Self-Encoded Spread Spectrum and Turbo Coding

Won Mee Jang, Lim Nguyen, and Michael Hempel

Abstract: **Self-encoded multiple access (SEMA) is a unique realization of random spread spectrum. As the term implies, the spreading code is obtained from the random digital information source instead of the traditional pseudo noise (PN) code generators. The time-varying random codes can provide additional security in wireless communications. Multi-rate transmissions or multi-level grade of services are also easily implementable in SEMA. In this paper, we analyze the performance of SEMA in additive white Gaussian noise (AWGN) channels and Rayleigh fading channels. Differential encoding eliminates the BER effect of error propagations due to receiver detection errors. The performance of SEMA approaches the random spread spectrum discussed in literature at high signal to noise ratios. For performance improvement, we employ multiuser detection and Turbo coding. We consider a downlink synchronous system such as base station to mobile communication though the analysis can be extended to uplink communications.**

Index Terms: **Spread spectrum, CDMA, multiuser detection, random sequence, Turbo coding.**

I. INTRODUCTION

In code division multiple access (CDMA) communications, each user is assigned a unique PN spreading sequence that has a low cross correlation with other users' sequences. Characteristic of the deterministic PN codes is that they can be duplicated, potentially compromising the transmission security. Self-encoded multiple access (SEMA) eliminates the need for traditional transmit and receive PN code generators. As the term implies, the spreading code is obtained from the random digital information source itself. Although random codes have often been employed for analysis purposes [1]–[3], they present a practical implementation problem because data recovery by the intended receiver requires a prior knowledge of the codes for signal despreading. It was generally believed that spread spectrum systems with time-varying random codes are not possible in practice [4]. As a result, the random codes in these studies would remain fixed once they have been generated. Recently, we proposed a novel spread spectrum technique, self-encoded spread spectrum, that does not use PN codes [5]. The enhanced transmission security arises from the stochastic nature of the unique spectrum spreading and despreading processes. Unless initially synchronized and having a complete knowledge of the tap register structure (intended receiver), data recovery will be extremely unreliable since the spreading codes as constructed are time-varying, random, and uncorrelated.

In this paper, we probe the possibility of SEMA applications to practical wireless channels. We begin with the matched filter (MF) receiver in AWGN channels. The output of the MF includes multiple access interference (MAI) from other users and receiver noise. We can eliminate the MAI by employing precoding or multiuser detection. Precoding eliminates the MAI at the transmitter while receiver-based decorrelator eliminates the MAI at the receiver. Both precoding and receiver-based decorrelator provide the same performance which shows a significant improvement over the MF receiver. The self-interference (SI) due to detection errors is crucial in SEMA performance analysis. Error propagation in SEMA is introduced by accumulated chip errors in the receiver shift registers. To ameliorate the problem, the differential encoder at the outside of the self-encoder was proposed in [7]. It was shown that the differential encoder eliminates the bit error rate (BER) effect of error propagations. Due to the stochastic nature of a data source, the performance of SEMA without SI is equivalent to that of spread spectrum with random spreading sequences discussed in [1]–[3] and [8]. The SEMA analysis is extended to Rayleigh fading channels and shows that a significant performance improvement is observed by using multiuser detection and Turbo coding.

In Section II, we propose the system model of SEMA. The performance of SEMA is analyzed in Section III. Section IV compares the analytical results to the simulations. Conclusions follow in Section V.

II. SYSTEM MODEL

A. SEMA and Synchronization

Fig. 1 shows the block diagram of SEMA with multiuser detection and channel coding. The SEMA spread block is illustrated by a simplified schematic in Fig. 2. The delay registers are constantly updated from an n-tap, serial delay of the data, where n is the spreading gain. One previous bit is used to update one chip of the current spreading sequence. As a result, the spreading sequence is not only randomly generated and independent of current symbol, but also dynamically changing from one symbol to the next. This smoothes out the spectrum of the signals and eliminates the spectral lines associated with PN sequences.

The self encoding operation at the transmitter is reversed at the receiver where data recovery is performed by means of a correlation detector. The recovered data are fed back to the n-tap delay registers which provide an estimate of transmitter's spreading codes required for signal despreading. The detection errors are accumulated in the delay registers, and are the source of the SI. Notice that the contents of the delay registers in the transmitter and receiver should be identical at the start of the transmission. This is accomplished as part of the initial synchronization procedure.

Acquisition and tracking of self-encoded sequence can be performed in a similar manner to PN sequences with the proviso

Manuscript received September 24, 2002; approved for publication by Jong-Seon No, Division I Editor, January 19, 2004.

W. M. Jang, L. Nguyen, and M. Hempel are with the Peter Kiewit Institute of Information Science, Technology & Engineering, Department of Computer and Electronics Engineering, University of Nebraska, U.S.A, email: {wjang, nguyenl}@unlnotes.unl.edu, mhempel@mail.unomaha.edu.

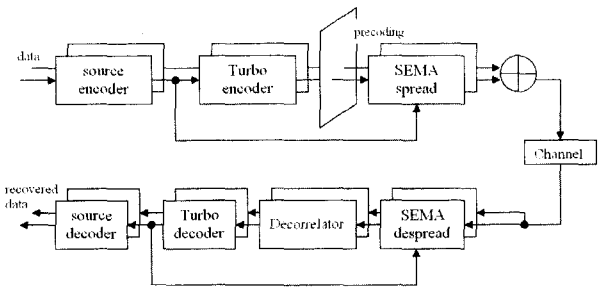


Fig. 1. SEMA transmitter and receiver structure.

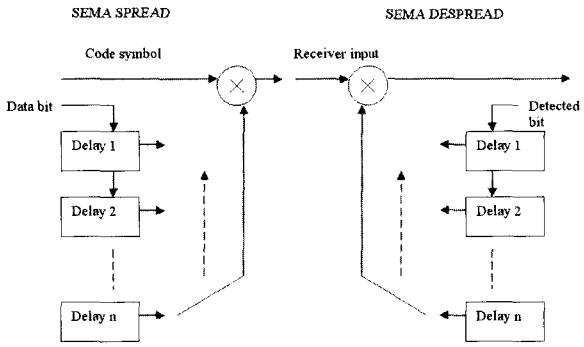


Fig. 2. SEMA spread/despread block.

that the chip updates are enabled once data transmission has commenced following code acquisition. At the chip rate, the self-encoded chips are latched at the output register by shifting the registers serially, with the output being fed back to the input register. The input feedback is switched to the data during the last chip period of the current symbol for a new chip input. This resembles a simple linear feedback register circuits of length n, with zero valued taps except for the input and output taps, where the input register is updated periodically by the data, and the output register provides the spreading sequence.

