Eavesdropping in the Synchronous CDMA Channel: An EM-Based Approach

Yingwei Yao and H. Vincent Poor, Fellow, IEEE

Abstract—The problem of blind detection in a synchronous code division multiple access (CDMA) system when there is no knowledge of the users' spreading sequences is considered. An expectation maximization (EM)-based algorithm that exploits the finite alphabet (FA) property of the digital communications source is proposed. Simulations indicate that this approach, which makes use of knowledge of the subspace spanned by the signaling multiplex, achieves the Cramér–Rao lower bound (CRB). The issues of subspace estimation and timing acquisition are also considered.

Index Terms—CDMA, code-free demodulation, EM algorithm.

I. INTRODUCTION

C ODE division multiple access (CDMA) is one of the most common multiple-access techniques for wireless communication systems involving nonorthogonal signaling. In recent years, various kinds of receivers have been proposed for CDMA systems [15]. All these receivers require some knowledge of the users’ spreading sequences. Here, we will consider the problem of demodulating the data in such a system without any prior knowledge of the spreading codes. This problem is essentially the same as the blind source separation problem arising in array processing. Recently, several algorithms have been proposed that take advantage of the finite alphabet (FA) property arising from the digital nature of the underlying information sources in multiple-access systems [1], [2], [6], [7], [12], [14]. One approach to this problem is to use a clustering algorithm to estimate all $2^K$ constellation points of a $K$-user binary system first and then use an assignment algorithm to resolve the directions of arrival (DOA) [1], [2]. The $K$-means algorithm [1] and a maximum-likelihood method [2] have been used to cluster the data in this type of algorithm. Two fixed-point iterative algorithms were proposed in [12]: One (ILSP) treats the problem as a continuous optimization problem and projects the results onto the discrete set, and the other one (ILSE) uses enumeration for the optimization over the discrete set. In [14], van der Veen and Paulraj present the analytical constant modulus algorithm. It is shown that in the noiseless case, this problem can be translated into a super-generalized eigenvalue decomposition and can be solved exactly and noniteratively. Here, we propose a new algorithm that treats the users’ signature sequences (equivalent to direction of arrival in array processing) as unknown parameters of a Gaussian mixture. The expectation-maximization (EM) algorithm [5], [8], [11] is then used to obtain a maximum-likelihood estimate (MLE) of these signature sequences.

We also use a subspace method to reduce the dimensionality of data before extracting the mixture parameters. Subspace-based methods have been applied widely to areas such as interference suppression and channel estimation. In CDMA systems for which the processing gain $P$ is larger than the number of users $K$, one can reduce the computational complexity and improve the tracking ability of adaptive algorithms by projecting the received signals onto the signal subspace, which has a lower dimensionality [16]. There are many algorithms for estimating the signal subspace from the received signals [19]. In this paper, we deal only with cases in which the number of users is smaller than the processing gain so that a filterbank is used as the front end of the receiver to project the received vectors onto the signal subspace.

Initially, and unless stated otherwise, we assume in this paper that the symbol timing and the signal subspace have been perfectly estimated. A discussion of the effects of the errors in these quantities is included at the end of the paper.

The rest of this paper is organized as follows. The signal model for our problem is described in Section II. In Section III, we develop an EM-based algorithm for solving this problem. In Section IV, we analyze the performance of the proposed algorithm; asymptotic and numerical results are presented. In Sections V and VI, the issues of subspace mismatch and timing acquisition, respectively, are addressed. Finally, we present our conclusions in Section VII.

II. SIGNAL MODEL

Consider a $K$-user synchronous DS-CDMA system with processing gain $P$. After chip-matched filtering and chip-rate sampling, we can model the output of such a system (in a single data symbol interval) as a $P$-dimensional vector $y$, given by

$$
y = S\hat{a} + \sigma m
$$

where $m$ is a $P$-dimensional Gaussian random vector with independent unit-variance components, $A = \text{diag}(A_1, \ldots, A_K)$ contains the $K$ users’ received amplitudes, $b = [b_1, \ldots, b_K]^T$ contains the symbols transmitted by the users, and the matrix $S$ is a $P \times K$ matrix whose columns are the $K$ users’ normalized spreading sequences

$$
S = [s_1 | \cdots | s_K].
$$

Assuming that $E\{b_kb_l^*\} = 1$ if $k = l$ and 0 if $k \neq l$, the autocorrelation matrix of the received signal $y$ is

$$
C = E\{yy^T\} = SA^2S^T + \sigma^2I_P
$$

where $I_p$ denotes the $P \times P$ identity matrix. By performing an eigenvalue decomposition on $C$, we can write

$$ C = U \Sigma U^T = [U_s \ U_n] \begin{bmatrix} \Sigma_s & 0 \\ 0 & \Sigma_n \end{bmatrix} \begin{bmatrix} U_s^T \\ U_n^T \end{bmatrix} $$

where the columns of $U_s$ are the $K$ eigenvectors associated with the $K$ largest eigenvalues of $C$. The columns of $U_s$ form a set of basis vectors of the signal subspace, that is, the subspace spanned by the spreading codes $s_1, \ldots, s_K$. By projecting the received signal $y$ onto the signal subspace, we have

$$ x = U_s^T y = Hb + cn $$

where $H = U_s^T S A$, and $n$ is a $K$-dimensional Gaussian random vector with zero mean and covariance matrix $I_K$.

