IOWA STATE UNIVERSITY
Digital Repository

Graduate Theses and Dissertations

Iowa State University Capstones, Theses and Dissertations

2015

The crypto-aided physical layer integrity check in cooperative relaying communication

Xudong Liu
Iowa State University

Follow this and additional works at: https://lib.dr.iastate.edu/etd

 Part of the Electrical and Electronics Commons

Recommended Citation
Liu, Xudong, "The crypto-aided physical layer integrity check in cooperative relaying communication" (2015). *Graduate Theses and Dissertations*. 14500.
https://lib.dr.iastate.edu/etd/14500

This Thesis is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.

www.manaraa.com

The crypto-aided physical layer integrity check in cooperative relaying communication

by

Xudong Liu

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Electrical Engineering

Program of Study Committee:
Sang W. Kim, Major Professor
Yong Guan
Thomas Daniels

Iowa State University

Ames, Iowa

2015

Copyright © Xudong Liu, 2015. All rights reserved.

www.manaraa.com

TABLE OF CONTENTS

www.manaraa.com

www.manaraa.com

LIST OF FIGURES

www.manaraa.com

ACKNOWLEDGMENTS

This thesis cannot be finished without help from my committee. Here I would like to thank my committee chair Dr. Sang. W Kim and committee members Dr. Yong Guan and Dr. Thomas Daniels with my highest sincerity for their guidance and support throughout the course of this research.

I would like to thank my parents, it is also their support and encouragement that make me finish the research and thesis.

Also I would like to thank my friend Wang Liao for help solving the technique issues I met. And thank the all the other two students Hien Tai and Mouhamadou Diallo who in the same research group for giving me helpful suggestions.

In addition, I would also like to thank all my friends, colleagues, the department faculty and staff for making my time at Iowa State University a wonderful experience.

www.manaraa.com

ABSTRACT

In the cooperative relaying communication, the system has to defend itself against the eavesdropper which may undermines the message integrity by sending the modified messages. We propose a physical layer integrity check scheme for cooperative relaying communication, where a source broadcast the signals to both destination target and an untrustworthy relay node. The approach exploits physical layer signals in detecting the modified messages conducted by the relay. We develop a scheme that utilizes a few cryptography information in the initial message packets to estimate the optimal detecting threshold. By applying the optimal detecting method, the proposed approach achieves almost same performance provided by perfect cryptography strategy that can detect all the modified messages but with high computational cost caused by applying cryptographic encryption to all the transmitted messages.

Keywords—physical layer, integrity check; modified messages; cryptography; optimal detecting threshold.

www.manaraa.com

CHAPTER 1: OVERVIEW

1.1 Introduction

With rapidly developing of wireless networks and signal processing techniques, the cooperative relaying communication [1] has been widely applied to many scenarios such as distributed sensors and cooperative nodes group [2] [3]. It has gained considerable attention in the literatures as a promising next generation wireless network [4].

Because of its inherent vulnerable nature, it is easy for eavesdropper to monitor the signals in the transmit path or intercept the messages. Thus substantial researches have been conducted to develop the techniques to guarantee the security requirement. And many physical layer approaches with lower computation cost and less protocol overhead [5] have been developed [6]. However, because of the highly development of cryptography algorithm, little attention has been paid to the integrity issues such as 'Man In the Middle attack' or malicious relay disruption [7], especially less researches have been conducted to exploit the physical layer property to accomplish the integrity check. In general, the advanced cryptographic algorithm requires more computation resource, so it is hard to apply to wireless networks where the destination nodes are resource constrained [8]. In this Thesis, instead of achieving security by merely transmitting highly encrypted messages [9] which consume a lot computational resource, we proposed a scheme that exploits the physical layer signals in detecting messages modification conducted by relay. Our results shows by applying optimal detecting threshold method, the proposed approach can achieves almost same performance provided by perfect cryptography strategy that can remove all the modified messages from relay.

www.manaraa.com

1.2 Thesis organization

This thesis is organized as follows, chapter 2 describes the system model been investigated, where source transmit messages to destination target. But due to channel poor quality between them, source also broadcast the signal to a near relay node and Let node help relaying the message to destination target. However since the relay is untrustworthy, it may forward modified messages to the destination to undermine the information integrity. And we analyze the error probability of system model based on the different detection results. In chapter 3, we proposed an optimal detection method to detect the modified messages in the physical layer by exploiting the hamming distance [10] property between channel codewords. This is followed with the theoretical analysis for applying optimal detecting threshold. Since the calculation of optimal detecting threshold requires the pre-knowledge of the attack probability, a cryptography-aided estimation strategy of attack probability is developed. The numerical results and conclusions are in chapter 4 and chapter 5 respectively.

www.manaraa.com

CHAPTER 2
THE COOPERATIVE COMMUNICATION

2.1 Problem statement

In cooperative relaying communication, the source transmitter broadcasts the message to the destination target. Sometimes the destination target is far away from the source transmitter or there are obstacles standing between them, these all will cause the channel gain decreasing significantly [11]. If the destination only decodes the message based on the signal overheard from the source, the probability of decoding error would is high. In order to avoid this situation, the source would choose a relay node [12] and also broadcasts the signals to it. Since the channel gain between relay and destination is efficiently high, relay will re-transmit the signals to the destination and destination can combine both identical signals together to decode the message. However, the source cannot guarantee all the relays in networks are trustworthy, so there is a high chance that relay node will modify the original message from source and sends another different message to the destination. If destination decodes the message based on modified signals, the probability of decoding error is much higher than just decoding signal from the source even if source-to-destination channel quality is poor. Thus destination has to check the message integrity by applying some detection techniques. Ideally this goal can be achieved if we encrypt all the messages by advanced cryptography, but compared with physical layer detection method, the computational cost of cryptography is much higher, so it is valuable to develop an approach in physical layer.

www.manaraa.com

2.2 System model

The system model being investigated is shown in Fig. 1. We consider the situation that source wishes to send message to the destination, but the channel quality between is poor due to the long distance between. So source transmitter also broadcasts signals to an untrustworthy relay and relay forward it to the destination. The S is the Source broadcaster, R represents intermediate Relay and D is Destination receiver. For simplicity, the system uses BPSK modulation mode.

Here S is designed based on the channel BCH (n, k) code [13], one of CEC (Cyclic Error-Correcting) channel code [14], let t denotes the CEC channel code's self-correct ability, it is to say if the erroneous bits in codeword is less than t bits, if could be automatically corrected.

In the first phase, S encodes the k-bits length original message m into an n-bits length codeword X, then broadcast X to relay and destination simultaneously. In phase 2, relay retransmit X to D, and we assume relay always receives X from source correctly because of the short distance between them. Last phase destination generates the decoded codeword $\hat{X}$ based on the signals received from relay and destination. And the decoded message $\hat{m}$ can be obtained by passing $\hat{X}$ through the BCH decoder.

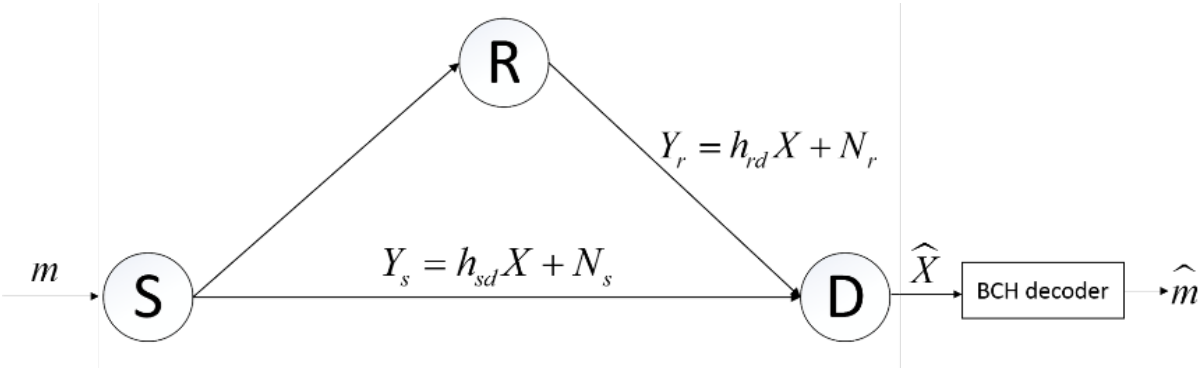

Figure 1. *The cooperative relaying model*

www.manaraa.com

As the we discussed in the chapter 2.1, the untrustworthy relay holds malicious intension, it may modifies X into another codeword X_r with probability α. Let $Y_s = h_{sd}X + N_s$ be the signal received from source and $Y_r = h_{rd}X_r + N_r$ be the signal received from the relay. Where $h_{sd} \sim CN(0, \sigma_s^2)$ and $h_{rd} \sim CN(0, \sigma_r^2)$ represent the channel fading coefficients respectively. Because the channel quality of relay-to-destination is better compared with the channel quality of source-to-destination, usually channel gain $\sigma_1^2 < \sigma_2^2$, N_s and N_r are the additive white Gaussian noise (AWGN) with the variance N_0, the transmit SNR is ε_b/N_0.

We already know if system decodes message based on modified codeword Y_r and original codeword Y_s, the probability of decoding error is efficiently high. In next section we describe the physical layer method that detects the integrity of Y_r, and Y_r is discarded if detection determines it contains the modified X_r, Otherwise Y_s and Y_r are combined together by applying the MRC [15] (Maximal-ratio combining) rule to improve the received SNR (signal noise ratio).

