$

b) DF scheme.

The scheme works in two phases as shown in figure 2.8 and 2.9 in order. For readers to understand the figures, I need to explain a little about notation of time slot. In the figures, there are two notations of time slot: (3n-1)th and (3n)th time slots. (3n-1)th time slot stands for time slot 2nd, 5th, 8th, 11th, etc. which are the corresponding "Source to Relay Transmission" time slot in figure 2.7. (3n)th time slot stand for 3rd , 6th , 9th , 12th , etc. which are the "Relay to Destination Transmission" time slot.

In the first phase (in (3n-1)th time slot) (figure 2.8), the source broadcast signal x(3n-1) to relay and also to eavesdropper. Simultaneously, the relay sends jamming signal q(3n-1) to eavesdropper. The signals received at relay and eavesdropper in this phase are given by:

$$y_R(3n-1) = \sqrt{P_S} h_{SR}^* x(3n-1) + n_R(3n-1), \tag{31}$$

$$y_E(3n-1) = \sqrt{P_S} h_{SE}^* x(3n-1) + \sqrt{P_J} h_{RE}^* q(3n-1) + n_E(3n-1), \tag{32}$$

where power of jamming signal is denoted by P_J and AWGN at relay and eavesdropper are $n_R(3n-1)$ and $n_E(3n-1)$ respectively.

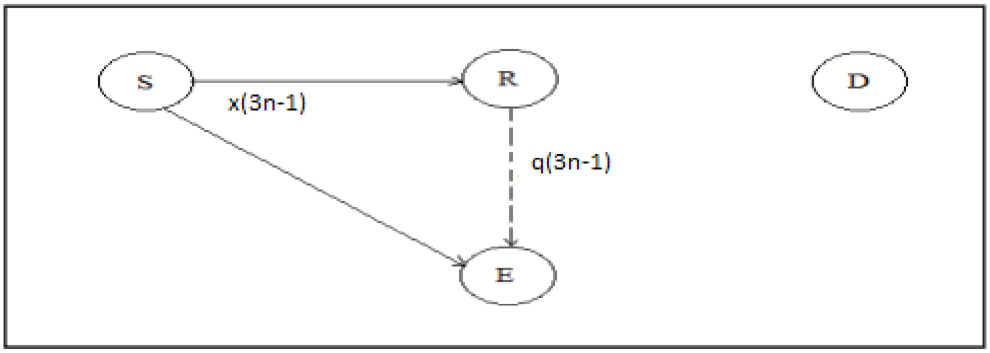

Figure 2.8: Transmission in (3n-1)th time slot.

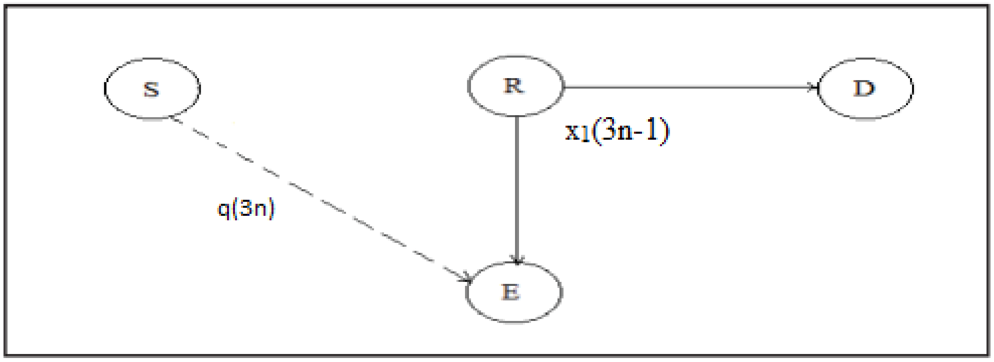

Figure 2.9: Transmission in (3n)th time slot.

In the second phase (in time slot (3n)th) (figure 2.9), relay decodes the signal from destination successfully and sends it to the destination (and also eavesdropper). At the same time, the source sends jamming signal to interfere the eavesdropper. The signal obtained at eavesdropper and destination in time slot (3n) is given as:

$$y_E(3n) = \sqrt{P_R} h_{RE}^* x_1(3n-1) + \sqrt{P_J} h_{SE}^* q(3n) + n_E(3n), \tag{33}$$

$$y_D(3n) = \sqrt{P_R} h_{RD}^* x_1(3n-1) + n_D(3n), \tag{34}$$

where $n_D(3n)$ denotes the AWGN at destination.

From the above formulas, the secrecy rates at destination and eavesdropper can be expressed as:

$$R_d = \frac{1}{2}\log_2\left(1+P_R\alpha_{RD}\right), \tag{35}$$

$$R_e = \frac{1}{2}\log_2\left(1+\frac{P_S\alpha_{SE}}{1+P_J\alpha_{RE}}+\frac{P_R\alpha_{RE}}{1+P_J\alpha_{SE}}\right), \tag{36}$$

where $\alpha_{RE} = \frac{|h_{RE}|^2}{\sigma^2}$, $\alpha_{RD} = \frac{|h_{RD}|^2}{\sigma^2}$, and $\alpha_{SE} = \frac{|h_{SE}|^2}{\sigma^2}$.

From (35) and (36), the secrecy rate of the whole system is shown as:

$$R_S = \max(R_d - R_e, 0) = \max\left(\frac{1}{2}\log_2\left(\frac{1+P_R\alpha_{RD}}{1+\frac{P_S\alpha_{SE}}{1+P_J\alpha_{RE}}+\frac{P_R\alpha_{RE}}{1+P_J\alpha_{SE}}}\right), 0\right). \tag{37}$$

c) AF scheme.

AF scheme also has two phases as the DF scheme. The first phase is similar to DF technique both in principle (shown in figure 2.8) and formulas. The second phase is similar in principle of DF technique but has a slight difference: the relay does not decode the signal but amplifies it and forward to the destination. Therefore, the formulas of received signal at eavesdropper and destination in (3n) time slot change to:

$$y_E(3n) = G\sqrt{P_S}h_{RE}^{*}y_R(3n-1)+\sqrt{P_J}h_{SE}^{*}q(3n)+n_E(3n), \tag{38}$$

$$y_D(3n) = G\sqrt{P_S}h_{RD}^{*}y_R(3n-1)+n_D(3n), \tag{39}$$

where G is scaling factor of amplification and given by: $G = \frac{1}{\sqrt{P_S|h_{SR}|^2+N}}$ (N is variance of noise).

From (38) and (39), the formulas for secrecy rates at destination and eavesdropper of AF scheme can be deduced as:

$$R_d = \frac{1}{2}\log_2\left(1+G^2 P_S \alpha_{RD}\right), \tag{40}$$

$$R_e = \frac{1}{2}\log_2\left(1+\frac{P_S\alpha_{SE}}{1+P_J\alpha_{RE}}+\frac{G^2 P_S\alpha_{RE}}{1+P_J\alpha_{SE}}\right). \tag{41}$$

The secrecy rate can be expressed as:

$$R_S = \max(R_d - R_e, 0) = \max\left(\frac{1}{2}\log_2\left(\frac{1+G^2 P_S\alpha_{RD}}{1+\frac{P_S\alpha_{SE}}{1+P_J\alpha_{RE}}+\frac{G^2 P_S\alpha_{RE}}{1+P_J\alpha_{SE}}}\right), 0\right). \tag{42}$$

2.3.3 Numerical and Simulation Results.

2.3.3.1 Setup for simulation.

In this EH and jamming case, I simulate three tests as the paper did. These tests still focus on showing the changes of secrecy rate R$_S$ in two common schemes AF and DF related to relay-eavesdropper distance d$_{RE}$, relay-destination distance d$_{RD}$, and path loss exponent c. Three tests have a bit difference in data setup but in overall, they are identical.

The channel coefficients are set the same as in cooperative jamming scene:

$$h = \left(d\right)^{\frac{-c}{2}} e, \tag{43}$$

where d is the distance between two nodes, e is a uniformly distributed random complex number (a+bi), c is the path loss exponent

In the first test secrecy rate versus relay-eavesdropper distance, I set $d_{BS} = d_{BR} = 7$ (m), $d_{SR} = 10$ (m), $d_{RD} = 15$ (m), noise power $\sigma^2 = -60$ dBm, beacon power $P_B = 30$ dBm, $\alpha = 0.99$, $\eta = 0.9$, $c = 3.5$, jamming power of relay and source are equal $P_J = 10$ dBm. Distance between relay and eavesdropper varies in range [15, 40] (m).

For the second test secrecy rate versus relay-destination distance, I set $d_{BS} = d_{BR} = 7$ (m), $d_{SR} = 10$ (m), $d_{RE} = 15$ (m), noise power $\sigma^2 = -60$ dBm, beacon power $P_B = 30$ dBm, $\alpha = 0.99$, $\eta = 0.9$, $c = 3.5$, jamming power of relay and source are equal $P_J = 10$ dBm. Distance between relay and destination increase one by one from 5 (m) to 30 (m).

For the last test secrecy rate versus path loss exponent, I set $d_{BS} = d_{BR} = 7$ (m), $d_{SR} = 10$ (m), $d_{RD} = d_{RE} = 15$ (m), noise power $\sigma^2 = -60$ dBm, beacon power $P_B = 30$ dBm, $\alpha = 0.99$, $\eta = 0.9$, jamming power of relay and source are equal $P_J = 10$ dBm. Path loss exponent increase 0.2 each step from 2 to 4.

Each simulation is done 10,000 times with the change of uniformly distributed random complex number e each time and the result is averaged at last.

2.3.3.2 Simulation result.

In all the figures, the x line belongs to AF scheme and the o line belongs to DF scheme.

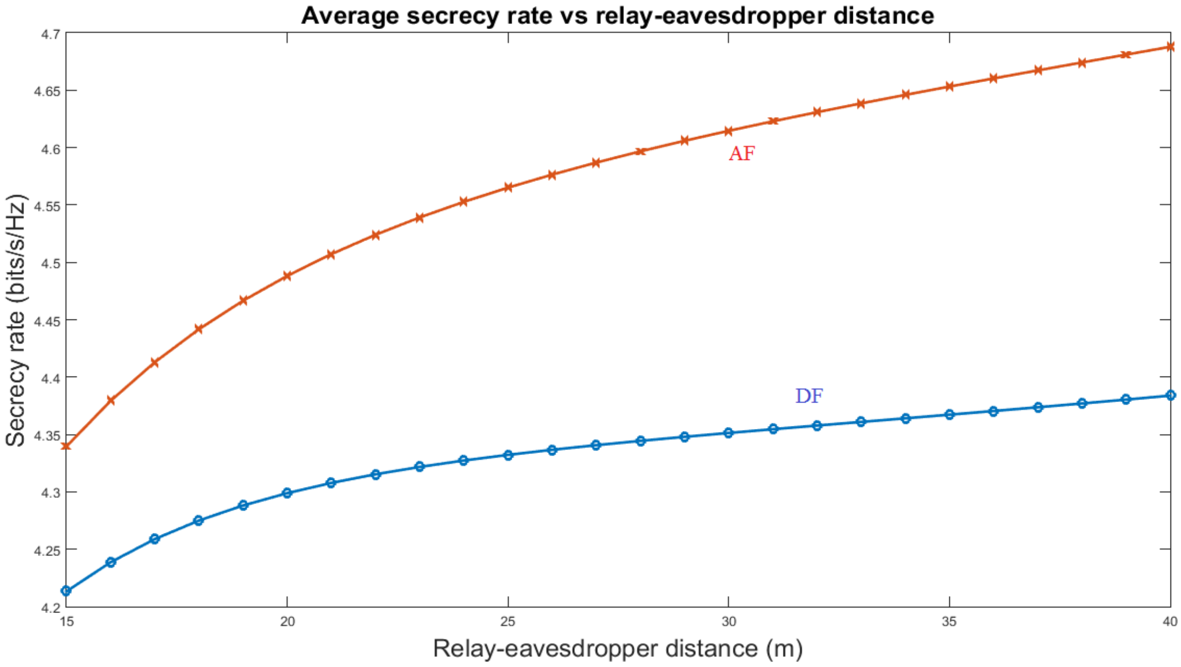

Figure 2.10: Secrecy rate versus relay-eavesdropper distance (EH).

Figure 2.10 above shows the plot of average secrecy rate versus relay-eavesdropper distance. Whenever the distance between relay and eavesdropper increase, the secrecy rate of both AF and DF increase. The trends of both line are the same as paper's result which is very good and stable (higher than 4). This is a big step forward in increasing secrecy rate compare to cooperative jamming (R_S<<1) and relay selection with cooperative jamming (0<R_S<2). One more thing to keep in mind is that the result of AF is better than the result of DF throughout the process (AF's result is higher than DF's at least 0.15 and maximum is 0.7 in the test).

Figure 2.11 below shows the plot of average secrecy rate versus relay-destination distance. In this case, the distance between relay and destination is inversely proportional to the secrecy rate of both AF and DF which is also identical to the author's test. The secrecy rates of both AF and DF can rise to 7 maximum makes this secrecy rate be the highest one from the beginning of this report and there are no result lower than 2. Moreover, the AF's secrecy rate line still shows better outcome than DF's line for the whole test although the difference is not so great.

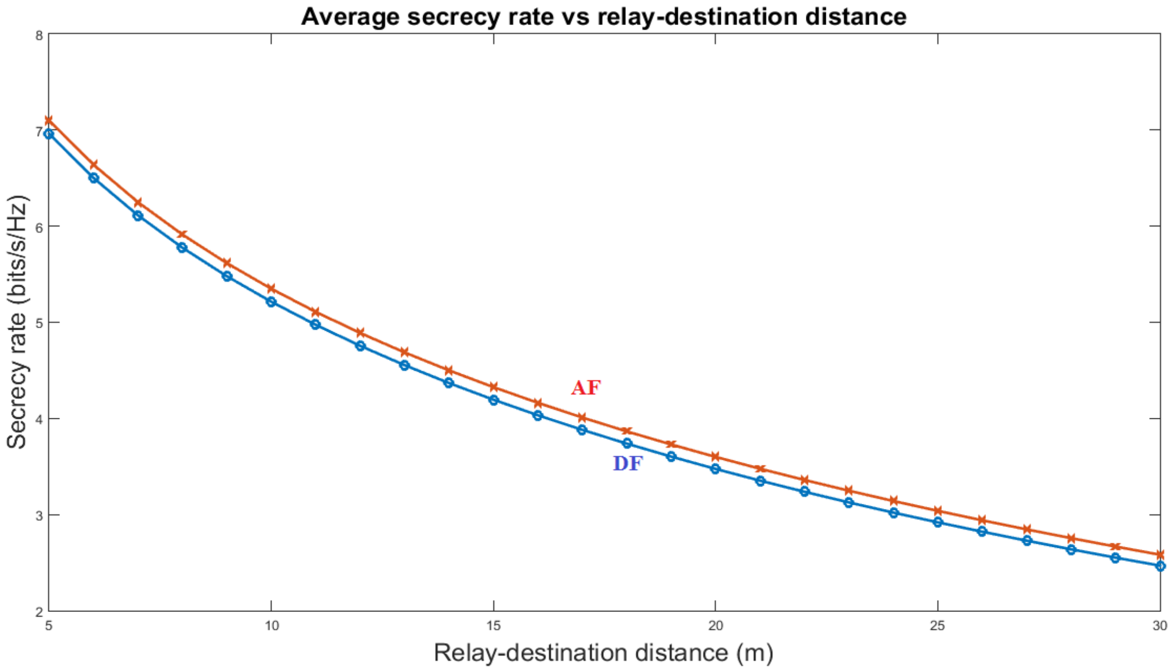

Figure 2.11: Secrecy rate versus relay-destination distance (EH).