B. Matched Filter Receiver

We consider a synchronous multiuser system with K users sharing a frequency non-selective and time-invariant channel, with the received signal at the i-th receiver given by

$$r_i(t) = x(t) + n_i(t), \quad 0 \le t < T_b, \tag{1}$$

where $n_i(t)$ represents additive white Gaussian noise of two-sided power spectral density σ_i^2. T_b is the bit duration and $x(t)$ is the transmitted signal. Let $\mathbf{A} = diag\{A_j\}_{K\times K}$ be the diagonal matrix of signal amplitudes and $\mathbf{b}$ the vector of the data bits of K users, such that $b_j \in \{-1, 1\}, \forall j \in [1, \cdots, K]$. Then,

$$x(t) = \sum_{j=1}^{K} A_j s_j(t) b_j = \mathbf{s}^T(t)\mathbf{Ab}, \quad 0 \le t < T_b, \tag{2}$$

where $\mathbf{s}(t) = \{s_1(t), \cdots, s_K(t)\}^T$ is the vector of signature waveforms. The j-th user's signature waveform, $s_j(t)$, consists of $n = T_b/T_c$ random chips where T_c is the chip duration. $\mathbf{s}^T(t)$ denotes the transpose of $\mathbf{s}(t)$. It is assumed that signature waveforms have unit energy, that is,

$$\int_0^{T_b} s_j^2(t)dt = 1, \quad j = 1, 2, \cdots, K. \tag{3}$$

The output of the matched filter matched to the i-th signature waveform is

$$y_i = \int_0^{T_b} r_i(t)s_i(t)dt, \quad i = 1, \cdots, K, \tag{4}$$

or

$$y_i = A_i b_i + \sum_{j=1, j\neq i}^{K} R_{ij}A_j b_j + \sigma_i n_i, \tag{5}$$

where n_i is an independent Gaussian random variable with unit variance. The crosscorrelation R_{ij} is

$$R_{ij} = \int_0^{T_b} s_i(t)s_j(t)dt, \tag{6}$$

where $\mathbf{R}$ is a positive semidefinite matrix[1]. The $K(K-1)/2$ crosscorrelations of R_{ij}'s are pairwise independent but not jointly independent [9]. The above synchronous model can be found in centralized transmitters such as forward links of mobile communications or satellite communications. As the chip sequences are random and time varying, so are both $\mathbf{R}$ and $\mathbf{s}(t)$ in each bit interval.

It is easy to check that the likelihood function depends on the observations only through the outputs of the bank of MFs that are matched to the signature waveforms [9]. By combining the MF outputs from K receiving sites in (4) into a single vector, $\hat{\mathbf{y}} = \{y_1, \cdots, y_K\}^T$, we get

$$\hat{\mathbf{y}} = \mathbf{RAb} + \mathbf{n}, \tag{7}$$

where $\mathbf{n}$ is a zero-mean Gaussian noise vector with a covariance matrix equal to $diag\{\sigma_i^2\}$.

C. Precoding and Multiuser Detection

To improve the performance of SEMA we consider multiuser detection. Transmitter precoding that reduces the effect of MAI is defined by a linear transformation matrix $\mathbf{T}$ [10]. The transmitted signal is then given by

$$x(t) = \mathbf{s}^T(t)\mathbf{TAb}, \tag{8}$$

where $\mathbf{T}$ is a $K \times K$ matrix to be chosen according to some optimality criterion. Therefore, with precoding the vector of MF outputs is

$$\mathbf{y} = \mathbf{RTAb} + \mathbf{n}. \tag{9}$$

The optimum precoding transformation $\mathbf{T}$ that minimizes the mean square error

$$J = E_{\mathbf{b},\mathbf{n}}\left\{ \| \mathbf{Ab} - \mathbf{y} \|^2 \right\}, \tag{10}$$

[1] Throughout this paper we will assume that $\mathbf{R}$ is positive definite so that $\mathbf{R}^{-1}$ exists.

where $E_{\mathbf{b},\mathbf{n}}$ is the average with respect to (w.r.t) data $\mathbf{b}$ and noise $\mathbf{n}$, was derived as [10]

$$\mathbf{T} = \mathbf{R}^{-1}. \tag{11}$$

So with optimum precoding

$$\mathbf{y} = \mathbf{Ab} + \mathbf{n}. \tag{12}$$

Thus, the multiuser detection problem is decoupled into K separate single-user detection problems, without the noise enhancement at the receiver. The total average transmit energy per bit interval is $E_{av} = E_{\mathbf{b}}\{\int_0^T x^2(t)dt\} = trace\{\mathbf{RA^2}\}$, where the expectation is over the data vector $\mathbf{b}$. It is easy to see that without precoding $E_{av} = \sum_{i=1}^{K} A_i^2$, whereas with precoding we get $E_{av}^p = trace\{\mathbf{T^T RTA^2}\} = trace\{\mathbf{R^{-1}A^2}\} = \sum_{i=1}^{K} A_i^2 R_{ii}^{-1}$, where R_{ii}^{-1} represents the i-th diagonal element in $\mathbf{R}^{-1}$. Since $\mathbf{R}$ is a correlation matrix, $R_{ii}^{-1} \geq 1$, $\forall i$. Hence, $E_{av}^p \geq E_{av}$, which means that precoding results in an average transmit power increase with the factor, $1/C$, where

$$C = \frac{\sum_{i=1}^{K} A_i^2}{\sum_{i=1}^{K} A_i^2 R_{ii}^{-1}}. \tag{13}$$

To maintain the average transmit power with precoding the same as without precoding, we modify the precoding transformation as [10]

$$\mathbf{T} = \sqrt{C}\mathbf{R}^{-1}. \tag{14}$$

Then the probability of bit error for the i-th user is given by

$$P_b^{pre} = Q\left(\sqrt{\frac{A_i^2}{\sigma_i^2}C}\right) = Q\left(\sqrt{2\left(\frac{E_b}{N_o}\right)C}\right), \tag{15}$$

where $Q(\beta) = \frac{1}{\sqrt{2\pi}}\int_\beta^\infty e^{-\frac{x^2}{2}}dx$. E_b/N_o is the bit energy to noise ratio, and N_o is one-sided noise spectral density.

Decorrelating detection is a suboptimal multiuser detection with comparatively low complexity. Receiver-based decorrelator can be found in [9], [11], and [12]:

$$\tilde{\mathbf{y}} = \mathbf{R}^{-1}\hat{\mathbf{y}} = \mathbf{R}^{-1}(\mathbf{RAb} + \mathbf{n}) = \mathbf{Ab} + \mathbf{R}^{-1}\mathbf{n}, \tag{16}$$

and the BER for the receiver-based decorrelator is

$$P_b^{dec} = Q\left(\sqrt{2\left(\frac{E_b}{N_o}\right)\frac{1}{R_{ii}^{-1}}}\right). \tag{17}$$

III. SYSTEM ANALYSIS

A. Self-Interference in SEMA

Due to detection errors, the despreading sequence may not be exactly the same as the spreading sequence at the transmitter. Since the recovered symbols are used to despread the signals, a chip error will remain in the shift registers and affect the following symbol decision until it is shifted out of the registers. This amounts to SI and the effect of the error propagation may cause the average BER to approach 0.5 as the number of transmitted symbols increases. The BER of SEMA is a dynamic quantity that depends on the signal-to-noise ratio (SNR), spreading factor, number of users, and number of transmitted symbols. The effect of the SI is reduced as the spreading factor or the SNR increases.

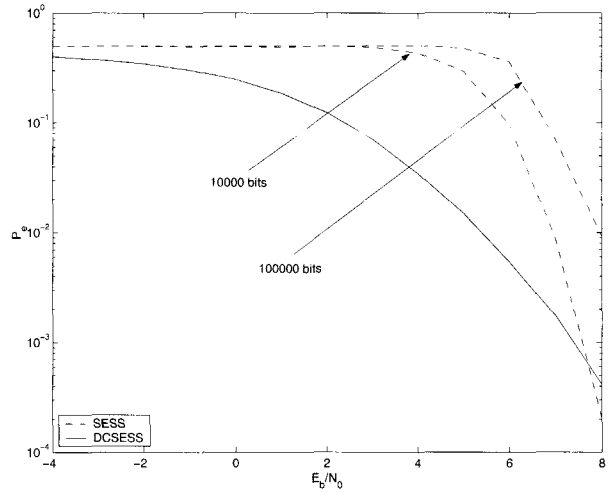


Fig. 3. Comparison of BER of self-encoded spread spread spectrum (SESS) and differentially encoded SESS (DESESS), reproduced from [7].

