ADVERSARY ANALYSIS OF COCKROACH NETWORK UNDER RAYLEIGH FADING CHANNEL: PROBABILITY OF ERROR AND ADVERSARY DETECTION

A Dissertation by

Tze Chien Wong

Master of Science, Wichita State University, 2008

Bachelor of Science, Wichita State University, 2005

Submitted to the Department of Electrical Engineering and Computer Science
and the faculty of the Graduate School of
Wichita State University
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

May 2015

ADVERSARY ANALYSIS OF COCKROACH NETWORK UNDER RAYLEIGH FADING CHANNEL: PROBABILITY OF ERROR AND ADVERSARY DETECTION

The following faculty members have examined the final copy of this dissertation for form and content, and recommend that it be accepted in partial fulfillment of the requirement for the degree of Doctor of Philosophy with a major in Electrical Engineering.

_____
Hyuck M. Kwon, Committee Chair

_____
John M. Watkins, Committee Member

_____
Mahmoud E. Sawan, Committee Member

_____
John S. Tomblin, Committee Member

_____
Xiaomi Hu, Committee Member

Accepted for the College of Engineering

_____
Royce Bowden, Dean

Accepted for the Graduate School

_____
Abu S.M. Masud, Interim Dean

DEDICATION

To my family and friends

Limits are meant to be broken,
boundaries are meant to be pushed.

ACKNOWLEDGMENTS

I would like to thank my adviser, Dr. Kwon, for his many years of thoughtful, patient guidance and support. I would also like to extend my gratitude to members of my committee—Dr. Watkins, Dr. Sawan, Dr. Tomblin, and Dr. Hu—for their helpful comments and suggestions on all stages of this dissertation.

This work was supported in part by the U.S. Air Force Summer Faculty Fellowship Program (USAF-SFFP), the Air Force Research Laboratory (AFRL) under Grant FA9453-15-1-0308, and the Asian Office of Aerospace R&D (AOARD) under Grant FA2386-14-1-0026. The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the AFRL or the U.S. government.

ABSTRACT

This paper extends the design of a cockroach network from a wire network, without considering thermal noise and channel fading, into a wireless Rayleigh fading channel. This research is developed and split into two directions: probability of error for data transmission and probability of detection for adversary node.

A lookup table is proposed in order to speed up the process of data decoding and also to identify the node that has the highest probability of behaving as an adversary. This table is a summary of all combination data received at the destination so that a decision can be made logically.

In the section relative to probability of error, the analysis begins with deriving the equation of probability of error between the source, nodes, and destination. Then, by taking the approximation, the probability of each data combination at the destination is determined. With the aid of the lookup table, the probability of error can be obtained by summing the combination causing the error. Similar to the probability of error, the probability of detection is also determined with the assistance of the lookup table by using a combination of signals received at the destination. By summing up the probability of this combination, the probability of detection and false alarms can be obtained, with and without the existence of an adversary.

In the end, the simulation result is compared to the derived equation of probability of error and detection. Both analysis and simulation results show that the probability of error achieves 10^{-2}, when the signal-to-noise ratio (SNR) is about 15 dB under the condition of no adversary and when the SNR is in the range of 19 to 24 dB when one of the nodes is compromised. On the other hand, the probability of false alarm is reduced significantly when the SNR is higher than 20 dB, and the rate of successful adversary detection is about 95% at 20 dB.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPSK	Binary Phase-shift Keying
MPSK	M-Ary Phase-shift Keying
OFDM	Orthogonal Frequency-Division Multiplexing
PSK	Phase-shift Keying
ROC	Receiver Operation Characteristic
QPSK	Quadrature Phase-shift Keying
SNR	Signal-to-Noise Ratio
TPSK	Ternary Phase-shift Keying
WSN	Wireless Sensor Network

CHAPTER 1

INTRODUCTION

1.1 Motivation

Recently, the use of telecommunication has been increased enormously due to its convenience, not only for personal pleasure, business, and marketing purposes, but also for the special task of protecting people. Due to the long distance involved in telecommunication and limitations in the range of broadcasting, several hops (or relays) are required to forward a signal from the transmitter to the destination. Because these hops can be controlled by a third party other than the sender and receiver, the system will become vulnerable to adversary attack.

In a special scenario, an adversary node may pretend to be one of the cooperative nodes in the hop network and alter data intentionally during its transmission. In this case, two questions arise: Is the receiver able to recover the data? and Is the receiver capable of determining the location of the adversary node?

1.2 Literature Review

A number of network designs have been studied [1, 2]. Also, some algorithms have been developed to handle this scenario [3, 4]. These network designs are built into a system whereby the hops are connected by a landline cable or backbones with no noise or fading. Under this circumstance, the probability of error during data transmission could be neglected and high efficiency could be achieved in detecting the location of the adversary. Moreover, only channel capacity performance has typically been studied in the entire system. For example, Kosut et al. [1] assumed only one active adversary node in the cockroach network. They proposed a network layer design to detect the location of the adversary node out of five relay nodes.

Similar to this paper, other researchers [5, 6, 7, 8] have proposed several methods to identify the adversary and reduce data error. Focusing on large-scale wireless sensor networks (WSNs), Vempaty et al. [5] describe the attack and defense strategy for both sides; however, these schemes do not involve any transmission technology such as noise, fading, and modulation. The performance of this scheme was improved by using error control coding [6, 8]. Later on, non-ideal channels were suggested [7, 8] to further investigate performance.

Other work related to WSNs has been undertaken [9, 10, 11, 12]. In contrast, the strategy purposed by Zhang and Blum [9] and Zhang et al. [10] claimed to have a better chance of identifying and categorizing the attacked sensors. Liu et al. [11] introduced an adapter to estimate the channel so that sensors could adjust the quantization threshold itself. Relative to the attacking strategy, Nadendla et al. [12] discuss the weakness of the distributed inference sensor network and found an optimal attack strategy.

On the other hand, Byzantine attacks on a small network such as a two-way relay has been studied as well [13, 14]. Network coding was developed by He and Yener [13] in order to detect and reduce the effectiveness of the adversary attack, while Graves and Wong [14] claimed that the integrity of information is guaranteed with the random coding scheme.

Moreover, network capacity in the presence of an adversary has been discussed [15, 16, 17]. While examining network capacity, some researchers [15, 17] compare the difference of capacity between noiseless and noisy channels. Liang and Vaidya [16] maximized throughput using a specific network structure.

After reviewing the previous work of others, the cockroach network was chosen as a model to be modified into wireless capability in this paper. First, nodes in the cockroach network could be applied to any telecommunication devices, such as base stations and satellites. Also, the

cockroach network is designed for one source and one destination, and a limited number of nodes between the two; therefore, it has fewer management requirements. Moreover, the mobility of the wireless cockroach network is ideally applied in the battlefield. It could detect the presence of an adversary node almost instantly, in order to protect any application that requires high secrecy.

Therefore, this paper extends the previous cockroach network design by reconstructing the ideal wire network layer into a physical layer network. By introducing additive white Gaussian noise (AWGN) and Rayleigh fading, which serve as thermal noise and signal distortion, respectively, to make the transmission more realistic, the difficulty of data recovery and adversary detection will be increased as well.

1.3 Dissertation Organization

In Chapter 2, the original design of the cockroach network from the work of Kosut et al. [1] is demonstrated, including the strategy and logic to detect an adversary. Also, the memoryless modulation M-ary phase shift keying (MPSK) is also demonstrated, since it will be applied to the transmission of digital information. The remodeling of the cockroach network will also be introduced in this chapter.

Most of the probability of error analysis will be covered in Chapter 3. First the probability of error will be carefully examined in each node. Based on the probability of error at the destination, a lookup table is proposed, which could be utilized to speed up the process of information recovery and adversary detection. From this lookup table, the analysis of overall probability of error could be obtained.

The analysis moves to the probability of detection in Chapter 4. With the aid of the lookup table, the chance of adversary detection is obtained.

Simulation results of the probability of error and detection are discussed in Chapter 5. Also, the theoretical result for bit error rate (BER) and chance of detection are compared and discussed with simulation results.

In Chapter 6, the contribution of this paper is summarized, and future research is proposed and discussed.

CHAPTER 2

SYSTEM MODEL

2.1 Original Cockroach Network

A nonlinear code for the cockroach network, as shown in Figure 2.1, was initially proposed by Kosut et al. [1]. The objective of sender S is to transmit a message to destination D with the help of five relays, labeled R_1 to R_5. Kosut et al. [1] claimed that the capacity could reach 2 under a noiseless channel. The x_1 and x_2 can be any number.

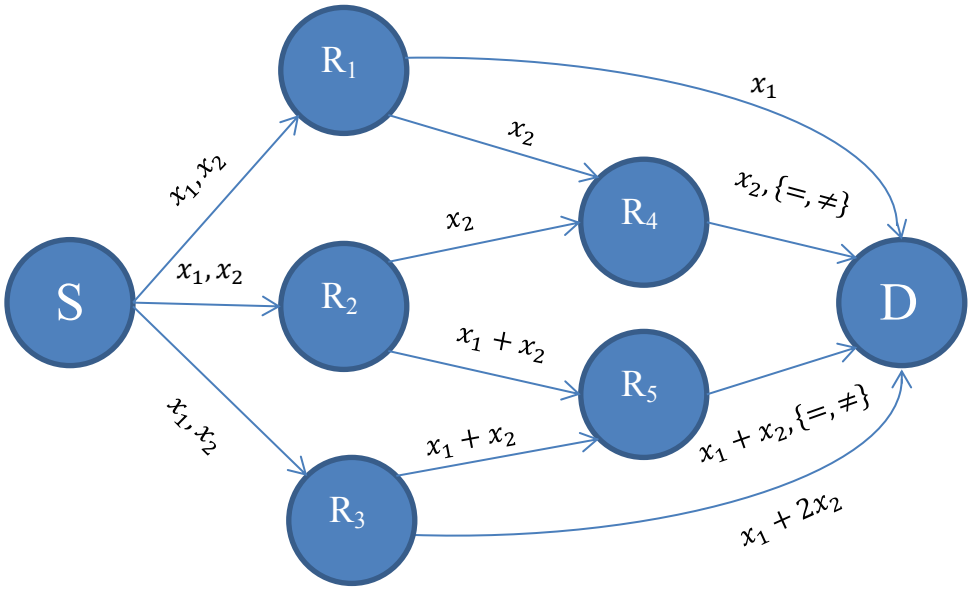


Figure 2.1: Nonlinear code for cockroach network [1].

First, sender S sends messages x_1 and x_2 to relays R_1, R_2, and R_3 at the same time. Next, R_1 forwards x_1 and x_2 to the destination and R_4, respectively. Similarly, R_2 forwards x_2 to R_4, as well as the sum of x_1 and x_2 to R_5. Again, R_3 sends the sum of x_1 and x_2 to R_5, but sends the sum of x_1 and $2x_2$ to the destination.

In contrast to the other relays, R_4 compares the x_2 messages from R_1 and R_2 and randomly chooses one of them to forward to the destination; it also sends an additional bit to indicate "="

or "≠". Similarly, R_5 also compares the $x_1 + x_2$ messages from R_2 and R_3, randomly chooses either one, with an additional bit for "=" or "≠," and forwards the message to the destination.

In a noiseless channel, no error will occur on x_1 and x_2. The destination performs the following strategy to decode the message and also identify the adversary node (which is, at most, one):

- If the destination receives "≠" and "=" from R_4 and R_5, respectively, then the adversary node could be either R_1 or R_4. Therefore, messages from R_3 and R_5 are trustworthy, and the original messages x_1 and x_2 could be retrieved from those relays. Next, the message x_1 from relay R_1 is compared. If the message is the same, then R_4 is the adversary; if not, then R_1 is the adversary.
- If the destination receives "=" and "≠" from R_4 and R_5, respectively, then R_3 and R_5 become the suspects. Original messages could be obtained from R_1 and R_2, and the adversary could be identified by comparing the message from R_3.
- If the destination receives "≠" from both R_4 and R_5, indicating R_2 is the adversary, then the information could be decoded from the messages from R_1 and R_3.
- If the destination receives "=" from both R_4 and R_5, then this means that no adversary is present in the system, and messages x_1 and x_2 could be obtained directly from relays R_1 and R_4, respectively.

2.2 M-Ary Phase-Shift Keying

For the digital information or data transmitted over a telecommunication channel, the modulator is required to map it into analog waveforms so that it can be transmitted through the channel [18, 19].

The M signal waveforms in digital phase modulation are represented as

$$s_m(t) = Re\left[g(t)e^{j2\pi(m-1)/M}e^{j2f_c t}\right], \quad m = 1,2,\dots M, \quad 0 \le t \le T$$

$$= g(t)cos\left[2\pi f_c t + \frac{2\pi}{M}(m-1)\right]$$

$$= g(t)cos\left[\frac{2\pi}{M}(m-1)\right]cos2\pi f_c t - g(t)sin\left[\frac{2\pi}{M}(m-1)\right]sin2\pi f_c t \quad (1)$$

where $g(t)$ is the signal pulse shape, and there are M different phases for the carrier to transmit the information. Therefore, this type of modulation is usually called phase-shift keying (PSK).

These M signal waveforms have equal energy:

$$\varepsilon = \int_0^T s_m^2(t)dt = \frac{1}{2}\int_0^T g^2(t)dt = \frac{1}{2}\varepsilon_g \quad (2)$$

where ε_g denotes the energy of $g(t)$. Moreover, they can be represented as a summation of two orthonormal signal waveforms, $f_1(t)$ and $f_2(t)$:

$$s_m(t) = s_{m1}f_1(t) + s_{m2}f_2(t) \quad (3)$$

where

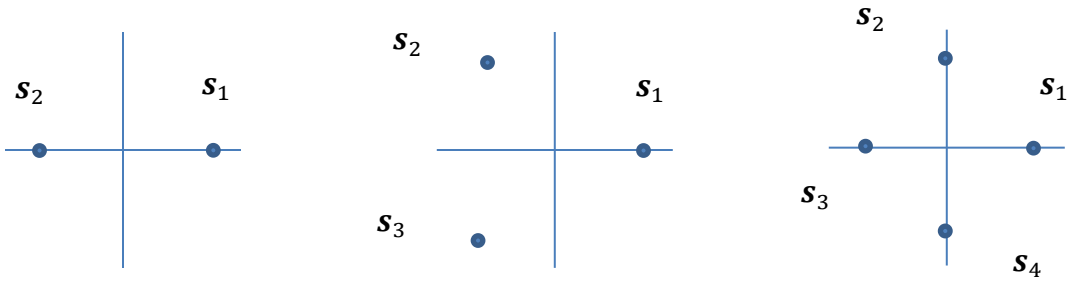
$$f_1(t) = \sqrt{\frac{2}{\varepsilon_g}}g(t)cos2\pi f_c t \quad (4)$$

$$f_2(t) = -\sqrt{\frac{2}{\varepsilon_g}}g(t)sin2\pi f_c t \quad (5)$$

and the two-dimensional coordinates of $\boldsymbol{s}_m = [s_{m1} \quad s_{m2}]$ are given by

$$\boldsymbol{s}_m = \left[\sqrt{\frac{\varepsilon_g}{2}}cos\frac{2\pi}{M}(m-1) \quad \sqrt{\frac{\varepsilon_g}{2}}sin\frac{2\pi}{M}(m-1)\right], \quad m = 1,2,\dots,M. \quad (6)$$

Signal space diagrams for M = 2, 3, and 4 are shown in Figure 2.2.