Contrary to the above figures, figure 2.12 shows a different result than the one in paper. In this test (secrecy rate vs. path loss exponent), the secrecy rates of DF decrease strongly from approximately 7.25 to 3.2 when the path loss exponent increases from 2 to 4. On the other hands, the secrecy rates of AF increase a bit from about 5 to 5.25 when path loss exponent goes from 2 to 2.6 and then begins dropping to around 3.5 when the path loss exponent reaches 4. Although the secrecy rates of both schemes drop a lot (especially in DF), in the end (path loss exponent equals to 4), they maintain higher than 3 (about 3.25 for DF and 3.4 for AF) which are favorable results.

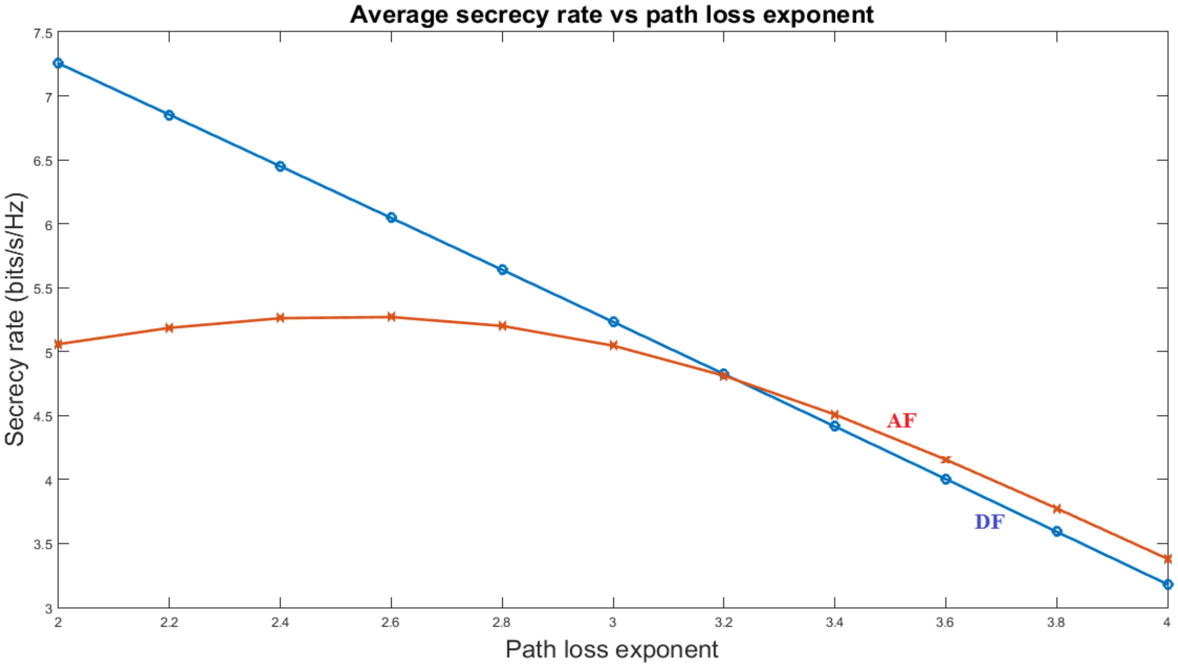

Figure 2.12: Secrecy rate versus path loss exponent (EH).

2.3.3.3 Conclusion.

After three simulations of energy harvesting and cooperative jamming, I can conclude that this combination technique is great and applicable for real life. Compared to the cooperative jamming only and relay selection combining with cooperative jamming, this combination is superior in both secrecy rate result and energy usage: for the same amount of total power for source and relay, for example P=30 dBm, the lowest secrecy rate in energy harvesting case is higher than 2 when the maximum secrecy rate in both cooperative jamming and relay selection case cannot get to 2. Although the result in the third simulation is not as similar as the paper’s simulation, I can still satisfy with it and acclaim that the difference relates to the error in the programs that I and the author used or some unknown reasons that I haven’t found out yet.

One more thing to conclude is that the AF scheme works better than DF in most cases if we only care about the physical setup and transmission in order to increase channel security. However, to make the right choice for a good scheme between AF or DF to focus in chapter 3, I will have paper [4] analyzed before changing to chapter 3 for beamforming and jamming combination technique.

2.4 Relaying mode selection for chapter 3: AF or DF.

In [1], the author's simulation result shows that the AF scheme is better than DF but the gap is not so big. From the simulations in 2.3, we can see that the AF is better than DF more clearly but the gap is not so big in second simulation and in third simulation, AF's result is lower than DF's for the first half part. Therefore, [4] will be a good reference to make the last decision in the main scheme that we concentrate in chapter 3.

2.4.1 System Model.

The author of [4] proposed a cooperative wireless network with multiple relays which considers both AF and DF protocols. Although there are multiple schemes the author examined such as multiple relay combining (MRC) and optimal relay selection (ORS) in normal and traditional way, I will analyze only the normal AF and DF based optimal relay selection schemes, abbreviated as P-AFbORS and P-DFbORS respectively. The result in the simulation part is not shown as secrecy rate but as intercept probability, which is the event happens when the channel capacity is negative (the channel capacity of main link (source-relay-destination) is smaller than wiretap link (relay-eavesdropper)).

This cooperative wireless network system make up of one source, one destination, M relays and one eavesdropper as shown in figure 2.13. In the figure, main links are represented by solid line and the wiretap links are represented by dash lines.

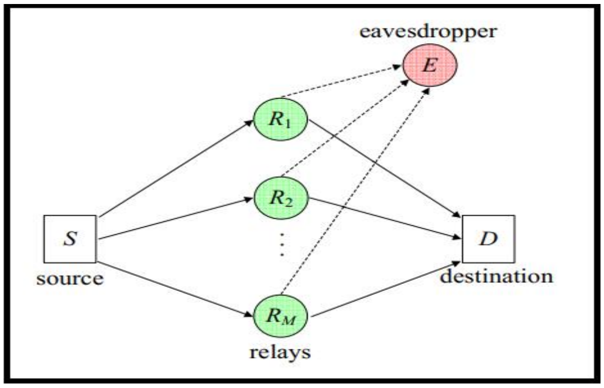

Figure 2.13: System model of optimal relay selection case.

All the links are modeled as Rayleigh fading channels and any noise at any node is modeled by complex Gaussian random variable with zero mean and variance σ_n^2. The paper has assumption that there are no direct links from source to destination and eavesdropper in AF and DF systems because of some reasons like source is too far from both destination and eavesdropper that the broadcast signal cannot reach or there is no sight of line between them.

2.4.2 Analytical Results.

This section introduces the analysis of paper [4] and gives the formulas in secrecy rate and the intercept probability of direct transmission, AF and DF relaying mode.

a) Direct Transmission

For showing the effect of AF and DF protocols, the conventional direct transmission (DT) is considered as well. Assume that the source transmits a signal s with power P, the received signal at destination is expressed as:

$$r_d = \sqrt{P} h_{sd} s + n_d , \tag{44}$$

where h_{sd} symbolizes for a fading coefficient of the channel from source to destination, n_d is AWGN at destination.

When the source broadcasts signal, the eavesdropper also receive a replica of the signal which is expressed as:

$$r_e = \sqrt{P} h_{se} s + n_e , \tag{45}$$

where h_{se} symbolizes for a fading coefficient of the channel from source to eavesdropper, n_e is AWGN at eavesdropper.

The direct transmission channel capacity (or secrecy rate) of the source-destination channel and the source-eavesdropper channel are expressed respectively as:

$$C_{sd}^{direct} = \log_2\left(1+\frac{|h_{sd}|^2 P}{\sigma_n^2}\right), \tag{46}$$

$$C_{se}^{direct} = \log_2\left(1+\frac{|h_{se}|^2 P}{\sigma_n^2}\right), \tag{47}$$

where σ_n^2 is the noise variance.

As we know from all the other parts of this report, the channel capacity of the whole direct transmission system is the difference between the main channel (source-destination) and the wiretap channel (source-eavesdropper):

$$C^{direct} = C_{sd}^{direct} - C_{se}^{direct} = \log_2\left(1+\frac{|h_{sd}|^2 P}{\sigma_n^2}\right) - \log_2\left(1+\frac{|h_{se}|^2 P}{\sigma_n^2}\right). \tag{48}$$

From the definition of probability of intercept in system model part, the formula for the direct transmission probability of intercept can be deduced as:

$$P_{\text{int}ercept}^{direct} = \Pr\left(C_{sd}^{direct} < C_{se}^{direct}\right) = \Pr\left(\left(1+\frac{|h_{sd}|^2 P}{\sigma_n^2}\right) < \left(1+\frac{|h_{se}|^2 P}{\sigma_n^2}\right)\right) = \Pr\left(|h_{sd}|^2 < |h_{se}|^2\right)$$

$$. \tag{49}$$

Since the Rayleigh fading model is considered, $|h_{sd}|^2$ and $|h_{se}|^2$ can be recognized to follow exponential distributions. Hence, a closed-form of direct transmission intercept probability is supposed to be:

$$P_{\text{int}ercept}^{direct} = \frac{\sigma_{se}^2}{\sigma_{se}^2 + \sigma_{sd}^2}, \tag{50}$$

where $\sigma_{se}^2 = E\left(|h_{se}|^2\right)$ and $\sigma_{sd}^2 = E\left(|h_{sd}|^2\right)$.

Formula shows that the intercept probability of direct transmission does not depend on transmit power P. Thus, increasing transmit power P does not improve the wireless security performance in this case.

b) Amplify-and-Forward protocol (P-AFbORS)

The AF system operates in two stages: the source transmits signal s to all M relays in first stage; then the optimal relay node is selected and it will transfer an amplified version of signal s to destination. Because the signal s is transmitted two times so to have a fair comparison with the direct transmission, the transmitted power in each stage must be cut down by half to $\frac{P}{2}$. As a result, received signal at relay R_i is given by:

$$r_i = \sqrt{\frac{P}{2}} h_{si} s + n_i , \tag{51}$$

where h_{si} symbolizes for a fading coefficient of the channel from source to destination, n_i is AWGN at relay R_i.

Received signal at destination is a little more complicated since the optimal selected relay R_i does the amplification of signal r_i with factor $\frac{h_{si}^*}{|h_{si}|^2 \sqrt{\frac{P}{2}}}$. To make the formula in paper clear, I decide to deduce the formula step by step:

$$r_d = \sqrt{\frac{P}{2}} h_{id} \frac{r_i h_{si}^*}{|h_{si}|^2 \sqrt{\frac{P}{2}}} + n_d = \sqrt{\frac{P}{2}} h_{id} \frac{h_{si}^* \left(\sqrt{\frac{P}{2}} h_{si} s + n_i \right)}{|h_{si}|^2 \sqrt{\frac{P}{2}}} + n_d = \frac{\sqrt{\frac{P}{2}} h_{si} h_{si}^* h_{id} s + n_i h_{id} h_{si}^*}{|h_{si}|^2} + n_d$$

$$= \sqrt{\frac{P}{2}} h_{id} s + \frac{h_{id} h_{si}^*}{|h_{si}|^2} n_i + n_d . \tag{52}$$

From the formula above I infer the channel capacity of AF protocol from R_i to destination step by step also:

$$C_{id}^{AF}=\log_2\left(1+\frac{\frac{|h_{id}|^2\frac{P}{2}}{1+\frac{|h_{id}|^2}{|h_{si}|^2}}}{\sigma^2}\right)=\log_2\left(1+\frac{\frac{|h_{id}|^2\frac{P}{2}}{\frac{|h_{id}|^2+|h_{si}|^2}{|h_{si}|^2}}}{\sigma^2}\right)=\log_2\left(1+\frac{|h_{si}|^2|h_{id}|^2\frac{P}{2}}{\left(|h_{si}|^2+|h_{id}|^2\right)\sigma^2}\right)$$

$$. \tag{53}$$

As same as the received signal form at destination, the signal receives at eavesdropper from R$_i$ is expressed as:

$$r_e=\sqrt{\frac{P}{2}}h_{ie}s+\frac{h_{ie}h_{si}^*}{|h_{si}|^2}n_i+n_e\cdot \tag{54}$$

AF protocol channel capacity of the link R$_i$-eavesdropper is obtained as:

$$C_{ie}^{AF}=\log_2\left(1+\frac{|h_{si}|^2|h_{ie}|^2\frac{P}{2}}{\left(|h_{si}|^2+|h_{ie}|^2\right)\sigma^2}\right). \tag{55}$$

Channel capacity of the entire AF protocol system with R$_i$ can be obtained as:

$$C_i^{AF}=C_{id}^{AF}-C_{ie}^{AF}=\log_2\left(\frac{1+\frac{|h_{si}|^2|h_{id}|^2P}{2(|h_{si}|^2+|h_{id}|^2)\sigma_n^2}}{1+\frac{|h_{si}|^2|h_{ie}|^2P}{2(|h_{si}|^2+|h_{ie}|^2)\sigma_n^2}}\right). \tag{56}$$

There is one more thing still missing up to this point: which condition is used to choose the optimal relay R$_i$? As in part 2.2. Relay Selection case above, the optimal relay R$_i$ is the relay that make the channel capacity of AF system as high as possible. It can be formulated as:

$$R_i = \arg\max_{i \in \Re} C_i^{AF} = \arg\max_{i \in \Re} \left(\frac{1 + \frac{|h_{si}|^2 |h_{id}|^2 P}{2(|h_{si}|^2 + |h_{id}|^2)\sigma_n^2}}{1 + \frac{|h_{si}|^2 |h_{ie}|^2 P}{2(|h_{si}|^2 + |h_{ie}|^2)\sigma_n^2}} \right), \tag{57}$$

where $\Re$ serves as a set of M relays.

The intercept probability of P-AFbORS scheme can be expressed as:

$$P_{\text{int}ercept}^{P-AFbORS} = \Pr\left(\max_{i \in \Re} C_i^{AF} < 0 \right) = \Pr\left(\max_{i \in \Re} \left(\frac{1 + \frac{|h_{si}|^2 |h_{id}|^2 P}{2(|h_{si}|^2 + |h_{id}|^2)\sigma_n^2}}{1 + \frac{|h_{si}|^2 |h_{ie}|^2 P}{2(|h_{si}|^2 + |h_{ie}|^2)\sigma_n^2}} \right) < 0 \right) = \prod_{i=1}^{M} \Pr\left(|h_{id}|^2 < |h_{ie}|^2 \right)$$

$$. \tag{58}$$

Assuming that $|h_{ie}|^2$ and $|h_{id}|^2$ are independent exponentially distributed random variables, we can formulate (58) as:

$$P_{\text{int}ercept}^{P-AFbORS} = \prod_{i=1}^{M} \frac{\sigma_{ie}^2}{\sigma_{ie}^2 + \sigma_{id}^2}, \tag{59}$$

where $\sigma_{ie}^2 = E\left(|h_{ie}|^2 \right)$ and $\sigma_{id}^2 = E\left(|h_{id}|^2 \right)$.

c) Decode-and-Forward (P-DFbORS)

The DF relaying protocol system operates also in 2 stages: in first stage, the source sends an encoded signal s to all M relays. In second stage, the optimal selected relay decodes the signal and forwards it to the destination. The same in P-AFbORS case, the operation of DF system has two stages which make the transmit power usage in each stage to be lower to $\frac{P}{2}$ to have a good comparison to direct transmission case.