The average probability of bit error, P_b, can be described by a Bernoulli distribution in terms of n and l where l is the number of chip errors in the despreading register at the receiver, and n is the spreading length. When n is large, the BER of SEMA can be well approximated by [6] and [7]

$$P_b = \sum_{l=0}^{n} P_{b|l}\binom{n}{l}P_b^l(1-P_b)^{n-l}, \tag{18}$$

where the conditional probability is

$$P_{b|l} = Q\left(\sqrt{\frac{2E_b}{N_o}\left(1-\frac{2l}{n}\right)^2}\right). \tag{19}$$

Due to the symmetry of $P_{b|l}$ and the binomial distribution, it can be shown that P_b=0.5 is a feasible (but undesirable) solution to (18) regardless of the SNR and the spreading length. This undesirable BER effect is caused by error propagation in the receiver shift registers: Sufficient chip errors may accumulate that exceed $n/2$ and reverse the binary decision regions. The symbol reversals result in an average BER of 0.5 as the number of transmitted symbols increases.

To ameliorate the problem, the differential encoder at the outside of the self-encoder was proposed and analyzed in [7]. Fig. 3 shows the performance with and without differential encoding for $n = 8$. The effect of error propagation was analyzed by averaging 100 simulation runs of 10,000 bits, followed by 100,000 bits. The results demonstrate that without differential encoding, the BER tends toward 0.5 as the number of transmitted bits increases. It can also be seen that differential encoding eliminates the BER effect of error propagations. Fig. 4 shows the BER performance with differential encoding for various values of n.

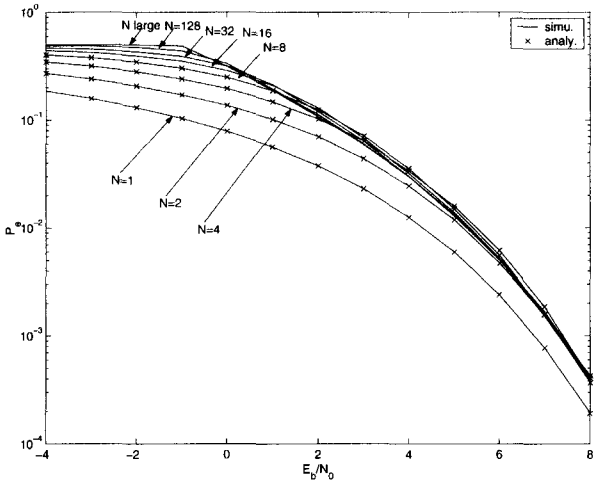


Fig. 4. BER of SESS with differential encoding where N is the spreading length, reproduced from [7].

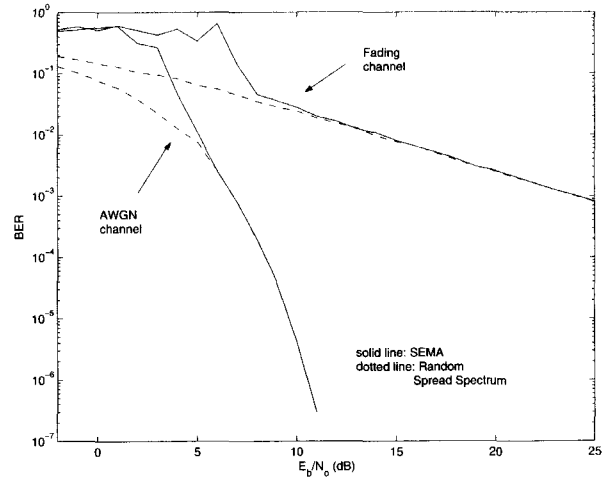


Fig. 5. BER of SEMA and random spread spectrum, single user, 16 chips/bit, AWGN and Rayleigh.

We can see that the effect of SI is negligible for $E_b/N_o \geq 2$ dB for $n \geq 4$. Since l in (19) is equal to the number of bit errors for n bit transmissions, as $n \to \infty$ and $l/n \to P_b$. Therefore, with differential encoding, the BER approaches the steady state solution of

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_o}(1-2P_b)^2}\right). \tag{20}$$

The probability of error in differentially encoded M-ary PSK is approximately twice the probability of error for M-ary PSK with absolute phase encoding [13]. However, this factor-of-2 increase in the error probability translates into little loss in SNR. Due to the random nature of a data source, the performance of SEMA without the SI is equivalent to random spread spectrum as illustrated in Figs. 5 and 6, in AWGN or fading channels, with and without channel coding. Fig. 6 shows that SEMA with Turbo coding approaches random spread spectrum not only asymptotically but also at every iteration for $E_b/N_o \geq 2.5$ dB. As a result, we do not include the SI in the theoretical analysis since our interest is in SEMA being operated outside the SI region, and partially due to difficulties of analyzing the SI with dynamic features.

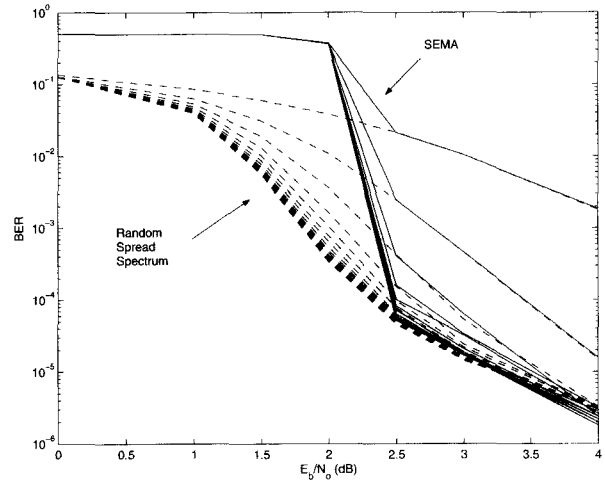


Fig. 6. BER of SEMA and random spread spectrum, Turbo coding, two users, 16 chips/bit, AWGN.

B. SEMA in AWGN and Rayleigh Channels

The performance of SEMA in an AWGN channel can be described in terms of the bit error probability [2], [3], [22],

$$P_b = Q\left(\sqrt{\frac{2E_b/N_o}{1+2(E_b/N_o)\left((K-1)/n\right)}}\right), \tag{21}$$

where K is the number of users in the system, and n is the number of chips per bit. The performance of SEMA in a Rayleigh fading channel can be obtained by taking the expectation w.r.t. the received SNR [13]

$$P_b = \int_0^\infty Q\left(\sqrt{\frac{2(E_b/N_o)\ \gamma}{1+2(E_b/N_o)\ \gamma\ \left((K-1)/n\right)}}\right) \times f_\Gamma(\gamma)\ d\gamma, \tag{22}$$

where $f_\Gamma(\gamma)$ is a chi-square probability distribution of the fading magnitude squared, $\Gamma = |\alpha^2|$. Here we assume a synchronous downlink channel, so that all users experience the same fading which is considered independent for every bit interval. For the same average received power without fading:

$$f_\Gamma(\gamma) = e^{-\gamma}. \tag{23}$$

To compute (22) numerically, the bit error rate is shown in Appendix A:

$$P_b = \frac{1}{2}\Bigg\{1 - \frac{1}{\sqrt{2\pi}}\frac{1}{\sqrt{\frac{K-1}{n}}} \times \int_0^{\pi/2} e^{-\frac{1}{\frac{K-1}{n}\frac{2E_b}{N_o}}[\tan^2\theta + \frac{E_b}{N_o}\sin^2\theta]}\, 2\cos\theta\ d\theta\Bigg\}. \quad (24)$$

