Performance of Reed–Solomon Coded Frequency-Hop Spread-Spectrum Communications in Partial-Band Interference

MICHAEL B. PURSLEY, FELLOW, IEEE, AND WAYNE E. STARK, MEMBER, IEEE

Abstract—This paper is concerned with the performance of a communications system which utilizes frequency-hop spread spectrum, diversity transmission, Reed–Solomon coding, and parallel error-correction and erasure-correction decoding. Both binary signaling and M-ary orthogonal signaling are considered. The goals are twofold. First, it is desirable to provide good performance in partial-band Gaussian noise interference by use of coding and diversity with an efficient error-correction algorithm. Second, it is necessary to totally neutralize narrow-band interference (regardless of the power level or statistical distribution of the interference) in order to have an effective spread-spectrum system. Through an analysis of the effects of partial-band interference on a frequency-hop spread-spectrum system with diversity, it is shown that the use of Reed–Solomon coding with a parallel errors and erasures decoding algorithm accomplishes these goals.

The paper also investigates the accuracy of the Chernoff bound as an approximation to the true performance of a frequency-hop spread-spectrum communication system with diversity, side information, M-ary orthogonal signaling, and Reed–Solomon coding. The performance results presented in the paper are based on analysis and computer evaluation. Approximate results based on the Chernoff bound are also given. It is shown that the Chernoff bound for M-ary orthogonal signaling gives a very poor approximation for many cases of interest. This is largely due to the looseness of the union bound.

I. INTRODUCTION

FREQUENCY-hop communication systems require a proper combination of spread-spectrum modulation, error-control coding, diversity, and decoding method in order to perform well in the presence of partial-band interference. The individual elements of such a system are well documented in the literature on frequency-hop spread spectrum (e.g., [1]–[6]). In particular, the use of coding, orthogonal modulation, and diversity is discussed in [6] and [4], and decoding approaches for enhancing protection against partial-band or pulsed interference are described in [3] and [7]. This paper presents quantitative results on the performance of a system which uses the combination of modulation, coding, and decoding that was first described in [3].

One of the primary applications is to provide effective antijam (AJ) communications against a partial-band jamming threat. One measure of the antijam capability is the minimum fraction of the band ρ^* that must be jammed in order for the

bit error probability to be above some desired value. Reed–Solomon codes can be utilized in a standard error-correction role to provide some AJ capability. If it is possible to obtain reliable side information to tell the decoder which of the received symbols have been jammed, the Reed–Solomon coding can be made considerably more effective (increased value of ρ^*) by erasing jammed symbols and employing a decoding technique that will correct erasures. However, it is not sufficient to correct only erasures since in the presence of full-band interference, all symbols will be erased. This is the reason for our use of the parallel decoding approach of [3] which will correct erasures due to partial-band interference or errors due to full-band interference.

Besides having a large value of ρ^*, it is also desirable that the system perform well in the presence of partial-band *Gaussian* noise. The performance in the presence of partial-band Gaussian noise is measured by the minimum signal-to-noise ratio (ENR*) needed for the bit error probability to be below the desired value. In order to provide reasonable performance in this case, we employ M-ary orthogonal signaling (such as modulating a carrier by a set of orthogonal baseband signals) as the form of modulation. This, however, uses more bandwidth (signal dimensions) than binary signaling. Because of this, for a fixed information rate and bandwidth, the Reed–Solomon code rate must be larger with M-ary orthogonal signaling than with binary signaling.

The outline of the paper is as follows. In Section II, we describe in detail the parallel errors and erasures decoding technique we are considering for Reed–Solomon codes. In Section III, we derive the Chernoff bounds for the error probability of binary orthogonal signals with diversity L in partial-band Gaussian noise. In order to apply this to M-ary orthogonal signaling, we make use of the union bound also, which we will call the union-Chernoff bound. This bound was employed in [6] for the analysis of the performance of a system with convolutional coding, diversity, and partial-band jamming and has been widely used subsequently in the evaluation of bit error probabilities. We compare this bound to the exact error probability of M orthogonal signals with diversity L in partial-band Gaussian noise which is derived in Section IV. The expressions obtained are based on those given by Lindsey [8] for the error probability with white Gaussian noise. As in the white Gaussian noise case, it is not possible to give closed-form solutions for the bit error rate. However, by use of numerical integration methods, we have evaluated the expressions for error probabilities in a diversity system with orthogonal modulation. In Section V, we examine the error probability of the parallel decoding technique described in Section II for orthogonal signals and a class of nonorthogonal signals (only orthogonal signals were considered in [9]). We derive an expression for the error probability of this signaling/decoding scheme under the assumption that the probability that the decoder incorrectly decodes (i.e., the decoder error) is negligible compared to the probability of decoder failure. From this, we derive the upper bounds stated in [9]. Finally, in Section VI, we

present the numerical results for several different combinations of codes and modulation. We show that the decoding approach, when used in conjunction with a proper combination of frequency hopping, diversity transmission, and side information, renders the narrow-band jammer harmless and requires a modest signal-to-noise ratio in the presence of Gaussian noise. As an example, a (256, 200) Reed-Solomon code with diversity 5 and 16-ary orthogonal signaling requires over 68 percent of the band to be jammed and a signal-to-noise ratio below 6.81 dB in order for the error probability to be above 10^{-4}.

II. Decoding Algorithm

The decoding approach we consider was introduced in [3], and the reader should consult [3] and [7] for related results on its performance. In this paper, we provide a more detailed description and analysis of the algorithm.

The output of the (n, k) Reed–Solomon encoder is a block of n symbols from an M-ary alphabet. For the codes considered in the present paper, n and M are equal, and they are a power of two. If diversity is employed, each symbol is transmitted L times (and interleaving of the diversity symbols may be used). We assume that the channel is noise free except for the jammer. This is a realistic assumption for a communication system operating in a high-power AJ mode. The results presented are indicative of the performance obtainable on a channel in which there is additional low-level background noise, and only minor modifications would need to be made to the implementation and the analysis.