Given such a model with a known signal subspace, our objective is to estimate $H$, and ultimately $b$, from multiple independent observations of $x$.

### III. EM-Based Algorithm

Assume without loss of generality that the transmitted data is binary and antipodally modulated with all symbol vectors being equally likely. Then, $x$ of (5) has a Gaussian mixture distribution with $2^K$ component densities:

$$ p(x|H) = \sum_{i=1}^{2^K} \frac{1}{2^{K}(2\pi\sigma^2)^{K/2}} \cdot \exp\left[ -\frac{1}{2\sigma^2} (x - Hb_i)^T (x - Hb_i) \right] $$

(6)

where $[b_i, \ i = 1, \ldots, 2^K]$ is the set of all $2^K$ possible transmitted vectors. Given $N$ independent snapshots of the received signals $X = [x(1), \ldots, x(N)]$, our objective is to obtain the maximum-likelihood estimate of the matrix parameter $H$. Once we have an estimate of $H$, the data can be demodulated from (5) using multiuser detection techniques.

Before we discuss an algorithm for this purpose, let us comment briefly on the identifiability of this problem. The identifiability of a finite mixture can be defined as follows [13].

Let $H$ denote the set of all finite mixtures of elements of a class $F$ of probability distributions. Suppose $H, H'$ are any two members of $H$ given by

$$ H = \sum_{j=1}^k \pi_j f_j \quad \text{and} \quad H' = \sum_{j=1}^ \pi_j' f'_j. $$

Then, $H$ is identifiable means that $H = H'$ if and only if $k = k'$, and we can order the summations such that $\pi_j = \pi'_j$ and $f_j = f'_j$ for all $j = 1, \ldots, k$.

It has been shown by Yakowitz and Spragins [18] that the finite mixtures of $n$-dimensional Gaussian distributions are identifiable. Thus, as the sample size $N$ goes to infinity, with probability 1, we can uniquely determine $2^K$ constellation points $\Gamma = [\mu_1, \ldots, \mu_{2^K}]$ from the received signals $X$. The decomposition $Y = H \tilde{B}$, where $B$ is a matrix with $\pm 1$ elements, can be shown to be unique up to a label switching and $\pm$ sign [12]. Thus, as $N \rightarrow \infty$, we can determine $H$ perfectly modulo these symmetries.

The EM algorithm is a natural choice for identifying mixture distributions. To apply the EM algorithm here, it is convenient to interpret the data $X$ as a set of incomplete data that is a part of the complete data $[x(1), \ldots, x(N), i_1, i_2, \ldots, i_N]$, where $i_n \in \{1, 2, \ldots, 2^K\}$ is a variable that indicates to which component population $x(n)$ belongs. Assuming that $x(1), \ldots, x(N)$ are independent and identically distributed (i.i.d.), the incomplete-data log-likelihood function is

$$ \log p(X|H) = \sum_{n=1}^N \log p(x(n)|H) $$

(8)

where $p(x(n)|H)$ is given in (6). The complete-data log-likelihood function is

$$ \log f(X, Z|H) = \sum_{n=1}^N \log \left[ \frac{1}{2^K} \pi_{i_n}(x(n)|H) \right] $$

(9)

where $Z = [i_1, i_2, \ldots, i_N]$, and

$$ \pi_{i_n}(x(n)|H) = \frac{1}{(2\pi\sigma^2)^{K/2}} \cdot \exp\left[ -\frac{1}{2\sigma^2} (x(n) - Hb_{i_n})^T (x(n) - Hb_{i_n}) \right]. $$

(10)

Note that since $-\log p_{i_n}$ is a quadratic function of $H$, the maximization of (9) is a much simpler problem than the maximization of (8), which corresponds to maximum-likelihood estimation. This fact is the essence of the utility of the EM algorithm for Gaussian mixtures. Basically, the EM algorithm as applied here attempts to maximize (8) by iteratively maximizing a version of (9) averaged over the “hidden” data $Z$. It is known that this technique increases (8) on each iteration, although it is possible that it could converge to a local maximum of (8). Each iteration of the EM algorithm for estimating $H$ from $X$ consists of the following two steps:

- **E-step** $Q(H|H^{(p)}) = E[\log f(X, Z|H)|X, H^{(p)}].$
- **M-step** $H^{(p+1)} = \arg \max_H Q(H|H^{(p)}).$

