2011

Security and Prioritization in Multiple Access Relay Networks

Taha Abdelshafy Abdelhakim Khalaf
Iowa State University

Security and prioritization in multiple access relay networks

by

Taha Abdelshafy Abdelhakim Khalaf

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Electrical Engineering

Program of Study Committee:
Sang Wu Kim, Major Professor
Daji Qiao
Yong Guan
Aditya Ramamoorthy
Jennifer Davidson

Iowa State University

Ames, Iowa

2011

DEDICATION

I would like to dedicate this thesis to my father, my mother, and my wife without whose support I would not have been able to complete this work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my thanks to those who helped me with various aspects of conducting research and the writing of this thesis. First and foremost, Dr. Sang Wu Kim for his guidance, patience and support throughout this research and the writing of this thesis. His insights and words of encouragement have often inspired me and renewed my hopes for completing my graduate education. I would also like to thank my committee members for their time and efforts. I would also like to thank Egyptian Cultural and Educational Bureau for the financial support. Finally many thanks to my friends Young Jin Chun, Navneet Malani, and Duk Hee Yoon for their guidance during my research.

CHAPTER 1. OVERVIEW

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. The mobile ad hoc network (MANET) is a collection of independent mobile nodes that communicate without a preexisting infrastructure which meets these requirements [1]. Since MANETs are decentralized environments, it comes out the idea of the devices in the network to be collaborative and help each other to better accomplish a common task with high performance such as quality, throughput, etc. Cooperative communications have recently become a key approach in realizing this idea [7].

The cooperative relaying approach has a great potential to provide substantial benefits in terms of reliability (diversity gain) [5]-[8] and rate (bandwidth or spectral efficiency)[9]-[12]. These benefits can extend the coverage, reduce network energy consumption, and promote uniform energy drainage by exploiting neighbors' resources. They can be of great value in many applications, including ad-hoc networks, mesh networks, and next generation wireless local area networks and cellular networks.

1.1 Cooperative Relaying

Figure 1.1 shows a wireless relay network composed of single source, single relay, and single destination. In this network, the transmission occurs in two phases. In the first phase, the source sends its message to the destination. Because of the broadcast nature of the wireless channel, the relay hears the first phase transmission. In the second phase, the relay assists the source by forwarding the received signal to the destination. In order to decode the source's

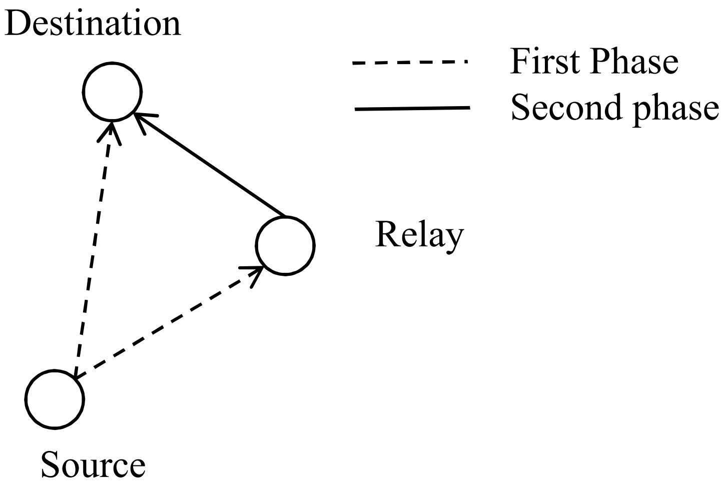


Figure 1.1 Single source, single relay, and single destination wireless network.

message, the destination combines the signals received from the source and the relay.

1.1.1 Cooperative diversity and cooperative spatial multiplexing

Cooperative diversity (C-DIV) is an approach that exploits the broadcast nature and inherent spatial diversity of the channel. Through cooperative diversity, relay nodes forward the signal received from the source to propagate redundant signals over multiple paths in the network. This redundancy allows the ultimate receiver to essentially average channel variations resulting from fading, shadowing, and other forms of interference [5].

Cooperative spatial multiplexing (C-SM) is another cooperative relaying architecture which simplifies the transmit and receive processing requirement on the relay node while providing significant savings in the transmit and receive energy over the C-DIV technique, particularly in the high spectral efficiency regime [9]. The idea of this approach is to make each relay node detects only a subset (called sub-stream) of the source data stream and all relay nodes forward their sub-streams simultaneously over the same physical channel. Then, multiple receive antennas at the base station (destination) allow the sub-streams to be detected separately based on their spatial characteristics.

1.1.2 Cooperation protocols

Several cooperation protocols have been proposed in the literature to achieve different tasks. Examples of these protocols can be explained as follow:

1.1.2.1 Amplify-and forward (AF) [5]

The transmission of the symbol x in AF scheme occurs in two phases or two time slots. In the first phase, the source sends x to the destination. because of the broadcast nature of the wireless channel the transmission of the first phase can be heard by the relay node. In the second phase, the relay amplifies the signal received from the source and forward it to the destination. The signal received at the relay in the first phase is given by

$$y_r = h_{sr}x + n_r \tag{1.1}$$

where h_{sr} is the gain channel of the channel between the source and the relay, n_r is an additive white Gaussian noise (AWGN) with zero mean and variance N_0. The signal transmitted by the relay node is given by

$$\begin{aligned} x_r =& \beta y_r \\ =& \beta h_{sr}x + \beta n_r \end{aligned} \tag{1.2}$$

where β is the amplifying gain. To remain within its power constraint (with high probability), an amplifying relay must use gain

$$\beta = \sqrt{\frac{P}{|h_{sr}|^2 P + N_0}} \tag{1.3}$$

where the amplifier gain is allowed to depend upon the fading coefficient h_{sr} between the source and relay, which the relay estimates to high accuracy. This scheme can be viewed as repetition coding from two separate transmitters, except that the relay transmitter amplifies its own receiver noise.

The signal received at the destination in the first phase is given by

$$y_{d_1} = h_{sd}x + n_{d_1} \tag{1.4}$$

where h_{sd} is the gain channel of the channel between the source and the destination, n_{d_1} is an additive white Gaussian noise (AWGN) with zero mean and variance N_0. The signal received at the destination in the second phase is given by

$$y_{d_2} = h_{rd}\beta h_{sr}x + h_{rd}\beta n_r + n_{d_2} \tag{1.5}$$

where h_{rd} is the gain channel of the channel between the relay and the destination, n_{d_2} is an additive white Gaussian noise (AWGN) with zero mean and variance N_0. The destination can decode its received signal by first appropriately combining the signals y_{d_1} and y_{d_2} using one of a variety of combining techniques such as maximum-ratio combiner.

1.1.2.2 Decode-and forward (DF)

The first phase of the DF scheme is similar to that of the AF scheme. In the second phase of the DF scheme, the relay nodes decodes the received signal first to fins an estimate of the transmitted symbol $\hat{x}$ and then forward the decoded symbol to the destination. The signal transmitted by the relay node is given by

$$x_r = \hat{x} \tag{1.6}$$

and the signal received at the destination in the second phase is given by

$$y_{d_2} = h_{rd}\hat{x} + n_{d_2} \tag{1.7}$$

Decoding at the relay can take on a variety of forms. For example, the relay might fully decode, i.e., estimate without error, the entire source codeword, or it might employ symbol-by-symbol decoding and allow the destination to perform full decoding. These options allow for trading off performance and complexity at the relay terminal.

1.1.2.3 Compress-and-forward (CF) [13, 14]

Compress and forward is another example of cooperation protocols which allows the relay nodes to compress the received signal from the source node and forward it to the destination without decoding the signal where Wyner-Ziv coding can be used for optimal compression.

1.1.2.4 Selection Relaying

since the fading coefficients are known to the appropriate receivers, h_{sr} can be measured to high accuracy by the cooperating terminals; thus, they can adapt their transmission format according to the realized value of h_{sr}. This observation suggests the following class of selection relaying algorithms If the measured $|h_{sr}|^2$ falls below a certain threshold, the source simply continues its transmission to the destination, in the form of repetition or more powerful codes. If the measured $|h_{sr}|^2$ lies above the threshold, the relay forwards what it received from the source, using either amplify-and-forward or decode-and-forward, in an attempt to achieve diversity gain.

Informally speaking, selection relaying of this form should offer diversity because, in either case, two of the fading coefficients must be small in order for the information to be lost. Specifically, if $|h_{sr}|^2$ is small, then $|h_{sd}|^2$ must also be small for the information to be lost when the source continues its transmission. Similarly, if $|h_{sr}|^2$ is large, then both $|h_{sd}|^2$ and $|h_{rd}|^2$ must be small for the information to be lost when the relay employs amplify-and-forward or decode-and-forward.

1.1.3 Multiple access relay networks

Figure 1.2 shows an example of mutiple access relay network. In multiple-access relay network (MARN), multiple sources communicate with a single destinations in the presence of relay nodes. Examples of such networks include hybrid wireless LAN/WAN networks and sensor and ad hoc networks where cooperation between sources is either undesirable or not possible, but one can use an intermediate relay nodes to aid communication between the sources and the destination. As in multiuser wireless systems, access coordination among sources may

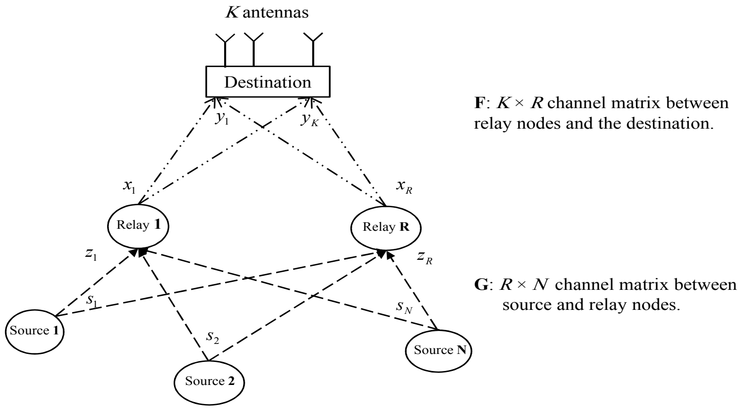

K antennas
Destination
y_1
y_K
F: K × R channel matrix between relay nodes and the destination.
x_1
x_R
Relay 1
Relay R
z_1
z_R
G: R × N channel matrix between source and relay nodes.
s_1
s_2
s_N
Source 1
Source 2
Source N

Figure 1.2 System Model: N sources, R relays, one destination with K antennas

be carried out in different domains: the frequency domain, time domain, code domain, and space domain. Signals of different sources are insulated in each domain by splitting the resource available into non-overlapping slots (frequency slot, time slot, code slot, and space slot) and assigning each signal a slot. Four main multiple access technologies are used by the wireless networks: frequency division multiple access (FDMA), time division multiple access (TDMA), code division multiple access (CDMA), and space division multiple access (SDMA).

In multiple source networks, in addition to providing a diversity and/or multiplexing gain, relay nodes can provide other tasks such as mitigating the interference effect among sources, maximizing the signal to noise ratio, and minimizing the mean square error. Zero forcing (ZF) relaying is a scheme in which the interference among sources can be completely removed by adjusting the weights at relay nodes [15]-[18]. The minimum mean square error (MMSE) relaying is another relaying scheme where the weights of relay nodes are adjusted to minimize the mean square error between the source signal and the received signal at the destination [20]-[22]. Coherent relaying, QR decomposition relaying, and distributed beamforming relaying proposed in [23, 24] and [25], respectively, are some other examples of relaying schemes in multiple source relay networks.

1.2 Network Coding

Network coding has been originally proposed in information theory [2], and has since emerged as one of the most promising information theoretic approaches to improve network performance. The main idea of network coding is to allow coding at intermediate nodes in information flows. It has been shown that random linear codes using a Galois field of a limited size are sufficient to implement network coding in a practical network setting [26]. It has recently been shown that network coding on GF(2) (i.e., XOR-only coding) is able to significantly improve end-to-end unicast throughput in multi-hop wireless networks, when implemented above the MAC layer of IEEE 802.11 [27, 28].

Physical layer network coding (PLNC) is a scheme that significantly enhances the throughput performance of multi-hop wireless networks [29, 30]. Instead of avoiding interference caused by simultaneous signals transmitted from multiple sources, PLNC exploits the interference among sources to increase network capacity. When two sources transmit simultaneously, the packets collide and the resulting signal is nothing but the sum of the two colliding signals. Thus, if the receiver knows the content of one of the packets, it can decode the other.

1.3 Security issues in MARN

One of the primary concerns of wireless networks is security. Whenever there is a data transmitted through the air, there is a higher chance of interceptions and illegal uses. Examples of vulnerabilities in wireless networks are: jamming, interference, disruption, interception, spoofing, intrusion, and protocol violation. In addition to these vulnerabilities, MARN is exposed to two other security concerns. The first concern is from an autonomous ad-hoc network perspective, where each node is an autonomous entity and may have a lack of motivation to cooperate, such as avoiding packet forwarding in order to preserve its own energy [32]. This selfish behavior is considered as a passive noncooperation. The recent literature addresses passive noncooperation using a credit system [33] or reputation propagation system [34]. The second concern is from the multi-hop network perspective. Relay nodes are usually deployed in open and unattended area and thus are vulnerable to physical tempering. An adversary may launch an attack on the network by altering the data through the relay nodes. If the access node adopts the information from the attacked relay nodes, the performance of the wireless multiple-access relay network can be degraded dramatically.

1.4 Message Ferrying

In Message Ferrying scheme, a moving relay or Message Ferry (MF) follows a "store, carry, and forward" paradigm by accomplishing consecutive events: 1) moves toward the transmitting node, 2) waits until it receives the message, 3) moves toward the receiving node, 4) waits until it delivers the message. Although some routing algorithms have been proposed [79]- [80], the design of the MF route is still an open research topic.

1.5 Related Work

In this section, we summarize some of the previous works which are related to our work.

1.5.1 Signatures for Content Distribution with Network Coding [38]

In this paper, the authors propose a signature scheme for network coding. The scheme makes use of the linearity property of the packets in a coded system, and allows nodes to check the integrity of the packets received easily. The authors show that the proposed scheme is secure, and its overhead is negligible for large files.

The network is modeled by a directed graph $G_d = (N, A)$, where N is the set of nodes, and A is the set of communication links. A source node $s \in N$ wishes to send a large file to a set of client nodes, $T \subset N$. All the clients referred to as peers. The large file is divided into m blocks, and any peer receives different blocks from the source node or from other peers. In this framework, a peer is also a server to blocks it has downloaded, and always sends out random linear combinations of all the blocks it has obtained so far to other peers. When a peer has received enough degrees of freedom to decode the data, i.e., it has received m linearly independent blocks, it can re-construct the whole file.

The m blocks of the file, $\overline{V}_1, \cdots, \overline{V}_m$, can be shown as elements in n-dimensional vector space $\mathbb{F}_p^n$, where p is a prime. The source node augments these vectors to create vectors $V_1, \cdots, V_m$, given by

$$V_i = (0, \cdots, 1, \cdots, 0, \overline{v}_{i1}, \cdots, \overline{v}_{in}) \tag{1.8}$$

where the first m elements are zero except that the i-th element is 1, and $\overline{v}_{ij} \in \mathbb{F}_p$ is the j-th element in $\overline{V}_i$. Packets received by the peers are linear combinations of the augmented vectors,

$$W = \sum_{i=1}^{m} \beta_i V_i \tag{1.9}$$

where β_i is the weight of V_i in W. We see that the additional m elements in the front of the augmented vector keeps track of the β values of the corresponding packet.

This kind of network coding scheme is vulnerable to pollution attacks by malicious nodes and the pollution can quickly spread to other parts of the network if the peer just unwittingly mixes this polluted packet into its outgoing packets. Unlike uncoded systems where the source knows all the blocks being transmitted in the network, and therefore, can sign each one of them, in a coded system, each peer produces "new" packets, and standard digital signature schemes do not apply here. In the next section, we introduce a novel signature scheme for the coded system.

The key observation for the proposed signature scheme is that the vectors $V_1, \cdots, V_m$ span a subspace V of $\mathbb{F}_p^{m+n}$, and a received vector W is a valid linear combination of vectors $V_1, \cdots, V_m$ if and only if it belongs to the subspace V. In the proposed scheme, the authors present a system that is based upon standard modulo arithmetic (in particular the hardness of the Discrete Logarithm problem) and upon an invariant signature $\sigma(V)$ for the linear span V. Each node verifies the integrity of a received vector W by checking the membership of W in V based on the signature $\sigma(V)$. The signature scheme is defined by the following ingredients, which are independent of the file(s) to be distributed:

- q: a large prime number such that p is a divisor of $q-1$. The standard techniques, such as that used in Digital Signature Algorithm (DSA), can be applied to find such q.

- g: a generator of the group G of order p in $\mathbb{F}_q$. Since the order of the multiplicative group $\mathbb{F}_q^*$ is $q-1$, which is a multiple of p, a subgroup, G, with order p in $\mathbb{F}_q^*$ can be found.

- Private key: $\mathbf{K}_{pr} = \{\alpha_i\}_{i=1,\cdots,m+n}$, a random set of elements in $\mathbb{F}_p^*$. $\mathbf{K}_{pr}$ is only known to the source.

- Public key: $\mathbf{K}_{pu} = \{h_i = g^{\alpha_i}\}_{i=1,\cdots,m+1}$. $\mathbf{K}_{pu}$ is signed by some standard signature scheme, e.g., DSA, and published by the source.

To distribute a file in a secure manner, the signature scheme works as follows.

1. Using the vectors $V_l, \cdots, V_m$ from the file, the source finds a vector $U = (u_l, \cdots, u_{m+n}) \in \mathbb{F}_p^{m+n}$ orthogonal to all vectors in V. Specifically, the source finds a nonzero solution, U, to the equations

$$V_i.U = 0, \qquad i = 1, \cdots, m. \tag{1.10}$$

2. The source computes vector $X = (u_1/\alpha_1, u_2/\alpha_2, \cdots, u_{m+n}/\alpha_{m+n})$

3. The source signs X with some standard signature scheme and publishes X. We refer to the vector X as the signature, $\sigma(V)$, of the file being distributed.

4. The client node verifies that X is signed by the source.

5. When a node receives a vector W and wants to verify that W is in V, it computes

$$d = \prod_{i=1}^{m+n} h_i^{x_i w_i} \tag{1.11}$$

and verifies that $d = 1$.

To see that d is equal to 1 for any valid W, we have

$$\begin{aligned} d = &\prod_{i=1}^{m+n} h_i^{x_i w_i} \\ = &\prod_{i=1}^{m+n} (g^{\alpha_i})^{u_i w_i/\alpha_i} \\ = &\prod_{i=1}^{m+n} g^{u_i w_i} \\ = &g^{\sum_{i=1}^{m+n}(u_i w_i)} \\ = &1 \end{aligned} \tag{1.12}$$

where the last equality comes from the fact that U is orthogonal to all vectors in V.

1.5.2 An Algebraic Watchdog for Wireless Network Coding [69]

In this paper, the authors proposed a scheme, called the algebraic watchdog for wireless network coding, in which nodes can detect malicious behaviors probabilistically, police their downstream neighbors locally using overheard messages, and, thus, provide a secure global self-checking network. The proposed scheme gives the senders an active role in checking the node downstream. The advantage of this watchdog scheme over the signature scheme discussed in Section 1.5.1 is that the signature scheme assumes that the packets has to be correctly received at the peer in order to check its integrity. However, this watchdog scheme assumes noisy wireless channel over which the packets may contain some errors because of channel impairments.

The wireless network in this paper is modeled with a hypergraph $G = (V, E1, E2)$, where V is the set of the nodes in the network, E_1 is the set of hyperedges representing the connectivity (wireless links), and E_2 is the set of hyperedges representing the interference. We use the hypergraph to capture the broadcast nature of the wireless medium. If $(v_1, v_2) \in E_1$ and $(v_1, v_3) \in E_2$ where $v_1, v_2, v_3 \in V$, then there is an intended transmission from v_1 to v_2, and v_3 can overhear this transmission (possibly incorrectly). There is a certain transition probability associated with the interference channels known to the nodes, and we model them with binary channels.

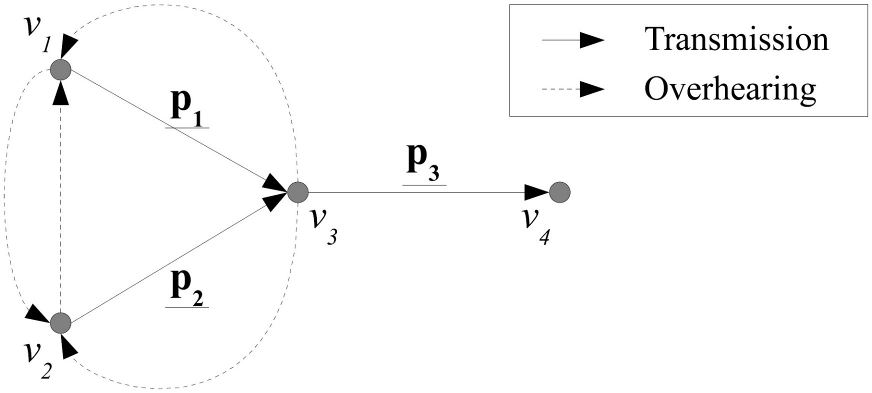


Figure 1.3 An example of a wireless network.

A node $v_i \in V$ transmits coded information x_i by transmitting a packet $\mathbf{p}_i$, where $\mathbf{p}_i = [\mathbf{a}_i, \mathbf{h}_{\mathbf{I}_i}, \mathbf{h}_{\mathbf{x}_i}, \mathbf{x}_i]$ is a $\{0,\ 1\}$-vector. A valid packet pi is defined as below:

- $\mathbf{a}_i$ corresponds to the coding coefficients $\alpha_j,\ j \in I_i$, where $I_i \subset V$ is the set of nodes adjacent to v_i in E_1
- $\mathbf{h}_{\mathbf{I}_i}$ corresponds to the hash $h(x_i)$, $v_j \in I_i$ where $h(.)$ is a h-bit polynomial hash function.
- $\mathbf{h}_{\mathbf{x}_i}$ corresponds to the hash $h(x_i)$, $v_j \in I_i$ where $h(.)$ is a h-bit polynomial hash function.
- $\mathbf{x}_i$ is the n-bit representation of $x_i = \sum_{j \in I} \alpha_j x_j$

The goal is to explore an approach to detect and prevent malicious behaviors in wireless networks using network coding. The scheme takes advantage of the wireless setting, where neighbors can overhear others transmissions albeit with some noise, to verify probabilistically that the next node in the path is behaving given the overheard transmissions.

As an example, consider the network (or a small neighborhood of nodes in a larger network) shown in figure 1.3. In this network, nodes v_1, v_2 want to transmit x_1, x_2 to v_4 via v_3. The

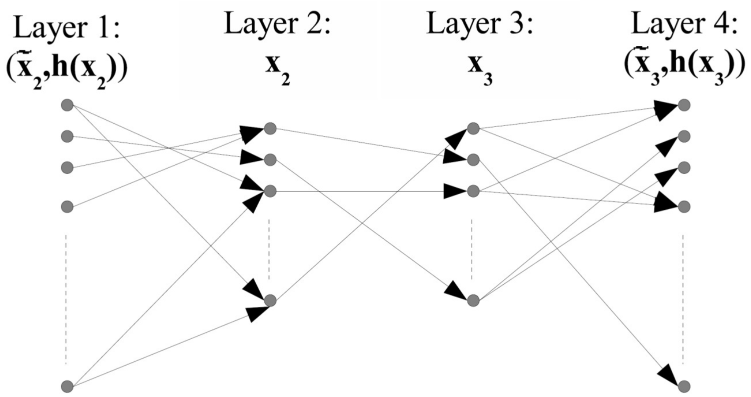

Layer 1:
$(\tilde{\mathbf{x}}_2,\mathbf{h}(\mathbf{x}_2))$
Layer 2:
$\mathbf{x}_2$
Layer 3:
$\mathbf{x}_3$
Layer 4:
$(\tilde{\mathbf{x}}_3,\mathbf{h}(\mathbf{x}_3))$

Figure 1.4 A graphical model from v_1s perspective.

authors proposed two models in their paper. The graphical model is used to explain how a node v_1 checks the behavior of its neighbor v_2. Then, the algebraic approach is used for analysis.

As shown in Figure 1.4, the graphical model has four layers: Layer 1 contains 2^{n+h} vertices, each representing a bit-representation of $[\widetilde{\mathbf{x}}_2, \mathbf{h}(\mathbf{x}_2)]$; Layer 2 contains 2^n vertices, each representing a bit-representation of $\mathbf{x}_2$; Layer 3 contains 2^n vertices corresponding to $\mathbf{x}_3$; and Layer 4 contains 2^{n+h} vertices corresponding to $[\widetilde{\mathbf{x}}_3, \mathbf{h}(\mathbf{x}_3)]$. Edges exist between adjacent layers as follows:

- Layer 1 to Layer 2: An edge exists between a vertex $[\mathbf{v}, \mathbf{u}]$ in Layer 1 and a vertex $\mathbf{w}$ in Layer 2 if and only if $\mathbf{h}(\mathbf{w}) = \mathbf{u}$. The edge weight is normalized such that the total weight of edges leaving $[\mathbf{v}, \mathbf{u}]$ is 1, and the weight is proportional to $\mathbf{P}(\mathbf{v}|$ Channel statistics and $\mathbf{w}$ is the original message) which is the probability that the inference channel outputs message $\mathbf{v}$ given an input message $\mathbf{w}$.

- Layer 2 to Layer 3: The edges represent a permutation. A vertex $\mathbf{v}$ in Layer 2 is adjacent to a vertex $\mathbf{w}$ in Layer 3 if and only if $w = c + \alpha_2 v$, where $c = \alpha_1 x_1$ is a constant, $\mathbf{v}$ and $\mathbf{w}$ are the bit-representation of v and w, respectively. The edge weights are all 1.

- Layer 3 to Layer 4: An edge exists between a vertex $\mathbf{v}$ in Layer 3 and a vertex $[\mathbf{w}, \mathbf{u}]$ in Layer 4 if and only if $\mathbf{h}(\mathbf{v}) = u$. The edge weight is normalized such that the total weight leaving v is 1, and is proportional to $\mathbf{P}(\mathbf{w}|$ Channel statistics and $\mathbf{v}$ is the original message)

Node $\mathbf{v}_1$ overhears the transmissions from $\mathbf{v}_2$ to $\mathbf{v}_3$ and from $\mathbf{v}_3$ to $\mathbf{v}_4$; therefore, it receives $[\widetilde{\mathbf{x}}_2, \mathbf{h}(\mathbf{x}_2)]$ and $[\widetilde{\mathbf{x}}_3, \mathbf{h}(\mathbf{x}_3)]$, corresponding to the starting point in Layer 1 and the destination point in Layer 4 respectively. By computing the sum of the product of the weights of all possible paths between the starting and the destination points, v_1 computes the probability that v_3 is consistent with the information gathered.

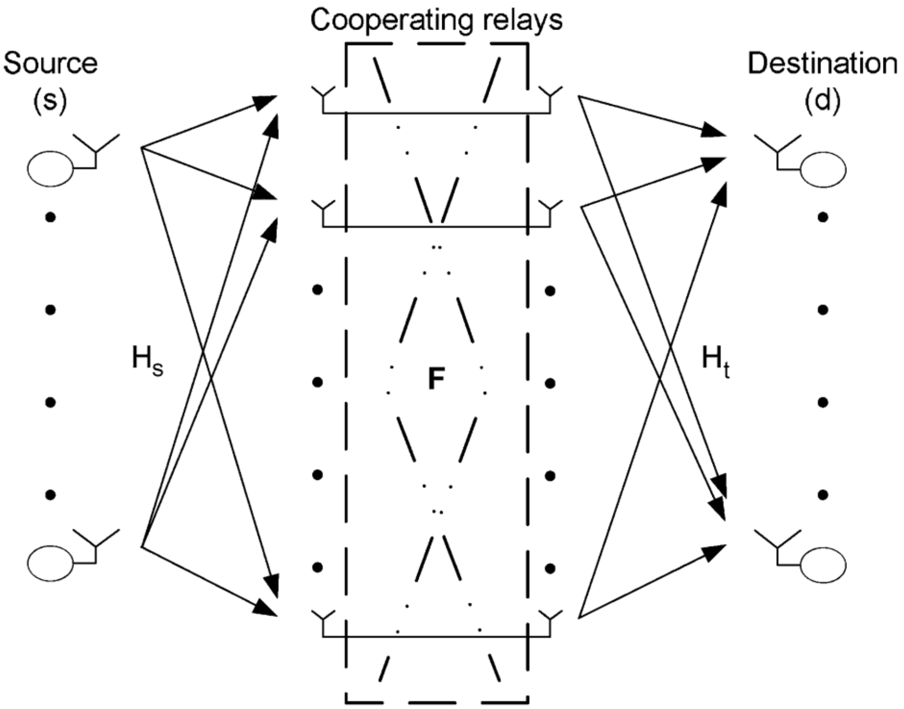


Figure 1.5 Relay network of M sources, M destinations, and N cooperating relay

1.5.3 A Cooperative MMSE Relay Strategy for Wireless Sensor Networks [21]

The authors of this paper proposed a minimum mean-square error (MMSE)-based signal forwarding technique for a cooperative relay network. They consider the transmission of information between multiple source-destination pairs through a set of relays. Transmission between M pairs of source-destination sensors through a set of N cooperative relay nodes is shown in 1.5. The signals vector $\mathbf{r}$ received at the relay nodes is given by

$$\mathbf{r} = H_s\mathbf{s} + \mathbf{v}_s \tag{1.13}$$

where H_s is the $N \times M$ channel matrix between source nodes and relay nodes, $\mathbf{s}$ is the transmitted data vector, and $\mathbf{v}_s$ is complex additive white Gaussian noise vector. The signals vector transmitted from the relay nodes is given by

$$\mathbf{x} = F\mathbf{r} \tag{1.14}$$

where F is an $N \times N$ transformation matrix to be determined in order to optimize receiver performance. The received signal at the destination sensors can be written as

$$\begin{aligned} \mathbf{t} &= H_t\mathbf{x} + \mathbf{v}_t \\ &= H_tFH_s\mathbf{s} + H_tF\mathbf{v}_s + \mathbf{v}_t \end{aligned} \tag{1.15}$$

where H_t is the $M \times N$ channel matrix between relay nodes and the destination nodes, and $\mathbf{v}_t$ is complex additive white Gaussian noise vector.

The authors in this paper aim to determine F in order to minimize the mean square error (MMSE) between the received signal $H_t\mathbf{x}$ and the transmitted signal $\mathbf{s}$, i.e.

$$\hat{F} = \arg\min F \sum_{m=1}^{M} E\left[\mathbf{h}_{t,m}\mathbf{x} - s_m\right]^2 \tag{1.16}$$

where $\mathbf{h}_{t,m}$ is the m-th column of H_t. The optimal value of F is given by

$$F_{opt} = \left(H_t^H H_t + \widetilde{\lambda} I\right)^{-1} H_t^H H_s^H \left(H_s H_s^H \sigma_s^2 + \sigma_{v_s}^2 I\right)^{-1} \sigma_s^2 \tag{1.17}$$

where σ_s^2 is the variance of the transmitted symbol, $\sigma_{v_s}^2$ is the variance of the noise components in $\mathbf{v}_s$, and $\widetilde{\lambda}$ is the Lagrangian multiplier and can be determined from the power constraint condition.

1.6 Research Contributions

In this work, we considered a multiple access relay network and investigated the following three problems: 1- Tradeoff Between Reliability and Security under Falsified Data Injection Attacks; 2- Prioritized Analog Relaying; 3- Mitigation of Forwarding Misbehaviors in Multiple Access Relay Network. We also consider the problem of delay Analysis in Message Ferrying System.

In the first problem, we consider a multiple access relay network where multiple sources send independent data to a single destination through multiple relays which may inject a falsified data into the network. To detect the malicious relays and discard (erase) data from them, tracing bits are embedded in the information data at each source node. Parity bits may be also added to correct the errors caused by fading and noise. When the total amount of redundancy, tracing bits plus parity bits, is fixed, an increase in parity bits to increase the reliability requires a decrease in tracing bits which leads to a less accurate detection of malicious behavior of relays, and vice versa. We investigate the tradeoff between the tracing bits and the parity bits in minimizing the probability of decoding error and maximizing the throughput in multi-source, multi-relay networks under falsified data injection attacks. The energy and throughput gains provided by the optimal allocation of redundancy and the tradeoff between reliability and security are analyzed.

In the second problem, we consider a multiple access relay network where multiple sources send independent data simultaneously to a common destination through multiple relay nodes. We present three prioritized analog cooperative relaying schemes that provide different quality of service (QoS) to different sources while being relayed at the same time in the same frequency band. The three schemes take the channel variations into account in determining the relay encoding (combining) rule, but differ in terms of whether or how relays cooperate. Simulation results on the symbol error probability and outage probability are provided to show the effectiveness of the proposed schemes.

In the third problem, we propose a physical layer approach to detect the relay node that injects false data or adds channel errors into the network encoder in multiple access relay networks. The misbehaving relay is detected by using the maximum a posteriori (MAP) detection rule which is optimal in the sense of minimizing the probability of incorrect decision (false alarm and miss detection). The proposed scheme does not require sending extra bits at the source, such as hash function or message authentication check bits, and hence there is no transmission overhead. The side information regarding the presence of forwarding misbehavior is exploited at the decoder to enhance the reliability of decoding. We derive the probability of false alarm and miss detection and the probability of bit error, taking into account the lossy nature of wireless links.

In the fourth problem, we consider the message ferrying system and analyze the total delay time in transferring the message between source and destination nodes taking into account the effect of channel fading, path loss, and forward error correction. The performance gain in terms of delay and energy provided by moving relay over static relay and the optimal locations of the moving relay that minimize the total delay are determined. Both simulations and analytical calculations are provided.

1.7 Thesis Organization

The remainder part of the thesis is organized as follows. In Chapter 2, we present an algorithm to detect malicious relays in MARN where the system model is described in Section 2.2, the error probability is analyzed in Section 2.3, and numerical results and discussions are presented in Section 2.4. In Chapter 3, we present prioritized relaying where the system model is described in Section 3.2, the prioritized relaying scheme is presented in Section 3.3, the tradeoff among cooperation extent, number of antennas per relay, and the number of relay nodes is analyzed in Section 3.3.3, and numerical results and discussions are presented in Section 3.4. In Chapter 4, we study the mitigation of forwarding misbehaviors in MARN where the system model is described in Section 4.2, the MAP detection scheme is presented in Section 4.3, and the derivations of probabilities of false alarm and miss detection are shown in Section 4.4. In chapter 4.8, we present the MAP detection scheme in the case of M-ary modulation. Finally, the conclusions and the future work are discussed in Chapter 6.

CHAPTER 2. Tradeoff Between Reliability and Security under Falsified Data Injection Attacks

We consider a multiple access relay network where multiple sources send independent data to a single destination through multiple relays which may inject a falsified data into the network. To detect the malicious relays and discard (erase) data from them, tracing bits are embedded in the information data at each source node. Parity bits may be also added to correct the errors caused by fading and noise. When the total amount of redundancy, tracing bits plus parity bits, is fixed, an increase in parity bits to increase the reliability requires a decrease in tracing bits which leads to a less accurate detection of malicious behavior of relays, and vice versa. We investigate the tradeoff between the tracing bits and the parity bits in minimizing the probability of decoding error and maximizing the throughput in multi-source, multi-relay networks under falsified data injection attacks. The energy and throughput gains provided by the optimal allocation of redundancy and the tradeoff between reliability and security are analyzed.

2.1 Introduction

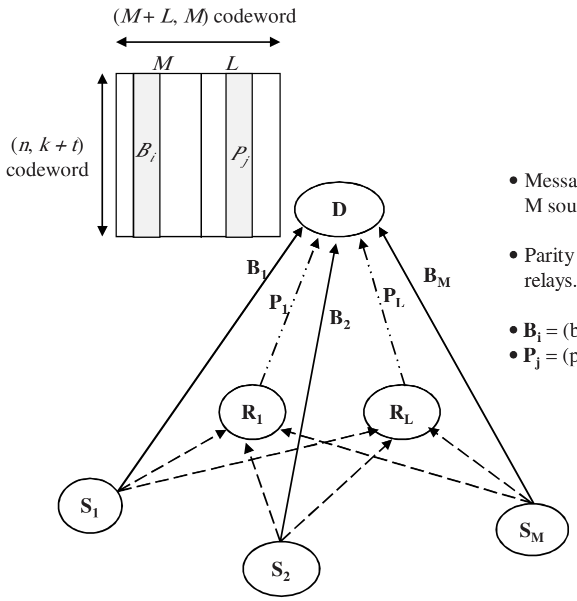
In multiple access relay networks, relay nodes may combine the symbols received from different sources to generate parity symbols and send them to the destination. Then, the destination may use the network generated parity symbols to enhance the reliability of decoding [31]-[37]. While this technology is promising in improving communication quality, it also presents a new challenge at the physical layer due to the dependency of the cooperation. That is, reliance on implicit trust relationship among participating nodes makes it more vulnerable to falsified data injection. Although this might also occur in a traditional system without cooperative communication, its effect is far more serious with cooperative communication. If a junk packet is mixed into the buffer of a node, the buffer will be polluted, the output of the node will become junk, and this may soon propagate to the entire network.

The problem of detecting malicious relay nodes in single-source, multi-relay networks has been studied in the literature for different relaying strategies [38]–[42]. Relay nodes in [38]–[40] apply network coding while those in [41, 42] follow the decode-and-forward protocol. In [38], the authors consider a peer-to-peer (P2P) network in which peers receive and forward a linear combination of the exogenous data packets. To check the integrity of the received packets, a signature vector is generated at the source node and broadcasted to all nodes where it is used to check the integrity of the received packets. In [39] and [40], several information theoretic algorithms for mitigating falsified data injection effects are proposed. The network model used in these works composed of single source, multiple intermediate nodes which apply network coding.