The demodulation/decoding system is shown in Fig. 1. The signal is first dehopped and demodulated. The output of the dehopper is a sequence of L diversity receptions for each of the n code symbols. Side information regarding the presence of interference is extracted from the dehopper and demodulator, and the L diversity receptions of a given symbol are employed along with the side information to form the decision statistic. The side information is used to attach flags to unreliable diversity receptions. The diversity combiner forms the square-law combination of all unflagged diversity receptions. If at least one of the diversity receptions is not flagged, the decision device is presented with a noise-free symbol. In the event that all of the diversity receptions of a particular symbol have been flagged, the diversity combiner output is the square-law combination of *all* L diversity receptions and the decision device is presented with a noisy symbol. A (hard) M-ary decision must be made on the symbol, and this decision is fed into the error-correction decoder. For any symbol in which all diversity receptions are flagged, the erasure-correction decoder sees only an erasure.

An (n, k) Reed-Solomon code will correct up to $e \triangleq n - k$ erasures out of n symbols or up to $t \triangleq \lfloor (n - k)/2 \rfloor$ errors out of n symbols. More generally, it will correct any combination of ϵ erasures and τ errors provided that $2\tau + \epsilon$ does not exceed $n - k$, and in practice, the erasure-correction decoder of Fig. 1 should probably correct a small number of errors that might be caused by low-level background noise or other interference on the channel. However, the performance results that we present are for the simpler system consisting of errors-only decoding in parallel with erasures-only decoding.

The input to the error-correction decoder contains no erasures; it is a sequence of M-ary symbols from the output of the decision device. The input to the erasure-correction decoder has an erasure in each position where all diversity receptions are flagged, and an M-ary symbol in each position where at least one diversity reception is not flagged. The erasure system counts how many erasures it makes, and if the number does not exceed e, the erasure-correction decoding algorithm produces the correct answer. The erasure-correction decoder does not attempt to decode if the number of erasures exceeds e. If there are too many erasures, the erasure-correction decoder defaults to the error-correction decoder. The
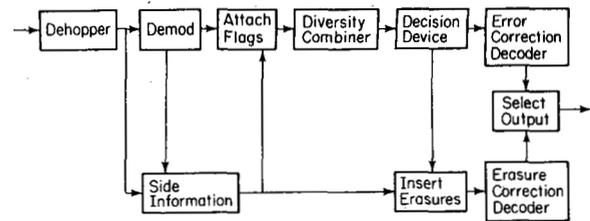

Fig. 1. Demodulator/decoder block diagram.

error-correction decoder is continually receiving the output of the decision device and attempting to decode. Most of the time it can decode, and its output will agree with the output of the erasure-correction decoder. An important property of bounded distance decoding of Reed-Solomon codes is that with high probability, it will default rather than decode into an incorrect codeword when the number of errors exceeds t. Thus, with high probability, the receiver will know if the two decoders have decoded correctly or not.

III. Union-Chernoff Bounds

We first consider M-ary orthogonal signaling in the presence of additive white Gaussian noise with (two-sided) spectral density $N_0/2$. The signal set is denoted by $\{s_i : 0 \leq i \leq M - 1\}$. Each signal has an energy E_d. A signal is sent by transmitting it L times on L different frequency hops where L is called the order of the diversity or the diversity level. We consider square-law combining of the L corresponding outputs of the optimum noncoherent detector. Thus, if the signal s_0 is sent, the receiver decision statistics are

$$R_0 = \left[\sum_{m=1}^{L} (X_{0,m} + v)^2 + (Y_{0,m})^2 \right]^{1/2} \tag{1}$$

and

$$R_i = \left[\sum_{m=1}^{L} (X_{i,m})^2 + (Y_{i,m})^2 \right]^{1/2} \tag{2}$$

for $1 \leq i \leq M - 1$ where $v^2 = 2E_d/N_0$. The $2ML$ random variables $\{X_{i,m}, Y_{i,m} : 1 \leq m \leq L, 0 \leq i \leq M - 1\}$ are mutually independent, zero-mean, unit-variance Gaussian random variables. The positive square root is assumed in (1) and (2) so $R_i \geq 0$ for each i.

The total energy required to transmit the L diversity repetitions of the signal is LE_d. If an (n, k) Reed–Solomon code (alphabet size M) is employed, the energy per information bit is

$$E_b = nLE_d/k(\log_2 M).$$

In this paper, we consider only the extended Reed-Solomon codes, so the block length is $n = M$ (see [10] for a description of these codes).

Consider the conditional probability of error given that s_0 is sent. This probability can be written as

$$P_e = P(R_0 < \max\{R_1, R_2, \cdots R_{M-1}\}) \tag{3}$$

where this and all subsequent probabilities are to be interpreted as conditional probabilities given that s_0 is sent. Since the random variables $\{R_i : 1 \leq i \leq M - 1\}$ are identically distributed, the union bound gives

$$P_e \leq (M - 1)P(R_0 < R_1).$$

For convenience, define $U = R_0^2$, $V = R_1^2$, and $Z = V - U$,

so that the bound on the probability of error is

$$P_e \leqslant (M - 1)P(Z > 0).$$

Applying the Chernoff bound to $P(Z > 0)$. we have

$$P_e \leqslant (M - 1)M_Z(s) \tag{4}$$

where $M_Z(s) = E\{e^{sZ}\}$ is the moment generating function for the random variable Z. This can be written in terms of the moment generating functions for U and V as

$$P_e \leqslant (M - 1)M_U(-s)M_V(s). \tag{5}$$

It is generally assumed for this decision statistic that the factor of 1/2 improvement in the Chernoff bound (originally suggested by Jacobs [11]) can be applied. This improved upper bound has been used in [6] and several subsequent papers. For the specific problem that we are considering, Levitt has shown in an unpublished manuscript that the factor of 1/2 can indeed be applied. Notice that the receiver under construction is not the maximum likelihood receiver, but it turns out that whether or not the receiver makes a maximum likelihood decision has very little to do with the applicability of the factor of 1/2. The improved version of (5) is

$$P_e \leqslant \frac{1}{2}(M - 1)M_U(-s)M_V(s). \tag{6}$$

Define two functions $g(s)$ and $h(s)$ as

$$g(s) = E\{\exp [s(X_{0,0} + v)^2]\}$$

and

$$h(s) = E\{\exp [s(Y_{0,0})^2]\}.$$

Then the fact that the random variables $\{X_{i,m}, Y_{i,m}: 1 \leqslant m \leqslant L, 0 \leqslant i \leqslant M - 1\}$ are independent and identically distributed implies that

$$M_U(-s)M_V(s) = [h(s)]^{2L}[g(-s)h(-s)]^L.$$

The moment generating functions $g(s)$ and $h(s)$ are given by

$$g(s) = (1 - 2s)^{-1/2} \exp \{sv^2/(1 - 2s)\}$$

and

$$h(s) = (1 - 2s)^{-1/2}$$

for $s < 1/2$. The resulting bound is

$$P_e \leqslant \frac{1}{2}(M - 1) \left[\frac{\exp \{-sv^2/(1 + 2s)\}}{(1 - 4s^2)} \right]^L \quad 0 < s < 1/2. \tag{7}$$