Considering that the encoded signal is sent from source to relays and the decoded signal is sent from chosen relay to destination are two kind of different signals, we can see two stages as two independent processes and the channel capacity of the main channel is deduced as the minimum between two stages channel capacities:

$$C_{sid}^{DF} = \min\left(C_{si}, C_{id}\right), \tag{60}$$

where C_{si} and C_{id} perform for channel capacity of source-relays links and chosen relay-destination link, respectively. They are formulated as:

$$C_{si} = \log_2\left(1 + \frac{|h_{si}|^2 P}{2\sigma_n^2}\right), \tag{61}$$

$$C_{id} = \log_2\left(1 + \frac{|h_{id}|^2 P}{2\sigma_n^2}\right), \tag{62}$$

Since the eavesdropper can wiretap the transmission of R$_i$, we can deduce the channel capacity of R$_i$-eavesdropper link as:

$$C_{ie}^{DF} = \log_2\left(1 + \frac{|h_{ie}|^2 P}{2\sigma_n^2}\right). \tag{63}$$

From (60), (61), (62) and (63), the capacity channel of DF protocol system with R$_i$ is given by:

$$\begin{aligned} C_i^{DF} = C_{sid}^{DF} - C_{ie}^{DF} &= \log_2\left(1 + \frac{\min\left(|h_{si}|^2, |h_{id}|^2\right)P}{2\sigma_n^2}\right) - \log_2\left(1 + \frac{|h_{ie}|^2 P}{2\sigma_n^2}\right) \\ &= \log_2\left(\frac{\min\left(|h_{si}|^2, |h_{id}|^2\right)P + 2\sigma_n^2}{|h_{ie}|^2 P + 2\sigma_n^2}\right). \end{aligned} \tag{64}$$

From formula of channel capacity above, the criteria for selecting optimal relay R$_i$ can be retrieved simply as:

$$R_i = \arg\max_{i\in\Re} C_i^{DF} = \arg\max_{i\in\Re}\left(\frac{\min\left(\left|h_{si}\right|^2, \left|h_{id}\right|^2\right)P + 2\sigma_n^2}{\left|h_{ie}\right|^2 P + 2\sigma_n^2}\right). \tag{65}$$

The probability of intercept of P-DFbORS scheme can be deduced from intercept event definition and formula above as:

$$P_{\text{int}ercept}^{P-DFbORS} = \Pr\left(\max_{i\in\Re} C_i^{DF} < 0\right) = \prod_{i=1}^{M} \Pr\left(\min\left(\left|h_{si}\right|^2, \left|h_{id}\right|^2\right) < \left|h_{ie}\right|^2\right). \tag{66}$$

Because $\left|h_{si}\right|^2$, $\left|h_{id}\right|^2$, and $\left|h_{ie}\right|^2$ are random exponent distributions with means σ_{si}^2, σ_{id}^2 , σ_{ie}^2 respectively. Let $\mathrm{X} = \min\left(\left|h_{si}\right|^2, \left|h_{id}\right|^2\right)$, [4] shows the cumulative density function (CDF) of X as:

$$P_X\left(X < x\right) = 1 - \exp\left(-\frac{x}{\sigma_{si}^2} - \frac{x}{\sigma_{id}^2}\right), \tag{67}$$

where $x \geq 0$.

From the formulas (66) and (67), I can have the deduction below:

$$\begin{aligned}\Pr\left(\min\left(\left|h_{si}\right|^2, \left|h_{id}\right|^2\right) < \left|h_{ie}\right|^2\right) &= \int_0^\infty \left[1 - \exp\left(-\frac{x}{\sigma_{si}^2} - \frac{x}{\sigma_{id}^2}\right)\right]\frac{1}{\sigma_{ie}^2}\exp\left(-\frac{x}{\sigma_{ie}^2}\right)dx \\ &= \frac{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2}{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{id}^2}.\end{aligned} \tag{68}$$

Put (68) into (66) we have:

$$P_{\text{int}ercept}^{P-DFbORS} = \prod_{i=1}^{M} \frac{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2}{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{id}^2}. \tag{69}$$

In comparison between AF and DF intercept probabilities, considering that $\frac{\sigma_{id}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{ie}^2}{\sigma_{id}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{id}^2}>0$ and $\frac{\sigma_{ie}^2}{\sigma_{ie}^2+\sigma_{id}^2}>0$, [4] said we can prove that $\frac{\sigma_{ie}^2}{\sigma_{ie}^2+\sigma_{id}^2}<\frac{\sigma_{id}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{ie}^2}{\sigma_{id}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{id}^2}$ without difficulty which leads to:

$$\prod_{i=1}^{M}\frac{\sigma_{ie}^2}{\sigma_{ie}^2+\sigma_{id}^2}<\prod_{i=1}^{M}\frac{\sigma_{id}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{ie}^2}{\sigma_{id}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{id}^2}. \tag{70}$$

The comparison above gives us the theoretic conclusion that P-AFbORS's intercept probability is less than P-DFbORS's without argument. We can temporarily conclude that AF scheme has more advantage compare to DF scheme.

2.4.3 Numerical and Simulation Results.

2.4.3.1 Setup for simulation.

In order to do the intercept probability versus main-to-eavesdropper ratio (MER) simulation in paper [4], diversity gain definition is introduced. Diversity gain is the gain in signal-to-interference ratio (SINR) (or signal-to-noise ratio (SNR)) or the reduction in transmission power when having diversity scheme (multiple schemes applied). From [8], the traditional diversity gain is expressed as:

$$d=-\lim_{SNR\to\infty}\left(\frac{\log P_e\left(SNR\right)}{\log SNR}\right), \tag{71}$$

where $P_e(SNR)$ represents bit error rate and SNR represents signal-to-noise ratio.

Nevertheless, all the equations of intercept probability in three cases DT, AF, AF do not have relation to SNR which make the definition of diversity gain inapplicable and [4] suggests another form of diversity gain as:

$$d_{another} = -\lim_{\lambda \to \infty} \left(\frac{\log\left(P_{\text{intercept}}\right)}{\log\left(\lambda\right)} \right), \tag{72}$$

where $\lambda = \frac{\sigma_{sd}^2}{\sigma_{se}^2}$ is introduced as main-to-eavesdropper ratio (MER) which is the average channel gain ratio between source-destination channel and source-eavesdropper channel.

For simulating the direct transmission versus MER as announced above, the intercept probability will be alternate in MER following form as:

$$P_{\text{intercept}}^{direct} = \frac{\sigma_{se}^2}{\sigma_{se}^2 + \sigma_{sd}^2} = \frac{1}{1 + \frac{\sigma_{sd}^2}{\sigma_{se}^2}} = \frac{1}{1 + \lambda_{de}}. \tag{73}$$

In P-AFbORS scheme, expressing $\sigma_{id}^2 = \alpha_{id}\sigma_{sd}^2$ and $\sigma_{ie}^2 = \alpha_{ie}\sigma_{se}^2$, the formula of intercept probability can be rewritten as:

$$P_{\text{intercept}}^{P-AFbORS} = \prod_{i=1}^{M} \frac{\sigma_{ie}^2}{\sigma_{ie}^2 + \sigma_{id}^2} = \prod_{i=1}^{M} \frac{\alpha_{ie}\sigma_{se}^2}{\alpha_{ie}\sigma_{se}^2 + \alpha_{id}\sigma_{sd}^2} = \prod_{i=1}^{M} \frac{\alpha_{ie}}{\alpha_{ie} + \alpha_{id}\frac{\sigma_{sd}^2}{\sigma_{se}^2}} = \prod_{i=1}^{M} \left(\frac{\alpha_{ie}}{\frac{\sigma_{sd}^2}{\sigma_{se}^2}\left(\alpha_{ie}\frac{\sigma_{se}^2}{\sigma_{sd}^2} + \alpha_{id} \right)} \right)$$

$$= \prod_{i=1}^{M} \left(\frac{\alpha_{ie}}{\lambda_{de}\left(\alpha_{ie}\lambda_{de}^{-1} + \alpha_{id} \right)} \right) = \prod_{i=1}^{M} \left(\frac{\alpha_{ie}}{\alpha_{ie} + \alpha_{id}\lambda_{de}} \right).$$

(74)

For P-DFbORS scheme, denoting $\sigma_{si}^2 = \alpha_{si}\sigma_{sd}^2$, deducing the intercept probability formula will give us the following expression:

$$P_{\text{intercept}}^{P-DFbORS} = \prod_{i=1}^{M} \frac{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2}{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{id}^2} = \prod_{i=1}^{M} \frac{\alpha_{id} + \alpha_{si}}{\lambda_{de}\left(\alpha_{id}\lambda_{de}^{-1} + \alpha_{si}\lambda_{de}^{-1} + \alpha_{si}\alpha_{id}\alpha_{ie}^{-1} \right)}$$

$$= \prod_{i=1}^{M} \frac{\alpha_{id} + \alpha_{si}}{\alpha_{id} + \alpha_{si} + \alpha_{si}\alpha_{id}\alpha_{ie}^{-1}\lambda_{de}}.$$

(75)

I set up $\alpha_{si} = \alpha_{id} = \alpha_{ie} = 1$, MER varies from -5 to 15 dB, number of relays M=2, 4.

Because the formulas (73), (74), (75) used in this simulation have only constants α_{si}, α_{si}, α_{si}, M, and variable λ; there are no generated randomly variables as the others simulation. Therefore, this simulation does not need to be run many times as the other parts' simulations.

2.4.3.2 Simulation result

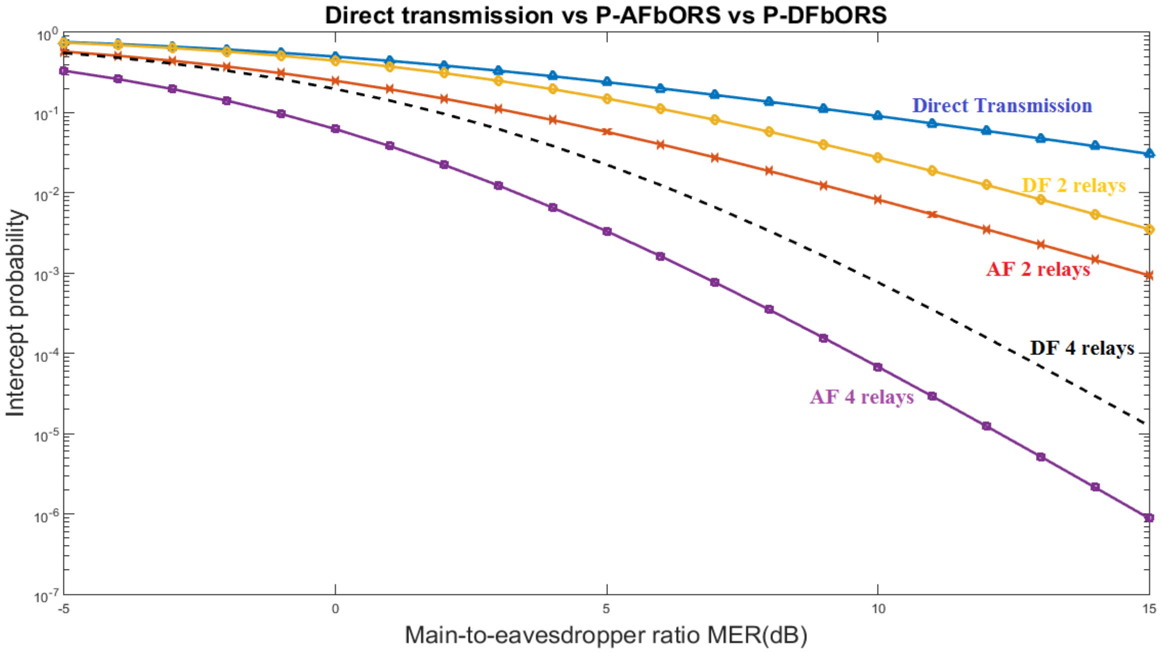

Figure 2.14: Intercept probability versus main-to-eavesdropper ratio (MER) (ORS).

The figure 2.14 has annotations inside for each line. We can see clearly that with the same number of relay M=2 or M=4, the P-AFbORS' intercept probability is always lower (which means better) than P-DFbORS' and both of them have better outcomes than the direct transmission scheme. As increasing the number of relays from 2 to 4, the probabilities of intercept event of both AF and DF systems decreases which means the enhancing in level of physical security network.

2.4.3.3 Conclusion

The main objective of this part is to compare between AF and DF protocol to decide which is better to concentrate mainly in chapter 3. After both theory proving and simulation in this 2.4 part combined with [1]'s simulation result and the result of 2.3 simulation, I can have final conclusion that the chosen protocol is AF since it is completely superior to DF in overall.

Chapter 3: Jamming and Beamforming.

This chapter focuses on combination schemes of jamming and beamforming. Section 3.1 presents a combination of beamforming and jamming methods and power allocation while Section 3.2 presents a combination of beamforming, jamming and multiple relays and jammers selection. In section 3.3, the model and analytical results of an extra scheme using beamforming and jamming supporting from the destination techniques are presented.

3.1 Beamforming, Jamming and Power Allocation.

Chapter 3.1 introduce the combination of beamforming, jamming techniques with the way to allocate power to receive the best secrecy rate result for the system.

3.1.1 System Model.

In this case, we will study an AF relay network in which there are a source S sending information to a destination D under the appearance of an eavesdropper E and N relays R between them. This network uses only single antenna in half-duplex mode for every nodes. To highlight the effect of beamforming and jamming techniques, there is no direct transmission from source to destination so every transmissions have to go through the cooperative relays network. In this part, aside from applying diversity scheme (beamforming and jamming) to increase channel secrecy, optimizing the source's power allocation is also considered to enhance the channel further.