In all algorithms proposed in [38]–[40], there are two fundamental assumptions. First, all exogenous data packets are known at a single node to generate the hash or the signature vector. Therefore, these algorithms cannot be applied in multi-source scenarios because each source generates the packets independently and thus the packets of all sources are not available at a single node. Second, each received packet is decoded independently, and then the integrity of the decoded packet is checked using the hash or the signature vector. However, when the received packets are combined before decoding, a different approach should be developed to check the credibility (integrity) of the received packets. For example, in three-terminal cooperative diversity systems, the packets from the source and that from the relay are combined (e.g. using maximal ratio combining (MRC)) before decoding the message packet and then the integrity is checked on the decoded message packet. In [41], the authors consider inserting a number of tracing bits in the data stream at the source in a cryptographically secure manner in single source scenario. The receiver then computes the ground truth of the tracing bits and compares them with the tracing bits received from the relay path to determine whether a relay node is adversarial or cooperative. If the correlation between them is above a threshold then we decide that the relay node is cooperative (H_0) and, otherwise, it is malicious (H_1). The authors of [42] propose a statistical detection technique in order to mitigate malicious behavior in adaptive decode-and-forward (DF) cooperative diversity.

In this work, we consider exploiting the information on the presence of attack in enhancing the reliability of decoding by erasing (discarding) the data received from adversarial nodes and correcting the erasures. The motivation is that erasures can be corrected twice as many as errors [43]. However, the information on the presence of attack may not be perfect in practice. The false alarm results in an erasure of correct bit, while the miss detection may result in an error in place of an erasure. Since the probability of false alarm and that of miss detection depend on the amount of tracing bits and the errors-and-erasures correction capability depends on the amount of parity bits, we expect there exists an optimal allocation of the redundancy between tracing bits and parity bits that minimizes the probability of decoding error at the destination. Here, the tracing bits are to identify the malicious relay nodes and erase the data received from them, while the parity bits are to the correct errors caused by channel and noise. For a given redundancy, more parity bits (more reliability) implies less tracing bits (less security), and vice versa. That is, there exists a tradeoff between reliability and security. Once the malicious relay nodes are identified, some security measures such as en-route filtering [45] and/or containment [46] may be applied to limit the spread of false data. We investigate the optimal allocation of a given amount of redundancy (tradeoff) between tracing bits and parity bits and the resulting performance gain in terms of the probability of decoding error and the throughput.

The contributions of this part can be summarized as follow: 1) we propose an algorithm to detect the malicious relays in multi-source, multi-relay wireless networks where the relay nodes linerly combine the symbols of different sources; 2) we drive a closed form expression for the probability of decoding error after applying the detection algorithm; 3) we present the tradeoff between reliability and security in multiple access relay networks.



At **D**

- Message packets are received from M sources through direct links.
- Parity packets are received from L relays.
- $\mathbf{B_i} = (b_{i1}, b_{i2}, \ldots, b_{in})^T$, i = 1,2,…,M
- $\mathbf{P_j} = (p_{j1}, p_{j2}, \ldots, p_{jn})^T$, j = 1,2,…,L

Figure 2.1 M sources, L relays, and one destination wireless network.

2.2 System Model

We consider a two-hop multi-access relay network composed of M sources, one destination, and multiple relays, as shown in Figure 2.1. Each source generates an independent packets, each is composed of an $(n, k + t)$ codeword, where n is the code length, k is the number of information bits, t is the number of tracing bits, and $n-k-t$ is the number of parity bits. Each source is assigned an orthogonal channel (time or frequency) and sends its codeword to the destination. Due to the broadcast nature of the wireless medium, the relays may also receive the codewords. Each relay, after decoding, checks for errors using the cyclic redundancy check (CRC) code[1]. The set of relays that receive the all M codewords without errors is called the *decoding set*.

Each relay in the decoding set stores the received codewords in an $n \times M$ array. Then, it generates a parity bit for each row of the array and forwards the parity bits (one column) to the destination. Given that L relays are in the decoding set, the parity bit p_{lj} generated by

[1] This can be implemented by adding parity check bits on a block of message bits from each source for error detection.

the l-th relay, $l = 1, 2, \cdots, L$, is given by

$$p_{lj} = \sum_{i=1}^{M} g_{li} b_{ij}, \qquad j = 1, 2, \cdots, n \tag{2.1}$$

where $\{b_{ij}\}$ are the channel coded bits, $\{g_{li}\}$ are chosen to generate an $(M + L, M)$ network code for each row of the array. Thus, the destination may construct a two-dimensional $(n, k + t) \times (M + L, M)$ product code.

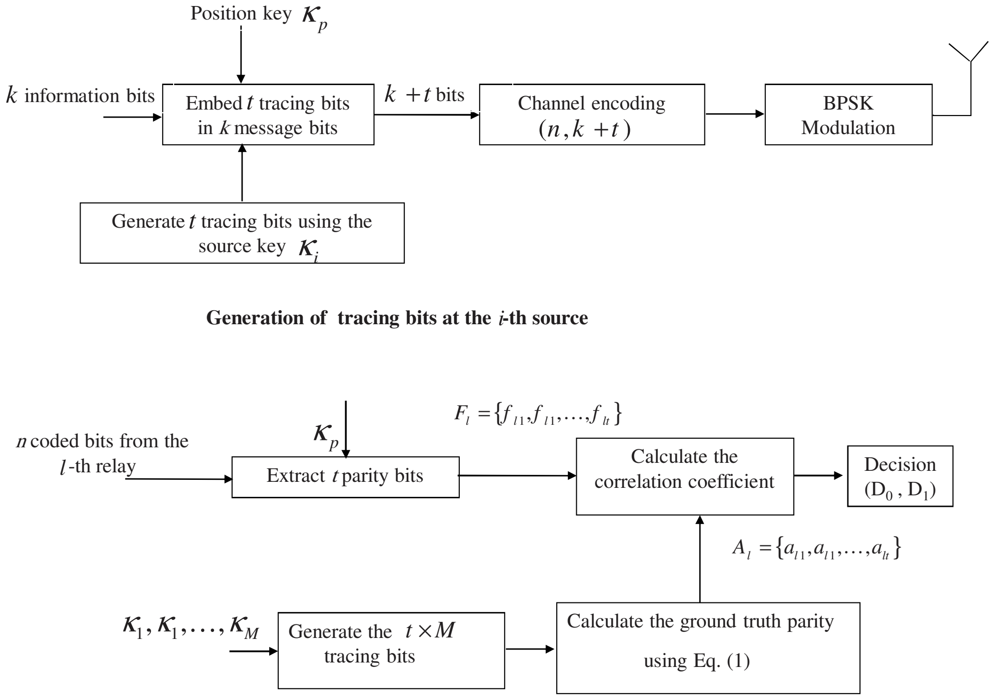
We assume that the channel between a node (source or relay) and the destination is modeled as Rayleigh flat fading and additive white Gaussian noise with mean zero and power spectral density of $N_0/2$. We assume that the message bits and the parity bits are transmitted using BPSK modulation.

2.2.1 Attack Model

One of the common adversarial attacks at the malicious relay node is to inject falsified data. In this work, we consider the attack model of changing the parity bit in (2.1) with probability ϵ at a malicious relay node. Here, $\epsilon = 1$ means all parity bits are flipped. In this case, once the malicious behavior of a relay is detected, the destination may invert the data to get the correct data. A more effective attack would be to change the parity bits with probability 1/2 which occurs when the malicious relay node sends a random bits instead of the original parity bits. In this case, the received data may not be useful at the destination. As ϵ is decreased, it becomes harder for the destination to detect the malicious behavior of the adversary. Hence, the adversary can better hide its malicious activity and complicate the detection process at the destination. We assume that traditional authentication schemes [47]–[50] are applied to ensure the authentication at the destination and thus the sources can be trusted.

2.2.2 Detection Algorithm

Figure 2.2 shows the schematic diagram of detecting malicious relay nodes. The i-th source node uses a secret key κ_i to generate a tracing sequence $C_i = \{c_{i1}, c_{i2}, \cdots, c_{it}\}$. We assume that κ_i is known only to the destination and the i-th source node. At each source, the tracing bits are embedded in the k message bits using a position key κ_p which is common for all sources


Position key K_p
k information bits
Embed t tracing bits in k message bits
$k+t$ bits
Channel encoding $(n,k+t)$
BPSK Modulation
Generate t tracing bits using the source key K_i
n coded bits from the l-th relay
K_p
Extract t parity bits
$F_l=\{f_{l1},f_{l1},\ldots,f_{lt}\}$
Calculate the correlation coefficient
Decision (D_0, D_1)
$A_l=\{a_{l1},a_{l1},\ldots,a_{lt}\}$
$K_1, K_1, \ldots, K_M$
Generate the $t\times M$ tracing bits
Calculate the ground truth parity using Eq. (1)

Generation of tracing bits at the *i*-th source

Testing of the *l*-th relay at the destination

Figure 2.2 Detection of malicious relays: source and destination work.

and is known to all source nodes and the destination. The generation and position keys are assumed to be unknown to the relay nodes. So, even if a relay is compromised the information on the tracing bits cannot be released to the attacker. The secret keys are exchanged at the time of setting the application layer keys. To increase the security level, keys may be updated periodically.

To detect malicious activity of the l-th relay, the destination calculates the Euclidean distance between the received linear combination of tracing sequences $F_l = (f_{l1}, f_{l2}, \cdots, f_{lt})$ and the ground truth bits $A_l = (a_{l1}, a_{l2}, \cdots, a_{lt})$:

$$\begin{aligned} d_l &= ||A_l - F_l||^2 \\ &= \sum_{m=1}^{t} (a_{lm} - f_{lm})^2 \\ &= \sum_{m=1}^{t} (a_{lm}^2 + f_{lm}^2) - \sum_{m=1}^{t} 2a_{lm}f_{lm} \end{aligned} \tag{2.2}$$

If d is greater than a threshold, the destination decides that the relay is malicious, and, otherwise, the relay is cooperative. The first term of (2.2) is $2t$ if $a_{lm}, f_{lm} \in \{+1, -1\}$, and the second term is the cross correlation between A_l and F_l. Since the first term of (2.2) is constant, the proposed detection algorithm relies only on the correlation coefficient between A_l and F_l. The following detection algorithm is applied at the destination to detect malicious relay nodes.

1. The secret key κ_i, $i = 1, 2, \cdots, M$, is used to generate the tracing sequence C_i of the i-th source.

2. The M tracing sequences, $C_1, C_2, \cdots, C_M$, are linearly combined bitwise using the same parity generation rule used at the relay nodes, i.e. (2.1), to generate the ground truth sequence $\{A_l = (a_{l1}, a_{l2}, \cdots, a_{lt})\}_{l=1}^{L}$, where $a_{lm} = \sum_{i=1}^{M} g_{li} c_{im}$, $m = 1, 2, \cdots, t$, and $a_{lm} \in \{-1, 1\}$.

3. The position key κ_p is used to extract the linearly combined tracing sequence $F_l = (f_{l1}, f_{l2}, \cdots, f_{lt})$ from what is received from the l-th relay node where $f_{lm} \in \{-1, 1\}$ [2] and $m = 1, 2, \cdots, t$. In case of no channel error and no attack, we should have $A_l = F_l$, $l = 1, 2, \cdots, L$.

4. The correlation coefficient ρ_l between A_l and F_l of the l-th relay is defined as

$$\rho_l = \frac{\sum_{j=1}^{t} a_{lj} f_{lj}}{\sqrt{\sum_{j=1}^{t} a_{lj}^2 \sum_{j=1}^{t} f_{lj}^2}} \qquad l = 1, 2, \cdots, L. \tag{2.3}$$

5. The correlation coefficient is compared with a threshold η to decide whether a relay is malicious (D_1) or cooperative (D_0) based on the following rule:

$$\rho_l \underset{D_1}{\overset{D_0}{\gtrless}} \eta \tag{2.4}$$

2.2.3 Decoding Process at the Destination

We assume that if a relay is determined to be malicious, then the parity bits from that relay are erased at the destination. The destination decodes the row vectors first to correct

[2] Soft detection of tracing bits is discussed in subsection 2.4.5.

the errors and erasures. Then the column vectors are decoded to correct the remaining errors after the row decoding.

2.3 Probability of Decoding Error

In this section, we drive the probability of decoding error at the destination. In our analysis, if a decoding error occurs in a row vector, we assume that the entire bits in the corresponding row vector are errornous (pessimistic assumption).

2.3.1 Probability Distribution of Correlation Coefficient

The probabilities of false alarm and miss detection depend on the probability distribution of the correlation coefficient ρ_l. Since $a_{lj}^2 = f_{lj}^2 = 1$, it follows from (2.3) that

$$\rho_l = \frac{1}{t} \sum_{j=1}^{t} a_{lj} f_{lj}. \tag{2.5}$$

We decide that the l-th relay is malicious (D_1) if $\rho_l < \eta$ and cooperative (D_0) otherwise. That is,

$$P(D_1) = P(\rho_l < \eta) \tag{2.6}$$

and

$$P(D_0) = P(\rho_l \geq \eta). \tag{2.7}$$

Let $x_{lj} = a_{lj} f_{lj}$. When the l-th relay is cooperative (H_0), the event $x_{lj} = -1$ (or $a_{lj} \neq f_{lj}$) occurs if the parity bit from the l-th relay node is received in error. Hence,

$$\begin{aligned} P(x_{lj} = -1 | H_0) =& \frac{1}{2} \left(1 - \sqrt{\frac{\bar{\gamma}_{RD}}{1 + \bar{\gamma}_{RD}}} \right) \\ =& p_{e_{RD}} \end{aligned} \tag{2.8}$$

where $\bar{\gamma}_{RD}$ is the average received SNR on the relay-to-destination channel. Assuming that errors within a codeword are independent (via interleaving), we obtain

$$P\left(\rho_l = \frac{2i}{t} - 1 | H_0 \right) = \binom{t}{i} (1 - p_{e_{RD}})^i p_{e_{RD}}^{t-i} \tag{2.9}$$

where $i = 0, 1, 2, ..., t$. When the relay is malicious (H_1), we have

$$\begin{aligned} P(x_{lj} = -1|H_1) =& \epsilon(1 - p_{e_{RD}}) + (1 - \epsilon)p_{e_{RD}} \\ =& \xi \end{aligned} \tag{2.10}$$

Hence,

$$P\left(\rho_l = \frac{2i}{t} - 1|H_1\right) = \binom{t}{i}(1 - \xi)^i \xi^{t-i} \tag{2.11}$$

2.3.2 Probability False Alarm and Miss Detection

The probability of false alarm is given by

$$\begin{aligned} P_{FA} &= P(D_1|H_0) \\ &= P(\rho_l < \eta|H_0) \\ &= \sum_{i=0}^{\left\lceil \frac{(\eta+1)t}{2} \right\rceil - 1} \binom{t}{i}(1 - p_{e_{RD}})^i p_{e_{RD}}^{t-i} \end{aligned} \tag{2.12}$$

and the probability of miss detection is given by

$$\begin{aligned} P_{MD} &= P(D_0|H_1) \\ &= P(\rho_l \geq \eta|H_1) \\ &= \sum_{i=\left\lceil \frac{(\eta+1)t}{2} \right\rceil}^{t} \binom{t}{i}(1 - \xi)^i \xi^{t-i} \end{aligned} \tag{2.13}$$

2.3.3 Probability of Bit Error and Bit Erasure

The parity bit from a relay node is erased if the destination decides that the relay node is malicious. Hence, the probability of erasing a relay-generated parity bit is given by

$$\begin{aligned} p_{er} &= P(D_1) \\ &= P(D_1|H_0)P(H_0) + P(D_1|H_1)P(H_1) \\ &= P_{FA}P(H_0) + (1 - P_{MD})\,P(H_1). \end{aligned} \tag{2.14}$$

The probability that an error occurs on a relay-generated parity bit is given by

$$\begin{aligned} p_{ep} = & P(\text{error}, D_0, H_0) + P(\text{error}, D_0, H_1) \\ & + P(\text{error}, D_1, H_0) + P(\text{error}, D_1, H_0) \end{aligned} \tag{2.15}$$

where the third and the fourth terms are zero because the relay parity bit is erased if D_1 occurs. Since $P(\text{error}|D_0, H_1) = \xi$, we obtain

$$\begin{aligned} p_{ep} &= P(\text{error}|D_0, H_0)P(D_0, H_0) \\ &\quad + P(\text{error}|D_0, H_1)P(D_0, H_1) \\ &= p_{e_{RD}} P(D_0, H_0) + \xi P(D_0, H_1) \\ &= p_{e_{RD}} \left(1 - P_{FA}\right) P(H_0) + \xi P_{MD} P(H_1) \end{aligned} \tag{2.16}$$

2.3.4 Probability of Decoding Error

In this subsection, we drive the probability of decoding error on the $(n, k+t) \times (M+L, M)$ product code. If the minimum distance of the $(M+L, M)$ code is d_h, the probability of decoding error on a row vector is given by

$$\begin{aligned} P_{E,R} = 1 - \sum_{m=0}^{A} \sum_{i=0}^{B} \sum_{j=0}^{C} & \binom{L}{m, i} p_{er}^{m} p_{ep}^{i} (1 - p_{er} - p_{ep})^{L-m-i} \\ & \times \binom{M}{j} p_{em}^{j} (1 - p_{em})^{M-j} \end{aligned} \tag{2.17}$$

where $A = d_h - 1$, $B = \left\lfloor \frac{d_h - 1 - m}{2} \right\rfloor$, $C = \left\lfloor \frac{d_h - 1 - m - 2i}{2} \right\rfloor$, $\binom{L}{m,i} = \frac{L!}{m!i!(L-m-i)!}$, and p_{em} is the probability of message bit error given by

$$p_{em} = \frac{1}{2}\left(1 - \sqrt{\frac{\bar{\gamma}_{SD}}{1 + \bar{\gamma}_{SD}}}\right) \tag{2.18}$$

where $\bar{\gamma}_{b_{SD}}$ is the average received SNR on the source-to-destination channel.

If a decoding occurs on a row vector then we assume that the entire bits in the corresponding row vector are erroneous (pessimistic assumption). This results in a bit error in all column vectors. If the column code $(n, k+t)$ can correct up to e errors, the probability on decoding error of a column vector is given by

$$P_{E,C} = \sum_{i=e+1}^{n} \binom{n}{i} P_{E,R}^{i} (1 - P_{E,R})^{n-i}. \tag{2.19}$$

Hence, the probability of decoding error for the $(n, k+t) \times (M+L, M)$ product code, hereafter referred to as *frame error rate*, is given by

$$P_B = 1 - (1 - P_{E,C})^{M}. \tag{2.20}$$

If there is no assistance from the relays, the probability of decoding error on a column vector is given by

$$P_{E,C} = \sum_{i=e+1}^{n} \binom{n}{i} p_{em}^{i} (1 - p_{em})^{n-i}. \tag{2.21}$$

Comparison of (2.19) and (2.21) suggests that the parity bits from relay nodes are helpful when $P_{E,R} < p_{em}$. Otherwise, it is better to discard the relay parity bits.

2.4 Numerical Results and Discussions

In this section, we present numerical results assuming that both row and column codes are BCH codes. Unless otherwise indicated, we assume that $\epsilon = 1/2$ and $\bar{\gamma}_{b_{SD}} = \bar{\gamma}_{b_{RD}} = \bar{\gamma}$.

2.4.1 Reliability-Security Tradeoff

When the total amount of redundancy $t + p$ is fixed, where p and t are the number of parity and tracing bits, respectively, an increase in t (more accurate detection of malicious relay nodes) requires a decrease in p (less error correction). Figures 2.3 and 2.4 show the frame error rate P_B versus the probability of false alarm P_{FA} and miss detection P_{MD}, respectively, when $t + p$ is fixed at 70 for an $(127, k + t)$ BCH code (i.e. $p = n - k - t$). In general, as t increases, P_{FA} and P_{MD} decrease, thereby achieving more accurate detection of malicious nodes. Once the malicious nodes are identified, security measures such as enroute filtering and/or containment techniques may be applied to limit the spread of false data. We find that there exists a fundamental tradeoff between the reliability measured by P_B and the security measured by P_{FA} and P_{MD}: as we require a higher security (lower P_{FA} and P_{MD}) we get a less reliability (higher P_B) and vice versa.

Figure 2.5 shows the frame error rate P_B versus the number of tracing bits t when $t + p$ is fixed at 70. We find that there exists an optimal t (and p) that minimizes P_B and that the optimal t is larger for higher $P(H_1)$. Hence, for higher $P(H_1)$, more redundancy should be allocated to the tracing bits in order to detect the malicious behavior of the relays more accurately. We also find that the optimal t that minimizes P_B decreases with decreasing SNR

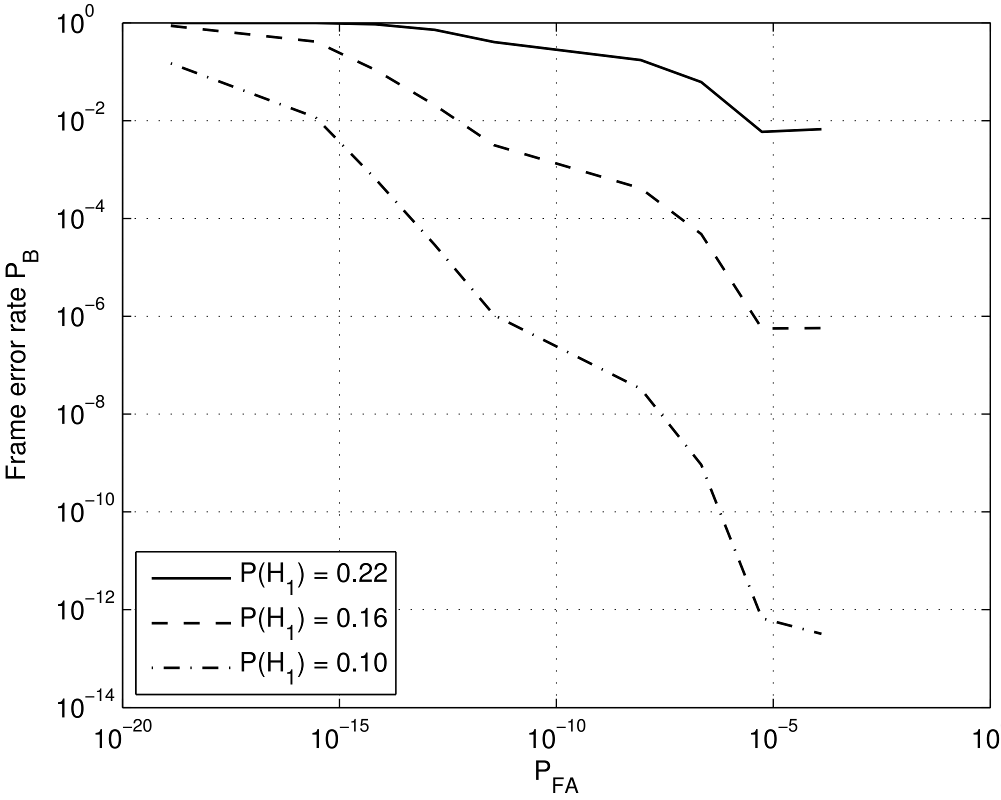


Figure 2.3 Frame error rate P_B versus probability of false alarm P_{FA}; $(127, 57+t)$ BCH code, $M = 7$, $L = 8$, $\bar{\gamma} = 20$ dB, $\eta = 0.65$.

$\bar{\gamma}$. Hence, for noisier channel, more redundancy should be allocated to the parity bits in order to correct more errors caused by the noise.

2.4.2 Optimal Choice of Decision Threshold

Since erasures can be corrected twice as many as errors and the number of errors and erasures depends on both P_{FA} and P_{MD}, we expect that there exists an optimal η that minimizes P_B. Figure 2.6 shows P_B versus the threshold η for several values of $P(H_1)$. We find that the optimal threshold that minimizes P_B lies in the range $0.45 \leq \rho_{opt} \leq 0.60$.

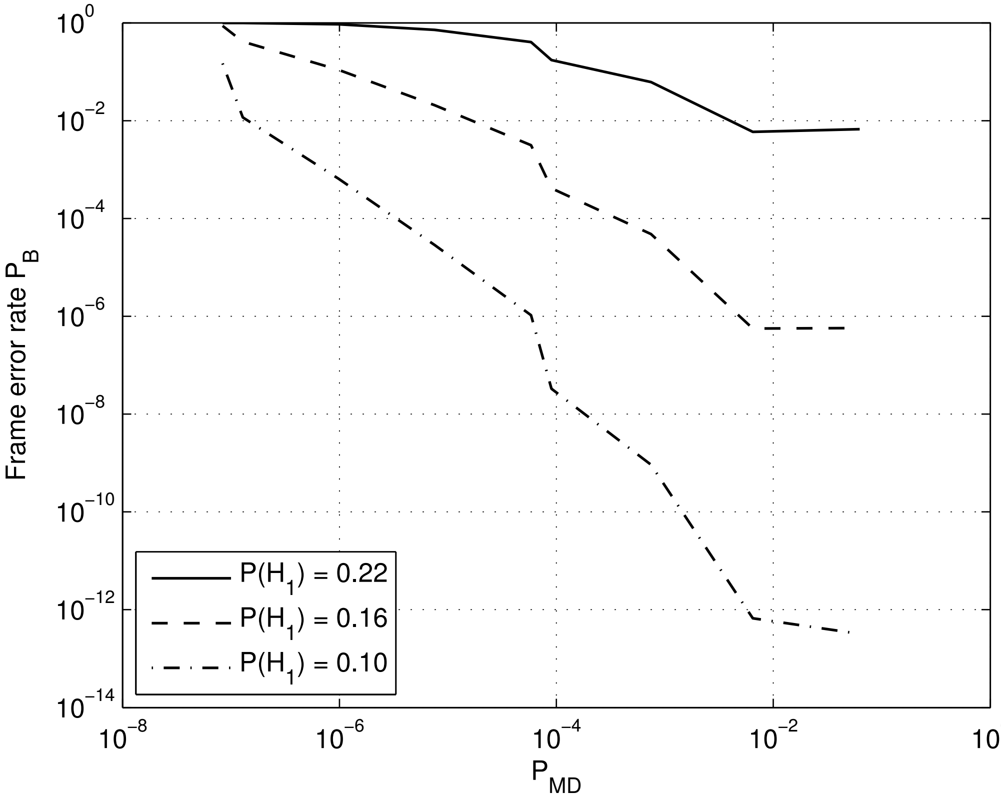


Figure 2.4 Frame error rate P_B versus probability of miss detection P_{MD}; $(127, 57+t)$ BCH code, $M = 7$, $L = 8$, $\bar{\gamma} = 20$ dB, $\eta = 0.65$.

2.4.3 SNR Gain

Figure 2.7 shows P_B versus the average bit SNR $\bar{\gamma}_b$, where $\bar{\gamma}_b = \bar{\gamma}\left(kM/(n(M+L))\right)^{-1}$ and $\bar{\gamma}$ is the average symbol SNR. We find that use of the optimal t provides a SNR gain of 10 dB at $P_B = 2 \times 10^{-4}$ over no tracing bits ($t = 0$). The error floor is due to a non-zero value of $P(H_1)$ that leads to a non-zero probability of erasure bit error regardless of SNR.

2.4.4 Throughput Gain

Figure 2.8 shows the throughput W versus the total redundancy $t + p$ for several values of $P(H_1)$, where the throughput is given by

$$W = \frac{kM}{n(M+L)}(1 - P_B) \tag{2.22}$$

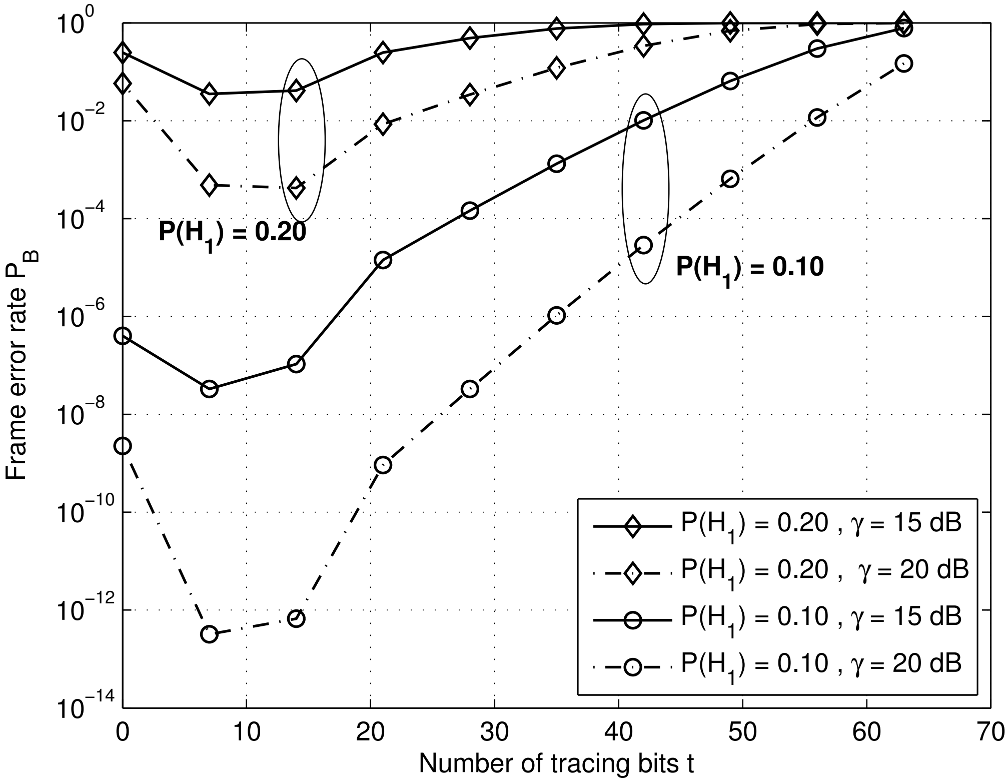


Figure 2.5 Frame error rate versus number of tracing bits t; $(127, 57 + t)$ BCH code, $t + p = 70$, $M = 7$, $L = 8$, $\eta = 0.65$.

The throughput is calculated using the optimal pair of t and p that minimizes P_B. We find that the optimal redundancy $t + p$ increases with the increase of $P(H_1)$ and that the falsified data injection can significantly reduce the throughput. When $P(H_1) = 0.2$, the maximum throughput is 0.293, whereas the maximum throughput in the case of no attack ($P(H_1) = 0)$ is 0.441.

2.4.5 Soft-Decision Correlation

The detection of malicious relays relies on the correlation between the ground truth bits and the detected parity bits. The accuracy of detection, measured by the probability of false alarm and miss detection, affects both security and reliability. If a relay node is identified to be malicious, then its data are erased (discarded) and erasure correction scheme can be used

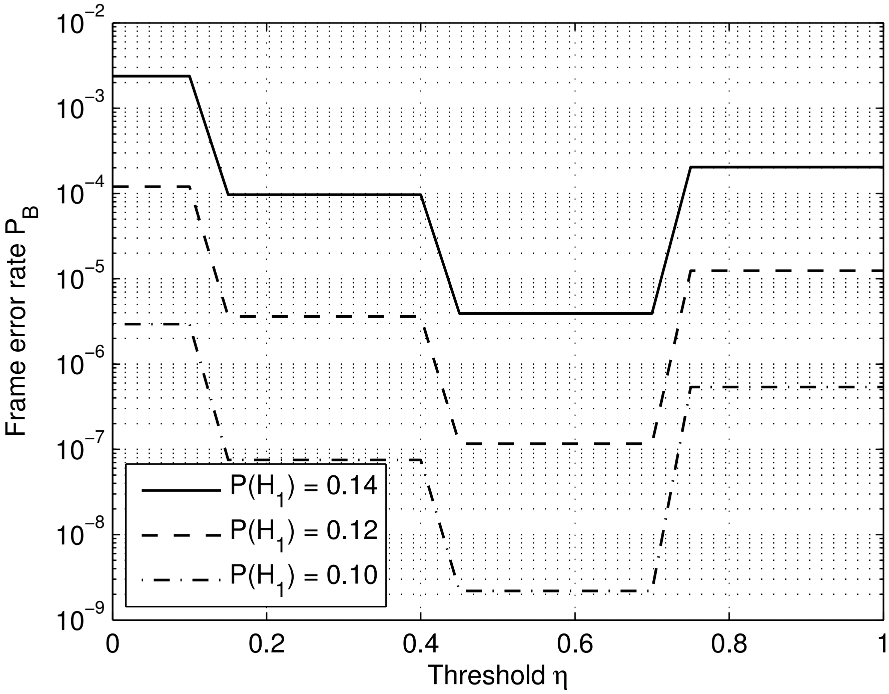


Figure 2.6 Frame error rate versus η; $(127, 57 + t)$ BCH code, $M = 7$, $L = 8$, $\bar{\gamma} = 22$ dB, $t = 7$.

to correct the erasures. Detection of malicious relay nodes may also allow further actions, such as en-route filtering [45] and/or containment [46] to limit the spread of falsified data, thereby enhancing the security. In this section, we discuss a soft-decision correlation (SC) technique that computes the correlation coefficient based on the soft (non-quantized) decision of the parity bits. We compare the performance of SC with the hard-decision correlation (HC) presented in Section 2.3.

Soft-decision Correlation Coefficient The received signal from the l-th relay node is given by

$$y_{lj} = h_{lj}s_{lj} + n_{lj} \qquad j = 1, 2, \cdots, n \tag{2.23}$$

where h_{lj} is the channel gain between the l-th relay and the destination, $s_{lj} \in \{+E_b, -E_b\}$ is the transmitted bit by the l-th relay, and n_{lj} is the additive white Gaussian noise. Without loss of generality, we assume that the t tracing bits are located in the first t coordinates of

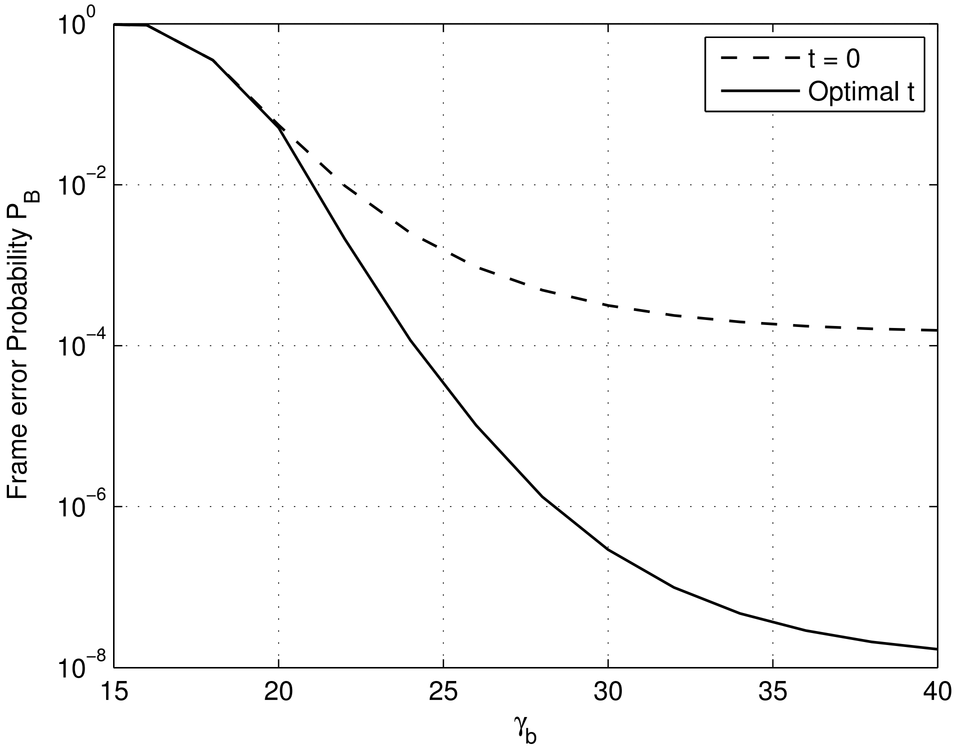


Figure 2.7 Frame error rate versus $\bar{\gamma}_b$; $(127, 50+t)$ BCH code, $M = 7$, $L = 8$, $P(H_1) = 0.18$, $\eta = 0.7$.

each codeword. Then, the soft-decision correlation coefficient is defined as

$$\begin{aligned}\rho_{S_l} =& \frac{\sum_{j=1}^{t} a_{lj} y_{lj}}{\sqrt{\sum_{j=1}^{t} a_{lj}^2 \sum_{j=1}^{t} y_{lj}^2}} \\ =& \frac{1}{\sqrt{t}} \frac{\sum_{j=1}^{t} a_{lj} y_{lj}}{\sqrt{\sum_{j=1}^{t} y_{lj}^2}} \qquad l = 1, 2, \cdots, L. \end{aligned} \tag{2.24}$$

It follows from Cauchy-Schwarz inequality that $-1 \leq \rho_{S_l} \leq +1$. Now, the value of ρ_{S_l} is compared with a threshold η to determine whether the l-th relay node is malicious ($\rho_{S_l} < \eta$) or cooperative ($\rho_{S_l} > \eta$).

Comparison between SC and HC Figure 2.9 shows the probability of false alarm P_{FA} and miss detection P_{MD} versus the number of tracing bits. We find that SC can significantly reduce P_{FA} and P_{MD} or the number of tracing bits for a given P_{FA} and P_{MD}. The saved redundancy can then be allocated to the parity bits to further enhance the reliability or be

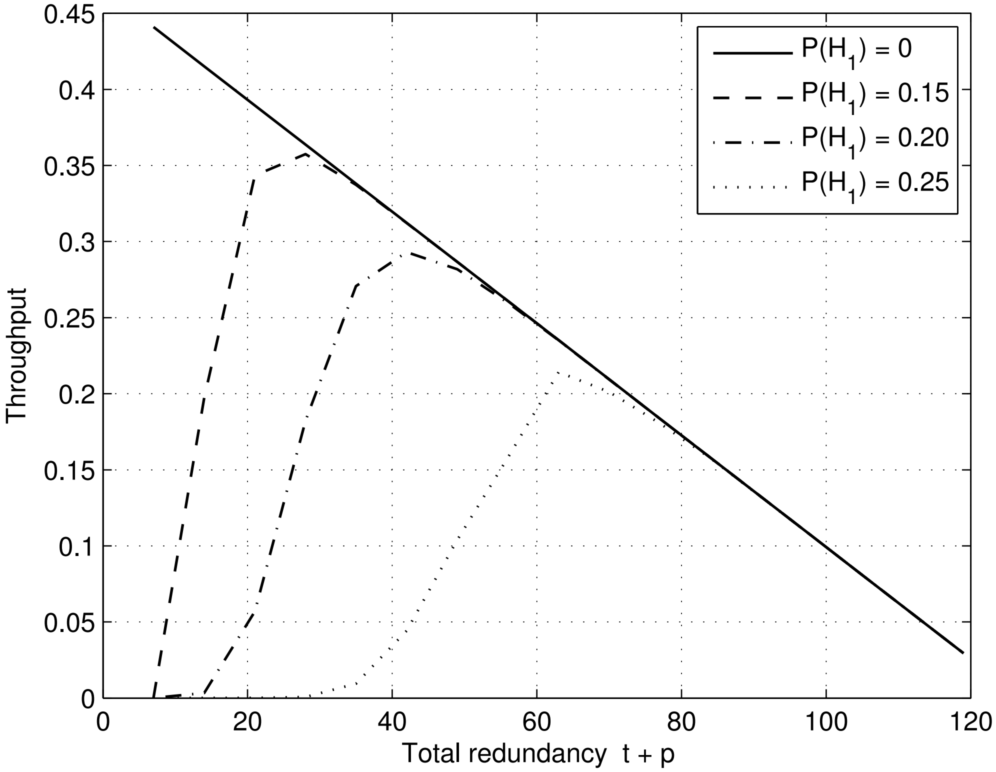


Figure 2.8 Throughput versus total redundancy $t+p$; $(127, 127-(t+p))$ BCH code, $M = 7$, $L = 8$, $\eta = 0.8$, $\bar{\gamma}_b = 30$ dB.

redirected towards sending more information bits to increase the throughput.