For a single user system, (22) is reduced to [13]

$$P_b = \frac{1}{2}\left(1 - \sqrt{\frac{E_b/N_o}{1+E_b/N_o}}\right). \quad (25)$$

The asymptotic BER of precoding and receiver-based decorrelator is shown to be the same for AWGN transmission as K and $n \to \infty$ [14]. Therefore, the asymptotic BER of multiuser detection (mud) is

$$P_b^{mud} = Q\left(\sqrt{2\left(\frac{E_b}{N_o}\right)(1-K/n)}\right), \quad (26)$$

and it was shown that the BER approaches rather quickly to its asymptotic value. We can extend (26) to a Rayleigh fading channel:

$$P_b^{mud} = \int_0^\infty Q\left(\sqrt{2\left(\frac{E_b}{N_o}\right)\gamma\,(1-K/n)}\right) f_\Gamma(\gamma)\ d\gamma, \quad (27)$$

and with (23)

$$P_b^{mud} = \frac{1}{2}\left(1 - \sqrt{\frac{(E_b/N_o)(1-K/n)}{(E_b/N_o)(1-K/n)+1}}\right). \quad (28)$$

C. SEMA, Multiuser Detection, and Turbo Coding in AWGN Channels

We assume n chips per code-symbol so the spreading factor is n/R_c chips per bit where R_c is a code rate, and that soft decision is made at the receiver. By shifting the generator functions for each user we can avoid code collisions and improve the performance [15]. We propose to apply the generator functions developed for a single user to a multiuser system. Therefore, multiuser generator matrices are provided by shifting the generator matrix of a conventional single user code. For example, a generator matrix G1=$[g^{(1)}g^{(2)}g^{(3)}]$ = [5 7 7] in octal generates a convolutional code with a code rate $R_c = 1/3$, a constraint length $L = 3$ and a free distance d_{free}=8. The shifted matrix can be G2= [7 5 7] or G3= [7 7 5]. Thus G1, G2, and G3 can be assigned to users 1, 2, and 3. In this case the codeword set for user 1 is [(1 1 1), (0 0 0), (0 1 1), (1 0 0)]. Codeword sets for user 2 and user 3 are [(1 1 1), (0 0 0), (1 0 1), (0 1 0)] and [(1 1 1), (0 0 0), (1 1 0), (0 0 1)]. Different codeword sets for different users randomize spreading sequences among users and avoid a code collision. It can be shown that shifting the matrix does not affect the code distance property of a single user. Since the number of permutations is limited, the constraint length must be increased for a larger number of users to provide a different generator matrix for all users. The advantage of shifting the matrix is obvious in Fig. 7.

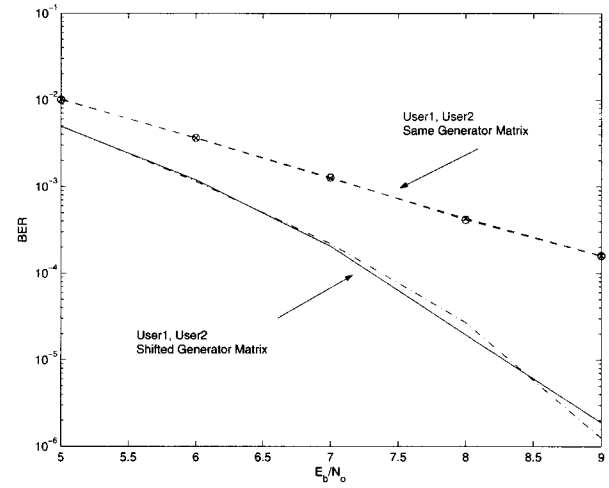


Fig. 7. Simulation for the same generator matrix (G1=G2=[5 7 7]) and the shifted generator matrices (G1=[5 7 7] and G2=[7 7 5]), reproduced from [15].

Turbo coding is powerful channel coding and approaches Shannon's capacity [16], [17]. The upper bound on the BER of SEMA with Turbo coding can be expressed as [18], [19]

$$P_b < \sum_{d=d_{free}}^{\infty} \frac{N_d \bar{w}_d}{N} P_2(d), \quad (29)$$

where $P_2(d)$ is the pairwise error probability of two codewords with a distance, d. The BER, P_b is upper-bounded by the union bound of $P_2(d)$, $\forall d$. N_d is the multiplicity of d-distance codewords, $\bar{w}_d$ is the average weight of the information sequences causing the d-distance codewords, and d_{free} is the free distance. N and d are an interleaver size and a distance from the all-zero path that merges with the all-zero path. For moderate and high signal-to-noise ratios, it is well known that the free-distance term in the union bound on the BER performance dominates the bound [18], [20]. Thus the free distance asymptote for an isolated single user is given by [18] and [19]

$$P_b = \frac{N_{free}\bar{w}_{free}}{N} Q\left(\sqrt{2r_c d_{free}}\right), \quad (30)$$

where $r_c = E_c/N_o$ is a symbol energy to noise ratio. N_{free} is the multiplicity of free-distance codewords and $\bar{w}_{free}$ is the average weight of the information sequences causing free-distance codewords. The asymptotic performance of a multiuser system with MAI [2], [3], [22] approaches

$$P_b = \frac{N_{free}\bar{w}_{free}}{N} Q\left(\sqrt{\frac{2r_c d_{free}}{1+2r_c(K-1)/n}}\right). \quad (31)$$

An algorithm for finding the free distance of Turbo code is described in [19]. For further system improvement, we applied multiuser detection to Turbo coding. The performance of SEMA with multiuser detection and Turbo coding in AWGN channels

can be derived from (26) and (30):

$$P_b^{mud} = \frac{N_{free}\bar{w}_{free}}{N} Q\left(\sqrt{2r_c d_{free}(1-K/n)}\right). \quad (32)$$

D. SEMA, Multiuser Detection, and Turbo Coding in Rayleigh Channels

The upper bound on the BER of SEMA with Turbo coding in Rayleigh fading channels can be expressed as in (29) where $P_2(d)$ can be obtained by taking the expectation w.r.t. the received SNR [13], [21],

$$P_2(d) = E\left[Q\left(\sqrt{\sum_{i=1}^{d}\left(\frac{2r_c\gamma_i}{1+2r_c\gamma_i(K-1)/n}\right)}\right)\right]. \quad (33)$$

Here γ_i's are independent and identically distributed chi-square random variables with $E[\gamma_i] = 1$ to maintain the averaged received signal power the same without fading. We assume that fadings are independent for every symbol intervals. The expectation E is taken over γ_i, for $i = 1, \cdots, d$. Thus the asymptotic performance can be obtained from (29) and (33):

$$P_b = \frac{N_{free}\bar{w}_{free}}{N} \times E\left[Q\left(\sqrt{\sum_{i=1}^{d_{free}}\left(\frac{2r_c\gamma_i}{1+2r_c\gamma_i(K-1)/n}\right)}\right)\right], \quad (34)$$

and as shown in Appendix B:

$$P_b = \frac{1}{2}\frac{N_{free}\bar{w}_{free}}{N}\left\{1 - \frac{1}{\sqrt{2\pi}}\frac{1}{\sqrt{\frac{K-1}{n}}} \times \int_0^{\pi/2} e^{-\frac{1}{\frac{K-1}{n}\frac{2E_c}{N_o}}(\tan^2\theta + \frac{E_c}{N_o}\sin^2\theta)} 2\cos\theta \; d\theta\right\}^{d_{free}}. \quad (35)$$