Here, $H^{(p)}$ is the estimate of $H$ generated by the $p$th iteration. Since (as is easily seen)

$$ Q \left( H \left| H^{(p)} \right. \right) $$

$$ = \sum_{i=1}^{2^K} \sum_{i=1}^{2^K} \sum_{m=1}^N \log \left[ \frac{1}{2^K} \pi_{i_n}(x(n)|H) \right] $$

$$ \cdot \frac{\sum_{l=1}^N p_l (x(l)|H^{(p)})}{2^K p_l (x(n)|H^{(p)})} $$

$$ = \sum_{i=1}^{2^K} \sum_{i=1}^{2^K} \sum_{m=1}^N \log \left[ \frac{1}{2^K} \pi_{i_n}(x(n)|H) \right] \cdot \frac{p_l (x(n)|H^{(p)})}{2^K p_l (x(n)|H^{(p)})} $$

(11)
the updating rule should satisfy

\[ H^{(p+1)} = \arg\max_H Q(H | H^{(p)}) \]

\[ = \arg\max_H \sum_{i=1}^{2^K} \sum_{n=1}^{N} \log[p_i(x(n) | H^{(p)})] \frac{p_i(x(n) | H^{(p)})}{p(x(n) | H^{(p)})} \]

\[ = \arg\min_H \sum_{i=1}^{2^K} \sum_{n=1}^{N} (x(n) - Hb_k)\top(x(n) - Hb_k) \]

\[ \cdot p_i(x(n) | H^{(p)}) \cdot p(x(n) | H^{(p)}) \]  

(12)

Solving this problem, we have that \( H^{(p+1)} \) solves the equation

\[ H^{(p+1)} \cdot \sum_{i=1}^{2^K} \sum_{n=1}^{N} b_{ki}b_k\top \frac{p_i(x(n) | H^{(p)})}{p(x(n) | H^{(p)})} = \sum_{i=1}^{2^K} \sum_{n=1}^{N} x(n)b_k\top \frac{p_i(x(n) | H^{(p)})}{p(x(n) | H^{(p)})} \]  

(13)

Note that if \( H^* \) is the true value of \( H \), then

\[ E \left\{ \sum_{i=1}^{2^K} \sum_{n=1}^{N} b_{ki}b_k\top \frac{p_i(x(n) | H^{*(p)})}{p(x(n) | H^{*(p)})} \right\} = 2^K I \]  

(14)

Therefore, if \( H^{(p)} \) is close to \( H^* \) and \( N \) is large, we can expect

\[ \sum_{i=1}^{2^K} \sum_{n=1}^{N} N b_{ki}b_k\top \frac{p_i(x(n) | H^{(p)})}{p(x(n) | H^{(p)})} \]

(15)

Table I

**EM-BASED ALGORITHM FOR ESTIMATING THE SPREADING CODES**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Given ( H^{(0)} ), ( p = 0 )</td>
</tr>
<tr>
<td>2</td>
<td>Compute ( w_i^{(p)}(n) = \frac{n_i(x(n)</td>
</tr>
<tr>
<td>3</td>
<td>( H^{(p+1)} = \sum_{i=1}^{2^K} \sum_{n=1}^{N} x(n)b_k\top w_i^{(p)}(n) \left( \sum_{i=1}^{2^K} \sum_{n=1}^{N} w_i^{(p)}(n)b_i\top b_i \right)^{-1} )</td>
</tr>
<tr>
<td>4</td>
<td>Repeat 2 until the algorithm converges</td>
</tr>
</tbody>
</table>

Suppose \( p \) is a finite mixture with parameter \( \Phi = (\xi_1, \ldots, \xi_v) \in \Omega \subseteq \mathbb{R}^v \) to be estimated, and \( \Phi^* \) is the true value of the parameter. Suppose further that the following conditions are satisfied.

1. There are functions \( f_i, f_{ij}, \) and \( f_{ijk} \) such that for all \( \Phi \in \Omega \), for almost all \( x \in \mathbb{R}^v \), and for \( i, j, k = 1, \ldots, v \), the partial derivatives \( \partial p_i / \partial \xi_i, \partial^2 p_i / \partial \xi_i \partial \xi_j, \) and \( \partial^3 p_i / \partial \xi_i \partial \xi_j \partial \xi_k \) exist and satisfy

\[ \left| \frac{\partial^3 p_i(x|\Phi)}{\partial \xi_i \partial \xi_j \partial \xi_k} \right| \leq f_{ijk}(x) \]  

(17)

2. The Fisher information matrix \( I(\Phi) \) is well defined and positive definite at \( \Phi^* \).

Then, given any sufficiently small neighborhood of \( \Phi^* \) in \( \Omega \), we have that with probability 1, there is for sufficiently large \( N \) a unique solution \( \Phi_N \) of the likelihood equation in that neighborhood, and this solution locally maximizes the log-likelihood function. Furthermore, \( \sqrt{N}(\Phi_N - \Phi^*) \) is asymptotically normally distributed with mean zero and covariance matrix \( I(\Phi^*)^{-1} \).

