RATE ADAPTIVE CODING AND ITS APPLICATION TO SPREAD SPECTRUM COMMUNICATIONS

by

Amir Masoud Yousef Bigloo

B.Eng., Tehran University, Tehran, Iran, 1988

A Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF APPLIED SCIENCE

in the Department of Electrical Engineering

We accept this thesis as conforming
to the required standard

[redacted]

Dr. Q. Wang, Supervisor, Dept. of Elect. & Comp. Eng.

[redacted]

Dr. V. K. Bhargava, Departmental Member, Dept. of Elect. & Comp. Eng.

[redacted]

Dr. Z. Dong, Outside Member, Dept. of Mech. Eng.

[redacted]

Dr. G. Shoja, External Examiner, Dept. of Computer Science

Supervisor: Dr. Qiang Wang.

Abstract

In this work, rate-adaptive coding (RAC) and its application to spread spectrum are investigated. Two RAC schemes are introduced and their performances are analyzed. The first one is based on punctured maximum distance separable (MDS) codes. For this scheme, the throughput and codeword error probability verses the code symbol error probability are derived. The performance of this protocol is also analyzed in a Rayleigh fading environment, with the maximum number of transmissions for each codeword limited.

The second scheme is based on the concatenation of punctured MDS codes, and convolutional codes. This concatenation benefits from the advantages of both block and convolutional codes. The throughput and codeword error probability in a Rayleigh fading environment with a limited number of transmissions for each codeword are derived.

Since spread spectrum multiple access (SSMA) is a self-interference limited system, any reduction in the interference converts directly into an increase in capacity, in terms of the number of simultaneous users [1]. The interference from each user is reduced by applying RAC to SSMA, thereby superseding the conventional fixed-rate system. Specifically, the RAC scheme based on MDS codes is applied to the

frequency hopped spread spectrum multiple access (FH/SSMA) and a remarkable increase in the capacity of the system is shown.

Examiners:

[redacted]

Dr. Q. Wa[redacted] & Comp. Eng.

[redacted]

Dr. V. K. Bhargava, Departmental Member, Dept. of Elect. & Comp. Eng.

[redacted]

Dr. Z. Dong, Outside Member, Dept. of Mech. Eng.

[redacted]

Dr. G. Shoja, External Examiner, Dept. of Computer Science

Contents

List of Figures

List of Tables

Acknowledgements

I wish to acknowledge the encouragement, suggestions, criticisms and financial support in the form of a research assistantship, provided by my supervisor Dr. Qiang Wang. I am indebted to Dr. Vijay K. Bhargava for his comments and guidance during my Master's studies. To the many teachers, computing personnel and secretarial staff who offered support and help, I express my gratitude. Finally I wish to thank Mr. D. Peterson and Miss C. Glover for providing editorial guidance.

To my father.

Chapter 1

Introduction

1.1 Introduction

The design of an error correction coding system usually consists of selecting a fixed-rate code with a certain rate and correction capability, adapted to the average or worst channel condition to be expected. If the channel is time varying or has insufficiently known parameters, one would like to be more flexible. Consequently, a rate-adaptive channel coding is required.

If a feedback channel is available, rate-adaptive coding can be accomplished in the form of type-I or type-II hybrid ARQ [2]. In a type-I hybrid ARQ scheme, an inner code for error correction and an outer code for error detection are used, or simply a single code is designed for simultaneous error correction and detection. When a received word is detected in error, the receiver first attempts to correct the error. If the number of errors is within the designed error-correcting capability of the code, the errors will be corrected and the decoded message will be delivered to the user. If an uncorrectable error pattern is detected, the receiver rejects the received word and requests a retransmission. The retransmission is the same codeword. This continues until the codeword is either successfully received or successfully decoded. In a type-II hybrid ARQ scheme, in the first transmission, information bits plus some parity check bits for error detection are transmitted. If this packet is detected in error, the packet is saved and a second transmission is requested. The second transmitted packet is a block of parity check bits which is formed based on the original message and an error correcting code. When the second packet is received, it is combined with the first packet to form a codeword for error correction.

1.2 Review of Literature

As we mentioned before, whenever a return channel is available, the code rate can be adapted, according to the channel condition. Mandelbaum [3] was the first to propose punctured codes for transmitting redundancy in incremental steps by using RS codes. Transmitting more redundancy lowers the code rate according to channel needs.

The first type-II hybrid ARQ, using a parity-retransmission strategy, was proposed by Metzner [4] [5]. He proposed two approaches. In the first approach he considered a long (n, k) block code, where the n-digit block is divided into smaller sub-blocks. These smaller sub-blocks are used as the data digits of a short, $1/2$ rate code. The second approach is to treat the first transmission as the data digits of a systematic convolutional code. Metzner's scheme was later extended and modified by many others [6]-[9], among them Lin-Yu's type-II hybrid ARQ scheme [6].

Lin-Yu's type-II hybrid ARQ scheme uses two codes. One is a high rate (n, k) code C_0, which is designed for error detection only, and the other is a 1/2 rate invertible $(2k, k)$ code C_1, which is designed for simultaneous error correction and error detection.

Chase [10] has suggested a maximum likelihood approach, known as code combining, for combining an arbitrary number of noisy packets. Specifically, he applied code combining to a type-II hybrid ARQ, by using convolutional codes. Hagenauer [11] and Kallel [12] [13] have also used convolutional codes in type-II hybrid ARQ schemes.

1.3 Why Rate-Adaptive Coding

When communication resources, such as spectrum or power, are in demand, adaptability plays a very important role in designing a system. An example of a system which demands spectral efficiency is personal communications services (PCS), where freedom for the user should be provided in terms of time and place. If communications is to become universal, the spectrum should be employed in the most efficient way. An example of a system where power efficiency is a crucial factor in system design, is satellite communications. Here the cost of a satellite is directly related to its mass, and the mass of a satellite is directly related to the power efficiency of the system.

Consider the communication system shown in Figure (1.1). If more than one user is supposed to communicate, in terms of modulation scheme, there are two ways to design the system. In the first strategy, when a user transmits signals through a

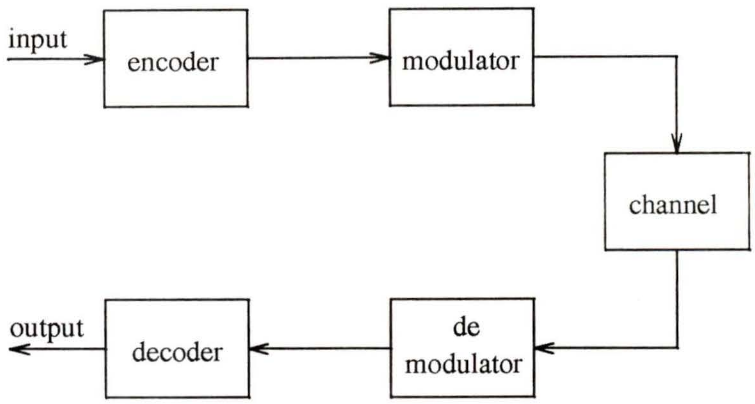

Figure 1.1: Block diagram of a typical digital communication system.

channel, no other user employs that channel at the same time. This can be done in the form of time division multiple access (TDMA) or frequency division multiple access (FDMA). In TDMA, each user employs the channel for a given period of time. This means the channel is shared on a time basis. In FDMA, the whole channel is divided into a number of sub-channels and each sub-channel is given to one user.

The second strategy for designing a multiuser communication system is based on sharing the whole spectrum at the same time among all the users, which is called spread spectrum multiple access (SSMA). In a spread spectrum modulation scheme, the transmission band width is much greater than the minimum band width required to transmit digital information. By using SSMA, the data band width of each user is expanded to the transmission band width and a code sequence is assigned to each user. At the receiver, this code sequence is used to extract the desired user's signal from the other users' signals. In this system, each user acts as an interferer to the others.

Consider a non-stationary communication channel. For various reasons, sometimes the channel is in a good state and sometimes the channel is in a bad condition. Whenever the channel is in a good state, there is no need for the transmitter and the receiver to put an extra effort to communicate (a higher code rate can be used). On the other hand, if the channel is in a bad state, by lowering the code rate, communications can be established with a tolerable error rate. This can be interpreted as the Shannon's coding theory, which states *by the proper choice of the code rate the error free communications is possible* [14].

Consider the communication system given in Figure (1.1). As shown in Chapter 3, employing rate-adaptive coding results in a higher throughput, compared to a similar fixed-rate code. Therefore, by using rate-adaptive coding, there is a reduction in the transmission power required for a given error performance. This is beneficial, where power is a crucial factor for the system, such as in satellite communications.

1.4 Spread Spectrum Employing Rate-Adaptive Coding.

Consider a multiple access communication system, where each user has its fixed share of band width (TDMA or FDMA). Suppose, due to a good channel condition, a user is able to communicate with less band width. Since, in this case, each user employs its channel exclusively, the system can not benefit from the spectrum that a user saves. Also, in a bad channel condition, it is not possible to devote more band width to a user for communications.

On the other hand, in a SSMA system, by establishing communications, each user contaminates the channel by pouring the signal into the channel. In this case, a reduction in the amount of interference from each user helps to increase the number of users that can utilize the channel simultaneously. In other words, since all users share the spectrum at the same time, the saving a user makes is beneficial to the others.

Consider the communication system shown in Figure (1.1), where SSMA is used as the modulation scheme. Assume a fixed band width for the channel. This means that the symbol transmission rate in the channel is constant. When the channel is in a good condition, the code rate can be increased. By increasing the code rate, the amount of time that a user utilizes the channel, for a given information rate, is decreased. As stated before, this means an increase in the number of simultaneous users that can utilize the channel.

1.5 Organization of Thesis

The organization of this thesis is as follows. In Chapter 2, a rate-adaptive coding scheme which is robust for non-stationary channels is introduced. The performance of this scheme is analyzed and the throughput and undetected error probability are derived.

In Chapter 3, the scheme introduced in Chapter 2, is applied to the frequency hopped spread spectrum multiple access. Rate-adaptive coding with a limited number of transmissions is compared to the fixed rate coding and is shown that the number of simultaneous users for a given band width is increased remarkably.

Chapter 4 considers the rate-adaptive coding, introduced in Chapter 2, in a Rayleigh fading environment. The effect of side information and error/erasure decoding for a fading channel is also considered and is shown that side information, regarding the channel amplitude, can improve the performance of the system.

In Chapter 5, a rate-adaptive coding using the concatenation of an RS code as the outer code, and a systematic convolutional code as the inner code is introduced. The outer code is based on the protocol introduced in Chapter 2.

Chapter 2

A New Rate-Adaptive Coding Scheme Using Maximum Distance Separable Codes

2.1 Introduction

According to Shannon's theory, with the correct choice of data rate transmission, error-free communications is possible. Therefore, the problem of reliable communications reduces to the problem of choosing the proper code rate. In other words, if channel parameters, such as bit error rate and symbol error rate, are constant, with a properly selected forward error correction (FEC) code, reliable communications is possible. Even if the channel parameters vary over a small range, a pure FEC strategy remains the most efficient way to communicate. Unfortunately, in most practical situations the range of channel variations is not small. For instance, sometimes no noise is present in the channel and sometimes the channel is in a deep fading. To ensure reliable communications with FEC alone, the efficiency of the system must be sacrificed. The greater the variation of the channel parameters, the greater the sacrifice in efficiency. Adaptive coding increases the system reliability without sacrificing efficiency.

In this chapter we introduce a new [1] rate-adaptive coding and analyze its performance.

2.2 Adaptability in Coding

Adaptability in coding can be employed in two ways; statistically and instantaneously. In an ARQ scheme, the number of retransmissions generated during a given period of time (channel statistics) indicates the average channel noise level during that period. Therefore, if changes in the channel conditions are slow, the statistical adaptability is useful to combat the channel variations [16].

In instantaneous adaptability, at each instant the channel is treated independently and the code rate is changed for each codeword (based on the channel condition during the time that the codeword is transmitted). Instantaneous adaptability is advantageous when the channel is unpredictable and rapidly varying. In particular, it can be useful for personal communications services (PCS) where the freedom of the user is of major concern.

In PCS, a user's freedom is measured in terms of time and place. In the sense of time, the user should be able to communicate at any occasion, regardless of the number of users who are utilizing the network simultaneously. Considering interference from the other users as the major part of noise in the channel, freedom in place means that the user should be able to communicate from anywhere, regardless of the level of the signal to the interference ratio. This can be interpreted as the near-far or shadowing problem.

---

[1] After we finished this work, we discovered that Stephen Wicker had submitted a similar work to Milcom'91 [15], as well as to the *IEEE Transactions on Communications*

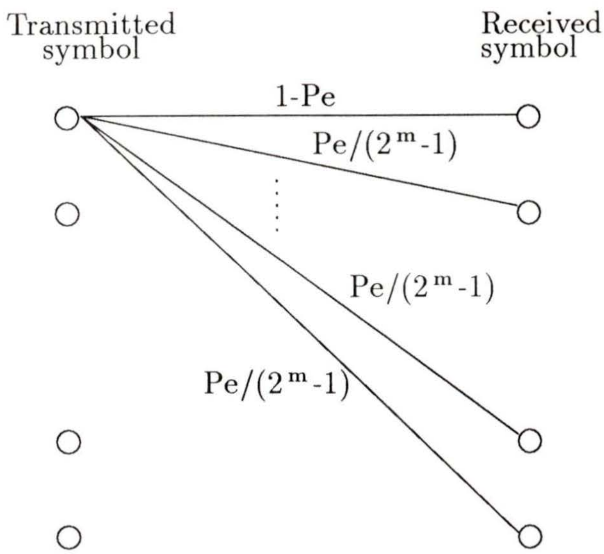

Figure 2.1: M-ary symmetric channel.

To guarantee user freedom without sacrificing efficiency, instantaneous rate-adaptive coding can be employed. The rate-adaptive coding introduced in this section is an instantaneous one, which makes the system more efficient and robust relative to the unpredictable changes in channel conditions.

2.3 Preliminaries, System Models and Assumptions

We model the channel between the encoder and the decoder as an M-ary symmetric channel, as shown in Figure (2.1). By definition, an M-ary symmetric channel causes independent symbol errors with probability p_e [17]. Therefore, a correct symbol is received with probability $1 - p_e$ and each of the $M - 1$ incorrect symbols is received with probability $p_e/(M-1)$.

A decoder for a t error-correcting block code can correct all error patterns of

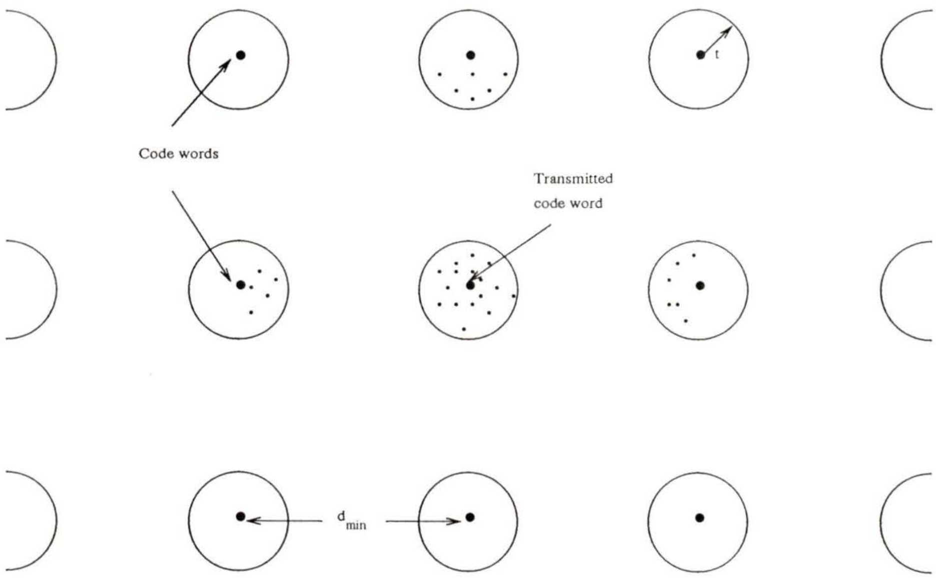

Figure 2.2: Decoding regions.

weight t or less and there will be at least one pattern of $t+1$ errors that can not be corrected properly. In most t error-correcting codes, there will be many error patterns of weight larger than t that could be corrected in principle but except for simple codes, this is rarely done in practice. A decoder that decodes only up to a fixed number of errors, say t errors, is called a bounded-distance decoder (BDD). The second type of decoder is a maximum likelihood decoder (MLD), where the decoder chooses the closest codeword to the received word, in terms of Hamming distance, as the transmitted codeword.

Figure (2.2) symbolically portrays the relationship between the codewords [17]. In a BDD, each codeword has a sphere of radius t drawn around it. This sphere encompasses all of the received words that will be decoded into that codeword. Between the decoding spheres lie many other received words that do not lie within distance t of any codeword and so are not decoded. When more than t errors occur, the received word will usually lie between the decoding spheres and then the decoder can declare that it has an uncorrectable message. Occasionally, however, the error pattern is such that the received word will lie in the decoding sphere of an incorrect codeword. Then the decoder makes a decoding error. Hence, in a BDD, the decoder output can be the correct message, an incorrect message, or a decoding default (an erased message). In our scheme, we assume a Reed-Solomon (RS) code with a BDD.

2.3.1 Maximum Distance Separable Codes

Since our scheme is based on maximum distance separable (MDS) codes, in this section we briefly review MDS codes and look at some of their properties [18] [19],which are being used in subsequent sections.

Consider an (n, k, d) linear code where n is the number of code symbols, k is the number of information symbols and d is the minimum distance of the code. In general we have

$$d \leq n - k + 1. \tag{2.1}$$

Codes with equality in Equation (2.1) are called MDS codes. The name comes from the fact that such a code has the maximum possible distance between codewords.

Let V be a subset of v coordinate positions of an MDS code, where $v \geq k$. If we project the original code onto V (this process is usually called puncturing the original code), the result will be a certain (v, k) code. Since the parent (n, k) code has a minimum distance $d = n - k + 1$, the punctured code must have a minimum distance $d' \geq d - (n - v) = v - k + 1$. Since it is impossible for d' to be greater than $v - k + 1$, equality must hold and it follows that the punctured code is an (v, k) MDS code [18]. This means that by erasing s symbols from a codeword of an

(n, k, d) MDS code, we will have a codeword in an $(n-s, k, d-s)$ MDS code. This code is capable of correcting e errors where

$$e \leq \lfloor \frac{d-s-1}{2} \rfloor. \tag{2.2}$$

Therefore the (n, k) MDS code is capable of correcting e errors and s erasures as long as

$$2e + s \leq d - 1. \tag{2.3}$$

The number of codewords of weight j in an (n, k) MDS code over GF(q) is given by [19]

$$A_j(n) = \binom{n}{j} \sum_{a=0}^{j-d} (-1)^a \binom{j}{a} (q^{j-d+1-a} - 1). \tag{2.4}$$

For an (n, k) RS code over GF(q), the equality holds in Equation (2.1). Therefore RS codes are MDS codes.

2.4 The New Protocol

In this section we describe the new rate-adaptive coding scheme. The block diagram of this scheme is shown in Figure (2.3). The scheme is based on the idea of breaking down a block of n symbols into m equal-length sub-blocks, which can be combined to provide an adaptive code rate.