M = 2 (BPSK) M = 3 (TPSK) M = 4 (QPSK)

Figure 2.2: Signal space diagrams for PSK signals.

From Figure 2.2, the Euclidean distance between any two signal points is

$$d_{mn}^{(e)} = \|\boldsymbol{s}_m - \boldsymbol{s}_n\| = \left\{\varepsilon_g \left[1 - cos\frac{2\pi}{M}(m-n)\right]\right\}^{1/2}. \quad (7)$$

Also, the minimum Euclidean distance, which is the shortest distance between two symbols, is

$$d_{min}^{(e)} = \sqrt{\varepsilon_g \left(1 - \cos\frac{2\pi}{M}\right)}. \quad (8)$$

2.3 Wireless Cockroach Network

The wireless cockroach network system will be studied in this paper by introducing physical layer digital communications environments such as AWGN and Rayleigh fading. Also, the source, destination, and nodes have the capability to map the digital information with PSK modulation, and demodulate the received signal back to digital messages, as shown in Figure 2.3.

First, the sender S will broadcast signals x_1 and x_2 to relays R_1, R_2, and R_3 at the same time. Since the digital information x is either "–1" or "+1," there are four different combinations of x_1 and x_2, and quadrature phase-shift keying (QPSK) could be applied as modulation. Next, R_1 needs to demodulate the received signal to retrieve $\hat{x}_1$ and $\hat{x}_2$ and then forwards $\hat{x}_1$ only to destination D by using binary phase-shift keying (BPSK) modulation. Note that $\hat{x}_i$ could be different from the original x_i because of thermal noise and fading in the channel.

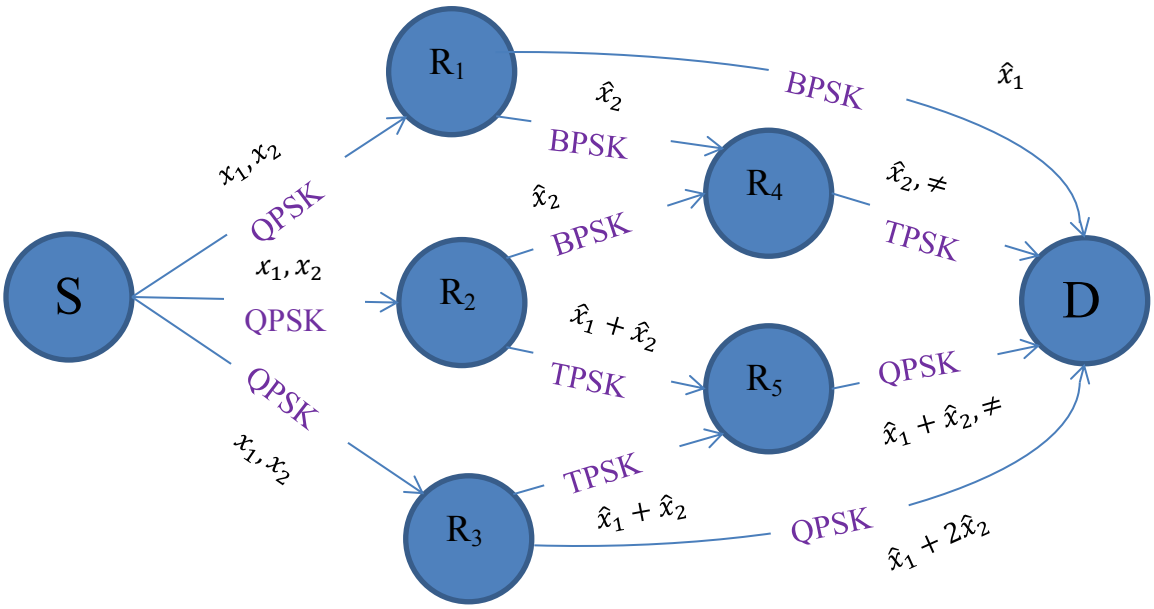


Figure 2.3: Proposed wireless cockroach network.

Similar to the previous signal x_1, R_1 and R_2 forward the x_2 information separately to R_4. At this point, R_4 will demodulate and compare the two signals from R_1 and R_2, and either forward $\hat{x}_2$, if the two pieces of information are the same, or issue the "≠" signal to D, if they are different. In contrast to the original cockroach network, relay R4 does not send the "=" symbol to D. Since the transmission from R_4 to D requires three different symbols, ternary phase-shift keying (TPSK) would be the best choice of modulation.

Next, R_2 and R_3 also decode $\hat{x}_1$ and $\hat{x}_2$, and forward the result of $\hat{x}_1 + \hat{x}_2$ as the symbol to R_5. Since the result of $\hat{x}_1 + \hat{x}_2$ could be either "–2," "0," or "+2," TPSK could be applied to this transmission. Again, R_5 will compare the received signal from R_2 and R_3, and either forward $\hat{x}_1 + \hat{x}_2$ or "≠" to D through QPSK modulation. Finally, R_3 follows a similar procedure described above, sending the result of $\hat{x}_1 + 2\hat{x}_2$ mapped into the QPSK signal to D.

At the destination, D decodes the information and identifies the adversary node based on the received signals from R_1, R_3, R_4, and R_5. If the signals are transmitted through a noiseless channel, then the combination of decoded signals at D can be summarized, as shown in Table 2.1.

TABLE 2.1

LOOKUP TABLE FOR BIT DECISION AND ADVERSARY DETECTION UNDER NOISELESS CHANNEL

	$\hat{x}_1 = -1 \quad \hat{x}_2 = -1$	$\hat{x}_1 = -1 \quad \hat{x}_2 = +1$	$\hat{x}_1 = +1 \quad \hat{x}_2 = -1$	$\hat{x}_1 = +1 \quad \hat{x}_2 = +1$
NA	-1 -1 -2 -3	-1 $+1$ 0 $+1$	$+1$ -1 0 -1	$+1$ $+1$ $+2$ $+3$
R_1	$+1$ $\neq$ -2 -3	$+1$ $\neq$ 0 $+1$	-1 $\neq$ 0 -1	-1 $\neq$ $+2$ $+3$
R_2	-1 $\neq$ $\neq$ -3	-1 $\neq$ $\neq$ $+1$	$+1$ $\neq$ $\neq$ -1	$+1$ $\neq$ $\neq$ $+3$
R_3	$-1 \quad -1$ $-1 \quad -1$ $\neq \quad \neq$ $+3 \quad -1$	$-1 \quad -1$ $+1 \quad +1$ $\neq \quad \neq$ $-1 \quad +3$	$+1 \quad +1$ $-1 \quad -1$ $\neq \quad \neq$ $-3 \quad +1$	$+1 \quad +1$ $+1 \quad +1$ $\neq \quad \neq$ $-3 \quad +1$
R_4	$-1 \quad -1$ $+1 \quad \neq$ $-2 \quad -2$ $-3 \quad -3$	$-1 \quad -1$ $-1 \quad \neq$ $0 \quad 0$ $+1 \quad +1$	$+1 \quad +1$ $+1 \quad \neq$ $0 \quad 0$ $-1 \quad -1$	$+1 \quad +1$ $-1 \quad \neq$ $+2 \quad +2$ $+3 \quad +3$
R_5	$-1 \quad -1 \quad -1$ $-1 \quad -1 \quad -1$ $0 \quad +2 \quad \neq$ $-3 \quad -3 \quad -3$	$-1 \quad -1 \quad -1$ $+1 \quad +1 \quad +1$ $-2 \quad +2 \quad \neq$ $+1 \quad +1 \quad +1$	$+1 \quad +1 \quad +1$ $-1 \quad -1 \quad -1$ $-2 \quad +2 \quad \neq$ $-1 \quad -1 \quad -1$	$+1 \quad +1 \quad +1$ $+1 \quad +1 \quad +1$ $0 \quad \neq \quad -2$ $+3 \quad +3 \quad +3$

Table 2.1 could be used to decode signals x_1 and x_2, as well as detect the adversary node instantly, according to the received signal from the relay nodes. Each column vector of four components in the Table 2.1 represents the received vector at the destination from R_1, R_3, R_4, and R_5, respectively. For example, the destination where $\begin{pmatrix} D_1 \\ D_2 \\ D_3 \\ D_4 \end{pmatrix} = \begin{pmatrix} +1 \\ \neq \\ 0 \\ +1 \end{pmatrix}$ decodes the received signals into $(\hat{x}_1 = -1 \quad \hat{x}_2 = +1)$ and also indicates R_1 as the adversary node.

However, under a noisy channel, such as AWGN and Rayleigh fading, Table 2.1 should contain more combinations of received vectors because of the decoding error due to noise. In

order to complete Table 2.1, details of the probability of error are required, which is explained in Chapter 3.

CHAPTER 3

PROBABILITY OF ERROR

3.1 Breakdown of Wireless Cockroach Network

In this chapter, the error probability of the wireless cockroach network model is examined. Theoretical analysis is derived in order to elaborate on its performance. Since data is transmitted in four different paths, the performance must be analyzed individually.

3.1.1 Top Branch of Cockroach Network

First, the probability of error of the top branch of the cockroach network is considered, as shown in Figure 3.1.

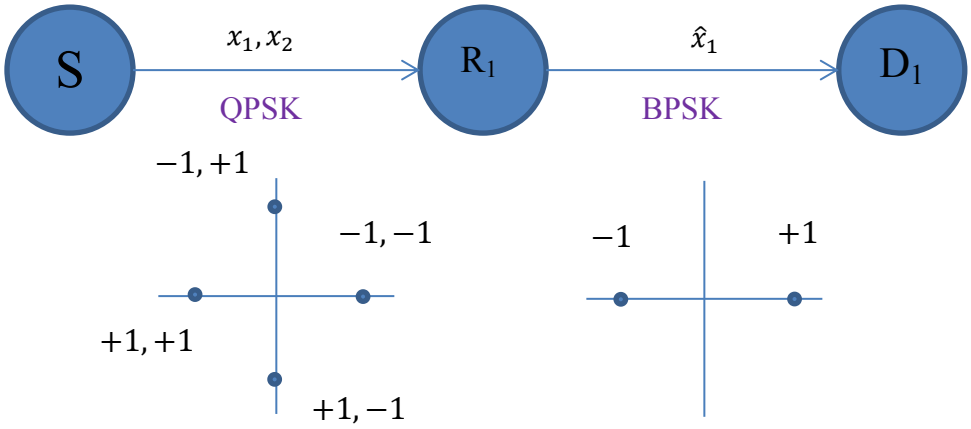


Figure 3.1: Top branch of cockroach network.

The same destination node D is represented by D_1 because the first branch from the top is connected to D. Although signals x_1 and x_2 are transmitted to relay R_1, that relay forwards x_1 only to the destination. Hence, the bit error rate from S to R_1 is

$$P_{b,SR_1} = \frac{1}{2}\left(1 - \sqrt{\frac{SNR}{SNR+2}}\right) \tag{9}$$

and the BER from R_1 to D is

$$P_{s,R_1D} = \frac{1}{2}\left(1 - \sqrt{\frac{SNR}{SNR+1}}\right) \tag{10}$$

where the signal-to-noise ratio is the average SNR over the Rayleigh fading coefficient channel. The overall BER of x_1 from S to D through R_1 is

$$P_{s,SR_1D} = (1 - P_{b,SR_1})P_{s,R_1D} + P_{b,SR_1}(1 - P_{s,R_1D}) \tag{11}$$

3.1.2 Bottom Branch of Cockroach Network

Next, the performance of signals x_1 and x_2 are examined at the bottom branch of the cockroach network, as shown in Figure 3.2.

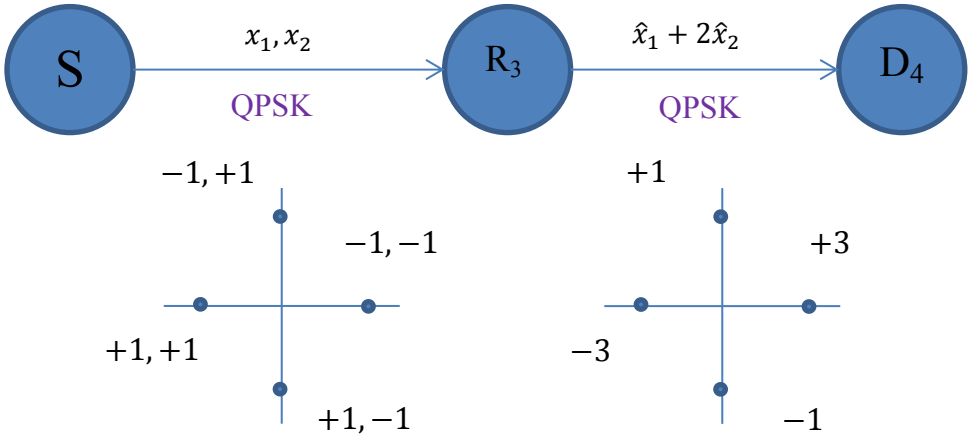


Figure 3.2: Bottom branch of cockroach network.

The same destination node D is represented by D_4 because the fourth branch from the top is connected to D. Since the signal modulation between the sender S and relay R_3 is QPSK, the symbol error rate from S to R_3 under Rayleigh fading is

$$P_{s,SR_3} = \frac{3}{4} - \sqrt{\frac{2}{\pi}\frac{SNR}{SNR+2}}\int_0^\infty Q\left(-\sqrt{\frac{SNR}{SNR+2}}z\right)e^{-\frac{z^2}{2}}dz. \tag{12}$$

Furthermore, the probability of making a two-bit error from S to R_3 is

$$P_{s,SR_3}|_{2bit} = \frac{1}{4} - \sqrt{\frac{2}{\pi}\frac{SNR}{SNR+2}}\int_0^\infty Q\left(\sqrt{\frac{SNR}{SNR+2}}z\right)e^{-\frac{z^2}{2}}dz \tag{13}$$

and the probability of a one-bit error from S to R_3 could be computed as

$$P_{s,SR_3}|_{1bit} = P_{s,SR_3} - P_{s,SR_3}|_{2bit}. \quad (14)$$

Next, focus is on the second half of the branch. Since the modulation here is the same as for the first half of the branch, the probability of error is similar. Therefore, the symbol error rate from R_3 to D is

$$P_{s,R_3D} = P_{s,SR_3}. \quad (15)$$

Also, the probability of a two-bit error from R_3 to D is

$$P_{s,R_3D}|_{2bit} = P_{s,SR_3}|_{2bit} \quad (16)$$

and the probability of a one-bit error from R_3 to D is

$$P_{s,R_3D}|_{1bit} = P_{s,SR_3}|_{1bit}. \quad (17)$$

Now, for the overall performance, the probability of no error from the sender S to the destination D through relay R_3 is

$$P_{c,SR_3D} = \left(1 - P_{s,SR_3}\right)\left(1 - P_{s,R_3D}\right) + \frac{1}{2}P_{s,SR_3}|_{1bit} \times P_{s,R_3D}|_{1bit} + P_{s,SR_3}|_{2bit} \times P_{s,R_3D}|_{2bit}. \quad (18)$$

This is because for all possibilities, D will receive the correct signal in the condition of no error occuring during transmission, or there is an error while decoding the data in R_3, but the same type of error occurs again while decoding the data in D. On the other hand, the symbol error rate of this branch is

$$P_{s,SR_3D} = 1 - P_{c,SR_3D}. \quad (19)$$

Similarly, the probability of a two-bit error from the sender S to the destination D through relay R_3 is

$$P_{s,SR_3D}|_{2bit} = \left(1 - P_{s,SR_3}\right)P_{s,R_3D}|_{2bit} + \frac{1}{2}P_{s,SR_3}|_{1bit} \times P_{s,R_3D}|_{1bit} + P_{s,SR_3}|_{2bit}\left(1 - P_{s,R_3D}\right) \quad (20)$$

and the probability of a one-bit error from S to D through R_3 can be calculated as

$$P_{s,SR_3D}|_{1bit} = 1 - P_{c,SR_3D} - P_{s,SR_3D}|_{2bit}. \quad (21)$$

3.1.3 Middle Top Branch of Cockroach Network

By referring back to Figure 3.1, Figure 3.3 shows that the middle top branch contains a similar structure to the top branch of the cockroach network.