Figure 2.10 compares the throughputs with SC, HC, and no tracing bits ($t = 0$). We find that SC can increase the maximum throughput by about 7% over HC and 31.8% over no tracing bits.

Figure 2.11 shows the receiver operating characteristics (ROC) at different values of SNR. We find that the improvement provided by SC over HC is more significant at lower SNR $\bar{\gamma}$. This is because the SC is based on the actual value of the received signal while the HC is based on its quantized value. This quantization introduces a significant number of errors in making decisions on $\{F_{l_j}\}$'s in low SNR region, hence providing a low performance.

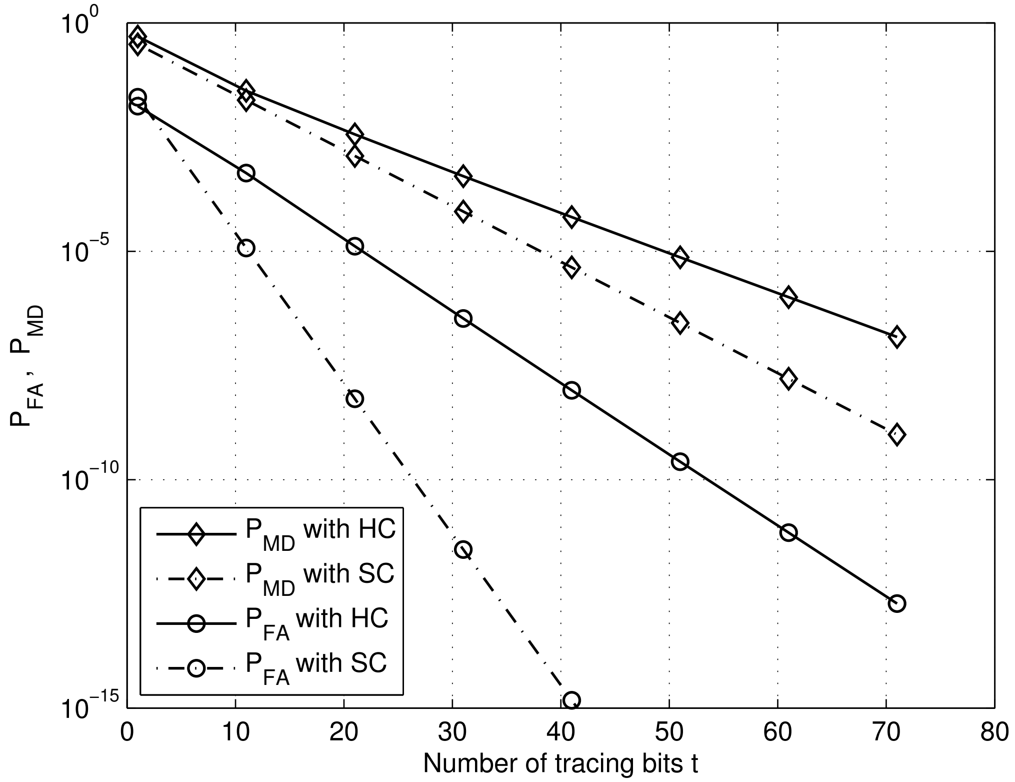


Figure 2.9 Probability of false alarm for SC and HC; $\bar{\gamma} = 12$ dB, $\eta = 0.60$.

2.4.6 Effect of Attack Probability ϵ

Figure 2.12 shows the frame error rate P_B against ϵ for different values of t when $t + p$ is fixed. We find that there exists an optimal ϵ (from adversary point of view) that maximizes P_B. This can be explained as follows. When ϵ is very small (close to 0), the adversary behaves almost like a cooperative relay. Hence, P_B would be small. However, if ϵ is very large (close to 1), almost all parity bits are changed by the adversary, making the received parity bits not useful for decoding. However, the malicious behavior can be easily detected (hence, corresponding parity bits are erased) by the destination due to low correlation. Hence, from the adversary point of view, there exists an optimal ϵ that maximizes P_B, and the optimal ϵ increases with decreasing t when $t + p$ is fixed. That is, if the communicator uses a small number of tracing bits (small t), then it is better for the adversary to increase the probability

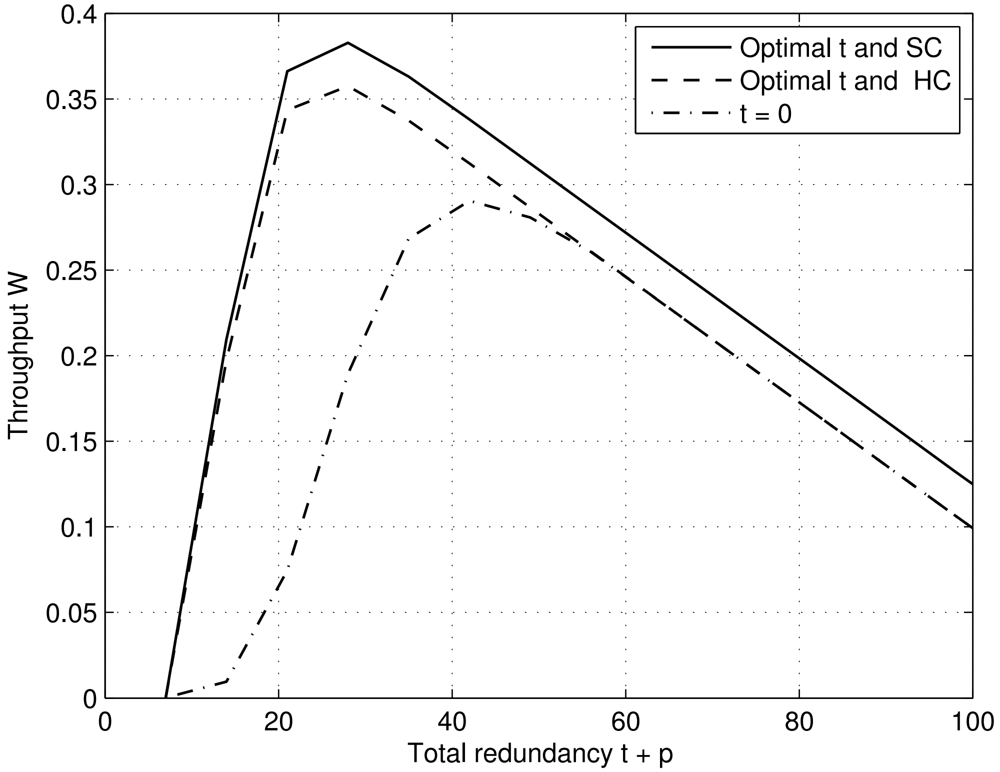


Figure 2.10 Throughput versus total redundancy $t+p$; $(127, 127-(t+p))$ BCH code, $M=7$, $L=8$, $\eta=0.8$, $\bar{\gamma}_b = 30$ dB, $P(H_1)=0.20$.

of changing the data (large ϵ), and vice versa. From the communicator point of view, when ϵ is small (say $\epsilon < 0.4$) allocating all available redundancy to the parity bits (hence, $t=0$) provides the lowest P_B. For higher ϵ, a proper combination of t and p provides the lowest P_B. For example, the optimal (t,p) pair is $(14,56)$ when $0.32 \leq \epsilon \leq 0.52$ for the given parameters in Figure 2.12.

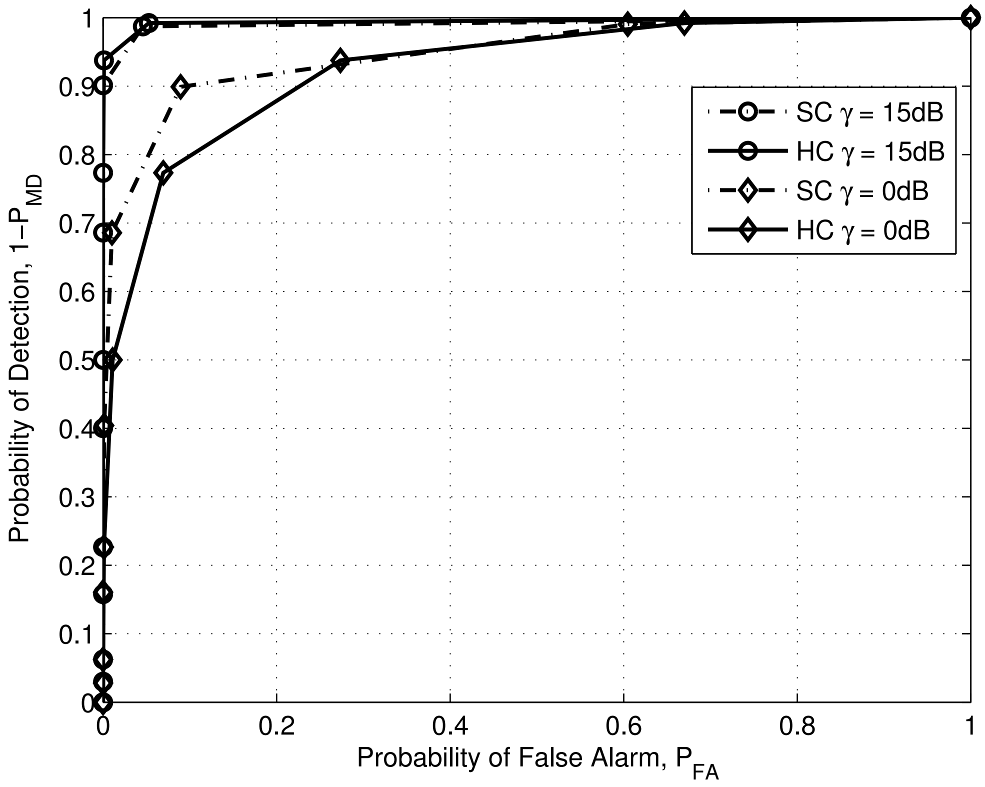


Figure 2.11 Receiver operating characteristics for SC and HC; $t = 7$.

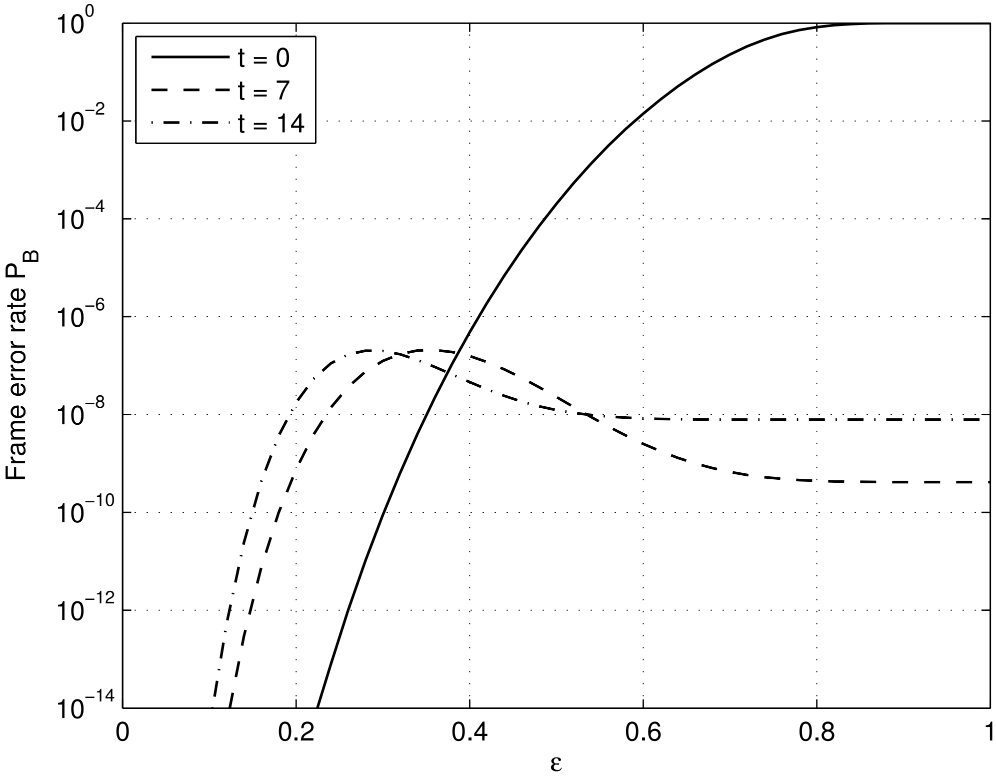


Figure 2.12 Frame error rate versus ϵ; $(127, 57 + t)$ BCH code, $t + p = 70$, $M = 7$, $L = 8$, $\bar{\gamma} = 25$ dB, $\eta = 0.65$.

CHAPTER 3. Prioritized Analog Relaying in Multiple Access Relay Networks

We consider a multiple access relay network where multiple sources send independent data simultaneously to a common destination through multiple relay nodes. We present three prioritized analog cooperative relaying schemes that provide different quality of service (QoS) to different sources while being relayed at the same time in the same frequency band. The three schemes take the channel variations into account in determining the relay encoding (combining) rule, but differ in terms of whether or how relays cooperate. Simulation results on the symbol error probability and outage probability are provided to show the effectiveness of the proposed schemes.

Keywords: Prioritized relaying, analog network coding, cooperation, multiple access relay network.

3.1 Introduction

Recently, cooperative relaying is gaining significant attention. In this approach, multiple intermediate nodes (relays) cooperate with each other to enhance the overall network efficiency. It exploits the physical-layer broadcast property offered by the wireless medium where the transmitted signals can be received and processed by any node in the neighborhood of a transmitter. The cooperative relaying approach has great potential to provide substantial benefits in terms of reliability (diversity gain) [5, 6] and rate (bandwidth or spectral efficiency) [9]-[12]. These benefits can extend the coverage, reduce network energy consumption, and promote uniform energy drainage by exploiting neighbors' resources. They can be of great value in many applications, including ad-hoc networks, mesh networks, and next generation wireless local area networks and cellular networks.

Several cooperative relaying protocols have been proposed in the literature to achieve different tasks. In the amplify-and forward (AF) protocol [5], the relay node simply amplifies the received signal and forwards the amplified version to the destination. The amplification weight at each relay node is chosen according to the relay power constraint. In the decode-and-forward (DF) protocol [5], the relay node decodes the received signal, re-encodes it, and forwards the encoded signal to the destination. In multiple-source relay networks, relay nodes may suppress the mutual interference among sources. Zero forcing (ZF) relaying is a scheme in which the interference among the sources can be completely removed by adjusting the weights at relay nodes [16]-[18]. The minimum mean square error (MMSE) relaying is another relaying scheme where the weights of relay nodes are adjusted to minimize the mean square error between the source signal and the received signal at the destination [20]-[22]. Coherent relaying, QR decomposition relaying, and distributed beamforming relaying, proposed in [23, 24] and [25], respectively, are some other examples of relaying schemes in multiple source relay networks. Although shown to be useful in a variety of theoretical and practical settings, they assume that all packets and nodes are *equally* important. In many communication scenarios, however, some packets may be more important (critical) than others or some nodes may require a higher priority than others. For instance, some nodes may need more assistance than others because of deep fading or limited battery. Providing a uniform protection of all nodes and packets may be either a wasteful or an infeasible approach in practical scenarios.

The role of relay nodes can be extended to provide different priorities to different sources. The authors of [19] consider a multiple-sources, multiple-destinations network and propose a distributed beamforming relaying scheme that provides different QoS requirements for each source-destination pair. The optimal beamforming weights are derived to meet a given set of target signal-to-interference-plus-noise ratio (SINR) while minimizing the total transmit power of the relay nodes. This work, however, assumes no cooperation among the relays and each relay is equipped with a single antenna.

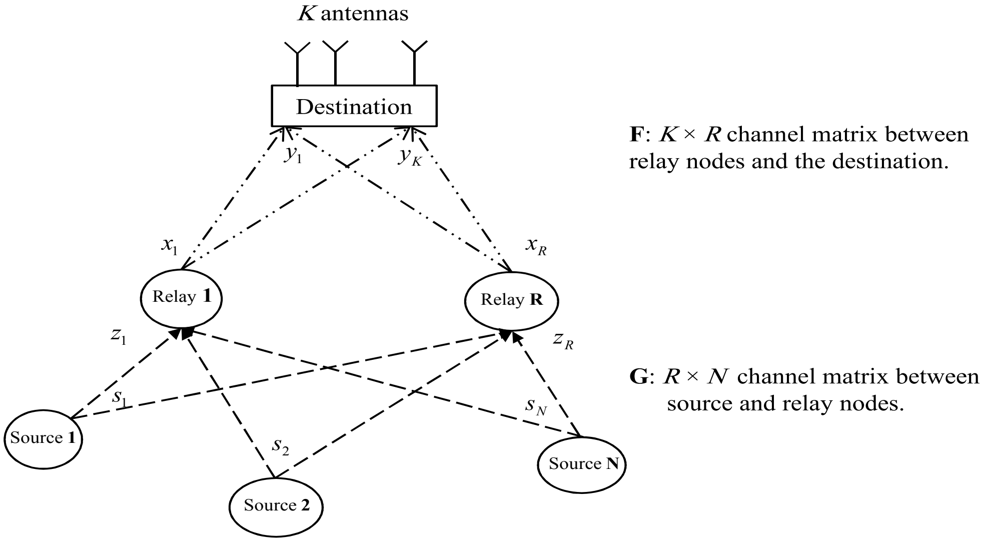
In this chapter, we consider a multiple access relay network in which the relays are equipped with multiple antennas and cooperate in relaying the messages in three different levels: no cooperation, partial cooperation, and full cooperation. We assume all nodes (sources or relays) send data simultaneously in the same frequency band, which enables the spectrum efficiency to be improved at the cost of increased computational complexity for suppressing the mutual interference. We present prioritized *analog* cooperative relaying schemes that provide different reliability or rate (QoS) to different sources in each relay cooperation scenario.

Method I considers the case where each relay does not know the received signals at other relays (i.e. no cooperation among relays). If there are N sources and the destination is equipped with K antennas, the required number of relays is KN assuming that each relay is equipped with a single antenna. Method II considers the case where each relay knows the received signals at other relays (i.e. full cooperation of relays). When each relay is equipped with a single antenna, this method requires $\max(N, K)$ relays. In Method III, relays are grouped and only the relays within a group are allowed to cooperate. Methods I and II can be considered as special cases of Method III where the group size is 1 and N, respectively. If the number of relays per group is L and each relay is equipped with M antennas, then the required number of relays with Method III can be shown to be $KN/(LM^2)$. This means that the required number of relays decreases on the order of $1/(LM^2)$. We present the symbol error rate and the outage probability of the three prioritized analog cooperative relaying schemes.

The remainder part of this chapter is organized as follows. The system model is described in Section 3.2. The prioritized cooperative relaying schemes are described in Section 3.3. The tradeoff among relay cooperations, number of antennas per relay, and the number of relays is discussed. Section 3.4 presents numerical results and discussions. Finally, the conclusions are drawn in Section 3.5.

3.2 System Model

We consider a two-hop multi-access relay network composed of N sources, R relays, and one destination, as illustrated in Figure 3.1. We first consider the case where source and relay nodes are equipped with a single antenna, and the destination node is equipped with K



K antennas
Destination
y_1
y_K
x_1
x_R
Relay 1
Relay R
z_1
z_R
s_1
s_2
s_N
Source 1
Source 2
Source N
F: $K \times R$ channel matrix between relay nodes and the destination.
G: $R \times N$ channel matrix between source and relay nodes.

Figure 3.1 System Model: N sources, R relays, one destination with K antennas

antennas. In Section 3.3.3, we consider a more general case where the relays have multiple antennas. We assume a two-phase communication scenario. In the first phase, the N sources send their symbols to the R relay nodes simultaneously over the same frequency band. In the second phase, each relay multiplies the received (mixed) signal by a certain weight and all relay nodes send their weighted signals to the destination simultaneously in the same frequency band. Because all nodes are sending simultaneously in the same frequency band, the spectrum efficiency can be significantly improved when compared to sending over orthogonal channels. We assume that the destination is located outside the transmission range of the N sources and therefore there is no direct link between source nodes and the destination. The destination determines the source messages based on the signals received from the relays.

We denote the normalized distance between the r-th relay and the n-th source by d_{rn} and that between the r-th relay and the destination by d_{rD}. The source-to-relay and relay-to-destination channels are modeled as Rayleigh flat fading with zero-mean additive complex white Gaussian noise. The channel gain matrix between sources and relays and that between relays and destination are denoted by $G \in \mathbb{C}_{R \times N}$ and $F \in \mathbb{C}_{K \times R}$, respectively. If we let g_{rn} be the entry in the r-th row and the n-th column of G, then the variance of g_{rn} is $d_{rn}^{-\alpha}$ where α is the path loss exponent. Similarly, the entries of F have variance $\{d_{rD}^{-\alpha}\}$. It is assumed that G and F are known at the destination node.

The received signal at the relay nodes in the first phase is given by

$$\mathbf{z} = G\mathbf{s} + \mathbf{n}_r \tag{3.1}$$

where $\mathbf{z} = [z_1 \; z_2 \; \cdots \; z_R]^T$ is an $R \times 1$ vector, $\mathbf{s} = [s_1 \; s_2 \; \cdots \; s_N]^T$ is the $N \times 1$ transmitted vector, and $\mathbf{n}_r$ is an $R \times 1$ ACWGN vector at the relay nodes. To enable a prioritized relaying, the received signals at the relay nodes are multiplied by a prioritization weight matrix A and sent to the destination simultaneously in the second phase. The transmit vector $\mathbf{x} = [x_1 \; x_2 \; \cdots \; x_R]^T$ at the relay nodes is given by

$$\mathbf{x} = \frac{q}{\sqrt{Tr\left(AA^{\dagger}\right)}} A\mathbf{z} \tag{3.2}$$

where A is an $R \times R$ prioritization wieght matrix, q is the amplification factor at each relay node, $\sqrt{Tr\left(AA^{\dagger}\right)}$ is a normalization factor, and "$\dagger$" stands for the conjugate transpose. The amplification factor q is chosen to adjust the transmit power of the relay nodes.

The received signal vector $\mathbf{y} = [y_1 \; y_2 \; \cdots \; y_K]^T$ at the destination in the second phase is given by

$$\begin{aligned} \mathbf{y} &= F\mathbf{x} + \mathbf{n}_d \\ &= \frac{q}{\sqrt{Tr\left(AA^{\dagger}\right)}} FA\mathbf{z} + \mathbf{n}_d \end{aligned} \tag{3.3}$$

where $\mathbf{n}_d$ is an $K \times 1$ ACWGN vector at the destination. The noise vectors $\mathbf{n}_r$, and $\mathbf{n}_d$ are assumed to have zero mean and covariance matrices $\sigma_{n_r}^2 I_R$, and $\sigma_{n_d}^2 I_K$, respectively, where I_R and I_K are identity matrices with sizes indicated in the subscripts.

Combining (3.1) and (3.3), the received signal vector at the destination can be expressed as

$$\mathbf{y} = \frac{q}{\sqrt{Tr\left(AA^{\dagger}\right)}} H\mathbf{s} + \mathbf{w} \tag{3.4}$$

where $H = FAG$ is $K \times N$ equivalent channel matrix and $\mathbf{w} = \mathbf{n}_d + \left(q/\sqrt{Tr\left(AA^{\dagger}\right)}\right) FA\mathbf{n}_r$ is a $K \times 1$ equivalent noise vector.

If we let E_s be the transmit symbol energy per source, i.e. $E_s = E\left[\left|s_i\right|^2\right]$, and E_r be the average transmit energy per relay, then the average transmit energy per symbol is given by

$$E_T = \frac{NE_s + RE_r}{N} \tag{3.5}$$

Since the total transmit energy of relay nodes is $Tr\left(E\left[\mathbf{x}\mathbf{x}^{\dagger}\right]\right)$, we obtain

$$\begin{aligned} RE_r =& Tr\left(E\left[\mathbf{x}\mathbf{x}^{\dagger}\right]\right) \\ =& E_s q^2 Tr\left(E\left[\frac{A^{\dagger}A}{Tr\left(AA^{\dagger}\right)} GG^{\dagger}\right]\right) + q^2 \sigma_{n_r}^2 \end{aligned} \tag{3.6}$$

Substituting (3.6) into (3.5) yields

$$q = \sqrt{\frac{N\left(E_T - E_s\right)}{E_s Tr\left(E\left[\frac{A^{\dagger}A}{Tr\left(AA^{\dagger}\right)} GG^{\dagger}\right]\right) + \sigma_{n_r}^2}} \tag{3.7}$$

3.3 Prioritized Analog Network Coding Schemes

In order to relay the n-th source with a higher priority than the m-th source, the average signal-to-interference-plus-noise ratio (SINR) of the n-th source, $\overline{\gamma}_n$, has to be higher than that of the m-th source, $\overline{\gamma}_m$. This prioritization can be achieved by carefully choosing the entries of the prioritization weight matrix A.

If $\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_N$ are the column vectors ($K \times 1$) of H, the received vector $\mathbf{y}$ in (3.4) can be written as

$$\mathbf{y} = \frac{q}{\sqrt{Tr\left(AA^{\dagger}\right)}} \left(\mathbf{h}_1 s_1 + \mathbf{h}_2 s_2 + \cdots + \mathbf{h}_N s_N\right) + \mathbf{w} \tag{3.8}$$

Then, the instantaneous SINR for the n-th source is given by

$$\gamma_n = \frac{\mathbf{h}_n^{\dagger}\mathbf{h}_n E_s q^2 / Tr\left(AA^{\dagger}\right)}{E_s q^2 \left(\sum_{\substack{i=1 \\ i \neq n}}^{N} \mathbf{h}_i^{\dagger}\mathbf{h}_i / Tr\left(AA^{\dagger}\right)\right) + E\left[\mathbf{w}^{\dagger}\mathbf{w}\right]} \tag{3.9}$$

After averaging the numerator and the denominator over A for a given $\mathbf{h}_n$, we obtain the average SINR

$$\overline{\gamma}_n = \frac{P_n E_s q^2 E\left[1/Tr\left(AA^\dagger\right)\right]}{E_s q^2 E\left[1/Tr\left(AA^\dagger\right)\right]\left(\sum_{\substack{i=1 \\ i\neq n}}^{N} P_i\right) + E\left[\mathbf{w}^\dagger \mathbf{w}\right]} \tag{3.10}$$

where $P_n = \mathbf{h}_n^\dagger \mathbf{h}_n$ is the received signal strength of the n-th source. Then, it is shown in Appendix A that $\overline{\gamma}_n \geq \overline{\gamma}_m$ if and only if $P_n \geq P_m$. Hence, the prioritization of the n-th source over the m-th source can be achieved by designing the prioritization matrix A such that $P_n > P_m$. Without loss of generality, we will assume $P_1 \geq P_2 \geq \cdots \geq P_N$ in what follows.

3.3.1 Method I (No Cooperation)

Method I assumes that each relay node does not know the received signals at other relays. Hence, the prioritization matrix A $(R \times R)$ is a diagonal matrix that satisfies

$$FAG = H \tag{3.11}$$

or

$$\sum_{r=1}^{R} f_{kr} g_{rn} a_{rr} = h_{kn} \tag{3.12}$$

where $k \in \{1, 2, \cdots, K\}$ and $n \in \{1, 2, \cdots, N\}$. Since the number of equations is KN and the number of unknowns $a_{11}, a_{22}, \cdots, a_{RR}$ is R, it is required R has to be KN in order to have a unique solution. This set of linear equations can be solved at the destination[1] and the solution $a_{11}, a_{22}, \cdots, a_{RR}$ can be fed back to the relay nodes.

3.3.2 Method II (Full Cooperation)

Method II assumes that each relay knows the received signals at all other relays. This requires a full cooperation among relays to share their received signals. Under this scenario, the solution for A that satisfies (3.11) can be obtained by multiplying H by the pseudo inverses of F and G as follows:

$$A = F^\dagger \left(FF^\dagger\right)^{-1} H \left(G^\dagger G\right)^{-1} G^\dagger \tag{3.13}$$

[1] It is assumed that the destination has all channel information $\{f_{kr}, g_{rn}\}$.

Table 3.1 Comparison between method I and method II

	Cooperation among relays	Minimum number of of relays	Minimum feedback overhead
Method I	None	NK	NK
Method II	Full	$\max(N, K)$	$[\max(N, K)]^2$

In order for the pseudo inverses of F $(K \times R)$ and G $(R \times N)$ to exist, it is required that $R \geq K$ and $R \geq N$, respectively. Therefore, the minimum number of relays is $\max(N, K)$. If K has to be at least N (e.g. zero-forcing), then the minimum number of relays is K. An alternate method to find A is to solve a set of linear equations. Since the number of equations is KN and the number of unknowns is R^2, the number of relays R should be $R \geq \sqrt{KN}$. When $P_1 = P_2 = \cdots = P_N$, A is found in [18] using the pseudo inverse solution. The matrix A may be calculated at the destination and fed back to the relay nodes.

Comparison Between Method I and Method II:

Table 3.1 summarizes the minimum number of relays and the amount of feedback from the destination to the relays with Method I and Method II. We can see that the cooperation among the relays can reduce the required number of relays by a factor of $1/N$ when $K = N$ at the cost of additional overhead of exchanging the received signals among the relays. In Section 3.3.3, we will discuss the tradeoff among the degree of relay cooperation, number of relays, and the number of antennas per relay.

Design of H: The decoding complexity at the destination can be reduced if H is a diagonal matrix with elements $\sqrt{P_1}, \sqrt{P_2}, \cdots, \sqrt{P_N}$ in the main diagonal for the case of $K = N$. This enables the interference among the sources to be completely removed while the received signal strengths are set to the desired levels.

3.3.3 Method III (Partial Cooperation)

Method I requires no cooperation among the relays but requires KN relays, while Method II requires full cooperation among the relays but requires $\max(K, N)$ relays. In both methods, it is assumed that each relay has a single antenna. In this subsection, we consider a more general scenario where R relays, each equipped with L antennas, are divided into groups and only those relays within a group are allowed to cooperate, i.e. share their received signals. Then, Methods I and II correspond to the special cases of group size being equal to 1 and N, respectively, and $L = 1$. We determine the relationship among the number of relays per group, number of antennas per relay, and the total number of relays in determining the prioritization matrix A that enables a certain prioritization.

If there are L relays in each group and each relay is equipped with M antennas, then the prioritization matrix A can have at most LM non-zero entries in each row. The matrix A is a *block diagonal* matrix of the form

$$A = \begin{bmatrix} A_1 & & & \mathbf{0} \\ & A_2 & & \\ & & \ddots & \\ \mathbf{0} & & & A_{R/L} \end{bmatrix} \qquad (3.14)$$

where $A_1, A_2, \cdots, A_{R/L}$ are $LM \times LM$ matrices. Since the number of equations in (3.11) is KN and the number of unknowns, i.e. the number of non-zero entries of A is $(R/L)(LM)^2$, the number of relays R has to be equal to $KN/(LM^2)$ in order to get a unique solution for (3.11). It should be noted that the required number of relays decreases on the order of $1/(LM^2)$. This shows that increasing the number of cooperating relays and, more importantly, the number of antennas per relay are vital in reducing the required total number of relays. The set of linear equations used to solve for entries of A that satisfies (3.11) is given by

$$\sum_{t=0}^{R/L-1} \sum_{i=1}^{LM} \sum_{j=1}^{LM} f_{k(i+LMt)} g_{(j+LMt)n} a_{(i+LMt)(j+LMt)} = h_{kn} \qquad (3.15)$$

for $k \in \{1, 2, \cdots, K\}$, $n \in \{1, 2, \cdots, N\}$.

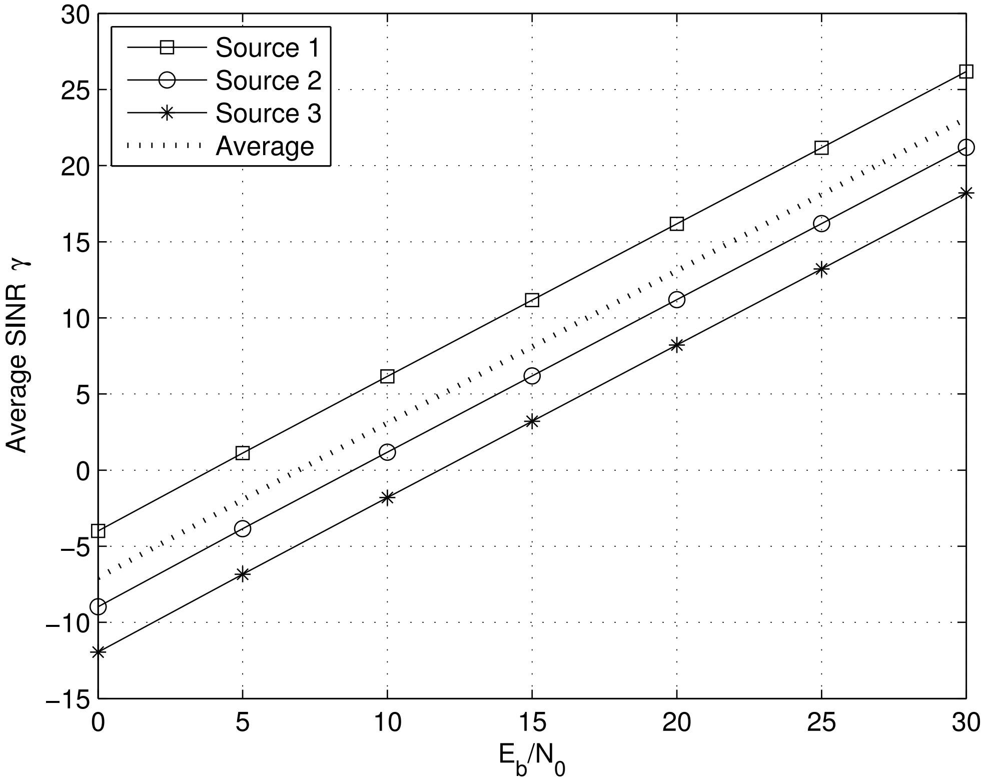


Figure 3.2 Average SINR $\overline{\gamma}$ vs E_b/N_0, Method I; $N = 3, K = 3, R = 9$, $\Delta_{12} = 5dB$, $\Delta_{23} = 3dB$.

3.4 Simulation Results and Discussion

In this section, we present simulation results for the average symbol error rate (SER) and the outage probability, P_{out}. We consider 4-QAM modulation with $E_s = E_T/2$ and H is a diagonal matrix with $P_1 = 1$ $(0dB)$. We assume that $\alpha = 3$, $d_{rD} = 1$ for all r, and d_{rn} is uniformly distributed between 0.5 and 1.5.

Fig. 3.2 shows the average SINR against E_b/N_0 with Method I for the case of 3 sources, 3 antennas at the destination $(K = 3)$, and 9 relays, where E_b/N_0 is the transmit SNR per information bit. The diagonal elements $\sqrt{P_1}, \sqrt{P_2}, \sqrt{P_3}$ of H are chosen such that $P_1 = 0dB$, $P_2 = -5dB$, and $P_3 = -8dB$. If we let $\Delta_{ij} = 10 \log_{10}(P_i/P_j)$ be the relative power gain for the i-th source over the j-th source, then $\Delta_{12} = 5dB$ and $\Delta_{23} = 3dB$. Fig. 3.3 shows

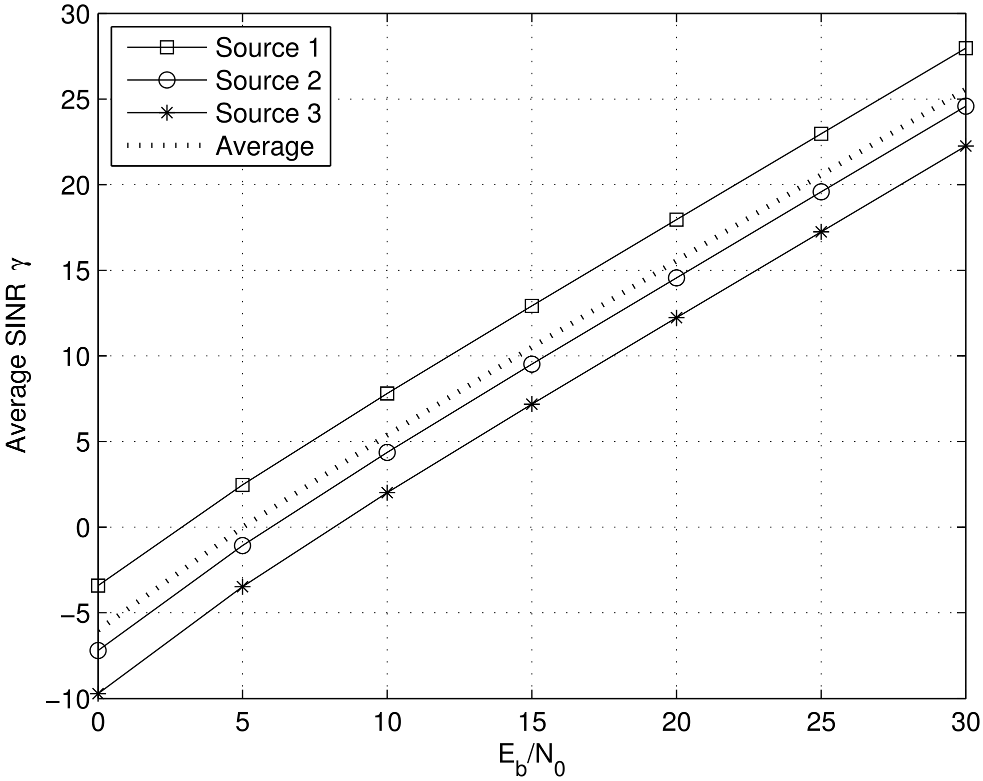


Figure 3.3 Average SINR $\overline{\gamma}$ vs E_b/N_0, Method II; $N = 3, K = 3, R = 3$, $\Delta_{12} = 5dB$, $\Delta_{23} = 3dB$.

the average SINR against E_b/N_0 with Method II for the case of 3 sources, 3 antennas at the destination ($K = 3$), and 3 relays. Figs 3.4 and 3.5 show the SER against E_b/N_0 with Method I and Method II, respectively, for the same set of SINRs. We can see that Methods I and II can indeed achieve a prescribed set of SINRs. Fig. 3.6 compares the average SER, averaged over all sources, with Method I and II when $N = 2, K = 2, R = 4$. We find that the average SER with Method II is much lower than that with Method I, mainly due to the diversity order of 3 with Method II and the diversity order of 1 with Method I. Method II requires $R = \max(K, N) = 2$ to get A from (3.13) while Method I requires $R = KN = 4$ to get a_{rr} from (3.12). Hence, the remaining two relays in Method II can be used to increase the diversity order by two. However, it should be noted that this diversity gain is achieved at the cost of relay cooperation.