Consider an (n, k) RS code. As stated in the previous section, if we erase s symbols from a codeword, where $s \leq n - k$, the remaining symbols form a codeword in an $(n - s, k)$ MDS code [18]. We use this property in our analysis. We should mention that in this scheme there is no code for error detection, but the error detection is being done by the RS decoder at the same time. There are some

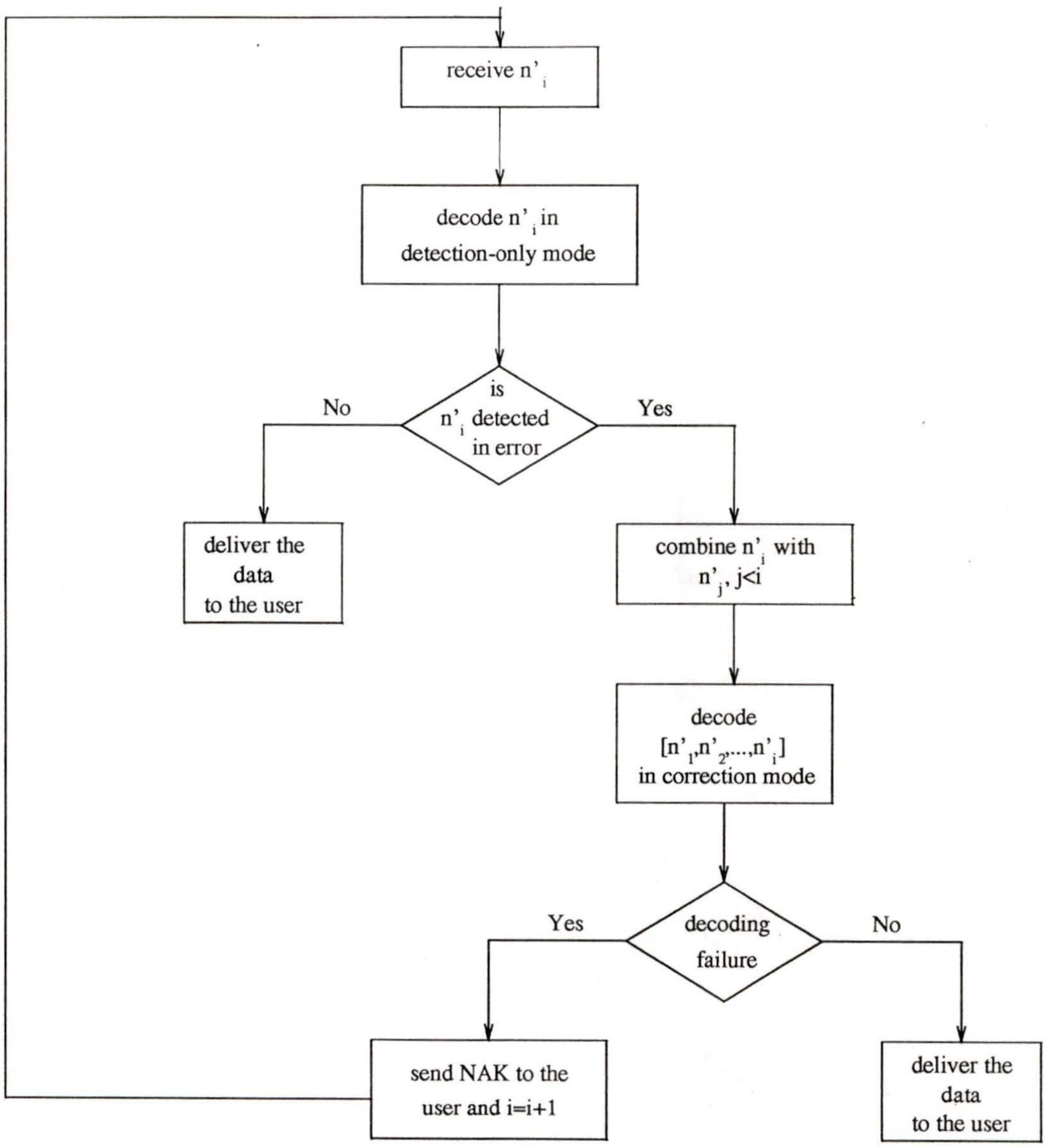

Figure 2.3: The block diagram of the new rate-adaptive coding scheme.

practical restrictions on n and k. The number of information symbols, k, cannot be very small because of the protocol overhead. The block length, n, is restricted by the existing technology. For example, an RS code for $n > 1024$ is difficult to implement. Now with suitably constrained choices of n and k, we write

$$n = m(k + r) + r', \qquad \text{where} \quad r' < k + r. \tag{2.5}$$

Here r represents the number of redundant symbols per transmission, m is the number of packets into which each codeword is divided and r' is the remainder from dividing n symbols into m equal packets. These packets can be packetized data or voice. As is shown in Figure (2.4b), the first $k + r$ symbols of the codeword are transmitted during the first transmission. We denote this set of symbols by $[n_1']$.

Depending on the value of r, during the first transmission, the decoder can work in three modes; detection-only mode, detection-correction-mode and correction-only mode. If r is large enough, the probability that a received word is decoded to a wrong codeword will be very small compared to the decoding failure, which occurs when the decoder fails to find any codeword at all as the transmitted codeword [18]. Therefore in this case, in the first transmission we can use the decoder in the correction-only mode and the error is detected whenever the decoder declares a decoding failure. If r is small, employing the decoder, after receiving the first block, in the correction-only mode can result in a high undetected error probability. This is because the RS decoder is used for error correction as well as error detection. Therefore it is appropriate that in this case, after receiving the first block, the decoder works in the detection-only mode. Also, for a moderate r, a combination of error correction and error detection can be used for the decoder's mode in the first transmission. In our analysis, we assume that in the first transmission the decoder works in the

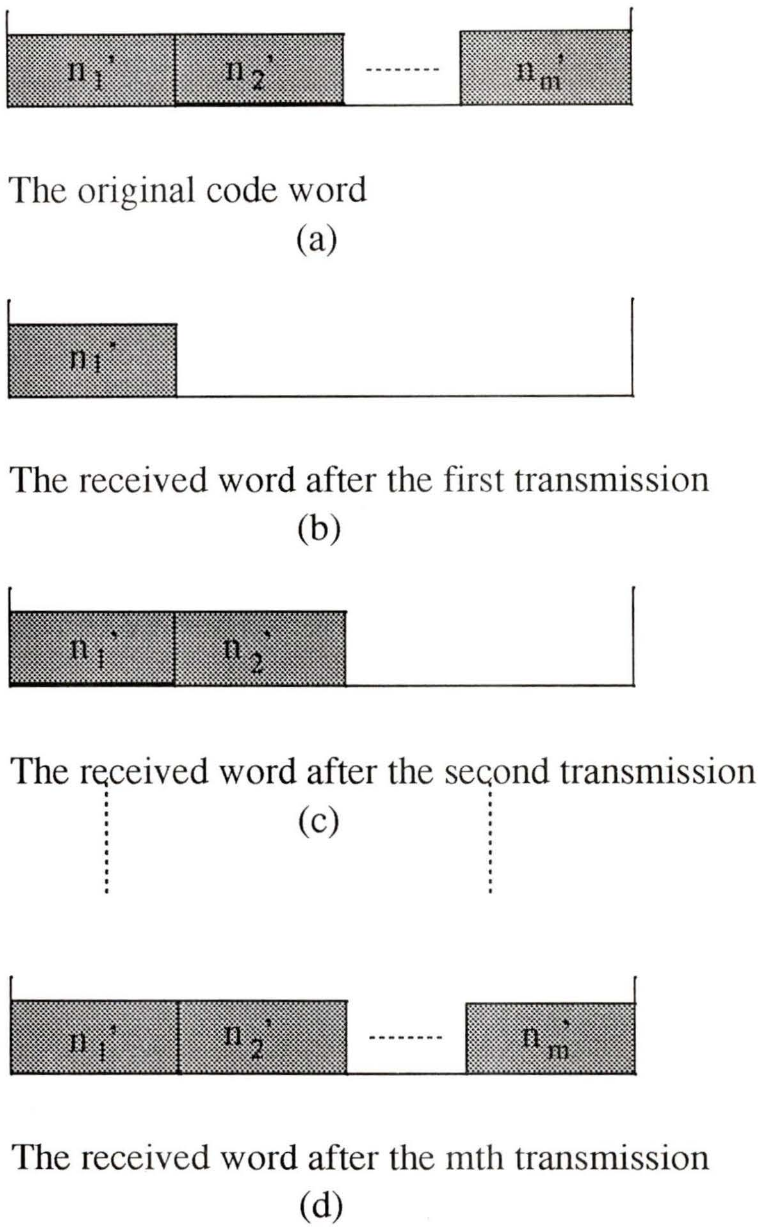

Figure 2.4: The received word after each transmission.

detection-only mode.

After receiving the first packet, if no error is detected in the received packet, the information symbols are recovered and delivered to the user. Otherwise a NAK signal is sent to the transmitter and the second set of $k + r$ symbols, $[n_2']$, is sent to the receiver.

After receiving the second packet, the receiver first tries, in the detection-only mode, to decode $[n_2']$ as a codeword in a $(k + r, k)$ MDS code. If this attempt fails, the decoder then tries to decode the composite block, $[n_1' + n_2']$, as a codeword in a $(2(k + r), k)$ MDS code, this time correcting all errors. If this attempt also fails, a NAK signal is sent to the transmitter and the third block is transmitted. This process continues until either the decoder is able to recover the data, or all the m packets are transmitted. If after transmitting the mth block, decoding is still impossible, several possibilities exist. Repetition of the whole procedure or stopping the attempt to recover the codeword after a specified number of retransmissions are two possibilities. The latter is being used in the next chapter, where this protocol is applied to a frequency hopping spread spectrum modulation scheme. Note that by first trying to decode each packet individually in the detection-only mode, data can be recovered if during any transmission the channel is in a "good" state.

The first transmission uses a $(k + r, k)$ MDS code with a code rate of $k/(k + r)$. The second transmission, if necessary, forms a codeword in a $(2(r + k), k)$ code with a rate of $k/2(k + r)$. If the mth transmission is required, the code rate drops to $k/m(k + r)$. This code rate adaptability makes this scheme a good choice for a wide variety of non-stationary channels. With this scheme, it is possible to choose p arbitrary packets from the set of received packets and attempt to decode them in the correction mode, as a codeword in a $(p(k + r), k)$ MDS code. This property is beneficial for non-stationary channels, where some packets may be badly damaged due to poor channel states.

If the channel introduces erasures, or channel side information (CSI) is available, erasure decoding, or error/erasure decoding, can improve the performance of the system. This protocol is capable of dealing with erasures.

2.5 Performance Analysis

Let c^i, e^i and d^i denote, respectively, the events "ith received block contains no error", "ith received block contains undetectable errors" and "ith received sequence contains detectable errors". Clearly we have

$$P(c^i) + P(e^i) + p(d^i) = 1. \tag{2.6}$$

Let C^i, E^i and D^i denote, respectively, the events that the data recovery after receiving the first $i-1$ blocks has been impossible and after receiving the ith block "the decoder recovers the data correctly", "the decoder recovers the data incorrectly" and "the decoder fails to recover the data".

For a transmitted data block to be successfully recovered by the receiver, the average number of transmissions, T, is given by

$$T = [P(C^1) + P(E^1)] + 2[P(C^2) + P(E^2)] + 3[P(C^3) + P(E^3)] + \cdots \tag{2.7}$$

We can express Equation (2.7) as

$$\begin{aligned} T &= [P(C^1) + P(E^1)] + 2[P(C^2) + P(E^2)] + 2P(D^2) - 2P(D^2) \\ &\quad +3[P(C^3) + P(E^3)] + 3P(D^3) - 3P(D^3) + 4[P(C^4) + P(E^4)] \\ &\quad +4P(D^4) - 4P(D^4) + \cdots, \end{aligned} \tag{2.8}$$

Manipulating Equation (2.8), we obtain

$$T = 1 + P(D^1) + P(D^2) + P(D^3) + \cdots. \tag{2.9}$$

To calculate T, when the number of transmissions for each codeword is limited, Equation (2.9) is used.

For the sake of simplicity, consider the case $m = 3$. In this section, we find the throughput and undetected error probability, for the channel without erasure. First, we obtain an expression for the decoding error, which by definition occurs when the decoder selects a codeword other than the transmitted codeword. Because an RS code is a linear code, we assume, without loss of generality, that the all-zero codeword is transmitted. In the first transmission, the probability of the decoding error, $P(E^1)$, is

$$P(E^1) = \sum_{j=1}^{n'} A_j(n')(p_e/(2^m-1))^j(1-p_e)^{n'-j}, \tag{2.10}$$

where p_e is the code symbol error probability and $A_j(n')$ is the number of codewords of weight-j in an (n', k) MDS code. $A_j(n')$ is given by Equation (2.4).

The probability of retransmission and the probability of correct decoding after the first transmission are given by

$$P(C^1) = (1-p_e)^{n'}, \tag{2.11}$$

$$P(D^1) = P(F^1) = 1 - P(C^1) - P(E^1), \tag{2.12}$$

where $P(F^1)$ is the probability of decoding failure after the first transmission.

Let $p(j,h)$ denote the probability that the received word falls within distance h of a particular weight-j codeword, which we call J. We then have

$$p(j,h) = \sum_{r=0}^{h}\sum_{i=0}^{h-r} \binom{n-j}{r}\binom{j}{h-r}\binom{h-r}{i}(2^m-1)^{i-j}(2^m-2)^{h-r-i}p_e^{j+r-i}(1-p_e)^{n-j-r+i}. \tag{2.13}$$

Formula (2.13) is derived in the appendix.

Let E_{2j} be the event that $[n'_1]$ and $[n'_2]$ are detected in error and $[n'_1 + n'_2]$ lies within distance $t + n'/2$ of the codeword J in the $(2(k+r), k)$ MDS code. Note that $t = \lfloor (n' - k)/2 \rfloor$. Then we have

$$P(E_{2j}) \le P(E_{2infj}) = \sum_{h=2}^{t+n'/2} \sum_{r=0}^{h} \sum_{i=0}^{h-r} \binom{2n'-j}{r} \binom{j}{h-r} \binom{h-r}{i} (2^m - 1)^{i-j} \times$$

$$(2^m - 2)^{h-r-i} p_e^{j+r-i} (1 - p_e)^{2n'-j-r+i}. \qquad (2.14)$$

The event E_{2infj} is the event that there are at least two randomly distributed errors in $[n'_1 + n'_2]$ and that $[n'_1 + n'_2]$ lies within distance $t + n'/2$ of the codeword J.

Define

$$P(E^2_{inf}) = \sum_{j=1}^{2n'} A_j(2n') P(E_{2infj}) + P(D^1) P(E^1), \qquad (2.15)$$

$$P(C^2) = \sum_{e_1=1}^{t+n'/2-1} \sum_{e_2=1}^{t+n'/2-e_1} \binom{n'}{e_1} \binom{n'}{e_2} (p_e)^{e_1+e_2} (1 - p_e)^{2n'-(e_1+e_2)} + P(D^1)(1 - p_e)^{n'}, \qquad (2.16)$$

$$P(D^2) = P(F^2) = 1 - P(C^1) - P(E^1) - P(C^2) - P(E^2)$$
$$< 1 - P(C^1) - P(E^1) - P(C^2) - P(D^1)P(E^1). \qquad (2.17)$$

Then $P(E^2_{inf})$ is an upper bound on the probability of the decoding error after receiving the second packet. $P(D^2)$ is the probability of retransmission after the reception of the second packet. $P(C^2)$ is the probability that the decoder finds the correct codeword after receiving the second packet.

If after the second transmission the decoder can not find the transmitted codeword, $[n'_3]$ is transmitted. In this case, we have

$$P(E_{3j}) \leq P(E_{3infj}) = \sum_{h=n'/2+t+2}^{t+n'} \sum_{r=0}^{h} \sum_{i=0}^{h-r} \binom{3n'-j}{r} \binom{j}{h-r} \binom{h-r}{i} (2^m-1)^{i-j} \times$$

$$(2^m-2)^{h-r-i} p_e^{j+r-i} (1-p_e)^{3n'-j-r+i}. \quad (2.18)$$

Here E_{3infj} is the event that there are at least $n'/2+t+2$ errors in $[n'_1+n'_2+n'_3]$ and the received word lies within the distance $(t+n')$ of a j-weight codeword in the $(3(k+r),k)$ MDS code.

The probability of decoding error after receiving the third packet, $P_3(E)$, is upper bounded by

$$P(E^3_{inf}) = \sum_{j=1}^{3n'} A_j(3n')P(E_{3infj}) + P(D^2)P(E^1). \quad (2.19)$$

The probability that the decoder finds the correct transmitted codeword after receiving $[n'_3]$ is

$$P(C^3) = \sum_{e_1=1}^{min(t+n'-2,n')} \sum_{e_2=max(1,t+n'/2-e_1+1)}^{min(t+n'-e_1-1,n')} \sum_{e_3=1}^{t+n'-e_1-e_2} \binom{n'}{e_1}\binom{n'}{e_2}\binom{n'}{e_3} \times$$
$$(p_e)^{e_1+e_2+e_3}(1-p_e)^{3n'-(e_1+e_2+e_3)} + P(D^2)(1-p_e)^{n'}. \quad (2.20)$$

The probability of retransmission after receiving $[n'_3]$ is

$$P(D^3) = P(F^3) = 1 - P(C^1) - P(E^1) - P(C^2) - P(E^2) - P(C^3) - P(E^3)$$
$$< 1 - P(C^1) - P(E^1) - P(C^2) - P(D^1)P(E^1) - P(C^3) - P(D^2)P(E^1).$$
$$(2.21)$$

Now that we have a bound on the probability of decoding error and the probability that the decoder finds the correct transmitted codeword, we find the throughput and undetected error probability.

The undetected error probability, $P(E)$, is given by

$$\begin{aligned} P(E) &= P(E^1) + P(E^2) + P(E^3) + P(D^3)P(E^3) + P(D^3)P(D^3)P(E^3) \\ &\quad + P(D^3)P(D^3)P(D^3)P(E^3) + \ldots \\ &= P(E^1) + P(E^2) + P(E^3) + P(D^3)P(E^3)/(1 - P(D^3)). \end{aligned} \quad (2.22)$$

Therefore,

$$\begin{aligned} P(E) < \quad & P(E^1) + (P(E^2_{inf}) + P(D^1)P(E^1)) + (P(E^3_{inf}) + P(D^2)P(E^1)) \; + \\ & P(D^3)(P(E^3_{inf}) + P(D^2)P(E^1))/(1 - P(D^3)). \end{aligned} \quad (2.23)$$

Using Equation (2.7), the average number of transmissions before a block is delivered to the user, T, is given by

$$\begin{aligned} T = \quad & [P(C^1) + P(E^1)] + 2[P(C^2) + P(E^2)] + 3[P(C^3) + P(E^3)] \; + \\ & 4P(D^3)[P(C^3) + P(E^3)] + 5P(D^3)P(D^3)[P(C^3) + P(E^3)] + \\ & 6P(D^3)P(D^3)P(D^3)[P(C^3) + P(E^3)] + \cdots. \end{aligned} \quad (2.24)$$

$$\begin{aligned} T \;<\; & [P(C^1) + P(E^1)] + 2[P(C^2) + P(D^1)P(E^1) + P(E^2_{inf}] + \\ & 3[P(C^3) + P(D^2)P(E^1) + P(E^3_{inf})] \; + \\ & \{P(D^3)[P(C^3) + P(D^2)P(E^1) + P(E^3_{inf})]\} \; [(4 - 3P(D^3)/(1 - P(D^3))^2]. \end{aligned} \quad (2.25)$$

The system throughput is

$$\eta = k/(Tn'). \quad (2.26)$$

Note that in our analysis we assumed that if decoding is still impossible after the third transmission, then receiving $[n'_4]$ is the same as receiving another copy of $[n'_3]$. In other words after receiving $[n'_4]$, we try to decode $[n'_1 + n'_2 + n'_4]$. This means that after receiving $[n'_4]$, the decoder first tries to decode $[n'_4]$ in the detection-only mode. If this fails, $[n'_1 + n'_2 + n'_4]$ is decoded in the correction mode.

The performance of this new rate-adaptive coding scheme is compared with the performance of the pure selective-repeat ARQ. In Figures (2.5) and (2.6), we consider the (63,17) RS code, where each block of 63 symbols is broken down into three sub-blocks, each containing 21 symbols. The throughput results are shown in Figure (2.5) and the undetected error probabilities are plotted in Figure (2.6).

2.6 Conclusion

In this chapter, a new rate-adaptive hybrid ARQ protocol, which is robust for non-stationary channels, is proposed and its performance is analyzed.

The major features of this new rate-adaptive hybrid ARQ scheme are as follows:

1. The code rate can be adapted from 1 to $1/m$, where $m > 2$.

2. In each transmission or retransmission, the block length is the same.

3. There is no code for error detection, but the same code (RS code) is used for error correction and detection.

4. In the first transmission, the decoder can work in three modes: detection-only, detection-correction or correction-only.

5. The protocol is capable of dealing with erased symbols which is beneficial when the demodulator cannot decide about the received symbol, or side information is available.