Likewise, the BER of precoding or receiver-based decorrelator is

$$P_b^{mud} = \frac{N_{free}\bar{w}_{free}}{N} \times E\left[Q\left(\sqrt{2r_c(1-K/n)\sum_{i=1}^{d_{free}}\gamma_i}\right)\right], \quad (36)$$

and following the similar procedure in Appendix B:

$$P_b^{mud} = \frac{1}{2}\frac{N_{free}\bar{w}_{free}}{N} \times \left[1 - \sqrt{\frac{(E_c/N_o)(1-K/n)}{(E_c/N_o)(1-K/n)+1}}\right]^{d_{free}}. \quad (37)$$

E. Comparison with Other Direct Sequence Spread Spectrum Systems

We compare SEMA with orthogonal sequence, maximum-length shift-register sequence (or m-sequence) and Gold sequence in AWGN channels without channel coding. For a $K = n$ user orthogonal sequence system, the BER in AWGN channels is equal to an isolated single user system. For synchronous CDMA systems, the performance is

$$P_b^{CDMA} = Q\left(\sqrt{\frac{2E_b/N_o}{1+\rho\frac{K-1}{n^2}\,2E_b/N_o}}\right), \quad (38)$$

where ρ is the absolute value of unnormalized crosscorrelation which is equal to unity for the preferentially phased Golde codes or m-sequences [22]. With large n and $K \approx n$, CDMA systems with Gold or m-sequences approach an isolated single user performance, while SEMA approaches (21) with $K = n$. The PN-based CDMA has regulated crosscorrelations. Thus the MAI is reduced compared with random spreading. The contributions of SEMA include a unique realization of random spreading, the potential for additional security in wireless communications, and easy implementation of multi-rate transmissions. Possible performance improvement of SEMA is expected for uplink communication according to the results on asynchronous random sequence analysis in [2] and [3].

IV. NUMERICAL RESULTS

Fig. 8 shows the example performance in AWGN channels with 8 users and 64 chips/bit. We can see that the simulation result approaches the theoretical result asymptotically. The discrepancy at low SNR is due to the effect of the SI in the simulation. Fig. 9 compares the simulation results of receiver-based decorrelator and precoding with the theoretical results for SEMA with multiuser detection in AWGN channels. The performance improvement over Fig. 8 is obvious due to the multiuser detection. Fig. 10 shows an 8 user system with 64 chips/bit and a two-user system with 16 chips/bit in a Rayleigh fading channel. Again the simulation results agree well with the theoretical results at high SNR.

All channel coding analyses in this paper employed Turbo code with the same constituent encoders and puncturing pattern as detailed in [16]. The algorithm in [19] was applied to the Turbo code with a particular pseudorandom interleaving pattern. The Turbo code generator polynomials for this code are $h_0 = D^4 + D^3 + D^2 + D + 1$ and $h_1 = D^4 + 1$ or $h_0 = 37$ and $h_1 = 21$ using octal notation. The pseudorandom interleaver size N is equal to 1000. This $(37, 21, 1000)$ code with puncturing was found to have $N_{free} = 3$ paths with weight $d_{free} = 6$ and $R_c = 1/2$. Each of these paths was caused by an input sequence of weight 2 and thus $\bar{w}_{free} = 2$ [18], [19]. The rate loss due to the addition of a 4-bit tail is ignored in the theoretical performance analysis. The performance improvement in AWGN channels due to Turbo coding is shown in Fig. 11. Fig. 12 shows the performance of Turbo coding with decorrelation detection. Decorrelation detection eliminates the SI effect for $E_b/N_o > 1.5$ dB (versus 2 dB without multiuser detection shown in Fig. 11). Fig. 13 shows precoding performance that

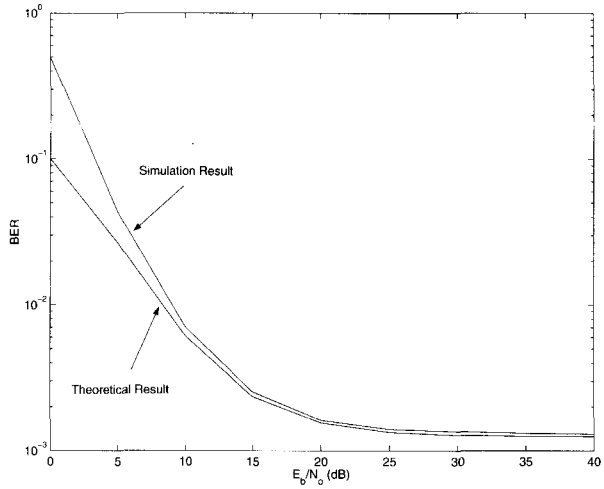


Fig. 8. SEMA, 8 users, 64 chips/bit, AWGN.

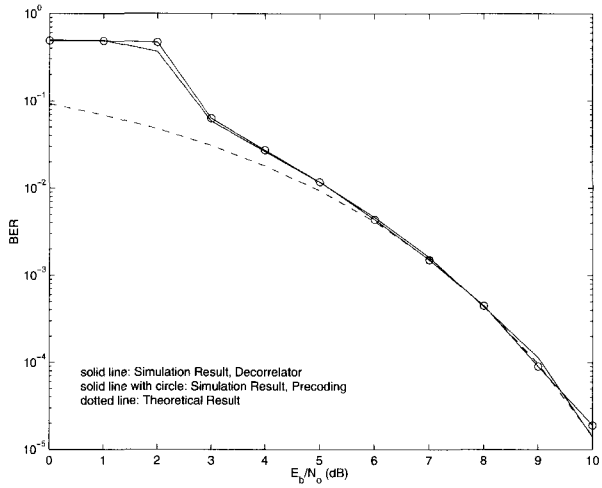


Fig. 9. SEMA with multiuser detection, 8 users, 64 chips/bit, AWGN.

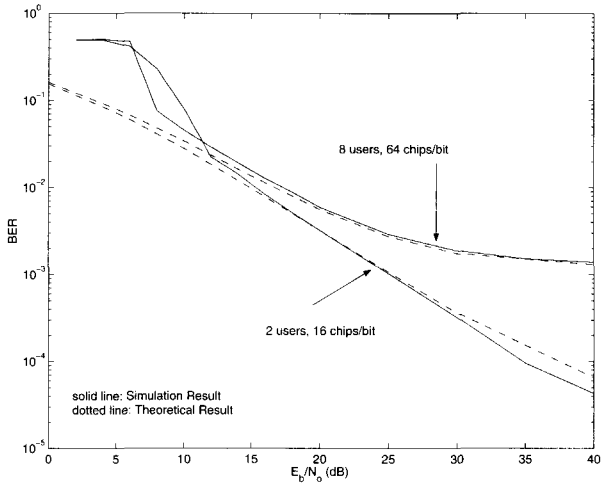


Fig. 10. SEMA, 2 users with 16 chips/bit and 8 users with 64 chips/bit, Rayleigh.