In our case, \( p \) is a Gaussian mixture density with \( 2^K \) component densities, and the parameter that needs to be estimated is the matrix \( H = U^T \Sigma A \). It is easy to show that if we restrict \( \Omega \) to be a bounded neighborhood around \( \Phi^* \), then Condition 1 is satisfied. Condition 2 can be shown to be satisfied for sufficiently large SNR through the computation of the information matrix. In particular, denote \( \Phi = [\hat{\Phi}_T, \ldots, \hat{\Phi}_K]^T \), where \( \hat{\Phi}_k \) is the \( k \)th row of \( \hat{H} \). Using the definition of the Fisher information matrix [9], we have

\[ I(\Phi) = E \left\{ \nabla_{\Phi} \log p(x|\Phi) \nabla_{\Phi}^T \log p(x|\Phi) \right\} = \{ I_{s,t} \} \]  

(18)

where \( I_{s,t} \) and \( s, t = 1, \ldots, K \) are \( K \times K \) matrices given by

\[ I_{s,t} = E \left\{ \frac{\partial \log p(x|\Phi)}{\partial s_i} \left( \frac{\partial \log p(x|\Phi)}{\partial t_j} \right)^T \right\} \]  

(19)

One can show that

\[ \frac{\partial \log p(x|\Phi)}{\partial s_i} = \frac{1}{2^K \sigma^2} \sum_{t=1}^{2^K} \frac{p_t(x|\Phi)}{p(x|\Phi)} (\bar{b}_t b_t\top s_i - x_s b_t) \]  

(20)

1In the case of binary spreading sequences and bounded signal powers, this restriction is satisfied automatically.
where \( x_s \) denotes the \( s \)th component of \( x \), and
\[
P_i(x|H) = \frac{1}{(2\pi\sigma^2)^{K/2}} \exp\left[ -\frac{1}{2\sigma^2} (x - Hb)^T (x - Hb) \right].
\]
(21)

Assuming the signal-to-noise ratios (SNRs) are sufficiently high, it follows that
\[
I(\Phi^*) \approx \frac{1}{\sigma^2} I_{K^2 \times K^2}.
\]
(22)

Therefore, we expect that \( \sqrt{N}(\Phi^N - \Phi^*) \sim N(0, \sigma^2 I_{K^2 \times K^2}) \).

The above analysis indicates that the estimation errors are asymptotically independent of the choice of the spreading sequences and users’ signal amplitudes and that the estimation errors for different entries of \( H \) are independent. Hence, the estimate of the matrix \( \hat{H} \) can be written approximately as
\[
\hat{H} = H + n_H
\]
(23)
where \( n_H = [n_{11}, \ldots, n_{K}] \) is a Gaussian random matrix, i.e.,
\[
[n_{11}^T, \ldots, n_{K}^T]^T \sim N\left(0, \sigma^2 I_{K^2 \times K^2}\right).
\]
(24)

The estimate of the \( k \)th user’s signal amplitude can be expressed as
\[
\hat{A}_k = \sqrt{\left(\hat{H}^T \hat{H}\right)_{k,k}} = \sqrt{\hat{h}_k^T h_k + 2\hat{b}_k^T n_k + n_k^T n_k}
\]
\[
\approx A_k + s_k^T U_s n_k
\]
(25)
so that the estimation error is \( s_k^T U_s n_k \sim N(0, (\sigma^2/N)) \). The estimate of the \( k \)th user’s spreading sequence is
\[
\hat{s}_k = \frac{1}{\hat{A}_k} U_s \hat{h}_k \approx \frac{1}{A_k + \frac{1}{\hat{A}_k} h_k^T n_k} U_s (h_k + n_k)
\]
\[
\approx s_k + \frac{1}{A_k} U_s n_k - \frac{1}{A_k} s_k^T U_s n_k s_k.
\]
(26)

Therefore, the estimation error here is
\[
\frac{1}{A_k} U_s n_k - \frac{1}{A_k} s_k^T U_s n_k s_k
\]
\[
\sim N\left(0, \frac{\sigma^2}{N A_k^2} (I_{K \times K} - s_k s_k^T)\right).
\]