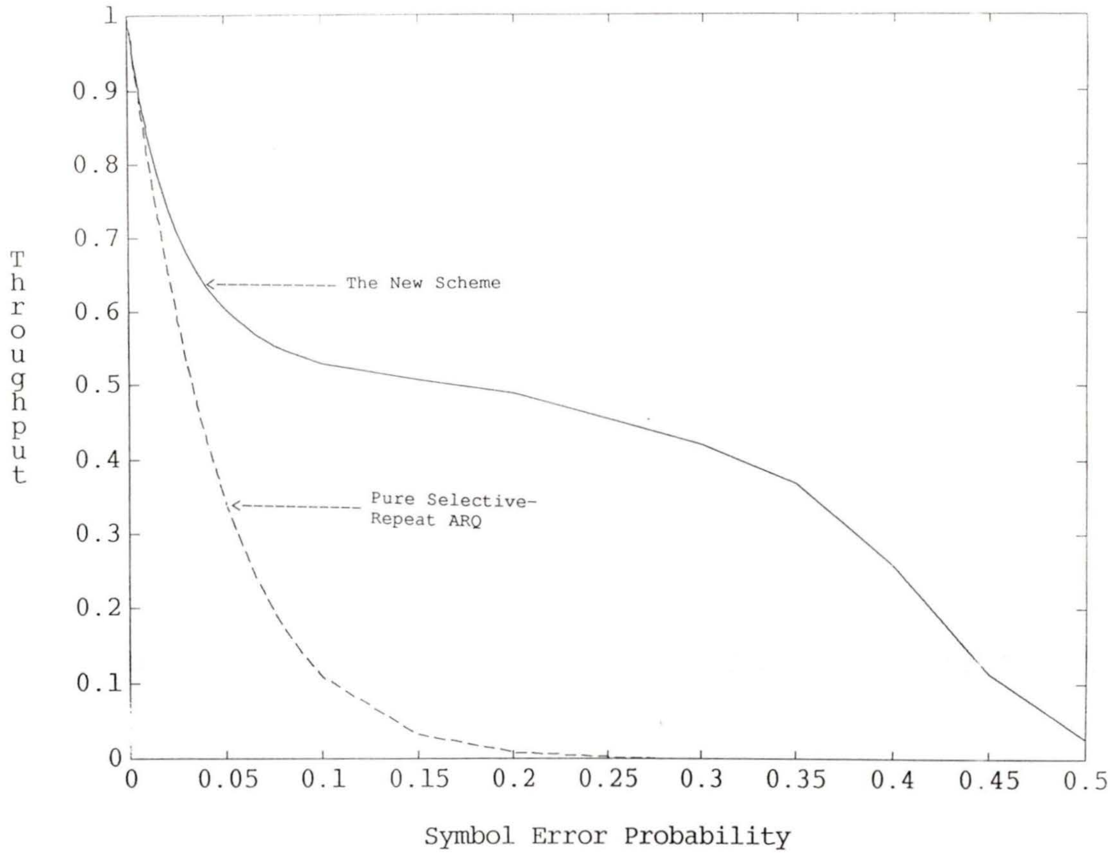

Figure 2.5: Throughput of the new protocol and the pure selective-repeat ARQ. (63,17) RS code is considered.

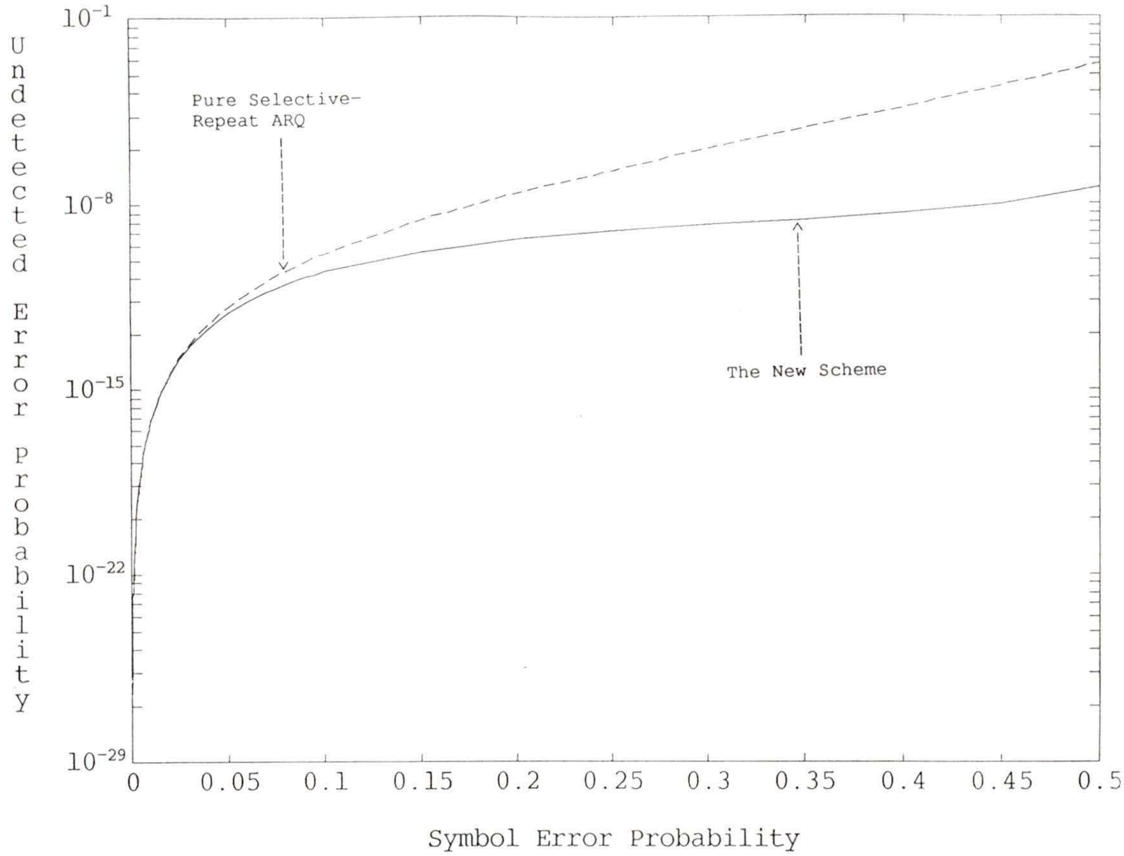

Figure 2.6: Undetected error probability of the new protocol and the pure selective-repeat ARQ. (63,17) RS code is considered.

Chapter 3

Frequency Hopping and Rate-Adaptive Coding for Multiple-Access Communication Systems

3.1 Introduction

Multiple access schemes are used to provide resources for establishing communications in a shared environment. In general, in terms of modulation, there are two multiple access schemes. In the first scheme, each user utilizes a channel exclusively (TDMA or FDMA). The second scheme uses spread spectrum as the modulation scheme and is called spread spectrum multiple access (SSMA). As we can see in Figure (3.1 b) [20], by utilizing spread spectrum, all users share the same channel, at the same time. This means that in the SSMA, each user's signal causes interference for the others. In such a system, increasing the number of users, increases the level of interference in the channel. For example, in Figure (3.1b), it is possible to increase the number of simultaneous users from six to seven at the expense of a lower quality for the others. Therefore, any interference reduction, by any means, converts directly and linearly to an increase in capacity.

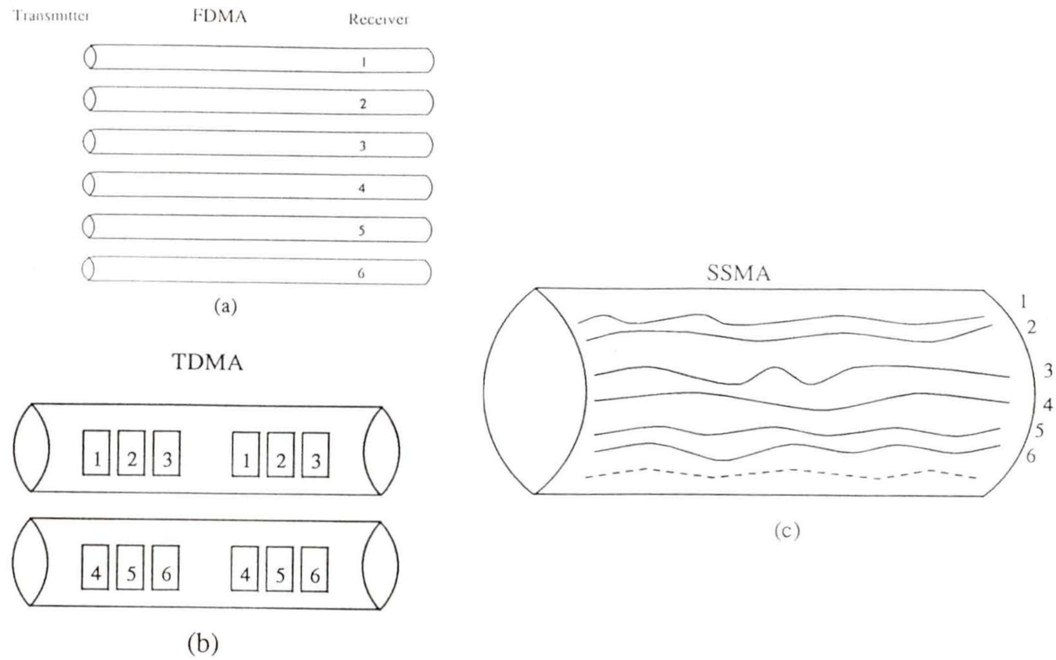

Figure 3.1: Illustration of different multiple access systems (a) FDMA (b) TDMA (c) SSMA.

There are two general spread spectrum techniques; direct sequence and frequency hopping [21]. In direct sequence the data-modulated signal is modulated a second time, using a very wide band spreading signal. In this technique the spreading code directly modulates the data-modulated carrier. The second method for widening the spectrum of a data-modulated carrier, which is called frequency hopping, is to change the frequency of the carrier periodically. Typically, each carrier frequency is chosen from a set of 2^k frequencies which are spaced approximately the width of the data modulation spectrum apart. The spreading code in this case does not directly modulate the data modulated carrier but instead is used to control the sequence of carrier frequencies.

In this chapter we consider frequency hopped SSMA in conjunction with a rate-adaptive coding scheme.

3.2 How to Increase the Capacity of the SSMA

One way of reducing interference in a SSMA system is considering the voice activity factor. In a voice communication system, the voice activity factor greatly reduces the self-noise of the spread spectrum system. SSMA voice services uses voice activated carrier transmission, so that when a user is listening or pausing during a conversation, the carrier is turned off and thus does not contribute to the system self-noise. Conventional telephone practice [22] for satellite circuits indicates that a given user will be talking approximately 35% of the time.

As we mention in this chapter, by using a rate-adaptive coding scheme in conjunction with frequency hopping spread spectrum (FHSS) a higher throughput results, compared to employing a fixed-rate code. The higher throughput can be interpreted as the shorter time that one user utilizes the channel, and therefore means less interference for the others. As a result, by using rate-adaptive coding in a SSMA system, the maximum number of users increases by the adaptability factor (AF), which will be defined in sections 3.3 and 3.4.

We consider two cases: channel without erasure and channel with perfect side information.

3.3 Performance Analysis

Consider a multiple access communication system as shown in Figure (3.2). Let FHSS be the modulation scheme and the rate-adaptive coding presented in the second chapter, be the coding scheme for this system.

When one user, the reference user, hops to a given sub-band, it is possible that

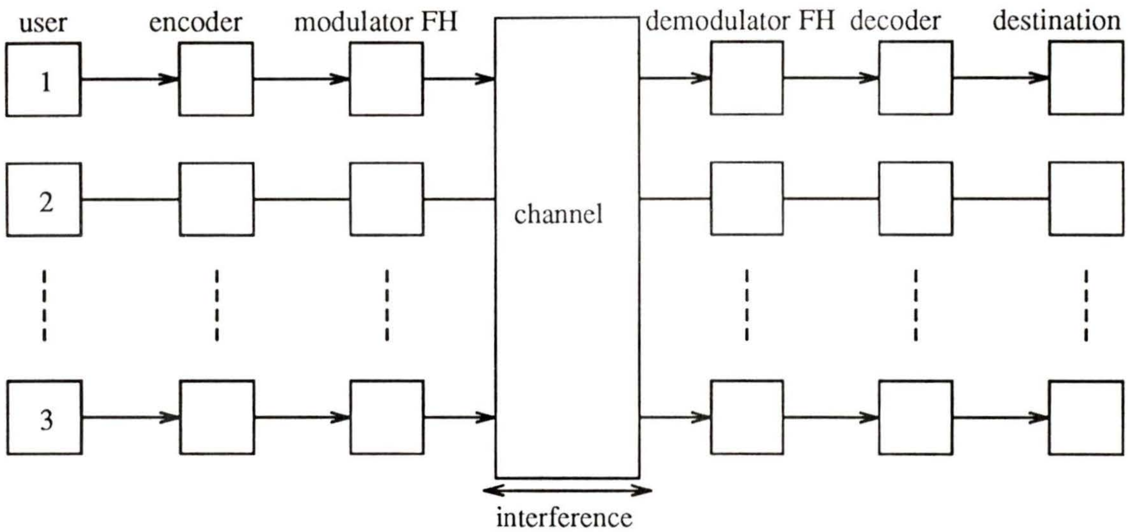

Figure 3.2: Frequency hopped multiple access system.

another user also hops to the same band and hits the reference user. The probability of being hit, p_h, is given by [23]

$$p_h = \begin{cases} \frac{1}{q}, & \text{hop synchronous,} \\ \\ \frac{2}{q} - \frac{1}{q^2}, & \text{hop asynchronous.} \end{cases} \tag{3.1}$$

where q is the total number of sub-bands. In our analysis we consider a hop synchronous system. Note that an N-ary FSK modulation scheme (with non-coherent detection) and perfect power control are assumed.

The demodulator for an N-ary FSK modulation scheme with non-coherent detection is given in Figure (3.3). To study the performance of the FHSS/NFSK, we need to obtain the probability density function (pdf) of sum of random phase vectors as a function of the number of vectors, m, in the sum. In short, one needs

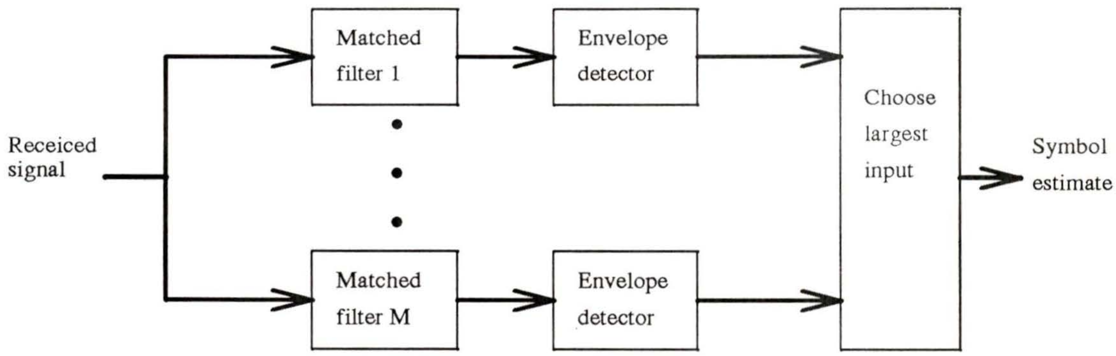

Figure 3.3: N-ary FSK non-coherent demodulator.

a complete set of above density functions for values of $m = 2, 3, \cdots, m_{max}$, where m_{max} represents the total number of users in the multiple access system.

3.3.1 pdf of the Squared Envelope of a Sum of Random Phase Vectors

In this section, the pdf of the squared envelope of a sum of m random phase vectors, $p_M(v_m)$, is given. This pdf will be used to derive the channel symbol and the code symbol error probabilities. The pdf is derived in [24] by a recursive solution.

Let A_i denote the amplitude, and θ_i denote the phase of vector i, where θ_i is uniformly distributed on the interval $(-\pi, \pi)$. Without loss of generality, we can assume $\theta_1 = 0$. Then for $p_2(v_2)$ we have [24]

$$p_2(v_2) = \begin{cases} \frac{1}{\pi\sqrt{4{A_1}^2{A_2}^2-({A_1}^2-v_2+{A_2}^2)}}; & (A_1 - A_2)^2 \leq v_2 \leq (A_1 + A_2)^2 \\ \\ 0; & \text{otherwise.} \end{cases} \tag{3.2}$$

For $p_M(v_m)$ we have

$$p_M(v_m) = \begin{cases} \frac{1}{\pi}\int_{\delta_{m-1}}^{\xi_{m-1}} \frac{p_{M-1}(v_m)}{\sqrt{4{A_m}^2 v_{m-1} - (v_{m-1} - v_m + {A_m}^2)^2}} dv_{m-1}; & v_{m_{min}} \leq v_m \leq (\sum_{i=1}^{m} A_i)^2 \\ 0; & \text{otherwise,} \end{cases} \tag{3.3}$$

where

$$\xi_{m-1} = \min((\sum_{i=1}^{m-1} A_i)^2, (A_m + \sqrt{v_m})^2), \tag{3.4}$$

$$\delta_{m-1} = \max(v_{m-1_{min}}, (A_m - \sqrt{v_m})^2), \tag{3.5}$$

and

$$v_{m_{min}} = \begin{cases} (\sum_{i=1}^{m-1} A_i)^2; & A_m \geq \sum_{i=1}^{m-1} A_i) \\ 0; & \sqrt{v_{m-1_{min}}} \leq A_m \leq \sum_{i=1}^{m-1} A_i \\ (\sqrt{v_{m-1_{min}}} - A_m)^2; & 0 \leq A_m \leq \sqrt{v_{m-1_{min}}}. \end{cases} \tag{3.6}$$

In general, for the envelope squared of the sum of m random phase vectors we have

$$V_m = (\sum_{i=0}^{m-1} A_i cos(\theta_i))^2 + (\sum_{i=0}^{m-1} A_i sin(\theta_i))^2 = {X_m}^2 + {Y_m}^2 \tag{3.7}$$

Define

$$\sigma_{X_m}{}^2 = \sigma_{Y_m}{}^2 = \frac{1}{2}\sum_{i=0}^{m-1} A_i{}^2. \tag{3.8}$$

When the number of vectors, m, is large, X_m and Y_m tend toward a Gaussian random variable with a zero mean and a variance given by Equation (3.8) (central limit theorem [25] [26]). Therefore, V_m approaches a chi-square random variable with 2 degrees of freedom and pdf given by

$$p_M(v_m) = \begin{cases} \frac{1}{\sum_{i=0}^{m-1} A_i{}^2} exp(\frac{-v_m}{\sum_{i=0}^{m-1} A_i{}^2}) & v_m \geq 0 \\ 0; & \text{otherwise} \end{cases} \tag{3.9}$$

The pdf of the squared envelope of the sum of three and five random phase vectors, with amplitude 1, are given in Figures (3.4) and (3.5).

3.3.2 Performance Analysis for Channel without Erasure

In this subsection, $p_E(K)$, the symbol error probability for the channel without erasure, is expressed in terms of the number of users K. This error probability is given by

$$p_E(K) = \sum_{m=1}^{K-1} p_e(m) p_{K,m}. \tag{3.10}$$

Here $p_{K,m}$ is the probability that m users, among $K-1$ users, hop to the reference user's sub-band and $p_e(m)$ is the conditional probability of symbol error given that m other users hop to the same band. $p_{K,m}$ and $p_e(m)$ are given by [27]

$$p_{K,m} = \binom{K-1}{m} p_h^m (1-p_h)^{K-1-m}, \tag{3.11}$$

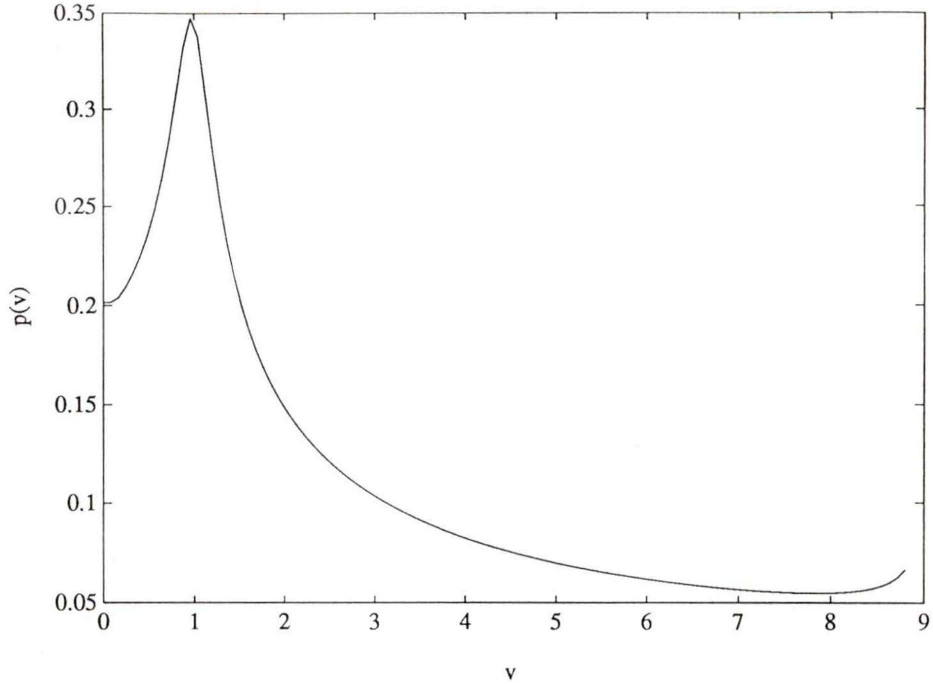

Figure 3.4: The pdf of the squared envelope of the sum of three random phase vectors with amplitude 1.