2.3 The detection method

Since source encodes the message by using BCH (n, k) code, let $X + E_s$ and $X + F + E_r$ denote two k-bits length vector corresponding to the source's Y_s and relay's Y_r respectively. Where " $+$ " represents XOR operation and F is the modification vector generated by relay. E_s and E_r are just "random error vector" represent Gaussian noise N_s and N_r respectively.

In general, $X + F$ must be a valid codeword in the designed BCH (n, k) codebook, or it will be abandoned as corrupt codeword due to the invalidity of channel code. Furthermore the relay should chooses the most similar codeword to original one. Since the noise exists, the

www.manaraa.com

more similarity between $X + F$ and X, the lower chance $X + F$ will be detected as a modified codeword.

So based on discussion above, define $W(X)$ be the hamming weight (the total bit 1s in binary vector) calculation function of X . The relay's "behavior" can described as below:

Relay may modifies the original codeword X into another valid codeword $X + F$ with the probability α. And$W(F) = d_{min}, if\ F \neq 0$, where d_{min} is the minimal hamming distance between two codewords. Let:

H_0 denotes the event that relay not modify X, so $F = 0$.

H_1 denotes the event that relay does modify X, so $F \neq 0$.

So we construct a hypothesis test [16] that compares the hamming distance between codeword $X + E_s$ sent by source and $X + F + E_r$ sent by relay, if the hamming distance is no less than some threshold δ, we decide there is an attack and reject event H_0, otherwise accept event H_0:

$$\begin{aligned} \hat{H}_1 &: W\left[\left(X + E_s\right) + \left(X + F + E_r\right)\right] \geq \delta \\ \hat{H}_0 &: W\left[\left(X + E_s\right) + \left(X + F + E_r\right)\right] < \delta \end{aligned} \tag{1}$$

if we assume $E = E_s + E_r$, then (1) equivalents to

$$\begin{aligned} \hat{H}_1 &: W\left(F + E\right) \geq \delta \\ \hat{H}_0 &: W\left(F + E\right) < \delta \end{aligned} \tag{2}$$

Under $\hat{H}_0$, destination combines Y_s and Y_r using MRC rule to increase the received SNR; under $\hat{H}_1$, the relay's Y_r is discarded and the message is decoded based on Y_s only.

Next section, we derive the decoding error based on the different detection results, for convince, the notation symbols used in the derivation is listed in appendix A.

www.manaraa.com

2.4 The probability of decoding error

In chapter 2.3, we know detection determine whether to combine Y_s with Y_r or not. If detection result is $\hat{H}_1$, the message only is decoded based on Y_s; otherwise destination combines Y_s and Y_r using MRC rule to decode the message. Thus the average probability of decoding error can be expressed as:

$$\begin{aligned}&\Pr\left(\hat{m} \neq m\right)\\&= P\left(\hat{m} \neq m|\hat{H}_1\right)P\left(\hat{H}_1\right) + P\left(\hat{m} \neq m|\hat{H}_0, H_0\right)P\left(\hat{H}_0, H_0\right) + P\left(\hat{m} \neq m|\hat{H}_0, H_1\right)P\left(\hat{H}_0, H_1\right)\end{aligned} \tag{3}$$

the three terms in (3) actually represent three condition decoding errors, from left to the right in (3) are ordered by: decoding error of modification decision; decoding error of correct detection and decoding error of miss detection.

And we assume the system uses BPSK modulation mode, from [17] let

$$\begin{aligned}e_s &= \frac{1}{2}\left(1 - \sqrt{\frac{\overline{\gamma_s}}{1+\overline{\gamma_s}}}\right)\\e_r &= \frac{1}{2}\left(1 - \sqrt{\frac{\overline{\gamma_r}}{1+\overline{\gamma_r}}}\right)\end{aligned} \tag{4}$$

denote the bit error probability in the source-to-destination channel and the relay-to-destination channel respectively, where

$$\begin{aligned}\overline{\gamma_s} &= \mathrm{E}(|h_{sd}|^2)\frac{\varepsilon_b}{N_0} = \sigma_s^2\frac{\varepsilon_b}{N_0}\\\overline{\gamma_r} &= \mathrm{E}(|h_{rd}|^2)\frac{\varepsilon_b}{N_0} = \sigma_r^2\frac{\varepsilon_b}{N_0}\end{aligned} \tag{5}$$

www.manaraa.com

are the average received SNR respectively. Then the probability e of a bit in vector $E = E_s + E_r$ is 1 is given by

$$e = e_s(1-e_r) + (1-e_s)e_r = e_s + e_r - 2e_s e_r \tag{6}$$

Next section we derive the decoding error of modification decision, the decoding error of correct detection and the decoding error of miss detection respectively.

2.4.1 Decoding error of modification decision

Given $\hat{H}_1$, Y_r is discarded and the message is decoded based the Y_s only. Since the bit error probability (before decoding) of the source-to-destination channel is e_s and error correction ability

is t, the probability of decoding error is given by

$$P\left(\hat{m} \neq m | \hat{H}_1\right) = \sum_{i=t+1}^{n} \binom{n}{i} e_s^{\,i} (1-e_s)^{n-i} \tag{7}$$

the probability of deciding $\hat{H}_1$ is given by

$$P\left(\hat{H}_1\right) = P\left(\hat{H}_1, H_0\right) + P\left(\hat{H}_1, H_1\right) \tag{8}$$

where (probability of false alarm)

$$P\left(\hat{H}_1, H_0\right) = P(H_0) P\left(W(E) \geq \delta \mid H_0\right) = (1-\alpha) \sum_{i=\delta}^{n} \binom{n}{i} e^i (1-e)^{n-i} \tag{9}$$

and (probability of modification detection)

$$P\left(\hat{H}_1, H_1\right) = P(H_1) P\left(W(F+E) \geq \delta | H_1\right) = \alpha P\left(W(F+E) \geq \delta | H_1\right) \tag{10}$$

Let J denote the number of the 1's in F that are changed by E, so its probability mass function is given by

www.manaraa.com

$$P(J=j)=\binom{d_{min}}{j}e^{j}(1-e)^{d_{min}-j},\ 0\le j\le d_{min} \tag{11}$$

In order to get $W(F+E)\ge\delta$, we need at least $(\delta-d_{min}-J)$ 1's in the other positions (not the position where in F is 1) of E. However there are two special condition:

If $\delta-(d_{min}-J)\le 0$, then $W(F+E)\ge\delta$ already satisfied. The value of equation (11) equals to 1.

If $\delta-(d_{min}-J)>n-d_{min}$, then $W(F+E)<\delta$ can't be achieved. The value of equation (11) equals to 0.

so we obtain:

$$P(W(F+E)\ge\delta\mid J)=\begin{cases}1, & J\le n-\delta\\ 0, & J>n-\delta\\ \sum_{L=\delta-(d_{min}-J)}^{n-d_{min}}\binom{n-d_{min}}{L}e^{L}(1-e)^{n-d_{min}-L}, & O.W\end{cases} \tag{12}$$

Combine equation (7) and (10), the (9) equals to

$$P(\hat{H}_1,H_1)=\alpha\sum_{j=0}^{d_{min}}P(W(F+E)\ge\delta\mid J=j)P(J=j) \tag{13}$$

Therefore it follows from (7) (8) (9)and (12)

$$\begin{aligned}P(\hat{m}\ne m|\hat{H}_1)P(\hat{H}_1)&=\left[\sum_{i=t+1}^{n}\binom{n}{i}e_s^{\,i}(1-e_s)^{n-i}\right]\\ &\times\left[(1-\alpha)\sum_{i=\delta}^{n}\binom{n}{i}e^{i}(1-e)^{n-i}+\alpha\sum_{j=0}^{d_{min}}P(W(F+E)\ge\delta\mid J=j)P(J=j)\right]\end{aligned} \tag{14}$$

www.manaraa.com

2.4.2 Decoding error of correct detection

Given $(\hat{H}_0, H_0)$ which is the ideal situation for communication system and the message is decoded based on the MRC combining of Y_s and Y_r (unmodified). The bit error probability e_m of MRC combining of Y_s and Y_r is given by (26) in the Appendix A.

Therefore the probability of decoding error is

$$P\left(\hat{m} \neq m | \hat{H}_0, H_0\right) = \sum_{i=t+1}^{n} \binom{n}{i} {e_m}^i \left(1 - e_m\right)^{n-i} \tag{15}$$

Since

$$P\left(\hat{H}_0, H_0\right) = \left(1-\alpha\right) - P\left(\hat{H}_1, H_0\right) = \left(1-\alpha\right)\left[1 - \sum_{i=\delta}^{n} \binom{n}{i} e^i \left(1-e\right)^{n-i}\right] \tag{16}$$

We obtain

$$\begin{aligned} &P\left(\hat{m} \neq m | \hat{H}_0, H_0\right) P\left(\hat{H}_0, H_0\right) \\ &= \left[\sum_{i=t+1}^{n} \binom{n}{i} {e_m}^i \left(1-e_m\right)^{n-i}\right]\left(1-\alpha\right)\left[1 - \sum_{i=\delta}^{n} \binom{n}{i} e^i \left(1-e\right)^{n-i}\right] \end{aligned} \tag{17}$$

2.4.3 Decoding error of miss detection

The $(\hat{H}_0, H_1)$ (miss detection) is the worst case, the bit error probability e'_m of MRC combining of Y_s and Y_r is given by (29) in the Appendix B

Therefore the probability of decoding error is

$$P\left(\hat{m} \neq m | \hat{H}_0, H_1\right) = \sum_{i=t+1}^{n} \binom{n}{i} {e'_m}^i \left(1 - e'_m\right)^{n-i} \tag{18}$$