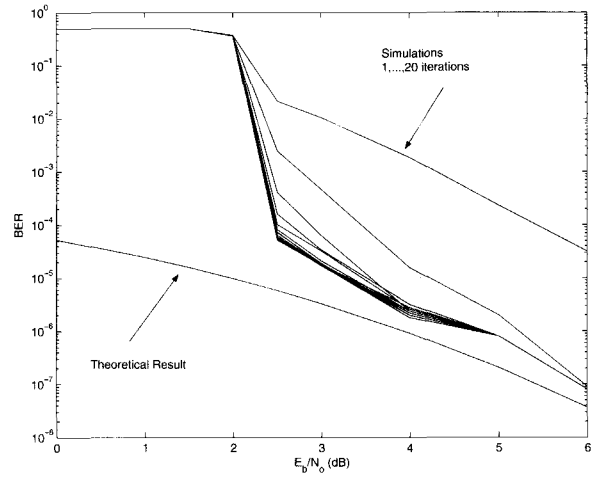


Fig. 11. SEMA with Turbo, puncturing, 2 users, 16 chips/symbol, AWGN.

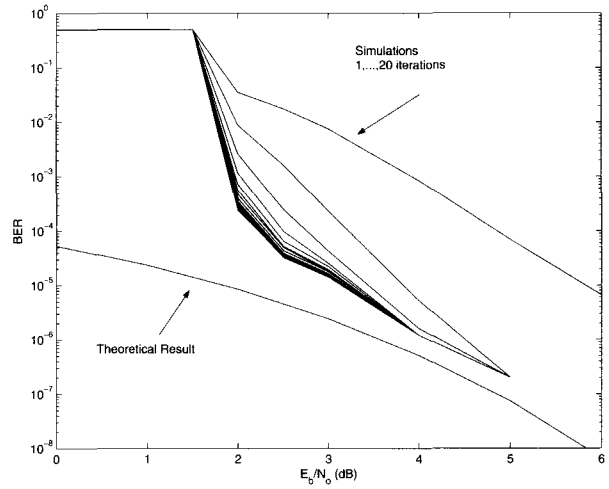


Fig. 12. SEMA with Turbo and decorrelation, puncturing, 2 users, 16 chips/symbol, AWGN.

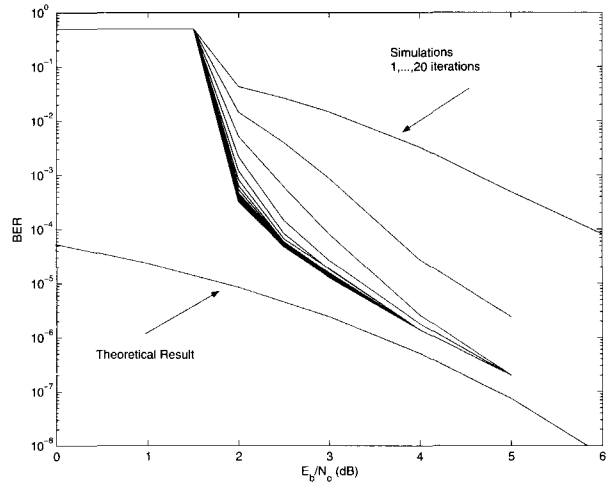


Fig. 13. SEMA with Turbo and precoding, puncturing, 2 users, 16 chips/symbol, AWGN.

is similar to decorrelation detection. Figs. 11, 12, and 13 show only a 0.5 dB difference between the simulations and theoretical result for high SNR.

The performance with Turbo coding in a Rayleigh fading channel is shown in Figs. 14, 15, and 16. For all cases, the SI effect becomes negligible for $E_b/N_o \geq 4$ dB in spite of the MAI.

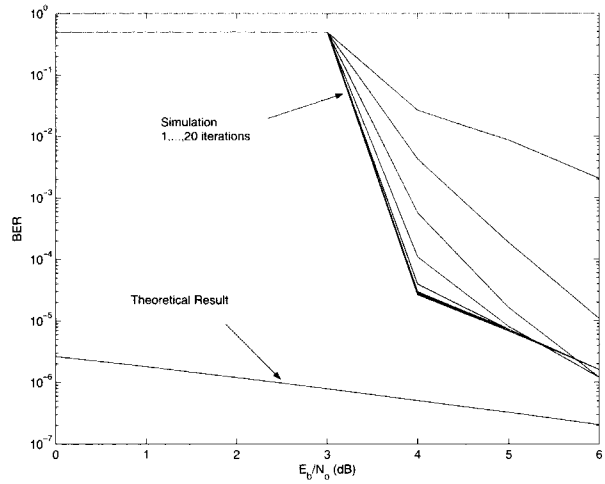


Fig. 14. SEMA with Turbo, puncturing, 2 users, 16 chips/symbol, Rayleigh.

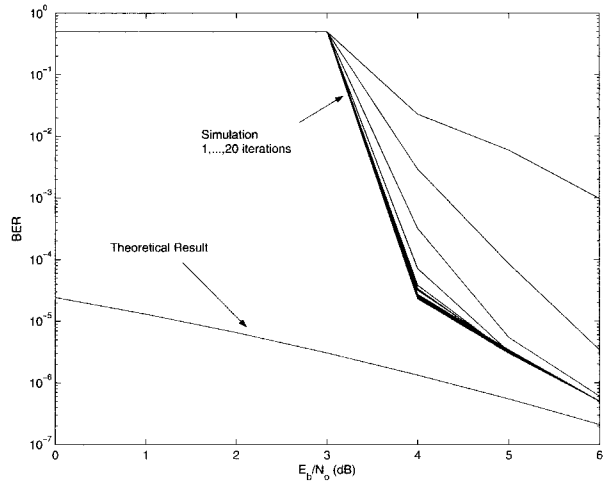


Fig. 15. SEMA with Turbo and decorrelation, puncturing, 2 users, 16 chips/symbol, Rayleigh.

Again, multiuser detection improves the system performance at high SNR as shown in Fig. 15 (decorrelation) and Fig. 16 (precoding) . For example, the BER in Figs. 15 and 16 show better improvement with multiuser detection for $E_b/N_o \geq 5$ dB compared to Fig. 14. A similar behavior can also be observed for AWGN channels as seen in Figs. 12 and 13 in comparison to Fig. 11. This effect would be more distinct with more users due to a larger MAI in the system.

The difference between simulation and theoretical results in Rayleigh channels is rather large compared with the difference in AWGN channels. This is due to the Q function approximation in the derivation of the theoretical BER in Rayleigh channels. In the simulations, we did not use the shifting generator matrix discussed in Section III.C. The difference can be reduced significantly if we apply the data randomization in multiuser Turbo coding procedure. Notice also in Figs. 11 through 16 that there is a critical SNR at which the SI is removed and the BER drops rapidly.

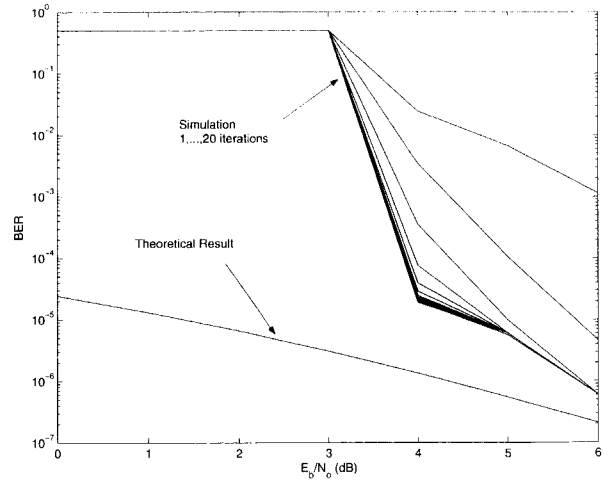


Fig. 16. SEMA with Turbo and precoding, puncturing, 2 users, 16 chips/symbol, Rayleigh.