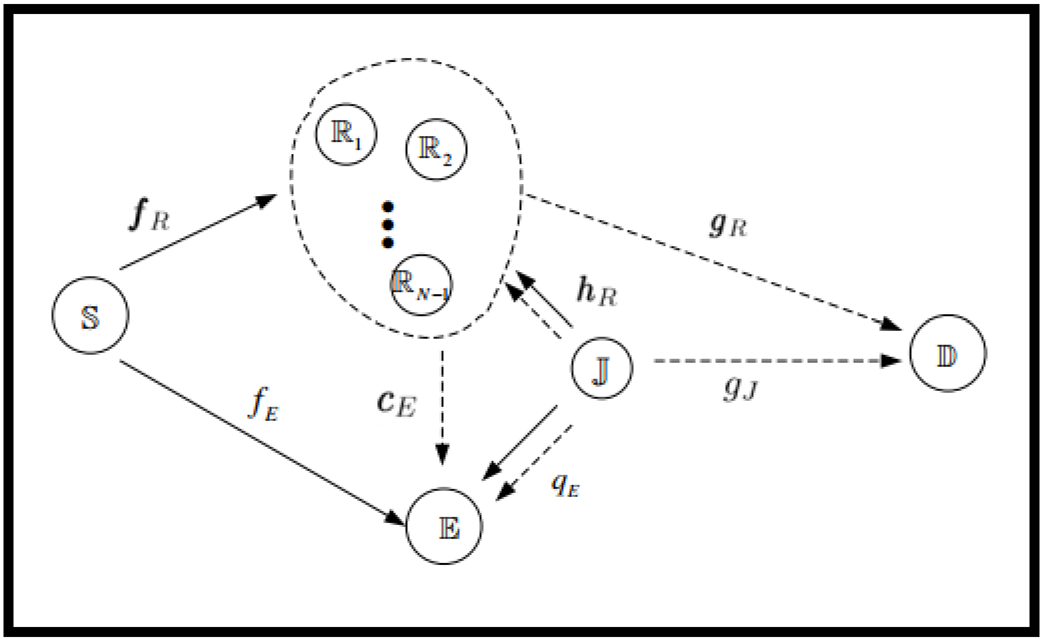

Figure 3.1: System model for beamforming, jamming and power allocation scheme.

The system model design is shown clearly in figure 3.1 above. The group of relays is divided into 2 subgroups: 1 jammer and N-1 relays. The relays subgroup will transmit the signal received from source to destination utilizing the cooperative beamforming. The jammer has only one important mission: broadcast artificial signal to disrupt the eavesdropper. In the figure, besides the notations of main nodes, the other notations represent for the quasi-stationary flat-fading channels between those main nodes which will be shown more detailed later.

3.1.2 Analytical Results.

Before reading further, I would notice a small note: if the transmission is single input single output (SISO), the signal, noise, and coefficients channel are in form of normal variable, denoting as lower case letters like: y, f, h; if the transmission is single input multiple output (SIMO) or multiple input single output (MISO), the signal, noise, and coefficients channel are in form of vector variable, , denoting as bold lower case letters like: $\mathbf{f}_R$, $\mathbf{h}_R$; if the transmission is multiple input multiple output (MIMO), the signal, noise, and coefficients channel are in form of matrix, , denoting as bold upper case letters like: $\mathbf{W}$, $\mathbf{R}$.

As a necessity in AF relaying system, the operation is commonly broken into two steps.

In step I, source transmit signal s to N-1 relay nodes while jammer covers the transmission with artificial noise. The received signal vector at relays subgroup is expressed as:

$$\mathbf{y}_R = \sqrt{P_S}\mathbf{f}_R s + \sqrt{P_J^{(1)}}\mathbf{h}_R z^{(1)} + \mathbf{n}_R, \tag{76}$$

where $\mathbf{y}_R = \left[y_{R,1}, y_{R,2}, ..., y_{R,N-1}\right]^T$, $\mathbf{f}_R = \left[f_{R,1}, \mathrm{f}_{R,2}, ..., \mathrm{f}_{R,N-1}\right]^T$, $\mathbf{h}_R = \left[h_{R,1}, \mathrm{h}_{R,2}, ..., \mathrm{h}_{R,N-1}\right]^T$. P_S and $P_J^{(1)}$ are the transmit powers of the source and the jammer, respectively. $z^{(1)}$ is the jamming signal, $\mathbf{n}_R$ is the additive noise at relay nodes.

Simultaneously, the eavesdropper can also obtain a copy of signal s which can be written in the form of:

$$y_E^{(1)} = \sqrt{P_S}\, f_E s + \sqrt{P_J^{(1)}} q_E z^{(1)} + n_E^{(1)}, \tag{77}$$

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

In step II, N-1 relays address the received signal to destination with the help of distributed beamforming technique. Concurrently, the jammer also uses the same method to broadcast artificial signal. Consequently, we can deduce the formulas of received signal at destination and eavesdropper, respectively, as:

$$y_D = \sqrt{P_S}\mathbf{g}_R^T\mathbf{W}\mathbf{f}_R s + \sqrt{P_J^{(1)}}\mathbf{g}_R^T\mathbf{W}\mathbf{h}_R z^{(1)} + \bar{n}_D, \tag{78}$$

$$y_E^{(2)} = \sqrt{P_S}\mathbf{c}_E^T\mathbf{W}\mathbf{f}_R s + \sqrt{P_J^{(1)}}\mathbf{c}_E^T\mathbf{W}\mathbf{h}_R z^{(1)} + \bar{n}_E^{(2)}, \tag{79}$$

where $\bar{n}_D = \sqrt{P_J^{(2)}} g_J z^{(2)} + \mathbf{g}_R^T\mathbf{W}\mathbf{n}_R + n_D$, $\bar{n}_E^{(2)} = \sqrt{P_J^{(2)}} q_E z^{(2)} + \mathbf{c}_R^T\mathbf{W}\mathbf{n}_R + n_E^{(2)}$, $\mathbf{c}_E = \left[\mathrm{c}_{\mathrm{E},1}, \mathrm{c}_{\mathrm{E},2}, ..., \mathrm{c}_{\mathrm{E},N-1}\right]^T$ and n_D, $n_E^{(2)}$ are additive noises at destination and eavesdropper during step II, respectively. $\mathbf{W} = diag\left(\left[w_1^*, w_2^*, ..., w_{N-1}^*\right]\right)$ is weight matrix in form of diagonal matrix. $P_J^{(2)}$ is transmit power of jammer in step II.

Equation (78) can be reformed as:

$$y_D = \sqrt{P_S}\mathbf{w}^\dagger \mathbf{a}_{fg} s + \sqrt{P_J^{(1)}}\mathbf{w}^\dagger \mathbf{a}_{gh} z^{(1)} + \bar{n}_D \,, \tag{80}$$

where $\mathbf{a}_{fg} = \left[f_{\mathrm{R},1} g_{\mathrm{R},1}, f_{\mathrm{R},2} g_{\mathrm{R},2}, ..., f_{\mathrm{R,N-1}} g_{\mathrm{R,N-1}} \right]^T$, $\mathbf{a}_{gh} = \left[g_{\mathrm{R},1} h_{\mathrm{R},1}, g_{\mathrm{R},2} h_{\mathrm{R},2}, ..., g_{\mathrm{R,N-1}} h_{\mathrm{R,N-1}} \right]^T$, and $\mathbf{w} = \left[w_1, w_2, ..., w_{N-1} \right]^T$

Combining $y_E^{(1)}$, $y_E^{(2)}$ and reformulating a bit gives the overall formula for the received signal at the eavesdropper:

$$\mathbf{y}_E = \begin{bmatrix} \sqrt{P_S} f_E \\ \sqrt{P_S}\mathbf{w}^\dagger \mathbf{a}_{cf} \end{bmatrix} s + \begin{bmatrix} \bar{n}_E^{(1)} \\ \sqrt{P_J^{(1)}}\mathbf{c}_E^T \mathbf{W}\mathbf{h}_R z^{(1)} + \bar{n}_E^{(2)} \end{bmatrix} = \mathbf{H}_E s + \mathbf{n}_E \,, \tag{81}$$

where $\mathbf{H}_E = \begin{bmatrix} \sqrt{P_S} f_E \\ \sqrt{P_S}\mathbf{w}^\dagger \mathbf{a}_{cf} \end{bmatrix}$, $\mathbf{n}_E = \begin{bmatrix} \bar{n}_E^{(1)} \\ \sqrt{P_J^{(1)}}\mathbf{c}_E^T \mathbf{W}\mathbf{h}_R z^{(1)} + \bar{n}_E^{(2)} \end{bmatrix}$, $\mathbf{a}_{cf} = \left[c_{\mathrm{E},1} f_{\mathrm{R},1}, \mathrm{c}_{\mathrm{E},2}\ f_{\mathrm{R},2}, ..., \mathrm{c}_{\mathrm{E,N-1}}\ f_{\mathrm{R,N-1}} \right]^T$, $\mathbf{a}_{cg} = \left[c_{\mathrm{E},1} g_{\mathrm{R},1}, \mathrm{c}_{\mathrm{E},2}\ g_{\mathrm{R},2}, ..., \mathrm{c}_{\mathrm{E,N-1}}\ g_{\mathrm{R,N-1}} \right]^T$, and $\bar{n}_E^{(1)} = \sqrt{P_J^{(1)}} q_E z^{(1)} + n_E^{(1)}$.

All the noises: n_D, $n_E^{(1)}$, $n_E^{(2)}$, $\mathbf{n}_R$ are assumed time-spatially white independent complex Gaussian random variables with zero mean and variance σ^2. Jamming signal $z^{(1)}$ and $z^{(2)}$ are both considered as complex Gaussian random variables.

Let $\mathbf{R}_{ff} = diag\left(\left| f_{R,1} \right|^2, \left| f_{R,2} \right|^2, ..., \left| f_{R,\mathrm{N-1}} \right|^2 \right)$, $\mathbf{R}_{gg}$ and $\mathbf{R}_{cc}$ are also set the same. $\mathbf{R}_{fg} = \mathbf{a}_{fg}\mathbf{a}_{fg}^\dagger$ and similarly for $\mathbf{R}_{cf}$, $\mathbf{R}_{gh}$, $\mathbf{R}_{ch}$. From received signal formulas at destination and eavesdropper, formulas for secrecy rate (channel capacity) at destination, eavesdropper and the whole system, respectively, can be inferred as:

$$R_D = \frac{1}{2}\log_2\left(1 + \frac{P_S \mathbf{w}^\dagger \mathbf{R}_{fg}\mathbf{w}}{\sigma^2\left(1 + \mathbf{w}^\dagger \mathbf{R}_{gg}\mathbf{w}\right) + P_J^{(1)}\mathbf{w}^\dagger \mathbf{R}_{gh}\mathbf{w} + P_J^{(2)}\left| g_J \right|^2} \right), \tag{82}$$

$$R_E = \frac{1}{2}\log_2\left[\det\left(\mathbf{I} + \mathbf{H}_E\mathbf{H}_E^{\dagger}\mathbf{Q}_E^{-1}\right)\right], \tag{83}$$

$$R_S = \max\left(R_D - R_E, 0\right), \tag{84}$$

where $\mathbf{Q}_E = \begin{pmatrix} \sigma^2 + P_J^{(1)}\left|q_E\right|^2 & P_J^{(1)}q_E\mathbf{h}_R^{\dagger}\mathbf{W}^{\dagger}\mathbf{c}_E^{*} \\ P_J^{(1)}q_E^{\dagger}\mathbf{c}_E^{T}\mathbf{W}\mathbf{h}_R & P_J^{(1)}\mathbf{c}_E^{T}\mathbf{W}\mathbf{h}_R\mathbf{h}_R^{\dagger}\mathbf{W}^{\dagger}\mathbf{c}_E^{*} \end{pmatrix}$, $\mathbf{I}$ is identity matrix.

To maximize the secrecy rate, searching for the optimal $\mathbf{w}$, $P_J^{(1)}$, $P_J^{(2)}$ and P_S is the work we must do and as you can see in the formulas above, it is very difficult to be done, even if fixing P_S as we commonly do. Hence, [5] propose a heuristic scheme which give us an acceptably better solution:

- $\mathbf{w}$ will be designed in the null space of $\mathbf{a}_{cf}$ which makes $w^{\dagger}\mathbf{a}_{cf} = 0$ and helps simplify matrix $\mathbf{H}_E$ to become a normal variable $H_E = \sqrt{P_S}\,f_E$. The author says this design will eliminate completely information exposure in step II.
- $\mathbf{w}$ will be considered in the null space of $\mathbf{a}_{gh}$ also, which makes $w^{\dagger}\mathbf{a}_{gh} = 0$. This consideration according to the author is to remove the artificial noise inside received signal at relays in step I so that it will indirectly eliminate the first part of interception effect from jammer to the destination.
- Because the information exposure in step II is completely eliminated (in first •), the jammer does not need to broadcast jamming signal ($P_J^{(2)} = 0$) and the destination node is not interfered directly in phase II which make the destination be totally free of jamming signal.

Following three proposes of design above, formula (82) and (83) can be reformulated as:

$$R_D = \frac{1}{2}\log_2\left(1 + \frac{P_S}{\sigma^2}\frac{\mathbf{w}^{\dagger}\mathbf{R}_{fg}\mathbf{w}}{1 + \mathbf{w}^{\dagger}\mathbf{R}_{gg}\mathbf{w}}\right), \tag{85}$$

$$R_E = \frac{1}{2}\log_2\left(1+\frac{P_S\,|f_E|^2}{\sigma^2+P_J^{(1)}|q_E|^2}\right). \tag{86}$$

In order to reduce the channel quality of the eavesdropper as poor as possible, Power of jammer in step I $P_J^{(1)}$ should be refined equally to the maximum power constraint of the jammer $\overline{P_J}$.

Placing (85) and (86) into (84), then fixing the equation a bit will give us the optimization problem below:

$$\begin{aligned}
\max_{\mathbf{w},P_S} \quad & \frac{\sigma^2+P_S\dfrac{\mathbf{w}^\dagger\mathbf{R}_{fg}\mathbf{w}}{1+\mathbf{w}^\dagger\mathbf{R}_{gg}\mathbf{w}}}{a+bP_S}, \\
s.t. \quad & \mathbf{w}^\dagger\mathbf{a}_{cf} = 0, \\
& \mathbf{w}^\dagger\mathbf{a}_{gh} = 0, \\
& \mathbf{w}^\dagger\mathbf{T}(P_S)\mathbf{w} \le P_R, \\
& P_S < P_T,
\end{aligned} \tag{87}$$

where $a=\sigma^2+\overline{P_J}|q_E|^2$, $b=|f_E|^2$, $\mathbf{T}(P_S)=P_S\mathbf{R}_{ff}+\overline{P_J}\mathbf{R}_{hh}+\sigma^2\mathbf{I}$, P_T is source power constraint and P_R is the total power constraint of relays.

The policy to select jammer: from secrecy rate equation at eavesdropper, we can assume that the relay which has the largest channel coefficient to the eavesdropper $|q_E|^2$ is the selected jammer.