If we use the estimates of the signature waveforms and the signal amplitudes to construct a linear MMSE multiuser detector [15], that is
\[
\hat{b}_k = \text{sgn}\left\{(\hat{M})_k\right\}
\]
(27)
where \( \hat{M} = (\hat{R} + \sigma^2 \hat{A}^2)^{-1} = \hat{A}(\hat{H}^T \hat{H} + \sigma^2)^{-1} \hat{A} \), then following the analysis of [10], the decision statistic for user 1 can be written approximately as
\[
\hat{z} = b_1 + \sum_{k=2}^{K} \hat{b}_k b_k + \frac{\sigma}{\hat{B}_1} \hat{h}_1
\]
(28)
where \( \hat{h}_1 \sim N(0, (\hat{M}R)_{1,1}) \), \( \hat{b}_k = \hat{B}_k/B_1 \), and \( \hat{B}_k = A_k (\hat{M}R)_{1,k} \). Given a realization of \( n_H \), the probability of error for user 1, say, \( P(\hat{b}_1 \neq b_1|n_H) \), can be written as
\[
P(\hat{b}_1 \neq b_1|n_H)
\]
\[
= \frac{1}{2^{K-1}} \sum_{b_2, \ldots, b_K \in \{-1, +1\}^{K-1}} Q\left(\frac{\hat{B}_1 \left(1 + \sum_{k=2}^{K} \hat{b}_k b_k\right)}{\sqrt{\hat{M}R_{1,1}} + \frac{\sigma^2}{\hat{B}_1} + \cdots + \frac{\sigma^2}{\hat{B}_K}}\right)
\]
(29)

where \( Q(\cdot) \) denotes the tail probability of the standard normal distribution. The average bit error rate \( P_1 = E\{P(\hat{b}_1 \neq b_1|n_H)\} \) can thus be evaluated using numerical integration.

### B. Numerical Examples

In the following simulation, we study the estimation errors of the EM algorithm for estimating \( H \). Assume we have a two-user synchronous CDMA system with spreading gain 31 and that the cross-correlation between the two users’ spreading sequences is equal to \(-0.29\). Both users’ signal amplitudes are set to be 1, and the SNR is 20 dB. When the number of received symbols used in the estimation is \( N = 256 \), we obtain the following results [with \( n_H \) written as in (24)]:
\[
\bar{n}_H = 10^{-4} \times [-0.7288, -0.2150, 0.1249, -0.9088]^T
\]
(30)
and
\[
\text{cov}(n_H) \times N/\sigma^2 = \begin{bmatrix}
1.0015 & -0.0006 & -0.0047 & -0.0009 \\
-0.0006 & 1.0108 & -0.0057 & -0.0002 \\
-0.0047 & -0.0057 & 0.9909 & -0.0153 \\
-0.0009 & -0.0002 & -0.0153 & 0.9908
\end{bmatrix}.
\]
(31)

We can see that the second-order statistics of \( n_H \) are well approximated by (24). While we make the assumptions that \( N \) and SNR should be sufficiently large in the derivation of (24), it holds quite well even when we use only a small number of received symbols for the estimation and when the SNR is not very high. This is shown in the following simulation results. Here, we use the same setting as the previous simulation, except now that \( N = 16 \), and the SNR is 10 dB.
\[
\bar{n}_H = [-0.0030, -0.0014, 0.0010, 0.0032]^T
\]
(32)
TABLE II
BER OBTAINED BY NUMERICAL INTEGRATION AND MONTE CARLO SIMULATIONS

<table>
<thead>
<tr>
<th>SNR(dB)</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numerical Int.</td>
<td>0.0080</td>
<td>0.0035</td>
<td>0.0012</td>
<td>3.4400×10⁻⁴</td>
<td>7.0740×10⁻⁵</td>
</tr>
<tr>
<td>Monte-Carlo</td>
<td>0.0079</td>
<td>0.0034</td>
<td>0.0012</td>
<td>3.5655×10⁻⁴</td>
<td>7.0250×10⁻⁵</td>
</tr>
</tbody>
</table>

Given a realization of \( \mathbf{n}_H \), we can compute the exact bit error rate (BER) of the linear MMSE detector constructed on the estimates of the spreading sequences using (29). Using numerical integration, we get the following results (see Table II) for the case when \( N = 256 \). For comparison, we also show the results obtained by Monte Carlo simulation of the estimation process and the decoding process. We can see that they agree with each other very well.

In Figs. 1 and 2, we compare the performance of our algorithm with several other algorithms proposed in the literature. Here, we also assume a system with two users and perfect power control. Data blocks of 16 symbols and 256 symbols are used, respectively. For comparison, we also plot the performance of the single user matched filter (designated by “MF” on the figures) and the linear MMSE detector (“MMSE”), assuming complete knowledge of the users’ spreading codes. The performance of the EM algorithm is close to that of a linear MMSE detector, especially when we use a larger data block. When we use a 16-symbol data block, the performance of all algorithms is almost indistinguishable from that of the linear MMSE detector, except that the BER of the ILSE algorithm seems to flatten out at higher SNRs.