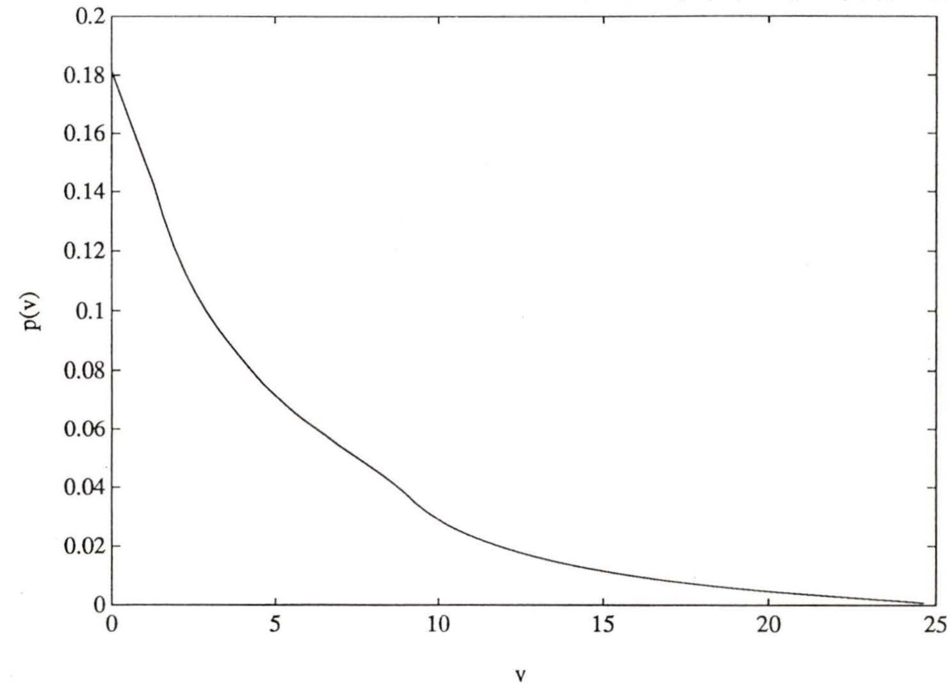

Figure 3.5: The pdf of the squared envelope of the sum of five random phase vectors with amplitude 1.

$$p_e(m) = \frac{N-1}{N^m} \sum_{k_1=0}^{m} \binom{m}{k_1} \int_0^\infty p_{k_1}(v_1)dv_1 \sum_{k_2=0}^{m-k_1} \binom{m-k_1}{k_2} \int_0^{v_1} p_{k_2+1}(v_2)dv_2 \times$$

$$\times \sum_{\substack{k_3,\ldots,k_N=0 \\ k_3 \le k_4 \ldots \le k_N \\ k_3+\ldots k_N = m-k_1-k_2}} \binom{m-k_1-k_2}{k_3,\ldots,k_N} A(m, k_3, \ldots, k_m) \times$$

$$\times \prod_{i=3}^{N} \int_0^{v_1} p_{k_i}(v_i)dv_i, \tag{3.12}$$

where

$$A(m, k_3, \ldots, k_N) = \frac{(N-2)!}{\prod_{n=0}^{m-k_1-k_2} (\sum_{i=3}^{N} \delta(n-k_i))!}, \tag{3.13}$$

and

$$\delta(x) = \begin{cases} 1, & \text{if } x = 0; \\ 0, & \text{otherwise.} \end{cases} \tag{3.14}$$

Note that $p_k(v)$ is the pdf of the squared envelope of the sum of k random phase vectors.

If we assume that L channel symbols form a code symbol, then the codeword error probability, $p_{CE}(K)$, is given by

$$p_{CE}(K) = 1 - (1 - p_E(K))^L. \tag{3.15}$$

Computing $p_e(m)$ and therefore $p_{CE}(K)$ is time consuming, but since $p_{K,m}$, for $m > 8$ and $K < 80$, is smaller than 10^{-6} (for a typical $p_h = 1/100$), the summation terms corresponding to $m > 8$ in Equation (3.10) can be ignored. The corresponding values of $p_e(m)$ and $p_{CE}(K)$, where $L = 2$, are tabulated in Tables (3.1) and (3.2).

m	$p_e(m)$
1	0.4375
2	0.5838
3	0.6361
4	0.6640
5	0.6836
6	0.7007
7	0.7166
8	0.7311

Table 3.1: The conditional probability of channel symbol error given that m other users hop to the reference user's sub-band. 8-ary FSK is used and $q = 100$.

The maximum number of transmissions, which is allowed for transmitting one block of data successfully, can be limited or unlimited. In the limited case, if after a specified number of transmissions the data recovery is still impossible, the incorrect data is delivered to the user. For the unlimited case, transmission continues until the receiver recovers the transmitted data.

The throughput and undetected error probability for the unlimited number of transmissions are calculated using the analysis in the second chapter.

If in the protocol, the maximum number of transmissions for each block is m, a slight modification in the analysis of Chapter 2 is necessary. In this case, the average number of transmissions for transmitting one block of data, T, is given by

$$T = 1 + p(D^1) + p(D^2) + p(D^3) + \cdots + p(D^{m-1}). \tag{3.16}$$

Therefore

$$\begin{aligned} T &= 1 + p(D^1) + p(D^2) + p(D^3) + p(D^3)p(D^3) + p(D^3)p(D^3)p(D^3) + \cdots + \\ &\quad (p(D^3))^{m-3}, \end{aligned} \tag{3.17}$$

K	$p_{CE}(K)$	K	$p_{CE}(K)$	K	$p_{CE}(K)$
2	0.0087	29	0.2117	56	0.3634
3	0.0174	30	0.2181	57	0.3683
4	0.0259	31	0.2245	58	0.3730
5	0.0344	32	0.2308	59	0.3778
6	0.0427	33	0.2370	60	0.3825
7	0.0510	34	0.2431	61	0.3871
8	0.0591	35	0.2492	62	0.3917
9	0.0672	36	0.2553	63	0.3962
10	0.0752	37	0.2612	64	0.4007
11	0.0831	38	0.2671	65	0.4052
12	0.0909	39	0.2730	66	0.4096
13	0.0987	40	0.2788	67	0.4139
14	0.1063	41	0.2845	68	0.4183
15	0.1193	42	0.2902	69	0.4225
16	0.1214	43	0.2958	70	0.4268
17	0.1288	44	0.3013	71	0.4309
18	0.1361	45	0.3068	72	0.4351
19	0.1434	46	0.3122	73	0.4392
20	0.1505	47	0.3176	74	0.4432
21	0.1576	48	0.3229	75	0.4472
22	0.1646	49	0.3281	76	0.4512
23	0.1716	50	0.3333	77	0.4552
24	0.1784	51	0.3385	78	0.4591
25	0.1852	52	0.3436	79	0.4629
26	0.1919	53	0.3486	80	0.4667
27	0.1986	54	0.3536		
28	0.2052	55	0.3585		

Table 3.2: Code symbol error probability. 8-ary FSK is used, $L = 2$ and $q = 100$.

where $p(D^i)$ is given in Chapter 2.

The codeword error probability, p(E), for the protocol with a maximum of m transmissions for each block is given by

$$p(E) = p_1(E) + p_2(E), \tag{3.18}$$

where $p_1(E)$ is the undetected error probability due to the decoding error, and $p_2(E)$ is the codeword error probability due to limiting the number of transmissions for each block. $p_1(E)$ and $p_2(E)$ are given by

$$p_1(E) = p(E^1) + p(E^2) + p(E^3) + \cdots + p(E^m), \tag{3.19}$$

$$p_2(E) = p(D^m), \tag{3.20}$$

where terms at the right side of Equations (3.19) and (3.20) are given in Chapter 2. Note that $p_2(E)$ is the probability of retransmission after the mth transmission.

We should mention that the channel between encoder and decoder, as shown in Figure (3.6), is modeled as an M-ary symmetric channel.

3.3.3 Performance Analysis for Channel with Perfect Side Information

In this section, we consider a channel with perfect side information. This means whenever there is a hit between two or more users, the corresponding symbols are erased. Since the decoder can recover $n - k$ erased symbols, by assuming the perfect side information, the performance of the system is improved remarkably.

For calculating the throughput and error probability, first we find the expression for the code symbol erasure probability. By modifying the analysis in the previous

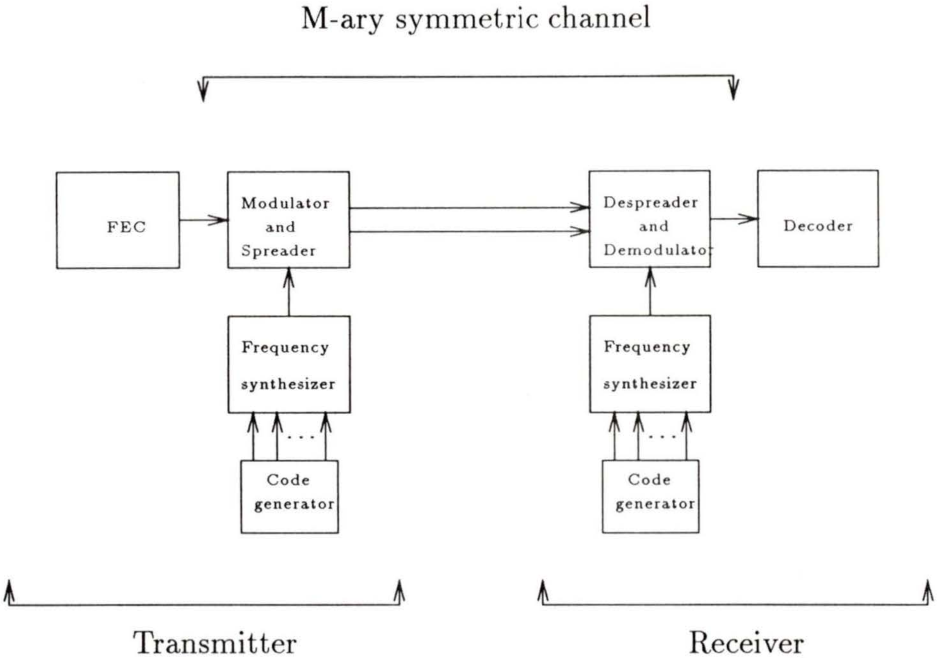

Figure 3.6: Transmitter and receiver block diagram.

section, one should be able to find the throughput and undetected error probability. The channel symbol erasure probability, $p_{cs}(K)$, is given by

$$p_{cs}(K) = \sum_{i=1}^{K-1} \binom{K-1}{i} p_h^i (1-p_h)^{K-1-i}. \tag{3.21}$$

If we assume there are L modulation symbols per code symbol, the codeword erasure probability, $p_{ws}(K)$, is given by

$$p_{ws}(K) = 1 - (1 - p_{cs}(K))^L. \tag{3.22}$$

Having perfect side information, makes the system robust relative to the power variations of the other users. The reason is that whenever there is a hit, the effect of inequality in power of different users is observed. In the case of the channel with perfect side information, the symbol that is hit is erased.

3.3.4 Performance Analysis for a Fixed-Rate Code

In this section, we consider a fixed-rate (n,k) RS code in conjunction with a frequency hopped spread spectrum modulation scheme. Since in our examples we assume $n >> k$, the decoding error is very small [18]. Therefore, the codeword error probability for the channel without erasure, $P_E(K)$, is given by

$$P_E(K) = \sum_{e=t+1}^{n} \binom{n}{e} p_{CE}(K)^e (1 - p_{CE}(K))^{n-e}, \tag{3.23}$$

where K represents the number of simultaneous users, $t = \lfloor \frac{n-k}{2} \rfloor$ and $p_{CE}(K)$ is the codeword error probability which is given in Table (3.2).

For the channel with perfect side information the codeword error probability, $P_{ES}(K)$, is given by

$$P_{ES}(K) = \sum_{s=n-k+1}^{n} \binom{n}{s} p_{cs}(K)^s (1 - p_{cs}(K))^{n-s}, \tag{3.24}$$

where $p_{cs}(K)$ is given by Equation (3.21).

3.4 Performance Examples

In this section some numerical results are presented. In all cases, 8-ary FSK is assumed, as the modulating scheme, and a (63,17) RS code is employed. There are $q = 100$ sub-bands. Adaptive rate coding is accomplished by breaking down the 63 symbols into three sub-blocks, each sub-block consisting of 21 symbols.

Figures (3.7) and (3.8) show the throughput and error probability versus the number of users for three cases; fixed-rate coding with the (63,17) RS code, rate-adaptive coding with a maximum of three transmissions, and rate-adaptive coding with a maximum of four transmissions. As we can see, the maximum number of users for $p_e < 10^{-6}$ are 17, 17, and 27, for each case, respectively. In the third case, the capacity of the network is increased due to an increase in the maximum number of transmissions for each word. In the first two cases, the maximum number of users is the same, but rate-adaptive coding provides a higher throughput. With 17 users utilizing the network simultaneously, the throughput (code rate) for the first case is 0.27, while for the second case it is increased to 0.42. This means that, on average, each information bit requires the transmission of 3.7 bits over the channel in the first case, and 2.4 bits in the second. Thus there is less interference to the channel in the latter case. Therefore, by employing rate-adaptive coding with a maximum of three transmissions, the number of users is increased by a factor of almost 1.56 (to a total of 26.4 users). We call this factor the adaptability factor (AF). Considering the AF in the case of rate-adaptive coding with a maximum of four transmissions, the number of users is further increased by a factor of 1.46 (to a total of 39.5 users).

Figures (3.9) and (3.10) show the throughput and error probability for the new scheme when there is no restriction in the number of transmissions.

In the following examples, perfect side information is assumed. Figures (3.11) and (3.12) show the throughput and error probability for rate-adaptive coding with perfect side information and a maximum of three and four transmissions. The maximum number of users for $p_e < 10^{-6}$ are 30 and 40, respectively. Considering AF, these numbers change to 45 and 54.5 users.

As we can see in the above examples, increasing the maximum number of transmissions for each codeword, increases the capacity of the system in terms of the number of users. Consequently, depending on the characteristics of the system and the time delay allowed, the number of users can be further increased. Also, we can see that with perfect side information, the capacity of the system is increased.

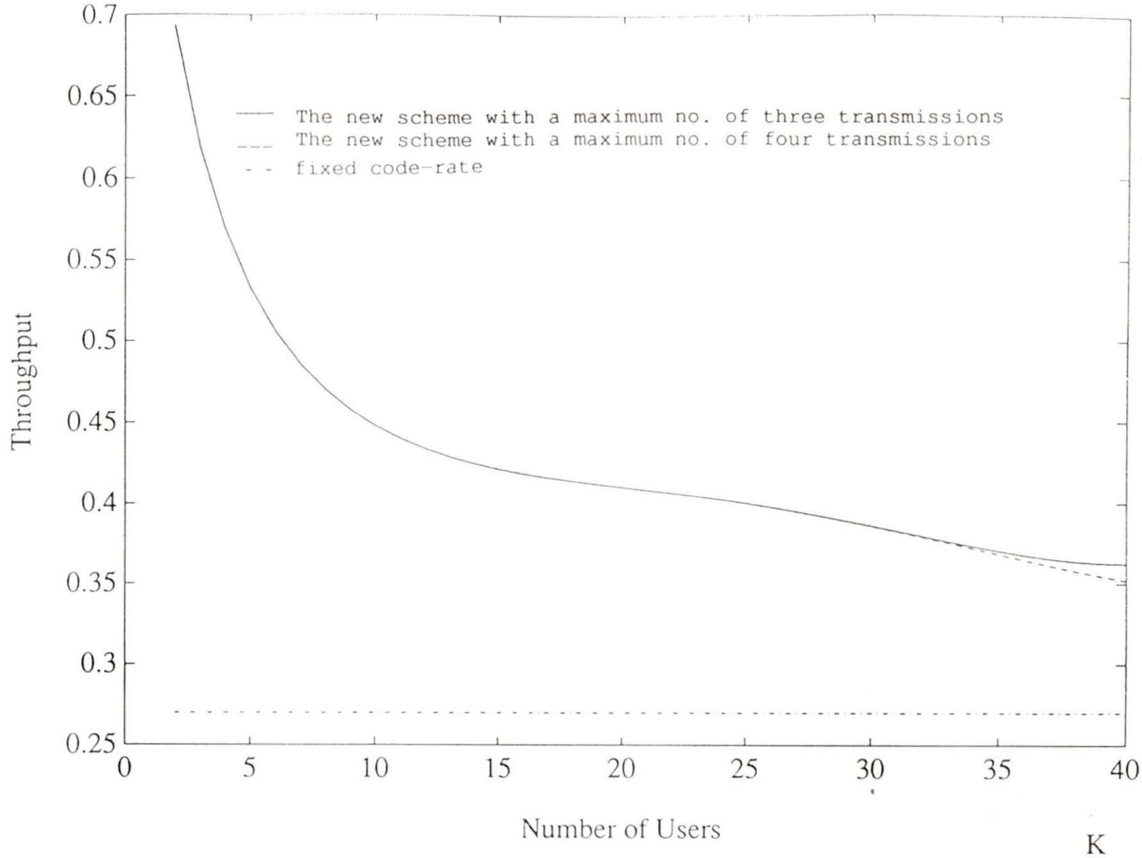

Figure 3.7: Throughput of the new scheme with the maximum number of transmissions for each codeword limited to 3 and 4. With $p_e < 10^{-6}$ the maximum number of users for fixed code-rate is 17, for adaptive code-rate with at most 3 transmissions is 17 and for adaptive code-rate with at most 4 transmissions is 27. 8-ary FSK, with $q = 100$, is used in conjunction with (63,17) RS code. There is no side information available.

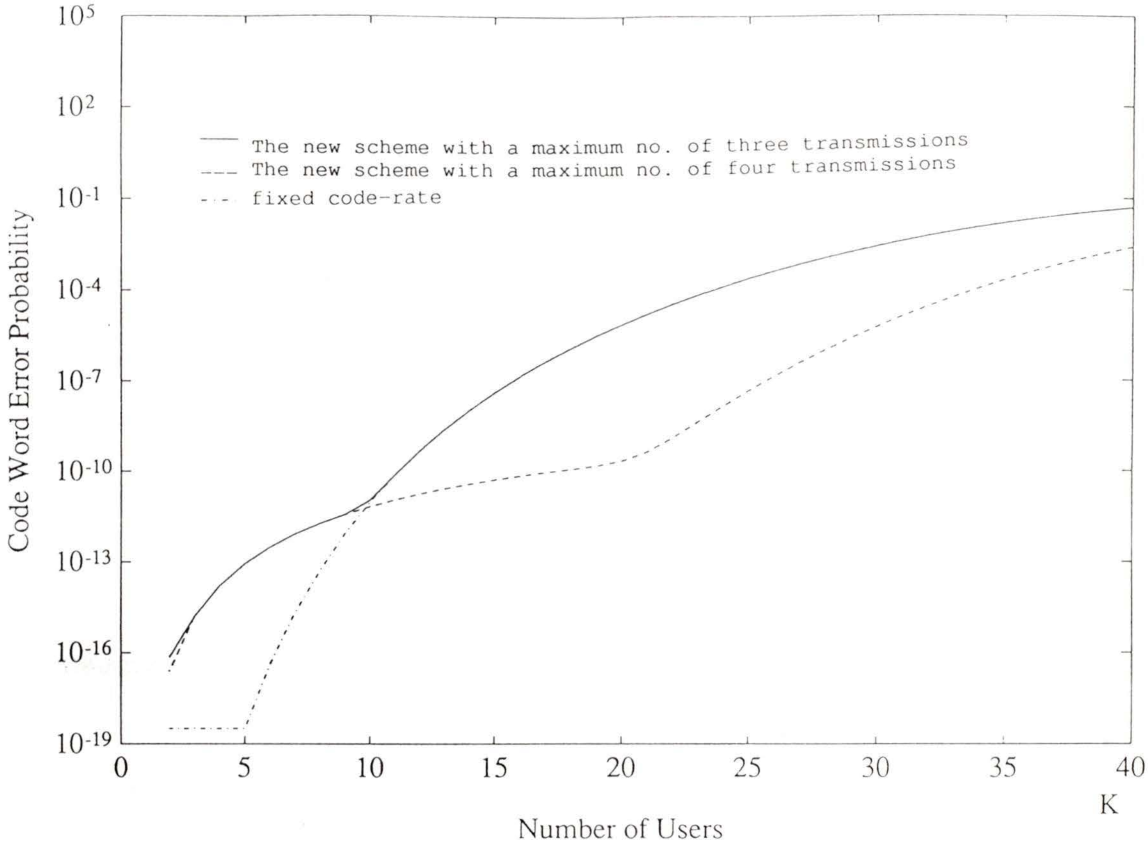

Figure 3.8: Codeword error probability of the new scheme with the maximum number of transmissions for each codeword limited to 3 and 4. With $p_e < 10^{-6}$ the maximum number of users for fixed code-rate is 17, for adaptive code-rate with at most 3 transmissions is 17 and for adaptive code-rate with at most 4 transmissions is 27. 8-ary FSK, with $q = 100$, is used in conjunction with (63,17) RS code. There is no side information available.