Since

www.manaraa.com

$$P\left(\hat{H}_0, H_1\right) = \alpha - P\left(\hat{H}_1, H_1\right) = \alpha\left[1 - \sum_{j=0}^{d_{min}} P\left(W\left(F+E\right) \geq \delta \mid J = j\right) P_J\left(J = j\right)\right] \quad (19)$$

We obtain

$$\begin{aligned} & P\left(\hat{m} \neq m | \hat{H}_0, H_1\right) P\left(\hat{H}_0, H_1\right) \\ & = \left[\sum_{i=t+1}^{n} \binom{n}{i} e_m^{'\,i} \left(1 - e_m^{'}\right)^{n-i}\right] \alpha\left[1 - \sum_{j=0}^{d_{min}} P\left(W\left(F+E\right) \geq \delta \mid J = j\right) P\left(J = j\right)\right] \end{aligned} \quad (20)$$

The $\Pr(\hat{m} \neq m)$ (average probability of decoding error) can be obtained by applying (14) (17) and (20) into equation (3). Since e_s, e_r, e_m and e'_m are the constant parameters which can be calculated based the transmit SNR, n and k are designed by the BCH code, the $\Pr(\hat{m} \neq m)$ is a function of the attack probability α and detection threshold δ. Next chapter we will describe the proposed optimal detection method that minimize the average probability of the decoding error.

www.manaraa.com

CHAPTER 3
THE COOPERATIVE COMMUNICATION

3.1 Optimal detection threshold

Since the goal of optimal detection is to minimize the $\Pr(\hat{m} \neq m)$ (average probability of decoding error). And from the analysis in the chapter 2, we know $\Pr(\hat{m} \neq m)$ is a function of α and δ, Then it is equivalent to find the optimal threshold $\delta_{opt}(\alpha)$ which satisfies:

$$\delta_{opt}(\alpha) \equiv \arg \ min_{\delta} \ \Pr(\hat{m} \neq m) \tag{21}$$

So given a specific value of attack probability α, the $\delta_{opt}(\alpha)$ can be obtained by exhaust search: changing δ from 0 to n and find the one that minimize the average probability of decoding error.

Fig. 2 illustrates the $\delta_{opt}(\alpha)$ versus α. And we compare situations $SNR = 5dB$ with $SNR = 20dB$.

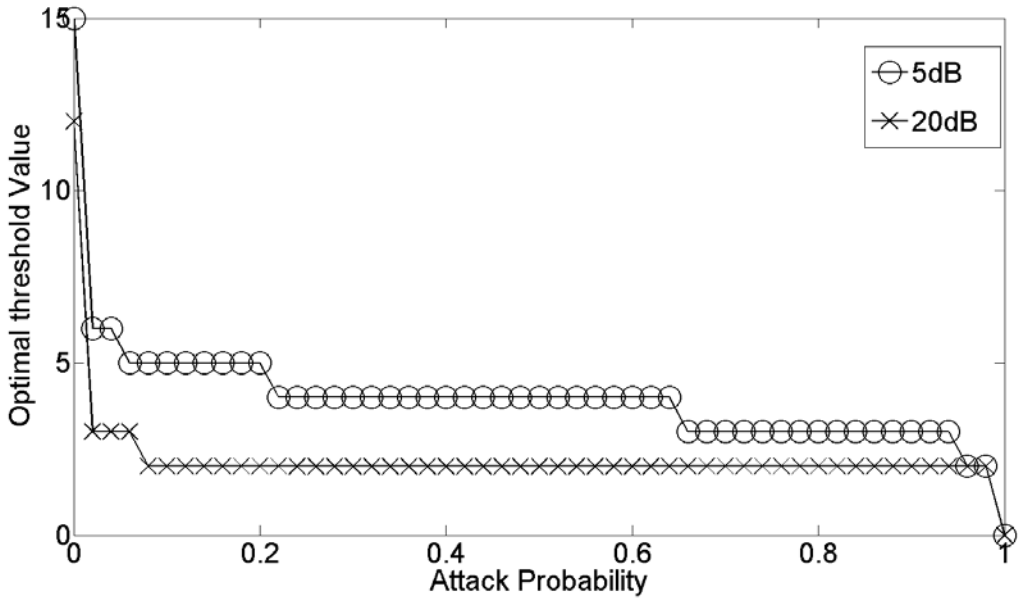

Figure 2. *Optimal threshold versus attack probability*

www.manaraa.com

It can be seen that the optimal threshold keep unchanged in certain range around attack probability. And higher attack probability produces a lower optimal detecting threshold value. Furthermore it can be observed that the optimal threshold becomes very robust against attack probability when transmit SNR achieve high level.

In conclusion, because α is a secret only known to relay and $\delta_{opt}(\alpha)$ depends on α, it is necessary to estimate α in finding optimal detecting threshold scheme, especially in the low transmit SNR case.

3.2 Crypto-aided estimation of attack probability

Since estimating the attack probability can help calculate the optimal detecting threshold, so we proposed a scheme that utilizes a few cryptographic [18] encrypted codewords in initial N codewords, which it used as the training reference to help estimating attack probability. Then use $\delta_{opt}(\hat{\alpha})$ to substitute $\delta_{opt}(\alpha)$ as the optimal threshold value for optimal detecting method.

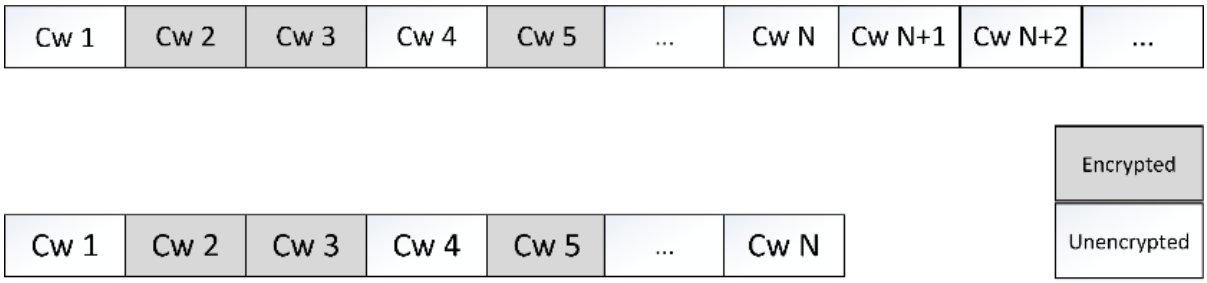

Figure 3. *The codewords forwarded by source transmitter*

As shown in Fig. 3, suppose source transmitter encrypt total number of N_c codewords by cryptography [19], and distributes these N_c codewords randomly into initial number of N codewords. We assume only source transmitter and destination know where those N_c

www.manaraa.com

encrypted codewords locate. Thus destination can directly know if these N_c codewords are modified or not once it receives first N codewords.

Take the timeliness issue into consideration, N usually be a small number (for example $N < 20$). Furthermore, set $N_c \ll N$ (for example $N_c = 2\sim6$) to reduce computation cost caused by cryptographic encryption.

The first step depicted in Fig. 4, destination check those N_c codewords and record the cryptographic outcomes in C. Where C is a length-N_c indicator vector whose element is 1 if the corresponding codeword is modified, otherwise it is 0.

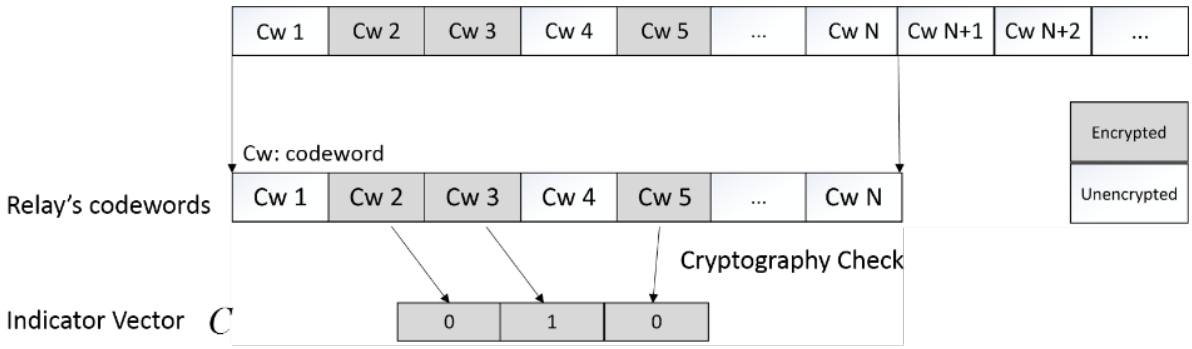

Figure 4. *Cryptography check for encrypted codewords*

Second step illustrated in Fig. 5, apply physical layer detection method to those N_c codewords. After compute the hamming weight $W(F+E)$ in (2), then record these hamming distance values in H. Where H is a length-N_c indicator vector whose element is the value of hamming weight $W(F+E)$.

Then compare H with threshold η to complete physical layer detection and record the detection results in C_η . Where C_η is a length-N_c indicator vector whose element is 1 if the detected codeword is determined been modified, otherwise it is 0. Vary η from 0 to n to

www.manaraa.com

complete the vectors set $\{C_0, C_1, C_2 \dots C_n\}$.