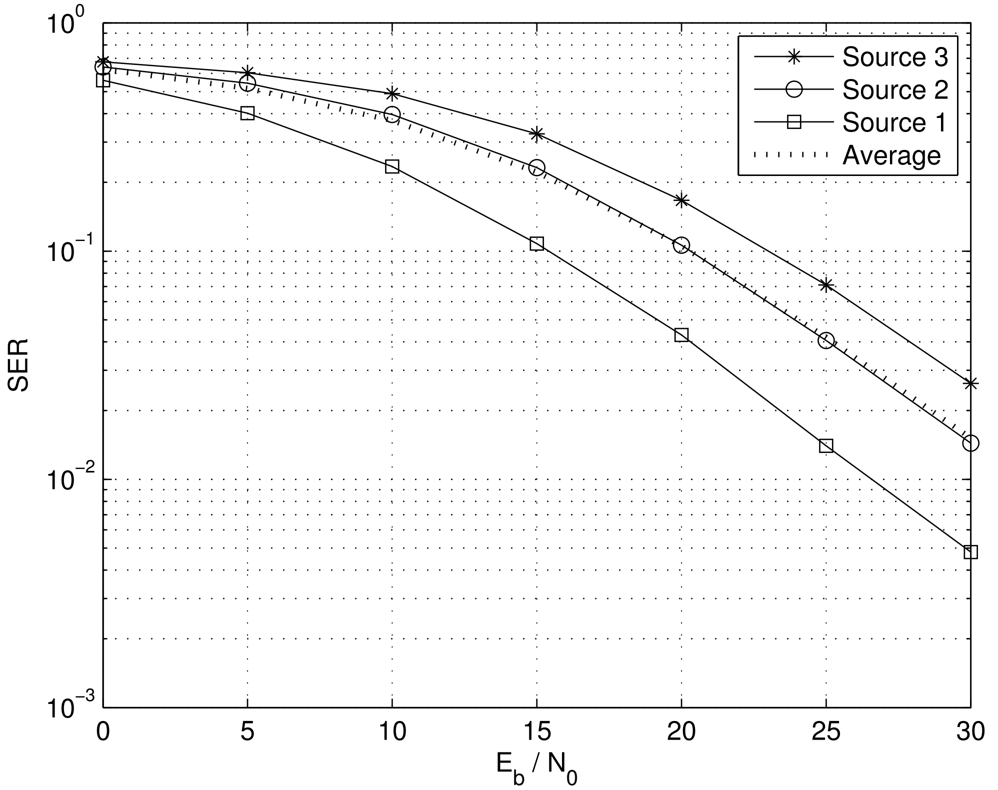


Figure 3.4 SER vs E_b/N_0 with Method I; $N = 3, K = 3, R = 9$, $\Delta_{12} = 5dB$, $\Delta_{23} = 3dB$.

Now, consider the case when $N = 4, K = 4$ and $\Delta_{n(n+1)} = 5dB$ where each relay has a single antenna and two relays are allowed to cooperate (i.e., $M = 1, L = 2$) in Method III. Therefore, the minimum number of relay nodes is $R = 8$. Fig. 3.7 shows the SER against E_b/N_0 for this case. We find that the n-th source has a better SER performance than the $(n+1)$-th source. We also find that the n-th source outperforms the $(n+1)$-th source by exactly $5dB$ at any given SER. Fig. 3.8 compares the average SER, averaged over all sources, for different sets of L and M. $L = 1, M = 1, R = 16$ corresponds to Method I, $L = 4, M = 1, R = 4$ corresponds to Method II, and $L = 2, M = 2, R = 2$ corresponds to Method III. We can see that Method II and III performs almost identically, while Method I performs worse than Methods II and III.

Figs 3.9 and 3.10 show the outage probability P_{out} against a target rate η when sources are prioritized using Method I and Method II, respectively. The outage probability of the n-th

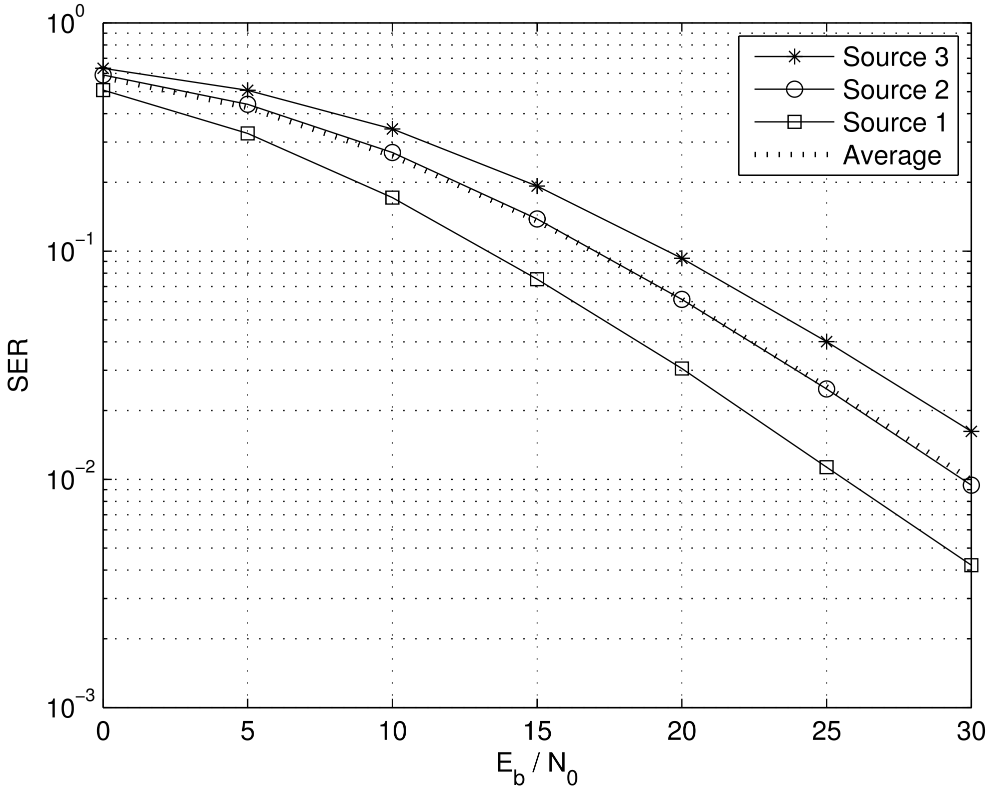


Figure 3.5 SER vs E_b/N_0 with Method II; $N = 3, K = 3, R = 3$, $\Delta_{12} = 5dB$, $\Delta_{23} = 3dB$.

source is defined by

$$P_{out} = Pr\left[\frac{1}{2}\log_2\left(1+\gamma_n\right) < \eta\right] \tag{3.16}$$

We can see that the prioritized sources can achieve a higher rate than non-prioritized sources for the same outage probability.

3.5 Conclusions

We proposed prioritized analog cooperative relaying schemes that provide different SINRs to different sources in multiple access relay networks. We considered a general system model in which relay nodes have multiple antennas and cooperate in relaying the overheard messages in three different levels: no cooperation, partial cooperation, and full cooperation. The proposed

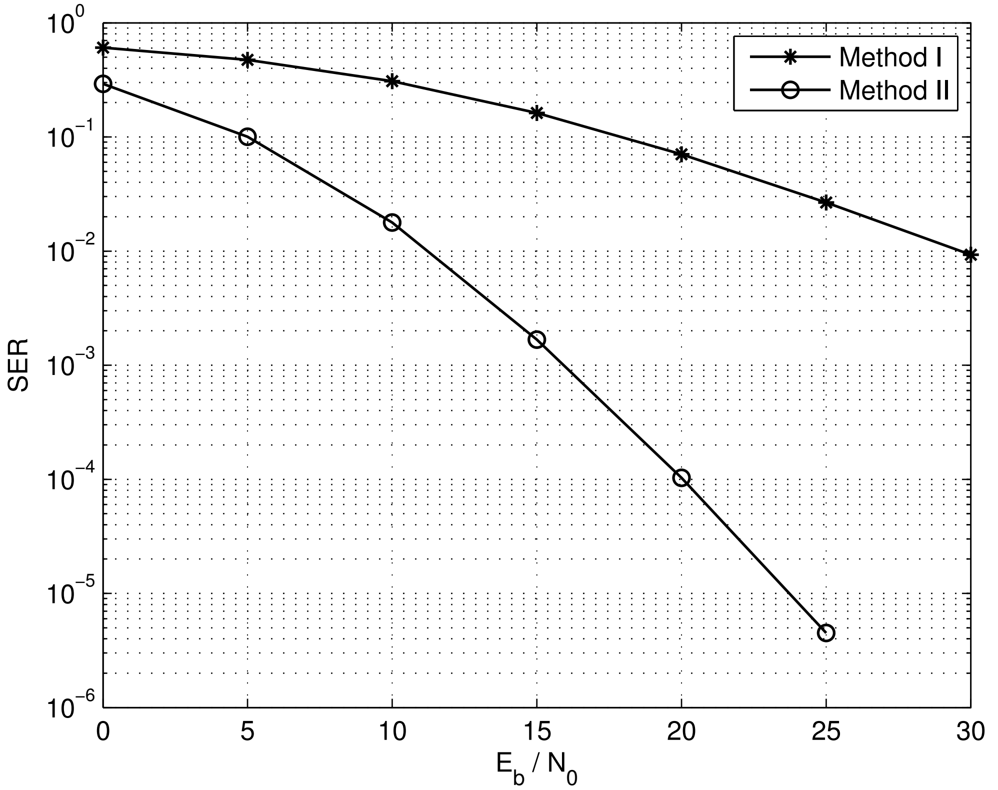


Figure 3.6 SER vs E_b/N_0; $N = 2, K = 2, R = 4$.

schemes enable the source with a higher priority level to send data at a higher rate or lower error probability while being relayed with other sources at the same time in the same bandwidth. This enables the spectrum efficiency to be improved at the cost of increased computational complexity for suppressing the mutual interference. We discussed the required number of relays as a function of the number of antennas per relay and the number of cooperating relays. Our simulation results show that the proposed cooperative relaying schemes can indeed achieve the prescribed set of prioritizations.

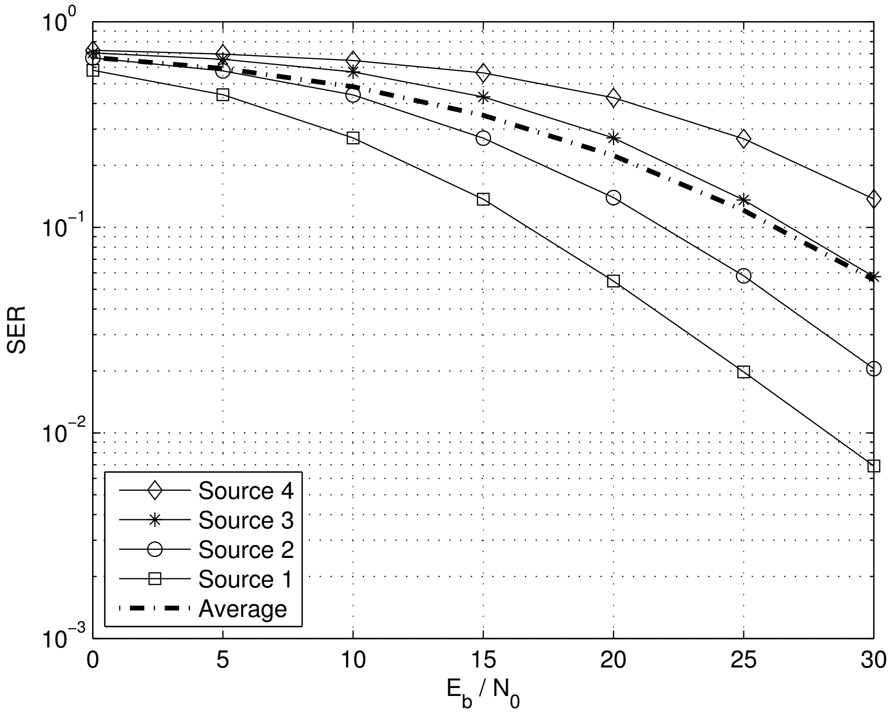


Figure 3.7 SER vs E_b/N_0 with Method III; $N = 4$, $K = 4$, $L = 2$, $M = 1$, $R = 8$, $\Delta_{12} = \Delta_{23} = \Delta_{34} = 5dB$.

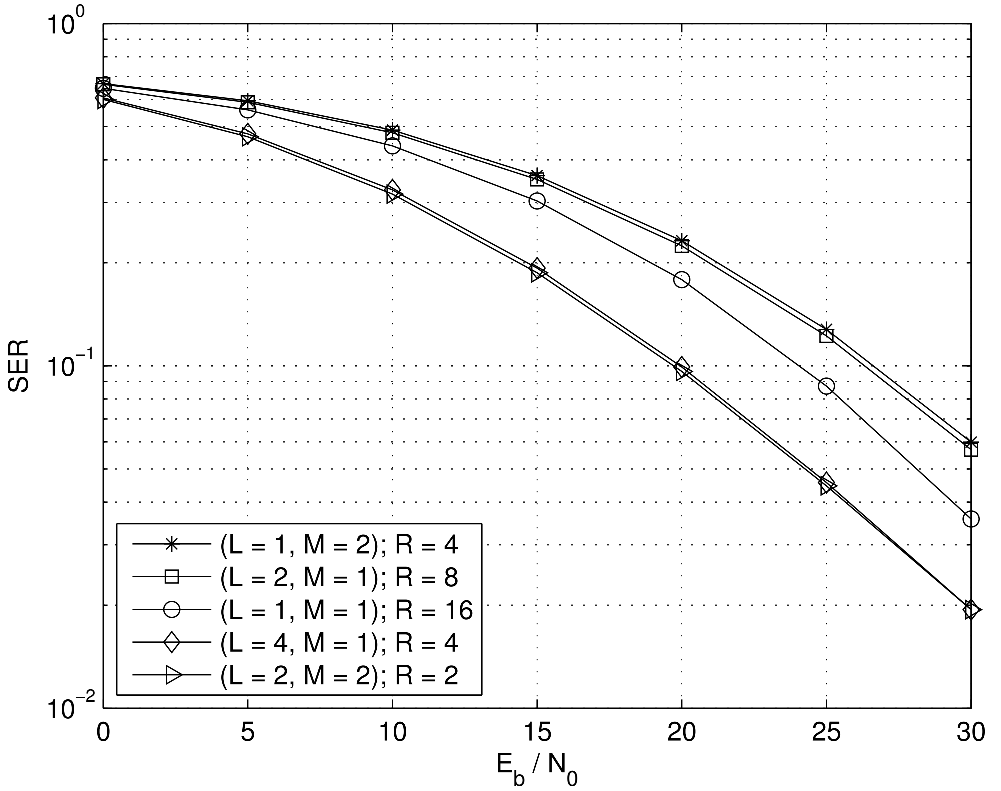


Figure 3.8 SER vs E_b/N_0; $N = 4, K = 4$.

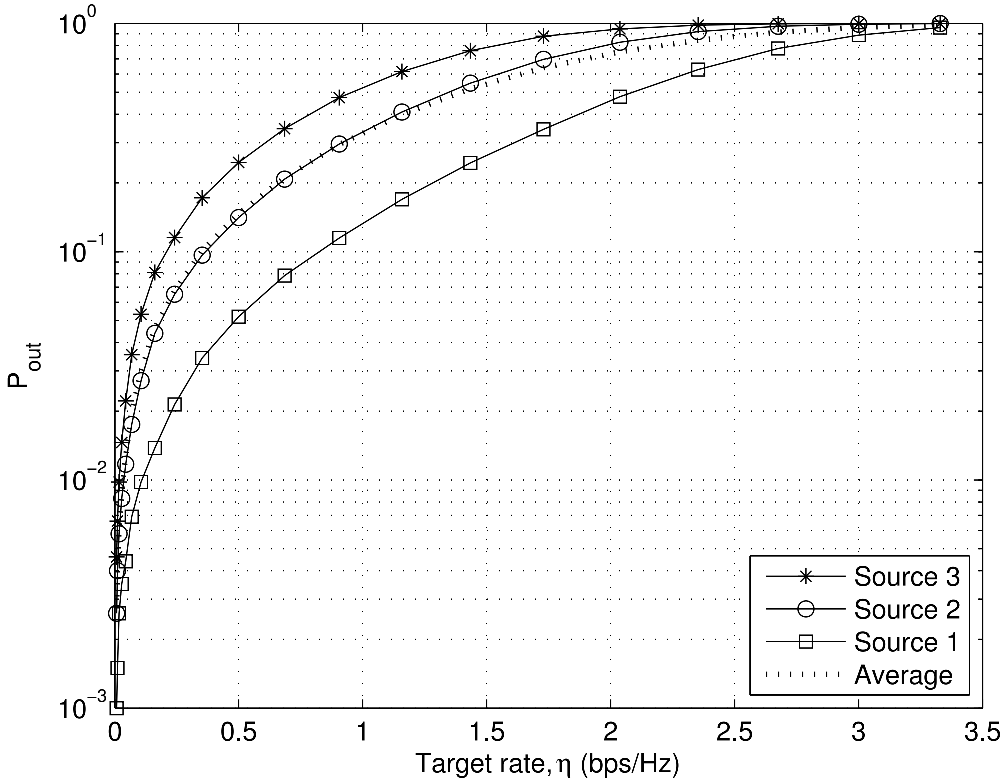


Figure 3.9 Outage Probability vs rate (η) with Method I; $N = 3$, $K = 3$, $R = 9$, $\Delta_{12} = 5dB, \Delta_{23} = 3dB$, $E_b/N_0 = 20dB$.

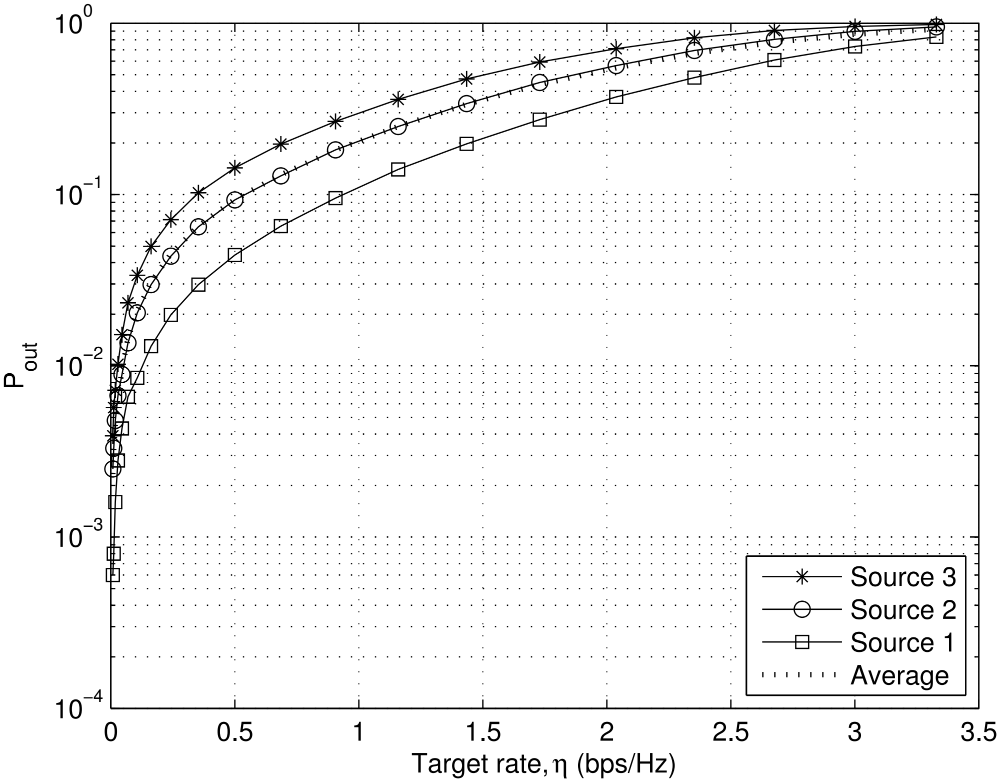


Figure 3.10 Outage Probability vs rate (η) with Method II; $N = 3$, $K = 3$, $R = 3$, $\Delta_{12} = 5dB$, $\Delta_{23} = 3dB$, $E_b/N_0 = 20dB$.

CHAPTER 4. Mitigation of Forwarding Misbehaviors in Multiple Access Relay Network

We propose a physical layer approach to detect the relay node that injects false data or adds channel errors into the network encoder in multiple access relay networks. The misbehaving relay is detected by using the maximum a posteriori (MAP) detection rule which is optimal in the sense of minimizing the probability of incorrect decision (false alarm and miss detection). The proposed scheme does not require sending extra bits at the source, such as hash function or message authentication check bits, and hence there is no transmission overhead. The side information regarding the presence of forwarding misbehavior is exploited at the decoder to enhance the reliability of decoding. We derive the probability of false alarm and miss detection and the probability of bit error, taking into account the lossy nature of wireless links.

4.1 Introduction

In recent years, several network coding techniques have been studied in multiple access relay networks where multiple sources communicate with a common destination with the assistance from a set of relays. The basic idea of network coding in multiple access relay networks is to combine the information along the direct path from the source with the information received from the relays, where information from multiple sources are encoded (mixed), to enhance the reliability of decoding at the destination.

Information theoretic study on the multiple access relay channel (MARC) was first introduced in [56]. Outer bounds on the capacity of the MARC has been studied in [57], the diversity-multiplexing tradeoff has been developed in [58], [59], [60], and an outage minimizing relaying strategy has been studied in [61]. Authors in [62] investigated the cooperative diversity gain offered by network coding, assuming that the relays are able to decode all source messages reliably. Authors in [63] proposed a network coding scheme based on lowdensity parity-check (LDPC) codes that accounts for the lossy nature of wireless networks and showed that a significant coding/diversity gain can be achieved.

While network coding has proven to be promising in enhancing the communication efficiency, it also presents a new security challenge at the physical layer due to the dependency of cooperation. That is, reliance on implicit trust relationship between source and relay nodes makes it more vulnerable to false data injection at the relay and channel errors between source and relay. Since network coding allows the relays to mix data contents, a few corrupted data caused by either falsely injected data or channel errors can end up corrupting all the data reaching the destination. Without properly addressing this problem, network coding would not be effectively used in realworld applications.

The problem of detecting misbehaving relays that inject false data in single-source networks has been studied in [64]- [67]. In [64] the authors consider a peer-to-peer (P2P) network in which peers receive and forward a linear combination of the exogenous data packets. To check the integrity of the received packets, a signature vector is generated at the source node and broadcasted to all nodes where it is used to check the integrity of the received packets. In [65] and [66] several information theoretic algorithms for mitigating Bizantine modification attack are proposed. In [67] the authors consider inserting tracing bits in the data stream at the source in a cryptographically secure manner. The receiver then computes the ground truth of the tracing bits and compares them with the tracing bits received from a relay to determine whether it is malicious or cooperative. Extensions to multiple-source network have been studied in [68], [69], where the tracing bits or polynomial hash functions are used in detecting the misbehaving relays. All these works, however, require sending extra reference data (overhead) at the source to detect the misbehaving relay.

In this paper, we propose the maximum a posteriori (MAP) approach in detecting the misbehaving relay that injects false data or adds channel errors into the network encoder in multiple access relay networks. The MAP detection rule is based on the log-likelihood ratio

(LLR) test which is optimal in the sense of minimizing the probability of incorrect decision (false alarm and miss detection). The proposed scheme does not require sending extra bits at the source, such as hash function or message authentication check bits, and hence there is no transmission overhead. In addition, it makes an instantaneous decision about whether a relay is behaving properly without a long term observation.

The side information regarding the presence of misbehaving relay can be exploited at the destination (decoder) to enhance the reliability of decoding. We propose an effective decoding scheme that exploits the side information and significantly enhances the reliability of decoding. In practice, however, the side information may not be perfect. The false alarm results in an incorrect usage of the side information provided by the well-behaving relay, while the miss detection results in a usage of wrong information provided by the misbehaving relay, in decoding the source messages. We derive the probability of false alarm and miss detection and the probability of bit error as a function of the signal-to-noise ratio, taking into account the lossy nature of wireless links. We show that the proposed decoding with the aid of the MAP detection of misbehaving relay is within 1dB away from the genie-aided decoding.

4.2 System Model

Consider a multi-access relay network composed of two sources, one relay, and one destination as shown in Figure 4.1. Extension to multiple relays will be considered later. The relay overhears the bits sent by the sources (possibly with some errors), encodes them, and forwards the encoded bit to the destination. We assume that all bits are sent through orthogonal Rayleigh fading channels with additive white Gaussian noise and path loss, and each node is equipped with single antenna.

Let $x_i \in \{+1, -1\}$ denote the bit transmitted by the i-th source, $i = 1, 2$, and $x_i^r \in \{+1, -1\}$denote the overheard bit by the relay, where $+1$ is the additive identity element under $\oplus$ (modulo-2) addition. The relay combines the overheard bits and produces a coded (parity) bit

$$p = x_1^r \oplus x_2^r \oplus f \tag{4.1}$$

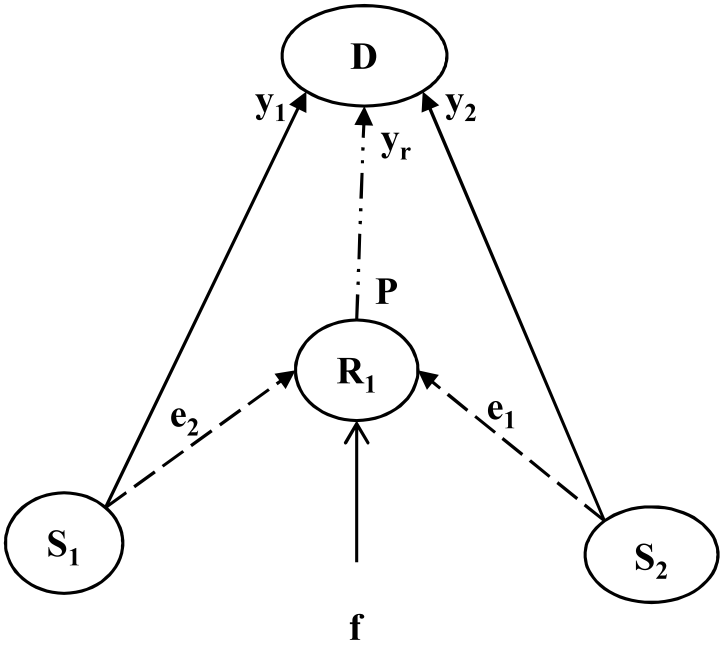


Figure 4.1 System Model

where $f \in \{+1, -1\}$ denotes the injected bit by the relay to corrupt the communication. If $f = -1$, false bit is injected, and if $f = +1$, no false bit is injected.

Let $e_i \in \{+1, -1\}$ be the error value between the i-th source and the relay, i.e. $x_i^r = x_i \oplus e_i$, where $e_i = -1$ means $x_i^r \neq x_i$, i.e. x_i is received in error at the relay, and $e_i = +1$ means $x_i^r = xi$. Then, 4.1 can be written as

$$\begin{aligned} p &= x_1 \oplus x_2 \oplus e_1 \oplus e_2 \oplus f \\ &= x_1 \oplus x_2 \oplus z \end{aligned} \tag{4.2}$$

where

$$z = e_1 \oplus e_2 \oplus f \tag{4.3}$$

captures the error events on the source-to-relay channels as well as the false data injection by

Table 4.1 Code book for Encoder (Relay)

	$z = +1$	$z = -1$
c_{t_0}	000	001
c_{t_1}	011	010
c_{t_2}	101	100
c_{t_3}	110	111

the relay.

Let $p_i := P(e_i = -1)$ be the probability of bit error between the i-th source and relay, $i = 1, 2$, and $p_f := P(f = -1)$ be the probability that a false bit ($f = -1$) is injected at the relay. Then, the event $z = -1$, i.e. wrong encoding (forwarding misbehavior), occurs when one or three of e_1, e_2, f are -1. Hence, we obtain

$$\begin{aligned} P(z = -1) =& p_f \left(1 - 2p_1 - 2p_2 + 3p_1p_2\right) \\ &+ \left(p_1 + p_2 - 2p_1p_2\right) \end{aligned} \tag{4.4}$$

and $P(z = +1) = 1 - P(z = -1)$. Table 4.1 shows the transmitter side code book when $z = +1$ and $z = -1$.

The received signals at the destination are given by

$$y_i = h_i x_i \sqrt{d_i^{-m} E_s} + n_i, i = 1, 2 \tag{4.5}$$

$$y_r = h_r p \sqrt{d_r^{-m} E_r} + n_r \tag{4.6}$$

where

- y_i and y_r are the received signals from the i-th source and the relay, respectively
- h_i and h_r are the channel fading gain between the i-th source and the destination and that between the relay and the destination, respectively
- d_i and d_r are the distance between the i-th source and the destination and that between the relay and the destination, respectively
- m is the path loss exponent
- E_s and E_r are the transmit energy per symbol at the source and the relay, respectively

- n_i and n_r are the noise at the destination.

It is assumed that h_i and h_r are independent complex Gaussian random variables with mean zero and variance one, and n_i and n_r are independent complex Gaussian random variables with mean zero and variance $N_0/2$ per dimension.

4.3 MAP Detection Scheme

The destination is interested in finding z whether z is $+1$ (well-behaving) or -1 (misbehaving). The maximum a posteriori (MAP) decision rule which minimizes the probability of incorrect decision is based on the LLR of z:

$$\begin{aligned} L\left(z|\mathbf{h},\mathbf{y}\right) &= \ln \frac{P\left(z=+1|\mathbf{h},\mathbf{y}\right)}{P\left(z=-1|\mathbf{h},\mathbf{y}\right)} \\ &= \ln \frac{P\left(p \oplus x_1 \oplus x_2 = +1|\mathbf{h},\mathbf{y}\right)}{P\left(p \oplus x_1 \oplus x_2 = -1|\mathbf{h},\mathbf{y}\right)} \\ &\approx \text{sign}\left(L(p|h_r,y_r)\right).\text{sign}\left(L(x_1|h_1,y_1)\right) \\ &\quad .\text{sign}\left(L(x_2|h_2,y_2)\right).\min\{|L(x_r|h_r,y_r)|, \\ &\quad |L(x_1|h_1,y_1)|,|L(x_2|h_2,y_2)|\} \end{aligned} \tag{4.7}$$

where $\mathbf{h} = [h_1\ h_2\ h_3]^T$, $\mathbf{y} = [y_1\ y_2\ y_r]^T$, and

$$\begin{aligned} L(x_i|h_i,y_i) &= \ln \frac{P(x_i=+1|h_i,y_i)}{P(x_i=-1|h_i,y_i)} \\ &= \frac{4\sqrt{d_i^{-m}E_s}}{N_0} Re\{h_i^* y_i\} \end{aligned} \tag{4.8}$$

is the LLR of x_i after knowing h_i and y_i. Similarly

$$\begin{aligned} L(p|h_r,y_r) &= \ln \frac{P(p=+1|h_r,y_r)}{P(p=-1|h_r,y_r)} \\ &= \frac{4\sqrt{d_r^{-m}E_r}}{N_0} Re\{h_r^* y_r\} \end{aligned} \tag{4.9}$$

is the LLR of p after knowing h_r and y_r. The approximation in (4.7) follows from [70]. Then the MAP decision rule is to decide

$$\hat{z} = \begin{cases} +1, & \text{if} \ \ L\left(z|\mathbf{h},\mathbf{y}\right) \geq 0 \\ -1, & \text{if} \ \ L\left(z|\mathbf{h},\mathbf{y}\right) < 0 \end{cases} \tag{4.10}$$

where $\hat{z}$ is the estimation of z. For simplicity of notation, $L(x_i|h_i, y_i)$ and $L(p|h_r, y_r)$ will be denoted by L_i and L_r, respectively, in what follows.

Extension to multiple relays:

If there are R relays, the above decision rule can be applied to each relay and decision can be made individually on each relay.

4.4 Probabilities of False Alarm and Miss Detection

In this section we drive the probability of false alarm P_{FA} and the probability of miss detection P_{MD}. The derivation follows from [54]. We first find P_{FA} for the case when there are two sources and then extend the result for K sources. In section 4.7, we generalize the derivation for the case when the destination is equipped with n_r antennas and T tracing bits are used. The probability of false alarm is defined as

$$P_{FA} = P(\hat{z} = -1|z = +1), \tag{4.11}$$

and the probability of miss detection is defined as

$$P_{MD} = P(\hat{z} = +1|z = -1), \tag{4.12}$$

The error probability in estimating z is given by

$$\begin{aligned} P_{E_z} &= P(\hat{z} = -1|z = +1)P(z = -1) + P(\hat{z} = +1|z = -1)P(z = -1) \\ &= P_{FA}P(z = -1) + P_{MD}P(z = -1) \end{aligned} \tag{4.13}$$

For binary symmetric channel (BSC), $P_{FA} = P_{MD}$. Therefore

$$P_{FA} = P_{E_z} \tag{4.14}$$

From (4.7) and (4.10), we have

$$\begin{aligned} \text{sign}(\hat{z}) =& \text{sign}\left(L(p|h_r, y_r)\right) .\text{sign}\left(L(x_1|h_1, y_1)\right) \\ & .\text{sign}\left(L(x_2|h_2, y_2)\right) \end{aligned} \tag{4.15}$$

which is equivalent to

$$\hat{z} = \tilde{x}_1 \oplus \tilde{x}_2 \oplus \tilde{p} \tag{4.16}$$

where $\tilde{x}_i$ is the estimated values of x_i given y_i only and $\tilde{p}$ is the estimated value of p given y_r only. The error probability of estimating z is given by

$$\begin{aligned} P_{E_z} = {} & P(\tilde{x}_1 \neq x_1, \tilde{x}_2 = x_2, \tilde{p} = p) \\ & + P(\tilde{x}_1 = x_1, \tilde{x}_2 \neq x_2, \tilde{p} = p) \\ & + P(\tilde{x}_1 = x_1, \tilde{x}_2 = x_2, \tilde{p} \neq p) \\ & + P(\tilde{x}_1 \neq x_1, \tilde{x}_2 \neq x_2, \tilde{p} \neq p) \end{aligned} \tag{4.17}$$

But

$$P(\tilde{x}_i \neq x_i) = \frac{1}{2}\left[1 - \sqrt{\frac{\gamma_s}{1+\gamma_s}}\right], \qquad i = 1, 2 \tag{4.18}$$

and

$$P(\tilde{p} \neq p) = \frac{1}{2}\left[1 - \sqrt{\frac{\gamma_r}{1+\gamma_r}}\right] \tag{4.19}$$

Assuming that all channels are independent, substitution from (4.18) and (4.19) into (4.17) yields

$$P_{FA} = \frac{1}{2}\left[1 - \sqrt{\frac{\gamma_r}{1+\gamma_r}\frac{\gamma_s}{1+\gamma_s}}\right] \tag{4.20}$$

Following the same procedure, we can calculate P_{FA} when $K = 3$ as follows

$$\begin{aligned} P_{FA} = {} & P(\tilde{x}_1 \neq x_1, \tilde{x}_2 = x_2, \tilde{x}_3 = x_3, \tilde{p} = p) \\ & + P(\tilde{x}_1 = x_1, \tilde{x}_2 \neq x_2, \tilde{x}_3 = x_3, \tilde{p} = p) \\ & + P(\tilde{x}_1 = x_1, \tilde{x}_2 = x_2, \tilde{x}_3 \neq x_3, \tilde{p} = p) \\ & + P(\tilde{x}_1 = x_1, \tilde{x}_2 = x_2, \tilde{x}_3 = x_3, \tilde{p} \neq p) \\ & + P(\tilde{x}_1 \neq x_1, \tilde{x}_2 \neq x_2, \tilde{x}_3 \neq x_3, \tilde{p} = p) \\ & + P(\tilde{x}_1 \neq x_1, \tilde{x}_2 \neq x_2, \tilde{x}_3 = x_3, \tilde{p} \neq p) \\ & + P(\tilde{x}_1 \neq x_1, \tilde{x}_2 = x_2, \tilde{x}_3 \neq x_3, \tilde{p} \neq p) \\ & + P(\tilde{x}_1 = x_1, \tilde{x}_2 \neq x_2, \tilde{x}_3 \neq x_3, \tilde{p} \neq p) \end{aligned} \tag{4.21}$$

Substitution from (4.18) and (4.19) into (4.21) yields

Table 4.2 Code book for MAP decoder without $\hat{z}$

c_{r_0}	000
c_{r_1}	011
c_{r_2}	101
c_{r_3}	110

$$P_{FA} = \frac{1}{2}\left[1 - \sqrt{\frac{\gamma_r}{1+\gamma_r}}\left(\frac{\gamma_s}{1+\gamma_s}\right)^{3/2}\right] \tag{4.22}$$

It follows from (4.20) and (4.22) and by induction that the probability of false alarm for K sources is given by [55]

$$P_{FA} = \frac{1}{2}\left[1 - \sqrt{\frac{\gamma_r}{1+\gamma_r}}\left(\frac{\gamma_s}{1+\gamma_s}\right)^{K/2}\right] \tag{4.23}$$

4.5 Decoding Schemes

In this section, we will consider four decoding schemes. The four schemes differ in terms of whether the receiver is aware of the misbehaving activity and how to utilize the knowledge of $\hat{z}$.