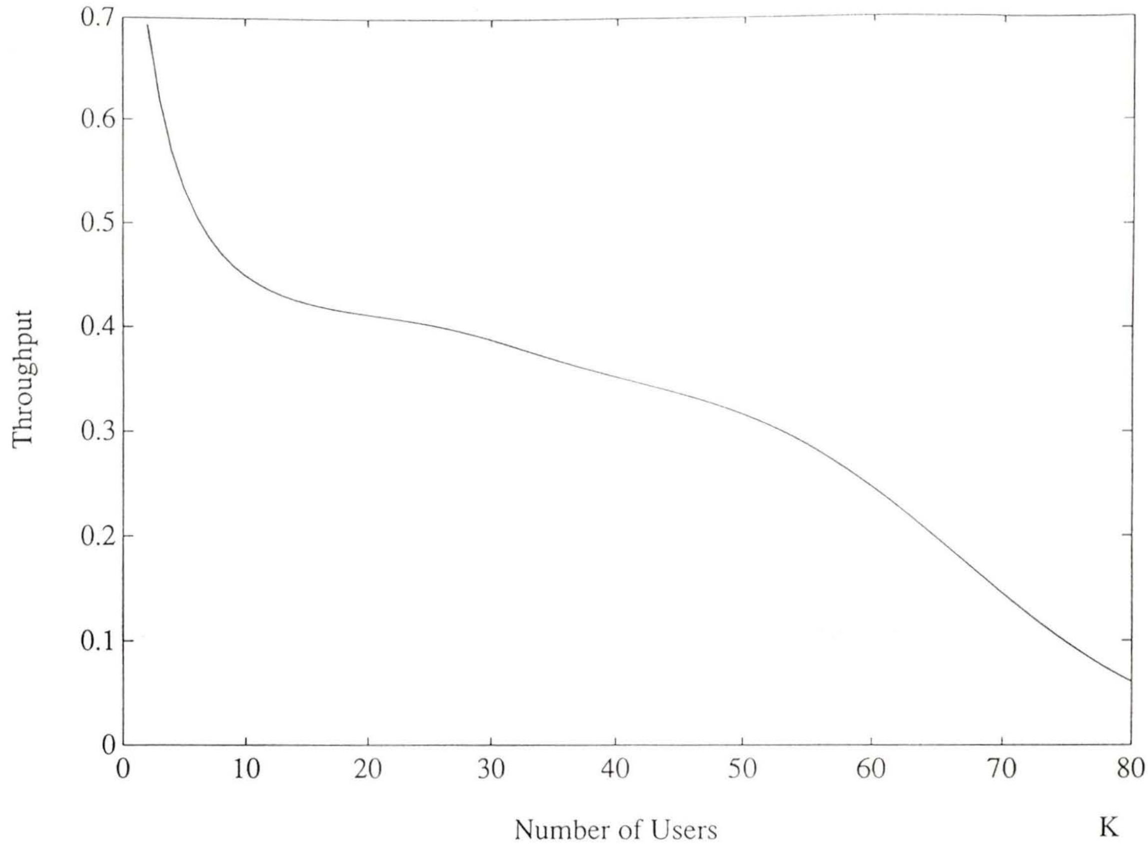

Figure 3.9: Throughput of the new scheme with the unlimited number of transmissions for each codeword. With $p_e < 10^{-8}$ the maximum number of users is 75. 8-ary FSK, with $q = 100$, is used in conjunction with (63,17) RS code. There is no side information available.

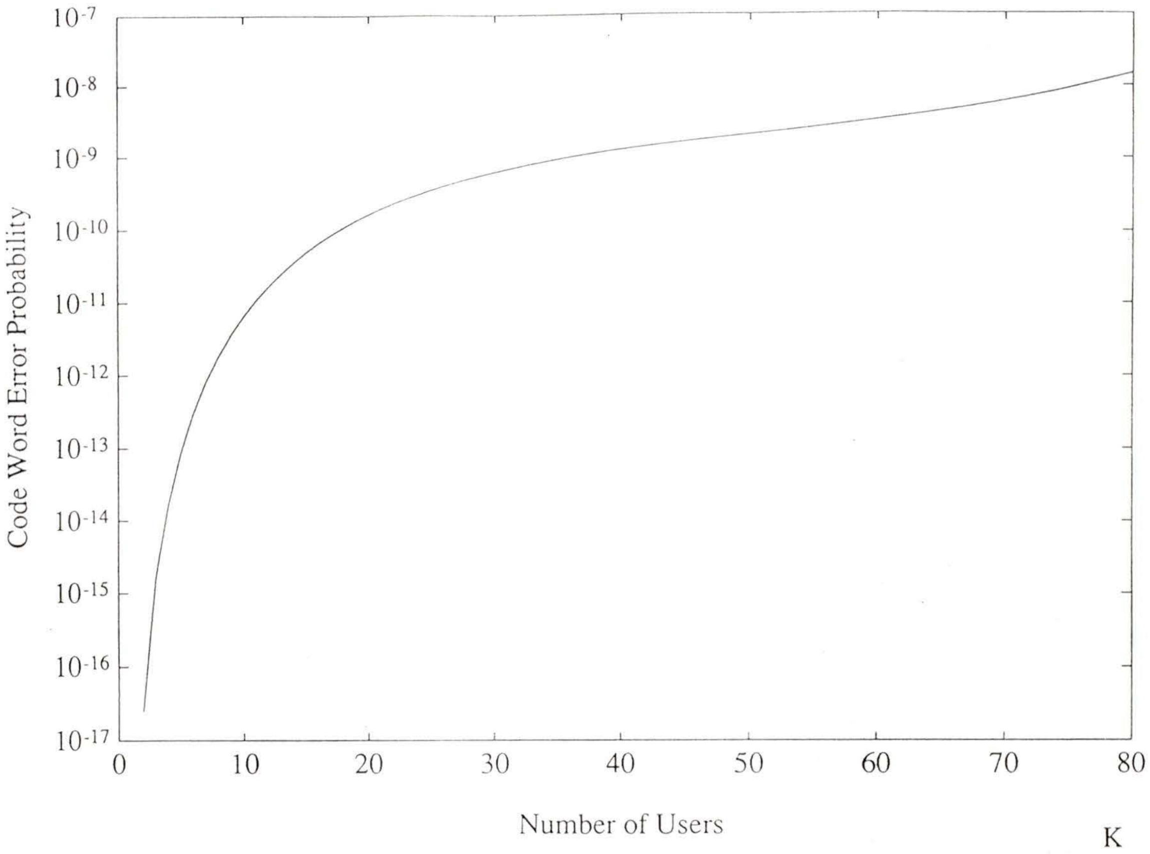

Figure 3.10: Codeword error probability of the new scheme with the unlimited number of transmissions for each codeword. With $p_e < 10^{-8}$ the maximum number of users is 75. 8-ary FSK, with $q = 100$, is used in conjunction with (63,17) RS code. There is no side information available.

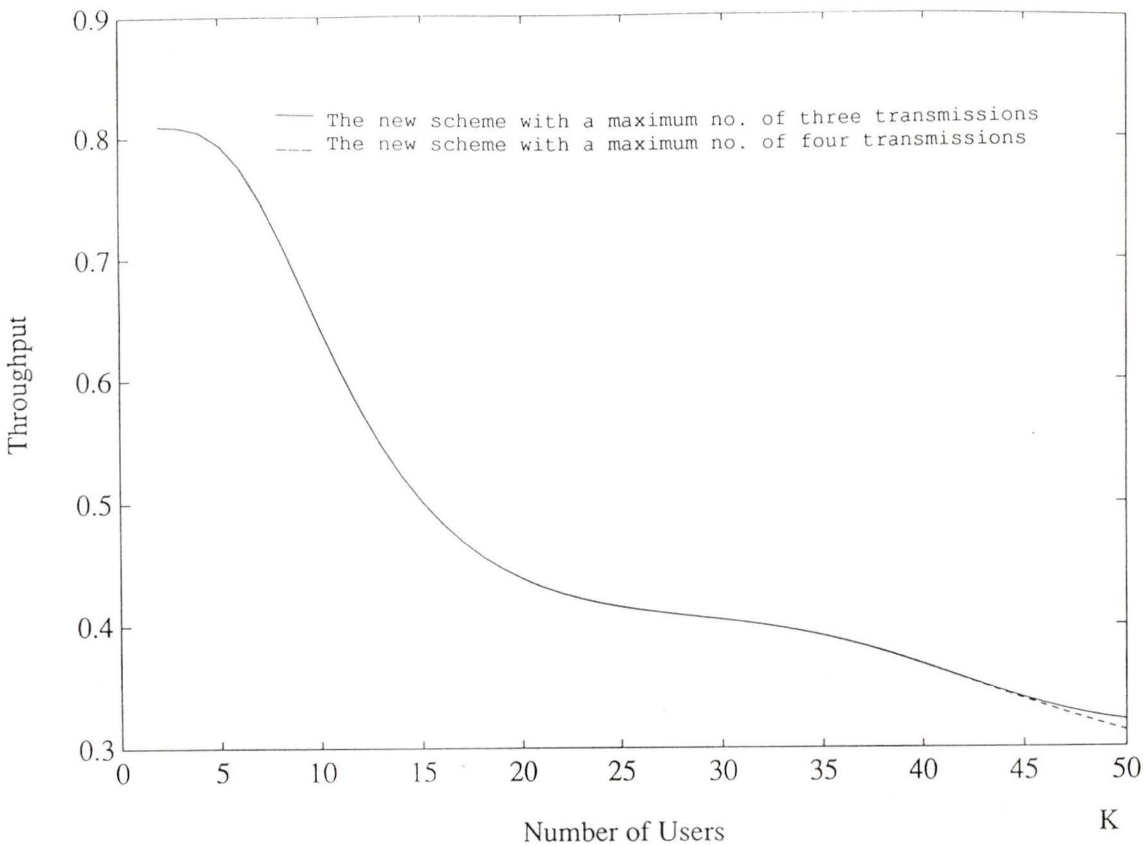

Figure 3.11: Throughput of the new scheme with the maximum number of transmissions for each codeword limited to 3 and 4. With $p_e < 10^{-6}$ the maximum number of users for fixed code-rate is 30, for adaptive code-rate with at most 3 transmissions is 30 and for adaptive code-rate with at most 4 transmissions is 40. 8-ary FSK, with $q = 100$, is used in conjunction with (63,17) RS code. Perfect side information is assumed.

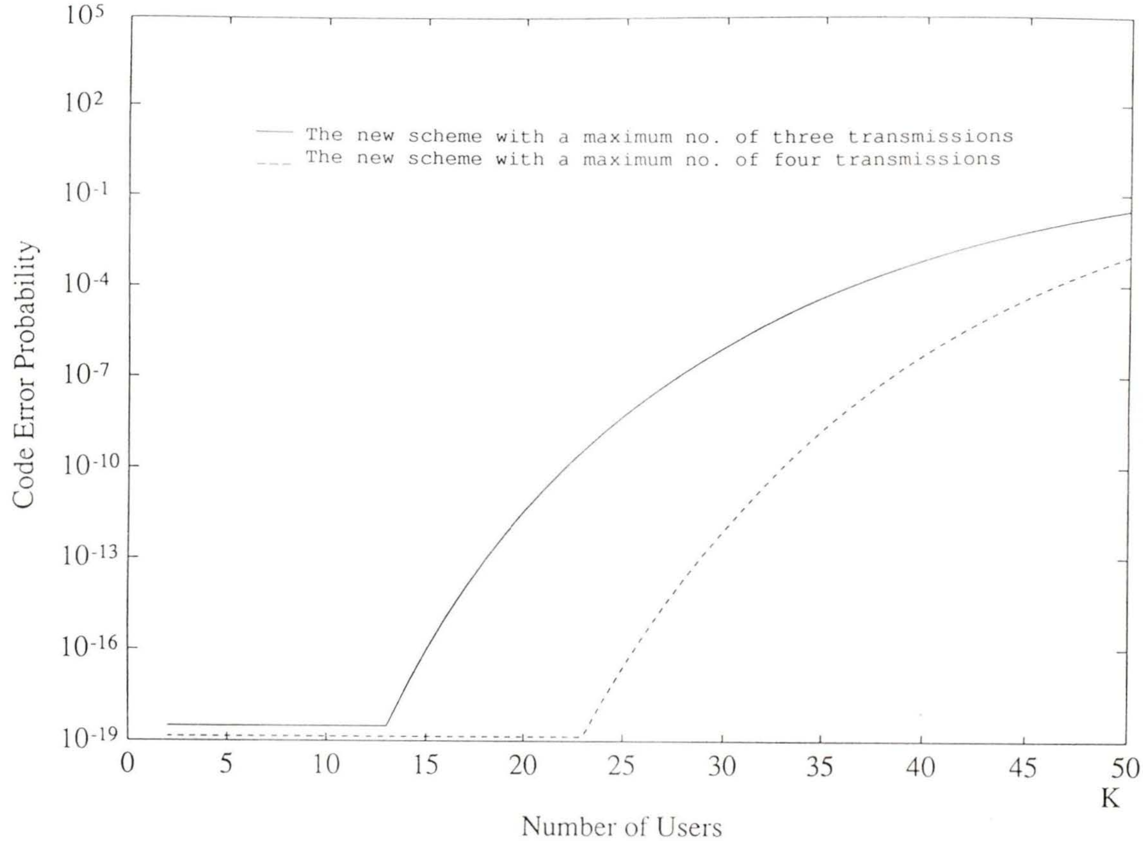

Figure 3.12: Codeword error probability of the new scheme with the maximum number of transmissions for each codeword limited to 3 and 4. With $p_e < 10^{-6}$ the maximum number of users for fixed code-rate is 30, for adaptive code-rate with at most 3 transmissions is 30 and for adaptive code-rate with at most 4 transmissions is 40. 8-ary FSK, with $q = 100$, is used in conjunction with (63,17) RS code. Perfect side information is assumed.

3.5 Conclusion

In this chapter, frequency hopped spread spectrum multiple access in conjunction with the rate-adaptive hybrid ARQ scheme, presented in the second chapter, is considered. It is shown that by using a rate-adaptive coding scheme, a higher number of users can be supported compared to the fixed-rate coding scheme. This increase in capacity, in terms of the number of simultaneous users, is accomplished in two ways:

1. Utilizing rate-adaptive coding increases the throughput. This causes a reduction in the interference that the user adds to the channel and thereby increases the capacity of the network by the adaptability factor.

2. If more time delay is allowed in the system, by increasing the maximum number of transmissions for each codeword (lowering the code rate), the capacity is increased.

Chapter 4

The Rate-Adaptive Coding Scheme, Based on MDS Codes, in a Rayleigh Fading Environment

4.1 Introduction

A multipath channel is one in which there are multiple propagation paths between the transmitter and the receiver [17]. A fading multipath channel is one in which the received signal strength varies with time because of the changing relationship between multiple propagation paths. Fading arises in free space propagation because of the changes in reflection layers in the ionosphere, or because of the changes due to the motion of the transmitter and the receiver. Multipath fading is a common occurrence in the mobile-radio environment. Also, multipath propagation and the dynamic environment create severe signal fading for indoor wireless communications. ARQ and hybrid ARQ schemes show very good results for compensating the fading effect [28]. It is emphasized that besides interleaving, which spread the error bursts, channel state and erasure information should be passed to the decoder. This information enables the decoder to distinguish between reliable symbols and unreliable symbols, the latter transmitted during bad channel conditions.

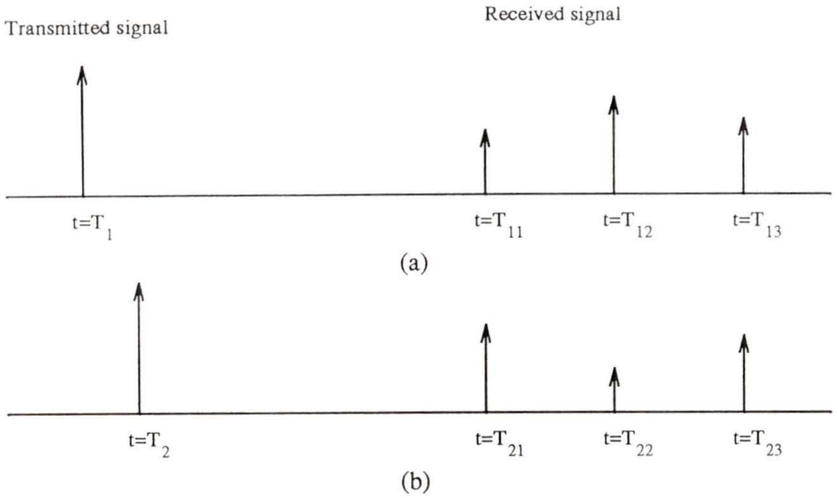

Figure 4.1: Example of the response of a time-variant multipath to a very narrow pulse.

4.2 Characterization of Fading Multipath Channels

A multipath medium has two characteristics [30]. The first one is the time spread introduced in the signal which is transmitted through the channel. For example, if we transmit an impulse (an extremely short pulse), over the channel, the received signal will appear as a train of pulses as shown in Figure (4.1 a).

The second characteristic is due to the time variations in the structure of the medium. As a result of such time variations, the nature of the multipath varies with time. This means by transmitting another pulse through the channel, the received pulse train will be different from Figure (4.1.a). (see Figure (4.1.b)).

Consider the transmission of a pure sine wave at the frequency f_c. Let $\alpha_n(t)$ and $\tau_n(t)$, respectively, denote the attenuation factor and the propagation delay for the

nth path. In this case the received signal, $r(t)$ is given by

$$\begin{aligned} r(t) &= \sum_n \alpha_n(t) e^{-j2\pi f_c \tau_n(t)} \\ &= \sum_n \alpha_n(t) e^{-j\theta_n(t)} \\ &= a_i + j a_q, \end{aligned} \tag{4.1}$$

where

$$\begin{aligned} a_i &= \sum_n \alpha_n(t) cos(\theta_n(t)) \\ a_q &= \sum_n \alpha_n(t) sin(\theta_n(t)). \end{aligned} \tag{4.2}$$

Therefore, the received signal consists of the sum of a number of complex waveforms arriving via different individual paths. If the number of paths is large, then by applying the *centeral limit theorem* [25] [26], one can conclude that both in-phase, a_i, and quadrature, a_q, components of the received signal are Gaussian. In a multipath fading channel without any direct path between the receiver and the transmitter, these Gaussian processes have a zero mean. Considering the fact that a_i and a_q are two zero-mean Gaussian processes, it can be shown that [26] fading envelope, $a = \sqrt{a_i^2 + a_q^2}$, has a Rayleigh distribution with a probability density function given by

$$p_A(a) = \frac{a}{\sigma^2} e^{-a^2/2\sigma^2} \qquad r \geq 0. \tag{4.3}$$

In the event that there is direct path between the transmitter and the receiver, as well as the fading multipath, a_i and a_q can no longer be modeled as having a zero mean. In this case, the fading envelope a has a Rice distribution and the channel is said to be a Ricean channel. In our analysis, we only consider the Rayleigh fading channel.

In this chapter, we consider the rate-adaptive coding scheme, presented in the second chapter, in a Rayleigh fading environment. We also consider the effect of the channel side information and error-erasure decoding in improving the system performance.

4.3 Performance Analysis

In this section the following assumptions are made [28].