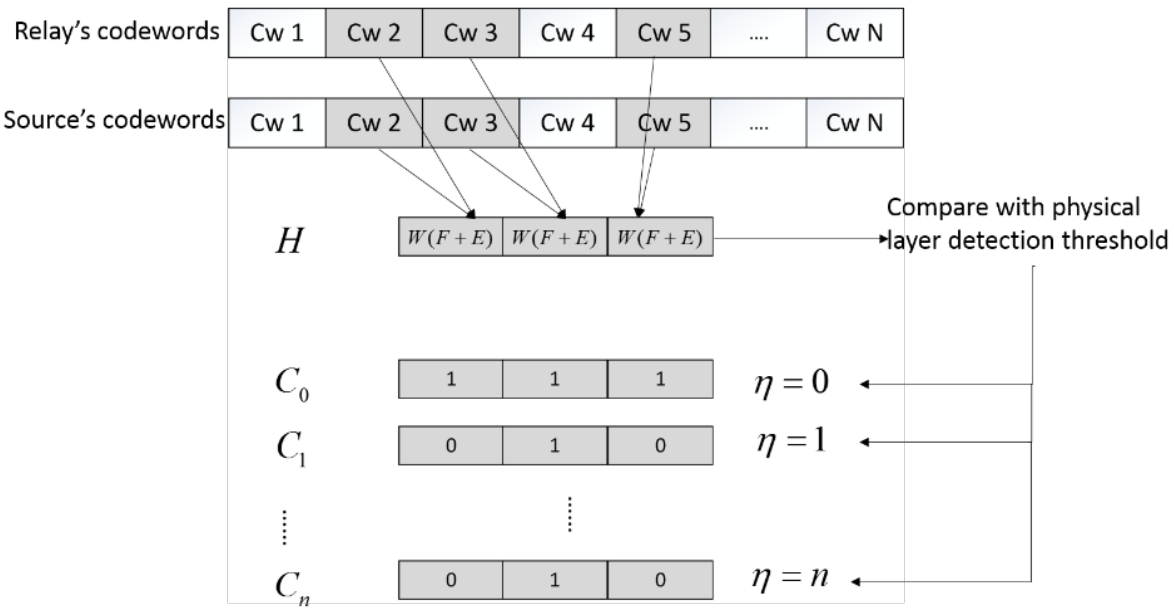

Figure 5. *Physical layer detection for encrypted codewords*

The third step, we calculate the hamming distance between vector C and $\{C_0, C_1, C_2 \dots C_n\}$ and choose the $\hat{\delta}$ satisfies

$$\hat{\delta} = \arg\ min_{0 \le \eta \le n} \ \left\{ W\left(C + C_\eta\right) \right\} \tag{22}$$

In case there are multiple $\hat{\delta}$ satisfy equation (22), depending on the situation, if the miss detection loss is more severe than false alarm does, system can choose the smallest δ_{min} to minimize the miss detection rate [19]. Otherwise choose the biggest $\hat{\delta}$ to minimize the false alarm rate.

Final step is drawn in Fig .6, apply physical layer detection to those $N - N_c$ unencrypted codewords with $\delta = \hat{\delta}$ in equation (2) and record the detection results in D. Where D is a length-$N - N_c$ indicator vector whose element is 1 if the detected codeword is determined been modified, otherwise it is 0.

www.manaraa.com

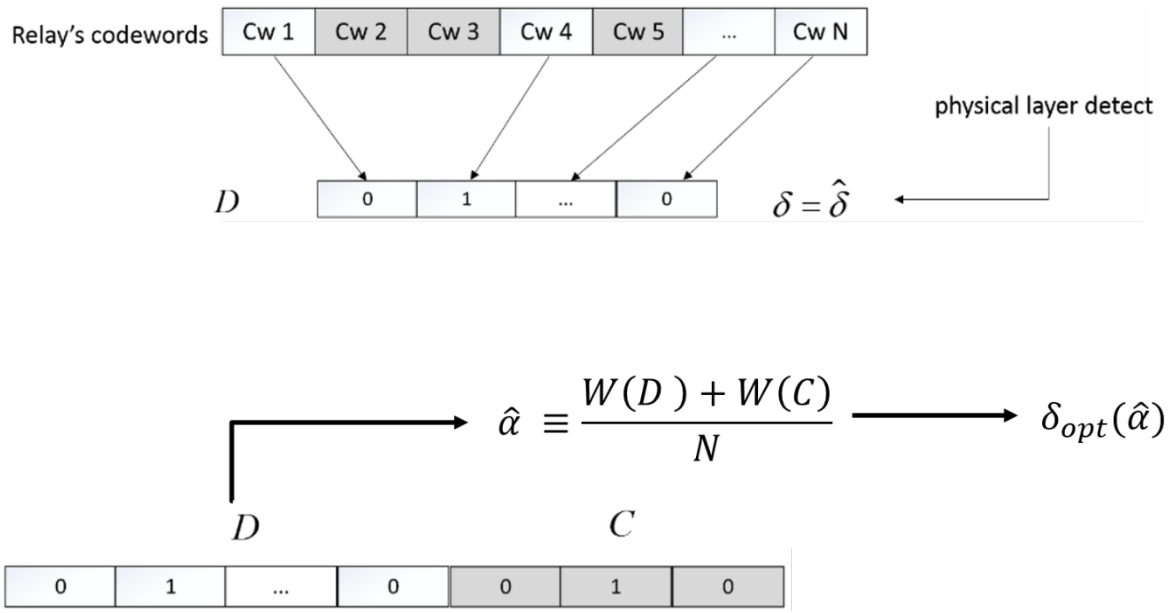

Figure 6. *Physical layer detection for unencrypted codewords*

Then calculate $\hat{\alpha}$ by

$$\hat{\alpha} \equiv \frac{W(D)+W(C)}{N} \tag{23}$$

Thus $\delta_{opt}(\hat{\alpha})$ can be obtained by equation (19).

3.3 Crypto-aided physical layer integrity check process

In chapter 3.1 we discuss optimal detecting threshold and in chapter 3.2 we develop a scheme to estimate the attack probability which is necessary to calculate the optimal detection threshold. In this section we describe our crypto-aided physical layer integrity check process as shown in Fig. 7.

After receive the signals from source transmitter and relay, destination first subtract initial N codewords and utilizes the N_c encrypted codewords information to estimate the attack probability α. Then the estimation $\hat{\alpha}$ can be used as pre-knowledge to produce the optimal

www.manaraa.com

detection threshold $\delta_{opt}(\hat{\alpha})$. Next step, destination applies $\delta_{opt}(\hat{\alpha})$ to the physical layer detection processor to detect the all the other unencrypted codewords. If the detection shows codewords is modified, it will be discarded; otherwise destination will combine both codeword by using MRC rule to decode the message.

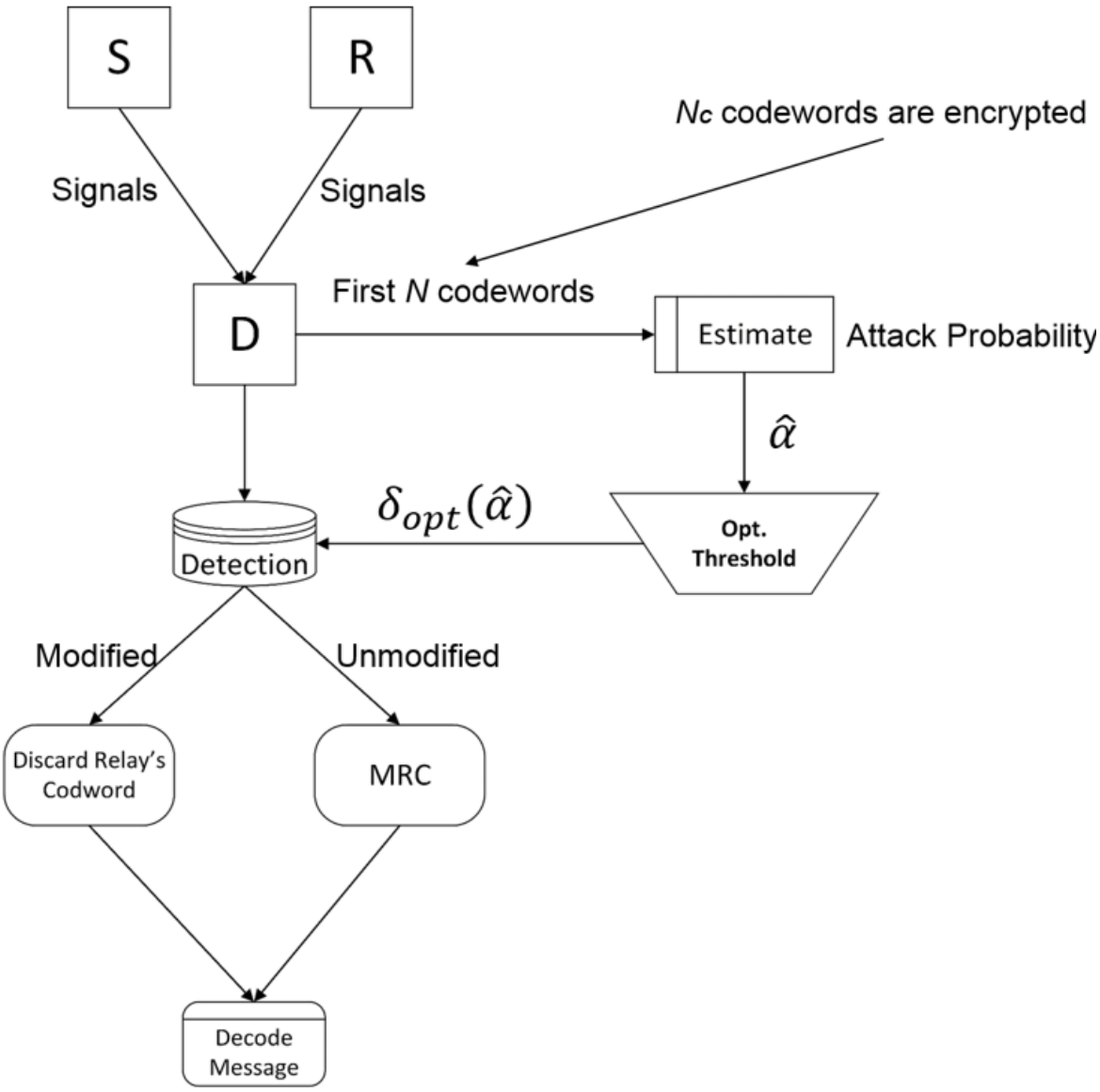

Figure 7. *Crypto-aided physical layer integrity check process*

www.manaraa.com

CHAPTER 4
NUMERITICAL RESULTS

This chapter will first analyze the proposed optimal detection scheme performance based on the different detection threshold value and compare them for several different attack probability cases. Then investigating the estimation of attack probability performance provided by the proposed algorithm. Finally we will show the simulation results of the cooperative relaying system by applying our crypto-aided physical layer integrity check technique.