4.5.1 MAP Decoder Without $\hat{z}$

We consider the case where the estimation of relay misbehavior $\hat{z}$ is not available at the decoder. Therefore, the decoder assumes that the relay is well-behaving i.e. $z = +1$. Therefore, the decoder considers (x_1, x_2, p_t) as a valid codeword, where $p_t = x_1 \oplus x_2$ is the true parity bit, and finds the most probable (closest) codeword given a received vector. Table 4.2 shows the code book for the conventional decoder.

4.5.2 MAP Decoder With $\hat{z}$

We consider the case where the estimation of z is available at the decoder. In this case, the MAP decoder considers $(x1, x2, p_t \oplus \hat{z})$ as a valid codeword and finds the most probable (closest) codeword given a received vector. Therefore, if false alarm ($\hat{z} = -1$ given $z = +1$) occurs, then the decoder considers $(x1, x2, -p_t)$ as a valid codeword while $(x1, x2, p_t)$ is valid. Similarly, if

Table 4.3 Code book for MAP decoder with $\hat{z}$

	$\hat{z} = +1$	$\hat{z} = -1$
c_{r_0}	000	001
c_{r_1}	011	010
c_{r_2}	101	100
c_{r_3}	110	111

miss detection ($\hat{z} = +1$ given $z = -1$) occurs, then the decoder considers $(x1, x2, p_t)$ as a valid codeword while $(x1, x2, -p_t)$ is valid. In case a wrong parity bit is applied, the reliability of decoding will be decreased. The codebook for this decoder is shown in Table 4.3. The decoder selects the most probable codeword in the second column if $\hat{z} = +1$ and that in the third column if $\hat{z} = -1$.

4.5.3 MAP Decoder With $P(z)$

The MAP decoder selects the codeword c that maximizes $P(z|\mathbf{y})$, i.e.

$$\hat{c} = \arg\max_{c_i} P(c_i|\mathbf{y}) \tag{4.24}$$

Applying Bayes theorem to (4.24) yields

$$\begin{aligned}\hat{c} &= \arg\max_{c_i} \frac{P(\mathbf{y}|c_i)P(c_i)}{P(\mathbf{y})} \\ &= \arg\max_{c_i} P(\mathbf{y}|c_i)P(c_i) \end{aligned} \tag{4.25}$$

This requires the *a prior* probability $P(c_i)$ which depends on $P(z)$. For the codebook shown in Table 4.4, the probability $P(c_i)$ is given by

$$P(c_i) = \begin{cases} \frac{P(z=+1)}{4}, & \text{for } \; i = 0, 1, 2, 3 \\ \frac{P(z=-1)}{4}, & \text{for } \; i =, 4, 5, 6, 7 \end{cases} \tag{4.26}$$

If we let $\mathbf{x}_i$ be the modulated signal corresponding to the codeword c_i, i.e. $\mathbf{x}_i = [\sqrt{E_s}(-1)^{c_{i1}} \; \sqrt{E_s}(-1)^{c_{i2}} \; \sqrt{E_s}(-1)^{c_{i3}}]$, where c_{ij} is the j-th bit in the i-th codeword, then

$$P(\mathbf{y}|c_i) = \frac{1}{(\pi N_0)^{3/2}} e^{-||\mathbf{y} - H\mathbf{x}_i||^2/N_0} \tag{4.27}$$

Table 4.4 Codebook for MAP decoder

$z = +1$	c_0	000
	c_1	011
	c_2	101
	c_3	110
$z = -1$	c_4	001
	c_5	010
	c_6	100
	c_7	111

where

$$H = \begin{bmatrix} h_1\sqrt{d_1^{-m}} & 0 & 0 \\ 0 & h_2\sqrt{d_2^{-m}} & 0 \\ 0 & 0 & h_r\sqrt{d_r^{-m}} \end{bmatrix} \tag{4.28}$$

An estimate of $P(z = -1)$ may be obtained from $\hat{z}$. Define g_t as

$$g_t = \begin{cases} 1, & \text{if} \quad \hat{z}_t = -1 \\ 0, & \text{if} \quad \hat{z}_t = +1 \end{cases} \tag{4.29}$$

where t is the time index. Then it follows from the law of large numbers (LLN) that an estimate of $P(z = -1)$ at time t can be aproximated by

$$P(z_t = -1) \approx \frac{1}{L}\sum_{i=0}^{L-1} g_t \tag{4.30}$$

where L is the averaging window length.

4.5.4 Genie-aided Decoder

Genie-aided decoder assumes the availability of perfect side information regarding z, i.e. $\hat{z} = z$. Therefore, the decoder considers $(x1, x2, -p_t)$ as a valid codeword when codewords are generated as $(x1, x2, -p_t)$ and, similarly, $(x1, x2, p_t)$ as a valid codeword when codewords are generated as $(x1, x2, p_t)$. This corresponds to the case of fully cooperative relay, and serves as a reference for performance comparison with other decoders.

4.6 Probability of Decoding Error

In this section, we drive the union bound on the probability of decoding error for the decoding schemes discussed in Section 4.5. We also drive the bit error probability of the MAP decoder as a function of log likelihood ratio.

4.6.1 MAP Decoder Without $\hat{z}$

When $\hat{z}$ is not available, the decoder assumes $z = +1$. Then, all codewords are equiprobable, and, therefore, the MAP decoder is equivalent to the ML decoder or the minimum distance decoder. In this section, we drive the union bound on the word error probability. The word error probability is given by

$$P_E = p(e|z = +1)p(z = +1) + p(e|z = -1)p(z = -1) \tag{4.31}$$

Without loss of generality, assume c_{t_0} is transmitted. First, consider the case when $z = +1$. Then the union bound on the probability of decoding error is given by

$$p(e|z = +1) \leq p(c_{t_0} \to c_{r_1}|z = +1) + p(c_{t_0} \to c_{r_2}|z = +1) + p(c_{t_0} \to c_{r_3}|z = +1) \tag{4.32}$$

The received vector at the destination is given by

$$\mathbf{y} = H\mathbf{x}_0 + \mathbf{n} \tag{4.33}$$

where

$$H = \begin{bmatrix} h_1 & 0 & 0 \\ 0 & h_2 & 0 \\ 0 & 0 & h_r \end{bmatrix} \tag{4.34}$$

where the pass loss is considered in the channel gains and $\mathbf{x}_0$ is the transmitted vector corresponding to the codeword c_{t_0}. When $z = +1$ we have

$$\mathbf{x}_0 = \begin{bmatrix} x_{00} \\ x_{01} \\ x_{02} \end{bmatrix} = \begin{bmatrix} \sqrt{E_s} \\ \sqrt{E_s} \\ \sqrt{E_r} \end{bmatrix} \tag{4.35}$$

$$p(c_{t_0} \rightarrow c_{r_1}|z=+1,\mathbf{h}) = p(||\mathbf{y}-H\mathbf{r}_1||^2 < ||\mathbf{y}-H\mathbf{r}_0||^2) \tag{4.36}$$

where $\mathbf{r}_i$ is the modulated signal corresponding to c_{r_i}. For example

$$\mathbf{r}_1 = \begin{bmatrix} r_{10} \\ r_{11} \\ r_{12} \end{bmatrix} = \begin{bmatrix} \sqrt{E_s} \\ -\sqrt{E_s} \\ -\sqrt{E_r} \end{bmatrix} \tag{4.37}$$

When $z=+1$, $\mathbf{r}_i = \mathbf{x}_i$.

$$\begin{aligned} p(c_{t_0} \rightarrow c_{r_1}|z=\hat{z},\mathbf{h}) &= p(||H\mathbf{x}_0+\mathbf{n}-H\mathbf{r}_1||^2 < ||H\mathbf{x}_0+\mathbf{n}-H\mathbf{r}_0||^2) \\ &= p(||H\left(\mathbf{x}_0-\mathbf{r}_1\right)+\mathbf{n}||^2 < ||\mathbf{n}||^2) \\ &= p\left((<\mathbf{n},H(\mathbf{x}_0-\mathbf{r}_1)>)\,||H(\mathbf{x}_0-\mathbf{r}_1)||^2/2\right) \end{aligned} \tag{4.38}$$

where

$$<\mathbf{n},H(\mathbf{x}_0-\mathbf{r}_1)> = \sum_{i=0}^{2} h_i(x_{0i}-r_{1i})n_i \tag{4.39}$$

is a random variable with zero mean and variance $\frac{N_0}{2}||H(\mathbf{x}_0-\mathbf{r}_1)||^2 = \frac{N_0}{2}\sum_{i=0}^{2}|h_i(x_{00}-r_{10})|^2$

$$\begin{aligned} p(c_{t_0} \rightarrow c_{r_1}|z=+1,\mathbf{h}) &= Q\left(\frac{||H(\mathbf{x}_0-\mathbf{r}_1)||}{\sqrt{2N_0}}\right) \\ &= Q\left(\frac{2\sqrt{h_2^2E_s+h_r^2E_r}}{\sqrt{2N_0}}\right) \end{aligned} \tag{4.40}$$

$$p(c_{t_0} \rightarrow c_{r_1}|z=+1) \leq \frac{1}{(1+\gamma_s)\,(1+\gamma_r)} \tag{4.41}$$

similarly, we can write

$$p(c_{t_0} \rightarrow c_{r_2}|z=+1) \leq \frac{1}{(1+\gamma_s)\,(1+\gamma_r)} \tag{4.42}$$

and

$$p(c_{t_0} \rightarrow c_{r_3}|z=+1) \leq \frac{1}{(1+\gamma_s)^2} \tag{4.43}$$

If $\gamma_s = \gamma_r$, then

$$p(e|z=\hat{z}) \leq \frac{1}{(1+\gamma_s)^2} \tag{4.44}$$

Next, consider the case of $z=-1$ where $\mathbf{r}_i \neq \mathbf{x}_i$. The union bound on the probability of decoding error is given by

$$p(e|z=-1) \leq p(c_{t_0} \rightarrow c_{r_1}|z=-1) + p(c_{t_0} \rightarrow c_{r_2}|z=-1) + p(c_{t_0} \rightarrow c_{r_3}|z=-1) \tag{4.45}$$

where

$$\begin{aligned} p(c_{t_0} \rightarrow c_{r_1}|z=-1,\mathbf{h}) =& p(||H\mathbf{x}_0+\mathbf{n}-H\mathbf{r}_1||^2 < ||H\mathbf{x}_0+\mathbf{n}-H\mathbf{r}_0||^2) \\ =& p(||H\left(\mathbf{x}_0-\mathbf{r}_1\right)+\mathbf{n}||^2 < ||H\left(\mathbf{x}_0-\mathbf{r}_0\right)+\mathbf{n}||^2) \\ =& p\left(\left(<\mathbf{n}, H(\mathbf{x}_0-\mathbf{r}_1)> + \frac{||H(\mathbf{x}_0-\mathbf{r}_1)||^2}{2}\right)\right. \\ & \left. < \left(<\mathbf{n}, H(\mathbf{x}_0-\mathbf{r}_0)> + \frac{||H(\mathbf{x}_0-\mathbf{r}_0)||^2}{2}\right)\right) \\ =& p\left(h_2\sqrt{E_s}n_2 + h_2^2E_s < h_r\sqrt{E_r}n_r + h_r^2E_r\right) \\ =& p\left(h_2\sqrt{E_s}n_2 - h_r\sqrt{E_r}n_r < h_r^2E_r - h_2^2E_s\right) \end{aligned} \tag{4.46}$$

The left hand side of (4.46) is a Gaussian RV with zero mean and variance $\frac{N_0}{2}(h_2^2E_s+h_r^2E_r)$. Hence,

$$p(c_{t_0} \rightarrow c_{r_1}|z=-1,\mathbf{h}) = Q\left(\frac{h_2^2E_s - h_r^2E_r}{\sqrt{(h_2^2E_s+h_r^2E_r)N_0/2}}\right) \tag{4.47}$$

If $E_s=E_r$ and $h_2=h_r$, then

$$p(c_{t_0} \rightarrow c_{r_1}|z \neq \hat{z},\mathbf{h}) = \frac{1}{2} \tag{4.48}$$

By simulations, it can be shown that

$$p(c_{t_0} \rightarrow c_{r_1}|z \neq \hat{z}) \approx \frac{1}{2} \tag{4.49}$$

Similarly,

$$p(c_{t_0} \rightarrow c_{r_2}|z \neq \hat{z}) \approx \frac{1}{2} \tag{4.50}$$

$$\begin{aligned}
p(c_{t_0} \to c_{r_3} | z=-1, \mathbf{h}) =& p(||H\mathbf{x}_0 + \mathbf{n} - H\mathbf{r}_3||^2 < ||H\mathbf{x}_0 + \mathbf{n} - H\mathbf{r}_0||^2) \\
=& p\left(||H\left(\mathbf{x}_0 - \mathbf{r}_3\right) + \mathbf{n}||^2 < ||H\left(\mathbf{x}_0 - \mathbf{r}_0\right) + \mathbf{n}||^2\right) \\
=& p\left(\left(< \mathbf{n}, H(\mathbf{x}_0 - \mathbf{r}_3) > + \frac{||H(\mathbf{x}_0 - \mathbf{r}_3)||^2}{2}\right)\right. \\
& \left. < \left(< \mathbf{n}, H(\mathbf{x}_0 - \mathbf{r}_0) > + \frac{||H(\mathbf{x}_0 - \mathbf{r}_0)||^2}{2}\right)\right) \\
=& p\left(h_1\sqrt{E_s}n_1 + h_2\sqrt{E_s}n_2 > E_s\left(h_1^2 + h_2^2\right)\right) \\
=& Q\left(\frac{\sqrt{h_1^2 E_s + h_2^2 E_s}}{\sqrt{N_0/2}}\right) \qquad (4.51)
\end{aligned}$$

$$p(c_{t_0} \to c_{r_3} | z=-1) \leq \frac{1}{\left(1+\gamma_s\right)^2} \qquad (4.52)$$

$$p(e|z=-1) \leq 1 + \frac{1}{\left(1+\gamma_s\right)^2} \qquad (4.53)$$

It follows from (4.45), (4.49), (4.50), and (4.52) that

$$p(e|z=-1) \leq 1 \qquad (4.54)$$

and therefore

$$P_E \leq \frac{P(z=+1)}{\left(1+\gamma_s\right)^2} + P(z=-1) \qquad (4.55)$$

This shows that is an error floor due to the term $P(z=-1)$ in (4.55).

4.6.2 MAP Decoder With $\hat{z}$

When $\hat{z}$ is available at the decoder, the MAP decoder considers $(x1, x2, p_t \oplus \hat{z})$ as a valid codeword and finds the most probable (closest) codeword given a received vector. Therefore, the minimum distance decoder chooses the closest codeword among the four codewords listed in the second column of Table 4.3 when $\hat{z}=+1$ and chooses the closest codeword among the four codewords listed in the third column when $\hat{z}=-1$. In this section, we find the ML union bound of the word error probability. The word error probability is given by

$$P_E = p(e|z=\hat{z})p(z=\hat{z}) + p(e|z \neq \hat{z})p(z \neq \hat{z}) \tag{4.56}$$

where

$$\begin{aligned} p(z \neq \hat{z}) &= p(\hat{z}=-1|z=+1)p(z=+1) + p(\hat{z}=+1|z=-1)p(z=-1) \\ &= P_{FA}p(z=+1) + P_{MD}p(z=-1) \\ &= P_{FA}\left(p(z=+1)+p(z=-1)\right) = P_{FA} \end{aligned} \tag{4.57}$$

Substituting from (4.57) into (4.56) yields

$$P_E = p(e|z=\hat{z})(1-P_{FA}) + p(e|z \neq \hat{z})P_{FA} \tag{4.58}$$

Without loss of generality, consider the case when c_{t_0} is transmitted, we will drive the union bound on the error probability. First, consider the case when $z = \hat{z} = +1$

$$p(e|z=\hat{z}) \leq p(c_{t_0} \rightarrow c_{r_1}|z=\hat{z}) + p(c_{t_0} \rightarrow c_{r_2}|z=\hat{z}) + p(c_{t_0} \rightarrow c_{r_3}|z=\hat{z}) \tag{4.59}$$

The vector received at the destination is given by

$$\mathbf{y} = H\mathbf{x}_0 + \mathbf{n} \tag{4.60}$$

where

$$H = \begin{bmatrix} h_1\sqrt{d_1^{-m}} & 0 & 0 \\ 0 & h_2\sqrt{d_2^{-m}} & 0 \\ 0 & 0 & h_r\sqrt{d_r^{-m}} \end{bmatrix} \tag{4.61}$$

and $\mathbf{x}_0$ is the transmitted vector which corresponds to the codeword c_{t_0} i.e.

$$\mathbf{x}_0 = \begin{bmatrix} x_{00} \\ x_{01} \\ x_{02} \end{bmatrix} = \begin{bmatrix} \sqrt{E_s} \\ \sqrt{E_s} \\ \sqrt{E_s} \end{bmatrix} \tag{4.62}$$

$$p(c_{t_0} \rightarrow c_{r_1}|z=\hat{z},\mathbf{h}) = p(||\mathbf{y}-H\mathbf{r}_1||^2 < ||\mathbf{y}-H\mathbf{r}_0||^2) \tag{4.63}$$

where $\mathbf{r}_i$ is the modulated signal corresponding to c_{r_i}. When $\hat{z} = +1$

$$\mathbf{r}_1 = \begin{bmatrix} r_{10} \\ r_{11} \\ r_{12} \end{bmatrix} = \begin{bmatrix} \sqrt{E_s} \\ -\sqrt{E_s} \\ -\sqrt{E_r} \end{bmatrix} \tag{4.64}$$

When $z = \hat{z}$, $\mathbf{r}_i = \mathbf{x}_i$.

$$\begin{aligned} p(c_{t_0} \rightarrow c_{r_1} | z = \hat{z}, \mathbf{h}) &= p(||H\mathbf{x}_0 + \mathbf{n} - H\mathbf{r}_1||^2 < ||H\mathbf{x}_0 + \mathbf{n} - H\mathbf{r}_0||^2) \\ &= p(||H\left(\mathbf{x}_0 - \mathbf{r}_1\right) + \mathbf{n}||^2 < ||\mathbf{n}||^2) \\ &= p\left((< \mathbf{n}, H(\mathbf{x}_0 - \mathbf{r}_1) >) \, ||H(\mathbf{x}_0 - \mathbf{r}_1)||^2/2\right) \end{aligned} \tag{4.65}$$

where

$$< \mathbf{n}, H(\mathbf{x}_0 - \mathbf{r}_1) >= \sum_{i=0}^{2} h_i(x_{0i} - r_{1i})n_i \tag{4.66}$$

is a random variable with zero mean and variance $\frac{N_0}{2}||H(\mathbf{x}_0 - \mathbf{r}_1)||^2 = \frac{N_0}{2}\sum_{i=0}^{2}|h_i(x_{00} - r_{10})|^2$

$$\begin{aligned} p(c_{t_0} \rightarrow c_{r_1} | z = \hat{z}, \mathbf{h}) &= Q\left(\frac{||H(\mathbf{x}_0 - \mathbf{r}_1)||}{\sqrt{2N_0}}\right) \\ &= Q\left(\frac{2\sqrt{h_2^2 E_s + h_r^2 E_r}}{\sqrt{2N_0}}\right) \end{aligned} \tag{4.67}$$

$$p(c_{t_0} \rightarrow c_{r_1} | z = \hat{z}) \leq \frac{1}{(1+\gamma_s)\,(1+\gamma_r)} \tag{4.68}$$

similarly, we can write

$$p(c_{t_0} \rightarrow c_{r_2} | z = \hat{z}) \leq \frac{1}{(1+\gamma_s)\,(1+\gamma_r)} \tag{4.69}$$

and

$$p(c_{t_0} \rightarrow c_{r_3} | z = \hat{z}) \leq \frac{1}{(1+\gamma_s)^2} \tag{4.70}$$

If $\gamma_s = \gamma_r$, then

$$p(e|z = \hat{z}) \leq \frac{1}{(1+\gamma_s)^2} \tag{4.71}$$

Now, consider the case when $z \neq \hat{z}$

$$p(e|z \neq \hat{z}) \leq p(c_{t_0} \to c_{r_1}|z \neq \hat{z}) + p(c_{t_0} \to c_{r_2}|z \neq \hat{z}) + p(c_{t_0} \to c_{r_3}|z \neq \hat{z}) \tag{4.72}$$

$$p(c_{t_0} \to c_{r_1}|z \neq \hat{z}, \mathbf{h}) = p(||\mathbf{y} - H\mathbf{r}_1||^2 < ||\mathbf{y} - H\mathbf{r}_0||^2) \tag{4.73}$$

When $z \neq \hat{z}$, $\mathbf{r}_i \neq \mathbf{x}_i$.

$$\begin{aligned}
p(c_{t_0} \to c_{r_1}|z \neq \hat{z}, \mathbf{h}) =& p(||H\mathbf{x}_0 + \mathbf{n} - H\mathbf{r}_1||^2 < ||H\mathbf{x}_0 + \mathbf{n} - H\mathbf{r}_0||^2) \\
=& p(||H\left(\mathbf{x}_0 - \mathbf{r}_1\right) + \mathbf{n}||^2 < ||H\left(\mathbf{x}_0 - \mathbf{r}_0\right) + \mathbf{n}||^2) \\
=& p\left(\left(< \mathbf{n}, H(\mathbf{x}_0 - \mathbf{r}_1) > + \frac{||H(\mathbf{x}_0 - \mathbf{r}_1)||^2}{2}\right)\right. \\
&\left. < \left(< \mathbf{n}, H(\mathbf{x}_0 - \mathbf{r}_0) > + \frac{||H(\mathbf{x}_0 - \mathbf{r}_0)||^2}{2}\right)\right) \\
=& p\left(h_2\sqrt{E_s}n_2 + h_2^2E_s < h_r\sqrt{E_r}n_r + h_r^2E_r\right) \\
=& p\left(h_2\sqrt{E_s}n_2 - h_r\sqrt{E_r}n_r < h_r^2E_r - h_2^2E_s\right)
\end{aligned} \tag{4.74}$$

the left hand side is Gaussian RV with zero mean and variance $\frac{N_0}{2}(h_2^2E_s + h_r^2E_r)$. Then,

$$p(c_{t_0} \to c_{r_1}|z \neq \hat{z}, \mathbf{h}) = Q\left(\frac{h_2^2E_s - h_r^2E_r}{\sqrt{(h_2^2E_s + h_r^2E_r)N_0/2}}\right) \tag{4.75}$$

Using simulations

$$p(c_{t_0} \to c_{r_1}|z \neq \hat{z}) \approx \frac{1}{2} \tag{4.76}$$

Intuitively, if $E_s = E_r$ and $h_2 = h_r$, then

$$p(c_{t_0} \to c_{r_1}|z \neq \hat{z}, \mathbf{h}) = \frac{1}{2} \tag{4.77}$$

Similarly,

$$p(c_{t_0} \rightarrow c_{r_2} | z \neq \hat{z}) \approx \frac{1}{2} \tag{4.78}$$

$$\begin{aligned} p(c_{t_0} \rightarrow c_{r_3} | z \neq \hat{z}, \mathbf{h}) =& p(||H\mathbf{x}_0 + \mathbf{n} - H\mathbf{r}_3||^2 < ||H\mathbf{x}_0 + \mathbf{n} - H\mathbf{r}_0||^2) \\ =& p\left(||H\left(\mathbf{x}_0 - \mathbf{r}_3\right) + \mathbf{n}||^2 < ||H\left(\mathbf{x}_0 - \mathbf{r}_0\right) + \mathbf{n}||^2\right) \\ =& p\left(\left(< \mathbf{n}, H(\mathbf{x}_0 - \mathbf{r}_3) > + \frac{||H(\mathbf{x}_0 - \mathbf{r}_3)||^2}{2}\right)\right. \\ & \left. < \left(< \mathbf{n}, H(\mathbf{x}_0 - \mathbf{r}_0) > + \frac{||H(\mathbf{x}_0 - \mathbf{r}_0)||^2}{2}\right)\right) \\ =& p\left(h_1\sqrt{E_s}n_1 + h_2\sqrt{E_s}n_2 > E_s\left(h_1^2 + h_2^2\right)\right) \\ =& Q\left(\frac{\sqrt{h_1^2E_s + h_2^2E_s}}{\sqrt{N_0/2}}\right) \end{aligned} \tag{4.79}$$

$$p(c_{t_0} \rightarrow c_{r_3} | z \neq \hat{z}) \leq \frac{1}{(1+\gamma_s)^2} \tag{4.80}$$

$$p(e | z \neq \hat{z}) \leq 1 + \frac{1}{(1+\gamma_s)^2} \tag{4.81}$$

But error probability is less than 1, then

$$p(e | z \neq \hat{z}) \leq 1 \tag{4.82}$$

$$P_E \leq \frac{1 - P_{FA}}{(1+\gamma_s)^2} + P_{FA} \tag{4.83}$$

4.6.3 MAP Decoder With $P(z)$

In this subsection, we first drive the union bound on the bit error probability. Then, we find the bit error probability as a function of LLR

4.6.3.1 The Union Bound

The codebook of the MAP decoder is given in table 4.4. The union bound on the word error probability is given by

$$P_E \leq \sum_{i=0}^{7} \sum_{\substack{j=0 \\ j\neq i}}^{7} P(c_i \rightarrow c_j) \tag{4.84}$$

where the a priori probability of the codeword c_i is given by

$$P(c_i) = \begin{cases} \frac{P(z=+1)}{4}, & \text{for} \quad i = 0,1,2,3 \\ \frac{P(z=+1)}{4}, & \text{for} \quad i = 4,5,6,7 \end{cases} \tag{4.85}$$

For mathematical traceability, we assume that $E_s = E_r = E$. Let's define P_1, P_2, and P_3 as follows:

$P_1 = P(c_i \rightarrow c_j)$ if c_i differs from c_j in one bit. For example c_0, c_4.

$P_2 = P(c_i \rightarrow c_j)$ if c_i differs from c_j in two bit. For example c_0, c_1.

$P_3 = P(c_i \rightarrow c_j)$ if c_i differs from c_j in one bit. For example c_0, c_7.

The union bound in (4.84) can be written as

$$P_E \leq 3P_1 + 3P_2 + P_3 \tag{4.86}$$

Now, consider $\mathbf{x}_i$ is the transmitted vector which corresponds to the codeword c_i. For example

$$\mathbf{x}_5 = \begin{bmatrix} x_{50} \\ x_{51} \\ x_{52} \end{bmatrix} = \begin{bmatrix} +\sqrt{E_s} \\ -\sqrt{E_s} \\ +\sqrt{E_s} \end{bmatrix} \tag{4.87}$$

The MAP decoder finds an estimate of $\mathbf{x}$ as follows:

$$\hat{\mathbf{x}} = \arg\max_{\mathbf{x}} \frac{1}{(\pi N_0)^{3/2}} e^{-\frac{||\mathbf{y}-H\mathbf{x}||^2}{N_0}} P(\mathbf{x}) \tag{4.88}$$

where $\mathbf{x} \in \{\mathbf{x}_0, \mathbf{x}_1, \cdots, \mathbf{x}_7\}$ and $P(\mathbf{x}_i) = P(c_i)$, $i = 0, 1, \cdots, 7$. After some mathematical manipulations, we can write (4.88) as

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} \left(||\mathbf{y} - H\mathbf{x}||^2 - N_0 \log(P(\mathbf{x})) \right) \tag{4.89}$$

It's clear from (4.86) that the error probability is not a function of the transmitted codeword. Without loss of generality, let's assume that the codeword c_0 was transmitted. Then

$$P_1 = P(c_0 \rightarrow c_4) \tag{4.90}$$

$$= E_{\mathbf{h}}\left[P(c_0 \rightarrow c_4|\mathbf{h})\right] \tag{4.91}$$

The probability $P(c_0 \rightarrow c_4|\mathbf{h})$ is given by

$$\begin{aligned}
P(c_0 \rightarrow c_4|\mathbf{h}) &= P\left(||\mathbf{y} - H\mathbf{x}_4||^2 - N_0 \log(P(\mathbf{x}_4)) < ||\mathbf{y} - H\mathbf{x}_0||^2 - N_0 \log(P(\mathbf{x}_0))\right) \\
&= P\left(||H(\mathbf{x}_0 - \mathbf{x}_4) + \mathbf{n}||^2 - N_0 \log \frac{P(z=+1)}{P(z=-1)} < ||\mathbf{n}||^2\right) \\
&= P\left(||H(\mathbf{x}_0 - \mathbf{x}_4) + \mathbf{n}||^2 - N_0 L(z) < ||\mathbf{n}||^2\right) \\
&= P\left((< n, H(\mathbf{x}_0 - \mathbf{x}_4) >) > \frac{||H(\mathbf{x}_0 - \mathbf{x}_4)||^2}{2} + \frac{N_0}{2} L(z)\right) \\
&= Q\left(\frac{2h_3^2 E + (N_0/2)L(z)}{\sqrt{2N_0 h_3^2 E}}\right) \\
&= Q\left(\sqrt{2h_3^2\gamma} + \frac{\frac{1}{2}L(z)}{\sqrt{2h_3^2\gamma}}\right)
\end{aligned} \tag{4.92}$$

where $\gamma = E/N_0$ and $L(z) = \log(P(z=+1)/P(z=-1))$. In order to find P_1, we average (4.92) over the distribution of h_3^2.

$$P_1 = E_{h_3^2}\left[Q\left(\sqrt{2h_3^2\gamma} + \frac{\frac{1}{2}L(z)}{\sqrt{2h_3^2\gamma}}\right)\right] \tag{4.93}$$

Since h_3 follows the Rayleigh distribution, the distribution of h_3^2 would be exponential. After averaging (4.92) over the exponential distribution we have

$$P_1 = \frac{1}{2}\left[1 - \sqrt{\frac{\gamma}{1+\gamma}}\right] e^{\frac{-L(z)}{2}(1+\sqrt{1+\frac{1}{\gamma}})} \tag{4.94}$$

The proof of (4.94) is provided in Appendix B. Similarly, we can find P_2 as follows

$$P_2 = P(c_0 \rightarrow c_1) \tag{4.95}$$

$$= E_{\mathbf{h}}\left[P(c_0 \rightarrow c_1|\mathbf{h})\right] \tag{4.96}$$

The probability $P(c_0 \to c_1|\mathbf{h})$ is given by

$$\begin{aligned}
P(c_0 \to c_1|\mathbf{h}) &= P\left(||\mathbf{y} - H\mathbf{x}_1||^2 - N_0 \log(P(\mathbf{x}_1)) < ||\mathbf{y} - H\mathbf{x}_0||^2 - N_0 \log(P(\mathbf{x}_0))\right) \\
&= P\left(||H(\mathbf{x}_0 - \mathbf{x}_1) + \mathbf{n}||^2 - N_0 \log \frac{P(z=+1)}{P(z=+1)} < ||\mathbf{n}||^2\right) \\
&= P\left((< n, H(\mathbf{x}_0 - \mathbf{x}_1) >) > \frac{||H(\mathbf{x}_0 - \mathbf{x}_1)||^2}{2}\right) \\
&= Q\left(\frac{2\sqrt{h_2^2 E + h_3^2 E}}{\sqrt{2N_0}}\right) \qquad (4.97)
\end{aligned}$$

Averaging (4.97) over the joint distribution of h_2^2 and h_3^3 yields

$$P_2 = \frac{1}{2}\left[1 - \sqrt{\frac{\gamma}{1+\gamma}}\right]^2 \left(1 + \frac{1}{2}\sqrt{\frac{\gamma}{1+\gamma}}\right) \qquad (4.98)$$

Since the distance between c_0 and c_7 is three, we can neglect the contribution of P_3 in the union bound calculations.

At high SNR, (4.94) is bounded by

$$P_1 \leq \frac{e^{-L(z)}}{4\gamma} \qquad (4.99)$$

and (4.98) is bounded by

$$P_2 \leq \frac{1}{16\gamma^2} \qquad (4.100)$$

Therefore the union bound on the word error probability is given by

$$\begin{aligned}
P_E \leq& \frac{e^{-L(z)}}{4\gamma} + \frac{1}{16\gamma^2} \\
=& \frac{1}{16\gamma^2}\left(1 + 4\gamma e^{-L(z)}\right) \qquad (4.101)
\end{aligned}$$

Hence,

$$P_E \leq \begin{cases} \frac{1}{16\gamma^2}, & \text{if } \ L(z) >> \log(4\gamma) \\ \frac{e^{-L(z)}}{4\gamma}, & \text{if } \ L(z) << \log(4\gamma) \end{cases} \qquad (4.102)$$

This shows that the diversity order is two when the attack probability $P(z=-1)$ is small, i.e. $L(z)$ is large.

4.6.3.2 Bit error probability as a function of LLR

When the destination uses the MAP decoder to estimate the transmitted bits, the probability of bit error of the first source is given by

$$P\left(\hat{x}_1 \neq x_1 \middle| \, \mathbf{y}\right) = \frac{1}{1+e^{|\Lambda|}} \tag{4.103}$$

where

$$\begin{aligned}
\Lambda &= L\left(x_1|y_1, y_2, y_r\right) \\
&= \log \frac{P\left(x_1 = 1|y_1, y_2, y_r\right)}{P\left(x_1 = -1|y_1, y_2, y_r\right)} \\
&= \log \frac{P\left(y_1, y_2, y_r|x_1 = 1\right)}{P\left(y_1, y_2, y_r|x_1 = -1\right)} \\
&= \log \frac{P\left(y_1|x_1 = 1\right) P\left(y_2, y_r|x_1 = 1\right)}{P\left(y_1|x_1 = -1\right) P\left(y_2, y_r|x_1 = -1\right)} \\
&= L\left(x_1|y_1\right) + L\left(x_1|y_2, y_r\right) \qquad (4.104)
\end{aligned}$$

Now, we need to calculate the log likelihood ratio of x_1 given y_2 and y_r. Since y_2 is the received signal when x_2 is transmitted from the second source and y_r is the received signal when p is transmitted from the relay, we can calculate $L\left(x_2 \oplus p| \, y_2, y_r\right)$ as follows

$$L\left(x_2 \oplus p|y_2, y_r\right) \approx sign\left(L_2\right) \cdot sign\left(L_r\right) \cdot min\left\{|L_2|, |L_r|\right\} \tag{4.105}$$

Let $f = x_2 \oplus p$. Since $p = x_1 \oplus x_2 \oplus z$, then $f = x_1 \oplus z$. We can write

$$\begin{aligned}
L\left(f|y_2, y_r\right) &= L\left(x_1 \oplus z|y_2, y_r\right) \\
&\approx sign\left(L_2\right) \cdot sign\left(L_r\right) \cdot min\left\{|L_2|, |L_r|\right\} \qquad (4.106)
\end{aligned}$$

The log likelihood ratio of x_1 given y_2 and y_r is given by

$$\begin{aligned}
L\left(x_1|y_2, y_r\right) &= \log \frac{P\left(x_1 = +1|y_2, y_r\right)}{P\left(x_1 = -1|y_2, y_r\right)} \\
&= \log \frac{P\left(f \oplus z = +1|y_2, y_r\right)}{P\left(f \oplus z = -1|y_2, y_r\right)} \\
&= \log \frac{P\left(f \oplus z = +1|y_2, y_r, z = +1\right) P_{z=+1} + P\left(f \oplus z = +1|y_2, y_r, z = -1\right) P_{z=-1}}{P\left(f \oplus z = -1|y_2, y_r, z = +1\right) P_{z=+1} + P\left(f \oplus z = -1|y_2, y_r, z = -1\right) P_{z=-1}} \\
&= \log \frac{P\left(f = +1|y_2, y_r, z = +1\right) P_{z=+1} + P\left(f = -1|y_2, y_r, z = -1\right) P_{z=-1}}{P\left(f = -1|y_2, y_r, z = +1\right) P_{z=+1} + P\left(f = +1|y_2, y_r, z = -1\right) P_{z=-1}} \\
&= \log \frac{P\left(f = +1|y_2, y_r\right) P(z = +1) + P\left(f = -1|y_2, y_r\right) P(z = -1)}{P\left(f = -1|y_2, y_r\right) P(z = +1) + P\left(f = +1|y_2, y_r\right) P(z = -1)} \\
&= \log \frac{P\left(f = +1|y_2, y_r\right) / P\left(f = -1|y_2, y_r\right) P(z = +1) + P(z = -1)}{P(z = +1) + P\left(f = +1|y_2, y_r\right) / P\left(f = -1|y_2, y_r\right) P(z = -1)} \\
&= \log \frac{e^{L(f|y_2,y_r)} P(z = +1) + P(z = -1)}{P(z = +1) + e^{L(f|y_2,y_r)} P(z = -1)} \qquad (4.107)
\end{aligned}$$

$$\begin{aligned}
\Lambda &= L\left(x_1|y_1\right) + L\left(x_1|y_2, y_r\right) \\
&= L\left(x_1|y_1\right) + log \frac{e^{L(x_2 \oplus p|y_2,y_r)} P(z = +1) + P(z = -1)}{P(z = +1) + e^{L(x_2 \oplus p|y_2,y_r)} P(z = -1)} \qquad (4.108)
\end{aligned}$$

$$P\left(\hat{x}_1 \neq x_1 |\, \mathbf{y}\right) = \frac{1}{1 + e^{|\Lambda|}} \qquad (4.109)$$

Special Cases:

Case I: $P(z = +1) = 1, P(z = -1) = 0$

$$\begin{aligned}
L\left(x_1|y_2, y_r\right) &= \log \frac{e^{L(f|y_2,y_r)} \times 1 + 0}{1 + e^{L(f|y_2,y_r)} \times 0} \\
&= \log e^{L(f|y_2,y_r)} \\
&= L\left(f|y_2, y_r\right) \\
&= L\left(x_2 \oplus p|y_2, y_r\right) \qquad (4.110)
\end{aligned}$$

This is the case when the relay node is fully cooperative which provides the minimum error rate.