The bound of (7) applies to communication in the presence of additive white Gaussian noise with spectral density $N_0/2$. The dependence on the spectral density is via the parameter $v = (2E_d/N_0)^{1/2}$. The noise due to a partial-band jammer does not have a constant spectral density across the frequency band. Rather, the spectral density is $N_0/2$ in the portion of the band that is jammed, and it is zero elsewhere. If ρ denotes the fraction of the total band that is being jammed and W denotes the (one-sided) bandwidth of the frequency-hopping signal, then the partial-band noise has total power $\rho W N_0$. Thus, the average spectral density across the band is $N_J/2$ where N_J is defined by $N_J = N_0 \rho$. Looking at this another way, the partial band jammer has a total power of $W N_J$, but this amount of power can be concentrated in any subband. For a subband which is a fraction ρ of the total band, the spectral density $N_0/2$ in this subband must be such that $(\rho W)N_0 = W N_J$.

For application of (7) to partial-band noise jamming, the parameter v is given by

$$v = (2E_d \rho/N_J)^{1/2}$$

$$= \{2(E_b/N_J)\rho k(\log_2 M)/nL\}^{1/2}. \tag{8}$$

When the signal is transmitted in a jammed frequency slot, the error probability is bounded as in (7), and this happens with probability ρ if the frequency-hopping pattern is random or the jammer randomly chooses the frequency slots to be jammed. Thus, the bound on the probability of error for frequency-hop communication in the presence of partial-band jamming is

$$P_e \leqslant \frac{1}{2}(M - 1)\rho^L(1 - 4s^2)^{-L} \exp \{-sLv^2/(1 + 2s)\} \tag{9}$$

for $0 < s < 1/2$ where v is given by (8). This bound is valid for any s in the interval $(0, 1/2)$, but we wish to select the value of s to make the bound as tight as possible. The optimum value of s is

$$s = \{-4 - v^2 + [16 + 24v^2 + v^4]^{1/2}\}/16. \tag{10}$$

The above bound on the symbol error probability is easily converted to a bound on the bit error probability by using results of [10] on the bit error probabilities for extended Reed-Solomon codes.

IV. SYMBOL ERROR PROBABILITY WITH DIVERSITY

In this section, we derive an exact expression for the symbol error probability of the decision device defined by (3). As mentioned previously, we consider M-ary orthogonal signaling, diversity level L, and noncoherent detection. The derivation of the error probability is based on the work of Lindsey [8] in which the error probability for M orthogonal signals with diversity level L is derived for additive white Gaussian noise and Rician fading.

Since we are assuming that side information is available and that there is no background noise, the only way an error can occur is if the jammer hits every diversity transmission. This happens with probability ρ^L. Given that each diversity transmission has been jammed, the error probability can be calculated using results of Lindsey [8].

In order to compute the error probability in (3), we first consider the random variables $\{Z_i: 0 \leqslant i \leqslant M - 1\}$ defined by $Z_i = R_i^2/2, 0 \leqslant i \leqslant M - 1$. The error probability is then the same as (3) with R_i replaced by Z_i. In order to evaluate the error probability, the conditional densities of the random variables $Z_i, 0 \leqslant i \leqslant M - 1$ must be determined. Given that symbol 0 was transmitted, the density of Z_0 is given by

$$p_{Z_0}(z_0) = \left(\frac{z_0}{\Lambda}\right)^{(L-1)/2} \exp (-z_0 + \Lambda)I_{L-1}(\sqrt{4z_0\Lambda}) \tag{11}$$

where

$$\Lambda = LE_d\rho/N_J. \tag{12}$$

The conditional density of Z_k given that symbol 0 was transmitted is

$$p_{Z_k}(z_k) = \frac{z_k^{L-1}}{(L - 1)!} e^{-z_k} \tag{13}$$

for $k \neq 0$. The probability of an error is then

$$P_e(L, \rho) = \rho^L \text{Prob} \{Z_k > Z_0 \text{ for some } k \neq 0\}. \tag{14}$$

This is given by

$$P_e(L, \rho)$$

$$= \rho^L [1 - \text{Prob} \{Z_0 > Z_k \text{ for all } k \neq 0\}]$$

$$= \rho^L \left[1 - \int_0^\infty p_{Z_0}(z_0) \left[\int_0^{z_0} p_{Z_k}(z_k) \, dz_k \right]^{M-1} dz_0 \right]$$

$$= \rho^L \left[1 - \int_0^\infty p_{Z_0}(z_0) \left(1 - \sum_{m=0}^{L-1} \frac{z_0^m}{m!} e^{-z_0} \right)^{M-1} dz_0 \right]$$

$$(15)$$

where $p_{Z_0}(z_0)$ is given in (11). When $M = 2$, the integral in (15) can be evaluated to be

$$P_e(L, \rho) = \rho^L \left[\frac{1}{2} \exp \left\{ -\frac{E_d L \rho}{2N_J} \right\} \sum_{i=0}^{L-1} \frac{(E_d L \rho / 2N_J)^i}{i!(L+i-1)!} \right.$$

$$\left. \cdot \sum_{j=i}^{L-1} \frac{(j+L-1)!}{(j-i)!2^{j+L-1}} \right], \qquad (16)$$

which for $\rho = 1$ is a standard result [12, p. 34] of Marcum for an additive white Gaussian noise channel.