4.1 Probability of decoding error versus detecting threshold

We will first analyze the proposed optimal detection scheme performance. Analytical results for probability of decoding error versus detecting threshold is shown in Fig.8. Let $\alpha = 0.3$, $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, and use BCH (15, 7) code. Compare the situations where transmit $SNR = 10dB, 15dB, 20dB$. It can be observed that when the detecting threshold approaches to the optimal value, the error probability decreases significantly. In the view of SNR aspect, when SNR increases, the optimal threshold value and the decoded error rate both decrease.

And in Fig. 9, we compare the probability of decoding error versus detecting threshold given different relay's attack probability scenarios, where $\alpha = 0.3, 0.5, 0.7$. Let $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, transmit $SNR = 15dB$. BCH (15, 7) code and use BCH (15, 7) code. It can be seen that as relay's attack probability decreases, the probability of decoding error and optimal detecting threshold both decrease due to less modification codewords received.

www.manaraa.com

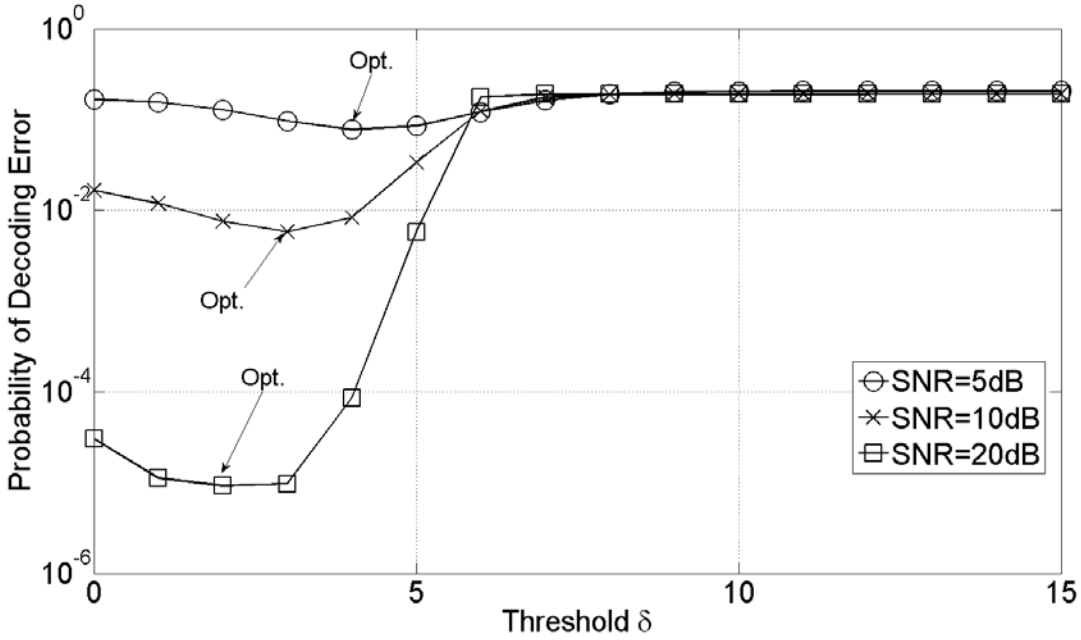

Figure 8. *Probability of decoding error* $P(\hat{m} \neq m)$ *versus detecting threshold* δ*;* $\alpha = 0.3$, $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$. *BCH* (15, *7) code*

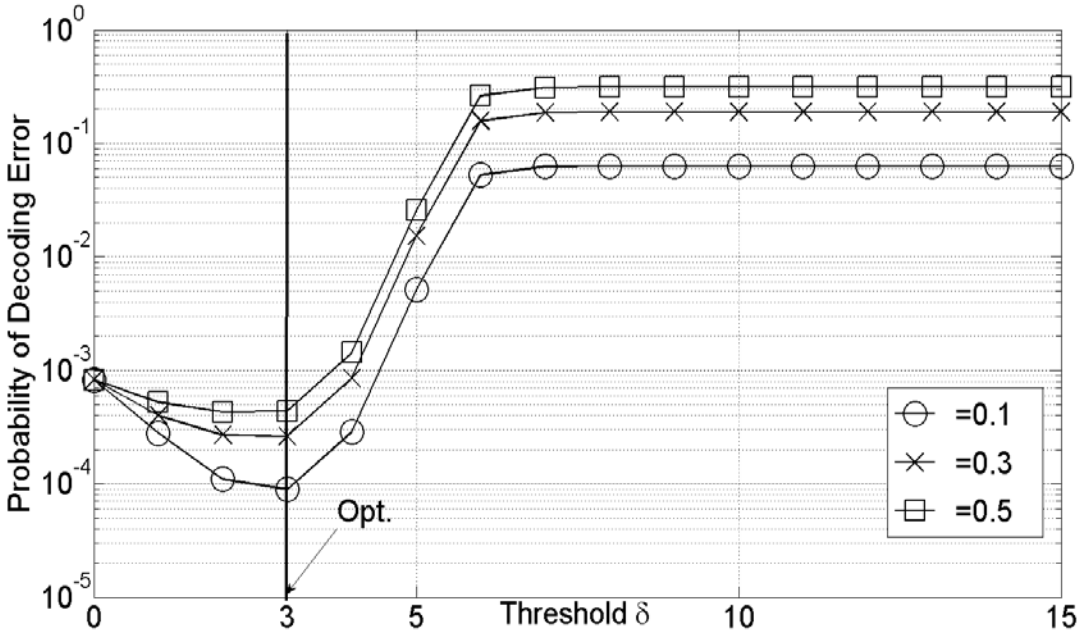

Figure. 9 *Probability of decoding error* $P(\hat{m} \neq m)$ *versus detecting threshold* δ*;* $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, $SNR = 15dB$. *BCH* (15, 7) *code*

www.manaraa.com

4.2 Attack probability estimation versus transmit SNR

This section we investigate the performance of our estimated attack probability. Fig. 10 shows the attack probability estimation simulation performance. Let $\alpha = 0.3$, $\sigma_r^2 = 1$, $N = 20$, $N_c = 3$, and use BCH (15, 7) code. We compare the situations where channel gain $\sigma_s^2 = 0.01,0.1,0.5$. It can be seen that $\hat{\alpha}$ produced by proposed scheme varies around α in a small range even when the channel gain of source-to-destination become very small.

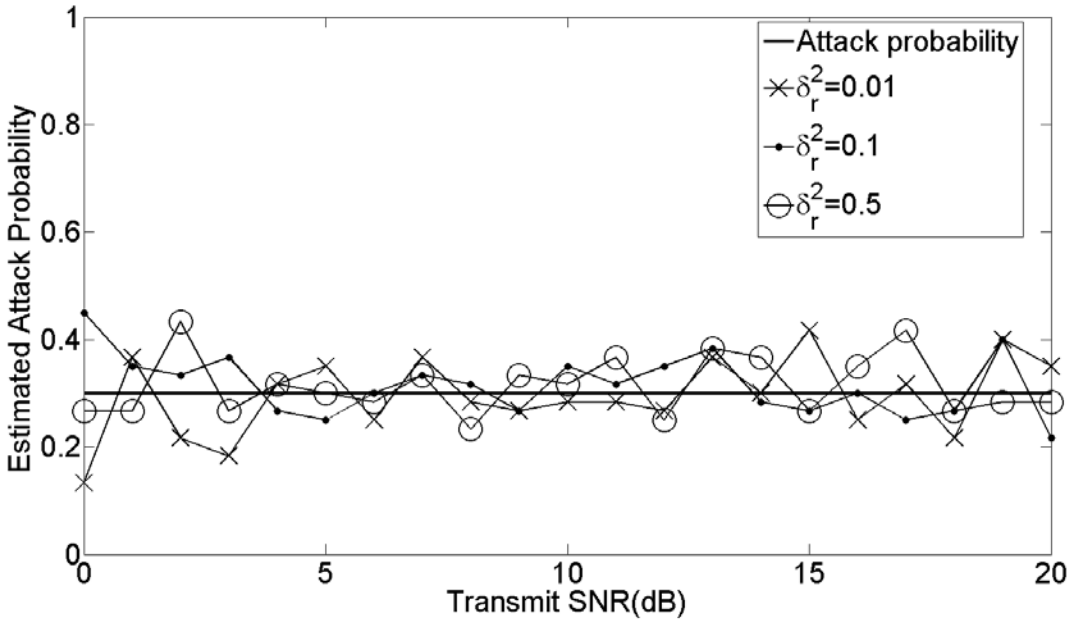

Figure. 10 *Attack probability estimation versus transmit SNR* $\alpha = 0.3, \sigma_r^2 = 1, N = 20, N_c = 3$. *BCH* (15, 7) *code*

4.3 Optimal detecting threshold and proposed optimal threshold estimation

The optimal detecting threshold has been analyzed in chapter 3.1 and the proposed optimal is described in chapter 3.2. The Fig. 11 shows simulation comparison results between optimal detecting threshold and proposed optimal detecting threshold estimation versus relay's attack probability. BCH (15, 7) code, Let $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, $N = 20$, $N_c = 3$, transmit $SNR = 10dB$ and use BCH (15, 7) code. Since $\delta_{opt}(\alpha)$ keep robust in a small range around α

www.manaraa.com

as shown in Fig. 2, it can be seen the corresponding $\delta_{opt}(\hat{\alpha})$ produced by proposed scheme is very close to $\delta_{opt}(\alpha)$. The only divergence exists in the special situation, where $\alpha = 0$. Because when there is no modified codewords, destination should always accept the signal from the relay, thus the analytical optimal threshold achieves a large value. Since we choose the scheme that minimizes the miss detection rate in simulations, it tends overestimates the α and produces a smaller value of $\delta_{opt}(\hat{\alpha})$. Furthermore it can be observed that the optimal detecting threshold is robust against relay's attack probability especially in high SNR. For another special situation where $\alpha = 1$, both analytical and proposed scheme estimation of optimal threshold converge to 0 that system always discard codewords from relay.