Case II: $P(z = +1) = 0, P(z = -1) = 1$

$$
\begin{aligned}
L\left(x_1|y_2,y_r\right) &= \log \frac{e^{L(f|y_2,y_r)} \times 0 + 1}{0 + e^{L(f|y_2,y_r)} \times 1} \\
&= \log e^{-L(f|y_2,y_r)} \\
&= -L\left(f|y_2,y_r\right) \\
&= -L\left(x_2 \oplus p|y_2,y_r\right) \qquad (4.111)
\end{aligned}
$$

This is the case when the relay node inverts every parity bit it generates. The destination should invert back every bit received from the relay node. The error rate performance in this case is the same as that of case I.

Case III: $P(z=+1)=0.5, P(z=-1)=0.5$

$$
\begin{aligned}
L\left(x_1|y_2,y_r\right) &= \log \frac{e^{L(f|y_2,y_r)} \times 0.5 + 0.5}{0.5 + e^{L(f|y_2,y_r)} \times 0.5} \\
&= 0 \qquad (4.112)
\end{aligned}
$$

In this case the relay node injects +1 and −1 with equal probability. This type of malicious attack eliminates the correlation between the data transmitted from the relay node and what is received from the source. Therefore, the received signal at the destination from the relay node will provide no information about x_1 or x_2.

4.6.4 Genie-aided Decoder

Genie-aided decoder assumes the availability of perfect side information regarding z, i.e. $\hat{z}=z$. Therefore, $P(\hat{z} \neq z)=0$ and $P(\hat{z}=z)=1$. The ML union bound on the word error probability can be found by setting $P(\hat{z} \neq z)=0$ and $P(\hat{z}=z)=1$ in (4.83) as follows

$$
P_E \leq \frac{1}{\left(1+\gamma_s\right)^2} \qquad (4.113)
$$

We can also find the bit error probability as a function of the log likelihood ratio as follows

$$
P\left(\hat{x}_1 \neq x_1\right) = \frac{1}{1+e^{|\Lambda|}} \qquad (4.114)
$$

where

$$
\Lambda = L\left(x_1|y_1\right) + L\left(x_1|y_2,y_r\right) \qquad (4.115)
$$

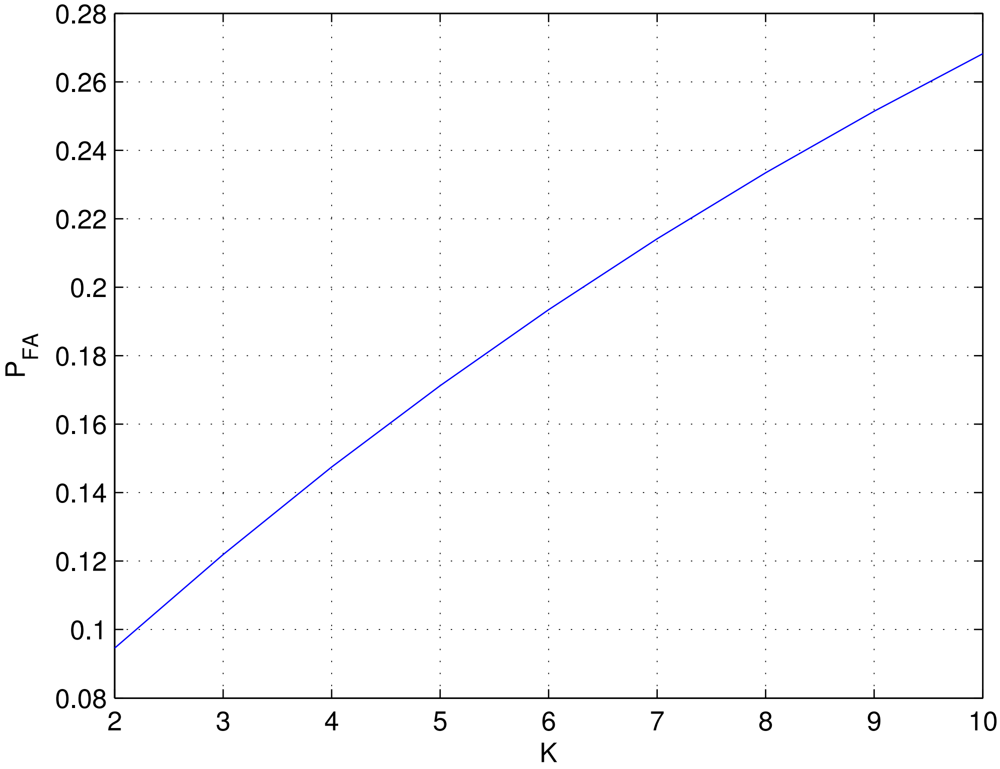


Figure 4.2 Probability of false alarm against number of sources for $\gamma_s = \gamma_r$ = 10dB

and

$$L\left(x_1|y_2,y_r\right)=\begin{cases} L\left(x_2\oplus p|y_2,y_r\right), & \text{if} \quad z=+1 \\ -L\left(x_2\oplus p|y_2,y_r\right), & \text{if} \quad z=-1 \end{cases} \tag{4.116}$$

Then

$$P\left(\hat{x}_1\neq x_1\right)=\frac{1}{1+e^{|L(x_1|y_1)+z.L(x_2\oplus p|y_2,y_r)|}} \tag{4.117}$$

4.7 Enhancing MAP Detection

In this section we propose three methods to enhance the MAP detection.

4.7.1 Tracing Bit Aided MAP detection

Figure 4.2 shows the probability of false alarm P_{FA} against the number of sources K. We see that P_{FA} increases as the number of sources increases. The MAP detection can be made more accurate by inserting a number of tracing bits in the data stream at the source in a cryptographically secure manner. Tracing bits are reference bits which are know at the destination. If T out of K source nodes send tracing bits it's easy to show that the probability of false alarm as a function of K and T is given by [55]

$$P_{FA} = \frac{1}{2}\left[1 - \sqrt{\frac{\gamma_r}{1+\gamma_r}}\left(\frac{\gamma_s}{1+\gamma_s}\right)^{(K-T)/2}\right] \tag{4.118}$$

(4.118) shows how the transmission of tracing bits by T source nodes improves the performance of the MAP detection scheme. As a special case, consider the scenario when all K bits are know at the destination, i.e. $T = K$. Without loss of generality, let's assume $x_1 \oplus x_2 \oplus \cdots \oplus x_K = 1$. Then the parity bit sent by the relay is $p = x_1 \oplus x_2 \oplus \cdots \oplus x_K \oplus z = z$. In this case the false alarm ($\hat{z} = -1$ given $z = 1$) will occur if the relay-to-destination channel is in error, i.e. the probability of false alarm is given by

$$P_{FA} = \frac{1}{2}\left[1 - \sqrt{\frac{\gamma_r}{1+\gamma_r}}\right] \tag{4.119}$$

Now, consider the case when each source transmits t tracing bits for every k information bits. Hence, the probability that a specific bit from a source being a tracing bit is t/n where $n = k + t$. In order to calculate the average probability of false alarm, we first consider the case of two sources and then we generalize the solution for K sources.

Two sources

If b_1 is the bits of the first source and b_2 is the bit of second source then there are four possible events each occurs with a specific probability as follows:

1. (Both b_1 and b_2 are tracing bits) with probability t^2/n^2

2. (b_1 is a tracing bit and b_2 is not) with probability $t(n-t)/n^2$

3. (b_2 is a tracing bit and b_1 is not) with probability $t(n-t)/n^2$

4. (Neither b_1 nor b_2 is a tracing bit) with probability $(n-t)^2/n^2$

Accordingly, the average probability of false alarm is given by

$$\begin{aligned} P_{FA} = \frac{1}{2}\Bigg[&\left(1-\sqrt{\frac{\gamma_r}{1+\gamma_r}\frac{\gamma_s}{1+\gamma_s}}\right)\frac{(n-t)^2}{n^2} \\ &+2\left(1-\sqrt{\frac{\gamma_r}{1+\gamma_r}\frac{\gamma_s}{1+\gamma_s}}\right)\frac{(n-t)t}{n^2} \\ &+\left(1-\sqrt{\frac{\gamma_r}{1+\gamma_r}}\right)\frac{t^2}{n^2}\Bigg] \end{aligned} \tag{4.120}$$

K sources

When there are K sources, it can be shown that the average probability of false alarm is

$$P_{FA} = \frac{1}{2}\sum_{T=0}^{K}\left(1-\sqrt{\frac{\gamma_r}{1+\gamma_r}}\left(\frac{\gamma_s}{1+\gamma_s}\right)^{(K-T)/2}\right)\binom{K}{T}\frac{(n-t)^{K-T}t^T}{n^K} \tag{4.121}$$

For further simplification of (4.121), let's assume $\alpha_s = \sqrt{\gamma_s/(1+\gamma_s)}$, $\alpha_r = \sqrt{\gamma_r/(1+\gamma_r)}$, and $p_{tn} = t/n$. Hence

$$\begin{aligned} P_{FA} =& \frac{1}{2}\sum_{T=0}^{K}\left(1-\alpha_r\alpha_s^{K-T}\right)\binom{K}{T}(1-p_{tn})^{K-T}p_{tn}^T \\ =& \frac{1}{2}\sum_{T=0}^{K}\binom{K}{T}(1-p_{tn})^{K-T}p_{tn}^T - \frac{1}{2}\alpha_r\sum_{T=0}^{K}\binom{K}{T}\alpha_s^{K-T}(1-p_{tn})^{K-T}p_{tn}^T \\ =& \frac{1}{2} - \frac{1}{2}p_{tn}^K\alpha_r\sum_{T=0}^{K}\binom{K}{T}\alpha_s^{K-T}\left(\frac{1}{p_{tn}}-1\right)^{K-T} \\ =& \frac{1}{2} - \frac{1}{2}p_{tn}^K\alpha_r\sum_{T=0}^{K}\binom{K}{T}\left(\frac{\alpha_s}{p_{tn}}-\alpha_s\right)^{K-T} \\ =& \frac{1}{2} - \frac{1}{2}p_{tn}^K\alpha_r\sum_{T=0}^{K}\binom{K}{T}\left(\frac{\alpha_s}{p_{tn}}-\alpha_s+1-1\right)^{K-T} \\ =& \frac{1}{2} - \frac{1}{2}p_{tn}^K\alpha_r\left(\frac{\alpha_s}{p_{tn}}-\alpha_s+1\right)^{K} \end{aligned} \tag{4.122}$$

Substituting back for the values of α_s, α_r, and p_{tn} yields

$$P_{FA} = \frac{1}{2}\left[1-\left(\frac{t}{n}+\left(1-\frac{t}{n}\right)\sqrt{\frac{\gamma_s}{1+\gamma_s}}\right)^K\sqrt{\frac{\gamma_r}{1+\gamma_r}}\right] \tag{4.123}$$

4.7.2 Channel Coding Aided MAP detection

Another method to increase the accuracy of the MAP detection scheme is to use channel coding. That is because the channel coding corrects some errors in the data received from the sources and accordingly the bit error probability of the i-th source bits ($P(\tilde{x}_i \neq x_i)$) decreases. Since the misbehaving relay node injects the falsified data randomly, the data comes through the relay-destination channel may not be consistent with the used channel code. Therefore, the decoding of the relay bits may be harmful.

Each source encodes it's data using a specific (n, k) code where k is the number of information bits, n is the code length, and $(n - k)$ is the number of parity bits. The detection of the misbehaving activity of the relay node is performed at the destination as follows. First, the destination decodes the data coming from the source nodes in order to correct channel errors. Then, the MAP detector is used to find $\hat{z}$.

If the code (n, k) can correct up to e errors, the probability on decoding error of a the i-th source bit is given by

$$P_{c_i} = \sum_{j=e+1}^{n} \frac{j}{n} \binom{n}{j} P_{b_i}^{j} (1 - P_{b_i})^{n-j} \tag{4.124}$$

where the probability of the i-th source bit error P_{b_i} is given in (4.18). Assuming perfect power control such that all source-to-destination channels have the same average SNR then $P_{b_1} = P_{b_2} = \cdots = P_{b_n} = P_b$ and $P_{c_1} = P_{c_2} = \cdots = P_{c_n} = P_c$. If the number of sources is K then the probability of false alarm is given by

$$P_{FA} = (1 - P_{b_r}) \sum_{\substack{i=1 \\ \text{Step } 2}}^{K} \binom{K}{i} P_c^i (1 - P_c)^{K-i} + P_{b_r} \sum_{\substack{i=0 \\ \text{Step } 2}}^{K} \binom{K}{i} P_c^i (1 - P_c)^{K-i} \tag{4.125}$$

4.7.3 Multiple Antennas Aided MAP detection

If the destination is equipped with n_r antennas and uses MRC to combine the received signals the probability of bit error of the i-th source is given

$$P_{b_i} = \left(\frac{1 - \Gamma_i}{2}\right)^{n_r} \sum_{j=0}^{n_r - 1} \binom{n_r - 1 + j}{j} \left(\frac{1 + \Gamma_i}{2}\right) \tag{4.126}$$

where

$$\Gamma_i = \sqrt{\frac{\gamma_i}{1+\gamma_i}} \tag{4.127}$$

and the probability of bit error of the relay node is given

$$P_{b_r} = \left(\frac{1-\Gamma_r}{2}\right)^{n_r} \sum_{j=0}^{n_r-1} \binom{n_r-1+j}{j} \left(\frac{1+\Gamma_r}{2}\right) \tag{4.128}$$

where

$$\Gamma_r = \sqrt{\frac{\gamma_r}{1+\gamma_r}} \tag{4.129}$$

Assuming that all source bits have the same receive SNR, i.e., $\gamma_i = \gamma_s$, the probability of false alarm is given by

$$P_{FA} = (1-P_{b_r}) \sum_{\substack{i=1\\ \text{Step } 2}}^{K-T} \binom{K-T}{i} P_{b_i}^i (1-P_{b_i})^{K-T-i} + P_{b_r} \sum_{\substack{i=0\\ \text{Step } 2}}^{K-T} \binom{K-T}{i} P_{b_i}^i (1-P_{b_i})^{K-T-i} \tag{4.130}$$

4.8 Detection of Misbehaving behavior in Multiple Access Relay Networks with M-ary Modulation

In this section, we present a MAP detection scheme which can handle the case of M-ary modulation to detect misbehaving activity of the relay node. Consider a multi-access relay network composed of two sources, one relay, and one destination as shown in Figure 4.3. The relay overhears the symbols sent by the sources (possibly with some errors), encodes them, and forwards the encoded symbol to the destination. We assume that all symbols are sent through orthogonal Rayleigh fading channels with additive white Gaussian noise and path loss, and each node is equipped with single antenna.

Let $x_i \in \{0, 1, 2, \cdots, M-1\}$ denote the data symbol of the i-th source, $i = 1, 2$, and x_i^r denote the overheard data symbol by the relay where $M = 2^b$ and b is the number of bits per symbol. The symbol x_i is modulated using M-ary modulation. The relay combines the overheard symbols and produces a coded (parity) symbol. The linear combination at the relay node is done over $GF(2^b)$. The parity symbol generated at the relay node is given by

$$p = x_1^r + x_2^r + f \tag{4.131}$$

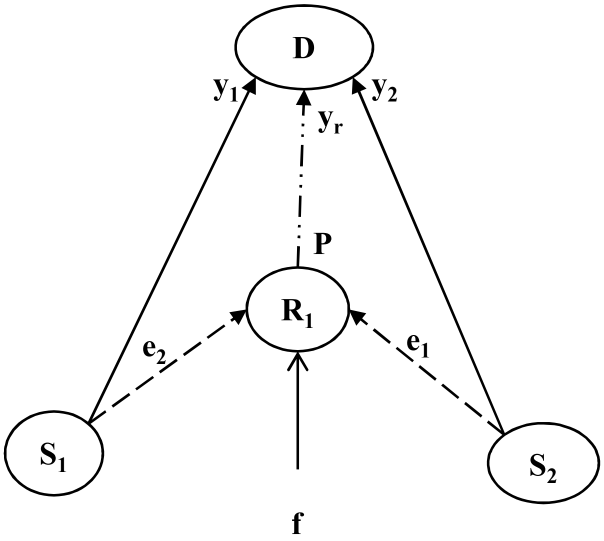


Figure 4.3 System Model for the M-ary Modulation case

where $f \in \{0, 1, 2, \cdots, M-1\}$ denotes the injected symbol by the relay to corrupt the communication and operation "+" is modulo-M addition. If $f \neq 0$, false symbol is injected, and if $f = 0$, no false symbol is injected.

Let $e_i \in \{0, 1, 2, \cdots, M-1\}$ be the error value between the i-th source and the relay, i.e. $x_i^r = x_i + e_i$, where $e_i \neq 0$ means $x_i^r \neq x_i$, i.e. x_i is received in error at the relay, and $e_i = 0$ means $x_i^r = xi$. Then, (4.131) can be written as

$$\begin{aligned} p &= x_1 + x_2 + e_1 + e_2 + f \\ &= x_1 + x_2 + z \end{aligned} \tag{4.132}$$

where

$$z = e_1 + e_2 + f \tag{4.133}$$

captures the error events on the source-to-relay channels as well as the false data injection by the relay. Note that, "+" in 4.131, 4.132, and 4.133 is the addition operation in $GF(M)$.

The destination is interested in finding z whether z is equal to 0 (well-behaving) or belongs to $\{1, 2, \cdots, M-1\}$ (misbehaving). The maximum a posteriori (MAP) decision rule which

Table 4.5 Bit representation of 4-ary symbol

symbol	b_2	b_1
$s_0 = 0$	0	0
$s_1 = 1$	0	1
$s_2 = 2$	1	0
$s_3 = 3$	1	1

minimizes the probability of incorrect decision is based on the LLR of z. Because of the complexity in calculating direct value of the LLR of z, we propose a simple procedure to estimate z by calculating the LLR's of its individual bits. Let L_{ij} denote the the LLR of the j-th bit of the symbol received from the i-th source given y_i and h_i, i.e.,

$$\begin{aligned} L_{ij} =& L(b_j|y_i, h_i) \\ =& \log \frac{P(b_j = 0|y_i, h_i)}{P(b_j = 1)|y_i, h_i)} \end{aligned} \tag{4.134}$$

where $i = 1, 2, r$ and $j = 1, 2, \cdots, b$.

As an example, consider the case when $M = 4$ which means that each symbol consists of two bits, i.e., $b = 2$. Table 4.5 represnts the symbol structure of the 4-ary case. The LLR of the second bit of the of the symbol received from the the first source is given by

$$\begin{aligned} L_{21} =& L(b_1|y_2, h_2) \\ =& \log \frac{P(b_1 = 0|y_2, h_2)}{P(b_1 = 1|y_2, h_2)} \\ =& \log \frac{P(s_0|y_2, h_2) + P(s_2|y_2, h_2)}{P(s_1|y_2, h_2) + P(s_3|y_2, h_2)} \end{aligned} \tag{4.135}$$

Generally, we can write

$$\begin{aligned} L_{ij} =& \log \frac{\sum_{\substack{m=0\\ b_j=0}}^{M-1} P(s_m|y_i, h_i)}{\sum_{\substack{m=0\\ b_j=1}}^{M-1} P(s_m|y_i, h_i)} \\ =& \log \frac{\sum_{\substack{m=0\\ b_j=0}}^{M-1} P(y_i|s_m, h_i)P(s_m)/P(y_i|h_i)}{\sum_{\substack{m=0\\ b_j=1}}^{M-1} P(y_i|s_m, h_i)P(s_m)/P(y_i|h_i)} \\ =& \log \frac{\sum_{\substack{m=0\\ b_j=0}}^{M-1} P(y_i|s_m, h_i)}{\sum_{\substack{m=0\\ b_j=1}}^{M-1} P(y_i|s_m, h_i)} \end{aligned} \tag{4.136}$$

where $P(s_m) = 1/M$ for all $m = \{0, 1, \cdots, M-1\}$ and $P(y_i|h_i)$ is common in the numerator and the denominator. The probability of Y_i given s_m and h_i is given by

$$P(y_i|s_m, h_i) = \frac{1}{\sqrt{\pi N_0}} e^{-\frac{|y_i - h_i x_m|^2}{N_0}} \tag{4.137}$$

where x_m is the M-ary modulated signal which corresponds to s_m. Substituting from (4.137) into (4.136) yields

$$L_{ij} = \log \frac{\sum_{\substack{m=0 \\ b_j=0}}^{M-1} e^{-\frac{|y_i - h_i x_m|^2}{N_0}}}{\sum_{\substack{m=0 \\ b_j=1}}^{M-1} e^{-\frac{|y_i - h_i x_m|^2}{N_0}}} \tag{4.138}$$

The terms of the summation in both numerator and denominator of (4.138) may tend to zero because of a large negative exponent. Therefore L_{ij} would be an unknown quantity. L_{ij} in (4.138) can be approximated by

$$\begin{aligned} L_{ij} \approx & \log \frac{\max \left\{ e^{-\frac{|y_i - h_i x_m|^2}{N_0}} \right\}_{\substack{m=0 \\ b_j=0}}^{M-1}}{\max \left\{ e^{-\frac{|y_i - h_i x_m|^2}{N_0}} \right\}_{\substack{m=0 \\ b_j=1}}^{M-1}} \\ = & \frac{1}{N_0} \left[\min \left\{ |y_i - h_i x_m|^2 \right\}_{\substack{m=0 \\ b_j=1}}^{M-1} - \min \left\{ |y_i - h_i x_m|^2 \right\}_{\substack{m=0 \\ b_j=0}}^{M-1} \right] \end{aligned} \tag{4.139}$$

In order to find the LLR's of bits of z, we first find the relation between the bits of z and the bits of the transmitted symbols from the source and relay nodes. Let b_{z_j} be the j-th bit of z and b_{ij}, $i = 1, 2, r$ be the j-th bit of the symbol transmitted from the source or relay nodes. For 4-ary case, bits of z are given by

$$b_{z_1} = b_{11} + b_{21} + b_{r1} \tag{4.140}$$

and

$$b_{z_2} = \text{xor}\left(b_{11}, b_{12}, b_{21}, b_{22}, b_{r2}, v_1, v_2\right) \tag{4.141}$$

where $v_1 = b_{11}.b_{21}$ and $v_2 = b_{r1}.(b_{11} + b_{21})$. The LLR of bits of b_{z_1} is given by

$$\begin{aligned} L_{z_1} =& L(b_{z_1}|\mathbf{y}, \mathbf{h}) \\ =& \log \frac{P(b_{z_1} = 0)}{P(b_{z_1} = 1)} \end{aligned} \tag{4.142}$$

Using the approximation of [70] to find the LLR of b_{z_1} from (4.140) yields

$$L_{z_1} \approx \mathrm{sign}(L_{11}) \cdot \mathrm{sign}(L_{21}) \cdot \mathrm{sign}(L_{31}) \cdot \min\{|L_{11}|, |L_{21}|, |L_{31}|\} \tag{4.143}$$

Similarly, we can calculate the LLR of b_{z_2} as follows

$$\begin{aligned} L_{z_1} \approx & \mathrm{sign}(L_{32}) \cdot \mathrm{sign}(L_{v_1}) \cdot \mathrm{sign}(L_{v_2}) \cdot \prod_{\substack{i=1,2 \\ j=1,2}} \mathrm{sign}(L_{ij}) \\ & \cdot \min\{|L_{11}|, |L_{12}|, |L_{21}|, |L_{22}|, |L_{32}|, |L_{v_1}|, |L_{v_2}|\} \end{aligned} \tag{4.144}$$

where

$$\begin{aligned} L_{v_1} =& L(v_1|\mathbf{y}, \mathbf{h}) \\ =& L(b_{11} \cdot b_{21}|\mathbf{y}, \mathbf{h}) \\ =& \log \frac{e^{L_{11}} e^{L_{21}}}{1 + e^{L_{11}} + e^{L_{21}}} \\ \approx& L_{11} + L_{21} - \max\{0, L_{11}, L_{21}\} \end{aligned} \tag{4.145}$$

and

$$\begin{aligned} L_{v_2} =& L(v_2|\mathbf{y}, \mathbf{h}) \\ =& L(b_{21} \cdot (b_{11} + b_{21})|\mathbf{y}, \mathbf{h}) \\ =& \log \frac{e^{L_{31}} e^{L_{11,21}}}{1 + e^{L_{31}} + e^{L_{11,21}}} \\ \approx& L_{21} + L_{11,21} - \max\{0, L_{31}, L_{11,21}\} \end{aligned} \tag{4.146}$$

where

$$L_{11,21} \approx \mathrm{sign}(L_{11}) \cdot \mathrm{sign}(L_{21}) \min\{|L_{11}|, |L_{21}|\} \tag{4.147}$$

Now, we find $\hat{b_{z_1}}$ and b_{z_2} by making a hard decision on L_{z_1} and L_{z_2} respectively as follows

$$\hat{b}_{z_1} = \begin{cases} 0, & \text{if } \; L_{z_1} \geq 0 \\ 1, & \text{if } \; L_{z_1} < 0 \end{cases} \tag{4.148}$$

$$\hat{b}_{z_2} = \begin{cases} 0, & \text{if } \; L_{z_2} \geq 0 \\ 1, & \text{if } \; L_{z_2} < 0 \end{cases} \tag{4.149}$$

4.8.1 Probability of False Alarm

In this section, we drive the probability of false alarm resulting from using the MAP algorithm to detect misbehaving activity in the M-ary case. Let $x_{in} \in \{0, 1, \cdots, M-1\}$ is the input to the channel and $x_{out} \in \{0, 1, \cdots, M-1\}$ is the output of the channel. The channel is said to be symmetric if

$$P(x_{out} = i | x_{in} = j) = P(x_{out} = j | x_{in} = i) \quad i, j \in \{0, 1, \cdots, M-1\} \tag{4.150}$$

Assuming that all channels are symmetric, the probability of false alarm can be written as

$$P_{FA} = P(\hat{z} \neq z) \tag{4.151}$$

The estimated value of z is given by

$$\hat{z} = \hat{p} - \hat{x_1} - \hat{x_2} \tag{4.152}$$

where $-$ is the subtraction operation in $GF(M)$ and $\hat{p}, \hat{x_1}$, and $\hat{x_2}$ are estimated values of the symbols transmitted from the first source, the second source, and the relay node respectively. Let e_i be the error provided by the channel between the i-th source and the destination where $i = 1, 2$, e_p be the error provided by the channel between the relay and the destination, and e_z be the error in estimating z. Hence

$$z + e_z = p + e_p - x_1 - e_1 - x_2 - e_2 \tag{4.153}$$

Since $p = x_1 + x_2 + z$, the error in estimating z can be written as

$$e_z = e_p - e_1 - e_2 \tag{4.154}$$

The probability of false alarm can be written as

$$\begin{aligned} P_{FA} &= P(e_z \neq 0) \\ &= 1 - P(e_z = 0) \\ &= 1 - P(e_p - e_1 - e_2 = 0) \end{aligned} \tag{4.155}$$

Table 4.6 All possible combinations of e_p, e_1, e_2 that yields $e_z = 0$ in the case 4-ary

e_p	e_1	e_2	$e_z = e_p - e_1 - e_2 = 0$
0	0	0	0
0	1	1	0
0	2	2	0
0	3	3	0
1	0	1	0
1	1	0	0
1	2	3	0
1	3	2	0
2	0	2	0
2	1	3	0
2	2	0	0
2	3	1	0
3	0	3	0
3	1	2	0
3	2	1	0
3	3	0	0

To find a closed form expression for the probability of false alarm, let's consider the 4-ary example. The same procedure can be generalized to find the probability of false alarm for M-ary case. Table 4.6 shows all possible values of e_p, e_1, and e_2 at which $e_z = 0$. For mathematical traceability, we assume that all channels have the same average receive SNR γ. Hence, $P(e_p = 0) = P(e_1 = 0) = P(e_2 = 0) = P_e$. The probability of $z = 0$ is given by

$$\begin{aligned} P(z = 0) = &(1 - P_e)^3 + 9P_e^2 (1 - P_e) + 6P_e^3 \\ =&1 - 3P_e + 12P_e^2 - 4P_e^3 \end{aligned} \tag{4.156}$$

Hence, the probability of false alarm is given by

$$P_{FA} = 3P_e - 12P_e^2 + 4P_e^3 \tag{4.157}$$

In case of 4-QAM modulation, and for Rayleigh channel, the error probability P_e is given by [44]

$$P_e \approx 1 - \sqrt{\frac{\gamma}{2 + \gamma}} \tag{4.158}$$

Hence, the probability of false alarm is given by

$$P_{FA} \approx 3\left(1-\sqrt{\frac{\gamma}{2+\gamma}}\right) - 12\left(1-\sqrt{\frac{\gamma}{2+\gamma}}\right)^2 + 4\left(1-\sqrt{\frac{\gamma}{2+\gamma}}\right)^3 \tag{4.159}$$

4.9 Estimation of Relay-Destination Channel

As described in the previous sections, the channel gains h_1, h_2, and h_r are required for both detection and decoding processes. The most common way of channel estimation is to insert pilot symbols in the transmitted signal that are known to the destination, and to compare the pilot symbols with corresponding received symbols. This method of channel estimation requires the compliance of the sender nodes with the transmission protocol. For the case of misbehaving relay, the relay node may send a falsified data instead of the actual pilot symbols which results in an incorrect estimation of the channel between this relay and the destination h_r. In order to cope with this problem, the destination should rely on the relay when estimating h_r. Blind channel estimation (BCE) is an alternative method which can be used to find h_r. BCE does not require the use of pilot symbols and moreover it possesses desirable advantages such as a better bandwidth efficiency. Many BCE methods in various types of communication systems have been developed since the early 80s (see [81] and references therein).

Figure 4.4 shows the baseband representation of a digital communication system. The communication channel is characterized as a linear time invariant (LTI) system which has a finite impulse response (FIR) due to finite delay spread of the channel. The impulse response $h(t)$ is a cascade of the pulse shaping filter in the transmitter, the physical multipath fading channel, and the receive filter. Assume the symbol interval of the input signal is T . The output signal can be written as

$$y(t) = h(t) * s(t) + w(t) \tag{4.160}$$

where "*" denotes the convolution. When the output signal is sampled at the baud rate (i.e., at the rate $1/T$), the system can be simplified as in Figure 4.4-(b), where the equivalent channel, $H(z)$, is a discrete LTI system. The received signal $y(n)$ is a noise corrupted version of the

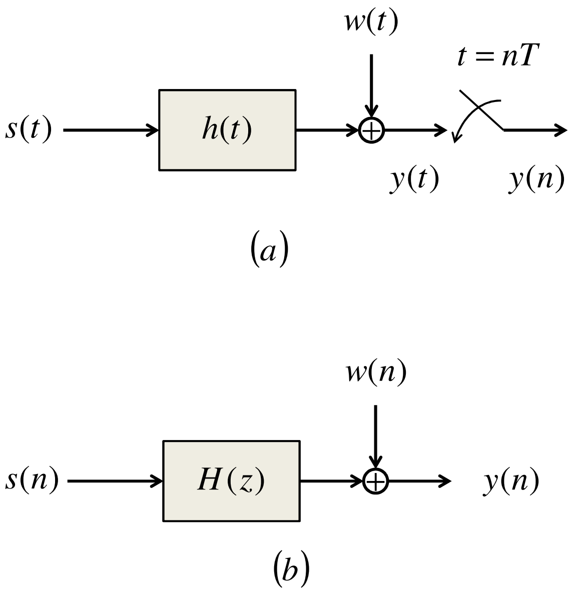


Figure 4.4 Baseband representation of a digital communication channel. (a) Analog model with a bandlimited channel impulse response $h(t)$; (b) Equivalent digital model with channel transfer function $H(z)$.

convolution of the input signal $s(n)$ and the channel impulse response $h(n)$ and it's given by

$$y(n) = h(n) * s(n) + w(n) \tag{4.161}$$

Blind channel estimation seeks to estimate the channel $H(z)$ without explicit knowledge of $s(n)$. Mathematically, it is similar to blind deconvolution problem in control or image processing literature.

A simple method for blind channel estimation is using the second order statistics (SOS) or higher order statistics (HOS). Consider the SOS case where the power spectral density of the output signal is given by

$$S_{yy}(z) = |H(z)|^2 S_{ss}(z) + S_{ww}(z) \tag{4.162}$$

where $S_{yy}(z) = \sum_m E\left[y(n)y^*(n-m)\right] z^{-m}$, $S_{ss}(z) = \sum_m E\left[s(n)s^*(n-m)\right] z^{-m}$, and $S_{ww}(z)$ $= \sum_m E\left[w(n)w^*(n-m)\right] z^{-m}$. Assume the input spectral density function $S_{ss}(z)$ is known, then the amplitude of the channel can be identified but the phase information of $H(z)$ is missing. In order to obtain the full information of the channel, HOS of $y(n)$ is employed in many blind algorithms (e.g., 4-th order) [82].

Another powerful technique for blind channel estimation is *ML Method* [83]. In general, consider the case of single input multiple output (SIMO) system. Consider a mathematical model where the input and the output are discrete, the system operator H is linear and shift invariant, the system is driven by a single-input sequence $s(k)$ and yields M output sequences $y_1(k), y_2(k), \cdots, y_M(k)$, and the system has finite impulse responses (FIRs) $h_i(k)$, $i = 1, 2, \cdots, M$, $k = 0, 1, \cdots, L$, and L is the filter length. Such a system model can be described as follows (in the absence of noise):

$$\begin{cases} y_1(k) = s(k) * h_1(k) \\ y_2(k) = s(k) * h_2(k) \\ \qquad\vdots \\ y_M(k) = s(k) * h_M(k) \end{cases} \tag{4.163}$$

All channel outputs can be stacked into a single vector as follows

$$\mathbf{y} = \left[\mathbf{y}_1^T \; \mathbf{y}_2^T \; \cdots \; \mathbf{y}_M^T\right]^T \tag{4.164}$$

with

$$\mathbf{y}_i = [y_i(0) \; y_i(1) \; \cdots \; y_i(N-1)]^T \tag{4.165}$$

where N is the number of output samples from each channel and "T" denotes the transpose. Accordingly, and after including the noise, (4.163) can be written as

$$\mathbf{y} = \mathbf{H}_M \mathbf{s} + \mathbf{w} \tag{4.166}$$

where $\mathbf{s}$ is the input vector and it is given by

$$\mathbf{s} = [s(-L) \; s(-L+1) \; \cdots \; s(N-1)]^T \tag{4.167}$$

and $\mathbf{w}$ is an additive circular white Gaussian noise vector. $\mathbf{H}_M$ is known as a generalized

Sylvester matrix and it is given by

$$\mathbf{H}_M = \begin{bmatrix} \mathbf{H}_{(1)} \\ \mathbf{H}_{(2)} \\ \vdots \\ \mathbf{H}_{(M)} \end{bmatrix} \tag{4.168}$$

where $\mathbf{H}_{(1)}$ is the $N \times (N+L)$ Sylvester matrix of the i-th channel response

$$\mathbf{H}_{(i)} = \begin{bmatrix} h_i(L) & \cdots & h_i(0) & \cdots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \cdots & h_i(L) & \cdots & h_i(0) \end{bmatrix} \tag{4.169}$$

The PDF of $\mathbf{y}$ is given by

$$p(\mathbf{y}) = \frac{1}{\pi^N \sigma^{2N}} \exp\left(-\frac{1}{\sigma^2} ||\mathbf{y} - \mathbf{H}_M \mathbf{s}||^2 \right) \tag{4.170}$$

where σ^2 is the variance of each complex element of $\mathbf{w}$, and $|| \cdot ||$ denotes two-norm. The ML estimates of $\mathbf{H}_M$ and $\mathbf{s}$ are given by those arguments that maximize the PDF , i.e.,

$$\begin{aligned} (\mathbf{H}_M, \mathbf{s})_{\mathrm{ML}} &= \arg\max_{\mathbf{H}_M, \mathbf{s}} p(\mathbf{y}) \\ &= \arg\min_{\mathbf{H}_M, \mathbf{s}} ||\mathbf{y} - \mathbf{H}_M \mathbf{s}||^2 \end{aligned} \tag{4.171}$$

For any given $\mathbf{H}_M$, the ML estimate of $\mathbf{s}$ that minimizes the quadratic function $||\mathbf{y} - \mathbf{H}_M \mathbf{s}||^2$ is known to be

$$\mathbf{s}_{\mathrm{ML}} = \left(\mathbf{H}_M^H \mathbf{H}_M \right)^{-1} \mathbf{H}_M^H \mathbf{y} \tag{4.172}$$

where "^{H}" denotes the conjugate transpose. Substituting from (4.172) into (4.171) yields

$$(\mathbf{H}_M)_{\mathrm{ML}} = \arg\min_{\mathbf{H}_M} ||(\mathbf{I} - \mathbf{P}_H)\mathbf{y}||^2 \tag{4.173}$$

where $\mathbf{P}_H$ is the orthogonal projection matrix onto the range of $\mathbf{H}_M$, i.e.,

$$\mathbf{P}_H = \mathbf{H}_M \left(\mathbf{H}_M^H \mathbf{H}_M \right)^{-1} \mathbf{H}_M^H \tag{4.174}$$

Although the minimization in (4.173) is computationally much more efficient than that in (4.171), it is still highly nonlinear. Therefore, the computation of (4.173) has to be iterative in nature. Many iterative optimization approaches such as [84, 85] can be applied to compute (4.173). For the case when the system is modeled by $y_r = \sqrt{E_r d_r^{-m}} h_r p + n_r$, the same solution can be found by setting $L = 1$ and $M = 1$.

4.10 Decoding Error Probability in The Case of K Sources

In this section we drive union bound on the decoding error probability for the MAP decoder with $P(z)$ when the network is compose of K sources, single relay, and single destination. In this case, the decoder codebook consists of 2^{K+1}. The codebook can be divided into two sets such that all codewords in the same set are equaprobable. Let A be the set of codewords which contains the "all-zeros" codeword and B be the other set. Therefore, the probability of any codeword in the set A, $\mathbf{c}_a$, is $P(\mathbf{c}_a) = P(z = +1)/(2^K)$ and that of any codeword in the set B, $\mathbf{c}_b$, is $P(\mathbf{c}_b) = P(z = -1)/(2^K)$. We notice that all codewords in the set A will have even weights and those in the set B will have odd weights. Without loss of generality, we assume that all-zeros codeword was transmitted. The union bound in the decoding error probability can be written as

$$P_E \leq \sum_{m=1}^{K+1} \binom{K+1}{m} P_m \tag{4.175}$$

where $P_m = \{P(c_i \rightarrow c_j)$ such that c_i differs from c_j in m bits $\}$. Since P_m decreases as m increases, we only consider the contribution of P_1 and P_2. Hence,

$$\begin{aligned} P_E \leq & \frac{K+1}{2}\left[1-\sqrt{\frac{\gamma}{1+\gamma}}\right] e^{\frac{-L(z)}{2}(1+\sqrt{1+\frac{1}{\gamma}})} \\ & + \frac{K(K+1)}{4}\left[1-\sqrt{\frac{\gamma}{1+\gamma}}\right]^2 \left(1+\frac{1}{2}\sqrt{\frac{\gamma}{1+\gamma}}\right) \end{aligned} \tag{4.176}$$

4.11 Results and discussions

For the results shown in section, we assume that all source and relay nodes have an equal receive signal-to-noise-ratio (SNR).