In (15) and (16), the error probability is given as a function of the fraction of the band being jammed. It easy to see that the integral in (15) and the expression in (16) depend on N_J, E_d, and ρ only through the ratio $E_d \rho / N_J$. The jammer may choose ρ to maximize the error probability. In this case, the worst case error probability is given by

$$P_e(L) = \max_{0 < \rho \leq 1} P_e(L, \rho). \qquad (17)$$

The maximum in (17) can be calculated to be

$$P_e(L) = \begin{cases} P_e(L, 1) & E_d/N_J < A_{L,M} \\ \dfrac{B_{L,M}}{(E_d/N_J)^L} & E_d/N_J \geq A_{L,M} \end{cases} \qquad (18)$$

where $A_{L,M}$ and $B_{L,M}$ are constants. The optimal jamming fraction ρ is given by

$$\rho = \begin{cases} 1 & E_d/N_J < A_{L,M} \\ \dfrac{A_{M,L}}{E_d/N_J} & E_d/N_J \geq A_{L,M}. \end{cases} \qquad (19)$$

Numerical results for the constants in (18) and (19) may be found in [13].

V. CODED ERROR PROBABILITY

In this section, we consider the bit error probability of the output of the decoder described in Section II. We obtain an analytical expression for the output bit error probability in terms of the error and erasure probabilities, rather than rely on the upper bounds that we employed in [9]. Two different modulation schemes are considered. The first scheme utilizes binary FSK with one M-ary symbol per hop. The M-ary sym-

bol is formed from a sequence $m = \log_2 M$ binary FSK tones, so that the resulting M-ary signals are *not orthogonal* (this signal set has dimension $\log_2 M$). For the partial-band jamming model considered in this paper, either all m bits representing a given symbol are jammed or else none of them is jammed. The second type of modulation considered is M-ary orthogonal signaling such as MFSK or M-orthogonal baseband signals modulating a carrier. Such a signal set has dimension M. We shall see that the analyses for these two different modulation schemes have much in common.

For the analysis presented in this section, we will assume that there is no background noise and that perfect side information is available. Furthermore, we assume that the interference is white Gaussian noise over the full band of a frequency slot when there is a hit. (For MFSK, a frequency slot includes all M possible tones.) The results can easily be extended to include imperfect side information and nonzero background noise. Assuming that perfect side information is available, the probability of each diversity transmission of an M-ary symbol being jammed is ρ. Since all L diversity transmissions of a particular symbol must be jammed in order for that symbol to have nonzero error probability, the probability of a channel symbol error is the probability of a symbol error given that all L diversity transmissions were jammed times ρ^L. The decoder consists of an erasure-correction decoder and an error-correction decoder. When a symbol is jammed, the input to the erasure-correction decoder for that symbol becomes an erasure, while the input to the error-correction decoder is the demodulated symbol. To determine the decoded error probability, we will need to compute the (conditional) error probability $\hat{P}_e(L, \rho)$ given that a symbol is jammed. For binary FSK signaling (the first scheme), the error probability is given by

$$\hat{P}_e(L, \rho) = 1 - [1 - P_2]^m \qquad (20)$$

where

$$P_2 = \frac{1}{2} \exp \left\{ -\frac{E_d L \rho}{2N_J} \right\} \sum_{i=0}^{L-1} \frac{(E_d L \rho / 2N_J)^i}{i!(L+i-1)!}$$

$$\cdot \sum_{j=i}^{L-1} \frac{(j+L-1)!}{(j-i)!2^{j+L-1}}. \qquad (21)$$

For M-ary orthogonal signaling, the error probability is

$$\hat{P}_e(L, \rho) = 1 - \int_0^\infty p_{Z_0}(z_0) \left(1 - \sum_{m=0}^{L-1} \frac{z_0^m}{m!} e^{-z_0} \right)^{M-1} dz_0.$$

$$(22)$$

Notice that (21) is the same as (16) and (22) is the same as (15) without the factor ρ^L.

Since an (n, k) Reed–Solomon code can correct up to $e = n - k$ erasures, the output of the combined decoder will be the output of the erasure-correction decoder if there are no more than e erasures. If more than e erasures are present, the combined decoder will take the output of the error-correction decoder. The error-correction decoder will be able to correct up to $t = \lfloor (n - k)/2 \rfloor$ errors. If more than t errors occur, then the decoder will (with high probability) recognize that the number of errors exceeds the error-correction capability of the decoder and the output is just the demodulated information symbols of the received signal. That is, the probability that the decoder fails to decode is much greater than the probability it decodes into the wrong codeword [10], [14]. If the latter

probability is neglected, the probability of a symbol error at the decoder output is derived as follows.

First, the symbol is always correct if no more than $n - k$ erasures occur in the decoder input. This is due to the assumption of perfect side information and no background noise. If more than $n - k$ erasures occur, the output of the combined decoder will be the output of the error correction decoder. A decoding failure will occur if the number of errors in the received vector is greater than the error-correcting capability of the code. Let $E_{s,i}$ be the event that the first symbol of the received vector is in error, let $E_{s,o}$ be the event that the first symbol of the decoder output is in error, let E_j be the event that j of the last $n - 1$ symbols are jammed, and let $\hat{E}_l$ be the event that l symbol errors occur in the last $n - 1$ symbols of the received vector.