Considering $\mathbf{H}=\left[\mathbf{a}_{cf},\mathbf{a}_{gh}\right]$ and $\mathbf{H}_\perp$ is the projection matrix onto null space of $\mathbf{H}$. Because matrix $\mathbf{H}$ has two components $\mathbf{a}_{cf}$ and $\mathbf{a}_{gh}$ as column vector, according to equation 5.13.2 from [9], $\mathbf{H}_\perp$ has the form as:

$$\mathbf{H}_\perp = \mathbf{H}\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T. \tag{88}$$

Then, $\mathbf{w}$ can be formulated as $\mathbf{w}=\mathbf{H}_{\perp}\mathbf{v}$, where $\mathbf{v}$ is any column vector. Assuming the condition $\mathbf{w}^{\dagger}\mathbf{T}\left(P_S\right)\mathbf{w}\le P_R$ can be simplified when $\mathbf{w}$ is optimum, the condition inequality becomes $\mathbf{w}^{o\dagger}\mathbf{T}\left(P_S\right)\mathbf{w}^{o}=P_R$. The problem (87) can be changed to:

$$\begin{aligned} &\max_{\mathbf{v},P_S} \quad \frac{\sigma^2+P_S\dfrac{\mathbf{v}^{\dagger}\overline{\mathbf{R}}_{fg}\mathbf{v}}{1+\mathbf{v}^{\dagger}\overline{\mathbf{R}}_{gg}\mathbf{v}}}{a+bP_S}, \\ &s.t. \quad \mathbf{v}^{\dagger}\overline{\mathbf{T}}\left(P_S\right)\mathbf{v}=P_R, \\ &\qquad\;\; P_S<P_T, \end{aligned} \tag{89}$$

where $\overline{\mathbf{R}}_{fg}=\mathbf{H}_{\perp}^{\dagger}\mathbf{R}_{fg}\mathbf{H}_{\perp}$, $\overline{\mathbf{R}}_{gg}=\mathbf{H}_{\perp}^{\dagger}\mathbf{R}_{gg}\mathbf{H}_{\perp}$, $\overline{\mathbf{T}}\left(P_S\right)=P_S\overline{\mathbf{R}}_{ff}+\overline{P_J}\overline{\mathbf{R}}_{hh}+\sigma^2\mathbf{I}$, $\overline{\mathbf{R}}_{ff}=\mathbf{H}_{\perp}^{\dagger}\mathbf{R}_{ff}\mathbf{H}_{\perp}$, $\overline{\mathbf{R}}_{hh}=\mathbf{H}_{\perp}^{\dagger}\mathbf{R}_{hh}\mathbf{H}_{\perp}$.

The author decides to break the problem above into a double-layer problem:

$$\begin{aligned} &\max_{P_S} \quad \frac{\sigma^2+P_S\max\limits_{\mathbf{v}}\left(\dfrac{\mathbf{v}^{\dagger}\overline{\mathbf{R}}_{fg}\mathbf{v}}{1+\mathbf{v}^{\dagger}\overline{\mathbf{R}}_{gg}\mathbf{v}}\right)}{a+bP_S}, \\ &s.t. \quad \mathbf{v}^{\dagger}\overline{\mathbf{T}}\left(P_S\right)\mathbf{v}=P_R, \\ &\qquad\;\; P_S<P_T, \end{aligned} \tag{90}$$

where the inner layer problem is to optimize $\mathbf{v}$ when considering P_S as constant and the outer layer problem focuses on maximizing P_S.

Firstly, we concentrate on inner layer optimization. As denoted, $\overline{\mathbf{T}}\left(P_S\right)$ is realized to be positive definite matrix so that there is an invertible matrix $\mathbf{A}\left(P_S\right)$ fulfilled the equation: $\overline{\mathbf{T}}\left(P_S\right)=\mathbf{A}\left(P_S\right)^{\dagger}\mathbf{A}\left(P_S\right)$. The matrix $\mathbf{A}\left(P_S\right)$ can be solved easily by using Cholesky decomposition (or Cholesky factorization) function in MATLAB. Let $\overline{\mathbf{v}}=\frac{1}{\sqrt{P_R}}\mathbf{A}\left(P_S\right)\mathbf{v}$ and substitute it into inner layer part of (90) to have the inner layer optimization problem rewritten as:

$$\begin{aligned} &\max_{\bar{\mathbf{v}}} \quad \left(\frac{\bar{\mathbf{v}}^{\dagger}\mathbf{B}\left(P_S\right)\bar{\mathbf{v}}}{\bar{\mathbf{v}}^{\dagger}\mathbf{D}\left(P_S\right)\bar{\mathbf{v}}} \right), \\ &s.t. \quad \bar{\mathbf{v}}^{\dagger}\bar{\mathbf{v}} = 1, \end{aligned} \tag{91}$$

where $\mathbf{B}\left(P_S\right) = P_R\mathbf{A}\left(P_S\right)^{-\dagger}\overline{\mathbf{R}}_{fg}\mathbf{A}\left(P_S\right)^{-1}$, and $\mathbf{D}\left(P_S\right) = \mathbf{I} + P_R\mathbf{A}\left(P_S\right)^{-\dagger}\overline{\mathbf{R}}_{gg}\mathbf{A}\left(P_S\right)^{-1}$.

Secondly, from problem (91), the optimal $\bar{\mathbf{v}}^{o}$ can be derived as follow:

$$\bar{\mathbf{v}}^{o} = \alpha\varepsilon\left(\mathbf{D}\left(P_S\right)^{-1}\mathbf{B}\left(P_S\right)\right), \tag{92}$$

where $\varepsilon\left(\mathbf{X}\right)$ is one eigenvector of matrix $\mathbf{X}$ correlated to the maximum eigenvalue, α is a scalar to normalize $\bar{\mathbf{v}}^{o}$ to fit $\bar{\mathbf{v}}^{\mathrm{o}\dagger}\bar{\mathbf{v}}^{o} = 1$ which is formulated as:

$$\alpha = \left\| \mathbf{D}\left(P_S\right)^{-1}\mathbf{A}\left(P_S\right)^{-\dagger}\mathbf{H}_{\perp}^{\dagger}\mathbf{a}_{fg} \right\|. \tag{93}$$

Finally, we have the optimal $\mathbf{v}^{o}$ equality as:

$$\mathbf{v}^{o} = \alpha\sqrt{P_R}\mathbf{A}\left(P_S\right)^{-1}\mathbf{D}\left(P_S\right)^{-1}\mathbf{A}\left(P_S\right)^{-\dagger}\mathbf{H}_{\perp}^{\dagger}\mathbf{a}_{fg}\,. \tag{94}$$

For the outer layer problem, formula (91) can be transferred to maximum objective function as:

$$f\left(P_S\right) = P_R\mathbf{a}_{fg}^{\dagger}\mathbf{H}_{\perp}\left(\overline{\mathbf{T}}\left(P_S\right) + P_R\overline{\mathbf{R}}_{gg}\right)^{-1}\mathbf{H}_{\perp}^{\dagger}\mathbf{a}_{fg}\,, \tag{95}$$

which is substituted into (90) provided the compacted outer layer optimization:

$$\begin{aligned} &\max_{P_S} \quad g\left(P_S\right) = \log_2\left(\sigma^2 + h\left(P_S\right)\right) - \log_2\left(a + bP_s\right), \\ &s.t. \quad 0 \le P_S \le P_T \end{aligned} \tag{96}$$

where $h\left(P_S\right) = P_R P_S \mathbf{h}^{\dagger}\mathbf{J}\left(P_S\right)\mathbf{h}$, $\mathbf{h} = \mathbf{H}_{\perp}^{\dagger}\mathbf{a}_{fg}$ and $\mathbf{J}\left(P_S\right) = \left(P_S\overline{\mathbf{R}}_{ff} + \overline{P}_J\overline{\mathbf{R}}_{hh} + \sigma^2\mathbf{I} + P_R\overline{\mathbf{R}}_{gg}\right)^{-1}$

At this point, the author of [5] suggests to check the condition to choose the optimal source power P_S^o. However, when I do the simulation, the first condition $m(0)\le 0$ is always right but I fixed $P_S^o = 0$ dBm as the author's suggestion. The function $m(P_S)$ we need to check the condition is:

$$m(P_S)=(a+bP_S)h^{'}(P_S)-b\sigma^2-bh(P_S), \tag{97}$$

where $h^{'}(P_S)=P_R\left(\mathbf{h}^{\dagger}\mathbf{J}(P_S)\mathbf{h}-P_S\mathbf{h}^{\dagger}\mathbf{J}^2(P_S)\overline{\mathbf{R}}_{ff}\mathbf{h}\right)$ is the first derivative of $h(P_S)$.

After having $P_S^o = 0$ dBm, I put it into (94) to have $\mathbf{v}^o$ and $\mathbf{w}^o=\mathbf{H}_{\perp}\mathbf{v}^o$. In the end, applying optimal power source P_S^o and optimal weight vector (beamforming vector) $\mathbf{w}^o$ into secrecy rate formulas (85), (86) to finish the problem.

3.1.3 Numerical and Simulation Results.

3.1.3.1 Setup for simulation.

The channel coefficients in this case are generated randomly as complex zero-mean Gaussian with unit covariance which are in the form of complex numbers: $a+bi$

I set number of relays N equal 8, power of source $P_S^o = 0$ dBm, and $\sigma^2 = 10^{-6}$.

The simulation I do in this 3.1 section is average secrecy rate versus power of relay and jammer so I let $P_M = P_R + \overline{P}_J$ increase from 8 to 40 dBm in step of 4 dBm each. P_R is calculated by following formula: $P_R = P_M + \frac{N-1}{N}$, and $\overline{P}_J = \frac{P_R}{N-1}$.

I have to admit that this simulation is very unstable since it contains a lot of complex matrix calculations which make it is difficult to manage the outcome after each stage and the final in overall. Moreover, as you can see above, the condition which should be tested up to three times is always right in the first test which is still a questionable problem for me to solve.

Therefore, I do not let this simulation run thousands of loop because it wastes time and do not let us see the true potential of the combination scheme. I will test this one by hand and show the suitable result that I choose.

3.1.3.2 Simulation result

This result is the most familiar to the result in the paper and the secrecy rate is quite acceptable compared to the other ones so I choose it to show. As we can see, the secrecy rate is proportional to the sum power of relay and jammer but the rise rate is not the same at each point. The secrecy rates increase very fast from 1.3 to 1.7 when the power increases from 8 to 16 dBm. After that, secrecy rate line increases slower from 1.7 to 2.2 in a large range of power [16; 40] dBm.

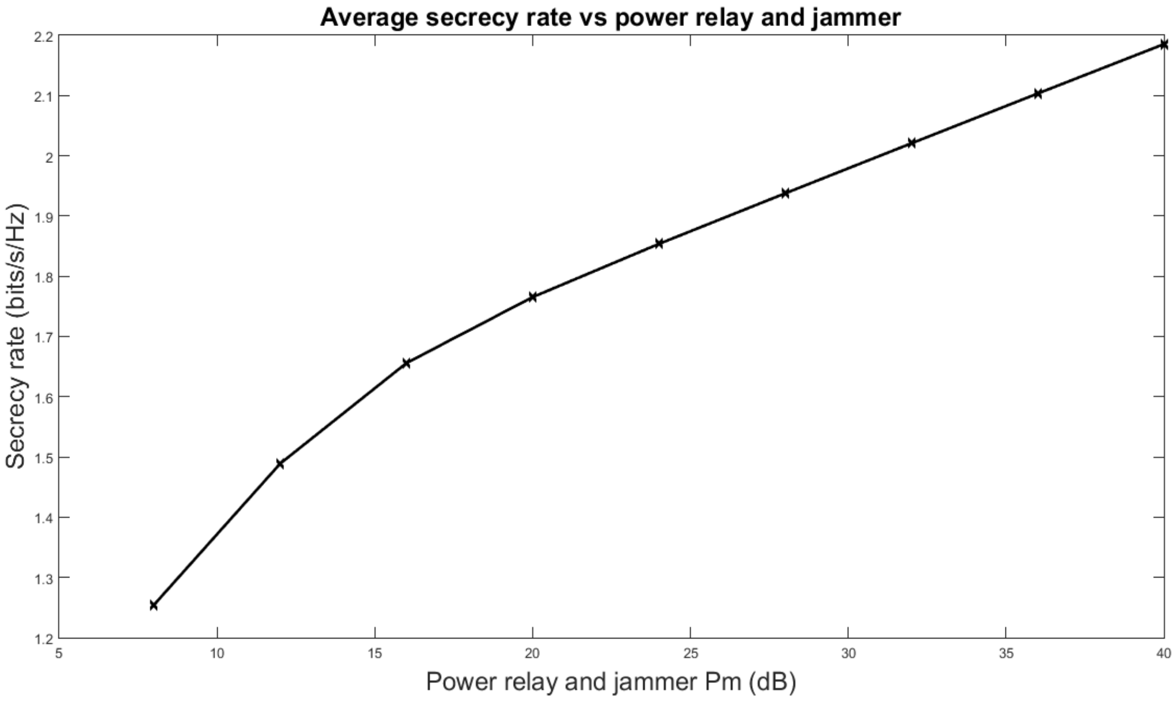

Figure 3.2: Secrecy rate versus power of relay and jammer (3.1).

3.1.3.3 Conclusion

The behavior of the secrecy rate line is not as same as the one in the paper which has the fast increase up to the power of 28 dBm. Since the paper I analyzed is a difficult one but I decide to simplify it in simulation a bit due to the problem in checking condition so the behavior of the scheme is not as good as I expected. I think in the real world, this scheme can be considered to apply because the result is still acceptable and in overall we can somehow accept it as a reference for future development. However, the secrecy rate cannot get higher than 2.2 which makes this scheme seems incomparable to the power harvesting combined with jamming case in this report. Therefore, we can move on to the next one to see the improvement and superior of beamforming and jamming combining scheme.

3.2 Beamforming, jamming and multiple relays, jammers selection.

This chapter shows the combination of beamforming and jamming with the selection policy for multiple relays and jammers. The relays are chosen first based on relays-destination links and jammers are chosen after that based on source-relays link.

3.2.1 System Model.

Section 3.2 comes up with a two-phase cooperative network with relay selection, cooperative jamming and cooperative beamforming scheme. Since the section 3.1 above simulated with 8 relays, this section applies the same number of relays to have a better comparison between schemes and to avoid unnecessary complexity that make the result worse than predicted. The system model in this scheme (figure 3.3) is familiar to the others in above sections: 1 source, 1 eavesdropper, 1 destination and M=8 relays. Every nodes uses a single omni-directional antenna running in the half-duplex mode which helps reduce the analysis' complexity. The eavesdropper is a passive one which receives and decodes the signal without disturbing the transmission by interfering or modifying it. Because this scheme is also to emphasize the role of AF cooperative networks (or role of multiple relays), the channel source-destination is assumed not available so all the transmissions have to go through the network. However, in this scheme, the direct channel from source to eavesdropper exists.

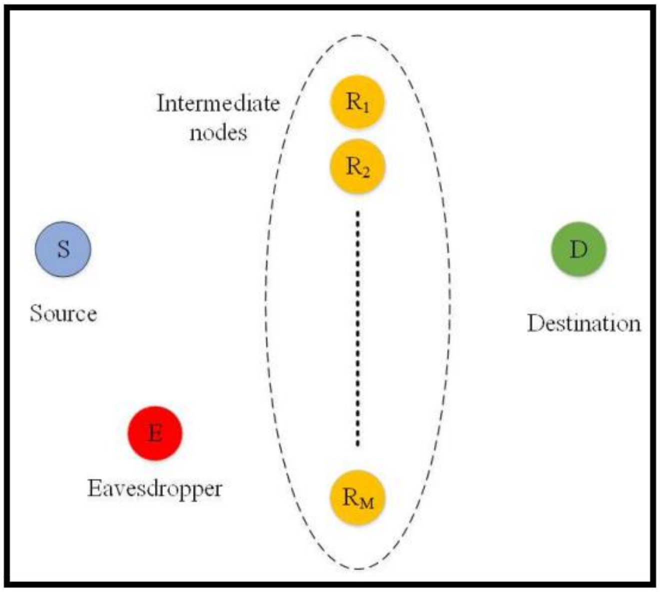

Figure 3.3: System model for chosen beamforming and jamming scheme.