V. CONCLUSIONS

SEMA is a unique realization of random spread spectrum that can provide another level of secure communication in vulnerable wireless channels. SEMA also affords easy implementation of multi-rate transmissions and multi-level grade of services. In this paper, we investigate possible application of SEMA to practical mobile environments. The performance analysis shows that there is a critical SNR at which the SI becomes negligible and BER improves rapidly. It is important that the operating point of SEMA should be beyond the critical SNR which depends on channel characteristics and system parameters. Beyond the critical SNR, the performance of SEMA is equivalent to the random spread spectrum. The performance can be significantly improved by applying multiuser detection and powerful channel coding such as Turbo coding.

APPENDIX A

SEMA in Rayleigh Fading Channel

The BER of SEMA in a Rayleigh channel is

$$P_b = \int_0^\infty Q\left(\sqrt{\frac{(2E_b/N_o)\gamma}{1+2(E_b/N_o)\gamma((K-1)/n)}}\right) e^{-\gamma}\, d\gamma. \quad (39)$$

Let $(K-1)/n = a$ and $2E_b/N_o = b$. Then (39) can be written as

$$P_b = \int_0^\infty Q\left(\sqrt{\frac{b\gamma}{1+ab\gamma}}\right) e^{-\gamma}\, d\gamma. \quad (40)$$

Integration by parts:

$$P_b = \left[Q\left(\sqrt{\frac{b\gamma}{1+ab\gamma}}\right)(-e^{-\gamma})\right]_0^\infty - \int_0^\infty e^{-\gamma}\left\{\frac{1}{\sqrt{2\pi}}e^{\frac{-b\gamma}{2(1+ab\gamma)}}\frac{1}{2}\left(\frac{b\gamma}{1+ab\gamma}\right)^{-\frac{1}{2}} \times\left(\frac{b(1+ab\gamma)-ab(b\gamma)}{(1+ab\gamma)^2}\right)\right\} d\gamma$$
$$= \frac{1}{2}\left\{1 - \frac{1}{\sqrt{2\pi}}\int_0^\infty e^{-\gamma(1+\frac{b}{2(1+ab\gamma)})} \times\sqrt{\frac{1+ab\gamma}{b\gamma}}\frac{b}{(1+ab\gamma)^2}d\gamma\right\}. \quad (41)$$

Perform a change of variable and let $1+ab\gamma = y$. Then $\gamma = (y-1)/ab$, $d\gamma = (1/ab)dy$:

$$P_b = \frac{1}{2}\left\{1 - \frac{1}{\sqrt{2\pi}}\frac{1}{\sqrt{a}} \times\int_1^\infty e^{-\frac{1}{ab}(y-1)[1+(b/2y)]}\sqrt{\frac{y}{y-1}}\frac{1}{y^2}\,dy\right\}. \quad (42)$$

Apply a change of variable $\cos^2\theta = 1/y$ and $2\cos\theta\sin\theta d\theta = y^{-2}dy$. Then

$$P_b = \frac{1}{2}\left\{1 - \frac{1}{\sqrt{2\pi}}\frac{1}{\sqrt{a}} \times\int_0^{\pi/2} e^{-\frac{1}{ab}(\tan^2\theta+\frac{b}{2}\sin^2\theta)}2\cos\theta\,d\theta\right\}, \quad (43)$$

or

$$P_b = \frac{1}{2}\left\{1 - \frac{1}{\sqrt{2\pi}}\frac{1}{\sqrt{\frac{K-1}{n}}} \times\int_0^{\pi/2} e^{-\frac{1}{\frac{K-1}{n}\frac{2E_b}{N_o}}(\tan^2\theta+\frac{E_b}{N_o}\sin^2\theta)}2\cos\theta\,d\theta\right\}. \quad (44)$$

APPENDIX B

SEMA with Turbo Coding in Rayleigh Fading channel.

The average BER of SEMA with Turbo coding in a Rayleigh fading is shown in (34) as $P_b = (N_{free}\bar{w}_{free}/N)E[P_2(d_{free})]$ where

$$E[P_2(d_{free})] = E\left[Q\left(\sqrt{\sum_{i=1}^{d_{free}}\left(\frac{2r_c\gamma_i}{1+2r_c\gamma_i(K-1)/n}\right)}\right)\right]. \quad (45)$$

Using the approximation $Q(\alpha) \approx 1/2\ e^{-\alpha^2/2}$

$$E[P_2(d_{free})] = \frac{1}{2}E\left[e^{-\frac{1}{2}\left(\sum_{i=1}^{d_{free}}\frac{2r_c\gamma_i}{1+2r_c\gamma_i(K-1)/n}\right)}\right] = \frac{1}{2}\int_0^\infty e^{-\frac{1}{2}\left(\sum_{i=1}^{d_{free}}\frac{2r_c\gamma_i}{1+2r_c\gamma_i(K-1)/n}\right)}f_{\bar{\Gamma}}(\bar{\gamma})d\bar{\gamma}, \quad (46)$$

where $\bar{\Gamma} = \Gamma_1\Gamma_2\cdots\Gamma_{d_{free}}$, and $\bar{\gamma} = \gamma_1\gamma_2\cdots\gamma_{d_{free}}$. Thus,

$$E[P_2(d_{free})] = \frac{1}{2}\int_0^\infty \prod_{i=1}^{d_{free}} e^{-\frac{1}{2}\left(\frac{2r_c\gamma_i}{1+2r_c\gamma_i(K-1)/n}\right)}f_{\bar{\Gamma}}(\bar{\gamma})d\bar{\gamma}. \quad (47)$$

Since γ_i's are independent and identically distributed,

$$E[P_2(d_{free})] = \frac{1}{2}\left(\int_0^\infty e^{-\frac{1}{2}\left(\frac{2r_c\gamma}{1+2r_c\gamma(K-1)/n}\right)}f_\Gamma(\gamma)d\gamma\right)^{d_{free}}$$
$$= \frac{1}{2}\ 2^{d_{free}}\left(\int_0^\infty \frac{1}{2}\ e^{-\frac{1}{2}\left(\frac{2r_c\gamma}{1+2r_c\gamma(K-1)/n}\right)}f_\Gamma(\gamma)d\gamma\right)^{d_{free}}. \quad (48)$$

Again using the approximation for $Q(\alpha) \approx 1/2\ e^{-\alpha^2/2}$, we have

$$E[P_2(d_{free})] = \frac{1}{2}\ 2^{d_{free}} \times\left(\int_0^\infty Q\left(\sqrt{\frac{2r_c\gamma}{1+2r_c\gamma(K-1)/n}}\right)\ f_\Gamma(\gamma)d\gamma\right)^{d_{free}}. \quad (49)$$

With (44) in Appendix A,

$$E[P_2(d_{free})] = \frac{1}{2}\left\{1 - \frac{1}{\sqrt{2\pi}}\frac{1}{\sqrt{\frac{K-1}{n}}} \times\int_0^{\pi/2} e^{-\frac{1}{\frac{K-1}{n}\frac{2E_c}{N_o}}(\tan^2\theta+\frac{E_c}{N_o}\sin^2\theta)}2\cos\theta\ d\theta\right\}^{d_{free}}, \quad (50)$$

and

$$P_b = \frac{1}{2}\frac{N_{free}\bar{w}_{free}}{N}\left\{1 - \frac{1}{\sqrt{2\pi}}\frac{1}{\sqrt{\frac{K-1}{n}}} \times\int_0^{\pi/2} e^{-\frac{1}{\frac{K-1}{n}\frac{2E_c}{N_o}}(\tan^2\theta+\frac{E_c}{N_o}\sin^2\theta)}2\cos\theta\ d\theta\right\}^{d_{free}}. \quad (51)$$

ACKNOWLEDGMENTS

This work was partially supported by NSF grant CCR-0098273, the Mobile Communications Research Project of the Nebraska Research Initiatives (NRI) and the Nebraska NSF-EPSCoR at the University of Nebraska-Lincoln. The authors would like to thank anonymous reviewers for their valuable comments.