We can write the decoded symbol error probability as the probability that the first symbol is received in error, at least e of the remaining $n - 1$ symbols were jammed, and at least t of these jammed symbols were received in error, that is,

$$P(E_{s,o}) = P\left\{E_{s,i} \cap \left(\bigcup_{j=e}^{n-1} E_j\right) \cap \left(\bigcup_{l=t}^{n-1} \hat{E}_l\right)\right\}.$$

We note the following facts about the events $E_{s,o}$, E_j, and $\hat{E}_l$. First, $E_{s,o}$ is independent of the events E_j and $\hat{E}_l$. Next, E_j and $E_{j'}$ are disjoint for $j \neq j'$. Also, $\hat{E}_l$ and $\hat{E}_{l'}$ are disjoint for $l \neq l'$. Using these facts in the above expression for $P(E_{s,i})$, we obtain

$$P(E_{s,o}) = P(E_{s,i}) \sum_{j=e}^{n-1} \sum_{l=t}^{n-1} P(E_j \cap \hat{E}_l), \tag{23}$$

which can be written as

$$P\{E_{s,o}\} = P\{E_{s,i}\} \sum_{j=e}^{n-1} P\{E_j\} \sum_{l=\lfloor (n-k)/2 \rfloor}^{j} P\{\hat{E}_l | E_j\}. \tag{24}$$

Next observe that

$$P\{E_{s,i}\} = \rho^L \hat{P}_e(L, \rho) = P_e(L, \rho), \tag{25}$$

$$P\{E_j\} = \binom{n - 1}{j} (\rho^L)^j (1 - \rho^L)^{n-1-j}, \tag{26}$$

and

$$P\{\hat{E}_l | E_j\} = \binom{j}{l} [\hat{P}_e(L, \rho)]^l (1 - \hat{P}_e(L, \rho))^{j-l} \tag{27}$$

for $l < j$. Clearly, $P(\hat{E}_l | E_j) = 0$ for $l > j$.

If $\rho = 1$, then $P(E_j) = 0$ for $j < n - 1$ and $P(E_{n-1}) = 1$, so (24) simplifies to

$$P\{E_{s,o}\} = \sum_{m=t+1}^{n} \binom{n}{m} \frac{m}{n} \hat{P}_e(L, 1)^m (1 - \hat{P}_e(L, 1))^{n-m} \tag{28}$$

which is just the output symbol error probability for an error-correcting decoder when the input symbol error probability is $\hat{P}_e(L, 1)$. Two simple upper bounds on the symbol error probability can be easily derived from (24). First, since the last summation in (24) is less than 1 and $\hat{P}_e(L, \rho) \leq 1$, we have from (24) and (25) that

$$P\{E_{s,o}\} < \sum_{j=n-k+1}^{n} \binom{n}{j} \left(\frac{j}{n}\right) (\rho^L)^j (1 - \rho^L)^{n-j}. \tag{29}$$

The right-hand side of (29) is just the error probability at the output of the erasure-correction decoder of Fig. 1 (the erasure probability is ρ^L). Notice that the upper bound in (29) depends only on the fraction ρ of the band that is jammed. Another bound can be obtained from the fact that

$$\sum_{j=e}^{n-1} P(E_j \cap \hat{E}_l) \leq P(\hat{E}_l). \tag{30}$$

The bound that results from (23) and (30) is

$$P\{E_{s,o}\} \leq P\{E_{s,i}\} \sum_{l=t}^{n-1} P\{\hat{E}_l\} \tag{31}$$

where

$$P\{\hat{E}_l\} = \binom{n - 1}{l} (\rho^L \hat{P}_e(L, \rho))^l (1 - \rho^L \hat{P}_e(L, \rho))^{n-1-l}. \tag{32}$$

This is easily recognized as the error probability at the output of the error-correction decoder of Fig. 1. Thus, we can upper bound the performance of the combined decoder strategy by the performance of error-correction decoding alone or by the performance of erasure correction alone. The performance results given in [9] are based exclusively on these bounds. The numerical results given in the next section will show that each of these bounds is tight for certain ranges of values of ρ.

The derivation so far has been for the symbol error probability of the Reed–Solomon code. We now relate this to the bit error probability for the two different types of signaling (nonorthogonal and orthogonal). For a (nonorthogonal) signal set in which the signals are sequences of binary signals, define $E_{b,i}$ to the event that the first bit of the first symbol of the received vector is in error, and let $E_{b,o}$ be the event that the first bit of the first symbol of the decoder output is in error. The same argument that gives (24) can be applied to $E_{b,i}$ and $E_{b,o}$ to prove that

$$P\{E_{b,o}\} = P\{E_{b,i}\} \sum_{j=e}^{n-1} P\{E_j\} \sum_{l=t}^{j} P\{\hat{E}_l | E_j\} \tag{33}$$

where

$$P\{E_{b,i}\} = \rho^L P_2 \tag{34}$$

and P_2 is given in (21). For M-ary orthogonal signaling, (33) is still valid, but (34) must be replaced by

$$P\{E_{b,i}\} = \rho^L \frac{M}{2(M - 1)} \hat{P}_e(L, \rho). \tag{35}$$

Finally, we note that the upper bound on the symbol error probability in (29) also holds for bit error probability, and the upper bound on symbol error probability in (31) also holds for bit error probability if $P\{E_{s,i}\}$ is replaced by $P\{E_{b,i}\}$. Similar results can be obtained when a sequence of m M-ary symbols is used as a code symbol.

VI. NUMERICAL RESULTS AND DISCUSSION

In this section, we discuss some numerical results that are presented for the decoding algorithm discussed in Section II and analyzed in Section V. First, we demonstrate the tightness of the two bounds given in Section V for the (32, 10) Reed–Solomon code with diversity $L = 5$. The two upper bounds

TABLE I
ERROR PROBABILITY FOR (32, 10) REED-SOLOMON CODE WITH
DIVERSITY 5 ($E_b/N_J = 5$ dB)

ρ	Parallel Decoding	Erasure-Correction Decoding	Error-Correction Decoding
0.50	0.156×10^{-27}	0.369×10^{-27}	0.221×10^{-11}
0.55	0.740×10^{-23}	0.179×10^{-22}	0.378×10^{-9}
0.60	0.124×10^{-18}	0.309×10^{-18}	0.346×10^{-7}
0.65	0.835×10^{-15}	0.213×10^{-14}	0.177×10^{-5}
0.70	0.242×10^{-11}	0.640×10^{-11}	0.520×10^{-4}
0.75	0.313×10^{-8}	0.856×10^{-8}	0.882×10^{-3}
0.80	0.174×10^{-5}	0.497×10^{-5}	0.850×10^{-2}
0.85	0.374×10^{-3}	0.111×10^{-2}	0.455×10^{-1}
0.90	0.228×10^{-1}	0.711×10^{-1}	0.134
0.95	0.205	0.662	0.234
1.00	0.308	1.000	0.308