We also investigate the performance of these algorithms in the near–far situation. We simulate a two-user system where the cross-correlation between the two users’ spreading sequences is \( -0.29 \). The SNR of the desired user is 8 dB, and the power of the interfering user is 10 dB greater than that of the desired user. Fig. 3 shows the BER performance of different algorithms when we use a 16-symbol block for the estimation. While the BER of the matched filter goes down very slowly as the SNR increases due to the severe near–far effect, the performance of the EM-based algorithm is close to that of the linear MMSE receiver, which knows the users’ spreading codes.

The dependence of the error probability on the number of received samples used \( (N) \) is plotted in Fig. 4. The system we simulate has two users with equal received power. The SNR is 8 dB, and the cross-correlation between the two users’ spreading sequences is \(-0.29\). Similarly to previous simulations, the performances of the EM-based algorithm and the ACMA algorithm
are very close to each other, and both outperform the ILSE algorithm. For the EM-based algorithm, the performance improves visibly when \( N \) is increased from 16 to 32. After the block size reaches 48, continuing to increase it yields very little further gain in performance.

Fig. 5 shows the BER performance of one user in a six-user system. The spreading gain is 31. The spreading sequences are randomly chosen and the cross-correlations between User 1’s spreading sequence and the other users’ are 0.2903, 0.1613, 0.1613, 0.0323, and 0.4194. We assume that all users have the same received power, and a block of 256 symbols has been used to estimate the users’ signature waveforms. As before, we also plot the performance of the conventional detector and the linear MMSE detector, which again, unlike the EM-based algorithm, require knowledge of all users’ spreading sequences. While the performance of our EM-based algorithm is very close to that of the MMSE detector, the performance of the traditional matched filter suffers greatly from the large multiple-access interference.

V. EFFECTS OF SUBSPACE MISMATCH

In the previous discussion, we have assumed that the signal subspace has been perfectly estimated. Here, we will investigate the effects of subspace estimation errors. Taking a block of \( L \) received symbols, we have

\[
Y = SAB + \sigma M
\]

where \( Y = [y(1) \cdots y(L)] \), \( B = [b(1) \cdots b(L)] \) contains the transmitted bits, and \( M = [m(1) \cdots m(L)] \) are independent additive white Gaussian noise vectors. The signal subspace can be estimated by performing a singular value decomposition on \( Y \):

\[
Y = [\hat{U}_s \hat{V}_s] \left[ \begin{array}{c} \Sigma_s \\ \Sigma_n \end{array} \right] \left[ \begin{array}{c} \hat{V}_s^T \\ \hat{V}_n^T \end{array} \right].
\]

It is shown in [20] that the estimated eigenvectors have the following behavior a.s.:

\[
||u_k - \hat{u}_k|| = O\left(\sqrt{\log \log L/L}\right), \quad k = 1, \ldots, P.
\]

Therefore, by projecting a received symbol onto the estimated signal subspace \( \hat{U}_s \), we have

\[
\hat{x} = \hat{U}_s^T y = Hb + \sigma n_1 + n_2
\]

where \( n_1 \) is a unit variance white Gaussian noise, and \( n_2 = (\hat{U}_s - U_s)^T y \). On denoting \( \Delta U_s = \hat{U}_s - U_s \), we have

\[
E\left\{ n_2 n_2^T | B, M \right\} = \Delta U_s^T E\left\{ yy^T \right\} \Delta U_s
\]

\[
\leq ||\Delta U_s||^2 ||SA^2S + \sigma^2 I||.
\]

Since \( ||SA^2S + \sigma^2 I|| \) is finite and \( ||\hat{U}_s - U_s|| = \sum_{k=1}^P ||\hat{u}_k - u_k|| = O(\sqrt{\log \log L/L}) \) a.s., we have that

\[
E\left\{ n_2 n_2^T \right\} = E\left\{ E\left\{ n_2 n_2^T | B, M \right\} \right\} = O(\log \log L/L).
\]

Therefore, if \( L \) is large enough, the effects of subspace estimation errors are negligible.

To illustrate this point, Fig. 6 shows the performance of the EM algorithm when different numbers of snapshots are used to estimate the signal subspace. We simulate a two-user system with perfect power control. The spreading gain is 31, and the cross-correlation between the two users’ spreading sequences is 0.29. For comparison, we also plot the performance of the single-user matched filter and the linear MMSE detector. We can see that when \( L = 256 \), the BER achieved is indistinguishable from the case where we assume perfect estimation of the signal subspace.