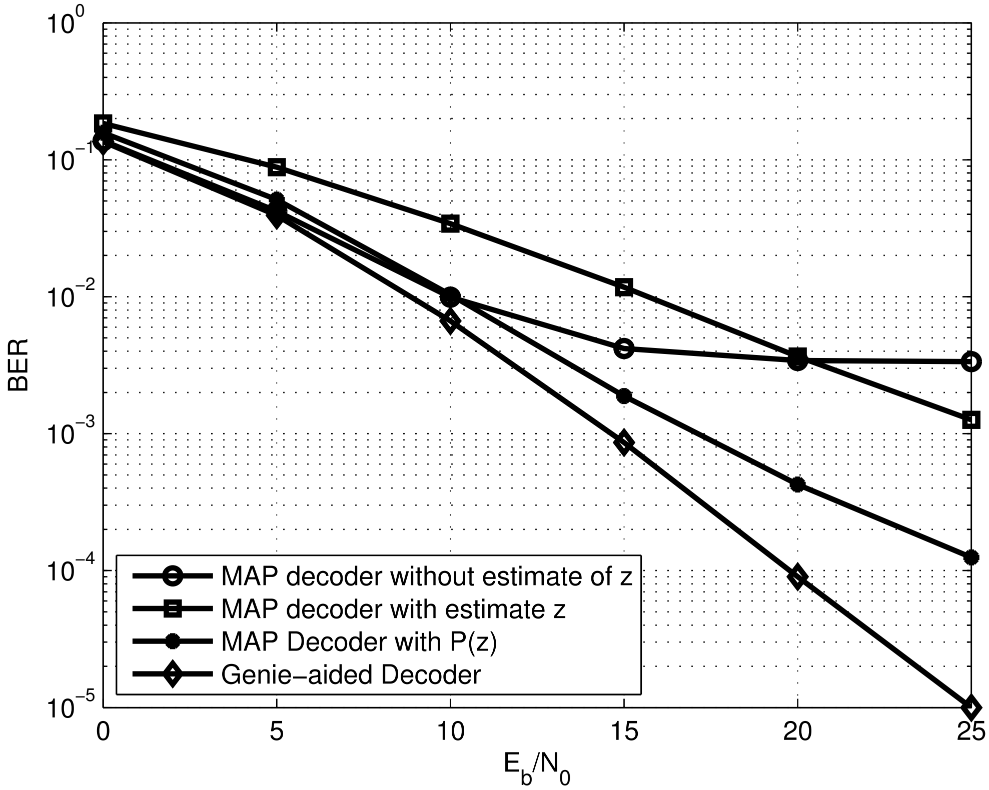


Figure 4.5 Bit error probability vs E_b/N_0 for $P(z = -1) = 0.01$

Figure 4.5 shows the simulation results of the bit error probability against the receive SNR E_b/N_0 for the discussed decoding schemes when $P(z = -1) = 0.01$. We see that there is an error floor in the case of ignorant receiver. This result matches with the union bound of (4.55). We also see that the error probability of proposed decoder falls in the rate of -1 i.e. diversity order = 1. That is because the false alarm and miss detection of the misbehaving activity of the relay node. This effect shows up in the second term of the right-hand side of (4.83). We also see that both MAP decoder and Genie-aided decoder provide a diversity order 2. There is about $4dB$ performance loss even with the use of MAP decoder. That because of the falsified data injection at the relay node.

Figure 4.6 shows the simulation results of the bit error probability against the receive SNR E_b/N_0 when $P(z = -1) = 0.99$. We see that the error floor of the ignorant receiver occurs

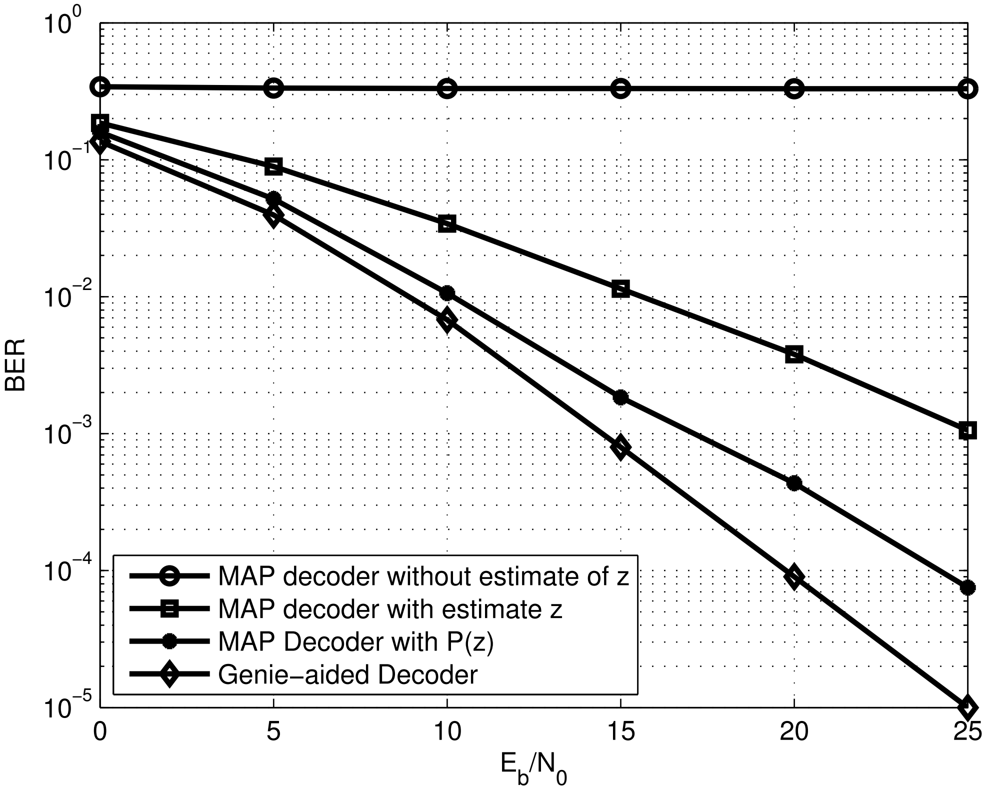


Figure 4.6 Bit error probability vs E_b/N_0 for $P(z = -1) = 0.99$

at higher value. That because $P(z = -1)$ was increased. Figure 4.7 shows the simulation results of the bit error probability against the receive SNR E_b/N_0 when $P(z = -1) = 0.5$. This figure shows the wrest case where the performance of the proposed decoder and the MAP decoder coincides. Figure 4.8 compares the union bounds on the decoding error probability of the proposed decoding schemes with the simulation results. We see that there is about 3 dB difference between the upper bound and the exact error probability found by simulations.

Figure 4.9 shows the average probability of false alarm against E_b/N_0 where E_b is the receive energy per the source bit. In this figure, we assume that the receive energy of the relay bit is as twice as that of the source bit. The number of formation bits is 45 bits. The number of parity bits used in the case of channel coding aided MAP and the number of tracing bits used in the case of tracing bit aided MAP are equal and this number is $t = 18$ bits. The

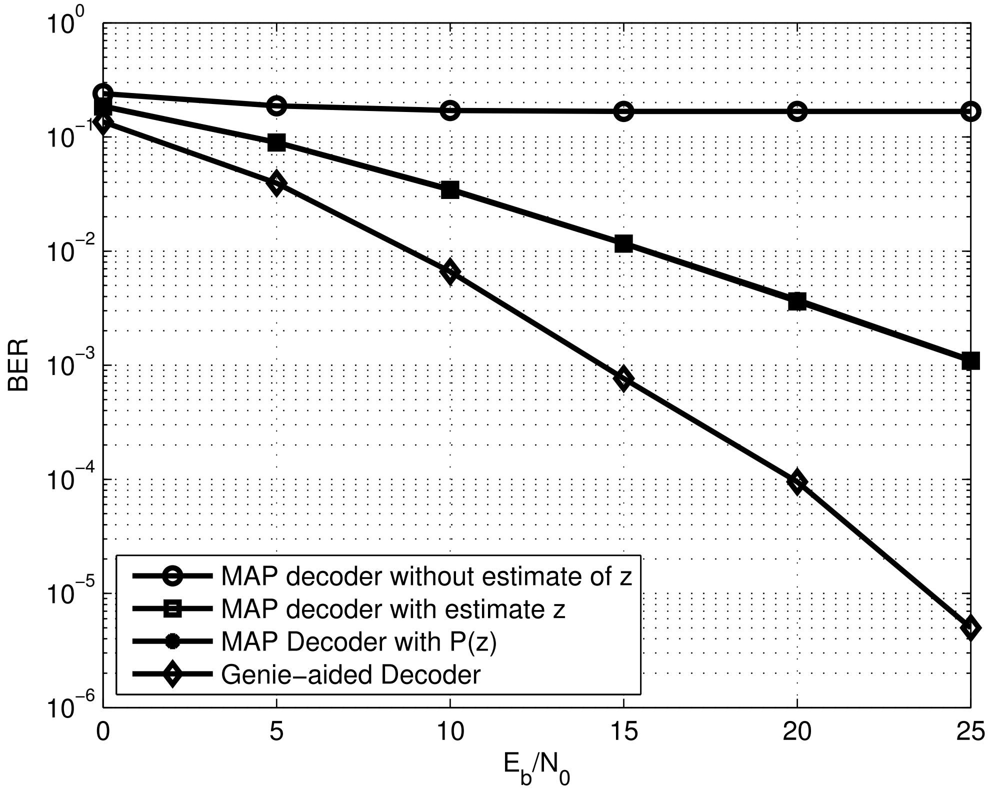


Figure 4.7 Bit error probability vs E_b/N_0 for $P(z=-1)=0.5$

total number of bits per source is $n=63$. For BCH code, the number of errors that can be corrected is 3 errors. We notice that the probability of false alarm for both tracing bit and channel coding aided MAP is less than that of the basic MAP at any SNR value. We also notice that channel coding aided MAP outperforms the tracing bit aided MAP at high SNR regime. That is because at high SNR regime the probability of error is small and the channel code can correct all channel errors. Therefore all bits from the source seem to be tracing bits, i.e. $t=63$. However, in the tracing bit aided MAP case the number of tracing bits is fixed, i.e. $t=18$.

Figure 4.10 shows the probability of false alarm against E_b/N_0 when the destination is equipped with two antennas. We notice that P_{FA} falls in the rate of -2 i.e. diversity order $=2$. Hence, there is a about 15 dB SNR gain over the single antenna case when $P_{FA}=10^{-3}$

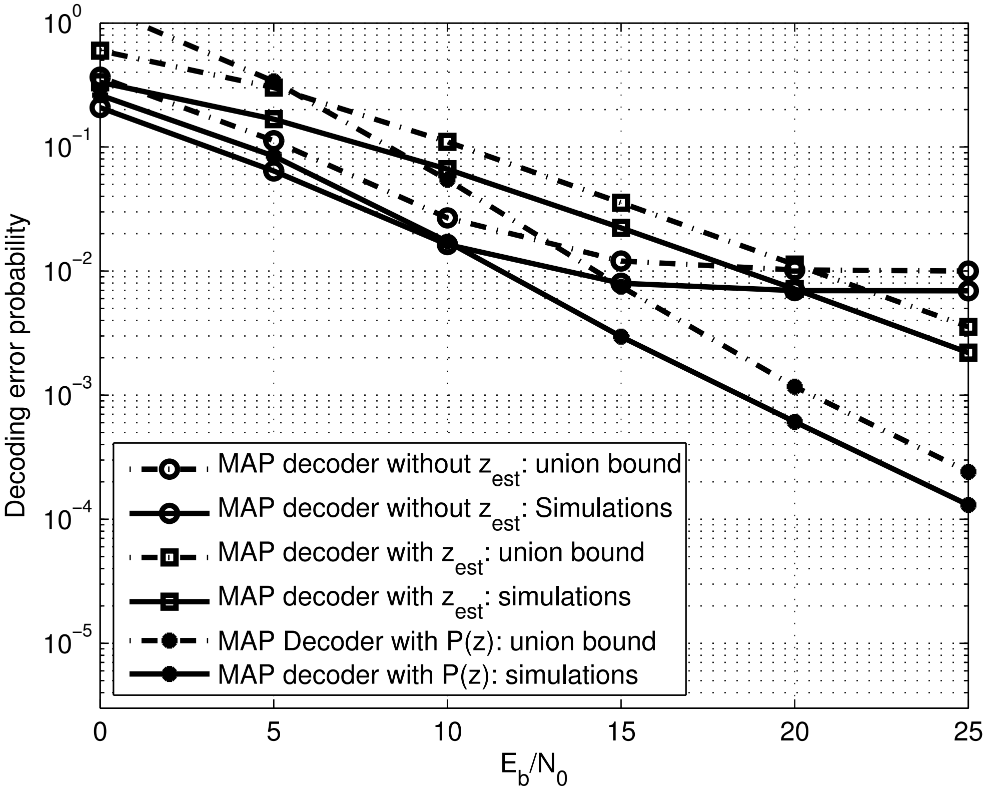


Figure 4.8 Comparing the union bounds on the decoding error probability with simulations results.

Figure 4.11 shows the probability of false alarm against E_b/N_0 In the case of M-ary modulation. The SNR γ in (4.159) is related to E_b/N_0 as follows

$$\gamma = \frac{K}{N}\frac{E_b}{N_0}\log_2(M) \tag{4.177}$$

where K is the number of source nodes and $N-K$ is the number of relay nodes. For the system model we considered in this section and for 4-ary modulation, the SNR is $\gamma = 4E_b/3N_0$. We notice that the probability of false alarm falls with diversity order 1. The techniques proposed in Section 4.7 such as tracing bits, error correcting codes, and multiple antennas can be used in order to enhance the performance of the MAP decoder. We also notice that the theoretical results matches with the simulation results except for the region below 10 dB. That is because the aproximation in (4.158) holds only at high SNR.

In order to study the effect of channel estimation error in the relay-destination link on the decoding error probability , we assume that the estimation error h_e is a complex Gaussian random variable with zero mean and variance σ_e^2. Hence, the estimated channel gain between the relay and the destination is given by

$$h_{r_{\text{est}}} = h_r + h_e \tag{4.178}$$

where h_r is the actual channel gain and it follows a complex Gaussian distribution with zero mean and variance σ_h^2. Figure 4.12 shows the simulation results for the bits error probability against E_b/N_0 when $K = 2$, $P(z = -1) = 0.005$, $\sigma_e^2/\sigma_h^2 = 5\%$. We see that there is about 1 dB SNR loss at 3×10^{-4} error rate because of the channel estimation error. Figure 4.13 shows the simulation results of the bit error probability against E_b/N_0 when $K = 2$, $P(z = -1) = 0.005$, $\sigma_e^2/\sigma_h^2 = 20\%$. We see that there is about 5 dB SNR loss at 3×10^{-4} error rate because of the channel estimation error. We notice that the SNR loss increases as the variance of the estimation error increases. Figure 4.14 shows the union bound on the decoding error probability of (4.176) vs the number of users K. We notice that the decoding error probability union bound increases as the number of users increases.

4.12 Conclusions

We proposed the MAP approach in detecting the misbehaving relay that injects false data or adds channel errors into the network encoder in multi-access relay networks. The proposed scheme does not require sending extra bits at the source, such as hash function or message authentication check bits, hence there is no transmission overhead. In addition, it makes an instantaneous decision about whether a relay node is behaving properly without a long-term observation. The side information regarding the presence of forwarding misbehavior is exploited at the probability of bit error, taking into account the lossy nature of wireless links. We found that the proposed decoder and the MAP decoder with the aid of the MAP detection are effective in mitigating the forwarding misbehaviors in multiple access networks with network coding.

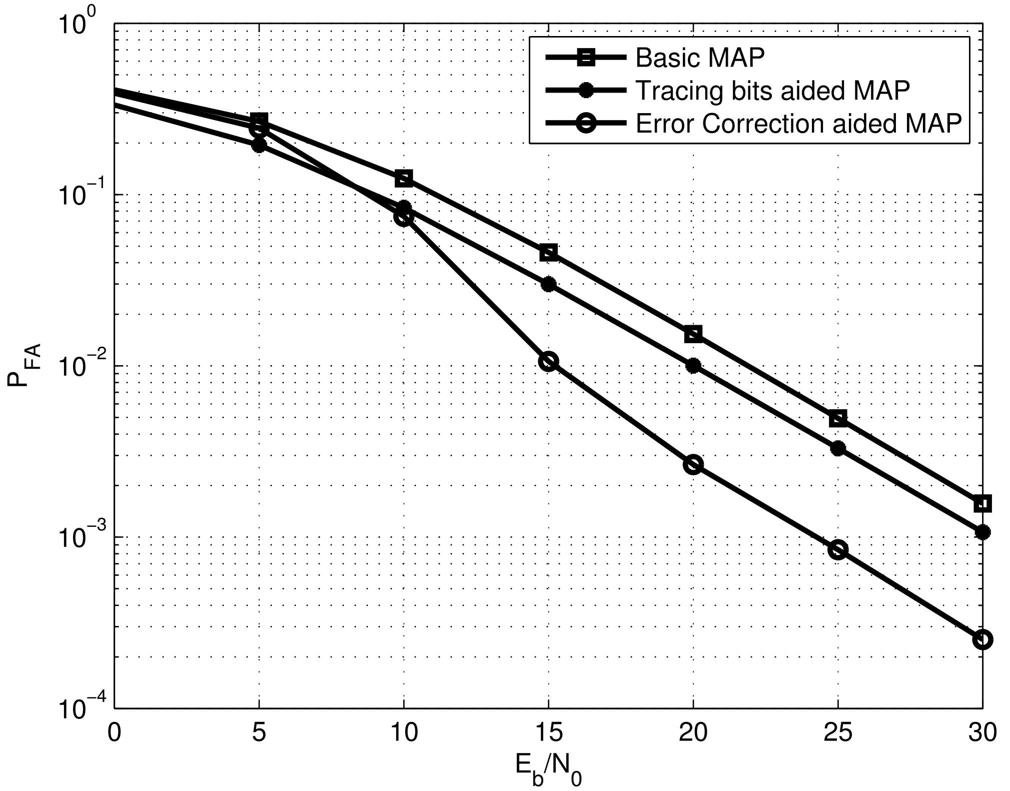


Figure 4.9 Probability of false alarm vs E_b/N_0

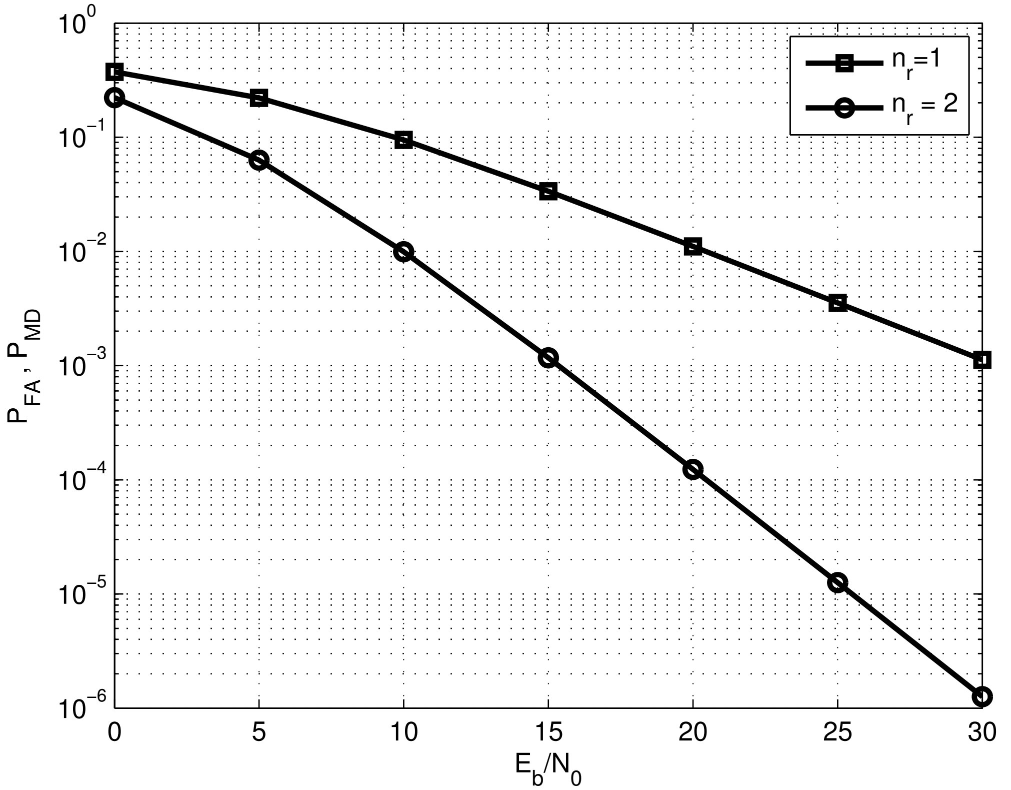


Figure 4.10 Probability of false alarm vs E_b/N_0 when the destination is equipped with two antennas

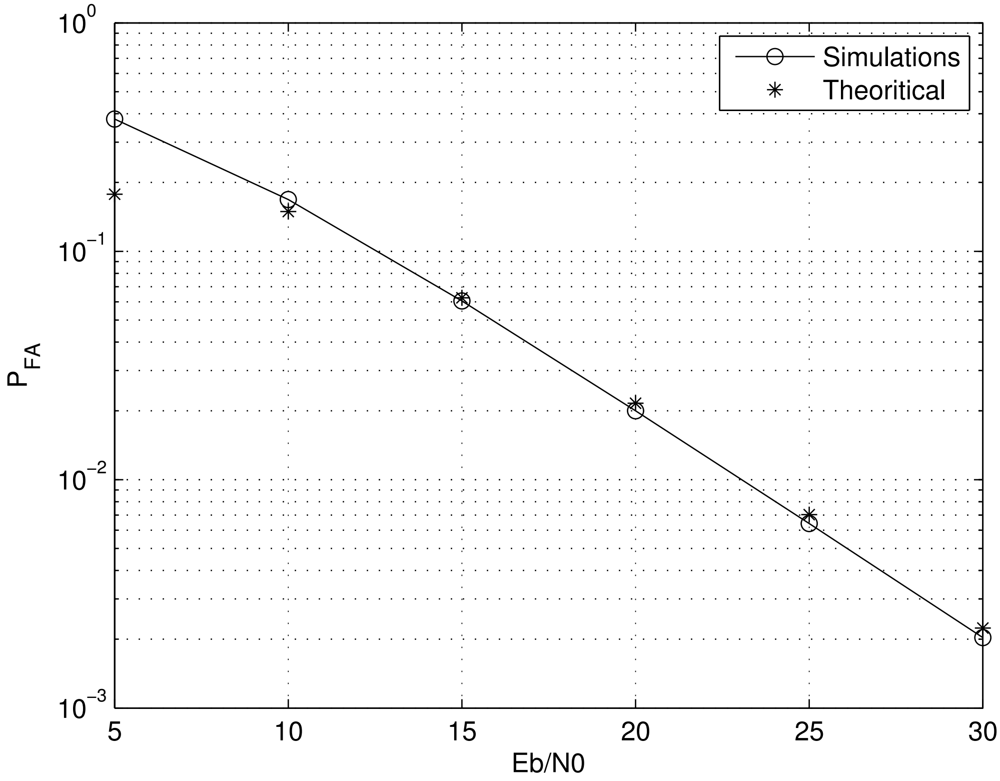


Figure 4.11 Probability of false alarm vs. E_b/N_0 for 4-QAM modulation case

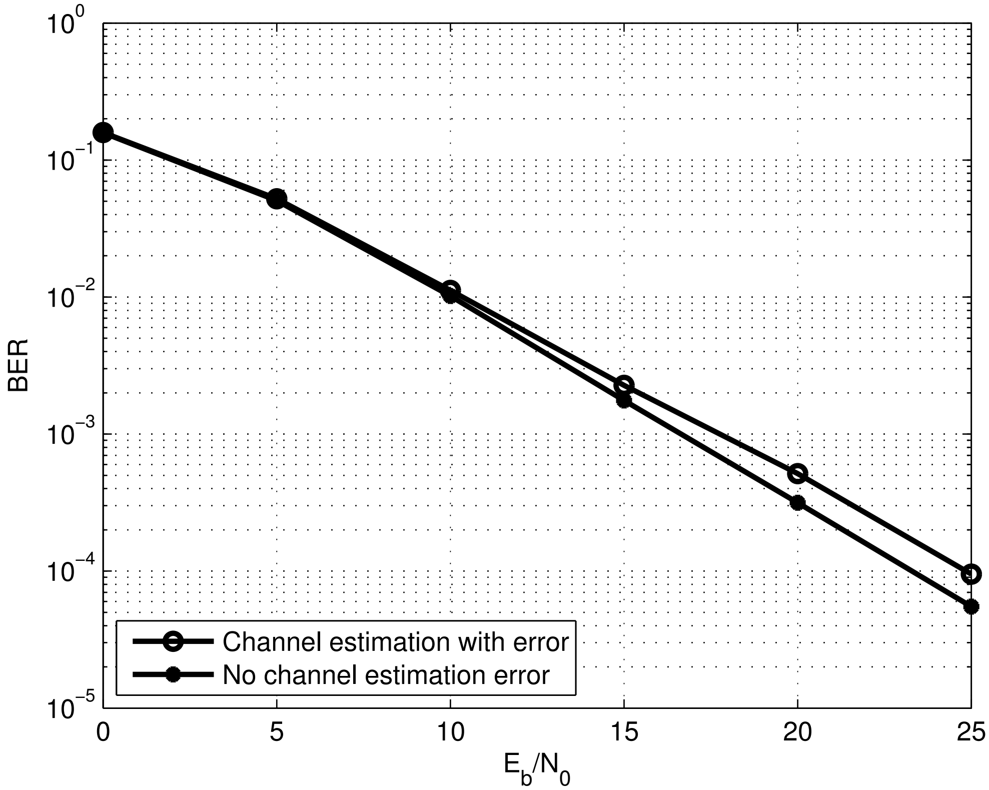


Figure 4.12 BER vs E_b/N_0 when $\sigma_e^2/\sigma_h^2 = 5\%$

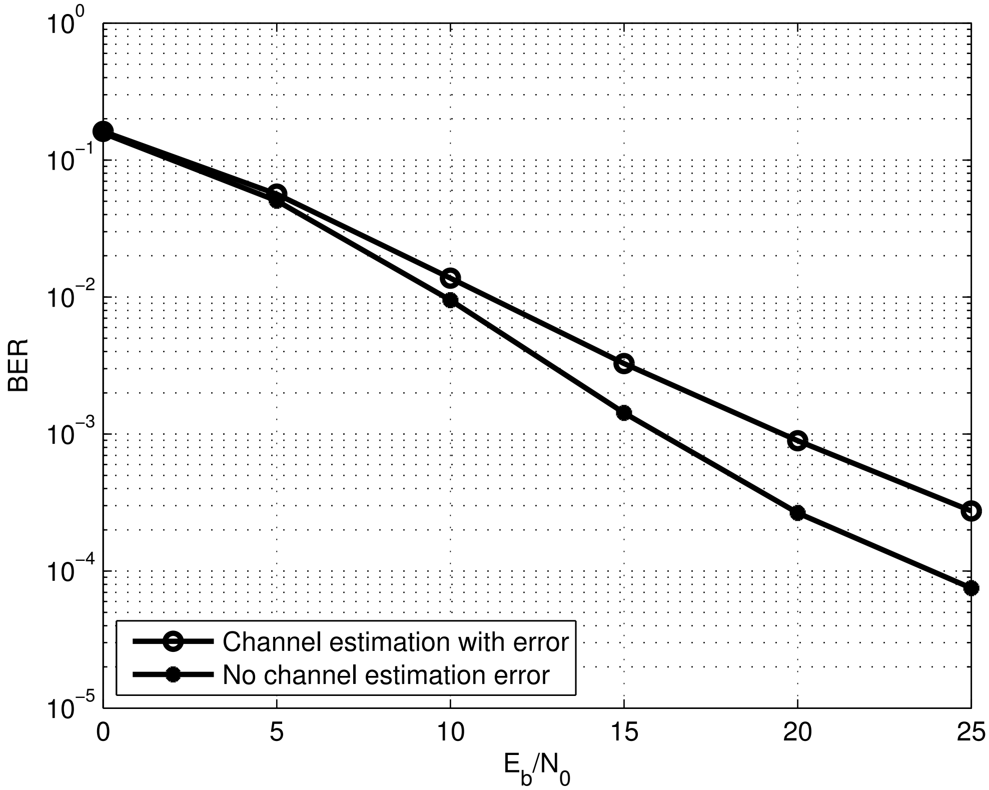


Figure 4.13 BER vs E_b/N_0 when $\sigma_e^2/\sigma_h^2 = 20\%$

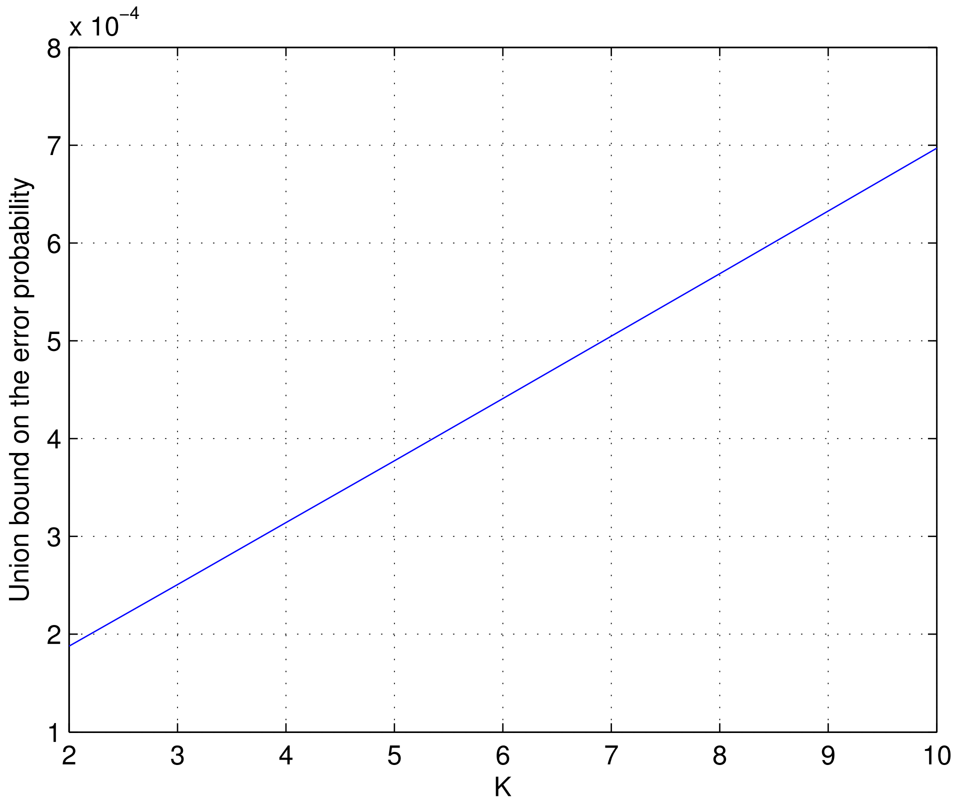


Figure 4.14 Union bound on the decoding error probability against number of users K

CHAPTER 5. Delay Analysis in Message Ferrying System

Message Ferrying is a network paradigm in which a moving node or relay is used to transfer messages between sparsely deployed and further separated nodes in mobile ad-hoc networks. In this paradigm, the moving relay - also called message ferry (MF)- stores, carries, and forwards the messages. This paper analyzes the total delay time in transferring the message between source and destination nodes taking into account the effect of channel fading, path loss, and forward error correction. The performance gain in terms of delay and energy provided by moving relay over static relay and the optimal locations of the moving relay that minimize the total delay are determined. Both simulations and analytical calculations are provided.

5.1 Introduction

Mobile ad hoc network (MANET) is an independent collection of mobile nodes that communicate without a pre-existing infrastructure [74]. MANETs are proposed to meet the requirements of the next generation of wireless communication systems. One of these requirements is the rapid deployment of mobile users. Another characteristic of MANET's is a resource limitation in terms of power and bandwidth, which requires an efficient routing protocols [75]. Several routing protocols have been proposed [76]- [77]. These protocols assume that all nodes are reachable and the network is fully connected.

There are several reasons that cause network partitioning (i.e., nodes are not reachable), such as mobility of nodes, limited radio range, weather conditions, and physical obstacles. In this case, the traditional "store and forward" paradigm is not possible in delivering the message. "Store, hold, and forward" paradigm was proposed to cope with this problem [78]. In this paradigm, nodes store and hold packets even when a route does not exist. Later, the

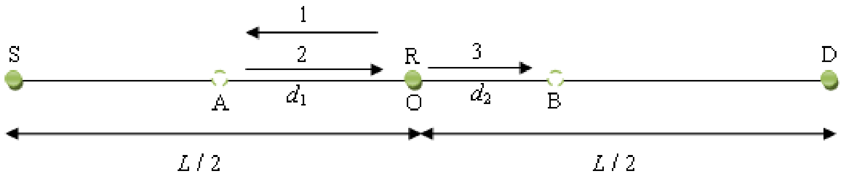


Figure 5.1 Source, destination, and relay locations.

packet may be passed to another node that has recently come into range. Zhao and Ammar presented another scheme called *message ferrying* [79]. In Message Ferrying scheme, a moving relay or Message Ferry (MF) follows a “store, carry, and forward” paradigm by accomplishing consecutive events: 1) moves toward the transmitting node, 2) waits until it receives the message, 3) moves toward the receiving node, 4) waits until it delivers the message. Although some routing algorithms have been proposed [79]- [80], the design of the MF route is still an open research topic.

In this paper, we investigate the trade-off between the two types of delay: 1) the delay involved in moving the relay toward the source and the destination and 2) the delay involved in correctly receiving the packet at the relay and the destination which depends on the location of the moving relay node. Our goal is to find the optimal location of the relay that minimizes the total delay, taking into account the effect of channel fading, path loss, and forward error correction (FEC). We analyze the performance gain in terms of delay and energy that can be provided by message ferrying in various scenarios and the optimal code rate that minimizes the delay.

The system model is described in Section 5.2. Delay calculations and the optimal location of the relay that minimizes the total delay are presented in Section 5.3 and Section 5.5 respectively. Section 5.4 presents numerical results. Finally, the conclusions are drawn in Section 5.6.

5.2 System Model

The system model is shown in Figure 5.1, where the source S and the destination D are L meters apart. The relay R is initially located at the midpoint between S and D (i.e., $L/2$

meters far from S and D). First, the relay moves d_1 meters toward S with velocity v m/s and stays at point A until it correctly receives the message. Then, it moves toward D by $d_1 + d_2$ meters with the same velocity v m/s and stays at point B until the message is correctly received by the destination. The total delay time τ is then given by:

$$\tau = \frac{d_1}{v} + \tau_{SR} + \frac{d_1 + d_2}{v} + \tau_{RD} \tag{5.1}$$

where τ_{SR} and τ_{RD} are the time for delivering the message from the source to the relay and that from the relay to the destination, respectively.

We assume that the message consists of N_P packets or code words and each code word is of length n bits in which k bits are information bits. The channel is modeled as slow Rayleigh fading with additive white Gaussian noise (AWGN) having power spectral density of $N_o/2$. We assume that BPSK modulation and BCH codes are used.

5.3 Delay

The average received SNR at point A, $\bar{\gamma}_{SR}$ is given by

$$\bar{\gamma}_{SR} = \frac{d_{SR}^{-m} P_S}{R N_o} \tag{5.2}$$

where P_S is the transmitted power of the source, R is the data rate (bits/s), m is the path loss exponent, and d_{SR} is the distance between the source and the relay. The probability of bit error at point A is given by

$$\begin{aligned} P_{b_{SR}} &= \frac{1}{2}\left[1 - \sqrt{\frac{\bar{\gamma}_{SR}}{1 + \bar{\gamma}_{SR}}}\right] && (5.3) \\ &\approx \frac{1}{4\bar{\gamma}_{SR}} && (5.4) \end{aligned}$$

If we assume the use of forward error correction (FEC) that corrects up to t errors, then the word error rate WER, $P_{E_{SR}}$ is given by

$$P_{E_{SR}} = \sum_{i=t+1}^{n} \binom{n}{i} P_{b_{SR}}^{i} \left(1 - P_{b_{SR}}\right)^{n-i} \tag{5.5}$$

The average number of transmissions from S to R before the message is correctly received by the relay is given by

$$N_{SR} = \sum_{i=1}^{\infty} i P_{E_{SR}}^{i-1} \left(1 - P_{E_{SR}}\right) \tag{5.6}$$

$$= \frac{1}{1 - P_{E_{SR}}} \tag{5.7}$$

and the time required to transmit one packet is n/R. Hence, the time delay in correctly receiving N_P packets by the relay is given by

$$\tau_{SR} = N_P \frac{n}{R\left(1 - P_{E_{SR}}\right)} \tag{5.8}$$

Similarly, the average received SNR at the destination receiver is given by

$$\bar{\gamma}_{RD} = \frac{d_{RD}^{-m} P_R}{R N_o} \tag{5.9}$$

where P_R is the transmitted power of the relay and d_{RD} is the distance between the relay and the destination. The probability of bit error at D is given by

$$P_{b_{RD}} = \frac{1}{2}\left[1 - \sqrt{\frac{\bar{\gamma}_{RD}}{1 + \gamma_{\bar{R}D}}}\right] \tag{5.10}$$

$$\approx \frac{1}{4\bar{\gamma}_{RD}} \tag{5.11}$$

Hence, the time delay in correctly receiving N_P packets by the destination node is given by

$$\tau_{RD} = N_P \frac{n}{R\left(1 - P_{E_{RD}}\right)} \tag{5.12}$$

where $P_{E_{RD}}$ can be calculated from (5.5) with replacing $P_{b_{SR}}$ by $P_{b_{RD}}$. Substituting from (5.8) and (5.12) into (5.1) yields

$$\tau = \frac{2d_1}{v} + \frac{N_P n}{R\left(1 - P_{E_{SR}}\right)} + \frac{d_2}{v} + \frac{N_P n}{R\left(1 - P_{E_{RD}}\right)} \tag{5.13}$$

Now, we want to find d_1 and d_2 that minimize the total delay τ. Since the first two terms of (5.13) depend only on d_1 and the remaining two terms depend only on d_2, the minimization of τ is achieved by minimizing

$$\tau_1 = \frac{2d_1}{v} + \frac{N_P n}{R\left(1 - P_{E_{SR}}\right)} \tag{5.14}$$

with respect to d_1 and minimizing

$$\tau_2 = \frac{d_2}{v} + \frac{N_P n}{R\left(1 - P_{E_{RD}}\right)} \tag{5.15}$$

with respect to d_2.