The specialty in this scheme is the number of chosen jammer and chosen relay are not only one for each. Three relays marking as R_o, R_p, R_q are selected jammers and two relays marking as R_m, R_n are selected relays (as shown in figure 3.4). Figure 3.4 shows not only the notations but also the operation of the system. As in another AF relaying network system, the operation is divided into two phase:

In phase I, the source transmit signal to five free relays while three selected relays as jammers cast jamming signal to confuse the eavesdropper.

In phase II, two selected forwarding relays send scaled version of the signal to the destination node by performing beamforming technique.

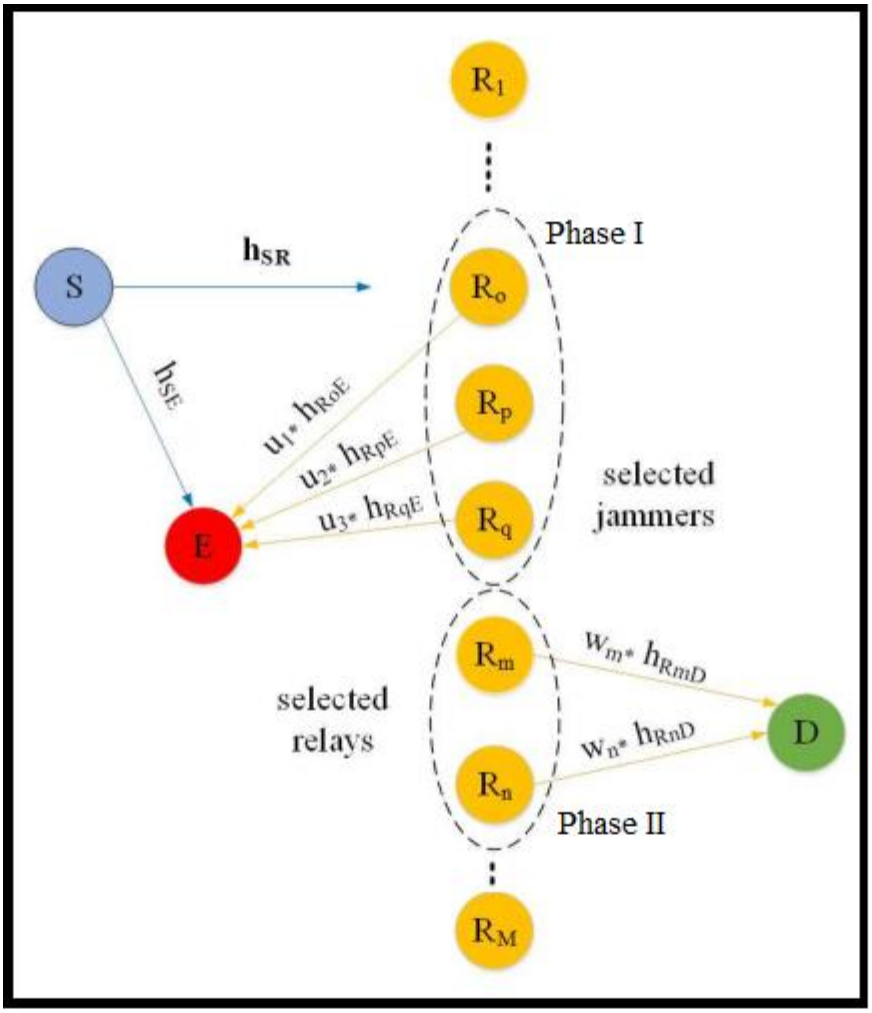

Figure 3.4: The operation of the chosen beamforming and jamming combination.

3.2.2 Analytical Results.

First, I will consider about the relays selection since the paper has priority for it before jammer selection. Expecting that R_m, R_n are chosen relays in phase II, the received signal formulas at destination and eavesdropper in phase II are given as:

$$y_D^{(2)} = \sqrt{P_R}\mathbf{w}^T\mathbf{h}_{RD,(m,n)}x + n_D^{(2)}, \tag{98}$$

$$y_E^{(2)} = \sqrt{P_R}\mathbf{w}^T\mathbf{h}_{RE,(m,n)}x + n_E^{(2)}, \tag{99}$$

where P_R is transmit power of relays, χ is the transmitted signal, $\mathbf{w}=\left[w_m \quad w_n\right]^T$, $\mathbf{h}_{RD,(m,n)}=\left[h_{RD,m} \quad h_{RD,n}\right]$ and $\mathbf{h}_{RE,(m,n)}=\left[h_{RE,m} \quad h_{RE,n}\right]$ are complex channel coefficient vectors of chosen relays to the destination and eavesdropper, respectively. $n_D^{(2)}$ and $n_E^{(2)}$ are the AWGN at the destination node and the eavesdropper node, respectively.

The signal-to-noise ratio (SNR) equations at the destination and the eavesdropper can be deduced from (98) and (99) are expressed as:

$$\gamma_D^{(2)}=\frac{P_R\left|\mathbf{w}^T\mathbf{h}_{RD,(m,n)}\right|^2}{\sigma_n^2}, \tag{100}$$

$$\gamma_E^{(2)}=\frac{P_R\left|\mathbf{w}^T\mathbf{h}_{RE,(m,n)}\right|^2}{\sigma_n^2}, \tag{101}$$

where σ_n^2 is noise power.

As in other sections, the achievable secrecy rate formulas at the destination, the eavesdropper and the whole system are given respectively as:

$$R_D=\frac{1}{2}\log_2\left(1+\gamma_D\right), \tag{102}$$

$$R_E=\frac{1}{2}\log_2\left(1+\gamma_E\right), \tag{103}$$

$$R_S=\max\left(R_D-R_E,0\right). \tag{104}$$

The beamforming vector the selected relays use is designed to eliminate the leakage information to eavesdropper which make SNR at eavesdropper equals zero and lead to the problem below:

$$\begin{aligned}&\mathbf{w}^T\mathbf{h}_{RE,(m,n)}=0,\\&s.t.\quad \mathbf{w}^\dagger\mathbf{w}=1.\end{aligned} \tag{105}$$

Changing above problem to vector form, we have the expression:

$$\begin{aligned}&\begin{bmatrix} w_m & w_n \end{bmatrix}\begin{bmatrix} h_{RE,m} \\ h_{RE,n} \end{bmatrix} = 0, \\ &s.t. \quad \mathbf{w}^\dagger \mathbf{w} = 1.\end{aligned} \tag{106}$$

From the expression we can deduce the components of vector $\mathbf{W}$ as:

$$w_m = \alpha h_{RE,n}, \tag{107}$$

$$w_n = -\alpha h_{RE,\mathrm{m}}, \tag{108}$$

where $\alpha = \dfrac{1}{\left|h_{RE,m}\right|^2 + \left|h_{RE,\mathrm{n}}\right|^2}$.

Substitute (107) and (108) into SNR at the destination (100), we have the new formula as:

$$\gamma_D^{(2)} = \alpha^2 \frac{P_R}{\sigma_n^2} \left| h_{RE,n} h_{RD,m} - h_{RE,\mathrm{m}} h_{RD,n} \right|^2. \tag{109}$$

After having the latest SNR formula at the destination, relay selection rule is the one I have to consider next. The principle is the same as the other selection rules in chapter 2 since I will choose the two relays that maximize the SNR at the destination. The rule can be shown as:

$$(m,n) = \arg \max_{\substack{m,n \in \{1,\ldots,8\} \\ m \neq n}} \gamma_{D,(m,n)}^{(2)} . \tag{110}$$

Return to phase I where the jammers selection happens, I suppose that selected jammers are R_o, R_p, R_q as said above and corresponding beamforming vector for jammers is $\mathbf{u} = \begin{bmatrix} u_1 & u_2 & u_3 \end{bmatrix}^T$. Although there are five relays accepting the signal from source, we care only the received signal at two selected relays R_m, R_n which is formulated as:

$$y_{R_m}^{(1)} = \sqrt{P_S} h_{SR_m} x + \sqrt{P_J} \mathbf{u}^T \mathbf{h}_{JR_m} z + n_{R_m}^{(1)}, \tag{111}$$

$$y_{R_n}^{(1)} = \sqrt{P_S}\, h_{SR_n} x + \sqrt{P_J}\, \mathbf{u}^T \mathbf{h}_{JR_n} z + n_{R_n}^{(1)}, \tag{112}$$

where x is transmitted signal, z is jamming signal, $\mathbf{h}_{JR_m} = \begin{bmatrix} h_{R_o R_m} & h_{R_p R_m} & h_{R_q R_m} \end{bmatrix}^T$ and $\mathbf{h}_{JR_n} = \begin{bmatrix} h_{R_o R_n} & h_{R_p R_n} & h_{R_q R_n} \end{bmatrix}^T$ are channel coefficient vectors of selected jammers R_o, R_p, R_q to corresponding selected relays R_m, R_n. h_{SR_m} and h_{SR_n} are the channel coefficients between source and two selected relays R_m, R_n, respectively. $n_{R_m}^{(1)}$ and $n_{R_n}^{(1)}$ are AWGN at R_m and R_n , respectively.

The signal eavesdropper receiving in phase I is given as:

$$y_E^{(1)} = \sqrt{P_S}\, h_{SE} x + \sqrt{P_J}\, \mathbf{u}^T \mathbf{h}_{JE} z + n_E^{(1)}, \tag{113}$$

where $\mathbf{h}_{JE} = \begin{bmatrix} h_{R_o E} & h_{R_p E} & h_{R_q E} \end{bmatrix}^T$ is channel coefficient vector between three selected jammers to eavesdropper.

In order to let the selected relays send a good version of received signal from source to destination, the artificial noise effect from jammers must be removed which give us a triple-condition design as:

$$\begin{cases} \mathbf{u}^T \mathbf{h}_{JR_m} = 0, \\ \mathbf{u}^T \mathbf{h}_{JR_n} = 0, \\ \mathbf{u}^\dagger \mathbf{u} = 1. \end{cases} \tag{114}$$

Translating the condition about to matrix form gives us:

$$\begin{pmatrix} h_{R_o R_m} & h_{R_p R_m} & h_{R_q R_m} \\ h_{R_o R_n} & h_{R_p R_n} & h_{R_q R_n} \\ u_1^* & u_2^* & u_3^* \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}. \tag{115}$$

Calculating the matrix multiplication above will lead to three equations of beamforming vector components in phase I as below:

$$u_1 = \frac{h_{R_pR_m} h_{R_qR_n} - h_{R_pR_n} h_{R_qR_m}}{\sqrt{\left(h_{R_pR_m} h_{R_qR_n} - h_{R_pR_n} h_{R_qR_m}\right)^2 + \left(h_{R_oR_n} h_{R_qR_m} - h_{R_oR_m} h_{R_qR_n}\right)^2 + \left(h_{R_oR_m} h_{R_pR_n} - h_{R_pR_m} h_{R_oR_n}\right)^2}} \\ , \tag{116}$$

$$u_2 = \frac{h_{R_oR_n} h_{R_qR_m} - h_{R_oR_m} h_{R_qR_n}}{\sqrt{\left(h_{R_pR_m} h_{R_qR_n} - h_{R_pR_n} h_{R_qR_m}\right)^2 + \left(h_{R_oR_n} h_{R_qR_m} - h_{R_oR_m} h_{R_qR_n}\right)^2 + \left(h_{R_oR_m} h_{R_pR_n} - h_{R_pR_m} h_{R_oR_n}\right)^2}} \\ , \tag{117}$$

$$u_3 = \frac{h_{R_oR_m} h_{R_pR_n} - h_{R_pR_m} h_{R_oR_n}}{\sqrt{\left(h_{R_pR_m} h_{R_qR_n} - h_{R_pR_n} h_{R_qR_m}\right)^2 + \left(h_{R_oR_n} h_{R_qR_m} - h_{R_oR_m} h_{R_qR_n}\right)^2 + \left(h_{R_oR_m} h_{R_pR_n} - h_{R_pR_m} h_{R_oR_n}\right)^2}} \\ . \tag{118}$$

Deducing from equation (113) we have the SNR formula at the eavesdropper in phase I as:

$$\gamma_E^{(1)} = \frac{P_S \left|h_{SE}\right|^2}{\sigma_n^2 + P_J \left|\mathbf{u}^T \mathbf{h}_{JE}\right|^2}. \tag{119}$$

Contradictory to the relay selection policy, the jammer selection policy focuses on minimize the $\gamma_E^{(1)}$ to decrease the quality of eavesdropper channel which means maximizing $\left|\mathbf{u}^T \mathbf{h}_{JE}\right|^2$ because it is the only component in the equation that relates to jammer. Hence, the jammer selection policy can be shown as:

$$\left(o, p, q\right) = \arg \max_{\substack{o,p,q \in \{1,\ldots,8\} \\ o,p,q \neq m,n}} \left|\mathbf{u}^T \mathbf{h}_{JE}\right|^2 .$$

In the end, summarizing from two phases gives us the achievable secrecy rate formula as:

$$R_S = \max\left\{\frac{1}{2}\log_2\left(\frac{1+\gamma_D^{(2)}}{1+\gamma_E^{(1)}+\gamma_E^{(2)}}\right), 0\right\}, \tag{120}$$

but the design of beamforming technique forces the SNR of eavesdropper in phase II equal 0 so the formula above will be fixed to suit the condition:

$$R_S = \max\left\{\frac{1}{2}\log_2\left(\frac{1+\gamma_D^{(2)}}{1+\gamma_E^{(1)}}\right), 0\right\}. \tag{121}$$

3.2.3 Numerical and Simulation Results.

3.2.3.1 Simulation Setup

In this simulation section, I use my most favorite setting which let destination stay away from source at (0, 0) 50 meters (means at (50, 0)) and the eavesdropper stays in the middle of the distance at (25, 0). The 8-relay group will be generated randomly between (1, 0) and (49, 0).

The channel coefficients uses the most popular form as:

$$h = (d)^{\frac{-c}{2}} e, \tag{122}$$

where d is the distance between two nodes, e is a uniformly distributed random complex number (a+bi), c is the path loss exponent which is equal 3.5 in this simulation.

In the simulation secrecy rate versus power of jammers, I set total power of system dBm, source power $P_S = 3$dBm, power of relays $P_R = P_T - P_S - P_J$. Power of jammer is set shifting in range [-15; 10] dBm which the length of each step is 0.5 dBm.

In the simulation secrecy rate versus eavesdropper's position, I set total power of system $P_T = 10$ dBm, source power $P_S = 3$dBm, power of jammer $P_J = 3$dBm, power of relays $P_R = P_T - P_S - P_J$. The eavesdropper's position is changed from 5 meters to 49 meters away from the source.

Although the first simulation shows very good results in every test, not all result shows exactly the trend of secrecy line in the paper since the relays' position are random and there are also random generated coefficients that affect the outcome. Therefore, I will also test by hand and let the program run 1000 times every test and choose the graph with good trend to show. After having a favorable simulation result from first simulation, I continue to run the second simulation which need some inherited data from the first such as relays' position, channel coefficients which need to be fixed.