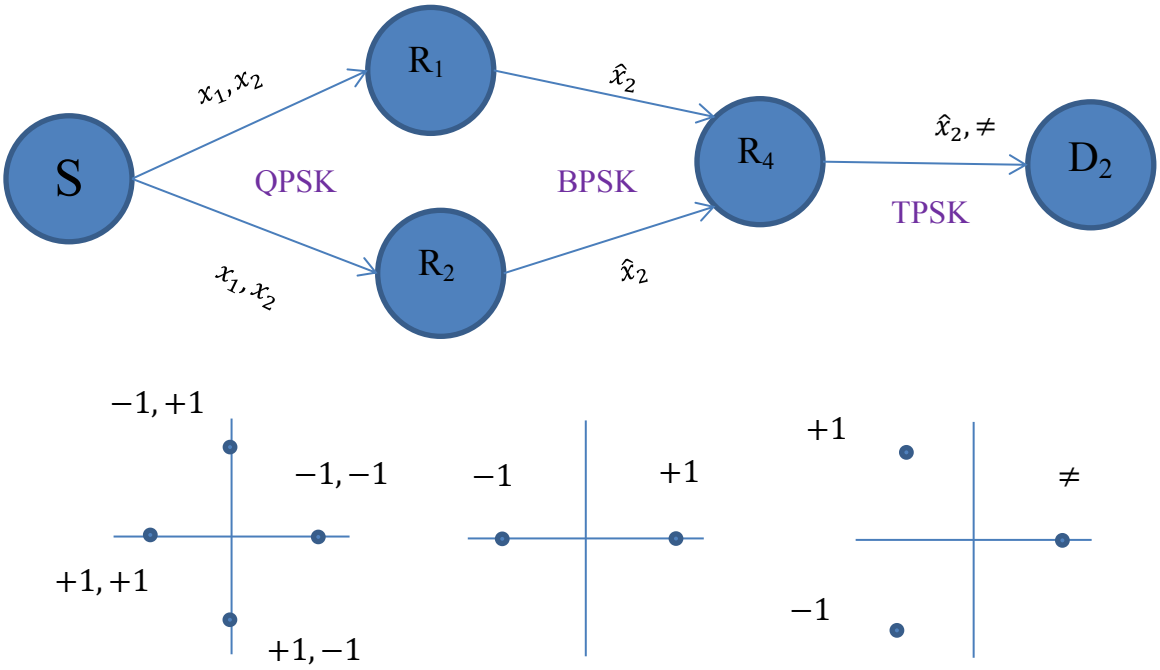


Figure 3.3: Middle top branch of the cockroach network.

The same destination node D is represented by D_2 because the second branch from the top is connected to D. Therefore, the probability of error of x_2 from S to R_4 through R_1 is

$$P_{s,SR_1R_4} = P_{s,SR_1D} \tag{22}$$

and the bit error rate from S to R_4 through R_2 is

$$P_{s,SR_2R_4} = P_{s,SR_1D}. \tag{23}$$

The symbol error rate from R_4 to D is

$$P_{s,R_4D} =$$

$$\int_{-\infty}^{\infty}\{1-[1-Q(t)]^2\}\frac{1}{\sqrt{2\pi}}e^{-\frac{z^2}{2}}\frac{1}{\frac{3}{2}SNR+1}\left[1+\right.$$

$$\left.e^{\frac{1}{2}\frac{3SNR}{3SNR+2}z^2}\sqrt{\frac{3SNR}{3SNR+2}}z\sqrt{2\pi}Q\left(-\sqrt{\frac{3SNR}{3SNR+2}}z\right)\right]dz. \quad (24)$$

The proof of equation (24) can be found in the Appendix.

Therefore, the probability of no error from the sender S to the destination D through relays R_1, R_2, and R_4 is

$$P_{c,SR_1R_2R_4D} = \left(1-P_{s,SR_1R_4}\right)\left(1-P_{s,SR_2R_4}\right)\left(1-P_{s,R_4D}\right)$$

$$+\frac{1}{2}\left[1-\left(1-P_{s,SR_1R_4}\right)\left(1-P_{s,SR_2R_4}\right)\right]\times P_{s,R_4D} \quad (25)$$

and the symbol error rate is

$$P_{s,SR_1R_2R_4D} = 1-P_{c,SR_1R_2R_4D}. \quad (26)$$

The overall probability of a one-bit error from S to D through R_1, R_2, and R_4 is

$$P_{sSR_1R_2R_4D}|_{1bit} = P_{s,SR_1R_4}\times P_{s,SR_2R_4}\left(1-P_{s,R_4D}\right)+\frac{1}{2}\left(1-P_{s,SR_1R_4}\times P_{s,SR_2R_4}\right)\times P_{s,R_4D}. \quad (27)$$

The probability of the received signal at D_2 detected as "≠" is

$$P_{s,SR_1R_2R_4D}|_{\neq} = \frac{1}{2}\left[\left(1-P_{s,SR_1R_4}\right)\left(1-P_{s,SR_2R_4}\right)+P_{s,SR_1R_4}\times P_{s,SR_2R_4}\right]\times P_{s,R_4D}$$

$$+\left[\left(1-P_{s,SR_1R_4}\right)P_{s,SR_2R_4}+P_{s,SR_1R_4}\left(1-P_{s,SR_2R_4}\right)\right]\left(1-P_{s,R_4D}\right). \quad (28)$$

3.1.4 Middle Bottom Branch of Cockroach Network

Lastly, the final branch of the cockroach network is examined for probability of error. The same destination node D is represented by D_3 in Figure 3.4 because the third branch from the top is connected to D. Because of the similarity, the symbol error rate from S to R_2 is the same as from S to R_3:

$$P_{s,SR_2} = P_{s,SR_3}. \quad (29)$$

Also, the probability of a two-bit error from S to R_2 is

$$P_{s,SR_2}|_{2bit} = P_{s,SR_3}|_{2bit} \tag{30}$$

and the probability of a one-bit error from S to R_2 is

$$P_{s,SR_2}|_{1bit} = P_{s,SR_3}|_{1bit}. \tag{31}$$

By checking the structure, showing that the relays R_2R_5 and R_3R_5 also use the same TPSK for modulation as R_4D, the symbol error rate from R_2 to R_5 is

$$P_{s,R_2R_5} = P_{s,R_4D} \tag{32}$$

and the symbol error rate from R_3 to R_5 is

$$P_{s,R_3R_5} = P_{s,R_4D}. \tag{33}$$

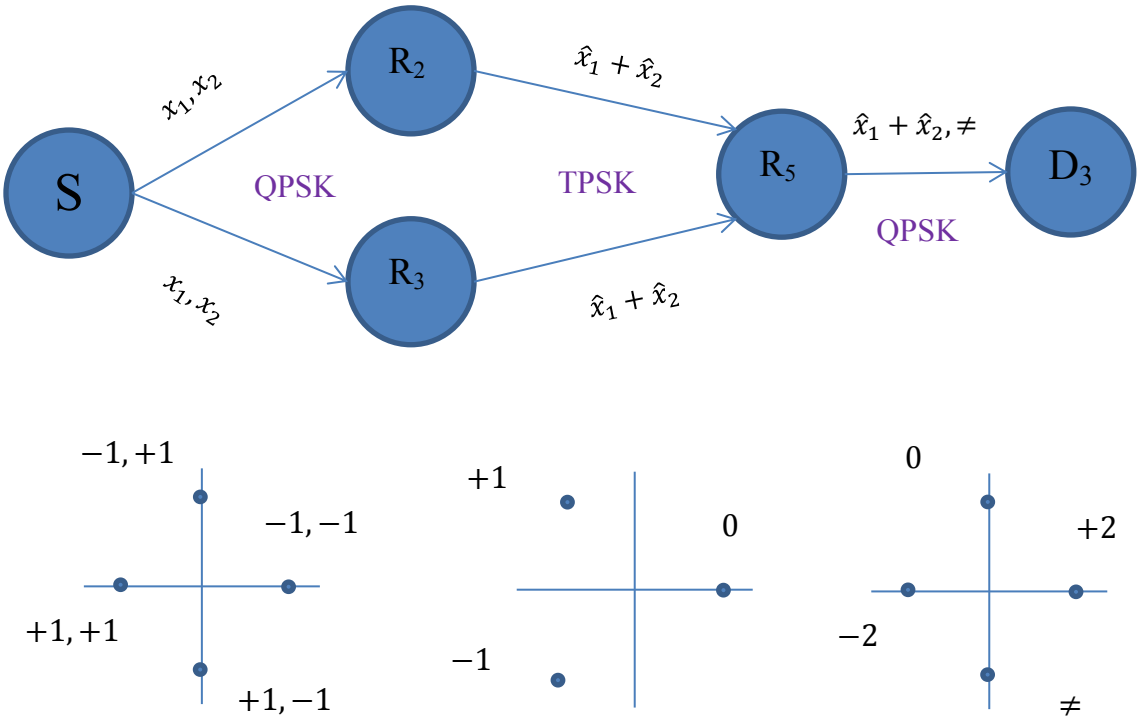


Figure 3.4: Middle bottom branch of cockroach network.

At this point, since the probability of error for the case of $x_1 = x_2$ is different from the case of $x_1 = -x_2$, the following equations for these two cases are written separately. First, the branch

from sender S to relay R_5 through R_2 is examined. The probability of no error from S to R_5 through R_2 when $x_1 = x_2$ is

$$P_{c,SR_2R_5}|_{x_1=x_2} = \left(1 - P_{s,SR_2}\right)\left(1 - P_{s,R_2R_5}\right) + \frac{1}{2}P_{s,SR_2} \times P_{s,R_2R_5}. \quad (34)$$

Also, the probability of a two-bit error from S to R_5 through R_2 when $x_1 = x_2$ is written as

$$P_{s,SR_2R_5}|_{2bit \quad x_1=x_2} = \frac{1}{2}\left(1 - P_{s,SR_2}|_{2bit}\right) \times P_{s,R_2R_5} + P_{s,SR_2}|_{2bit}\left(1 - P_{s,R_2R_5}\right) \quad (35)$$

and the probability of a one-bit error from S to R_5 through R_2 when $x_1 = x_2$ is

$$P_{s,SR_2R_5}|_{1bit \quad x_1=x_2} = \frac{1}{2}\left(1 - P_{s,SR_2}|_{1bit}\right) \times P_{s,R_2R_5} + P_{s,SR_2}|_{1bit}\left(1 - P_{s,R_2R_5}\right). \quad (36)$$

For the other case, the probability of no error from sender S to relay R_5 through R_2 when $x_1 = -x_2$ is

$$P_{c,SR_2R_5}|_{x_1=-x_2} = \left(1 - P_{s,SR_2}|_{1bit}\right)\left(1 - P_{s,R_2R_5}\right) + \frac{1}{2}P_{s,SR_2}|_{1bit} \times P_{s,R_2R_5}. \quad (37)$$

Again, the probability that the received signal is 2 from S to R_5 through R_2 when $x_1 = -x_2$ is

$$P_{s,SR_2R_5}|_{2 \quad x_1=-x_2} = \frac{1}{2}\left(1 - \frac{1}{2}P_{s,SR_2}|_{1bit}\right)P_{s,R_2R_5} + \frac{1}{2}P_{s,SR_2}|_{1bit}\left(1 - P_{s,R_2R_5}\right) \quad (38)$$

and the probability that the received signal is –2 from S to R_5 through R_2 when $x_1 = -x_2$ is

$$P_{s,SR_2R_5}|_{-2 \quad x_1=-x_2} = P_{s,SR_2R_5}|_{2 \quad x_1=-x_2}. \quad (39)$$

Since the modulation and structure of the branch of S to R_5 through R_3 is exactly the same as through R_2, the equations are just mirroring each other. Hence, the probability of no error from S to R_5 through R_3 when $x_1 = x_2$ is

$$P_{c,SR_3R_5}|_{x_1=x_2} = P_{c,SR_2R_5}|_{x_1=x_2} \quad (40)$$

and the probability of a two-bit error from S to R_5 through R_3 when $x_1 = x_2$ is

$$P_{s,SR_3R_5}|_{2bit \quad x_1=x_2} = P_{s,SR_2R_5}|_{2bit \quad x_1=x_2} \quad (41)$$

and the probability of a one-bit error from S to R_5 through R_3 when $x_1 = x_2$ is

$$P_{s,SR_3R_5}|_{1bit \quad x_1=x_2} = P_{s,SR_2R_5}|_{1bit \quad x_1=x_2}. \quad (42)$$

For the case of $x_1 = -x_2$, the probability of no error from S to R_5 through R_3 when $x_1 = -x_2$ is

$$P_{c,SR_3R_5}|_{x_1=-x_2} = P_{c,SR_2R_5}|_{x_1=-x_2} \tag{43}$$

and the probability that the received signal is 2 from S to R_5 through R_3 when $x_1 = -x_2$ is

$$P_{s,SR_3R_5}|_{2 \quad x_1=-x_2} = P_{s,SR_2R_5}|_{2 \quad x_1=-x_2} \tag{44}$$

and the probability that the received signal is –2 from S to R_5 through R_3 when $x_1 = -x_2$ is

$$P_{s,SR_3R_5}|_{-2 \quad x_1=-x_2} = P_{s,SR_2R_5}|_{-2 \quad x_1=-x_2}. \tag{45}$$

Next, the branch on the right between R_5 and D is examined. Since its transmission and modulation are the same as R_3 to D, the symbol error rate from R_5 to D can be written as

$$P_{s,R_5D} = P_{s,R_3D} \tag{46}$$

and the probability of a two-bit error from R_5 to D is

$$P_{s,R_5D}|_{2bit} = P_{s,R_3D}|_{2bit} \tag{47}$$

and the probability of a one-bit error from R_5 to D is

$$P_{s,R_5D}|_{1bit} = P_{s,R_3D}|_{1bit}. \tag{48}$$

Finally, the overall probability analysis from S to D, as shown in Figure 3.4, also needs to be split into two cases. For the case of $x_1 = x_2$, the probability of no error from S to D through R_2, R_3, and R_5 is

$$P_{c,SR_2R_3R_5D}|_{x_1=x_2} = P_{c,SR_2R_5}|_{x_1=x_2} \times P_{c,SR_3R_5}|_{x_1=x_2} \times \left(1 - P_{s,R_5D}\right)$$

$$+P_{s,SR_2R_5}|_{2bit \quad x_1=x_2} \times P_{s,SR_3R_5}|_{2bit \quad x_1=x_2} \times P_{s,R_5D}|_{2bit}$$

$$+\frac{1}{2}\left(1 - P_{c,SR_2R_5}|_{x_1=x_2} \times P_{c,SR_3R_5}|_{x_1=x_2} - P_{s,SR_2R_5}|_{2bit \quad x_1=x_2} \times P_{s,SR_3R_5}|_{2bit \quad x_1=x_2}\right)P_{s,R_5D}|_{1bit}. \tag{49}$$