TABLE II
VALUES OF ρ^* FOR PARALLEL ERRORS/ERASURES DECODING WITH
PERFECT SIDE INFORMATION AND BER = 10^{-4}

L	(32,10) code	(32,16) code	(64,20) code	(64,32) code
1	0.400	0.240	0.482	0.306
2	0.632	0.490	0.694	0.553
3	0.738	0.621	0.784	0.674
5	0.833	0.752	0.864	0.789
7	0.877	0.816	0.901	0.844
9	0.903	0.853	0.922	0.877

L	(32,6) code	(32,24) code	(64,12) code	(64,48) code
1	0.532	0.080	0.619	0.115
2	0.729	0.282	0.787	0.339
3	0.810	0.431	0.852	0.486
5	0.881	0.603	0.909	0.649
7	0.914	0.697	0.934	0.734
9	0.932	0.755	0.948	0.786

on the performance of the parallel decoding algorithm are the performance of an erasure-correction decoder only and the performance of an error-correction decoder only. These probabilities are shown in Table I for $E_b/N_J = 5$ dB. Notice that for small values of ρ, the bound based on the performance of erasure-correction decoding is tighter, while for larger values of ρ, the bound based on the performance of error-correction decoding is tighter.

We are now interested in the ENR (in the notation of Section of Sections III and IV, ENR is E_b/N_J) that is required to achieve a specified bit error rate (BER). We compute ENR as a function of ρ for two different codes and for various diversity levels. As discussed in [3], there is a minimum effective value of ρ, denoted by ρ^*, such that for $\rho < \rho^*$, the specified BER will be achieved regardless of the amount of power or noise distribution of the jammer. The value of ρ^* will depend on the code, the diversity level, and the specified BER. In our analysis, we are assuming that the background noise is negligible.[1]

For the parallel decoding technique, ρ^* can be evaluated as follows. For a given Reed-Solomon code, let p_s be the code symbol erasure probability at the decoder input which gives the specified output BER for the erasure-correction decoder. In order to cause the erasure probability to be at least p_s, the probability of a jammed diversity transmission must be at least the Lth root of p_s, that is, ρ^L must be at least as large as p_s. It follows that

$$\rho^* = (p_s)^{1/L}.$$

For $\rho < \rho^*$, the specified BER is achieved for arbitrarily small values of ENR (any nonzero value); that is, the upper bound in (29) is less than the desired BER. For $\rho \geq \rho^*$, there will (with high probability) be more than $n - k$ erasures. If there are more than $n - k$ erasures, the output of the error-correction decoder is taken as the decoded data (the erasure-correction decoder is not used). The analyses of Sections III and IV indicate how to calculate the error probabilities for the output of the error-correction decoder. The overall BER can be upper bounded by the error probability for the erasure-correction decoder for $\rho < \rho^*$ and by the error probability for the error-correction decoder for $\rho \geq \rho^*$. All the results presented assume perfect side information. However, these results are indicative of the performance that can be obtained even if the side information is not perfect if some minor modifications are made in the decoder. For example, the erasure-correction decoder could be modified to correct τ errors and ϵ erasures for a small value of τ (e.g., $\tau = 1$ or 2) as long as the constraint $2\tau + \epsilon \leq n - k$ is satisfied.

In Table II, we show the different ρ^* values for two different codes and several levels of diversity. As an example of the tightness of this bound for fixed BER, we plot the bound based on the performance of the error-correction decoder alone and the exact result for parallel decoding in Fig. 2 for
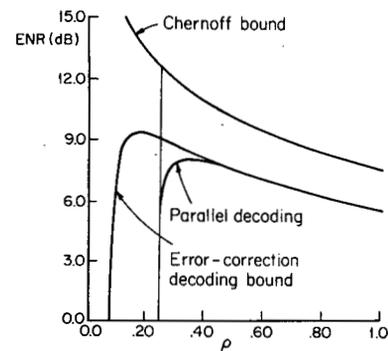
Fig. 2. E_b/N_J necessary for 10^{-4} BER for (32, 16) Reed-Solomon code with diversity 1.

the (32, 16) Reed-Solomon code and diversity 1 and orthogonal signaling. In Figs. 3-6, we will plot the performance of the error-correction decoder only, since for values of ρ greater than ρ^*, this upper bound is fairly tight, and for ρ less than ρ^*, the error probability is always less than the specified BER for any positive value of E_b. In Figs. 3-6, we consider the case of orthogonal signals, while in Fig. 7, nonorthogonal signals are considered. In Fig. 3, the ENR necessary for a BER of 10^{-4} using a (32, 16) Reed-Solomon code is shown for diversity values of 3 and 7 with orthogonal signaling, and in Fig. 4, the results for the (64, 32) code with diversity 3 and 5 are shown. In Figs. 5 and 6, analogous results are shown for the (32, 10), and (64, 20) Reed-Solomon codes, respectively, with diversity 1 and 3 and orthogonal signaling. Both the Chernoff bound and the exact result are shown. The Chernoff bound is about 2 dB larger than the exact result for all values of ρ, and is considerably larger than the exact results for small values of ρ. The vertical line in these figures occurs at $\rho = \rho^*$. The parallel decoder will have error probability less than 10^{-4} for any $E_b > 0$ when ρ is less than ρ^*. Finally, in Fig. 7, the exact ENR necessary for a BER of 10^{-4} using a (32, 16) Reed-Solomon code is shown for diversity values of 1, 3, 5, and 7 with nonorthogonal signaling ($m = 5$).