VI. TIMING ACQUISITION

Up to now, we have assumed both chip-level synchronization and symbol synchronization. However, in practice, these are very difficult to achieve without knowledge of the spreading
code. Between these two, the problem of chip-level synchronization is easier to deal with. In the worst case, it means 3 dB loss of SNR, and this loss may be avoided by oversampling [4]. The problem of symbol synchronization is much more serious. Near–far resistant timing acquisition algorithms have been proposed only recently, and they all require at least the knowledge of the desired user’s spreading sequence. The problem of timing acquisition when we have no knowledge of the users’ spreading sequences is even more complicated. In Fig. 7, we plot the performance of our EM-based algorithm when there are different timing offsets. These results were obtained by simulating a synchronous two-user system with perfect power control and chip-level synchronization. The SNR is 10 dB, and the crosscorrelation between two users is \(-0.29\). The performance degrades quickly when the timing offset becomes larger. Therefore, we must find a way to achieve symbol-level synchronization. Here, we will propose two possible solutions, mainly to show that it can, in principle, be done.

Let us look at a \(K\)-user synchronous system. While the setting of synchronism among different users is idealistic, it may find application in downlink communications, and it also provides some insights into the asynchronous case. Here, we assume that the symbol duration is known. If we divide the output of the chip-matched filter and chip-rate sampling into segments of length \(T\), then in the \(l\)th such segment, we get

\[
y(l) = \sum_{k=1}^{K} b_k(l)s_k^r + \sum_{k=1}^{K} b_k(l+1)s_k^l + m(l) \tag{40}
\]

where \(s_k^r, s_k^l\) is the right (left) part of the \(k\)th user’s spreading code. When synchronization is achieved, the energy in this signal will be contained in the first \(K\) principal components of the signal covariance matrix; otherwise, it will spill out to the rest of the principal components. Therefore, a heuristic way to find the synchronization point will be to try to find the point that minimizes \(\bar{\lambda} = \sum_{i=K+1}^{P} \lambda_i/(P-K)\), where \(\lambda_i\), \(i = 1, \ldots, P\) are the sample principal components.

Denote the true principal components as \(\lambda_i\), \(i = 1, \ldots, P\) and the number of snapshots used to obtain the sample covariance matrix as \(L\); then, asymptotically, \(\sqrt{L-1}(\bar{\lambda} - (\sum_{i=K+1}^{P} \lambda_i)/(P-K))\) will be distributed as a Gaussian random variable with zero mean and variance \(2\sum_{i=K+1}^{P} \lambda_i^2/(P-K)^2\) [3]. To apply this method, we need to estimate the source number \(K\) first, which can be done using AIC or MDL criteria [17]. Since we do not know the symbol timing, in general, the observation window has a timing offset with respect to the symbol intervals, and this complicates the estimation of \(K\). In Fig. 8, we show the estimated number of users \(K\) obtained using the MDL criterion under different timing offsets for a six-user system. The spreading sequences used here are the same as the ones we use for obtaining the results in Fig. 5. All users have the same power, and the SNR is 4 dB. By shifting the observation window and looking for the maximum of \(\bar{K}\), we can get a reliable estimate of \(K\), even when the SNR is very low.

Fig. 9 shows \(\bar{\lambda}\) versus different timing offsets under several situations. Here, we assume a two-user synchronous system with perfect power control and perfect chip-level synchronization. The number of snapshots used is 256. As we would have
expected, the performance degrades as the noise level and cross-correlation between users increase. The performance will also degrade in the near–far case so that this is not a near–far resistant method. To give an idea of how this algorithm will perform, we numerically evaluate the probability that \( P_1 \) the value of \( X \) at \( t_{\text{off}} = 0 \) is larger than that at \( t_{\text{off}} = 1 \) or \( -1 \). As mentioned above, asymptotically, \( X(t_{\text{off}}) \sim N\left(\mu(t_{\text{off}}), \sigma^2(t_{\text{off}})\right) \), where 
\[
\mu(t_{\text{off}}) = \sum_{i=K+1}^{P} \lambda_i(t_{\text{off}}) / (P - K), \quad \sigma^2(t_{\text{off}}) = 2 \sum_{i=K+1}^{P} \lambda_i^2(t_{\text{off}}) / (P - K)^2 / (L - 1), \quad \text{and} \quad \lambda_i(t_{\text{off}}) \text{ is the value of the true principal components when the timing offset is} \ t_{\text{off}}.
\]
Assuming that the distributions when \( t_{\text{off}} = -1, 0, 1 \) are independent from each other, we can write

\[
P_1 = 1 - \frac{1}{\sqrt{2\pi\sigma^2(0)}} \exp\left[-\frac{1}{2\sigma^2(0)} (x - \mu(0))^2\right] \cdot \left(1 - Q\left(\frac{\mu(1) - x}{\sigma(1)}\right)\right) \left(1 - Q\left(\frac{\mu(-1) - x}{\sigma(-1)}\right)\right)
\]

\[
= \int \frac{1}{\sqrt{2\pi\sigma^2(0)}} \exp\left[-\frac{1}{2\sigma^2(0)} (x - \mu(0))^2\right] \cdot \left[Q\left(\frac{\mu(1) - x}{\sigma(1)}\right) + Q\left(\frac{\mu(-1) - x}{\sigma(-1)}\right)\right] \, dx
\]

\[
= Q\left(\frac{\mu(1) - \mu(0)}{\sqrt{\sigma^2(0) + \sigma^2(1)}}\right) + Q\left(\frac{\mu(-1) - \mu(0)}{\sqrt{\sigma^2(0) + \sigma^2(-1)}}\right).
\]