The probability of a two-bit error from S to D through R_2, R_3, and R_5 when $x_1 = x_2$ is

$$P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2} = P_{c,SR_2R_5}|_{x_1=x_2} \times P_{c,SR_3R_5}|_{x_1=x_2} \times P_{s,R_5D}|_{2bit}$$

$$+P_{s,SR_2R_5}|_{2bit \quad x_1=x_2} \times P_{s,SR_3R_5}|_{2bit \quad x_1=x_2}\left(1-P_{s,R_5D}\right)$$

$$+\frac{1}{2}\left(1-P_{c,SR_2R_5}|_{x_1=x_2} \times P_{c,SR_3R_5}|_{x_1=x_2}-P_{s,SR_2R_5}|_{2bit \quad x_1=x_2} \times P_{s,SR_3R_5}|_{2bit \quad x_1=x_2}\right)P_{s,R_5D}|_{1bit}. \quad (50)$$

The probability of a one-bit error from S to D through R_2, R_3, and R_5 when $x_1 = x_2$ is

$$P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2}=\frac{1}{2}\begin{pmatrix}P_{c,SR_2R_5}|_{x_1=x_2} \times P_{c,SR_3R_5}|_{x_1=x_2}+P_{s,SR_2R_5}|_{2bit \quad x_1=x_2}\\ \times P_{s,SR_3R_5}|_{2bit \quad x_1=x_2}\end{pmatrix}P_{s,R_5D}$$

$$+P_{s,SR_2R_5}|_{1bit \quad x_1=x_2} \times P_{s,SR_3R_5}|_{1bit \quad x_1=x_2}\left(1-P_{s,R_5D}\right)$$

$$+\begin{pmatrix}1-P_{c,SR_2R_5}|_{x_1=x_2} \times P_{c,SR_3R_5}|_{x_1=x_2}-P_{s,SR_2R_5}|_{2bit \quad x_1=x_2} \times P_{s,SR_3R_5}|_{2bit \quad x_1=x_2}\\ -P_{s,SR_2R_5}|_{1bit \quad x_1=x_2} \times P_{s,SR_3R_5}|_{1bit \quad x_1=x_2}\end{pmatrix}P_{s,R_5D}|_{2bit}. \quad (51)$$

And the probability of D_3 equal to '$\neq$' when $x_1 = x_2$ is

$$P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2}=$$

$$\frac{1}{2}\left(P_{c,SR_2R_5}|_{x_1=x_2} \times P_{c,SR_3R_5}|_{x_1=x_2}+P_{s,SR_2R_5}|_{2bit \quad x_1=x_2} \times P_{s,SR_3R_5}|_{2bit \quad x_1=x_2}\right)P_{s,R_5D}|_{1bit}+$$

$$P_{s,SR_2R_5}|_{1bit \quad x_1=x_2} \times P_{s,SR_3R_5}|_{1bit \quad x_1=x_2} \times P_{s,R_5D}|_{2bit}$$

$$+\begin{pmatrix}1-P_{c,SR_2R_5}|_{x_1=x_2} \times P_{c,SR_3R_5}|_{x_1=x_2}-P_{s,SR_2R_5}|_{2bit \quad x_1=x_2} \times P_{s,SR_3R_5}|_{2bit \quad x_1=x_2}\\ -P_{s,SR_2R_5}|_{1bit \quad x_1=x_2} \times P_{s,SR_3R_5}|_{1bit \quad x_1=x_2}\end{pmatrix}\left(1-\right.$$

$$\left.P_{s,R_5D}\right). \quad (52)$$

For the case of $x_1 = -x_2$, the probability of no error from S to D through R_2, R_3, and R_5 is

$$P_{c,SR_2R_3R_5D}|_{x_1=-x_2}=P_{c,SR_2R_5}|_{x_1=-x_2} \times P_{c,SR_3R_5}|_{x_1=-x_2}\left(1-P_{s,R_5D}\right)$$

$$+P_{s,SR_2R_5}|_{2 \quad x_1=-x_2} \times P_{s,SR_3R_5}|_{2 \quad x_1=-x_2} \times P_{s,R_5D}|_{1bit}$$

$$+\left(1-P_{c,SR_2R_5}|_{x_1=-x_2} \times P_{c,SR_3R_5}|_{x_1=-x_2}-2P_{s,SR_2R_5}|_{2 \quad x_1=-x_2} \times P_{s,SR_3R_5}|_{2 \quad x_1=-x_2}\right)P_{s,R_5D}|_{2bit} \quad (53)$$

The probability of D_3 being equal to 2 when $x_1 = -x_2$ is

$$P_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2}=P_{s,SR_2R_5}|_{2 \quad x_1=-x_2} \times P_{s,SR_3R_5}|_{2 \quad x_1=-x_2}\left(1-P_{s,R_5D}|_{1bit}\right)$$

$$+\frac{1}{2}\left(1-2P_{s,SR_2R_5}|_{2 \quad x_1=-x_2} \times P_{s,SR_3R_5}|_{2 \quad x_1=-x_2}\right)P_{s,R_5D}|_{1bit}. \quad (54)$$

The probability of D_3 being equal to –2 when $x_1 = -x_2$ is

$$P_{s,SR_2R_3R_5D}|_{-2 \quad x_1=-x_2} = P_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2}. \tag{55}$$

And the probability of D_3 being equal to '$\neq$' when $x_1 = -x_2$ is

$$P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2} = P_{c,SR_2R_5}|_{x_1=-x_2} \times P_{c,SR_3R_5}|_{x_1=-x_2} \times P_{s,R_5D}|_{2bit}$$

$$+P_{s,SR_2R_5}|_{2 \quad x_1=-x_2} \times P_{s,SR_3R_5}|_{2 \quad x_1=-x_2} \times P_{s,R_5D}|_{1bit}$$

$$+\left(1 - P_{c,SR_2R_5}|_{x_1=-x_2} \times P_{c,SR_3R_5}|_{x_1=-x_2} - 2P_{s,SR_2R_5}|_{2 \quad x_1=-x_2} \times P_{s,SR_3R_5}|_{2 \quad x_1=-x_2}\right)\left(1 - P_{s,R_5D}\right). \tag{56}$$

Finally, the overall symbol error rate for this branch can be written as

$$P_{s,SR_2R_3R_5D} = 1 - \frac{1}{2}\left(P_{c,SR_2R_3R_5D}|_{x_1=x_2} + P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\right). \tag{57}$$

3.2 Extended Lookup Table for Noisy Channel

By referring to Figure 5.1, the comparison of symbol error rates for these four branches can be shown as

$$P_{s,SR_2R_3R_5D} \; > \; P_{s,SR_1R_2R_4D} \; > \; P_{s,SR_3D} \; > \; P_{s,SR_1D} \tag{58}$$

With this relationship of the symbol error rate for each branch, the uncompleted Table 2.1 can be supplied with other combinations that are caused by noise and fading. For example, in the case of $\hat{x}_1 = -1, \quad \hat{x}_2 = -1$, and R_1 as an adversary node, there should be one vector, which is $\begin{pmatrix} +1 \\ \neq \\ -2 \\ -3 \end{pmatrix}$.

However, other vectors such as $\begin{pmatrix} +1 \\ \neq \\ 0 \\ -3 \end{pmatrix}$, $\begin{pmatrix} +1 \\ \neq \\ +2 \\ -3 \end{pmatrix}$, and $\begin{pmatrix} +1 \\ \neq \\ \neq \\ -3 \end{pmatrix}$ also belong to the same category, because the middle bottom branch has the highest chance of causing error at a low SNR. Therefore, after completing Table 2.1 with the other combinations, the final result of decoding the message and detecting the adversary is shown in Table 3.1.

TABLE 3.1

COMPLETE LOOKUP TABLE FOR BIT DECISION AND ADVERSARY DETECTION

	$\hat{x}_1 = -1 \quad \hat{x}_2 = -1$	$\hat{x}_1 = -1 \quad \hat{x}_2 = +1$	$\hat{x}_1 = +1 \quad \hat{x}_2 = -1$	$\hat{x}_1 = +1 \quad \hat{x}_2 = +1$
NA	$-1 \quad -1 \quad -1$ $-1 \quad -1 \quad -1$ $-2 \quad -2 \quad -2$ $-3 \quad -1 \quad +1$	$-1 \quad -1 \quad -1$ $+1 \quad +1 \quad +1$ $0 \quad 0 \quad 0$ $-3 \quad +1 \quad +3$	$+1 \quad +1 \quad +1$ $-1 \quad -1 \quad -1$ $0 \quad 0 \quad 0$ $-3 \quad -1 \quad +3$	$+1 \quad +1 \quad +1$ $+1 \quad +1 \quad +1$ $+2 \quad +2 \quad +2$ $-1 \quad +1 \quad +3$
R_1	$+1 \quad +1 \quad +1 \quad +1 \quad +1$ $-1 \quad \neq \quad \neq \quad \neq \quad \neq$ $-2 \quad -2 \quad 0 \quad +2 \quad \neq$ $-3 \quad -3 \quad -3 \quad -3 \quad -3$	$+1 \quad +1 \quad +1 \quad +1 \quad +1 \quad +1$ $-1 \quad +1 \quad \neq \quad \neq \quad \neq \quad \neq$ $0 \quad 0 \quad -2 \quad 0 \quad +2 \quad \neq$ $+1 \quad +1 \quad +1 \quad +1 \quad +1 \quad +1$	$-1 \quad -1 \quad -1 \quad -1 \quad -1 \quad -1$ $-1 \quad +1 \quad \neq \quad \neq \quad \neq \quad \neq$ $0 \quad 0 \quad -2 \quad 0 \quad +2 \quad \neq$ $-1 \quad -1 \quad -1 \quad -1 \quad -1 \quad -1$	$-1 \quad -1 \quad -1 \quad -1 \quad -1$ $+1 \quad \neq \quad \neq \quad \neq \quad \neq$ $+2 \quad -2 \quad 0 \quad +2 \quad \neq$ $+3 \quad +3 \quad +3 \quad +3 \quad +3$
R_2	-1 $\neq$ $\neq$ -3	$-1 \quad -1 \quad -1$ $\neq \quad \neq \quad \neq$ $-2 \quad +2 \quad \neq$ $+1 \quad +1 \quad +1$	$+1 \quad +1 \quad +1$ $\neq \quad \neq \quad \neq$ $-2 \quad 2 \quad \neq$ $-1 \quad -1 \quad -1$	$+1$ $\neq$ $\neq$ $+3$
R_3	$-1 \quad -1 \quad -1 \quad -1 \quad -1$ $-1 \quad -1 \quad -1 \quad -1 \quad -1$ $-2 \quad 0 \quad +2 \quad \neq \quad \neq$ $+3 \quad +3 \quad +3 \quad +3 \quad -1$	$-1 \quad -1 \quad -1 \quad -1$ $+1 \quad +1 \quad +1 \quad +1$ $-2 \quad +2 \quad \neq \quad \neq$ $-1 \quad -1 \quad -1 \quad +3$	$+1 \quad +1 \quad +1 \quad +1$ $-1 \quad -1 \quad -1 \quad -1$ $-2 \quad +2 \quad \neq \quad \neq$ $+1 \quad +1 \quad -3 \quad +1$	$+1 \quad +1 \quad +1 \quad +1 \quad +1$ $+1 \quad +1 \quad +1 \quad +1 \quad +1$ $-2 \quad 0 \quad +2 \quad \neq \quad \neq$ $-3 \quad -3 \quad -3 \quad -3 \quad +1$
R_4	$-1 \quad -1 \quad -1 \quad -1$ $+1 \quad +1 \quad \neq \quad +1$ $-2 \quad -2 \quad -2 \quad \neq$ $-3 \quad +3 \quad -3 \quad -3$	$-1 \quad -1 \quad -1$ $-1 \quad \neq \quad -1$ $0 \quad 0 \quad \neq$ $+1 \quad +1 \quad +1$	$+1 \quad +1 \quad +1$ $+1 \quad \neq \quad +1$ $0 \quad 0 \quad \neq$ $-1 \quad -1 \quad -1$	$+1 \quad +1 \quad +1 \quad +1$ $-1 \quad -1 \quad \neq \quad -1$ $+2 \quad +2 \quad +2 \quad \neq$ $-3 \quad +3 \quad +3 \quad +3$
R_5	$-1 \quad -1 \quad -1 \quad -1$ $-1 \quad -1 \quad -1 \quad -1$ $0 \quad +2 \quad +2 \quad +2$ $-3 \quad -3 \quad -1 \quad +1$	$-1 \quad -1 \quad -1$ $+1 \quad +1 \quad +1$ $-2 \quad +2 \quad \neq$ $+1 \quad +1 \quad +1$	$+1 \quad +1 \quad +1$ $-1 \quad -1 \quad -1$ $-2 \quad +2 \quad \neq$ $-1 \quad -1 \quad -1$	$+1 \quad +1 \quad +1 \quad +1$ $-1 \quad +1 \quad +1 \quad +1$ $-2 \quad -2 \quad -2 \quad -2$ $+3 \quad -1 \quad +1 \quad +3$
	$-1 \quad -1 \quad -1 \quad -1$ $+1 \quad \neq \quad \neq \quad -1$ $+2 \quad 0 \quad +2 \quad \neq$ $-3 \quad -3 \quad -3 \quad -3$			$+1 \quad +1 \quad +1 \quad +1$ $+1 \quad \neq \quad \neq \quad +1$ $0 \quad -2 \quad 0 \quad \neq$ $+3 \quad +3 \quad +3 \quad +3$

3.3 Bit Error Rate

Next, the bit error rate of the message received at the destination could be obtained by referring to Table 3.1. Starting at a BER of x_1 given that $x_1 = -1$, the error occurs when x_1 is decoded as +1, which is

$$BER_{x_1}|_{x_1=-1} = P(\hat{x}_1 = +1 | x_1 = -1). \tag{59}$$

By checking Table 3.1, the vectors in the last two columns show the combination where x_1 is decoded as +1; therefore, the probability that the destination receives these vectors when –1 is transmitted from S is

$$BER_{x_1}|_{x_1=-1} = P\{D_1 = +1 | x_1 = -1\} + P\{(D_1 = -1, \quad D_2 = '\neq', \quad D_4 = -1) | x_1 = -1\}$$

$$+ P\{(D_1 = -1, \quad D_2 = '\neq', \quad D_4 = +3) | x_1 = -1\}$$

$$+ P\{(D_1 = -1, \quad D_2 = -1, \quad D_3 = 0, \quad D_4 = -1) | x_1 = -1\}$$

$$+P\{(D_1=-1,\quad D_2=+1,\quad D_3=0,\quad D_4=-1)|x_1=-1\}$$

$$+P\{(D_1=-1,\quad D_2=+1,\quad D_3=+2,\quad D_4=+3)|x_1=-1\}$$

$$-P\{(D_1=+1,\quad D_2='\neq',\quad D_4=-3)|x_1=-1\}$$

$$-P\{(D_1=+1,\quad D_2='\neq',\quad D_4=+1)|x_1=-1\}$$

$$-P\{(D_1=+1,\quad D_2=-1,\quad D_3=-2,\quad D_4=-3)|x_1=-1\}$$

$$-P\{(D_1=+1,\quad D_2=-1,\quad D_3=0,\quad D_4=+1)|x_1=-1\}$$

$$-P\{(D_1=+1,\quad D_2=+1,\quad D_3=0,\quad D_4=+1)|x_1=-1\}. \qquad (60)$$

Since the elements of the vector are actually dependent, it is cumbersome to derive the equations to compute the exact probability. However, it is possible to get an approximation by assuming that D_1, D_2, D_3, and D_4 are independent. The independence assumption is reasonable because each branch has independent fading and noise. The approximation results will be compared to simulation results in Chapter 5. Both almost overlap each other.