In comparing the performance of two different coded systems, one must be careful to keep certain system parameters the same. The parameters that should be held constant in any comparison are: 1) energy per information bit E_b, 2) total RF bandwidth W, 3) information bit rate R_b, and 4) total interference power $N_J W$. In the systems considered above, keeping the total RF bandwidth and the information bit rate constant requires the overall information rate to be constant. Note that $k \log_2 M/nL$ is the number of information bits per channel symbol. For a signal set of dimensionality D, diversity of level L, and an (n, k) code with an alphabet of size M, the in-
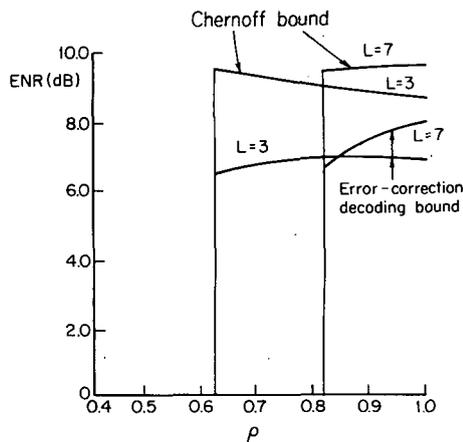
Fig. 3. E_b/N_J necessary for 10^{-4} BER for (32, 16) Reed–Solomon code with diversity 3 and 7.

Fig. 4. E_b/N_J necessary for 10^{-4} BER for (64, 32) Reed–Solomon code with diversity 3 and 5.

Fig. 5. E_b/N_J necessary for 10^{-4} BER for (32, 10) Reed–Solomon code with diversity 1 and 3.
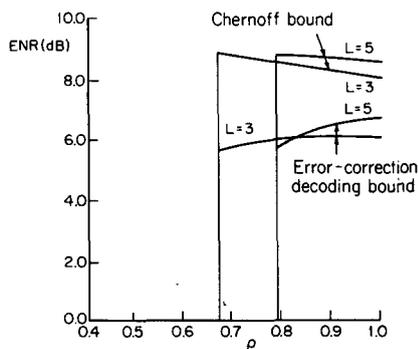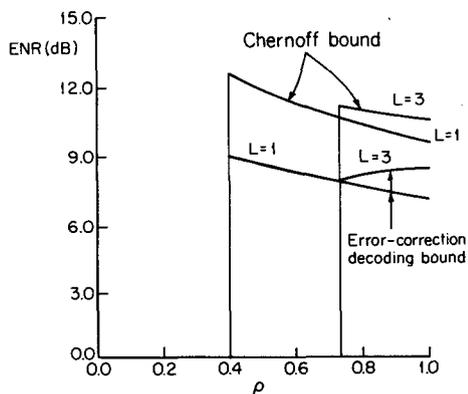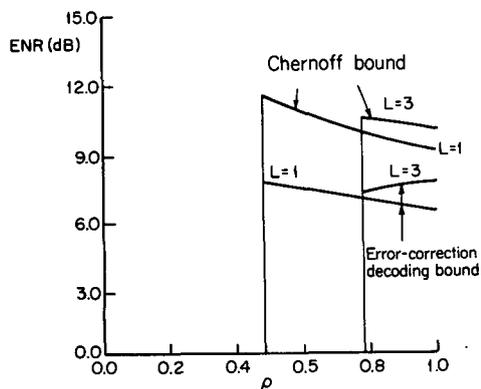

Fig. 6. E_b/N_J necessary for 10^{-4} BER for (64, 20) Reed–Solomon code with diversity 1 and 3.
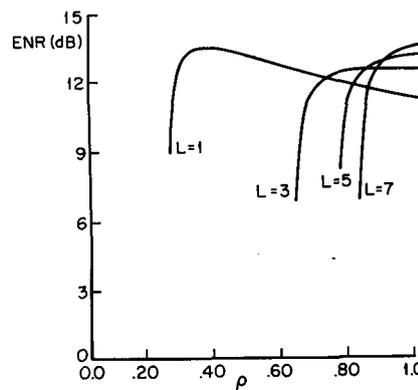

Fig. 7. E_b/N_J necessary for 10^{-4} BER for (32, 16) Reed–Solomon code with diversity 1, 3, 5, and 7 for nonorthogonal signals.

formation rate (in bits per dimension) is

$$R = \frac{k \log_2 M}{nLD} .$$

For an M-ary orthogonal signal set, the dimensionality is $D = M$. If the M-ary signals are sequences of m binary FSK tones, the dimensionality is $D = 2m = 2 \log_2 M$.

In designing a spread-spectrum system to have a certain overall bit error probability p_b, there are two parameters that we feel are important. The first is ρ^*, which is the minimum fraction of the band that must be jammed for the error probability to be at least p_b (regardless of the power or statistical distribution of the interference). It is desired to make ρ^* as large as possible. The second is ENR* which we define to be the maximum E_b/N_J (over $0 \leqslant \rho \leqslant 1$) required to obtain the specified bit error probability p_b in the presence of partial-band *Gaussian* noise. It is desired to make ENR* as small as possible. Different coding strategies provide a tradeoff between these two important parameters. In Table III, we list these parameters for various codes, along with the value of ρ (denoted by $\hat{\rho}$) which requires the maximal signal-to-noise ratio ENR*. With orthogonal modulation, which is decoded with soft decisions (square-law combining), repetition coding (diversity), and Reed–Solomon coding, we note the following. First, the orthogonal code has dependent bit errors. This is because all code symbols are sent on the same hop which is either jammed or is noise free. However, the orthogonal code (because of its low rate) can be decoded easily with soft decisions (square-law combining). The repetition code and Reed–Solomon code are interleaved; each symbol is received in interference that is independent of the interference on all other symbols (different symbols are sent on different hops). The repetition code is decoded using soft decisions (square-law combining). The Reed–Solomon code is decoded with hard decisions. Nonorthogonal signaling uses considerably fewer dimensions per transmitted bit than orthogonal signaling because the signal set has dimension $\log_2 M$. This allows us to use lower rate interleaved codes (i.e., repetition and Reed–Solomon codes) than with orthogonal signaling. If we fix the overall information rate (in bits per dimension) of the system, then the following conclusion is evident from Figs. 1–7 and Table III. Orthogonal signals (which perform well on the AWGN channel) have lower values of ENR*, but they also have lower values of ρ^* than nonorthogonal signals with the same overall rate. The lower ENR* values are due to the performance gained by soft decision decoding of the orthogonal code. The lower values of ρ^* are due to the bandwidth inefficiency of orthogonal signaling. Thus, if the primary interest is in ρ^*, it appears that binary signaling is most effective. If the primary interest is in ENR*, then orthogonal signaling is