3.2.3.2 Simulation results.

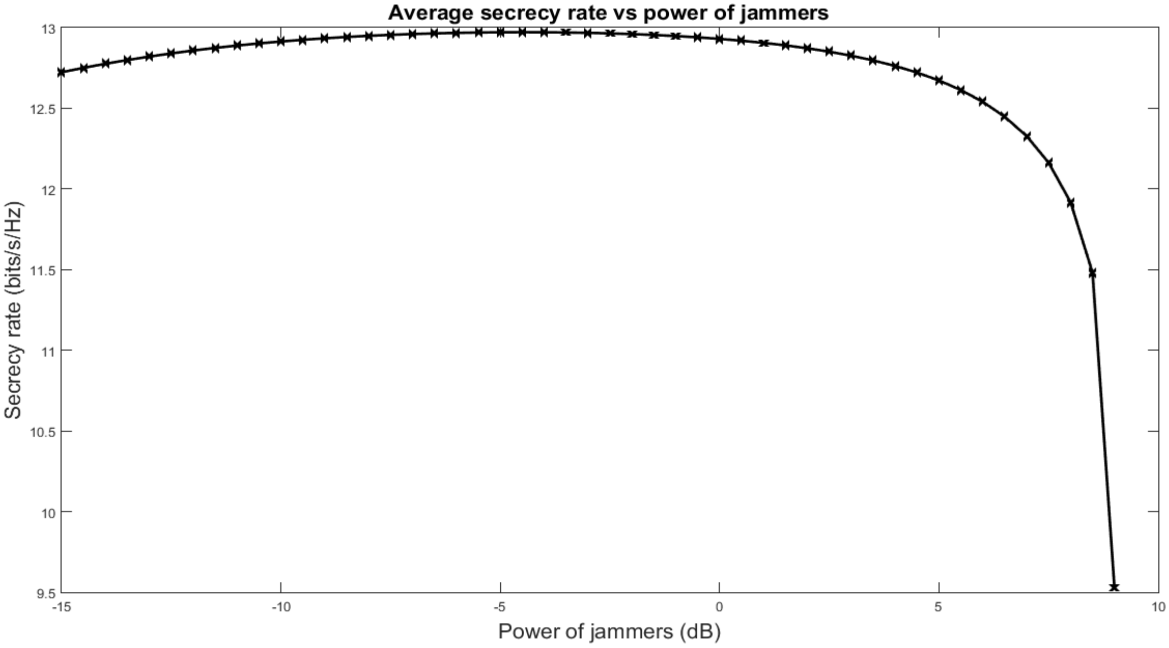

Figure 3.5: Secrecy rate versus power of jammers (final).

The first simulation result is shown in figure 3.5 above. The trend can be seen clearly that the secrecy rate rises gradually from approximate 12.7 to maximum around 13 at first. After reaching the top, it falls very fast and suddenly reach bottom at 9.5 when power of jammers at about 9 dBm. The movement of the line can be explained that when increase the jammers' power, the jamming signal helps strengthen the transmission channel. Nevertheless, when the jammers' power rises too high, the jammers drains all the power for the source and relays so the transmission is interrupted and the secrecy rate decreases dramatically.

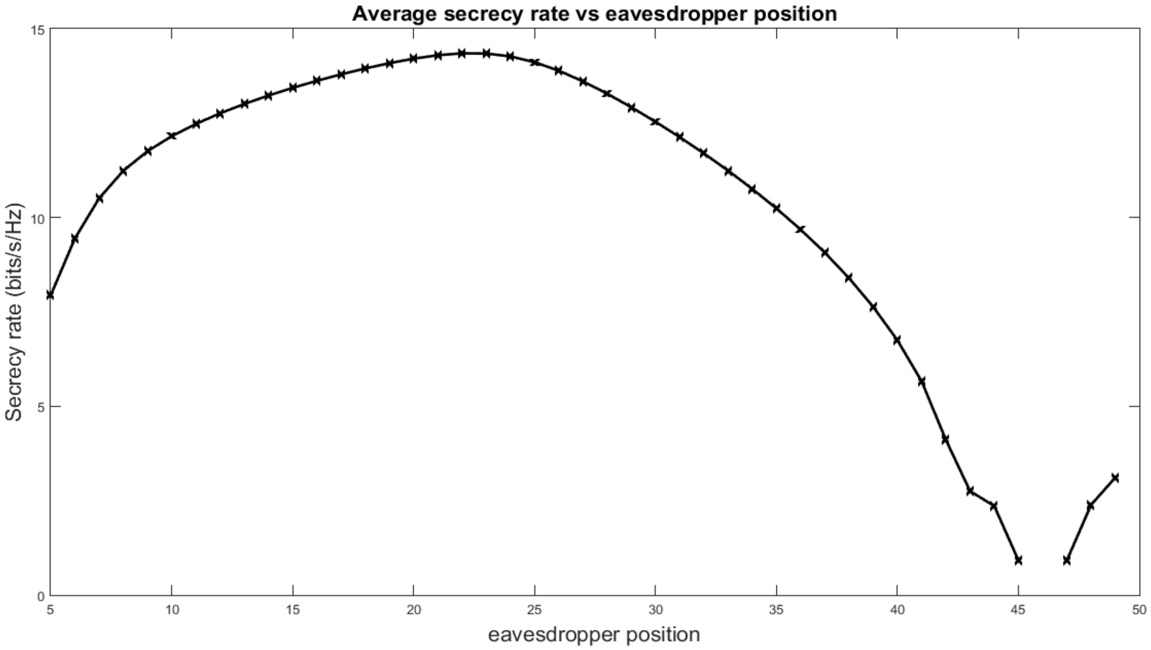

Figure 3.6 Secrecy rate versus eavesdropper's position (final).

The second simulation shown in figure 3.6 gives us not only an overview of the relationship between eavesdropper's position and secrecy rate but also the relationship between eavesdropper's position, selected relays' position and jammers' position. As noted from first simulation, the position of selected relays are (3; 0) and (46; 0), the position of jammers are (20; 0), (32; 0), (37; 0). The secrecy rate increase fast when the eavesdropper is in the range of two first jammers combined with first relay from 5 to around 25. After that, although there is another jammer at (37; 0), it is too far from two selected relays which make the secrecy rate decrease because there are no relay around. When the eavesdropper passes the second relay at (46; 0), the secrecy rate increase a bit but not so much because there are no jammer in range to support it. If we compare the simulation result with the result in the paper when eavesdropper is in range from 5 to 30 only, we can see the similarity in trend of two lines.

3.2.3.3 Conclusions

Even though the simulation still has some problems when running, there are good results as expected as the paper results and can be considered to apply in real project. Comparing to the best secrecy rate outcome in energy harvesting and jamming case which just reaches over 7 and lower than 8, the outcome of this beamforming, jamming and multiple relays, jammers selection combination technique is far more superior when it can go up to nearly 15 (in the second simulation) or nearly 13 (in the first simulation). Therefore, this combination scheme is the one I will choose to develop more in future due to its dominating performance in increasing secrecy rate compared to the other schemes.

3.3 Beamforming and Jamming supporting from destination.

As mentioned in chapter 1, this 3.3 section is only a review of paper [10] which I studied but failed to simulate due to the requirement of using CVX add-on tool for MATLAB. This section can be seen as extra that is added to provide another beamforming and jamming using method.

3.3.1 System Model.

The author calls the scheme in this paper as “Destination assisted jamming and beamforming” (DAJB) which takes advantage of all relays nodes to transfer the signal by making use of destination node as a jammer. This scheme also has assumption that there is no direct channel between source and destination, and all the relay nodes work in half-duplex mode.

Figure 3.7 presents the system model of DAJB scheme. The model consists of one source, one eavesdropper, one destination and N relays. The source, relay and destination nodes are set up with only single antenna. Every channels in this system are the quasi-stationary flat-fading channel. The notations link to arrows in the figure presenting the channel coefficients between two nodes at the two ends of the arrow. The figure also shows that the operation of the system has two phase. In phase I, the source broadcasts signal to relays and also eavesdropper. At the same time, the destination node acting as jammer casts jamming signal to confuse the eavesdropper. In phase II, the relay nodes amplify the received signal and forwards it to the destination (and the eavesdropper receives a copy of transmitted signal too) using distributed beamforming technique.

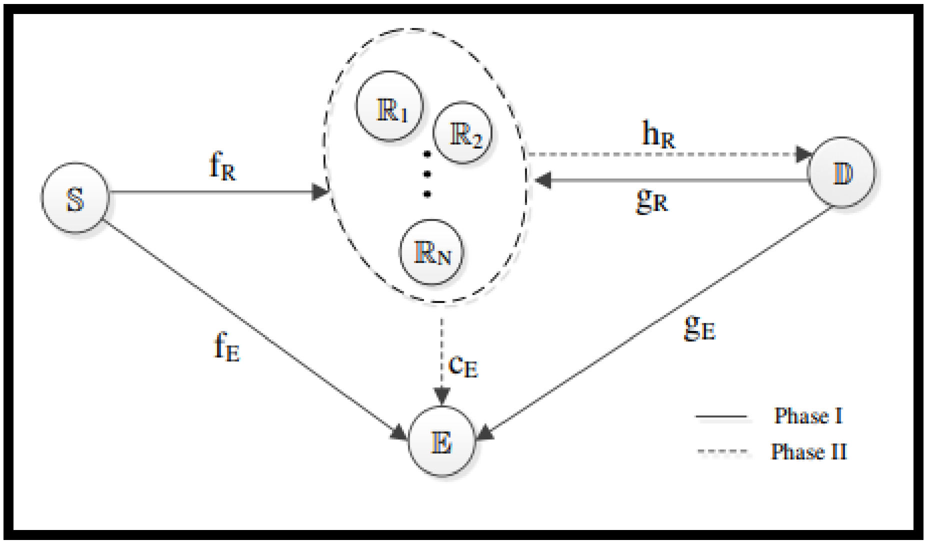

Figure 3.7: System model of DAJB (extra).

3.3.2 Analytical Results.

The received signals in phase I at relays and eavesdropper are given respectively as:

$$\mathbf{y}_R = \sqrt{P_S}\mathbf{f}_R s + \sqrt{P_J}\mathbf{g}_R z + \mathbf{n}_R, \tag{123}$$

$$y_E^{(1)} = \sqrt{P_S}\, f_E s + \sqrt{P_J}\, g_E z + n_E^{(1)}, \tag{124}$$

where P_S and P_J are the power constraint of the source and the jammer (or destination), respectively. s is the transmitted signal, z is jamming signal which is complex Gaussian random variable. $\mathbf{n}_R$ and $n_E^{(1)}$ are noises at relays and eavesdropper, respectively, which are time-spatially white independent complex Gaussian random variables with zero mean and variance σ^2.

During phase II, to limit the eavesdropper overhearing the forward signal, all N relay nodes attach artificial noise to signal $\mathbf{y}_R$ when transmitting it to the destination. The signal relay nodes transmit is formulated as:

$$\mathbf{x}_R = \mathbf{W}\mathbf{y}_R + \mathbf{n}_a, \tag{125}$$

where $\mathbf{x}_R = \left[x_{R,1},...,x_{R,\mathrm{N}} \right]^T$, $\mathbf{W} = diag\left(\left[w_1^*,...,w_N^* \right]\right)$ is the beamforming matrix, $\mathbf{n}_a$ is the artificial noises vector.

The received signals at destination and eavesdropper in phase II, respectively, are expressed as:

$$y_D = \sqrt{P_S}\mathbf{h}_R^T\mathbf{W}\mathbf{f}_R s + \sqrt{P_J}\mathbf{h}_R^T\mathbf{W}\mathbf{g}_R z + \mathbf{h}_R^T\mathbf{n}_a + \bar{\mathbf{n}}_D, \tag{126}$$

$$y_E^{(2)} = \sqrt{P_S}\mathbf{c}_E^T\mathbf{W}\mathbf{f}_R s + \sqrt{P_J}\mathbf{c}_E^T\mathbf{W}\mathbf{g}_R z + \mathbf{c}_E^T\mathbf{n}_a + \bar{\mathbf{n}}_E. \tag{127}$$

where $\bar{\mathbf{n}}_D = \mathbf{h}_R^T\mathbf{W}\mathbf{n}_R + n_D$, $\bar{\mathbf{n}}_E = \mathbf{c}_E^T\mathbf{W}\mathbf{n}_R + n_E^{(2)}$, $\mathbf{c}_E = \left[c_{E,1},...,c_{E,\mathrm{N}} \right]^T$, n_D and $n_E^{(2)}$ are the time-spatially white independent complex Gaussian random variables with zero mean and variance σ^2 at the destination and the eavesdropper, respectively.

Although formula (126) contains artificial noises attached by relays, the destination can eliminate it since they are ally so the new formula for received signal at destination can be expressed as:

$$y_D = \sqrt{P_S}\mathbf{w}^\dagger\mathbf{p}_{fh}s + \sqrt{P_J}\mathbf{w}^\dagger\mathbf{p}_{gh}z + \bar{\mathbf{n}}_D, \tag{128}$$

where $\mathbf{p}_{fh} = \left[f_{R,1}h_{R,1},..., f_{R,\mathrm{N}}h_{R,\mathrm{N}} \right]^T$, $\mathbf{p}_{gh} = \left[g_{R,1}h_{R,1},..., g_{R,\mathrm{N}}h_{R,\mathrm{N}} \right]^T$, $\mathbf{w} = \left[w_1,...,w_N \right]^T$.

On the other hand, the eavesdropper received signal can be combined from (124) and (127) to give an expression as:

$$\mathbf{y}_E = \begin{pmatrix} \sqrt{P_S}\, f_E \\ \sqrt{P_S}\mathbf{w}^\dagger\mathbf{p}_{fc} \end{pmatrix} s + \begin{pmatrix} \sqrt{P_J}\mathbf{g}_E z + n_E^{(1)} \\ \sqrt{P_J}\mathbf{w}^\dagger\mathbf{p}_{gc}z + \mathbf{c}_E^T\mathbf{n}_a + \bar{\mathbf{n}}_E \end{pmatrix}, \tag{129}$$

where $\mathbf{p}_{fc} = \left[f_{R,1}c_{\mathrm{E},1},..., f_{R,\mathrm{N}}c_{E,\mathrm{N}} \right]^T$, $\mathbf{p}_{gc} = \left[g_{R,1}c_{\mathrm{E},1},..., g_{R,\mathrm{N}}c_{E,\mathrm{N}} \right]^T$.

Before going further, we need to define some terms: $\mathbf{R}_{fh} = \mathbf{p}_{fh}\mathbf{p}_{fh}^\dagger$, $\mathbf{R}_{gh} = \mathbf{p}_{gh}\mathbf{p}_{gh}^\dagger$, $\mathbf{R}_{fc} = \mathbf{p}_{fc}\mathbf{p}_{fc}^\dagger$, $\mathbf{R}_{gc} = \mathbf{p}_{gc}\mathbf{p}_{gc}^\dagger$, $\mathbf{R}_{hh} = diag\left(\left|h_{R,1}\right|^2,...,\left|h_{R,\mathrm{N}}\right|^2\right)$, $\mathbf{R}_{cc} = diag\left(\left|c_{E,1}\right|^2,...,\left|c_{\mathrm{E},\mathrm{N}}\right|^2\right)$,

$\mathbf{\Lambda} = diag\left(\sigma^2_{z_a,1}, ..., \sigma^2_{z_a,\mathrm{N}-1}\right)$ where $\sigma^2_{z_a}$ is variance of vector $\mathbf{z}_a$ which consists of independent identically distributed (i.i.d) Gaussian variables and be defined by $\mathbf{n}_a = \mathbf{T}\mathbf{z}_a$ with $\mathbf{T}$ is the projection matrix.