$$BER_{x_1}|_{x_1=-1}=P(\hat{x}_1=+1|x_1=-1)$$

$$\approx P(D_1=+1|x_1=-1)$$

$$+P(D_1=-1|x_1=-1)\times$$

$$\{P(D_2='\neq'\ |x_1=-1)\times[P(D_4=-1|x_1=-1)+P(D_4=+3|x_1=-1)]+P(D_2=-1|x_1=$$

$$-1)\times P(D_3=0|x_1=-1)\times P(D_4=-1|x_1=-1)+P(D_2=+1|x_1=-1)\times[P(D_3=$$

$$0|x_1=-1)\times P(D_4=-1|x_1=-1)+P(D_3=+2|x_1=-1)\times P(D_4=+3|x_1=-1)]\}$$

$$-P(D_1=+1|x_1=-1)\times$$

$$\{P(D_2='\neq'\ |x_1=-1)\times[P(D_4=-3|x_1=-1)+P(D_4=+1|x_1=-1)]+P(D_2=+1|x_1=$$

$$-1)\times P(D_3=0|x_1=-1)\times P(D_4=+1|x_1=-1)+P(D_2=-1|x_1=-1)\times[P(D_3=$$

$$0|x_1=-1)\times P(D_4=+1|x_1=-1)+P(D_3=-2|x_1=-1)\times P(D_4=-3|x_1=-1)]\}. \qquad (61)$$

From here, the equation needs to be split into two cases again. For the case of $x_1 = x_2$, the bit error rate when x_1 is transmitted can be written as

$$BER_{x_1}|_{x_1=x_2} = P_{s,SR_1D} + \left(1 - P_{s,SR_1D}\right) \times \left[P_{s,SR_1R_2R_4D}|_{\neq} \times \left(\frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_3D}|_{2bit}\right) + P_{c,SR_1R_2R_4D} \times P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_1R_2R_4D}|_{1bit} \times \left(P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2} \times P_{s,SR_3D}|_{2bit}\right)\right] - P_{s,SR_1D} \times \left\{P_{s,SR_1R_2R_4D}|_{\neq} \times \left[P_{c,SR_3D} + \frac{1}{2}P_{s,SR_3D}|_{1bit}\right] + P_{s,SR_1R_2R_4D}|_{1bit} \times P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{c,SR_1R_2R_4D} \times \left[P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{c,SR_2R_3R_5D}|_{x_1=x_2} \times P_{c,SR_3D}\right]\right\}. \quad (62)$$

On the other hand, for the case of $x_1 = -x_2$, the bit error rate when $x_1 = -1$ is

$$BER_{x_1}|_{x_1=-x_2} = P_{s,SR_1D} + \left(1 - P_{s,SR_1D}\right) \times \left[P_{s,SR_1R_2R_4D}|_{\neq} \times \left(\frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_3D}|_{2bit}\right) + P_{s,SR_1R_2R_4D}|_{1bit} \times P_{c,SR_2R_3R_5D}|_{x_1=-x_2} \times P_{s,SR_3D}|_{2bit} + P_{c,SR_1R_2R_4D} \times \left(P_{c,SR_2R_3R_5D}|_{x_1=-x_2} \times P_{s,SR_3D}|_{2bit} + P_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit}\right)\right] - P_{s,SR_1D} \times \left\{P_{s,SR_1R_2R_4D}|_{\neq} \times \left[P_{c,SR_3D} + \frac{1}{2}P_{s,SR_3D}|_{1bit}\right] + P_{c,SR_1R_2R_4D} \times P_{c,SR_2R_3R_5D}|_{x_1=-x_2} \times P_{c,SR_3D} + P_{s,SR_1R_2R_4D}|_{1bit} \times \left[P_{s,SR_2R_3R_5D}|_{-2 \quad x_1=-x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{c,SR_2R_3R_5D}|_{x_1=-x_2} \times P_{c,SR_3D}\right]\right\}. \quad (63)$$

Therefore, the overall bit error rate for x_1 is

$$BER_{x_1} = \frac{1}{2}\left(BER_{x_1}|_{x_1=x_2} + BER_{x_1}|_{x_1=-x_2}\right). \quad (64)$$

By applying the same procedure for finding the BER of x_1, the BER of x_2 for the case $x_1 = x_2$ is

$$BER_{x_2}|_{x_1=x_2} = P_{s,SR_1R_2R_4D}|_{1bit} + P_{s,SR_1R_2R_4D}|_{\neq} \times \left(\frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_3D}|_{2bit}\right)$$

$$+P_{c,SR_1R_2R_4D}\times\Big\{P_{s,SR_2R_3R_5D}|_{1bit\quad x_1=x_2}\times\frac{1}{2}P_{s,SR_3D}|_{1bit}+P_{s,SR_1D}$$

$$\times\left[P_{s,SR_3D}|_{2bit}\times\left(1-P_{s,SR_2R_3R_5D}|_{1bit\quad x_1=x_2}\right)+P_{s,SR_2R_3R_5D}|_{2bit\quad x_1=x_2}\right.$$

$$\left.\times P_{c,SR_3D}\right]+\left(1-P_{s,SR_1D}\right)\times P_{s,SR_2R_3R_5D}|_{\neq\quad x_1=x_2}\times\frac{1}{2}P_{s,SR_3D}|_{1bit}\Big\}$$

$$-P_{s,SR_1R_2R_4D}|_{1bit}\times\Big\{P_{s,SR_2R_3R_5D}|_{1bit\quad x_1=x_2}\times\frac{1}{2}P_{s,SR_3D}|_{1bit}+\left[1-P_{s,SR_1D}\right]\times\left[P_{c,SR_3D}\left(1-\right.\right.$$

$$\left.P_{s,SR_2R_3R_5D}|_{1bit\quad x_1=x_2}\right)+P_{c,SR_2R_3R_5D}|_{x_1=x_2}\times P_{s,SR_3D}|_{2bit}\Big]+P_{s,SR_1D}\times P_{s,SR_2R_3R_5D}|_{\neq\quad x_1=x_2}\times$$

$$\left.\frac{1}{2}P_{s,SR_3D}|_{1bit}\right\}. \tag{65}$$

Also, the bit error rate of x_2 for the case $x_1 = -x_2$ can be written as

$$BER_{x_2}|_{x_1=-x_2}=P_{s,SR_1R_2R_4D}|_{1bit}+P_{s,SR_1R_2R_4D}|_{\neq}\times\left(\frac{1}{2}P_{s,SR_3D}|_{1bit}+P_{s,SR_3D}|_{2bit}\right)$$

$$+P_{c,SR_1R_2R_4D}\times\Big\{P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\times P_{s,SR_3D}|_{2bit}+\left(1-P_{s,SR_1D}\right)$$

$$\times\left[\frac{1}{2}P_{s,SR_3D}|_{1bit}\times\left(1-P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\right)+P_{s,SR_2R_3R_5D}|_{2\quad x_1=-x_2}\right.$$

$$\left.\times\frac{1}{2}P_{s,SR_3D}|_{1bit}\right]+P_{s,SR_1D}\times P_{s,SR_2R_3R_5D}|_{\neq\quad x_1=-x_2}\times P_{s,SR_3D}|_{2bit}\Big\}$$

$$-P_{s,SR_1R_2R_4D}|_{1bit}\times$$

$$\Big\{P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\times P_{c,SR_3D}+P_{s,SR_1D}\times\Big[\frac{1}{2}P_{s,SR_3D}|_{1bit}\left(1-P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\right)+$$

$$P_{s,SR_2R_3R_5D}|_{-2\quad x_1=-x_2}\times\frac{1}{2}P_{s,SR_3D}|_{1bit}\Big]+\left(1-P_{s,SR_1D}\right)\times P_{s,SR_2R_3R_5D}|_{\neq\quad x_1=-x_2}\times P_{c,SR_3D}\Big\}. \tag{66}$$

And the overall bit error rate for x_2 is

$$BER_{x_2}=\frac{1}{2}\left(BER_{x_2}|_{x_1=x_2}+BER_{x_2}|_{x_1=-x_2}\right). \tag{67}$$

Finally, combining equations (64) and (67), the overall bit error rate at the destination could be obtained as

$$BER=\frac{1}{2}\left(BER_{x_1}+BER_{x_2}\right). \tag{68}$$

3.4 Probability of Error with Presence of Adversary

Since the adversary is making the error on purpose by forwarding other data instead of the detected data to the next relay or destination, the probability of error is different from the no-adversary case, depending on the location of the adversary. Similar to the work of Kosut et al. [1], this paper assumes only one adversary node, if there is an adversary.

3.4.1 Adversary at R_1 Node

The adversary located at R1 node decodes the message from the source, and then alters the decoded information x_1 and x_2 and forwards it to the destination and R_4, respectively, as shown in Figure 3.5

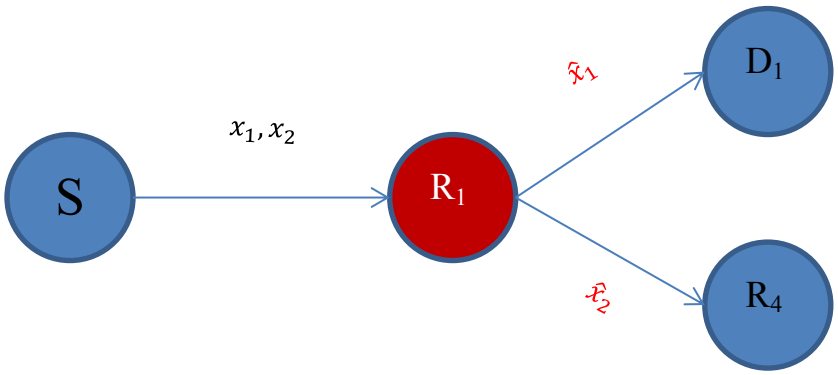


Figure 3.5: Adversary R_1 and modified signals.

Hence, equations (11) and (22) must be modified to reflect the activity of the adversary as follows:

$$P'_{s,SR_1D} = \left(1 - P_{b,SR_1}\right)\left(1 - P_{s,R_1D}\right) + P_{b,SR_1} \times P_{s,R_1D}, \tag{69}$$

$$P'_{s,SR_1R_4} = \left(1 - P_{s,SR_2R_4}\right). \tag{70}$$

3.4.2 Adversary at R_2 Node

If the adversary appears at R_2 node, it can alter messages to R_4 and R_5, as shown in Figure 3.6.

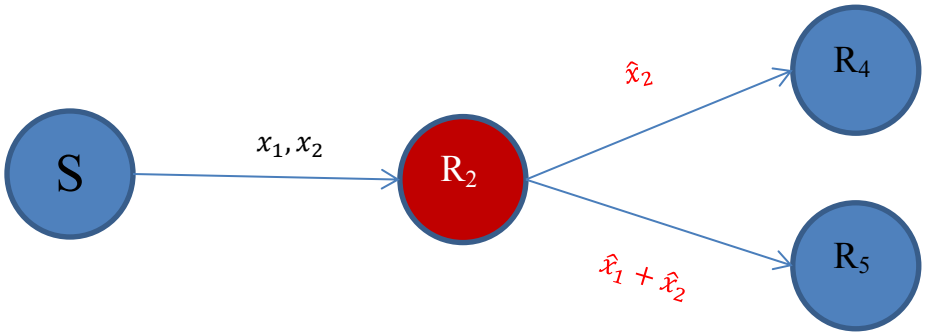


Figure 3.6: Adversary R_2 and modified signals.

For the branch from S to R_4, equation (23) is modified to

$$P'_{s,SR_2R_4} = \left(1 - P_{s,SR_1R_4}\right). \tag{71}$$

Also, for the branch toward R_5, equations (34) to (36) for case $x_1 = x_2$ must be modified as follows:

$$P'_{c,SR_2R_5}|_{x_1=x_2} = \frac{1}{2}P_{s,SR_2}\left(1 - P_{s,R_2R_5}\right) + \frac{1}{4}\left(2 - P_{s,SR_2}\right)P_{s,R_2R_5} \tag{72}$$

$$P'_{s,SR_2R_5}|_{1bit \quad x_1=x_2} = \frac{1}{2}\left(1 - P_{s,SR_2}|_{1bit}\right)\left(1 - P_{s,R_2R_5}\right) + \frac{1}{4}\left(1 + P_{s,SR_2}|_{1bit}\right)P_{s,R_2R_5} \tag{73}$$

$$P'_{s,SR_2R_5}|_{2bit \quad x_1=x_2} = \frac{1}{2}\left(1 - P_{s,SR_2}|_{2bit}\right)\left(1 - P_{s,R_2R_5}\right) + \frac{1}{4}\left(1 + P_{s,SR_2}|_{2bit}\right)P_{s,R_2R_5} \tag{74}$$

and equations (37) to (39) for the case $x_1 = -x_2$ must be modified as follows:

$$P'_{c,SR_2R_5}|_{x_1=-x_2} = \frac{1}{2}P_{s,SR_2}|_{1bit}\left(1 - P_{s,R_2R_5}\right) + \frac{1}{2}\left(1 - \frac{1}{2}P_{s,SR_2}|_{1bit}\right)P_{s,R_2R_5} \tag{75}$$

$$P'_{s,SR_2R_5}|_{2 \quad x_1=-x_2} = \frac{1}{2}\left(1 - \frac{1}{2}P_{s,SR_2}|_{1bit}\right)\left(1 - P_{s,R_2R_5}\right) + \frac{1}{4}\left(1 + \frac{1}{2}P_{s,SR_2}|_{1bit}\right)P_{s,R_2R_5} \tag{76}$$

$$P'_{s,SR_2R_5}|_{-2 \quad x_1=-x_2} = P'_{s,SR_2R_5}|_{2 \quad x_1=-x_2} \tag{77}$$

3.4.3 Adversary at R_3 Node

Similar to what has been shown previously, once node R_3 is compromised, it will flip the signal toward R_5 and D, as shown in Figure 3.7.

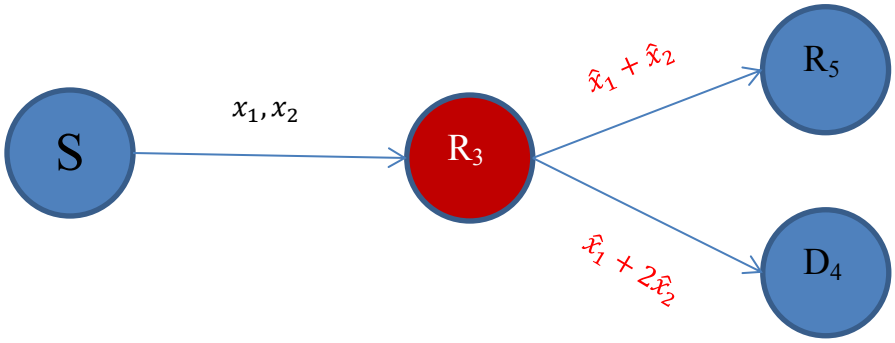


Figure 3.7: Adversary R_3 and modified signals.