TABLE III
VALUES OF ρ^*, ENR*, AND $\hat{\rho}$ FOR VARIOUS CODES AND BER $= 10^{-4}$

k	L	n=M	m	Rate	ρ^*	ENR*	$\hat{\rho}$
5	2	32	5	0.039062	0.755	15.98	0.95
10	4	32	5	0.039062	0.795	14.31	1.00
15	6	32	5	0.039062	0.801	13.77	1.00
20	8	32	5	0.039062	0.790	13.42	1.00
10	2	64	6	0.039062	0.809	15.69	0.95
20	4	64	6	0.039062	0.833	14.12	1.00
30	6	64	6	0.039062	0.833	13.46	1.00
35	7	64	6	0.039062	0.828	13.35	1.00
40	8	64	6	0.039062	0.820	13.20	1.00
45	9	64	6	0.039062	0.808	13.27	1.00
50	10	64	6	0.039062	0.790	13.27	1.00
30	3	128	7	0.039062	0.855	14.64	1.00
40	4	128	7	0.039062	0.858	14.04	1.00
50	5	128	7	0.039062	0.857	13.64	1.00
60	6	128	7	0.039062	0.854	13.37	1.00
70	7	128	7	0.039062	0.848	13.19	1.00
80	8	128	7	0.039062	0.840	13.09	1.00
90	9	128	7	0.039062	0.829	13.06	1.00
100	10	128	7	0.039062	0.812	13.13	1.00
80	4	256	8	0.039062	0.875	14.03	1.00
100	5	256	8	0.039062	0.872	13.62	1.00
120	6	256	8	0.039062	0.868	13.34	1.00
160	8	256	8	0.039062	0.854	13.04	1.00
180	9	256	8	0.039062	0.841	13.00	1.00
200	10	256	8	0.039062	0.826	13.05	1.00
220	11	256	8	0.039062	0.800	13.23	1.00
5	2	16	1	0.039062	0.548	9.15	0.81
40	1	256	2	0.039062	0.756	9.90	0.83
80	2	256	2	0.039062	0.764	7.97	0.87
120	3	256	2	0.039062	0.753	7.16	1.00
160	4	256	2	0.039062	0.729	6.82	1.00
200	5	256	2	0.039062	0.682	6.81	1.00
8	1	32	1	0.039062	0.463	8.45	0.63
16	2	32	1	0.039062	0.490	6.76	0.69
24	3	32	1	0.039062	0.430	6.63	0.63
27	1	64	1	0.039551	0.376	6.88	0.47
53	2	64	1	0.038818	0.259	7.11	0.36

more effective. For both large ρ^* and small ENR*, $M = 16$ with two 16-ary symbols per code symbol is quite effective with the length 256 Reed–Solomon code. This, however, requires additional decoding complexity and delay.

REFERENCES

[1] 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-31, pp. 996–1009, May 1982.

[2] S. W. Houston, "Modulation techniques for communication, Part 1: Tone and noise jamming performance of spread spectrum M-ary FSK and 2, 4-ary DPSK waveforms," in *Proc. IEEE Nat. Aerosp. Electron. Conf.*, June 1975, pp. 51–58.

[3] M. B. Pursley, "Coding and diversity for channels with fading and pulsed interference," in *Proc. 1982 Conf. Inform. Sci. Syst.*, Mar. 1982.

[4] W. E. Stark, "Coding for frequency-hopped spread-spectrum channels with partial-band interference," Coordinated Sci. Lab., Univ. Illinois, Urbana, Rep. R-945 (also Ph.D. dissertation), July 1982.

[5] D. J. Torrieri, *Principles of Military Communication Systems.* Dedham, MA: Artech, 1981.

[6] A. J. Viterbi and I. M. Jacobs, "Advances in coding and modulation for noncoherent channels affected by fading partial band, and multiple-access interference," in *Advances in Communication Systems*, vol. 4. New York: Academic, 1975, pp. 279–308.

[7] M. B. Pursley, "Throughput of frequency-hopped spread-spectrum communications for packet radio networks," in *Proc. 1982 Conf. Inform. Sci. Syst.*, Mar. 1983, pp. 550–556.

[8] W. C. Lindsey, "Error probabilities for Rician fading multichannel reception of binary and N-ary signals," *IEEE Trans. Inform. Theory*, vol. IT-10, pp. 339–350, Oct. 1964.

[9] M. B. Pursley and W. E. Stark, "Antijam capability of frequency-hop spread-spectrum with Reed–Solomon coding," in *Proc. 1983 IEEE Mil. Commun. Conf.*, Oct. 1983, pp. 7–11.

[10] E. R. Berlekamp, "The technology of error-correcting codes," *Proc. IEEE*, vol. 68, pp. 564–593, May 1980.

[11] I. M. Jacobs, "Probability of error bounds for binary transmission on the slowly fading Rician channel," *IEEE Trans. Inform. Theory*, vol. IT-12, pp. 431–441, Oct. 1966.

[12] G. C. Clark and J. B. Cain, *Error-Correction Coding for Digital Communications.* New York: Plenum, 1981.

[13] W. E. Stark, "Coding for frequency-hopped spread-spectrum communication with partial-band interference—Part II: Coded performance," *IEEE Trans. Commun.*, accepted for publication.

[14] T. Kasami and S. Lin, "On the probability of undetected error for the maximum distance separable codes," *IEEE Trans. Commun.*, vol. COM-32, pp. 998–1006, Sept. 1984.

★

Michael B. Pursley (S'68–M'68–SM'77–F'82), for a photograph and biography, see p. 508 of the June 1985 issue of this TRANSACTIONS.

★

Wayne E. Stark (S'77–M'78) was born in Harvey, IL, on February 26, 1956. He received the B.S. (with highest honors), M.S., and Ph.D. degrees in electrical engineering from the University of Illinois, Urbana, in 1978, 1979, and 1982, respectively.

Since September 1982 he has been an Assistant Professor of Electrical and Computer Engineering at the University of Michigan, Ann Arbor. He has been selected as a 1985 Presidential Young Investigator. His research interests are in the areas of information, coding, and communication theory, especially for spread-spectrum communication systems.

Dr. Stark is a member of Eta Kappa Nu, Phi Kappa Phi, and Tau Beta Pi.