- The fading is slow compared to the data rate, resulting in a constant amplitude during one code symbol.

- Perfect interleaving of the code symbols results in statistically independent symbol errors.

- Perfect timing recovery with exact tracking of phase variations due to multipath effects is assumed.

- The side information containing the exact value of the channel amplitude, a, is available.

Under these assumptions, we calculate channel parameters such as symbol error and erasure probabilities.

4.3.1 Channel Parameters

We consider binary phase-shift keying (BPSK) with coherent detection. In this case the bit error probability, for a fixed channel amplitude a is given by [17]

$$p_b(a) = Q(\sqrt{a^2 \frac{2E_b}{N_o}}), \tag{4.4}$$

where

$$Q(x) = \frac{1}{2\pi}\int_{x}^{\infty} e^{-y^2/2}dy. \tag{4.5}$$

Considering Rayleigh fading, a has a Rayleigh distribution with the probability density function given by

$$p_A(a) = 2ae^{-a^2}. \tag{4.6}$$

Note that in Equation (4.6), we considered $E[a^2] = 1$. This means that the mean bit energy-to-signal ratio, E_b/N_o, is not affected by the fading multipath ($E[a^2E_b] = E_b$).

The bit error probability for the channel without erasure, p_b, is given by

$$p_b = \int_0^{\infty} p_b(a)p_A(a)da. \tag{4.7}$$

Consider perfect interleaving for channel symbols. If each code symbol consists of m channel symbols, then the code symbol error probability for channel without erasure, p_{ec}, is given by

$$p_{ec} = 1 - (1 - p_b)^m. \tag{4.8}$$

Since an RS code is an MDS code, as discussed in the second chapter, a codeword with e errors and s erasures can be decoded correctly as long as

$$2e + s \leq d - 1, \tag{4.9}$$

where

$$d = n - k + 1. \tag{4.10}$$

As we mentioned in our assumptions, side information regarding channel amplitude is available. For generating erasure, we use the same strategy as [28]. A code symbol is considered unreliable if the channel amplitude during the symbol is below a certain threshold, T_s. The probability of the code symbol erasure, p_s, is given by

$$p_s = \int_0^{T_s} p_A(a)da. \tag{4.11}$$

Let $p_e(a)$ denote the code symbol error probability conditional on the given a. Then we have

$$p_e(a) = 1 - (1 - p_b(a))^m. \tag{4.12}$$

The code symbol error probability for the channel with erasure, p_e, is given by

$$p_e = \int_{T_s}^{\infty} p_e(a)p_A(a). \tag{4.13}$$

Using the channel parameters derived in this section, the throughput and undetected error probability are calculated. For the channel without erasure, we use the analysis given in Chapter 2. For the channel with erasure, the analysis in the next section is used.

4.3.2 Throughput and Undetected Error Probability

Again we assume that each codeword is divided into three sub-blocks and in each transmission, one sub-block is transmitted. Further, without loss of generality, we assume that the all-zero codeword is transmitted. After the first transmission, the probability of decoding error, $P(E^1)$, is given by

$$P(E^1) = \sum_{j=1}^{n'} A_j(n')(p_e/(2^m - 1))^j(1 - p_e - p_s)^{n'-j}. \tag{4.14}$$

The probability of retransmission, $P(D^1)$, and the probability of the correct decoding after the first transmission, $P(C^1)$, is given by

$$P(C^1) = (1 - p_e - p_s)^{n'}, \tag{4.15}$$

$$P(D^1) = 1 - P(C^1) - P(E^1). \tag{4.16}$$

Let $p(j, h, n, s)$ denote the probability that the received word ,with a length of n, has s erased symbols and falls within a distance h of a particular weight-j codeword, which we call J. Note that J is a codeword in an $(n - s, k)$ MDS code. We then have

$$\begin{aligned} p(j,h,n,s) \;=\; & \sum_{r=0}^{h}\sum_{i=0}^{h-r} \binom{n-s-j}{r}\binom{j}{h-r}\binom{h-r}{i}\binom{n}{s}(2^m-1)^{i-j}(2^m-2)^{h-r-i} \times \\ & p_e^{j+r-i}(1-p_e-p_s)^{n-s-j-r+i}p_s^s. \end{aligned} \tag{4.17}$$

Formula (4.17) is derived in the appendix.

Let (E_{2j}, s_1, s_2) be the event that there are s_1 erasures in $[n'_1]$, s_2 erasures in $[n'_2]$, $[n'_1]$ and $[n'_2]$ each one contains erroneous or erased symbols, and $[n'_1 - s_1\ n'_2 - s_2]$ lies within distance $t+(n'-s_1-s_2)/2$ of a j-weight codeword in the $(2(k+r)-s_1-s_2, k)$ MDS code. Then we have

$$P(E_{2j}, s_1, s_2) \leq P(E_{2infj}, s_1, s_2) =$$

$$\begin{aligned} & \sum_{h=\delta(s_1)+\delta(s_2)}^{t+(n'-s_1-s_2)/2}\;\sum_{r=0}^{h}\sum_{i=0}^{h-r} \binom{2n'-s_1-s_2-j}{r}\binom{j}{h-r}\binom{h-r}{i}\binom{n'}{s_1}\binom{n'}{s_2}(2^m-1)^{i-j} \times \\ & (2^m-2)^{h-r-i}p_e^{j+r-i}(1-p_e-p_s)^{2n'-s_1-s_2-j-r+i}p_s^{s_1+s_2}, \end{aligned} \tag{4.18}$$

where

$$\delta(x) = \begin{cases} 1; & \text{if } \; x = 0, \\ 0: & \text{otherwise.} \end{cases} \tag{4.19}$$

In summation (4.18), h has such a lower bound, because the decoder has not been able to decode $[n_1']$ and $[n_2']$ in the detection-only mode. The undetected error probability after the second transmission, $P(E^2)$, is upper bounded by $P(E^2_{inf})$ where

$$\begin{aligned} P(E^2_{inf}) &= \sum_{s_1=0}^{n'} \sum_{s_2=0}^{n'-s_1} \sum_{j=1}^{2n'-s_1-s_2} A_j(2n'-s_1-s_2)p(E_{2infj}, s_1, s_2) \\ &\quad + P(D^1)P(E^1). \end{aligned} \tag{4.20}$$

The probability of having s_1 erasures in $[n_1']$, s_2 erasures in $[n_2']$ and correct decoding is given by $P(C^2, s_1, s_2)$

$$\begin{aligned} &P(C^2, s_1, s_2) = \\ &\sum_{e_1=\delta(s_1)}^{n'} \quad \sum_{\substack{e_2 = \delta(s_2) \\ e_2 \leq t + \frac{n'-s_1-s_2}{2} - e_1}}^{n'} \binom{n'}{s_1}\binom{n'}{s_2}\binom{n'-s_1}{e_1}\binom{n'-s_2}{e_2} \times \\ &(p_e)^{(e_1+e_2)}(p_s)^{(s_1+s_2)}(1-p_e-p_s)^{(2n'-s_1-s_2-e_1-e_2)}, \end{aligned} \tag{4.21}$$

where $\delta(x)$ is given by (4.19).

After receiving the second packet, the probability of correct decoding, $P(C^2)$, and the probability of retransmission, $P(D^2)$, is given by

$$P(C^2) = \sum_{s_1=0}^{n'} \sum_{s_2=0}^{n'-s_1} P(C^2, s_1, s_2) \; + \; P(D^1)P(C^1) \tag{4.22}$$

$$\begin{aligned} P(D^2) = P(F^2) &= 1 - P(C^1) - P(E^1) - P(C^2) - P(E^2) \\ &< 1 - P(C^1) - P(E^1) - P(C^2) - P(D^1)P(E^1). \end{aligned} \tag{4.23}$$

After receiving $[n'_3]$ with a similar analysis we have

$$P(E_{3j}, s_1, s_2, s_3) \leq P(E_{3infj}, s_1, s_2, s_3) =$$

$$\sum_{h=\delta(s_1)+\delta(s_2)+\delta(s_3)}^{t+n'-(s_1+s_2+s_3)/2} \sum_{r=0}^{h} \sum_{i=0}^{h-r} \binom{3n'-s_1-s_2-s_3-j}{r} \times$$

$$\binom{j}{h-r} \binom{h-r}{i} \binom{n'}{s_1} \binom{n'}{s_2} \binom{n'}{s_3} (2^m-1)^{i-j} (2^m-2)^{k-r-i} \times$$

$$p_e^{j-r+i} (1-p_e-p_s)^{3n'-s_1-s_2-s_3-j-r+i} p_s^{(s_1+s_2+s_3)}. \tag{4.24}$$

The undetected error probability after the third transmission, $P(E^3)$, is upper bounded by $p(E^3_{inf})$ where

$$P(E^3_{inf}) = \sum_{s_1=0}^{n'} \sum_{s_2=0}^{n'} \sum_{\substack{s_3=0 \\ s_1+s_2+s_3 \leq 2n'}}^{n'} \sum_{j=1}^{3n'-s_1-s_2-s_3} A_j(3n'-s_1-s_2-s_3) \times$$
$$\times P(E_{3infj}, s_1, s_2, s_3) + P(D^2)P(E^1). \tag{4.25}$$

For computing the probability of correct decoding after receiving the third transmission, $P(C^3)$, we have

$$P(C^3, s_1, s_2, s_3) =$$
$$\sum_{e_1=\delta(s_1)}^{n'-s_1} \sum_{\substack{e_2=\delta(s_2) \\ e_1+e_2 > t+\lfloor \frac{n'-s_1-s_2}{2} \rfloor}}^{n'-s_2} \sum_{\substack{e_3=\delta(s_3) \\ e_1+e_2+e_3 \leq (t+n'-s_1-s_2-s_3)}}^{n'-s_3} \times$$
$$\times \binom{n'}{s_1} \binom{n'}{s_2} \binom{n'}{s_3} \binom{n'-s_1}{e_1} \binom{n'-s_2}{e_2} \binom{n'-s_3}{e_3} (p_e)^{e_1+e_2+e_3} (p_s)^{s_1+s_2+s_3} \times$$
$$\times \ (1-p_e-p_s)^{(3n'-s_1-s_2-s_3-e_1-e_2-e_3)}, \tag{4.26}$$

$$P(C^3) = \sum_{s_1=0}^{n'} \sum_{s_2=0}^{n'-s_1} \sum_{\substack{s_3 = 0 \\ s_1+s_2+s_3 \leq 2n'}}^{n'} P(C^3, s_1, s_2, s_3) \; + \; P(D^2)(1-p_e-p_s)^{n'}. \tag{4.27}$$

The probability of retransmission after receiving the third packet is given by

$$\begin{aligned} P(D^3) = P(F^3) &= 1 - P(C^1) - P(E^1) - P(C^2) - P(E^2) - P(C^3) - P(E^3) \\ &< 1 - P(C^1) - P(E^1) - P(C^2) - P(D^1)P(E^1) - P(C^3) - P(D^2)P(E^1). \end{aligned} \tag{4.28}$$

For calculating the throughput and undetected error probability, Formulas (2.25), (2.26) and (2.23) are used.

4.4 Performance Examples

In this section we consider a maximum of three transmissions for each codeword. This means, if after the third transmission the data recovery is still impossible, the incorrect data is delivered to the user. This is a realistic assumption since it is impossible to have an infinite delay. We consider a (63,17) RS code, where 63 symbols are broken down into three sub-blocks, each one consisting of 21 symbols. In calculating the throughput and codeword error probability, the decoding error is neglected. This is because the codeword error probability, which results from limiting the maximum number of transmissions for each codeword, is much higher than the codeword error probability due to the decoding error. Also, we assume that there is no erasure in the first transmission. This means that even if the channel amplitude during the transmission of one symbol is below the erasure threshold T_s, the demodulator does not erase the symbol.

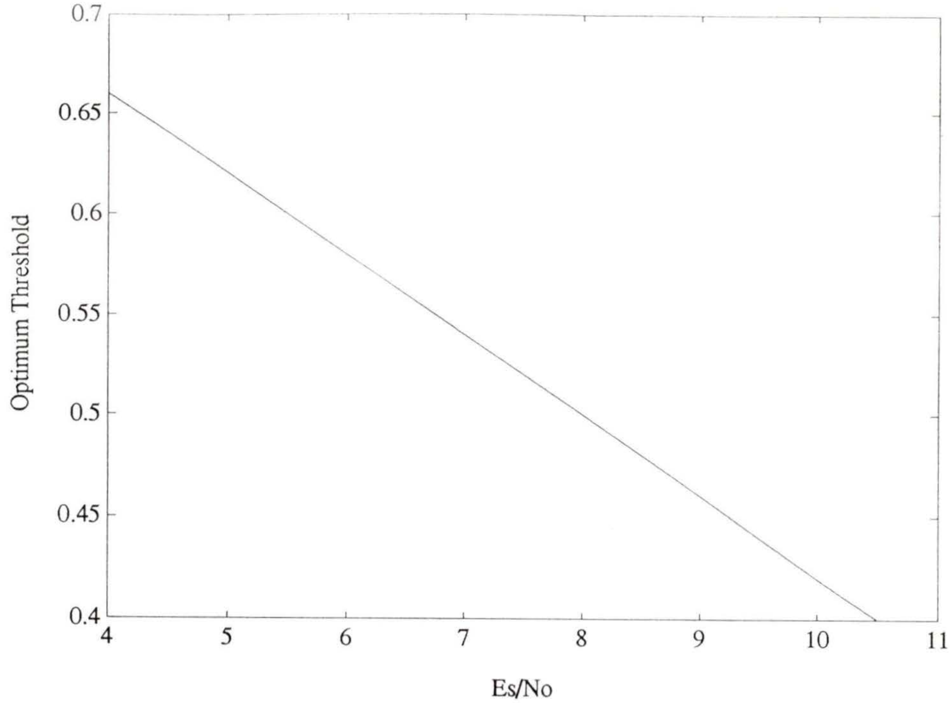

Figure 4.2: The optimum value for erasure threshold in a Rayleigh fading channel.

To have an idea of what value should be chosen for the erasure threshold, T_s, the optimum value of the threshold is found for a (63,17) RS code. Note that for finding this optimum value, a fixed-rate code is considered. The optimum value verses E_s/N_o is shown in Figure (4.2). Note that we describe the channel signal-to-noise ratio by E_s/N_o rather than by $E_b/N_o = E_b/RN_o$, where R is the code rate.

The throughput and codeword error probability for a Rayleigh fading channel employing the rate-adaptive coding scheme is shown in Figures (4.3) and (4.4). In these figures, the performance is shown for the case of a channel without erasure as well as a channel with perfect side information, with the optimum erasure threshold. Also, the throughput and error probability for the optimum erasure threshold and $T_s = 0.5, 0.6$ are shown in Figures (4.5) and (4.6).

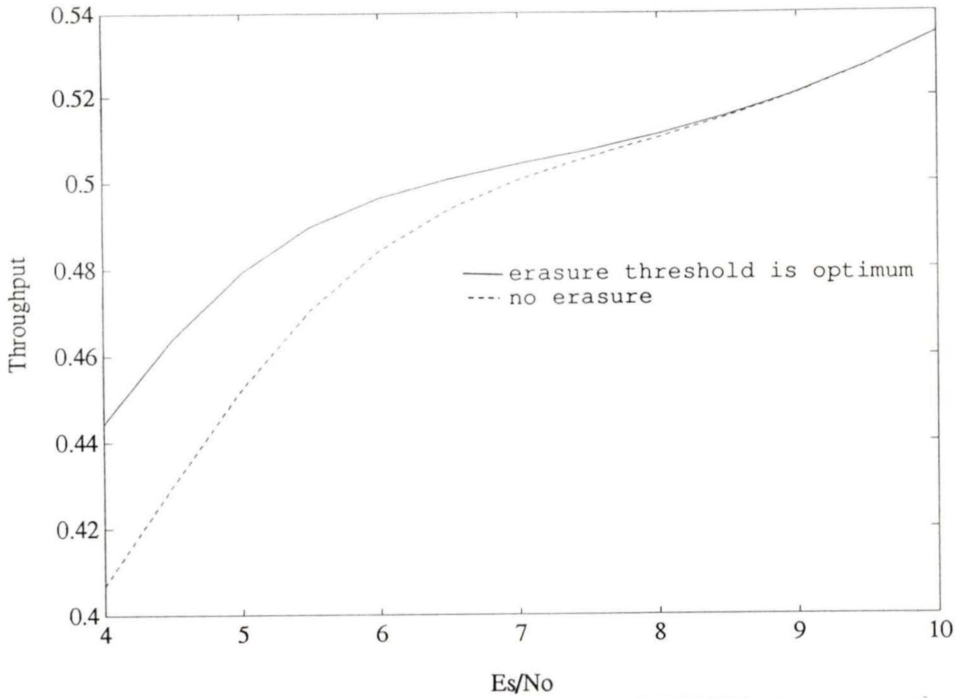

Figure 4.3: Throughput of the (63,17) rate-adaptive RS code in a Rayleigh fading channel with side information. The optimum erasure threshold is considered

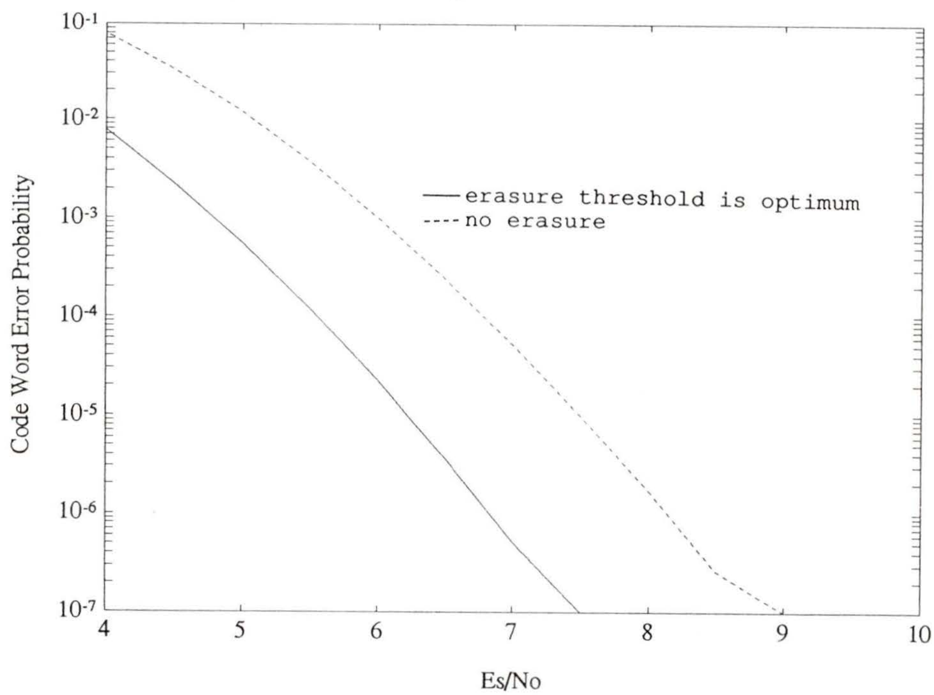

Figure 4.4: Codeword error probability of the (63,17) rate-adaptive RS code in a Rayleigh fading channel with side information. The optimum erasure threshold is considered

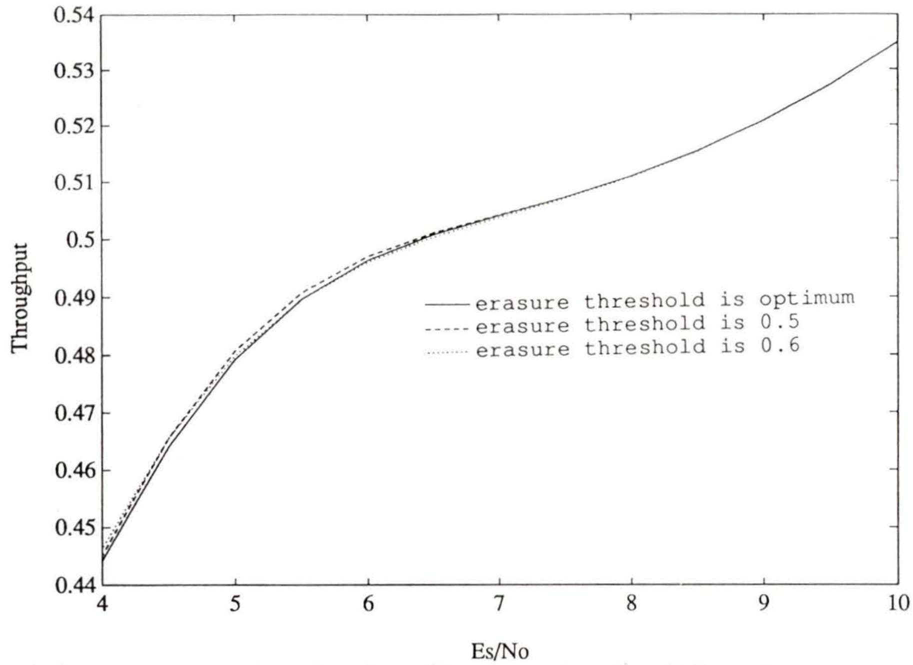

Figure 4.5: Throughput of the (63,17) rate-adaptive RS code in a Rayleigh fading channel with side information. The optimum erasure threshold, $T_s = 0.5$ and $T_s = 0.6$ are considered.