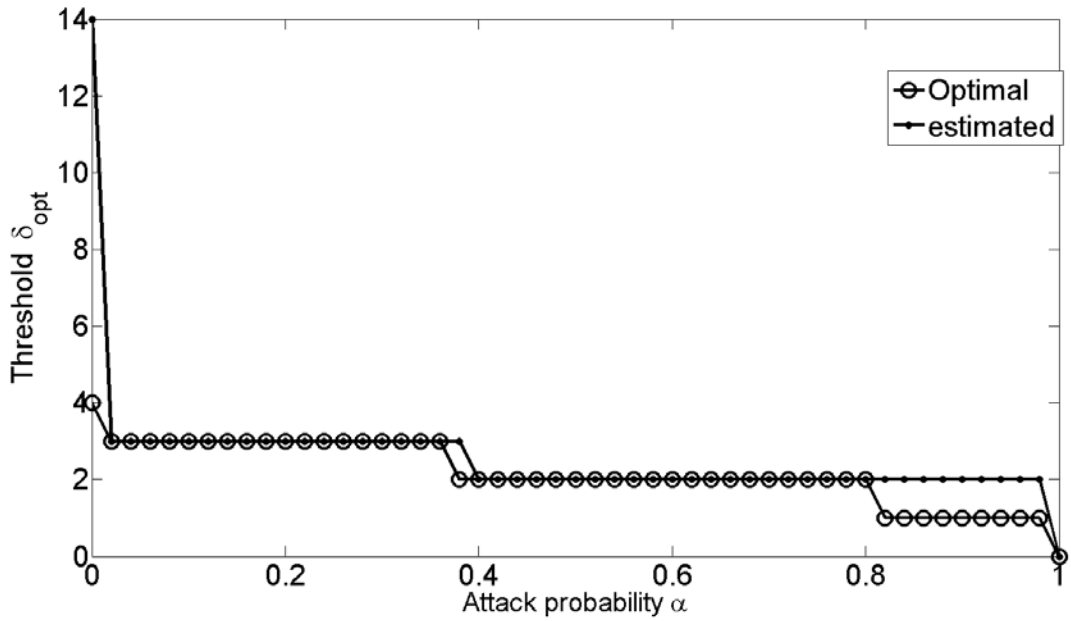

Figure. 11 *Comparison of optimal detecting threshold with proposed optimal detecting threshold estimation.* $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, $N = 20$, $N_c = 3$. $SNR = 10dB$. *BCH* (15, 7) *code*

4.4 False alarm rate and miss detection rate

We investigate the how false alarm rate and miss detection rate varies against threshold closed by destination in the section. Fig. 12 shows the analytical results for False Alarm rate

www.manaraa.com

and Miss Detection rate versus detecting threshold with $\alpha = 0.5$, $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, transmit $SNR = 10dB$ and use BCH (15, 7) code. It is straightforward to see that the false alarm rate diminishes as threshold approaches to the maximum value and meanwhile the miss detection rate gets to the minimum value.

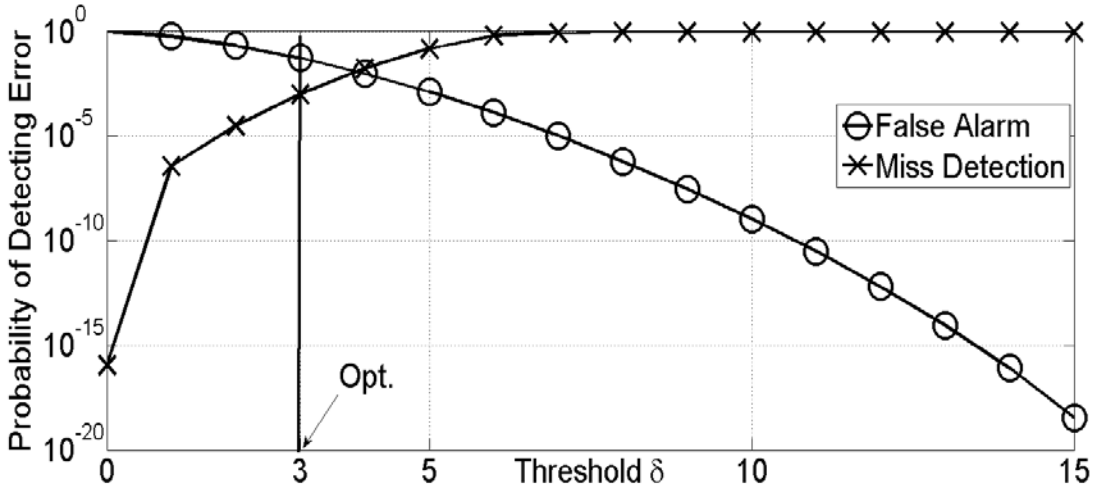

Figure. 12 *Probability of false alarm and miss detection versus detecting threshold;* $\alpha = 0.5$, $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, $SNR = 10dB$. *BCH* (15, 7) *code*

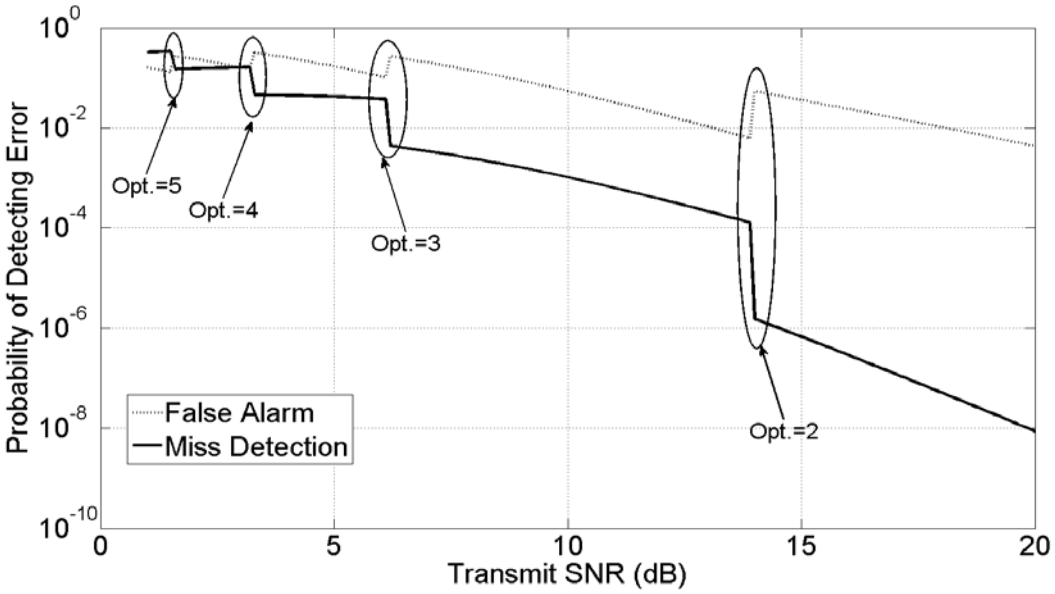

Figure. 13 *Probability of false alarm and miss detection versus transmit SNR;* $\alpha = 0.5$, $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$. *BCH* (15, 7) *code*

www.manaraa.com

Then in Fig. 13 we show the analytical results of False Alarm rate and miss detection rate versus transmit SNR applied with the optimal threshold. Let $\alpha = 0.5$, $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, and use BCH (15, 7) code. Overall, both false alarm rate and miss detection rate decrease with SNR increases. But there exists several "change" points in both curves, it is because the optimal threshold changes a smaller value when SNR achieves the efficient high level (as shown in Fig.8). And a smaller optimal threshold produces a higher false alarm rate and a lower miss detection rate.

4.5 Crypto-aided physical layer integrity check

This section we show the simulation results of cooperative relaying system performance by applying our crypto-aided physical layer integrity check technique.