5.4 Optimal Relay Location

In high SNR, the probability of bit error in (5.4) is small and therefore the WER in (5.5) can be approximated by

$$P_{E_{SR}} \approx \binom{n}{t+1} P_{b_{SR}}^{t+1} \tag{5.16}$$

Substituting (5.4) into (5.16) yields

$$\begin{aligned} P_{E_{SR}} &\approx \binom{n}{t+1}\left(\frac{RN_o}{4P_S}\right)^{t+1} d_{SR}^{m(t+1)} \qquad (5.17)\\ &= \beta_1\left(\frac{L}{2} - d_1\right)^{m(t+1)} \qquad (5.18)\end{aligned}$$

where $d_{SR} = L/2 - d_1$ and $\beta_1 = \binom{n}{t+1}\left(\frac{RN_o}{4P_S}\right)^{t+1}$ and it will be small in high SNR regime. Substitute (5.17) into (5.14) yields

$$\begin{aligned} \tau_1 &\approx \frac{2d_1}{v} + N_P\frac{n}{R}\left(1 - \beta_1\left(\frac{L}{2} - d_1\right)^{m(t+1)}\right)^{-1} \qquad (5.19)\\ &\approx \frac{2d_1}{v} + N_P\frac{n}{R}\left(1 + \beta_1\left(\frac{L}{2} - d_1\right)^{m(t+1)}\right) \qquad (5.20)\end{aligned}$$

Differentiating (5.20) with respect to d_1 and setting it to zero, yields

$$\frac{2}{v} - \frac{N_P n\beta_1 m(t+1)}{R}\left(\frac{L}{2} - d_{1_{opt}}\right)^{m(t+1)-1} = 0 \tag{5.21}$$

Hence, the optimal value of d_1 that minimizes τ_1 is given by

$$d_{1_{opt}} \approx \frac{L}{2} - \left(\frac{2R}{vN_P n\beta_1 m(t+1)}\right)^{1/(m(t+1)-1)} \tag{5.22}$$

Similarly, the optimal value of d_2 that minimizes τ_2 is

$$d_{2_{opt}} \approx \frac{L}{2} - \left(\frac{R}{vN_P n\beta_2 m(t+1)}\right)^{1/(m(t+1)-1)} \tag{5.23}$$

where $\beta_2 = \binom{n}{t+1}\left(\frac{RN_o}{4P_R}\right)^{t+1}$.

5.5 Numerical Results and Discussions

In this section, we present numerical values of d_1 and d_2 that minimize delays τ_1 and τ_2 in (5.14) and (5.15). When the relay is located at the middle point O, we assume that $\bar{\gamma}_{SR} = \bar{\gamma}_{RD} = \bar{\gamma}_i$. We assume BCH code of code rate $R_C = k/n$ where k is the number of information bits per packet. In other words, there are $n - k$ parity bits within each packets. Hence, the number of packets N_P is q/k where q is the total data size. The code rate R_C is chosen to minimize the total delay in both cases of mobility and no-mobility. To calculate the optimal code rate, we choose n (e.g., $n = 63$) and for each possible value of k, we find the corresponding value of t and calculate N_P. Fixing all other parameters and for each pair t and N_P, we calculate the minimum delay τ_{min} and the value of R_C corresponding to the minimum τ_{min} is chosen. We define two performance measures:

1. **Delay Gain**

   The delay gain G_τ is defined as the difference between the delay when the relay is located at O and the minimum delay provided by message ferrying.

2. **Energy Gain**

   The energy gain G_E (or *energy saving*) is defined as the difference between the transmission energy when the relay is fixed at middle point O and that when the relay is moved to the position where the total delay is minimized. The energy per coded bit E_s is $N_o\bar{\gamma}_{SR}$ and the noise PSD N_o is given by

$$N_o = 2KT \tag{5.24}$$

   where K is the Boltzmann constant and T is the absolute temperature.

- **Experiment 1**

Figures 5.2 and 5.3 show the delays τ_1 and τ_2 versus the distances d_1 and d_2, respectively. The parameters used in this experiment are provided in Table 5.1. Optimal values of d_1, d_2, SNR, and WER at which the minimum delay is achieved are listed in Table 5.2.

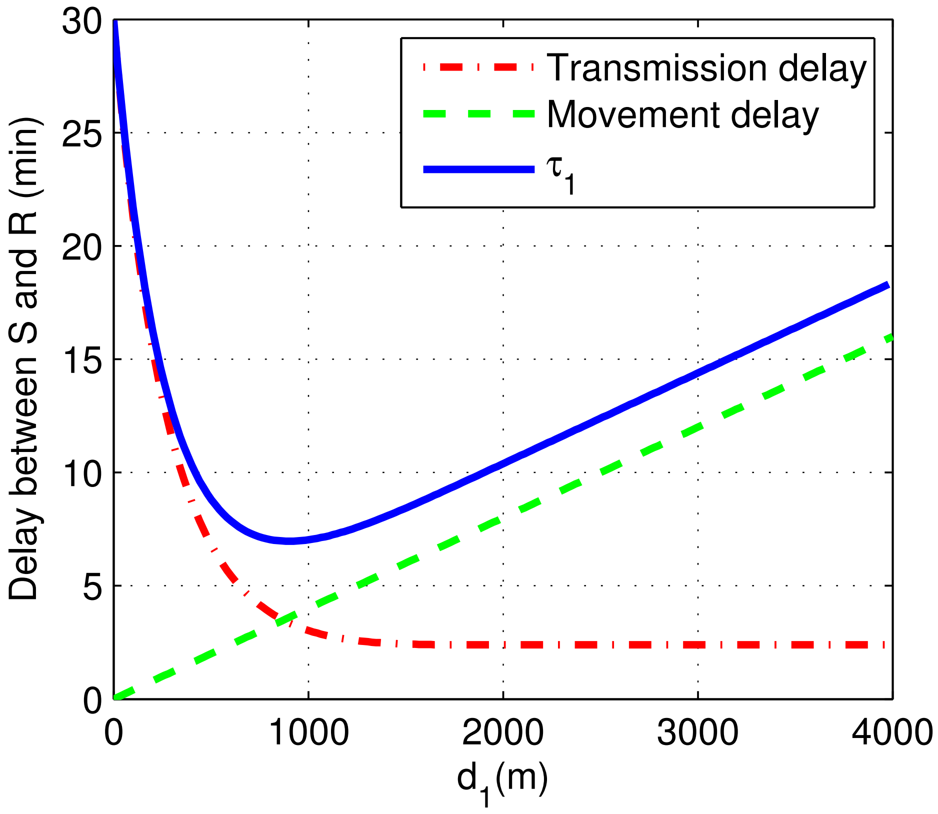


Figure 5.2 Delay versus d_1: parameters are listed in Table 5.1.

- **Experiment 2**

In this experiment, we increase the velocity of the relay to 100 Km/h. Results for this experiment are listed in Table 5.3.

It is notable that increasing the relay velocity increases the optimal values of d_1 and d_2 and consequently the optimal values of SNR which reduce the WER.

In experiment 2, (5.22) and (5.23) yields $d_{1_{opt}} = 1.9$ Km and $d_{2_{opt}} = 2$ Km and the corresponding values of τ_1 and τ_2 are 3.97 min and 2.84 min respectively, and the total delay is 6.81 min. Comparing with those values in Table 5.3 indicates that (5.22) and (5.23) are fairly close. Using parameters of experiment 1, the total delay is 14.35 min which is not that close to the value in Table 5.2 because the optimal SNR is lower.

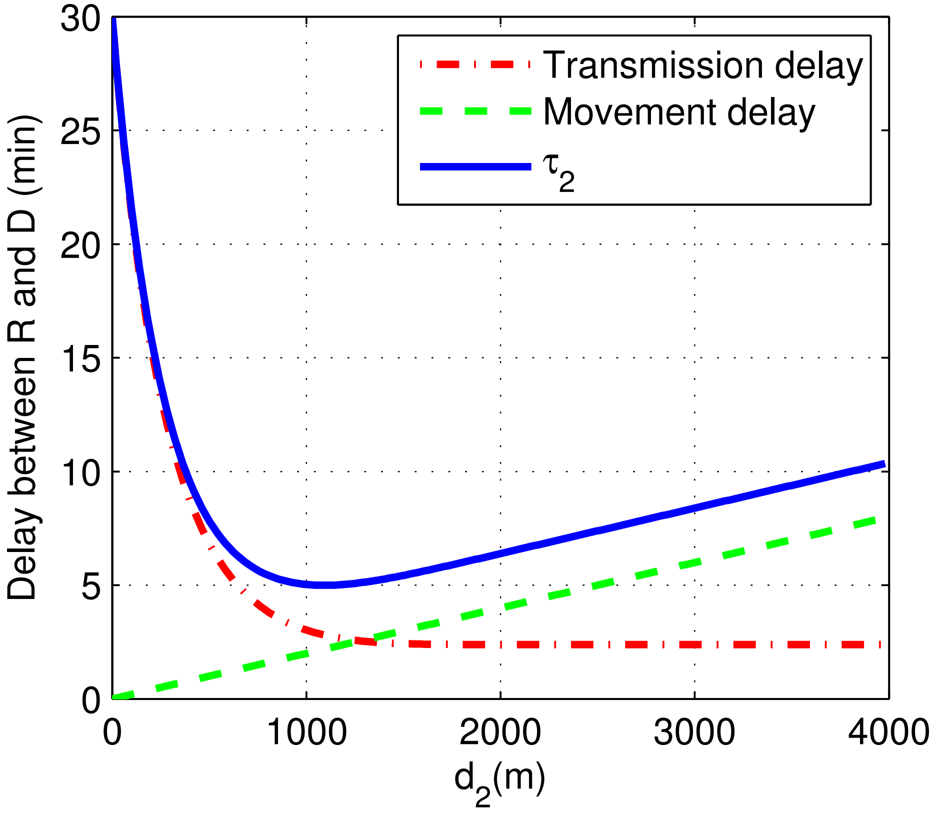


Figure 5.3 Delay versus d_2: parameters are listed in Table 5.1.

5.6 Conclusion

In this study we have investigated the optimal locations of the relay in the " store, carry, and forward" paradigm. Optimal locations are calculated to minimize the total delay. We presented an analytical method for finding the optimal locations of the relay and the total delay. Results show that the analytical method provides an accurate estimate of the total delay and the optimal location of the relay.

Table 5.1 Parameters used in experiment 1

D	v	R	q	n	m	$\bar{\gamma}_{b_i}$
8 Km	30 Km/h	1200 bps	10KB	63	4	-1 dB

Table 5.2 Results of experiment 1

d_1 (m)	d_2 (m)	$\bar{\gamma}_{SR}$ (dB)	$\bar{\gamma}_{RD}$ (dB)	$\tau_{1_{min}}$ (min)	$\tau_{2_{min}}$ (min)	τ_{min} (min)	G_τ (min)	G_E (Joule)
904.52	1085.43	3.45	4.50	6.97	5	11.96	2	0.98

Table 5.3 Results of experiment 2

d_1 (Km)	d_2 (Km)	$\bar{\gamma}_{SR}$ (dB)	$\bar{\gamma}_{RD}$ (dB)	$\tau_{1_{min}}$ (min)	$\tau_{2_{min}}$ (min)	τ_{min} (min)	G_τ (min)	G_E (Joule)
1.69	1.85	8.53	9.78	3.88	2.82	6.70	7.32	1.31

CHAPTER 6. Conclusions and Future Work

6.1 Conclusions

In this research, we investigated four problems related to security, prioritized relaying, message ferrying in wireless relay network. In the first problem, we investigated the tradeoff between tracing bits and parity bits, where the former is to identify the malicious relay nodes and discard (erase) the bits received from them and the latter is to correct the errors caused by channel impairments such as fading and noise. We found that there exists an optimal allocation of redundancy between tracing bits and parity bits that minimizes the probability of decoding error or maximizing the throughput. When the total amount of redundancy (sum of tracing bits and parity bits) is fixed, more redundancy should be allocated to the tracing bits for higher $P(H_1)$ and less on the tracing bits for lower SNR. We analyzed the energy gain (saving) and the throughput gain provided by the optimal redundancy allocation in a multiple access relay network under falsified data injection attack.

In the second problem, we proposed prioritized analog relaying schemes that provide different SINR's to different sources in multiple access relay networks. The proposed prioritized relaying schemes enable the source with a higher priority level to send data with a higher rate and/or a lower error probability while being relayed with other source at the same time in the same bandwidth. We presented prioritized relaying methodologies and derived the required number of relays as a function of the number of antennas per relay and the degree of cooperation among relays. Our simulation results indicate that the proposed relaying methodologies can indeed achieve the prescribed set of prioritization among sources.

In the third problem, we proposed the MAP approach in detecting the misbehaving relay that injects false data or adds channel errors into the network encoder in multi-access relay networks. The proposed scheme does not require sending extra bits at the source, such as hash function or message authentication check bits, hence there is no transmission overhead. In addition, it makes an instantaneous decision about whether a relay node is behaving properly without a long-term observation. The side information regarding the presence of forwarding misbehavior is exploited at the probability of bit error, taking into account the lossy nature of wireless links. We found that the proposed decoder and the MAP decoder with the aid of the MAP detection are effective in mitigating the forwarding misbehaviors in multiple access networks with network coding.

In the fourth problem, we investigated the optimal locations of the relay in the " store, carry, and forward" paradigm. Optimal locations are calculated to minimize the total delay. We presented an analytical method for finding the optimal locations of the relay and the total delay. Results show that the analytical method provides an accurate estimate of the total delay and the optimal location of the relay.

6.2 Future Work

As an extension to the work we have done in this thesis, we are planning to address three problems in the future. In Section 4.5.3, we proposed a method to find $P(z)$ which is required to decode the sources' bits in the case of MAP decoder with $P(z)$. The accuracy of estimating $P(z)$ increases as the averaging window length L increases which results in a more accurate decoding and, accordingly, the decoding error probability will decrease. In the first problem, we will analyze and study the effect of L on the decoding error probability. In the second problem, we need to drive the the union bound on the decoding error probability in the case of M-ary modulation. In The third problem, we will study the effect of probability of false alarm and miss-detection on the decoding error probability. We also need to differnetiate between the effect of $P(f = -1)$ and $P(z = -1)$ on the decoding error probability.

APPENDIX A. Proof of SNR ordering

In this Appendix we show that $\overline{\gamma}_n \geq \overline{\gamma}_m$ if and only if $P_n \geq P_m$. Let $c_1 = E_s q^2 E\left[1/Tr\left(AA^\dagger\right)\right]$ and $c_2 = E\left[\mathbf{w}^\dagger \mathbf{w}\right]$. Then

$$\begin{aligned} \overline{\gamma}_n =& \frac{c_1 P_n}{c_1 \sum_{i=1}^{N} P_i - c_1 P_n + c_2} \\ =& \frac{c_1 P_n}{c_3 - c_1 P_n} \end{aligned} \tag{A.1}$$

where $c_3 = c_1 \sum_{i=1}^{N} P_i + c_2$. If $\overline{\gamma}_n \geq \overline{\gamma}_m$, then

$$\frac{P_n}{c_3 - c_1 P_n} \geq \frac{P_m}{c_3 - c_1 P_m} \tag{A.2}$$

Therefore, $P_n \geq P_m$.

APPENDIX B. Proof of (4.94)

In this Appendix we prove (4.94). (4.92) can be written as

$$P(c_0 \to c_4|\mathbf{h}) = \frac{1}{2}\text{erf}\left(\sqrt{X} + \frac{b}{\sqrt{X}}\right) \tag{B.1}$$

where $X = h_3^2\gamma$, $b = 0.25\log\left(P(z=+1)/P(z=-1)\right)$, and erf is the error function which is defined as

$$\text{erf}\left(\sqrt{X} + \frac{b}{\sqrt{X}}\right) = \frac{2}{\sqrt{\pi}}\int_0^{\sqrt{X}+\frac{b}{\sqrt{X}}} e^{-t^2}dt \tag{B.2}$$

The probability distribution function of X is given by

$$f_X(x) = \frac{1}{\gamma}e^{-x/\gamma} \tag{B.3}$$

Averaging (B.1) over the distribution of x yields

$$P_1 = \frac{1}{2\gamma}\int_0^\infty \text{erf}\left(\sqrt{x} + \frac{b}{\sqrt{x}}\right) e^{-x/\gamma}dx \tag{B.4}$$

In what follows, we use the following formulas

$$\text{erfc}\left(\sqrt{x} + \frac{b}{\sqrt{x}}\right) = \frac{2}{\sqrt{\pi}}\int_{\sqrt{x}+\frac{b}{\sqrt{x}}}^\infty e^{-t^2}dt \tag{B.5}$$

$$\frac{d}{dx}\text{erfc}\left(\sqrt{x} + \frac{b}{\sqrt{x}}\right) = \frac{-1}{\sqrt{\pi x}}\left(1 - \frac{b}{x}\right)e^{-\frac{(x+c)^2}{x}} \tag{B.6}$$

$$\frac{d}{dx}\text{erfc}\left(\sqrt{x} + \frac{b}{\sqrt{x}}\right) = \frac{1}{\sqrt{\pi x}}\left(1 - \frac{b}{x}\right)e^{-\frac{(x+c)^2}{x}} \tag{B.7}$$

Integrating (B.4) using integration by parts yields

$$\begin{aligned} P_1 =& \frac{1}{2\gamma}\left[-\gamma\text{erfc}\left(\sqrt{x} + \frac{b}{\sqrt{x}}\right)e^{-x/\gamma}\right. \\ & \left. -\frac{\gamma}{\sqrt{\pi}}\int \frac{1}{\sqrt{x}}\left(1 - \frac{b}{x}\right)e^{-x/\gamma-(x+b)^2/x}dx\right]_0^\infty \\ =& \frac{-1}{2\sqrt{\pi}}\int_0^\infty \frac{1}{\sqrt{x}}\left(1 - \frac{b}{x}\right)e^{-x/\gamma-(x+b)^2/x}dx \end{aligned} \tag{B.8}$$

After some mathematical manipulations, (B.8) can be written as

$$P_1 = \frac{-e^{-r}}{2\sqrt{\pi}} \int_0^{\infty} \frac{1}{\sqrt{u}} \left(\sqrt{\frac{\gamma}{1+\gamma}} - \frac{d}{u} \right) e^{-\frac{(u+d)^2}{u}} du \tag{B.9}$$

where $r = 2b(1 - \sqrt{1 + 1/\gamma})$, $d = b\sqrt{1 + 1/\gamma}$, and $u = x(1 + 1/\gamma)$. We can write (B.9) as follows

$$\begin{aligned} P_1 =& \frac{-e^{-r}}{2\sqrt{\pi}} \int_0^{\infty} \frac{1}{\sqrt{u}} \left(-1 + \sqrt{\frac{\gamma}{1+\gamma}} + 1 - \frac{d}{u} \right) e^{-\frac{(u+d)^2}{u}} du \\ =& \frac{-e^{-r}}{2\sqrt{\pi}} \int_0^{\infty} \frac{1}{\sqrt{u}} \left(1 - \frac{d}{u} \right) e^{-\frac{(u+d)^2}{u}} du \\ &+ \left(1 - \sqrt{\frac{\gamma}{1+\gamma}} \right) \frac{e^{-r}}{2\sqrt{\pi}} \int_0^{\infty} \frac{1}{\sqrt{u}} e^{-\frac{(u+d)^2}{u}} du \\ =& \frac{-e^{-r}}{2} \left[\operatorname{erf} \left(\sqrt{u} + \frac{d}{\sqrt{u}} \right) \right]_0^{\infty} \\ &+ \left(1 - \sqrt{\frac{\gamma}{1+\gamma}} \right) \frac{e^{-r}}{2\sqrt{\pi}} \int_0^{\infty} \frac{1}{\sqrt{u}} e^{-\frac{(u+d)^2}{u}} du \\ =& \left(1 - \sqrt{\frac{\gamma}{1+\gamma}} \right) \frac{e^{-r}}{2\sqrt{\pi}} \int_0^{\infty} \frac{1}{\sqrt{u}} e^{-\frac{(u+d)^2}{u}} du \end{aligned} \tag{B.10}$$

By changing variables, let $y = \sqrt{u}$ and $dy = dy/(2\sqrt{u})$. After substitution in (B.10) we have

$$\begin{aligned} P_1 &= \left(1 - \sqrt{\frac{\gamma}{1+\gamma}} \right) \frac{e^{-r}}{\sqrt{\pi}} \int_0^{\infty} e^{-\left(\frac{y+d}{y}\right)^2} dy \\ &= \left(1 - \sqrt{\frac{\gamma}{1+\gamma}} \right) \frac{e^{-(2d+r)}}{\sqrt{\pi}} \int_0^{\infty} e^{-\left(-y^2 - \frac{d^2}{y^2}\right)} dy \end{aligned} \tag{B.11}$$

Using integration tables to find the integral in (B.11) yields

$$P_1 = \frac{1}{2} \left(1 - \sqrt{\frac{\gamma}{1+\gamma}} \right) e^{-4d-r} \tag{B.12}$$

After substituting for the d and r, we have

$$P_1 = \frac{1}{2} \left[1 - \sqrt{\frac{\gamma}{1+\gamma}} \right] \left(\frac{P(z=-1)}{P(z=+1)} \right)^{\frac{1}{2}(1+\sqrt{1+\frac{1}{\gamma}})} \tag{B.13}$$

BIBLIOGRAPHY

[1] B. Kannhavong *et al.*, “A survey of routing attacks in mobile ad hoc networks,” *IEEE Wireless Communications,* vol. 14, no. 5, pp. 85–91, Oct. 2007.

[2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Weung, “Network information flow,” *IEEE Trans. on Information Theory*, vol. 46, no. 4, pp. 1204-1216, July 2000

[3] P. Razaghi,Wei Yu, “Parity Forwarding For Multiple-Relay Networks,” *IEEE International Symposium on Information Theory*, pp. 1678–1682, July 2006.

[4] W. Pu, C. Luo, S. Li, C. W. Chen, “Continuous Network Coding in Wireless Relay Networks,” *IEEE Infocom*, pp. 2198–2206, April 2008.

[5] J. N. Laneman, D.N.C.Tse, G. Wornell, “Cooperative diversity in wireless networks: Efficient protocols and outage behavior,” *IEEE Transactions on Information Theory*, pp. 3062–3080, Dec. 2004.

[6] A. Sendonaris, E. Erkip, B.Azhang, “User cooperation diversity Part I: System description,” *IEEE Transactions on Communications*, pp. 1927–1938, Nov. 2003.

[7] A. Scaglione, D. L. Goeckel, J. N. Laneman, “Cooperative communications in mobile ad hoc networks,” *IEEE Signal Processing Magazine*, vol. 23, no. 5, pp. 18–29, Sept. 2006.

[8] A. Nosratinia, et al., “Cooperative communication in wireless networks,” *IEEE Communications Magazine*, pp. 74–80, Oct. 2004.

[9] S. W. Kim, “Cooperative spatial multiplexing in mobile ad hoc networks,” *Proc. of IEEE International Conference on Mobile Ad hoc and Sensor Systems Conference (MASS,)* 2005.

[10] Y. Zhang, G. Wang, M. G. Amin, “Cooperative spatial multiplexing in multi-hop wireless networks,” *Proc. of IEEE ICASSP06*, pp. IV821–IV824, May 2006.

[11] Z. Ding, T. Ratnarajah, C. C. F. Cowan, “On the diversity-multiplexing tradeoff for wireless cooperative multiple access systems,” *IEEE Transactions on Signal Processing*, vol. 55, no. 9, pp. 4627–4638, Sept. 2007.

[12] A. Host-Madsen and A. Nosratinia, “The multiplexing gain of wireless networks,” *Proc. of IEEE International Symposium on Information Theory*, 2005.

[13] T. M. Cover, A. A. El Gamal, “Capacity theorems for the relay channel”, *IEEE Transactions on Information Theory*, vol. IT-25, No 5, pp 572-584, Sept. 1979.

[14] A.D. Wyner, “The rate-distortion function for source coding with side information at the decoder II: General Sources”, *Information and Control*, Vol 38, pp 60-80, 1978.

[15] R. U. Nabar, Ö. Oyman, H. Bölcskei, A. J. Paulraj, “Capacity scaling laws in MIMO wireless networks,” *Proc. of Allerton Conf. on Commun. Control and Comp.*, Monticello, USA, Oct. 2003.

[16] A. Wittneben, “A theoretical analysis of multiuser zero forcing relaying with noisy channel state information,” *in Proc. IEEE VTC* , May 2005.

[17] C. Esli, S. Berger, A. Wittneben, “Optimizing Zero-Forcing Based Gain Allocation for Wireless Multiuser Networks,” *Proc. IEEE ICC*, Glasgow, Scotland, June 2007.

[18] R. Louie, Y. Li, B. Vucetic , “Zero Forcing Processing in Two Hop Networks with Multiple Source, Relay and Destination Nodes,” *Proc. IEEE ICC*, Dresden, Germany, June 2009.

[19] D. H. N. Nguyen, H. H. Nguyen, H. D. Tuan, “Distributed Beamforming in Relay-Assisted Multiuser Communications,” *in Proc. IEEE ICC*, Dresden, Germany, June 2009.

[20] S. Berger, A. Wittneben, “Cooperative distributed multiuser MMSE relaying in wireless ad-hoc networks,” *in Proc. IEEE Signals, Systems and Computers conf.*, November 2005.

[21] R. Krishna, Z. Xiong, S. Lambotharan, “A cooperative MMSE relay strategy for wireless sensor networks,” *IEEE Signal Process. Letters*, vol. 15, pp. 549–552, 2008.

[22] N. Khajehnouri, A. H. Sayed, “Distributed MMSE relay strategies for wireless sensor networks,” *IEEE Trans. Signal Process.*, vol. 55, pp. 3336–3348, July 2007.

[23] H. Bölcskei, R. U. Nabar, Ö. Oyman, A. J. Paulraj, “Capacity scaling laws in MIMO wireless networks,” *IEEE Trans. on Wireless Comm.*, vol.5, no.6, pp.1433–1444, June 2006.

[24] H. Shi, T. Abe, T. Asai, H. Yoshino, “Relaying schemes using matrix triangularization for MIMO wireless networks,” *IEEE Trans. Commun.*, vol. 55, no. 9, pp. 1683–1688, Sep. 2007.

[25] Y. Jing, H. Jafarkhani, “Network beamforming using relays with perfect channel information,” *in Proc. IEEE ICASSP*, April 2007.

[26] T. Ho, R. Koetter, M. Medard, D. Karger, and M. Effros, “The Benefits of Coding Over Routing in a Randomized Setting,” *in Proc. of International Symposium on Information Theory (ISIT)*, 2003.

[27] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, “XORs in The Air: Practical Wireless Network Coding,” *in Proc. of ACM SIGCOMM*, 2006.

[28] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, “Trading Structure for Randomness in Wireless Opportunistic Routing,” *in Proc. of ACM SIGCOMM*, 2007.

[29] S. Zhang, S. Liew, and P. Lam, “Physical layer network coding,” *ACM Mobicom2006*, 2006.

[30] S. Katti, S Gollakota, D. Katabi, “Embracing Wireless Interference: Analog Network Coding,” *ACM SIGCOMM*, 2007.

[31] Y. Chen, S. Kishore, J. Li, “Wireless diversity through network coding,” *IEEE Wireless communications and networking conference (WCNC)*, April 2006.

[32] W. Yu and K. J. R. Liu, “Attack-resistant cooperation stimulation in autonomous ad hoc networks,” *IEEE J. Selected Areas Commun.*, vol. 23, no. 12, pp. 22602271, Dec. 2005.

[33] S. Zhong, J. Chen, and Y. R. Yang, “Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks,” *in Proc. IEEE INFOCOM*, San Francisco, CA, Mar. 2003, pp. 19871997.

[34] P. Michiardi and R. Molva, “Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” *in Proc. IFIP Commun. Multimedia Security Conf.*, Portoroz, Slovenia, Sep. 2002, pp. 107121.

[35] X. Bao, J. Li, “Matching code-on-graph with networks-on-graph: adaptive network coding for wireless relay networks,” *Proc. Allerton Conf. on Commun., Control and Computing*, Urbana Champaign, IL, Sept. 2005.

[36] C. Hausl, P. Dupraz, “Joint network-channel coding for the multiple-access relay channel,” *3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks (SECON)*, pp. 817–822, Sept. 2006.

[37] S. W. Kim and S. G. Kim, B.K.Yi, “Decentralized random parity forwarding in multi-source wireless relay networks,” *Proc. of IEEE Globecom*, 2007.

[38] F. Zhao, T. Kalkert, M. Medard, K. J. Han, “Signatures for content distribution with network coding,” *Proc. of IEEE International Symposium on Information Theory*, Nice, France, June 2007.

[39] T. Ho, B. Leong, R Koetter, M. Medard, M. Effros, D. R. Karger, “Byzantine modification detection in multicast networks with random network coding,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2798–2803, June 2008.

[40] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, M. Effros, “Resilient network coding in the presence of byzantine adversaries,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2596–2603, June 2008.

[41] Y. Mao, M. Wu, "Tracing malicious relays in cooperative wireless communications," *IEEE Transaction on Information Forensics and Security,* vol. 2, no. 2, pp. 198–212, June 2007.

[42] S. Dehnie, H. T. Sencar, N. Memon, "Detecting malicious behavior in cooperative diversity," *Proc. of Conference on Information Sciences and Systems CISS*, 2007.

[43] Shu Lin, Daniel J. Costello, *Error Control Coding*, 2nd edition, Prentice Hall, 2004. Cambridge University Press , 2005.

[44] Andrea Goldsmith, *Wireless communications*, Cambridge University Press , 2005.

[45] F. Ye, H. Luo, S. Lu, L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE Journal on Selected Areas in Communications*, vol.23, no.4, pp. 839–850, April 2005.

[46] S. Kim, A. L. N. Reddy, "Real-time detection and containment of network attacks using QoS regulation," *Proc. of IEEE International Conference on Communications ICC05*, pp. 311–315 , May 2005.

[47] B. Kaliski, "The MD2 message-digest algorithm", RFC 1319, RSA, Laboratories, April 1992.

[48] R. Rivest, "The MD5 message-digest algorithm", RFC 1321, MIT, Laboratory for Computer Science and RSA Data Security, Inc., April 1992.

[49] A. H. Lashkari, M. M. S. Danesh, B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," *Proc. of 2nd IEEE International Conference on Computer Science and Information Technology ICCSIT 2009*, pp.48–52, Aug. 2009.

[50] IEEE Standard for Information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput

[51] B. Masnick and J. Wolf, “On linear unequal error protection codes,” *IEEE Trans. Inf. Theory*, vol. IT-13, no. 3, pp. 600–607, Oct. 1967.

[52] G. Yang, D. Shen, V. O. K. Li, “Unequal error protection for MIMO systems with a hybrid structure,” *in proc. IEEE Int. Symp. on Circuits and Systems ISCAS*, Island of Kos, Greece, May 2006.

[53] Y. Lin, B. Li, B Liang, “Differentiated Data Persistence with Priority Random Linear Codes,” *in Proc. IEEE Int. Conf. on Distributed Computing Sys. ICDCS*, Ontario, Canada, June 2007.

[54] Sang Wu Kim, “Mitigation of forwarding misbehaviors in multiple access networks with network coding,” *Proc. IEEE Globecom Conference* Dec. 2010

[55] Sang Wu Kim,”Integrity of network coded information in adversarial multiple access relay networks”, *Proc. of International Symposium on Network Coding Netcod*, 2011.

[56] G. Kramer and A. J. van Wijngaarden, “On the white Gaussian multipleaccess relay channel,” in *Proc. 2000 IEEE Int. Symp. Inform. Theory*, pp.40, Jun. 2000.

[57] L. Sankaranarayanan, G. Kramer, and N. B. Mandayam, “Capacity theorems for the multiple-access relay channel,” in *Proc. of Allerton Conference on Communication, Control, and Computing*, Oct. 2004.

[58] K. Azarian, H. E. Gamal, and P. Schniter, “On the optimality of the ARQDDF protocol”, *IEEE Trans. Inform. Theory*, pp. 1718 - 1724, Apr. 2006.

[59] D. Chen and J.N.Laneman, “The diversity-multiplexing tradeoff for multipleaccess relay channel,” in *Proc. of Conf. on Information Sciences and Systems (CISS)*, Mar. 2006.

[60] M. Yuksel and E. Erkip. “Multi-antenna cooperative wireless systems: A diversity multiplexing tradeoff perspective,” *IEEE Trans. Inform. Theory*, pp. 3371 - 3393, Oct. 2007.

[61] N. Prasad and X. Wang, “Outage minimization and fair rate allocation for the multiple access relay channel,” in *Proc. of IEEE ISIT*, pp. 1333 - 1337, 2008.

[62] Y. Chen, S. Kishore, and J. Li, "Wireless diversity through network coding," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, May 2006.

[63] X. Bao and J. Li, "Matching code-on-graph with network-on-graph: adaptive network coding for wireless relay networks," in *Proc. of Allerton Conference on Communication, Control, and Computing*, Sept. 2005.

[64] F. Zhao, T. Kalkert, M. Medard, K. J. Han, "Signatures for content distribution with network coding," *Proc. of IEEE International Symposium on Information Theory*, Nice, France, June 2007.

[65] T. Ho, B. Leong, R Koetter, M. Medard, M. Effros, D. R. Karger, "Byzantine modification detection in multicast networks with random network coding", *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 27982803, June 2008.

[66] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, M. Effros, "Resilient network coding in the presence of byzantine adversaries", *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 25962603, June 2008.

[67] Y. Mao, M. Wu, "Tracing malicious relays in cooperative wireless communications," *IEEE Transaction on Information Forensics and Security*, vol. 2, no. 2, pp. 198212, June 2007.

[68] T.Khalaf and S.W.Kim, "Error analysis in multi-source, multi-relay, multi-destination networks under falsified data injection attacks," in *Proc. of IEEE MILCOM*, San Diego, 2008.

[69] M. Kim, M. Medard, J. Barros, and R. Kotter, "An algebraic watchdog for wireless network coding," *Proc. of IEEE International Symposium on Information Theory*, June 2009.

[70] J. Hagenauer, E. Offer, and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 429 445, 1996.

[71] S. W. Kim and E. Y. Kim, "Optimum receive antenna selection minimizing error probability," *in Proc. IEEE Wireless Communications and Networking Conference*, vol. 1, pp. 441 447, Mar. 2003.

[72] P. Hoeher, L. Ingmar, and U. Sorger , Log-likelihood values and Monte Carlo simulation Some fundamental results, In 2nd International Symposium on Turbo Codes and Related Topics, pp. 4346, 2000.

[73] I.S.Gradshteyn and I.M.Ryzhik, Tables of Integrals, Series, and Products, pp.341, Eq. 3.472, Academic Press, 1980.

[74] S. Ci, M. Guizani,H. Chen, and H. Sharif, "Self-Regulating Network Utilization in Mobile Ad Hoc Wireless Networks," *IEEE Trans. on Vehic. Tech.,* vol. 55, no. 4, pp. 1302–1310, July 2006.

[75] B. Kannhavong *et al.*, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Communications,* vol. 14, no. 5, pp. 85–91, Oct. 2007.

[76] S. Gwalani, E. Belding-Royer, C. Perkins, "AODV-PA: AODV with path accumulation," in *Proc. IEEE International Conference on Communications*, May 2003, vol. 1, pp. 527–531.

[77] T. Clausen *et al.*, "Optimized Link State Routing Protocol", in *Proc. IEEE INMIC*, Pakistan, 2001.

[78] J. Davis, A. Fagg, B. Levine, "Wearable computers as packet transport mechanisms in highly-partitioned ad-hoc networks," in *Proc. Wearable Computers*, Oct. 2001, pp. 141–148.

[79] Wenrui Zhao, Mostafa Ammar, "Message Ferrying: Proactive Routing in Highly-Partitioned Wireless Ad Hoc Networks," in *Proc. IEEE Workshop on Futrure Trends in Distributed Computing Systems*, Puerto Rico, May 2003.

[80] Y. Chen; J. Yang; W. Zhao; M. Ammar, E. Zegura, “Multicasting in sparse MANETs using message ferrying,”in *Proc. IEEE WCNC06*, 2006, vol. 2, pp. 691–696.

[81] Z. Ding and Y. Li, *Blind Equalization and Identification*, Marcel Dekker, Inc., 2001.

[82] O. Shalvi and E. Weinstein, “New criteria for blind deconvolution of non-minimum phase systems (channels),” *IEEE Trans. Inform. Theory*, vol. 36, pp. 312–321, Mar. 1990.

[83] K. Abed-Meraim, W. Qiu, and Y. Hua, “Blind system identification,” *Proc. IEEE*, vol. 85, no. 8, pp. 13101322, Aug 1997.

[84] K. Abed-Meraim and E. Moulines, “A maximum likelihood solution to blind identification of multichannel FIR filters,” *in Proc. EUSIPCO*, Edinburgh, Scotland, vol. 2, 1994, pp. 10111014.

[85] D. Starer and A. Nehorai, “Passive localization of near-field sources by path following,” *IEEE Trans Signal Processing*, vol. 42, pp. 677680, Mar. 1994.