For the branch toward R_5, equations (40) to (42) for case $x_1 = x_2$ are modified as follows:

$$P'_{c,SR_3R_5}|_{x_1=x_2} = \frac{1}{2}P_{s,SR_3}\left(1 - P_{s,R_3R_5}\right) + \frac{1}{4}\left(2 - P_{s,SR_3}\right)P_{s,R_3R_5} \tag{78}$$

$$P'_{s,SR_3R_5}|_{1bit \quad x_1=x_2} = \frac{1}{2}\left(1 - P_{s,SR_3}|_{1bit}\right)\left(1 - P_{s,R_3R_5}\right) + \frac{1}{4}\left(1 + P_{s,SR_3}|_{1bit}\right)P_{s,R_3R_5} \tag{79}$$

$$P'_{s,SR_3R_5}|_{2bit \quad x_1=x_2} = \frac{1}{2}\left(1 - P_{s,SR_3}|_{2bit}\right)\left(1 - P_{s,R_3R_5}\right) + \frac{1}{4}\left(1 + P_{s,SR_3}|_{2bit}\right)P_{s,R_3R_5} \tag{80}$$

and for the case $x_1 = -x_2$, equations (43) to (45) are modified as follows:

$$P'_{c,SR_3R_5}|_{x_1=-x_2} = \frac{1}{2}P_{s,SR_3}|_{1bit}\left(1 - P_{s,R_3R_5}\right) + \frac{1}{2}\left(1 - \frac{1}{2}P_{s,SR_3}|_{1bit}\right)P_{s,R_3R_5} \tag{81}$$

$$P'_{s,SR_3R_5}|_{2 \quad x_1=-x_2} = \frac{1}{2}\left(1 - \frac{1}{2}P_{s,SR_3}|_{1bit}\right)\left(1 - P_{s,R_3R_5}\right) + \frac{1}{4}\left(1 + \frac{1}{2}P_{s,SR_3}|_{1bit}\right)P_{s,R_3R_5} \tag{82}$$

$$P'_{s,SR_3R_5}|_{-2 \quad x_1=-x_2} = P'_{s,SR_3R_5}|_{2 \quad x_1=-x_2} \tag{83}$$

For the branch from S to D, equations (19) and (20) are changed to the following:

$$P'_{c,SR_3D} = P_{s,SR_3D}|_{2bit} \tag{84}$$

$$P'_{s,SR_3D}|_{2bit} = 1 - P_{c,SR_3D} \tag{85}$$

3.4.4 Adversary at R_4 Node

The adversary at node of R_4 compares the information from R_1 and R_2 first, and then sends an alternate signal instead of the correct signal, as shown in Figure 3.8.

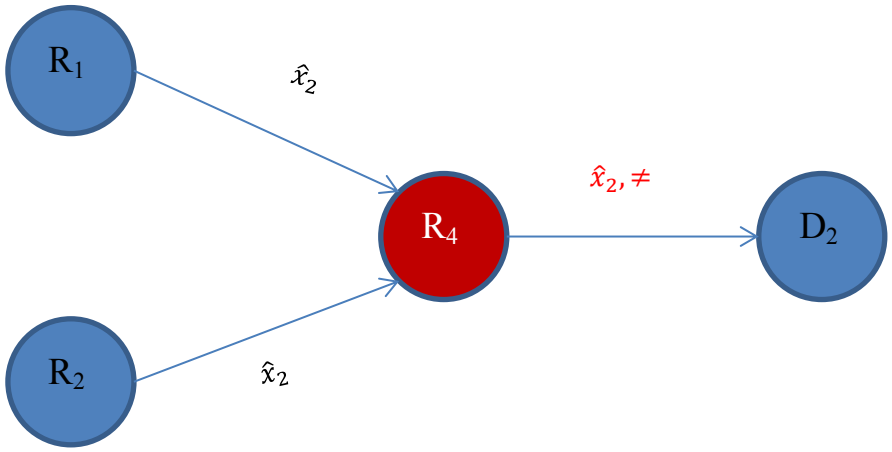


Figure 3.8: Adversary R_4 and modified signals.

Equations (25), (27), and (28) need to be changed to the following:

$$P'_{c,SR_1R_2R_4D} = \frac{1}{2}\left[1-\left(1-P_{s,SR_1R_4}\right)\left(1-P_{s,SR_2R_4}\right)\right]\left(1-P_{s,R_4D}\right) + \frac{1}{4}\left[1+\left(1-P_{s,SR_1R_4}\right)\left(1-P_{s,SR_2R_4}\right)\right]P_{s,R_4D} \quad (86)$$

$$P'_{s,SR_1R_2R_4D}|_{1bit} = \frac{1}{2}\left(1-P_{s,SR_1R_4}\times P_{s,SR_2R_4}\right)\left(1-P_{s,R_4D}\right) + \frac{1}{4}\left(1+P_{s,SR_1R_4}\times P_{s,SR_2R_4}\right)P_{s,R_4D} \quad (87)$$

$$P'_{s,SR_1R_2R_4D}|_{\neq} = \frac{1}{2}\left[1-\left(1-P_{s,SR_1R_4}\right)P_{s,SR_2R_4} - P_{s,SR_1R_4}\left(1-P_{s,SR_2R_4}\right)\right]\left(1-P_{s,R_4D}\right) + \frac{1}{4}\left[1+\left(1-P_{s,SR_1R_4}\right)P_{s,SR_2R_4} + P_{s,SR_1R_4}\left(1-P_{s,SR_2R_4}\right)\right]P_{s,R_4D} \quad (88)$$

3.4.5 Adversary at R_5 Node

At last, the adversary node R_5 will change the signal to the destination after comparing the message from R_2 and R_3, as shown in Figure 3.9.

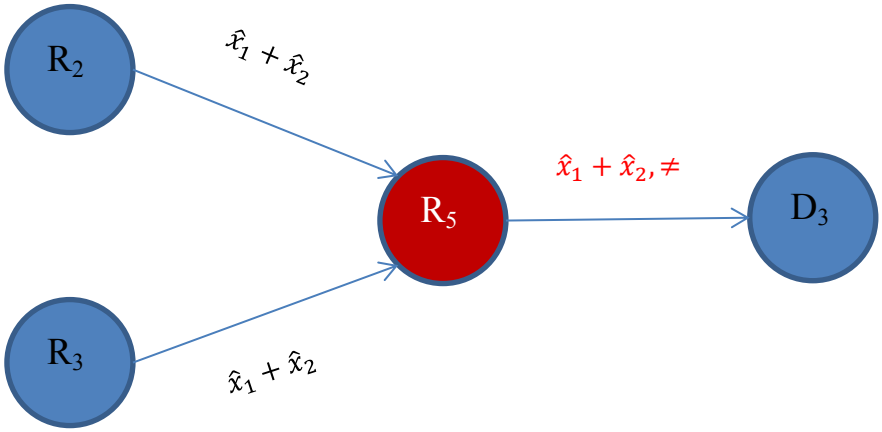


Figure 3.9: Adversary R_5 and modified signals.

The modification of equations (49) to (56) are for the case where R_5 is the adversary when $x_1 = x_2$:

$$P'_{c,SR_2R_3R_5D}|_{x_1=x_2} = P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2} \tag{89}$$

$$P'_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2} = P_{c,SR_2R_3R_5D}|_{x_1=x_2} \tag{90}$$

$$P'_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} = P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2} \tag{91}$$

$$P'_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2} = P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} \tag{92}$$

and when $x_1 = -x_2$:

$$P'_{c,SR_2R_3R_5D}|_{x_1=-x_2} = P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2} \tag{93}$$

$$P'_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2} = P_{c,SR_2R_3R_5D}|_{x_1=-x_2} \tag{94}$$

$$P'_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2} = P_{s,SR_2R_3R_5D}|_{-2 \quad x_1=-x_2} \tag{95}$$

$$P'_{s,SR_2R_3R_5D}|_{-2 \quad x_1=-x_2} = P_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2} \tag{96}$$

CHAPTER 4

ADVERSARY DETECTION

In this chapter, the probability of adversary detection is focused on for derivation. Similar to the bit error rate analysis in the previous chapter, the probability of detection also could be obtained by checking the rows in Table 1.

First, the probability that the detected data has no adversary when $x_1 = x_2$ is

$$P_{D,NA}|_{x_1=x_2} = P_{c,SR_1D}\Big[P_{c,SR_1R_2R_4D} \times P_{c,SR_2R_3R_5D}|_{x_1=x_2}\big(1 - P_{s,SR_3D}|_{2bit}\big) + P_{s,SR_1R_2R_4D}|_{1bit} \times P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2}\Big(1 - \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big)\Big] + P_{s,SR_1D}\Big[P_{c,SR_1R_2R_4D} \times P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2}\Big(1 - \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big) + P_{s,SR_1R_2R_4D}|_{1bit} \times P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2}\big(1 - P_{c,SR_3D}\big)\Big] \tag{97}$$

and probability that the detected data has no adversary when $x_1 = -x_2$ is

$$P_{D,NA}|_{x_1=-x_2} = P_{c,SR_1D}\Big[P_{s,SR_1R_2R_4D}|_{1bit} \times P_{s,SR_2R_3R_5D}|_{-2 \quad x_1=-x_2}\Big(1 - \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big) + P_{c,SR_1R_2R_4D} \times P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\big(1 - P_{s,SR_3D}|_{2bit}\big)\Big] + P_{s,SR_1D}\Big[P_{s,SR_1R_2R_4D}|_{1bit} \times P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\big(1 - P_{c,SR_3D}\big) + P_{c,SR_1R_2R_4D} \times P_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2}\Big(1 - \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big)\Big]. \tag{98}$$

By combining equations (97) and (98), the overall probability that no adversary is detected can be obtained as

$$P_{D,NA} = \frac{1}{2}\big(P_{D,NA}|_{x_1=x_2} + P_{D,NA}|_{x_1=-x_2}\big). \tag{99}$$

Similarly, the probability that R_1 is detected as an adversary when $x_1 = x_2$ is

$$P_{D,R_1}|_{x_1=x_2} = P_{s,SR_1D}\Big[P_{c,SR_1R_2R_4D} \times P_{c,SR_2R_3R_5D}|_{x_1=x_2} \times P_{c,SR_3D} + P_{s,SR_1R_2R_4D}|_{\neq}\Big(P_{c,SR_3D} + \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big) + \big(1 - P_{s,SR_1R_2R_4D}|_{\neq}\big)P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big] + P_{c,SR_1D}\Big[(1 -$$

$$P_{s,SR_1R_2R_4D}|_{\neq})P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_1R_2R_4D}|_{\neq}\left(\frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_3D}|_{2bit}\right) + P_{s,SR_1R_2R_4D}|_{1bit} \times P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2} \times P_{s,SR_3D}|_{2bit}\Big] \quad (100)$$

and the probability that R_1 is detected as an adversary when $x_1 = -x_2$ is

$$P_{D,R_1}|_{x_1=-x_2} = P_{s,SR_1D}\Big[P_{s,SR_1R_2R_4D}|_{1bit} \times P_{s,SR_2R_3R_5D}|_{-2 \quad x_1=-x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_1R_2R_4D}|_{\neq}\left(P_{c,SR_3D} + \frac{1}{2}P_{s,SR_3D}|_{1bit}\right) + \left(1 - P_{s,SR_1R_2R_4D}|_{\neq}\right)P_{c,SR_2R_3R_5D}|_{x_1=-x_2} \times P_{c,SR_3D}\Big] + P_{c,SR_1D}\Big[\left(1 - P_{s,SR_1R_2R_4D}|_{\neq}\right)P_{c,SR_2R_3R_5D}|_{x_1=-x_2} \times P_{s,SR_3D}|_{2bit} + P_{s,SR_1R_2R_4D}|_{\neq}\left(\frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_3D}|_{2bit}\right) + P_{c,SR_1R_2R_4D} \times P_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big]. \quad (101)$$

Next, the probability of R_2 is detected as an adversary when $x_1 = x_2$ is

$$P_{D,R_2}|_{x_1=x_2} = P_{s,SR_1R_2R_4D}|_{\neq}\Big\{P_{c,SR_1D}\Big[P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2} \times P_{c,SR_3D} + \left(1 - P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2}\right) \times \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big] + P_{s,SR_1D}\Big[\left(1 - P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2}\right) \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2} \times P_{s,SR_3D}|_{2bit}\Big]\Big\} \quad (102)$$

and the probability of R_2 is detected as an adversary when $x_1 = -x_2$ is

$$P_{D,R_2}|_{x_1=-x_2} = P_{s,SR_1R_2R_4D}|_{\neq}\Big\{P_{c,SR_1D}\Big[P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + \left(1 - P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\right) \times P_{c,SR_3D}\Big] + P_{s,SR_1D}\Big[\left(1 - P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\right) \times P_{s,SR_3D}|_{2bit} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big]\Big\}. \quad (103)$$

For the R_3 case, the probability that R_3 is detected as an adversary when $x_1 = x_2$ is

$$P_{D,R_3}|_{x_1=x_2} = P_{c,SR_1D}\Big\{P_{c,SR_1R_2R_4D}\left(P_{s,SR_3D}|_{2bit} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit}\right) + P_{s,SR_1R_2R_4D}|_{1bit}\Big[\left(1 - P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2}\right) \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2} \times$$

$$P_{s,SR_3D}|_{2bit}\Big]\Big\} + P_{s,SR_1D}\Big\{P_{c,SR_1R_2R_4D}\Big[\big(1 - P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2}\big) \times \frac{1}{2}P_{s,SR_3D}|_{1bit} +$$

$$P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2} \times P_{c,SR_3D}\Big] + P_{s,SR_1R_2R_4D}|_{1bit}\Big(P_{c,SR_3D} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2} \times$$

$$\frac{1}{2}P_{s,SR_3D}|_{1bit}\Big)\Big\} \tag{104}$$

and the probability that R_3 is detected as an adversary when $x_1 = -x_2$ is

$$P_{D,R_3}|_{x_1=-x_2} = P_{c,SR_1D}\Big\{P_{s,SR_1R_2R_4D}|_{1bit}\Big(\frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2} \times P_{s,SR_3D}|_{2bit}\Big) +$$

$$P_{c,SR_1R_2R_4D}\Big[\big(1 - P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\big) \times P_{s,SR_3D}|_{2bit} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big]\Big\} +$$

$$P_{s,SR_1D}\Big\{P_{s,SR_1R_2R_4D}|_{1bit}\Big[\big(1 - P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\big) \times P_{c,SR_3D} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2} \times$$

$$\frac{1}{2}P_{s,SR_3D}|_{1bit}\Big] + P_{c,SR_1R_2R_4D}\Big(\frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2} \times P_{c,SR_3D}\Big)\Big\}. \tag{105}$$