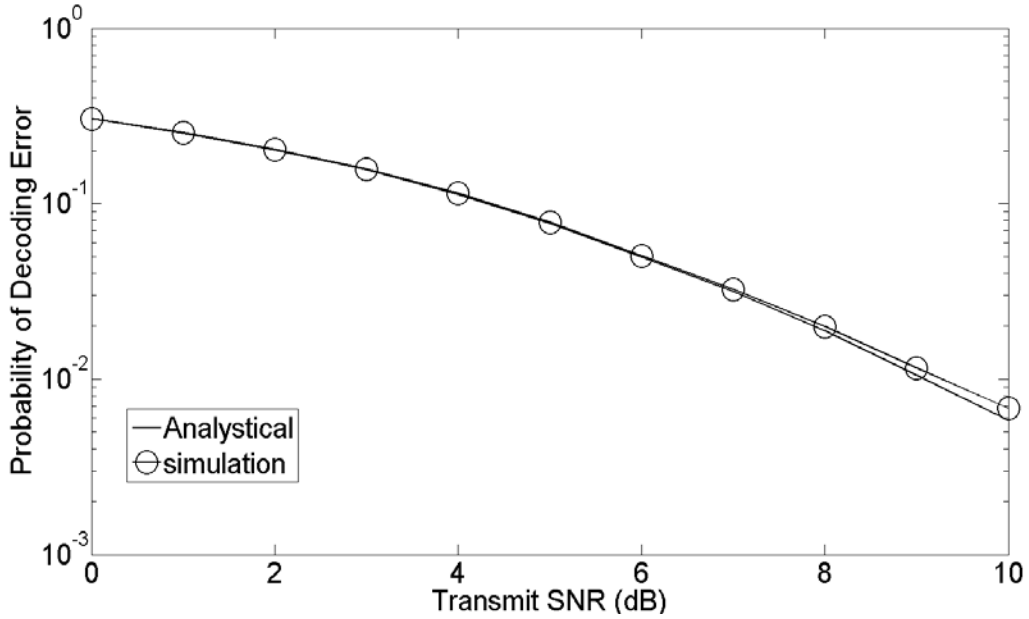

Figure. 14 *Probability of decoding error comparison between simulations and analysis;* $\alpha = 0.3$, $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, $N = 20$. *BCH* (15, 7) *code*

Fig. 14 shows the simulations and analytical results comparison for the probability of decoding error versus transmit SNR. Let $\alpha = 0.3$,$\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$ and use BCH (15, 7) code.

www.manaraa.com

It can be observed that our simulations matches with analysis.

Since the Fig. 14 shows our simulation process matches with analysis. Fig. 15 depicts the simulation results for the probability of decoding error versus transmit SNR. Let $\alpha = 0.3$,$\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, $N = 20$, and use BCH *(15, 7)* code. We compare the proposed scheme with different $N_c = 0,2,4,6$. It can be observed that the proposed estimation scheme's performance is almost as good as the ideal cryptography scheme where destination can always remove the modified codewords. And with the proportion of N_c/N becomes larger, proposed scheme curve converges to cryptography's. Moreover, if system applies no detecting techniques, the performance cannot be improved by increasing the transmit SNR. That is lose caused by the modification conducted by the relay.

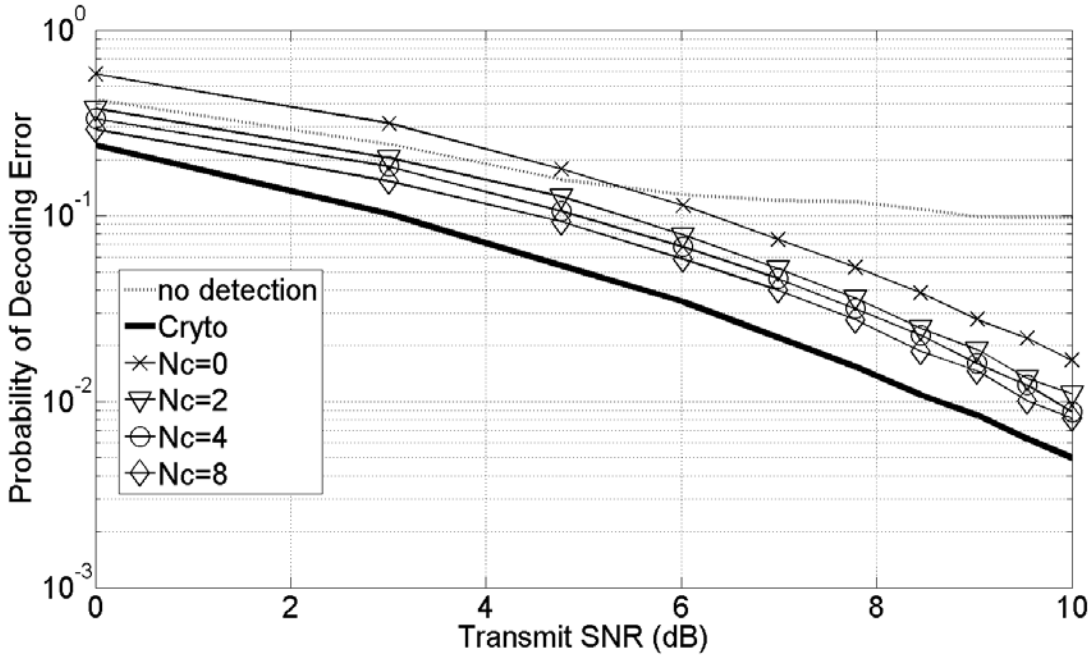

Figure. 15 *Probability of decoding error versus transmit SNR I for different Nc;* $\alpha = 0.3$, $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, $N = 20$. *BCH* (15, 7) *code*

Fig. 16 shows the simulation results for probability of versus transmit SNR given several attack probability $\alpha = 0.1, 0.3, 0.5$. Set $\sigma_s^2 = 0.5$, $\sigma_r^2 = 1$, $N = 20$, $N_c = 2$, and use

www.manaraa.com

BCH *(15, 7)* code. It can be seen that the probability of decoding error increases when α become larger, this is because when more modified codewords received, the more messages have to be decoded based on source information only or the modified codewords sent by relays.

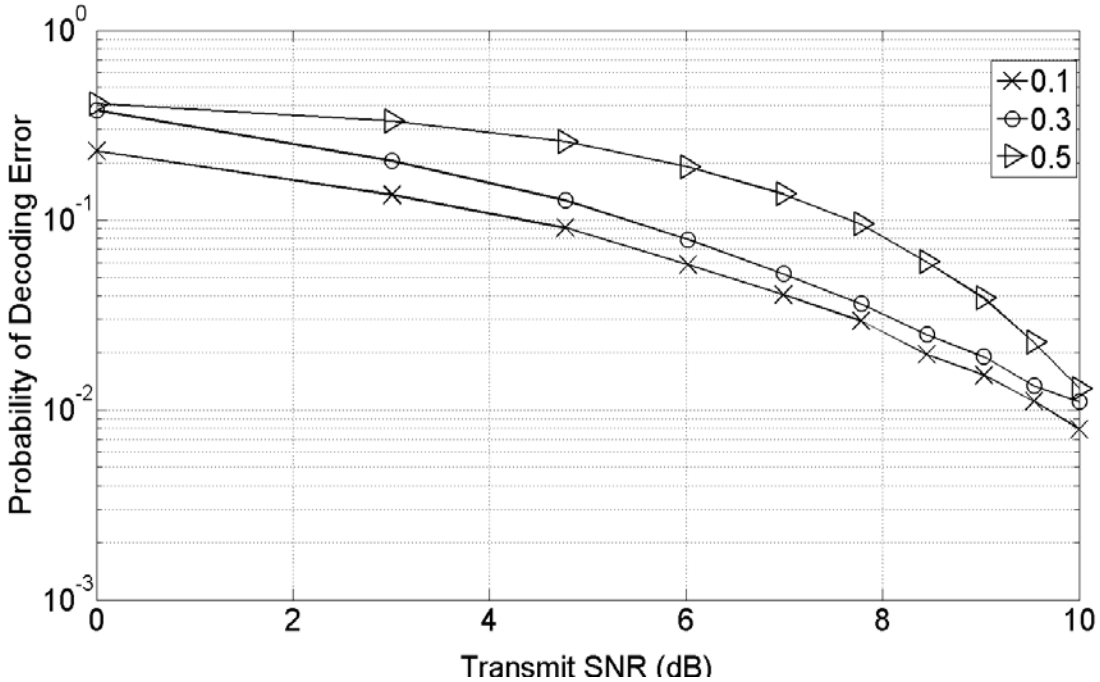

Figure. 16 *Probability of decoding error versus transmit SNR II for different attack probability;* $\sigma_s^2 = 0.5, \sigma_r^2 = 1,\ N = 20, N_c = 3$. *BCH* (15, 7) *code*

www.manaraa.com

CHAPTER 5

CONCLUSIONS

We investigate a scenario in cooperative relaying communication where source transmitter broadcasts the signals to destination and relay, and relay re-transmits the signals to destination. Since the relaying node is not trustworthy, instead of helping source, it may forward the modified signals to attack the destination. So the destination has to do the detection to decide whether the signals from relay if modified or not. Based on the detection results, the destination may discard the signals from the relay and only decodes based on the signal from the source, otherwise both signals are combined together by using the maximum ration combining rule to decode the message. In analysis we show that by applying the optimal detection threshold method, the average probability of decoding error can be minimized. However the optimal detection threshold calculation requires the pre-knowledge of the relay's attack probability.

Since the optimal threshold value is robust against the relay's attack probability in a certain range around and with transmit SNR increases it tend to keep unchanged. Thus we proposed a scheme to estimate the attack probability that utilizes this property. And our results show that the performance provided by optimal threshold based on the proposed cryptography-aided scheme estimation achieves a good performance as the perfect cryptography strategy. Even though perfect cryptography strategy can detect all the modified messages, it consumes a significant high computational resource to apply cryptographic encryption to all the transmitted messages.