The destination node's SNR formula is deduced as:

$$\gamma_D = \frac{P_S \mathbf{w}^\dagger \mathbf{R}_{fh} \mathbf{w}}{\sigma^2 \left(1 + \mathbf{w}^\dagger \mathbf{R}_{hh} \mathbf{w}\right) + P_J \mathbf{w}^\dagger \mathbf{R}_{gh} \mathbf{w}}, \tag{130}$$

The eavesdropper's SNR formulas in phase I and phase II is deduced as:

$$\gamma_E^{(1)} = \frac{P_S \left| f_E \right|^2}{P_J \left| g_E \right|^2 + \sigma^2}, \tag{131}$$

$$\gamma_E^{(2)} = \frac{P_S \mathbf{w}^\dagger \mathbf{R}_{fc} \mathbf{w}}{\sigma^2 + \mathbf{w}^\dagger \left(P_J \mathbf{R}_{gc} + \sigma^2 \mathbf{R}_{cc}\right) \mathbf{w} + \mathbf{c}_E^\dagger \mathbf{U} \mathbf{\Lambda} \mathbf{U}^\dagger \mathbf{c}_E}, \tag{132}$$

where $\mathbf{U}$ is a unitary matrix.

The objective of DAJB scheme is to maximum secrecy rate by finding optimal beamforming vector $\mathbf{w}$ and optimal jammer power P_J while fixing source power P_S. The formula to calculate secrecy rate is the same as in other section:

$$R_S = \max\left(R_D - R_E, 0\right). \tag{133}$$

In order to maximize R_S, we should find a way to increase R_D as large as possible and decrease R_E as small as possible. Because the relays and destination don't need the jamming signal broadcasted by destination node in phase I, we can assume $\mathbf{w}^\dagger \mathbf{p}_{gh} = 0$ which helps increase R_D and simplify the formula of SNR at destination to be:

$$\gamma_D = \frac{P_S \mathbf{w}^\dagger \mathbf{R}_{fh} \mathbf{w}}{\sigma^2 \left(1 + \mathbf{w}^\dagger \mathbf{R}_{hh} \mathbf{w}\right)}, \tag{134}$$

which lead the formula for secrecy rate at destination as:

$$R_D = \log_2\left(1+\frac{P_S\mathbf{w}^\dagger\mathbf{R}_{fh}\mathbf{w}}{\sigma^2\left(1+\mathbf{w}^\dagger\mathbf{R}_{hh}\mathbf{w}\right)}\right) \tag{135}$$

In two phases, the total power used by N relays is $P_R = P_{ST} + P_{AN}$. P_{ST} is power for signal transmission, defined as: $P_{ST} = \mathbf{w}^\dagger\mathbf{Q}\mathbf{w}$, with $\mathbf{Q} = P_S\mathbf{R}_{ff} + P_J\mathbf{R}_{gg} + \sigma^2\mathbf{I}_N$, where $\mathbf{R}_{ff} = diag\left(\left|f_{R,1}\right|^2,...,\left|f_{R,\mathrm{N}}\right|^2\right)$, $\mathbf{R}_{gg} = diag\left(\left|g_{R,1}\right|^2,...,\left|g_{R,\mathrm{N}}\right|^2\right)$. $P_{AN} = E\left\{\mathbf{n}_a^\dagger\mathbf{n}_a\right\}$ is power for artificial noise attached with forwarding signal by relays. Within the power constraint of P_R, the power P_{ST} should be lower to minimum so that P_{AN} can be maximized to produce stronger artificial noise to confuse eavesdropper. Therefore, we have a mathematically optimization problem below:

$$\begin{array}{ll} \min & P_{ST} \\ s.t. & \gamma_D \geq \varsigma, \\ & E\left\{\left|x_{(R,i)}\right|^2\right\} \leq \overline{P}_{Ri},\ i=1,2,...,N, \end{array} \Leftrightarrow \begin{array}{ll} \min\limits_{\mathbf{w}} & \mathbf{w}^\dagger\mathbf{Q}\mathbf{w} \\ s.t. & \dfrac{P_S\mathbf{w}^\dagger\mathbf{R}_{fh}\mathbf{w}}{\sigma^2\left(1+\mathbf{w}^\dagger\mathbf{R}_{hh}\mathbf{w}\right)} \geq \varsigma, \\ & \left[\mathbf{w}\mathbf{w}^\dagger\right]_{(i,i)}\left[\mathbf{Q}\right]_{(i,i)} \leq \overline{P}_{Ri},\ i=1,2,...,N, \end{array} \tag{136}$$

where ς is the received SNR threshold of γ_D which depends on quality of service (QoS) requirement.

Define $\mathbf{G}$ is the projection matrix onto null space of $\mathbf{p}_{gh}$ which satisfies $\mathbf{w} = \mathbf{G}\mathbf{v}$. Substituting $\mathbf{w} = \mathbf{G}\mathbf{v}$ into above problem give us:

$$\begin{array}{ll} \min\limits_{\mathbf{v}} & \mathbf{v}^\dagger\overline{\mathbf{Q}}\mathbf{v} \\ s.t. & \mathbf{v}^\dagger\overline{\mathbf{R}}_{fh}\mathbf{v} \geq \dfrac{\sigma^2\varsigma}{P_S}\left(1+\mathbf{v}^\dagger\overline{\mathbf{R}}_{hh}\mathbf{v}\right), \\ & \left[\mathbf{G}\mathbf{v}\mathbf{v}^\dagger\mathbf{G}^\dagger\right]_{(i,i)} \leq \dfrac{\overline{P}_{Ri}}{\left[\mathbf{Q}\right]_{(i,i)}},\ i=1,2,...,N, \end{array} \tag{137}$$

where $\overline{\mathbf{Q}} = \mathbf{G}^{\dagger}\mathbf{Q}\mathbf{G}$, $\overline{\mathbf{R}}_{fh} = \mathbf{G}^{\dagger}\mathbf{R}_{fh}\mathbf{G}$, $\overline{\mathbf{R}}_{hh} = \mathbf{G}^{\dagger}\mathbf{R}_{hh}\mathbf{G}$.

From definition, $\mathbf{Q}$ is a diagonal matrix with positive components so we can let denote the element-wise square root of $\mathbf{Q}$ as $\sqrt{\mathbf{Q}}$ and the optimization problem becomes:

$$\begin{aligned} \min_{\mathbf{v}} \quad & \left\|\sqrt{\mathbf{Q}}\mathbf{G}\mathbf{v}\right\|^{2} \\ s.t. \quad & \left\|\begin{matrix}\sqrt{\mathbf{R}_{hh}}\mathbf{G}\mathbf{v} \\ 1\end{matrix}\right\|^{2} \leq \frac{P_S}{\sigma^2\varsigma}\left\|\mathbf{v}^{\dagger}\mathbf{G}^{\dagger}\mathbf{p}_{fh}\right\|^{2}, \\ & \left|\mathbf{G}^{(i)}\mathbf{v}\right| \leq \sqrt{\frac{\overline{P}_{Ri}}{[\mathbf{Q}]_{(i,i)}}},\ i = 1, 2, ..., N. \end{aligned} \tag{138}$$

There are some new definitions we need to know:

$$\begin{aligned} &\mathbf{Q} = diag\left(\sqrt{\mathbf{Q}}\mathbf{G}, 0, 0\right), \\ &\mathbf{R}_{hh} = diag\left(\sqrt{\mathbf{R}_{hh}}\mathbf{G}, 0, 1\right), \\ &\mathbf{v} = \left[\mathbf{v}^{T}, q, 1\right]^{T}, \\ &\mathbf{p}_{fh}^{\dagger} = \left[\mathbf{G}^{\dagger}\mathbf{p}_{fh}, 0, 0\right], \\ &\mathbf{G}^{(i)} = \left[\mathbf{G}^{(i)}, 0, 0\right]. \end{aligned}$$

From new definitions, we can reformed formula (138) as:

$$\begin{aligned} \min_{\mathbf{v}} \quad & q \\ s.t. \quad & \left\|\mathbf{Q}\mathbf{v}\right\| \leq q, \\ & \left\|\mathbf{R}_{hh}\tilde{v}\right\|^{2} \leq \sqrt{\frac{P_S}{\sigma^2\varsigma}}\mathbf{p}_{fh}^{\dagger}\mathbf{v}, \\ & \left|\mathbf{G}^{(i)}\mathbf{v}\right| \leq \sqrt{\frac{\overline{P}_{Ri}}{[\mathbf{Q}]_{(i,i)}}},\ i = 1, 2, ..., N, \\ & \left[\mathbf{v}\right]_{(N+2)} = 1. \end{aligned} \tag{139}$$

The problem (139) is a second-order convex cone programming (SOCP) with linear equation constraints which can be solved by running CVX tool on MATLAB to find the optimal $\mathbf{v}^o$ and then, the optimal $\mathbf{w}^o$ with formula $\mathbf{w}^o = \mathbf{G}\mathbf{v}^o$. After that, we can find $P_{STi} = \left[\mathbf{w}^o \mathbf{w}^{o\dagger}\right]_{(i,i)} [\mathbf{Q}]_{(i,i)}$ and $P_{ANi} = \overline{P}_{Ri} - P_{STi}$. However, we have another optimization problem besides finding optimal $\mathbf{w}^o$ as mentioned above which is finding the optimization of P_{AN}. Since $P_{AN} = E\left\{\mathbf{n}_a^\dagger \mathbf{n}_a\right\} = \sum_{j=1}^{N-1} \sigma_{(z_a,j)}^2$, the new optimization problem can be expressed as:

$$\begin{aligned} &\max_{\sigma_{(z_a,j)}^2} \quad \sum_{j=1}^{N-1} \sigma_{(z_a,j)}^2 \\ &s.t. \quad E\left\{\left|[\mathbf{n}_a]_{(i,1)}\right|^2\right\} \le P_{Ai}, \quad i = 1,2,...,N, \end{aligned} \tag{140}$$

where $[\mathbf{n}_a]_{(i,1)} = \mathbf{T}^{(i)} \mathbf{z}_a = \sum_{j=1}^{N-1} t_{(i,j)} z_{a_j}$, Because z_{a_j} is independent identically distributed, we have $E\left\{\left|[\mathbf{n}_a]_{(i,1)}\right|^2\right\} = \sum_{j=1}^{N-1} \left|t_{(i,j)}\right|^2 \sigma_{(z_a,j)}^2$.

Reformulating (140) provides us the problem:

$$\begin{aligned} &\max_{\sigma_{(z_a,j)}^2} \quad \mathbf{1}^T \boldsymbol{\sigma} \\ &s.t. \quad \mathbf{T}\boldsymbol{\sigma} \le \mathbf{b}_{AN}, \\ &\qquad [\boldsymbol{\sigma}]_{(i,1)} \ge 0, \end{aligned} \tag{141}$$

Where $\mathbf{T}$ is a $N \times (N-1)$ matrix, $\mathbf{1} = [1,1,...,1]^T$, $\mathbf{b}_{AN}$, $\overline{\mathbf{b}}_{RN}$, $\mathbf{b}_{ST}$ are $N \times 1$ vector with the components are i-th element of P_{Ai}, $\overline{P}_{Ri}$, and P_{STi}, respectively. $\boldsymbol{\sigma} = \left[\sigma_{(z_a,1)}^2, ..., \sigma_{(z_a,\mathrm{N}-1)}^2\right]^T$, $\mathbf{b}_{AN} = \overline{\mathbf{b}}_{RN} - \mathbf{b}_{ST}$, $\left[\mathbf{T}\right]_{(i,j)} = \left|t_{(i,j)}\right|^2$.

Problem (141) is a linear programming (LP) problem which can also be solve by CVX tool in MATLAB and the result will provide us the optimal $\boldsymbol{\sigma}^o$. With both $\boldsymbol{\sigma}^o$ and $\mathbf{w}^o$, substituting them into SNR formula at destination and eavesdropper (130), (131), (132) and we can solve the secrecy rate with (133) and these two formulas below:

$$R_D = \frac{1}{2}\log_2\left(1+\gamma_D\right), \tag{142}$$

$$R_E = \frac{1}{2}\log_2\left(1+\gamma_E\right). \tag{143}$$

Chapter 4: Conclusion & Future works

I am quite satisfied with the result from the combination of jamming and beamforming scheme (section 3.2) and also from the combination of energy harvesting and jamming (section 2.3). These two combination schemes can be applied on different projects depending on the requirements and constraints. For example, if the project needs minimizing the power usage and the scale of system is not so large (short distance, small amount of nodes and small amount of power required), energy harvesting is a good choice. If the scale of project is big, beamforming is very useful since it helps focus the signal and transmit it further in a stable way. Even if the projects require both characteristics above, combination of all best techniques in this report is not a bad choice. Although the results in this report comes from computer programming tests, I believe with further developments these schemes are not only theoretical but also applicable for real life project.

If I continue to work in the field of physical layer security, I will find a way to solve the errors in my simulations and improve the systems in the scale of real life projects. For example, I can study and solve the problem in more difficult models like in a three-dimension with random position of many eavesdroppers or an effective way to interfere the transmission with small amount of power required. Moreover, the distance of real life projects can be as large as a size of city, a nation, or even the size of the Earth. Therefore, an effective way to use power and minimize the number of relay stations is necessary to be considered. In addition, as I mentioned above, the number of combination techniques is not just two or three so I would like to study and find out a better scheme which can combines all the best techniques and make the main channel absolutely dominate the wiretap channel.

References

[1] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving Wireless Physical Layer Security via Cooperating Relays,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[2] I. Krikidis, J. S. Thompson, and S. Mclaughlin, “Relay selection for secure cooperative networks with jamming,” *IEEE Trans. Wirel. Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[3] R. Sinha and P. Jindal, “A study of physical layer security with energy harvesting in single hop relaying environment,” in *2017 4th International Conference on Signal Processing and Integrated Networks (SPIN)*, 2017, pp. 530–533.

[4] Y. Zou, X. Wang, and W. Shen, “Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[5] H. M. Wang, F. Liu, and M. Yang, “Joint Cooperative Beamforming, Jamming, and Power Allocation to Secure AF Relay Systems,” *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4893–4898, Oct. 2015.

[6] M. Hatami, M. Jahandideh, and H. Behroozi, “Two-phase cooperative jamming and beamforming for physical layer secrecy,” in *2015 23rd Iranian Conference on Electrical Engineering*, 2015, pp. 456–461.

[7] D. J. Costello, “Fundamentals of Wireless Communication (Tse, D. and Viswanath, P.) [Book review],” *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 919–920, Feb. 2009.

[8] Lizhong Zheng and D. N. C. Tse, “Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels,” *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[9] C. D. Meyer, *Matrix analysis and applied linear algebra*, vol. 71. Siam, 2000.

[10] N. Ouyang, X. Q. Jiang, E. Bai, and H. M. Wang, “Destination Assisted Jamming and Beamforming for Improving the Security of AF Relay Systems,” *IEEE Access*, vol. 5, pp. 4125–4131, 2017.