Next, the probability that R_4 is detected as an adversary when $x_1 = x_2$ is

$$P_{D,R_4}|_{x_1=x_2} = P_{c,SR_1D}\Big\{P_{s,SR_1R_2R_4D}|_{1bit}\big[\big(P_{c,SR_2R_3R_5D}|_{x_1=x_2} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2}\big)P_{c,SR_3D} +$$

$$P_{c,SR_2R_3R_5D}|_{x_1=x_2} \times P_{s,SR_3D}|_{2bit}\big] +$$

$$P_{s,SR_1R_2R_4D}|_{\neq}\Big(P_{c,SR_2R_3R_5D}|_{x_1=x_2} \times P_{c,SR_3D} + P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big) +$$

$$P_{c,SR_1R_2R_4D}\big(P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2}\big) \times \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big\} +$$

$$P_{s,SR_1D}\Big\{P_{c,SR_1R_2R_4D}\big[\big(P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2}\big)P_{s,SR_3D}|_{2bit} +$$

$$P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2} \times P_{c,SR_3D}\big] + P_{s,SR_1R_2R_4D}|_{\neq}\Big(P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2} \times P_{s,SR_3D}|_{2bit} +$$

$$P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big) + P_{s,SR_1R_2R_4D}|_{1bit}\big(P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} +$$

$$P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=x_2}\big) \times \frac{1}{2}P_{s,SR_3D}|_{1bit}\Big\}. \tag{106}$$

Also, the probability that R_4 is detected as an adversary when $x_1 = -x_2$ is

$$P_{D,R_4}|_{x_1=-x_2} = P_{c,SR_1D}\left\{P_{c,SR_1R_2R_4D}\left[\left(2P_{s,SR_2R_3R_5D}|_{-2 \quad x_1=-x_2} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2}\right)\times\right.\right.$$

$$\left.\frac{1}{2}P_{s,SR_3D}|_{1bit}\right] + P_{s,SR_1R_2R_4D}|_{\neq}\left(P_{s,SR_2R_3R_5D}|_{-2 \quad x_1=-x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{c,SR_2R_3R_5D}|_{x_1=-x_2} \times\right.$$

$$\left.\left.P_{c,SR_3D}\right) + P_{s,SR_1R_2R_4D}|_{1bit}\left(P_{c,SR_2R_3R_5D}|_{x_1=-x_2} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2}\right)P_{c,SR_3D}\right\} +$$

$$P_{s,SR_1D}\left\{P_{s,SR_1R_2R_4D}|_{1bit}\left[\left(2P_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2}\right)\times\frac{1}{2}P_{s,SR_3D}|_{1bit}\right] +\right.$$

$$P_{s,SR_1R_2R_4D}|_{\neq}\left(P_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + P_{c,SR_2R_3R_5D}|_{x_1=-x_2} \times P_{s,SR_3D}|_{2bit}\right) +$$

$$\left.P_{c,SR_1R_2R_4D}\left(P_{c,SR_2R_3R_5D}|_{x_1=-x_2} + P_{s,SR_2R_3R_5D}|_{\neq \quad x_1=-x_2}\right)P_{s,SR_3D}|_{2bit}\right\}. \tag{107}$$

At last, the probability that R_5 is detected as an adversary when $x_1 = x_2$ is

$$P_{D,R_5}|_{x_1=x_2} = P_{c,SR_1D}\left\{P_{c,SR_1R_2R_4D}\left[\left(1 - P_{c,SR_2R_3R_5D}|_{x_1=x_2}\right)P_{c,SR_3D} + P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2} \times\right.\right.$$

$$\left.P_{s,SR_3D}|_{1bit}\right] +$$

$$P_{s,SR_1R_2R_4D}|_{1bit}\left[P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2} \times P_{c,SR_3D} + \left(1 - P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2}\right)\times\right.$$

$$\left.\frac{1}{2}P_{s,SR_3D}|_{1bit}\right] + P_{s,SR_1R_2R_4D}|_{\neq}\left(P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2} + P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2}\right)P_{c,SR_3D}\Big\} +$$

$$P_{s,SR_1D}\left\{P_{s,SR_1R_2R_4D}|_{1bit}\left[\left(1 - P_{s,SR_2R_3R_5D}|_{2bit \quad x_1=x_2}\right)P_{s,SR_3D}|_{2bit} + P_{c,SR_2R_3R_5D}|_{x_1=x_2} \times\right.\right.$$

$$\left.P_{s,SR_3D}|_{1bit}\right] + P_{c,SR_1R_2R_4D}\left[P_{c,SR_2R_3R_5D}|_{x_1=x_2} \times P_{s,SR_3D}|_{2bit} + \left(1 - P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2}\right)\times\right.$$

$$\left.\left.\frac{1}{2}P_{s,SR_3D}|_{1bit}\right] + P_{s,SR_1R_2R_4D}|_{\neq}\left(P_{c,SR_2R_3R_5D}|_{x_1=x_2} + P_{s,SR_2R_3R_5D}|_{1bit \quad x_1=x_2}\right)P_{s,SR_3D}|_{2bit}\right\} \tag{108}$$

and the probability that R_5 is detected as an adversary when $x_1 = -x_2$ is

$$P_{D,R_5}|_{x_1=-x_2} = P_{c,SR_1D}\left\{P_{s,SR_1R_2R_4D}|_{1bit}\left[\left(1 - P_{s,SR_2R_3R_5D}|_{-2 \quad x_1=-x_2}\right)\times\frac{1}{2}P_{s,SR_3D}|_{1bit} +\right.\right.$$

$$\left.P_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2} \times \left(1 - P_{s,SR_3D}|_{1bit}\right)\right] +$$

$$P_{c,SR_1R_2R_4D}\left[P_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2} \times \frac{1}{2}P_{s,SR_3D}|_{1bit} + \left(1 - P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\right)P_{c,SR_3D}\right] +$$

$$P_{s,SR_1R_2R_4D}|_{\neq}\left(P_{c,SR_2R_3R_5D}|_{x_1=-x_2} + P_{s,SR_2R_3R_5D}|_{2 \quad x_1=-x_2}\right)\times\frac{1}{2}P_{s,SR_3D}|_{1bit}\Big\} +$$

$$P_{s,SR_1D}\left\{P_{c,SR_1R_2R_4D}\left[\left(1-P_{s,SR_2R_3R_5D}|_{2\quad x_1=-x_2}\right)\times\frac{1}{2}P_{s,SR_3D}|_{1bit}+P_{s,SR_2R_3R_5D}|_{-2\quad x_1=-x_2}\left(1-\right.\right.\right.$$

$$\left.\left.\left.P_{s,SR_3D}|_{1bit}\right)\right]+\right.$$

$$P_{s,SR_1R_2R_4D}|_{1bit}\left[P_{s,SR_2R_3R_5D}|_{-2\quad x_1=-x_2}\times\frac{1}{2}P_{s,SR_3D}|_{1bit}+\right.$$

$$\left.\left(1-P_{c,SR_2R_3R_5D}|_{x_1=-x_2}\right)P_{s,SR_3D}|_{2bit}\right]+$$

$$P_{s,SR_1R_2R_4D}|_{\neq}\left(P_{c,SR_2R_3R_5D}|_{x_1=-x_2}+P_{s,SR_2R_3R_5D}|_{-2\quad x_1=-x_2}\right)\times\frac{1}{2}P_{s,SR_3D}|_{1bit}\Big\}. \tag{109}$$

Therefore, the probability of each node being detected as an adversary is

$$P_{D,R_i}=\frac{1}{2}\left(P_{D,R_i}|_{x_1=x_2}+P_{D,R_i}|_{x_1=-x_2}\right)\quad i=1,2,\cdots,5. \tag{110}$$

Finally, a false alarm occurs when the system detects one of the nodes as an adversary when actually no adversary exists. The probability of false alarm can be written as

$$P_{FA}=\sum_{i=1}^{5}P_{D,R_i}|_{NA} \tag{111}$$

The average probability of successful detection of the system is

$$P_D=\frac{1}{5}\sum_{i=1}^{5}P_{D,R_i}|_{R_i} \tag{112}$$

CHAPTER 5

SIMULATION

This section discusses how the entire scheme is simulated and compared with the approximated theoretical equations that were derived in Chapter 4. Ten million samples were simulated using a Monte Carlo trail in each SNR in each case. All cases were simulated under a Rayleigh fading channel, assuming that each node, including the destination, knows the channel perfectly and the signal is detected coherently.

The first simulation compares the performance of each branch. Figure 5.1 shows that the derived equation and the simulation result perfectly match each other.

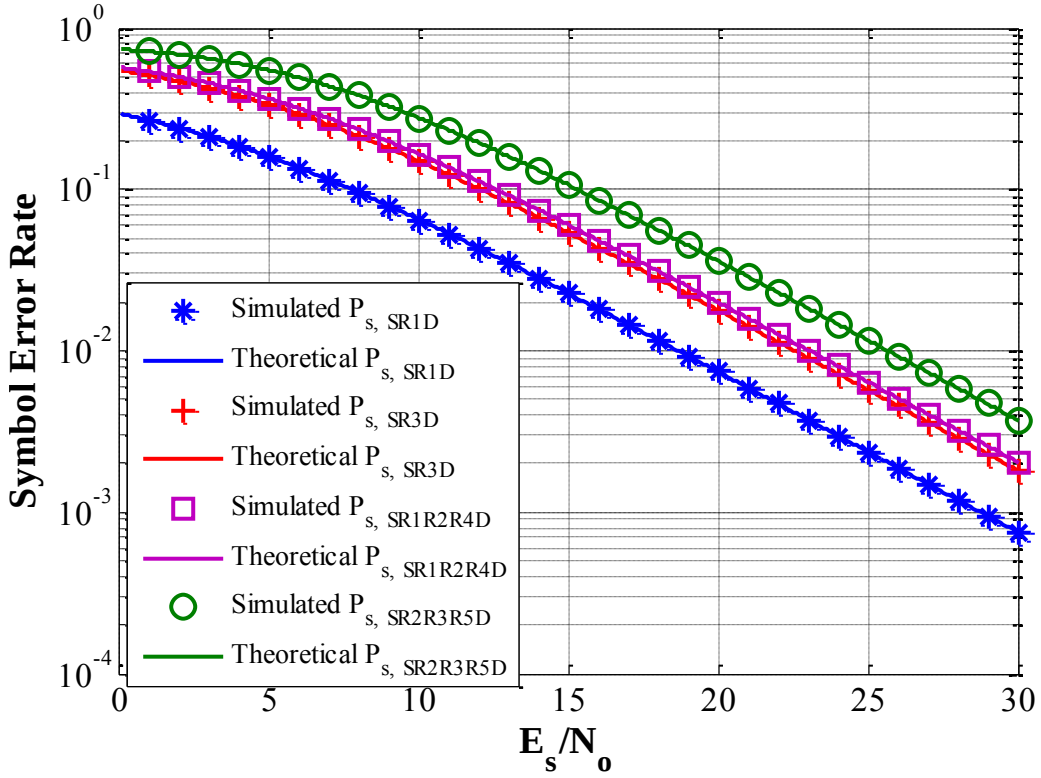


Figure 5.1: Theoretical analysis and simulated result of symbol error rate for four branches of cockroach network.

The next simulation is the bit error rate comparison between no adversary and the presence of each adversary. From the result, Figure 5.2 shows that the R_5 node has the least

influence if it is infected, and R_3 is affected most if attacked. Overall, the SNR losses range from 4 to 10 dB if attacked by an adversary; however, the probability of error could be reduced in a high SNR. Also, the theoretical BER in BPSK under Rayleigh fading channel is inserted in this figure as a reference.

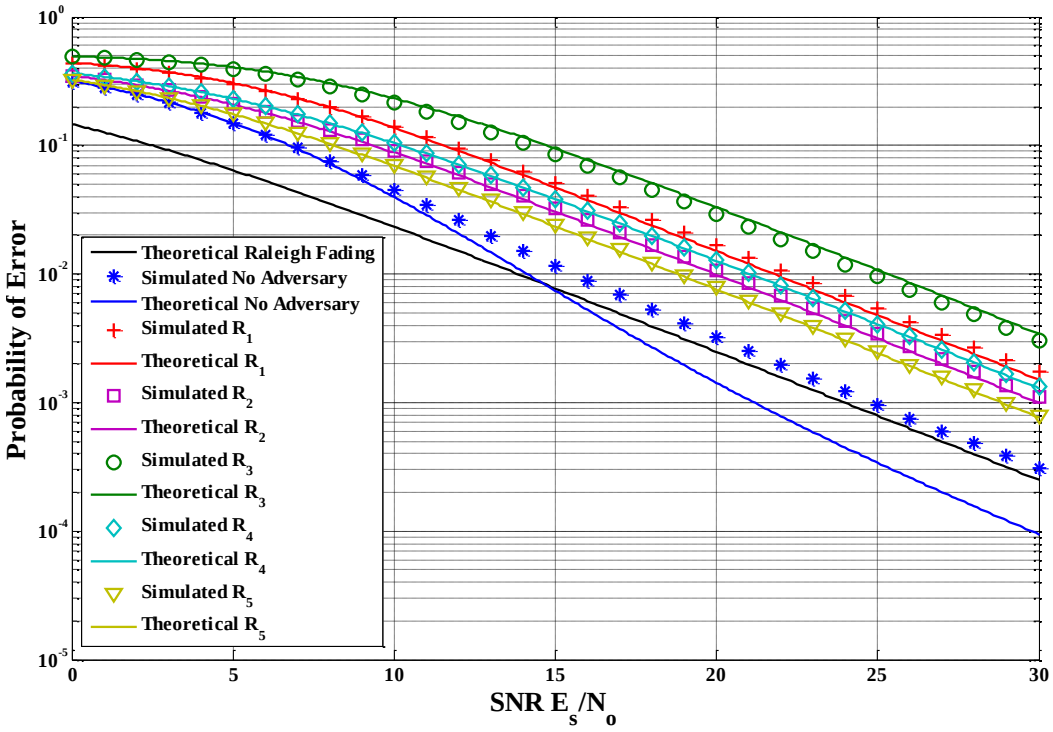
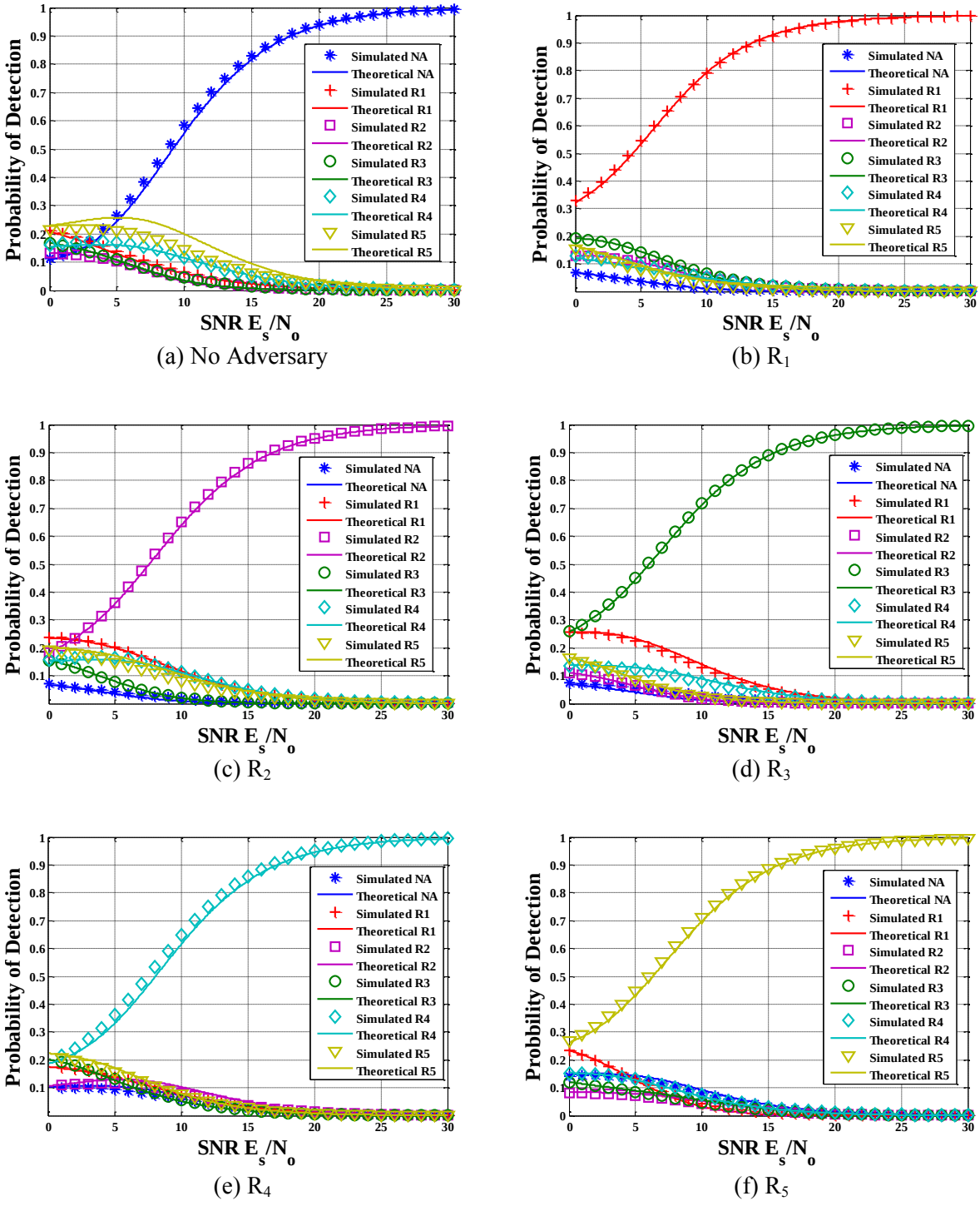


Figure 5.2: Comparison of BER among no-adversary cases, R_1 to R_5.