From (41), we can see that as the number of snapshots used \( L \) goes to infinity, \( P_1 \) goes to 0 exponentially. Table III gives the value of \( P_1 \) under different SNRs. The parameters we use are \( K = 2, A_1 = A_2 = 1, L = 256, P = 31, \) and \( \rho = 0.74 \).

A second possible scheme for estimating timing offset is to treat the system as one with \( 2K \) virtual users and to estimate the signal amplitude of each virtual user. By comparing the received data of these virtual users, we can group them into \( K \) pairs, where each is associated with a real user. An estimate of the synchronization point can be achieved from the ratio of the signal energies of the two virtual users that form a pair. (Note that this idea can be applied to asynchronous systems as well.)

We have also implemented this second scheme, treating the system as having \( 2K \) virtual synchronous users but ignoring the dependencies between the data streams from the pair of virtual users that come from one real user. We have simulated a case of two users in which the spreading gain is 31 and the cross-correlation between two users is \( -0.29 \). When the timing offset is 15, the estimated timing offset and its covariance are

\[
E\{\hat{t}_{\text{off}}\} = 15.0384, \quad E\{(\hat{t}_{\text{off}} - E\{\hat{t}_{\text{off}}\})^2\} = 0.6636.
\]

When the timing offset is 25, they are

\[
E\{\hat{t}_{\text{off}}\} = 24.7335, \quad E\{(\hat{t}_{\text{off}} - E\{\hat{t}_{\text{off}}\})^2\} = 0.6378.
\]

As we expect, the estimation is most accurate when the timing offset is about half the spreading gain. The performance deteriorates when the timing offset is close to zero or to the spreading gain. This may be attributed to the following two phenomena: When the timing offset is close to the edge of the spreading sequences, some virtual users will contain very little energy, and the virtual signature waveforms of the virtual users may have high cross-correlations. (Of course, in these two extremes, the timing offset is minimal.)

VII. CONCLUSION

In this paper, we have considered the problem of blindly detecting the users’ data in a CDMA system with no knowledge of the users’ spreading sequences by first estimating these spreading sequences. For this estimation problem, we have proposed an EM-based algorithm that exploits the finite alphabet property of digital communications. Simulations indicate that the EM algorithm’s performance attains the CR lower bound. Effects due to subspace estimation errors and the problem of timing acquisition have also been discussed.

Although this paper deals only with the cases of synchronous systems and instantaneous channels, it is straightforward to extend this technique to asynchronous systems. When there are multipath and channel fading, we may use blind channel identification techniques to estimate the channel first before applying our algorithm. To make any blind signal separation technique practical in a CDMA system, the problem of blind timing acquisition must be solved. This latter problem can be a significant challenge in a multipath, fading channel.

REFERENCES


Yingwei Yao received B.S. and M.S. degrees in electrical engineering from Beijing University, Beijing, China, in 1994 and 1997, respectively. Currently, he is pursuing the Ph.D. degree with the Department of Electrical Engineering, Princeton University, Princeton, NJ.

His research interests are in the areas of multiuser detection and signal processing for wireless communications.

H. Vincent Poor (S’72–M’77–SM’82–F’87) received the Ph.D. degree in electrical engineering and computer science in 1977 from Princeton University, Princeton, NJ.

He is currently a Professor of electrical engineering at Princeton. He is also affiliated with Princeton’s Department of Operations Research and Financial Engineering and with its Program in Applied and Computational Mathematics. From 1977 until he joined the Princeton faculty in 1990, he was a faculty member at the University of Illinois, Urbana-Champaign. He has also held visiting and summer appointments at several universities and research organizations in the United States, Britain, and Australia. His research interests are in the area of statistical signal processing and its applications, primarily in wireless multiple-access communication networks. His publications in this area include the book *Wireless Communications: Signal Processing Perspectives*.

Dr. Poor is a member of the National Academy of Engineering and is a Fellow of the Acoustical Society of America, the American Association for the Advancement of Science, and the Institute of Mathematical Statistics. He has been involved in a number of IEEE activities, including serving as President of the IEEE Information Theory Society in 1990 and as a member of the IEEE Board of Directors in 1991 and 1992. Among his other honors are the Frederick E. Terman Award of the American Society for Engineering Education (1992), the Distinguished Member Award from the IEEE Control Systems Society (1994), the IEEE Third Millennium Medal (2000), and the IEEE Graduate Teaching Award (2001).