REFERENCES

[1] T. F. Wong, T. M. Lok, and J. S. Lehnert, "Asynchronous multiple-access interference suppression and chip waveform selection with aperiodic random sequences," *IEEE Trans. Commun.*, vol. 47, no. 1, pp. 103–114, Jan. 1999.

[2] J. S. Lehnert and M. B. Pursley, "Error probability for binary direct-sequence spread-spectrum communications with random signature sequences," *IEEE Trans. Commun.*, vol. COM-35, no. 1, pp. 87–98. Jan. 1987.

[3] E. Geraniotis and B. Ghaffari, "Performance of binary and quaternary direct-sequence spread-spectrum multiple-access systems with random

signature sequences," *IEEE Trans. Commun.*, vol. 39, no. 5, pp. 713–724, May 1991.

[4] M. Simon *et al.*, *Spread Spectrum Communications*, vol. 1, p. 262, Computer Science Press, 1985.

[5] L. Nguyen, "Self-encoded spread spectrum and multiple access communications," in *IEEE International Symposium on Spread Spectrum Techniques and Applications*, Parsippany, NJ, Sept. 2000, pp. 394–398.

[6] Y. Kong, L. Nguyen, and W. Jang, "On the BER of self-encoded spread spectrum communication system," in *Proc. IASTED Int. Conf. Wireless and Optical Commun.*, Banff, Canada, June 27–29, 2001, pp. 202–206.

[7] Y. Kong, L. Nguyen, and W. M. Jang, "Self-encoded spread spectrum modulation with differential encoding," in *IEEE International Symposium on Spread Spectrum Techniques and Applications*, Sept. 2–5, 2002, pp. 471–474.

[8] R. K. Morrow and J. S. Lehnert, "Bit-to-bit error dependence in slotted DS/SSMA packet system with random signature sequences," *IEEE Trans. Commun.*, vol. 37, no. 10, pp. 1052–1061, Oct. 1989.

[9] S. Verdu, *Multiuser Detection*, pp. 72, 104-119, New York, Cambridge University Press, 1998.

[10] B. Vojčić and W. M. Jang, "Transmitter precoding in synchronous multiuser communications," *IEEE Trans. Commun.*, vol. 46, no. 10, pp. 1346–1355, Oct. 1998.

[11] R. Lupas and S. Verdú, "Linear multiuser detectors for synchronous code-division multiple-access channels," *IEEE Trans. Inform. Theory*, vol. 35, no. 1, pp. 123–135, Jan. 1989.

[12] W. M. Jang, B. Vojčić, and R. Pickholtz, "Joint transmitter/receiver optimization in synchronous multiuser communications over multipath channels," *IEEE Trans. Commun.*, vol. 46, no. 2, pp. 269–278, Feb. 1998.

[13] J. G. Proakis, *Digital Communications*, 4th ed., pp. 41-24, 272, 442, 824, McGraw-Hill, 2001.

[14] W. M. Jang, L. Nguyen, and M. Hempel, "Precoded random spreading multiple access system in AWGN channels," accepted to *IEEE Trans. Wireless Commun.* , 2003.

[15] J. H. Jung, W. M. Jang, and L. Nguyen, "Implementation of self-encoded spared spectrum multiple access with convolutional codes," in *Proc. IASTED Int. Conf. Wireless and Optical Commu.*, pp. 250-254, Banff, Canada, July 2002.

[16] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," in *Proc. IEEE ICC'93*, Geneva, Switzerland, 1993, pp. 1064–1070.

[17] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, 623–656, July–Oct. 1948.

[18] L. C. Perez, J. Seghers, and D. J. Costello, "A distance spectrum interpretation of turbo codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, Part I, pp. 1698–1709, Nov. 1996.

[19] J. Seghers, "On the free distance of TURBO codes and related product codes," *Final Rep., Diploma Project SS 1995*, no. 6613, p. 14, Swiss Federal Institute of Technology, Zurich, Switzerland, Aug. 1995.

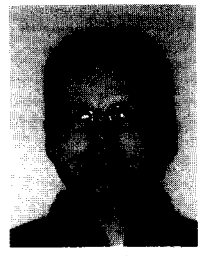
[20] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, p. 325, Englewood Cliffs, NJ: Prentice-Hall, 1983.

[21] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes*, 4th ed., pp. 89–90, McGraw-Hill, 2002.

[22] R. D. Gaudenzi, C. Elia, and R. Viola, "Bandlimited quasi-synchronous CDMA: A novel satellite access techniques for mobile and personal communication Systems," *IEEE J. Select. Areas Commun.*, vol. 10, no. 2, pp. 328–342, Feb. 1992.

Won Mee Jang received the D.Sc. Electrical Engineering degree from the George Washington University in 1996. She was with Information and Electronics Division at the Research Institute of Science and Technology (RIST), Korea, from 1988 to 1991. From 1995 to 1998, she was a wireless engineer at Comsearch, VA. She has been an assistant professor in the department of Computer and Electronics Engineering at the University of Nebraska since 1998. Her research interests include spread spectrum, satellite communications, CDMA, OFDM, signal modulation/demodulation, coding, information theory, and communication theory.

Lim Nguyen was born in Viet Nam. He received the B.S. degrees in electrical engineering and mathematics from the Massachusetts Institute of Technology in 1983, the M.S. degree in electrical engineering from the California Institute of Technology in 1991, and the Ph.D. degree from Rice University in 1996. He was an EMC engineer with the Xerox Corp. from 1983 to 1985, an RF and microwave engineer with the Hughes Aircraft Co. in 1985, and then with the Jet Propulsion Laboratory from 1985 to 1991. From 1991 to 1996, he was an electronics-optical engineer with the U.S. Air Force Phillips Laboratory. Since 1996, he has been with the Department of Computer and Electronics Engineering at the University of Nebraska-Lincoln where he is presently an Associate Professor. His current research interests include self-encoded spread spectrum, optical communications, and low-coherence interferometry using microwave photonics.



Michael Hempel was born in 1976 in Germany. He is currently working towards his Ph.D. in Computer Engineering at the University of Nebraska. His specific interests are directed at simulation software, network programming, and 3D programming. He has designed simulation tools for Information Theory. His works include simulators for Convolutional Codes and Turbo Codes. For his current research in Networking, he has been developing various network analysis tools for Internet2 and the Stream Reflector Suite. He is currently involved in the development of network simulators and secure multicast routing protocols.