4.5 Conclusion

In this chapter, the rate-adaptive coding scheme presented in Chapter 2 is considered in a Rayleigh fading environment. It is assumed that side information, regarding channel amplitude, is available. A code symbol is erased if the channel amplitude during the symbol is below a certain threshold. The throughput and error probability for the channel with erasure is derived. As an example, it was shown that for (63,17) RS code, by applying this simple erasure criterion and using error/erasure decoding, 1 dB improvement is achievable (for the codeword error probability $P(E) = 10^{-5}$). This improvement in codeword error probability is obtained in addition to the improvement in throughput.

For error/erasure decoding, the threshold setting is not too critical. As we can

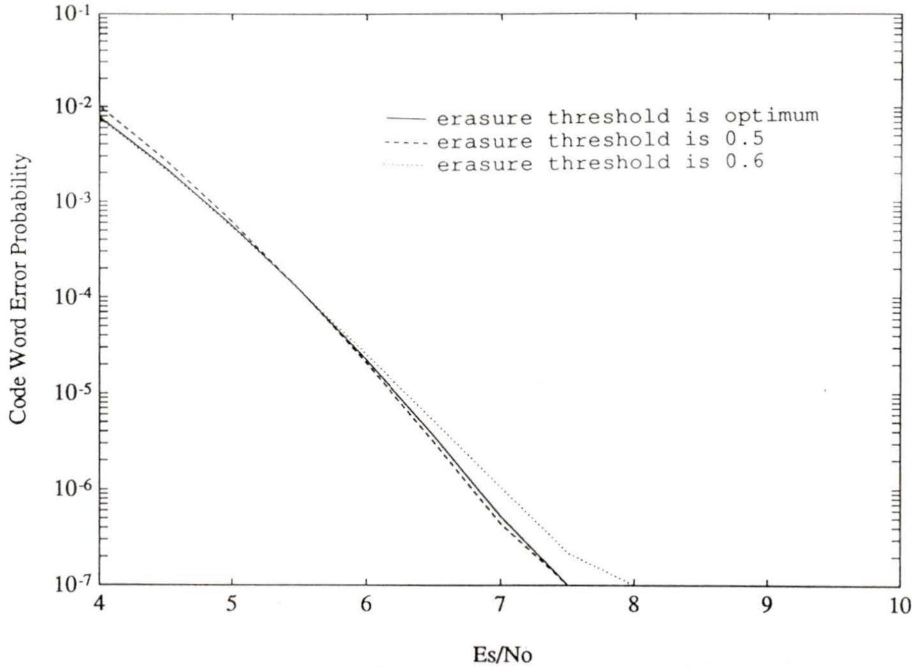

Figure 4.6: Codeword error probability of the (63,17) rate-adaptive RS code in a Rayleigh fading channel with side information. The optimum erasure threshold, $T_s = 0.5$ and $T_s = 0.6$ are considered.

see from Figures (4.5) and (4.6), for the optimum value of erasure threshold and $T_s = 0.5$, the performance is almost the same.

Chapter 5

A Rate-Adaptive Concatenated Coding Scheme

5.1 Introduction

Concatenation schemes, involving fixed-rate RS and convolutional codes, are well established [31]. These schemes are effective methods for communications in low SNR environments. In this chapter, we introduce a rate adaptive coding scheme based on the concatenation of RS and convolutional codes, and analyze its performance.

Consider the rate-adaptive coding scheme presented in Chapter 2. Assume that each codeword is broken down into two sub-blocks. If, after the second transmission, the decoder is still unable to recover the data, the first received sub-block is discarded and the third transmitted sub-block will be another copy of the first one.

In the concatenation scheme, the first and the third transmitted packets are not the same, but they form a code sequence in a 1/2 rate systematic convolutional code. In the same manner, the second and the fourth transmitted packets form a codeword in the 1/2 rate systematic convolutional code.

Since convolutional codes are used in this chapter, in the next section we look

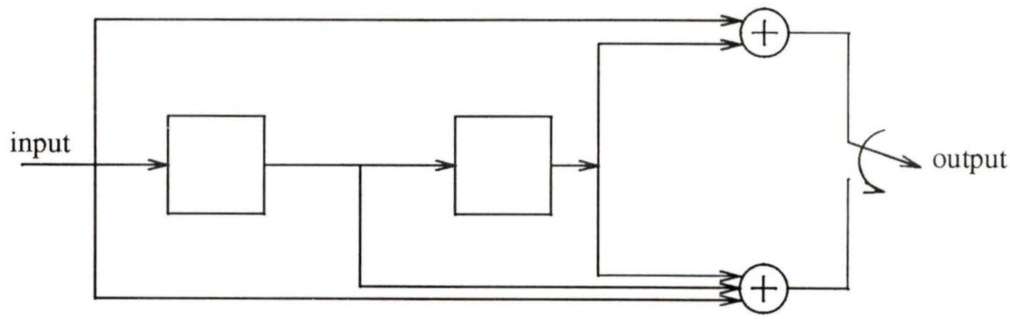

Figure 5.1: Encoder for a (2,1,2) convolutional code with octal generators (5,7).

at the convolutional codes and the Viterbi decoder.

5.2 Convolutional Codes and the Viterbi Decoder

A convolutional code is generated by passing the information, to be transmitted, through a linear finite state shift register. For the sake of simplicity, let us consider a 1/2 rate convolutional code. The shift register consists of m stages with the outputs of selected stages being added modulo-2 to form the encoded symbols. A simple example of a 1/2 rate convolutional encoder, with $m = 2$, which is denoted by (2,1,2), is given in Figure (5.1). Information bits are shifted in at the left, and for each information bit the outputs of modulo-2 adders provide two bits. The connections between the shift register stages and the modulo-2 adders are conveniently described by generator polynomials. The polynomials $g_1(x) = 1 + x^2$ and $g_2(x) = 1 + x + x^2$ represent the upper and lower connections in Figure (5.1), respectively. These connections can also be given by the generator functions $g_1 = (1\ 0\ 1)$ and $g_2 = (1\ 1\ 1)$, or more conveniently in octal form as (5,7).

One method to describe a convolutional code is the trellis diagram [32]. The trellis diagram for the code of Figure (5.1) is shown in Figure (5.2). When the encoded sequence is transmitted through the channel, due to the channel noise, the received sequence is different from the transmitted one. Therefore, the decoder should remove the noise and recover the transmitted data. The Viterbi algorithm [33] can be used to search for the most probable path as the transmitted sequence (the maximum-likelihood decoding (MLD)).

Consider the trellis structure shown in Figure (5.2). Let y_1^j and y_2^j denote the received symbols at time unit j (the received symbols corresponding to the branch j). The metric for the branch j is, in general, a measure of closeness of y_1^j and y_2^j to the transmitted symbols corresponding to that branch. Assuming a discrete memoryless channel, the path metric for each path is determined by adding the branch metrics on that path. Employing the Viterbi algorithm [33], the path with the largest metric is chosen as the correct path. Note that in each node, a number of paths are discarded and therefore the number of surviving paths are not increased. If the demodulator output for each transmitted bit is either 0 or 1, by using Viterbi algorithm, a hard decision decoding is performed. On the other hand, if at the output of the demodulator each transmitted bit is available in analog or quantized form, the decoder is called soft decision Viterbi decoder. Performance bounds for convolutional codes are given in [33] [34] [35] [36].

Since Viterbi algorithm is a maximum-likelihood decoder, by combining repeated packets, encoded with a code rate R, a lower code rate is obtained [10]. For example, by transmitting the encoded sequence in Figure (5.1) twice, a 1/4 rate convolutional code with a generator polynomial (5,7,5,7) will result. The trellis for this 1/4 rate convolutional code will be the same as Figure (5.2), with four bits on each branch

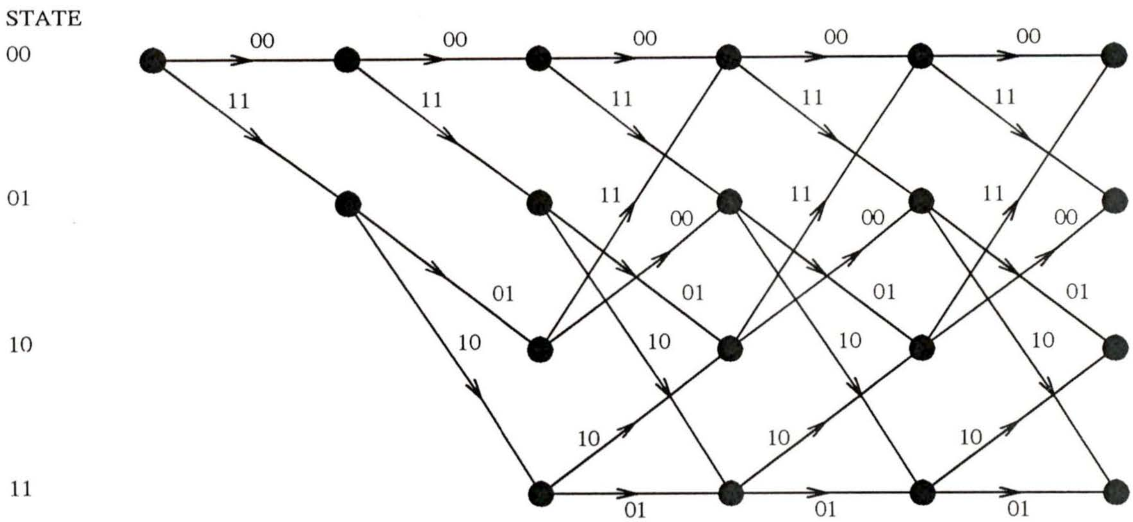

Figure 5.2: The trellis structure for a (2,1,2) convolutional code with generators (5,7).

(which is the repetition of two bits on each branch in Figure (5.2)). These repeated convolutional codes are usually good codes [10] [13], and this property makes the convolutional code a good choice for ARQ schemes.

5.3 Type II Hybrid ARQ Using Concatenated Coding Scheme

The block diagram for this scheme is shown in Figure (5.3). We assume a maximum of four transmissions for this scheme. This means, if after the fourth transmission, the received word is still detected in error, the incorrect data will be delivered to the user. Notice that in this scheme, ideal interleaving between the two codes is assumed.

Consider an (n, k) RS code over $GF(2^M)$, C_1, as the outer code, and a systematic, 1/2 rate, $(2, 1, m)$ convolutional code with the generator polynomials $(1\ ,\ g(x))$,

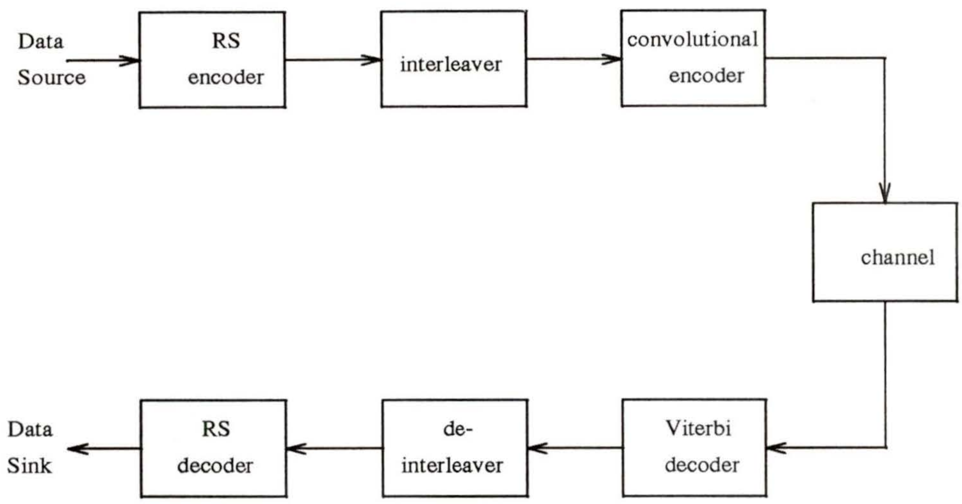

Figure 5.3: Concatenated Coding Scheme.

C_2, as the inner code. Let $k = n/2 - r$, where r is the space left for the error detection. When a message $M(x)$, $k \times M$ bits long, is ready for transmission, it is first encoded into a codeword in C_1, $I(x)$, with n symbols. We divide $I(x)$ into two sub-blocks. One sub-block, which is called $I_1(x)$, contains the first $n/2$ symbols of $I(x)$. The other sub-block, consists of the second $n/2$ symbols of $I(x)$, is called $I_2(x)$. Therefore, we can write $I(x) = [I_1(x)\ I_2(x)]$. The sequence $I_1(x)$ is then transformed to the sequence $P_1(x) = I_1(x)g(x)$, $k \times M$ bits long.[1] In the same way, the sequence $I_2(x)$ is transformed to the sequence $P_2(x) = I_2(x)g(x)$.

In the first transmission, $I_1(x)$ is transmitted. Let the received sequence corresponding to $I_1(x)$ be denoted by $I_1^1(x)$. If $I_1^1(x)$ is the same as $I_1(x)$, by using the outer decoder in the detection mode, $I(x)$ is recovered and delivered to the user.

[1] $P_1(x)$ is actually $k \times M + m$ bits long, where m is the number of known bits for clearing the memory of the encoder. Since $k \times M >> m$, we assume $k \times M + m \simeq k \times M$.

Note that in this situation, $I_1(x)$ will be a punctured codeword in C_1, and C_1 works in the detection-only mode. If $I_1^1(x)$ is detected in error, a NAK signal is sent to the transmitter and the second block, $I_2(x)$, is transmitted.

Let $I_2^1(x)$ denote the received packet after the second transmission. If $I_2^1(x)$ is the same as $I_2(x)$, $I(x)$ and therefore $M(x)$ is recovered and delivered to the user. Otherwise $I_1^1(x)$ and $I_2^1(x)$ are put together, $[I_1^1(x)\ I_2^1(x)]$, as a sequence of the outer decoder, and the outer decoder tries to recover the data, in the correction-only mode. If a decoding failure is declared, a NAK signal is sent to the transmitter, and $P_1(x)$ is transmitted.

Let $P_1^1(x)$ denote the received sequence in the third transmission. At this stage, $I_1^1(x)$ and $P_1^1(x)$ are interleaved together, as a received sequence of the $(2, 1, m)$ convolutional code. By using the Viterbi algorithm, this sequence is decoded to $I_1^2(x)$. If $I_1^2(x)$ is error-free, with the aid of the outer decoder, $I(x)$ is recovered. Otherwise, $[I_1^2(x)\ I_2^1(x)]$ form a code sequence of the outer decoder, and the outer decoder tries to decode this code sequence. Should the decoded sequence be detected in error, a NAK signal is sent to the transmitter and $P_2(x)$ is transmitted.

After the fourth transmission, $I_2^1(x)$ and $P_2^1(x)$ are interleaved together and are decoded as a sequence of C_2. Let $I_2^2(x)$ denote this decoded sequence. If $I_2^2(x)$ is error-free, by using the outer decoder, $I(x)$ is recovered. Otherwise, $I_1^2(x)$ and $I_2^2(x)$ are combined together and form a sequence of C_2, $[I_1^2(x)\ I_2^2(x)]$. This combined word will be decoded by the outer decoder and the decoded word, whether it is correct or not, is delivered to the user. Note that in this protocol, the error detection is done by the RS code.

In general, two or more separable codes can be concatenated to form a type II hybrid ARQ scheme such as the one described above. A codeword of a separable code can be broken into several parts each of which can be used in successive transmissions to recover the information. By properly concatenating codes with different properties, the scheme benefits from the advantages of all codes in the concatenation.

5.4 Performance Analysis

Let D, D_C^i and D_{RS}^i denote, respectively, the events " received block contains error", " after combining i received packet, the decoded sequence after the convolutional decoder still contains error" and "after the ith attempt by the RS decoder, the decoded block contains error". Consider the concatenation coding scheme. Define

$$T \;=\; 1 + P(D) + P(D, D, D_{RS}^1) + P(D, D, D_{RS}^1, D_C^2, D_{RS}^2). \tag{5.1}$$

Then T is the average number of transmissions for a given codeword, with a maximum of four transmissions. We can write

$$P(D, D, D_{RS}^1) = \sum_{e_1=1}^{n/2} \sum_{\substack{e_2 = 1 \\ e_1 + e_2 > t}}^{n/2} \binom{n'}{e_1}\binom{n'}{e_2} p_1^{e_1+e_2}(1-p_1)^{n-e_1-e_2}, \tag{5.2}$$

$$P(D, D, D_{RS}^1, D_C^2, D_{RS}^2) \leq P(D, D_C^2, D_{RS}^2), \tag{5.3}$$

where

$$P(D, D_C^2, D_{RS}^2) = \sum_{e_1=1}^{n/2} \sum_{\substack{e_2 = 1 \\ e_1 + e_2 > t}}^{n/2} \binom{n'}{e_1}\binom{n'}{e_2} p_1^{e_1} p_2^{e_2}(1-p_1)^{n/2-e_1}(1-p_2)^{n/2-e_2}. \tag{5.4}$$

Note that t is the error correction capability of the outer code, p_1 is the channel symbol error probability, and p_2 is the code symbol error probability after the $(2, 1, m)$ convolutional code.

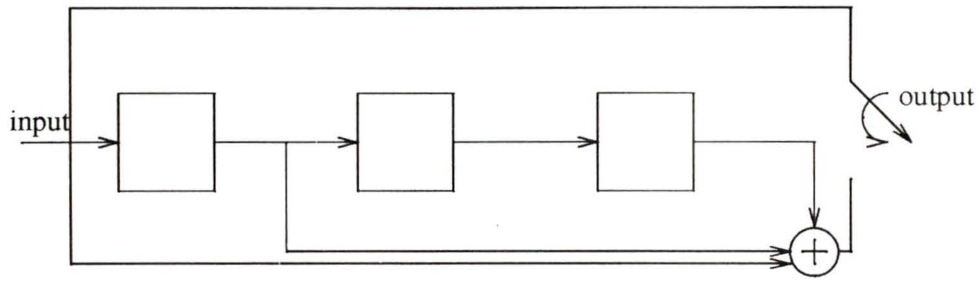

Figure 5.4: Encoder for (2,1,3) systematic convolutional code with generator function (10,15).

The codeword error probability, $P(E)$, is the same as the probability of retransmission after receiving the fourth block, or

$$P(E) = P(D, D, D_{RS}^1, D_C^2, D_{RS}^2, D_C^2, D_{RS}^3) \leq P(D_C^2, D_{RS}^2, D_C^2, D_{RS}^3), \tag{5.5}$$

where

$$P(D_C^2, D_{RS}^2, D_C^2, D_{RS}^3) = \sum_{e_1=1}^{n/2} \sum_{\substack{e_2 = 1 \\ e_1 + e_2 > t}}^{n/2} \binom{n'}{e_1}\binom{n'}{e_2} p_2{}^{(e_1+e_2)}(1-p_2)^{(n-e_1+e_2)}. \tag{5.6}$$

5.5 Examples

In this section, a shortened $(60, 26)$ RS code with symbols over $GF(2^6)$ is considered as the outer code, and a systematic $(2, 1, 3)$ convolutional code is considered as the inner code. The encoder for the inner code is shown in Figure (5.4). As we can see, this encoder has a generator function (10,15). The code symbol error probability in the first transmission, p_1, is given by Equation (4.8). Note that we consider perfect interleaving for channel symbols. p_2, the code symbol error probability after the (2,1,3) systematic convolutional code, is evaluated by simulation. The simulation result, for p_2, is given in Figure (5.5).