Furthermore since the optimal threshold value is very robust against the relay's attack in high SNR, the can be used for a long duration to achieve the high efficiency in practice. It

www.manaraa.com

is unnecessary to refresh estimated optimal threshold value frequently; furthermore the total amount cryptography computation cost in the proposed scheme can be very small so that it can be easily applied to the resource-constrained distributed wireless network system.

www.manaraa.com

REFERENCES

[1] [Michalopoulos, Diomidis S., and George K. Karagiannidis. "Performance analysis of single relay selection in Rayleigh fading." *Wireless Communications, IEEE Transactions on* 7.10 (2008): 3718-3724.

[2] Laneman, J. Nicholas, David NC Tse, and Gregory W. Wornell. "Cooperative diversity in wireless networks: Efficient protocols and outage behavior."*Information Theory, IEEE Transactions on* 50.12 (2004): 3062-3080.

[3] Bletsas, A., Khisti, A., Reed, D. P., & Lippman, A. (2006). A simple cooperative diversity method based on network path selection. *Selected Areas in Communications, IEEE Journal on*, *24*(3), 659-672.W.-K. Chen, *Linear Networks and Systems*. Belmont, CA: Wadsworth, 1993, pp. 123–135.

[4] Raychaudhuri, Dipankar, et al. "Overview of the ORBIT radio grid testbed for evaluation of next-generation wireless network protocols." *Wireless Communications and Networking Conference, 2005 IEEE*. Vol. 3. IEEE, 2005.

[5] Dong, Lun, et al. "Improving wireless physical layer security via cooperating relays." *Signal Processing, IEEE Transactions on* 58.3 (2010): 1875-1888..

[6] Bloch, Matthieu, and Joao Barros. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[7] Dehnie, Sintayehu, Husrev T. Sencar, and Nasir Memon. "Detecting malicious behavior in cooperative diversity." *Information Sciences and Systems, 2007. CISS'07. 41st Annual Conference on*. IEEE, 2007.

[8] Porret, A-S., et al. "A low-power low-voltage transceiver architecture suitable for wireless distributed sensors network." *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*. Vol. 1. IEEE, 2000.

[9] Forouzan, Behrouz A. *Cryptography & Network Security*. McGraw-Hill, Inc., 2007.

[10] Hamming, Richard W. "Error detecting and error correcting codes." *Bell System technical journal* 29.2 (1950): 147-160.

[11] Tse, David, and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[12] Wang, Beibei, Zhu Han, and KJ Ray Liu. "Distributed relay selection and power control for multiuser cooperative communication networks using buyer/seller game." *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. IEEE, 2007.

www.manaraa.com

[13] Bose, Raj Chandra, and Dwijendra K. Ray-Chaudhuri. "On a class of error correcting binary group codes." *Information and control* 3.1 (1960): 68-79.

[14] MacWilliams, Florence Jessie, and Neil James Alexander Sloane. *The theory of error correcting codes*. Vol. 16. Elsevier, 1977.

[15] Chen, Zhuo, Jinhong Yuan, and Branka Vucetic. "Analysis of transmit antenna selection/maximal-ratio combining in Rayleigh fading channels." *Vehicular Technology, IEEE Transactions on* 54.4 (2005): 1312-1321.

[16] Casella, George, and Roger L. Berger. Statistical inference. Vol. 2. Pacific Grove, CA: Duxbury, 2002.

[17] Proakis, John G. "Digital communications. 1995." *McGraw-Hill, New York*

[18] Trappe, Wade, and Lawrence C. Washington. *Introduction to cryptography with coding theory*. Pearson Education India, 2006.

[19] Macmillan, Neil A., and C. Douglas Creelman. *Detection theory: A user's guide*. Psychology press, 2004.

www.manaraa.com

APPENDIX A
NOTATION

Symbol	Meaning
$\boldsymbol{m}$	Original message
$\boldsymbol{\hat{m}}$	Decoded message
$\boldsymbol{k}$	Length of message
$\boldsymbol{X}$	The BCH codeword for message m
$\boldsymbol{\hat{X}}$	The BCH codeword for decoded message $\hat{m}$
$\boldsymbol{n}$	The length of the BCH codeword
$+$	XOR operation
$\boldsymbol{W(X)}$	Hamming weight of X
$\boldsymbol{d_{min}}$	The minimal hamming distance in BCH code
$\boldsymbol{t}$	The BCH code self-correct ability
$\boldsymbol{E_s}$	Random noise vector represents N_s
$\boldsymbol{E_r}$	Random noise vector represents N_r
$\boldsymbol{E}$	$E_s + E_r$

www.manaraa.com

$\boldsymbol{F}$	Relay's modification vector
$\boldsymbol{J}$	number of the 1's in F been reversed by E
$\boldsymbol{e_s}$	probability that single bit in vector E_s is 1
$\boldsymbol{e_r}$	probability that single bit in vector E_r is 1
$\boldsymbol{e}$	probability that single bit in vector E is 1
$\boldsymbol{e_m}$	the error rate by applying MRC rule to $X + E_s$ and $X + E_r$
$\boldsymbol{e'_m}$	the error rate by applying MRC rule to $X + E_s$ and $X + F + E_r$
$\boldsymbol{\sigma_s^2}$	Channel gain of source-to-destination
$\boldsymbol{\sigma_r^2}$	Channel gain of relay-to-destination
$\boldsymbol{\delta}$	Threshold of detection method
$\boldsymbol{\alpha}$	The relay's attack probability

www.manaraa.com

APPENDIX B

PROBAILITY OF MRC COMBINING

In this section we derive the expression of e_m and e'_m. Since the transmit SNR is ε_b/N_0, and $h_{sd} \sim CN(0,\sigma_s^2)$ and $h_{rd} \sim CN(0,\sigma_r^2)$, $\sigma_s^2 < \sigma_r^2$. So $|h_{sd}|^2$ and $|h_{rd}|^2$ has chi-square probability distribution with two degrees of freedom. And system uses the BPSK modulation.

e_m is the probability of decoding error by applying MRC to Y_s and Y_r, where Y_r is not modified. From [17] we know the error rate is $Q(\sqrt{2\gamma_1})$, where received SNR γ_1 is

$$\gamma_1 = \left(|h_{rd}|^2 + |h_{sd}|^2\right)\frac{\varepsilon_b}{N_0} \tag{24}$$

define $Z = |h_{rd}|^2 + |h_{sd}|^2$, Then the PDF of Z is

$$p_Z(z) = \frac{1}{\left(\sigma_r^2 - \sigma_s^2\right)}\left[e^{-\frac{z}{\sigma_r^2}} - e^{-\frac{z}{\sigma_s^2}}\right] \tag{25}$$

Then the expression for e_m is

$$\begin{aligned} e_m &= \int_0^\infty Q\left(\sqrt{2\gamma_1}\right)\frac{N_0}{\varepsilon_b}\, p_z\left(\frac{N_0}{\varepsilon_b}\gamma_1\right)d\gamma_1 \\ &= \frac{1}{2\left(\sigma_r^2 - \sigma_s^2\right)}\left[\sigma_r^2\left(1 - \sqrt{\frac{\overline{\gamma_r}}{1+\overline{\gamma_r}}}\right) - \sigma_s^2\left(1 - \sqrt{\frac{\overline{\gamma_s}}{1+\overline{\gamma_s}}}\right)\right] \end{aligned} \tag{26}$$

$e_m{}'$ is the probability of decoding error by applying MRC to Y_s and Y_r, but Y_r contains the modified codewords. Because the relay does not change all the bits in codeword, so the unchanged bit keep the same error rate as e_m. The error rate for the modified bit will be $Q(\sqrt{2\gamma_2})$, where γ_2

www.manaraa.com

$$\gamma_2 = \left(\left|h_{rd}\right|^2 - \left|h_{sd}\right|^2\right)\frac{\varepsilon_b}{N_0} \tag{27}$$

define $Z = |h_{sd}|^2 - |h_{rd}|^2$, The PDF of Z is

$$p_Z(z) = \begin{cases} \dfrac{1}{\left(\sigma_r^2 + \sigma_s^2\right)} e^{\frac{z}{\sigma_r^2}}, z < 0 \\ \dfrac{1}{\left(\sigma_r^2 + \sigma_s^2\right)} e^{-\frac{z}{\sigma_s^2}}, z \geq 0 \end{cases} \tag{28}$$

Then the expression for e'_m is

$$\begin{aligned} e_m^{'} &= \frac{d_{min}}{n}\int_0^{\infty} Q\left(\sqrt{2\gamma_2}\right)\frac{N_0}{\varepsilon_b}\, p\left(\frac{N_0}{\varepsilon_b}\gamma_2\right) d\gamma_2 + \frac{n - d_{min}}{n} e_m \\ &= \frac{d_{min}}{n}\left\{\frac{\sigma_r^2}{\left(\sigma_r^2 + \sigma_s^2\right)} + \frac{1}{2\left(\sigma_r^2 + \sigma_s^2\right)}\left[\sigma_r^2\left(1 - \sqrt{\frac{\overline{\gamma_r}}{1+\overline{\gamma_r}}}\right) - \sigma_s^2\left(1 - \sqrt{\frac{\overline{\gamma_s}}{1+\overline{\gamma_s}}}\right)\right]\right\} \\ &+ \frac{n - d_{min}}{2n\left(\sigma_r^2 - \sigma_s^2\right)}\left[\sigma_r^2\left(1 - \sqrt{\frac{\overline{\gamma_r}}{1+\overline{\gamma_r}}}\right) - \sigma_s^2\left(1 - \sqrt{\frac{\overline{\gamma_s}}{1+\overline{\gamma_s}}}\right)\right] \end{aligned} \tag{29}$$

www.manaraa.com