Note that there is a gap between the theoretical and simulated results for the no-adversary case, mainly due to the dependency of the branches. For example, under the no-adversary case, if R_2 makes a decoding error, then R_4 and R_5 receive and forward the wrong message as well. Similarly, if R_3 makes an error, then this causes the error to be broadcast to both R_5 and the destination. However, R_1 will not cause a dependence issue, because this relay sends two independent messages to two different nodes.

Another comparison involves the probability of detection for each presence of an adversary. Figure 5.3 shows the approximated analysis compared to the simulation in linear scale,

indicating that successful detection is achieved more that 50% of the time when the SNR is 10 dB, and that rate reaches 100% at 20 dB. These results are displayed in log-scale in Figure 5.4.

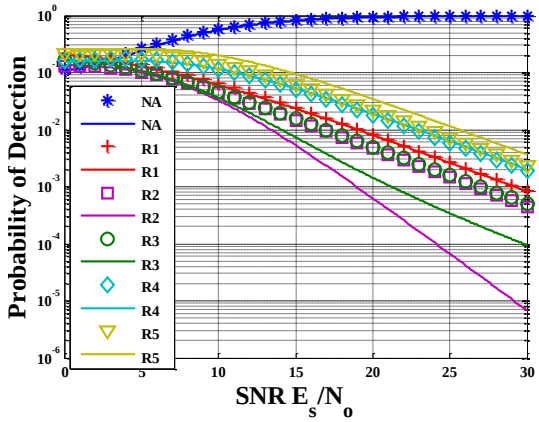


(a) No Adversary (b) R_1

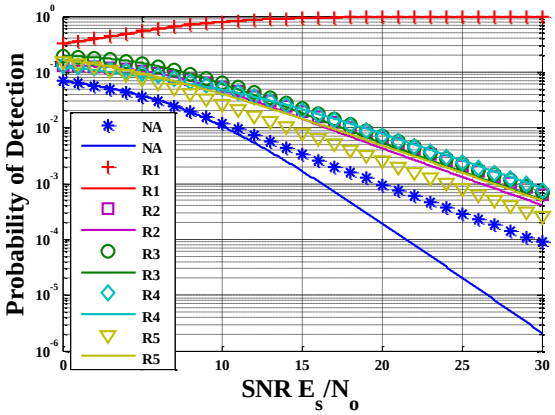
(c) R_2 (d) R_3

(e) R_4 (f) R_5

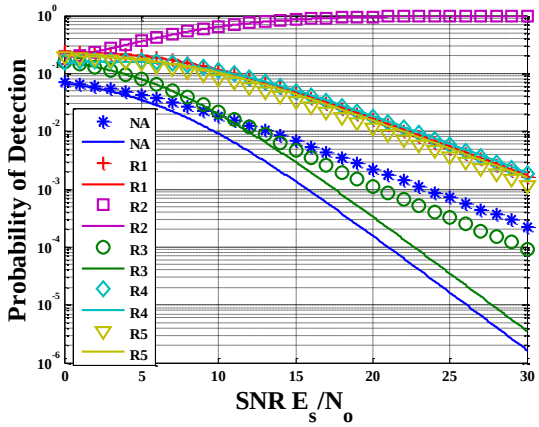
Figure 5.3: Probability of detection for no-adversary cases, R_1 to R_5, in linear scale.



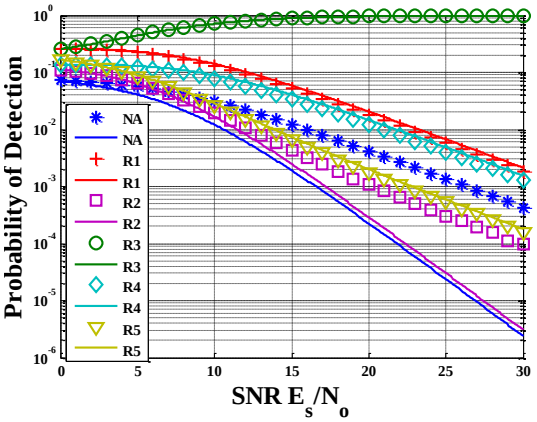
(a) No Adversary



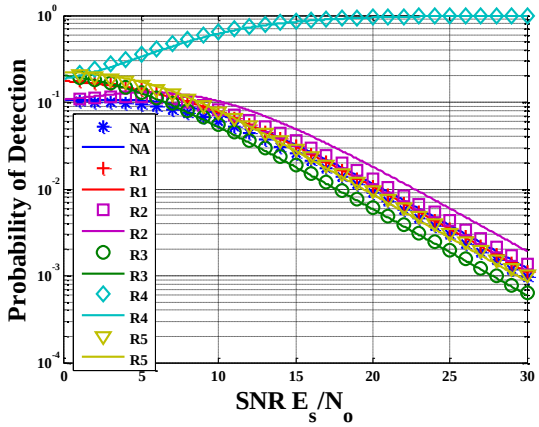
(b) R_1



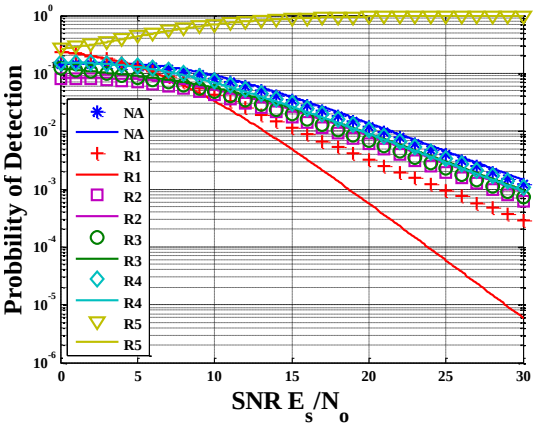
(c) R_2



(d) R_3



(e) R_4



(f) R_5

Figure 5.4: Probability of detection for no-adversary cases, R_1 to R_5, in log scale.

CHAPTER 6

CONCLUSION

This paper presented further work on the cockroach network system. By building this model in a wireless telecommunication system, thermal noise, channel fading, and modulation are added to the system to approach reality. Bit error rate and probability of detection were examined in order to show the capability of the system under new conditions.

Analyses on the probability of error and the probability of adversary detection were conducted in order to examine network performance. Several theoretical equations obtained by taking approximations were verified by results of the simulation.

Relative to the performance of the cockroach network system and from the point of view of the probability of error, it was observed that the system suffers some losses in decibels when an adversary exists. However, with the assistance of logic and an algorithm suggested here in this dissertation, the error rate could be reduced when the signal-to-noise ratio is increased. Also, the accuracy of adversary detection increased when the SNR increased.

In future work, a receiver operation characteristic (ROC) will be introduced into the analysis. This signal detection method provides a plot that optimizes the performance of a system by adjusting the determination threshold, thereby possibly improving the accuracy and sensitivity of the system.

In addition, with a new logic and algorithm, a smart adversary will be introduced in order to bring more challenge into the system. This smart adversary could be used to play any number of tricks in order to fool detection so that it can remain secret. In this case, more advanced tactics and strategies at the receiver will be required to overcome this issue.

REFERENCES

REFERENCES

[1] O. Kosut, L. Tong, and D. Tse, "Nonlinear network coding is necessary to combat general Byzantine attacks," in *Proceedings of IEEE 4th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 30–October 2, 2009, pp. 593–599.

[2] O. Kosut, L. Tong, and D. Tse, "Polytope codes against adversaries in networks," *Proceedings of 2010 IEEE International Symposium on Information Theory (ISIT)*, Vol. 60, No. 6, pp. 2423–2427, June 2013.

[3] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, Vol. 4, pp. 382–401, 1982.

[4] D. Dolev, "The Byzantine generals strike again," *Journal of Algorithms*, Vol. 3, No. 1, pp. 14–30, 1982.

[5] A. Vempaty, O. Ozdemir, K. Agrawal, H. Chen, and P. K. Varshney, "Localization in wireless sensor networks: Byzantines and mitigation techniques," *IEEE Trans. Signal Processing*, Vol. 61, No. 6, pp. 1495–1508, March 2013.

[6] A. Vempaty, Y. S. Han, and P. K. Varshney, "Target localization in wireless sensor networks using error correcting codes in the presence of Byzantines," in *Proceedings of International Conference on Acoustics, Speech, and Signal Processing (ICASSP2013)*, Vancouver, Canada, May 2013.

[7] A. Vempaty, Y. S. Han, and P. K. Varshney, "Byzantine tolerant target localization in wireless sensor networks over non-ideal channels," in *Proceedings of 13th IEEE International Symposium on Information Theory (ISIT),* Istanbul, Turkey, Sept. 2013, pp. 407–411.

[8] A. Vempaty, Y. S. Han, and P. K. Varshney, "Target localization in wireless sensor networks using error correcting codes," *IEEE Transactions on Information Theory*, Vol. 60, No. 1, pp. 697-712, January 2014.

[9] J. Zhang and R. S. Blum, "Distributed estimation in the presence of attacks for large scale sensor networks," 48th Annual Conference on Information Sciences and Systems, Princeton, New Jersey, March 2014.

REFERENCES (continued)

[10] J. Zhang, R. S. Blum, X. Lu, and D. Conus, "Asymptotically optimum distributed estimation in the presence of attack," *IEEE Trans. Signal Processing*, Vol. 63, No. 5, pp. 1086-1101, March 1, 2015.

[11] G. Liu, H. Liu, H, Chen, J. Xiang, and Z. Xiao, "Channel Aware Adaptive Quantization for Target Localization in Wireless Sensor Networks," IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE), Baltimore, MD, Nov. 2013.

[12] V. S. S. Nadendla, Y. S. Han, and P. K. Varshney, "Distributed Inference with M-ary quantized data in the presence of Byzantine attacks," *IEEE Trans. Signal Processing*, Vol. 62, No. 10, pp. 2681-2695, May 15, 2014

[13] X. He and A. Yener, "Strong secrecy and reliable byzantine detection in the presence of an untrusted relay," *IEEE Transactions on Information Theory*, Vol. 59, No. 1, pp. 177-192, January 2013.

[14] E. Graves and T. Wong, "A coding approach to guarantee information integrity against a Byzantine relay," *Proceedings of 13th IEEE International Symposium on Information Theory (ISIT),* Istanbul, July 2013, pp. 2780-2784.

[15] O. Kosut and J. Kliewer, "Equivalence for networks with adversarial state," IEEE International Symposium on Information Theory (ISIT), Honolulu, Hawaii, June 2014.

[16] G. Liang and N. Vaidya, "Capacity of Byzantine agreement with finite link capacity," IEEE Proceedings of INFOCOM, Shanghai, China, April 2011.

[17] M. Bakshi, M. Effros, and T. Ho, "On equivalence for networks of noisy channels under Byzantine attacks," IEEE International Symposium on Information Theory Proceedings (ISIT), St. Petersburg, July 2011.

[18] J. G. Proakis, *Digital Communication*, 4th Ed. New York: McGraw-Hill, 2001.

[19] J. G. Proakis, M. Salehi, and G. Bauch, *Contemporary Communication Systems Using MATLAB® and Simulink®*, 2nd Ed. Thomson-Brooks/Cole, 2004.

[20] A. Papoulis and S. U. Pillai, Probability, *Random Variables and Stochastic Process*, 4th Ed. New York: McGraw-Hill, 2002.

APPENDIX

APPENDIX

PROOF OF EQUATION (24)

By referring to the three symbols of orthogonal frequency-division multiplexing (OFDM), bit error rate analysis of Proakis [18], and the integration method described in Papoulis [20], the following is the proof of equation (24).

$$P_{s,R_4D} = \int_0^\infty \int_{-\infty}^\infty \{1-[1-Q(t)]^2\} \frac{1}{\sqrt{2\pi}} e^{-\frac{(3SNRh)^2}{2}} dt\, e^{-h} dh$$

$$= \int_{-\infty}^\infty \{1-[1-Q(t)]^2\} \int_0^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{(3SNRh)^2}{2}} e^{-h} dh\, dt$$

$$= \int_{-\infty}^\infty \{1-[1-Q(t)]^2\} \int_0^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} e^{\left(\frac{1}{2}\sqrt{\frac{3SNR}{\frac{3}{2}SNR+1}}t\right)^2} e^{-\left(\sqrt{\frac{3}{2}SNR+1}\sqrt{h}-\frac{1}{2}\sqrt{\frac{3SNR}{\frac{3}{2}SNR+1}}t\right)^2} dh\, dt$$

Let $\frac{u}{\sqrt{2}} = \sqrt{\frac{3}{2}SNR+1}\sqrt{h} - \frac{1}{2}\sqrt{\frac{3SNR}{\frac{3}{2}SNR+1}}t$

$$\therefore P_{s,R_4D} = \int_{-\infty}^\infty \{1-[1-Q(t)]^2\} \frac{1}{\sqrt{2\pi}} e^{-\frac{z^2}{2}} \frac{1}{\frac{3}{2}SNR+1} \left[1 + e^{\frac{1}{2}\frac{3SNR}{3SNR+2}z^2} \sqrt{\frac{3SNR}{3SNR+2}} z\sqrt{2\pi} Q\left(-\sqrt{\frac{3SNR}{3SNR+2}} z\right)\right] dz$$