Note that a BPSK modulation with a coherent detection, and Viterbi decoder with both hard decision and soft decision with 8-level of quantization are assumed. The throughput and codeword error probability for a maximum of four transmissions, for each codeword, are shown in Figures (5.6) and (5.7), respectively. In these figures, the performance of the rate-adaptive RS code with code combining, presented in Chapter 2, is shown as well. In the case of an RS code with code combining, perfect interleaving for code symbols are considered. Therefore, the code symbol error probability is given by Equation (4.13), where $T_s = 0$. As we can see in Figure (5.7), at the codeword error probability $P(E) = 10^{-5}$, the concatenation scheme, with a hard decision decoding, has a 2 dB advantage over the scheme using an RS code and code combining. This improvement in codeword error probability is obtained in addition to the improvement in throughput. By applying soft decision to the Viterbi decoder, another 4 dB improvement, at $P(E) = 10^{-5}$, is achievable.

5.6 Conclusion

In this section, a rate-adaptive concatenation coding scheme is introduced. The scheme is based on the rate-adaptive RS code, as the outer code, and the convolutional code, as the inner code. The throughput and error probability for this scheme are derived. As an example, the scheme is applied to the Rayleigh fading channel and is compared to the system using only the rate-adaptive RS code. It is shown that, by using a 1/2 rate memory $m = 3$ systematic convolutional code (with hard decision decoding) in conjunction with a (60,26) RS code, a 2 dB improvement is

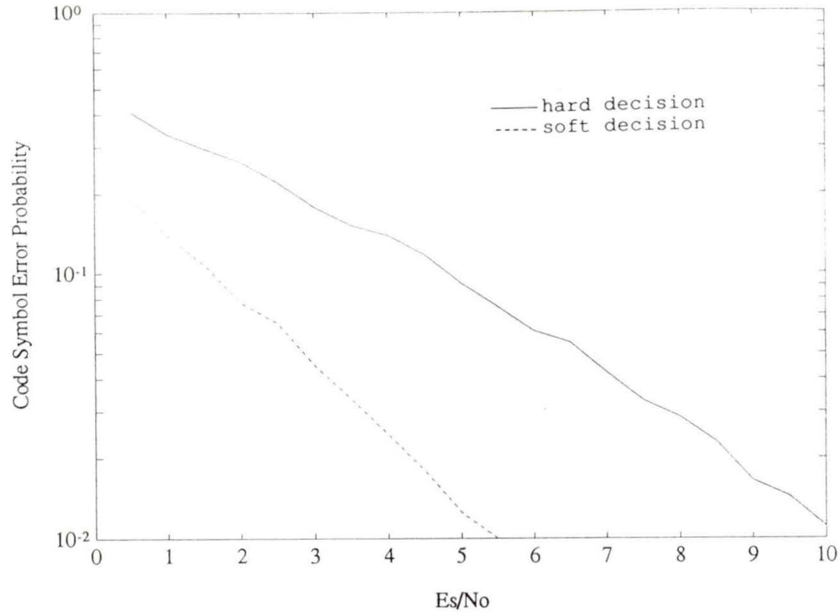

Figure 5.5: Simulation result for the code symbol error probability after the (2,1,3) convolutional code, with the generator function (10,15). Each code symbol consists of six channel symbols. BPSK with coherent detection is assumed.

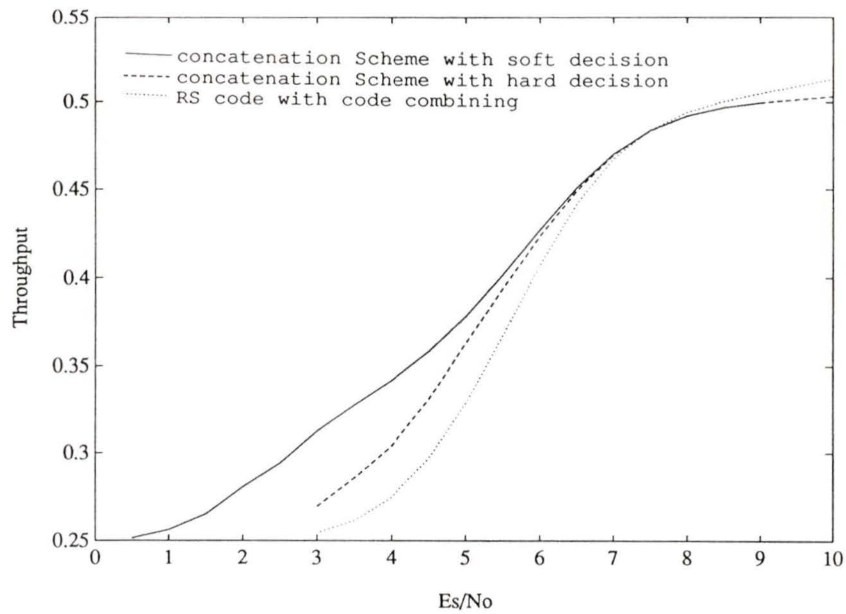

Figure 5.6: The throughput for the rate-adaptive concatenated coding scheme in a Rayleigh fading channel. A (60,26) RS code is considered with a (2,1,3) convolutional code.

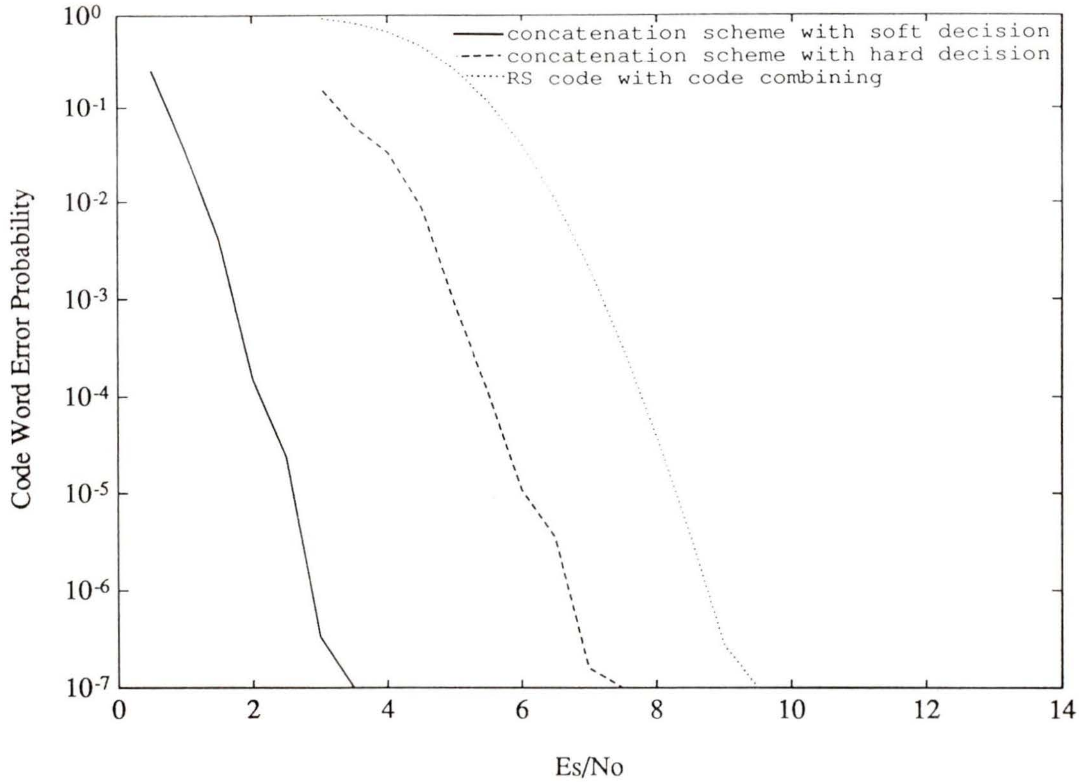

Figure 5.7: The codeword error probability for the rate-adaptive concatenated coding scheme in a Rayleigh fading channel. A (60,26) RS code is considered with a (2,1,3) convolutional code.

achievable, compared to a rate-adaptive RS code. It is also shown that applying soft decision to the Viterbi decoder has a 4 dB advantage over the hard decision decoding.

Chapter 6

Summary and Future Work

6.1 Summary

In this thesis, rate-adaptive coding was studied. A protocol based on maximum distance separable codes was developed and its performance was analyzed. In particular, the throughput and error probability were derived. In this scheme, after the first transmission, the code rate is very close to one. After the second transmission, the code rate is decreased to 1/2, and with the mth transmission, if it is necessary, the code rate is reduced to $1/m$. In this scheme, the block length for each transmission or retransmission is the same, and there is no need for another code for error detection. If the channel state and erasure information are available, this scheme is capable of dealing with erased symbols.

The new concept of using rate-adaptive coding in conjunction with spread spectrum multiple access was introduced. In particular, our scheme was employed to the frequency hopped spread spectrum multiple access. Also, the concept of rate-adaptive coding with a limited number of transmissions for each codeword was introduced. The throughput and error probability, in a multiple access environment, verses the number of simultaneous users were derived. It was shown that by using rate-adaptive coding in conjunction with a frequency hopped multiple access, the number of simultaneous users is increased by the adaptivity factor, compared to the frequency hopping using the fixed-rate coding. This increase is due to a higher throughput that results in less interference, which a user adds to the channel. This effect is similar to the effect of the voice activity factor. One should note that rate-adaptive coding, using block or convolutional codes, can also be applied to the direct sequence spread spectrum to increase the maximum number of simultaneous users.

The performance of the rate-adaptive coding (based on maximum distance separable codes) in a Rayleigh fading channel was analyzed. As we mentioned, this protocol is capable of dealing with erased symbols. It was shown that in a Rayleigh fading environment, if side information, regarding the channel amplitude, is passed to the decoder, the performance of the decoder is improved.

A rate-adaptive concatenated coding scheme was introduced. The scheme is based on an RS code, as the outer code, and a convolutional code, as the inner code. The performance of this scheme is analyzed for a Rayleigh fading channel, and is compared with the scheme introduced in Chapter 2.

6.2 Future Work

Since spread spectrum multiple access is a self-interference limited system, applying other rate-adaptive coding protocols to spread spectrum (frequency hopping or direct sequence) is a good topic for further research.

Passing the channel side information to the inner decoder and exchanging the reliability information between the two decoders can improve the system performance.

The exchange of reliability information has already been considered in literature for the fixed-rate concatenation scheme [37] [38] [39].

Bibliography

[1] K. S. Gilhousen, I. M. Jacobs, R. Padovani, A. J. Viterbi, L. A. Weaver, C. E. Wheatley, " On the Capacity of a Cellular CDMA System," *IEEE Trans. Veh. Tech.*, vol. 40, No. 2 pp 303-312, May 1991.

[2] Lin, S, Costello,Jr., D.J., and Miller, M.J.: " Automatic-repeat-request error-control schemes," *IEEE Commun. Mag.*, vol.22, No. 12, pp. 5-17, Dec. 1984.

[3] D. M. Mandelbaum, " Adaptive-Feedback Coding Scheme Using Incremental Redundancy," *IEEE Trans. Inform. Theory*, IT-20, pp. 388-389, May 1974.

[4] J. J. Metzner, " Improvements in Block-Retransmission Schemes," presented at *IEEE Int. Symp. Inform. Theory,* Ithaca, NY, Oct. 10-14, 1977.

[5] J. J. Metzner, " Improvements in Block-Retransmission Schemes," *IEEE Trans. Commun.*, COM-27, pp. 525-532, Feb. 1979.

[6] S. Lin and P. S. Yu, " A Hybrid ARQ Scheme with Parity-Retransmission for Error Control of Satellite Channels," *IEEE Trans. Commun.*, COM-30, No. 7, pp. 1701-1719, July 1982.

[7] Y. M. Wang and S. Lin, "Modified Selective Repeat Type II hybrid ARQ System

and It's Performance Analysis."*IEEE Trans. Commun.*, vol. COM-31, pp 593-608, May 1983.

[8] J. Du, M. Kasahara and T. Namekawa, "Separable Codes on Type-II ARQ Systems." *IEEE Trans. Commun.*, vol. 36, No.10, pp 1089-1097, October 1988.

[9] H. Krishna and S. D. Morgera, " New Error Control Scheme for Hybrid ARQ System, " *IEEE Trans. Commun.*, vol. COM-35, pp. 981-990, Oct. 1987.

[10] D. Chase, " Code Combining- A Maximum-Likelihood Decoding Approach for Combining an Arbitrary Number of Noisy packets," *IEEE Trans. Commun.*, Vol. COM-33, pp 385-393, May 1985.

[11] J. Hagenauer, " Rate-Compatible Punctured Convolutional Codes (RCPC codes) and Their Applications,"*IEEE Trans. Commun.*, vol. COM-36, pp. 389-400, Apr. 1988.

[12] S. Kallel and D. Haccoun, " Generalized Type II Hybrid ARQ Scheme Using Punctured Convolutional Coding," *IEEE Trans. Commun.*, vol 38, pp. 1938-1947, Nov. 1990.

[13] S. Kallel, "Analysis of a Type II Hybrid ARQ Scheme with Code Combining," *IEEE Tran. Commun.*, vol. 38, No.8, pp. 1133-1137 Aug. 1990.

[14] C. E. Shannon, " A Mathematical Theory of Communication," Bell Syst. Tech. J., 27, pp 379-423 (part I), 623-656 (part II), July 1948.

[15] S. B. Wicker, " Type-II Hybrid ARQ Protocols Using Punctured Reed-Solomon Codes." *Milcom Proc.* pp. 52.2.1.-52.2.6, 1991.

[16] S. B. Wicker, " Hybrid-ARQ Reed Solomon Coding in An Adaptive Rate System," *ICC Proc.* pp 45.5.1-45.5.5, 1989.

[17] R. E. Blahut, *Digital Transmission of Information,* Addison-Wesley 1990.

[18] R. J. McEliece and L. Swanson, " On the Decoder Error Probability for Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. IT-32, No. 5, September 1986.

[19] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error- Correcting Codes*, North-Holland, 1977.

[20] W. C. Y. Lee, " Overview of CDMA," *IEEE Trans. Veh. Tech.*, vol. 40, No. 2, pp 291-302, May 1991.

[21] R. E. Ziemer, R. L. Peterson, *Digital Communications and Spread Spectrum Systems*, Macmillan, 1985.

[22] J. M. Fraser, " Engineering aspects of TASI." Bell syst. Tech. J., vol. 38, pp. 353-365, Mar. 1959.

[23] E. A. Geraniotis and M. B. Pursley, " Error Probabilities for Slow Frequency-Hopped Spread-Spectrum Multiple Access Communications over Fading Channels," *IEEE Trans. Commun.*, Vol. COM-30, No.5, May 1982, pp 996-1009.

[24] M. K. Simon, " On the Probability Density Function of the Squared Envelope of a Sum of Random Phase Vectors." *IEEE Trans. Commun.*, vol. COM-33, No.9, pp 993-996 Sep. 1985.

[25] P. Z. Peebles *Probability, Random Variables, and Random Signal Principals*, Second Edition, McGraw-Hill, 1987.

[26] A. Papoulis, *Probability, Random Variables and Stochastic Processes*, Second Edition, McGraw-hill 1984.

[27] Q. Wang and Y. Chao, " Frequency Hopped Multiple Access Communications with Coding and Side Information," *IEEE Journal Select. Areas commun.*, vol 10, No. 2, pp 317-327 Feb. 1992.

[28] J. Hagenauer, E. Lutz, " Forward Error Correction Coding for Fading Compensation in Mobile Satellite Channels." *IEEE Tran. Selected Areas commun.*, vol. Sac-5, N0. 2, pp 215-225 Feb. 1987.

[29] J. G. Proakis, *Digital Communications*, McGraw-Hill, 1983.

[30] A. Papoulis, *Probability, Random Variables and Stochastic Processes*, Second Edition, McGraw-hill 1984.

[31] J. P. Odenwalder, " Optimum Decoding for Convolutional Codes," Ph.D. dissertation, Univ. California, Los Angeles, 1970.

[32] G. C. Clark, Jr., J. B. Cain, " Error-Correction Coding for Digital Communications," Plenum Press, 1981.

[33] A. J. Viterbi, " Error bounds for Convolutional codes and an Asymptotically Optimum Decoding Algorithm," *IEEE Trans. Info. Theory,* vol IT-13, pp. 260-269, April 1967.

[34] A. J. Viterbi " Convolutional Codes and Their Performance in Communication Systems," *IEEE Trans. Commun.*, vol. COM-19, pp. 751-772, Oct. 1971.

[35] A. J. Viterbi and J. K. Omura, *Principles of Digital Communication and Coding.* New York: McGraw Hill, 1979.

[36] J. Hagenaure, " Viterbi Decoding of Convolutional Codes for Fading and Burst Channel," in *Proc. 1980 Zurich Seminar Digital Commun.*, IEEE Cat. No. 80 CH 1521-4 Com., pp. G2.1-G2.7.

[37] L. N. Lee, " Concatenated Coding Systems Employing a Unit-Memory Convolutional Code and Byte-Oriented Decoding Algorithm." *IEEE Trans. Commun.*, vol. COM-25, pp. 1064-1074 Oct. 1977.

[38] R. H. Deng, D. J. Costello, "High Rate Concatenation Coding Systems Using Band Width Efficient Trellis Inner Codes." *IEEE Trans. Commun.*, vol. 37, No. 5, pp. 420-427 May 1989.

[39] E. Paaske, " Improved Decoding for a Concatenated Coding System Recommended by CCSDS."*IEEE Trans. Commun.*, vol. 38, No. 8, pp. 1138-1144 Aug. 1990.

Appendix

The Derivation of Equations (2.13) and (4.17)

Equation (2.13) is derived by modifying the analysis in [16]. Considering an (n, k) RS code, without loss of generality we assume that the all zero code word is transmitted.

Let $p(j, h)$ be the probability that the received word lies at a distance h from a particular weight-j code word, which we call J. There are four cases to be considered in order to calculate $p(j, h)$.

1. Among the h positions in which J and the received word differ, r of them correspond to zeros in J and non-zeros in the received word. Therefore, among the j non-zero positions in J, there are $h - r$ positions at which J and the received word differ.

2. From these $h - r$ positions, i of them correspond to non-zeros of J and zeroes in the received word.

3. $h - r - i$ positions corresponding to non-zeros in J and non-zeros in received word, but different with each other.

4. The remaining case occurs when the symbols of J and the received word coincide.

By counting all the possibilities, we obtain:

$$p(j,h) = \sum_{r=0}^{h}\sum_{i=0}^{h-r} \binom{n-j}{r}\binom{j}{h-r}\binom{h-r}{i}(2^m-1)^{i-j}(2^m-2)^{h-r-i}p_e^{j+r-i}(1-p_e)^{n-j-r+i}. \quad (A.1)$$

With a similar logic the probability that the received word ,with length n, has s erased symbols and falls within distance h of a particular weight j codeword, $p(j,h,n,s)$, is given by

$$\begin{aligned} p(j,h,n,s) &= \sum_{r=0}^{h}\sum_{i=0}^{h-r} \binom{n-s-j}{r}\binom{j}{h-r}\binom{h-r}{i}\binom{n}{s}(2^m-1)^{i-j}(2^m-2)^{h-r-i} \times \\ & \quad p_e^{j+r-i}(1-p_e-p_s)^{n-s-j-r+i}p_s^s. \end{aligned} \quad (A.2)$$

VITA

Surname: Yousef Bigloo | Given Names: Amir Masoud

Place of Birth: Tehran, Iran | Date of Birth: December 14, 1961

Educational Institutions Attended:

University of Victoria, Canada	1990 to 1992
Tehran University, Iran	1979 to 1988

Degrees Awarded:

B.Eng.	Tehran University, Iran	1988

Publications:

1)A. M. Y. Bigloo, Q. Yang, Q. Wang and V. K. Bhargava, " A Robust Rate-Adaptive Hybrid ARQ Scheme for Nonstationary Channels," in Proc. *16th Biennial Symposium on Communications,* Kingston, Ont. pp 123-126, May 1992.

2)A. M. Y. Bigloo, Q. Wang and V. K. Bhargava, " A Robust Rate-Adaptive Hybrid ARQ Scheme and Frequency Hopping for Multiple-Access Communication Systems," to be persented at *IEEE Globecom'92*, Orlando, Florida, U.S.A., December 6-9, 1992.

3)A. M. Y. Bigloo, Q. Wang and V. K. Bhargava, " A Robust Rate-Adaptive Hybrid ARQ Scheme and Frequency Hopping for Multiple-Access Communication Systems," submitted to *IEEE Journal Select. Areas commun.*

Title of Thesis :

RATE ADAPTIVE CODING AND ITS APPLICATION TO SPREAD SPECTRUM COMMUNICATIONS

Author: [redacted]

Amir Masoud Yousef Bigloo

September 9, 1992