Secure Multiple Access Based on Multicarrier CDMA With Induced Random Flipping

Jinho Choi, *Senior Member, IEEE*, and Euiseok Hwang, *Member, IEEE*

***Abstract*—In this paper, we study secure multiple access based on multicarrier (MC) code division multiple access (CDMA) systems with induced random (chip) flipping of spreading sequence, which is suitable for machine-type communications (MTC). In MTC, devices may use low-cost hardware-based random number generators for pseudo-random noise (PN) sequences in secure communications. Since PN sequences can be estimated by correlation attacks at an eavesdropper, induced random (chip) flipping of spreading sequences is proposed to make correlation attacks infeasible. However, induced random flipping can also degrade the performance of detection and decoding at a legitimate receiver that only knows original spreading sequences. To avoid the performance degradation, we derive low-complexity iterative receiver algorithms for multiuser signal detection and decoding based on the expectation-maximization (EM) algorithm.**

***Index Terms*—Code division multiple access (CDMA), machine-type communications (MTC), random flipping, secure communications.**

I. Introduction

DUE to low hardware complexity and fast operations, stream ciphers are widely adopted for secure communications [1], [2]. In general, stream ciphers use linear feedback shift registers (LFSRs) to generate a key stream [2]. For example, the A5/1 cipher in global system for mobile communication is a stream cipher that uses LFSRs. Since stream ciphers based on LFSRs are not immune to correlation attacks, in order to avoid such attacks, a nonlinear Boolean function is considered [3], which combines the output sequences of multiple LFSRs to generate a key stream. However, exploiting the fact that the output of the nonlinear Boolean function is correlated with the output of an LFSR, it is possible to perform a correlation attack under the assumption that the output of the nonlinear Boolean function is a perturbation of a specific LFSR with a certain correlation probability. From this point of view, in [4] and [5], it is shown that there exist fast correlation attacks if the lengths of LFSRs are not long and the number of feedback taps is not large. Fast correlation attacks based on convolutional codes are further studied in [6] to apply correlation attacks to the case of a large number of feedback taps.

Although there are some well-known attacks for LFSRs, LFSRs would be still attractive for low-cost secure communications in machine-type communications (MTC) [7]–[10] as devices have limited resources and complexity. Thus, it might be important to improve the security when LFSRs are used for secure communications in MTC. In [11], the notion of physical layer security [12]–[14] is employed to strengthen the keystream generator based on LFSRs for secure communications over noisy channels. In particular, it is assumed that the channel to an eavesdropper, called Eve, has a worse quality than that to a legitimate receiver, call Bob. Both the channels are modeled as binary symmetric channels (BSCs). Furthermore, channel coding is applied to ciphertext. To Bob's channel, channel coding is to provide reliable communications or error-free transmissions. On the other hand, since Eve's channel has a worse quality than Bob's channel, there should be bit errors after decoding at Eve, which can result in a noisy ciphertext. Due to errors in ciphertext, it is shown that correlation attacks can reduce to brute-force attacks. In [15], correlation attacks are studied when Pseudo-random Noise (PN) sequences generated by LFSRs are used for physical-layer security algorithms.

Motivated by the approach in [11], in this paper, we consider a secure multiple access scheme for MTC based on multicarrier (MC) code division multiple access (CDMA) systems that use PN sequences generated by LFSRs for spreading. An eavesdropper is to recover PN sequences for despreading. In order to make correlation attacks computationally infeasible, we introduce random chip flipping in spreading sequences. That is, in the proposed approach, the spread signal is passed through a BSC prior to transmissions. As a result, some chips in a spreading sequence for a symbol duration are randomly flipped and the eavesdropper can only have a noisy ciphertext. There is a key difference from [11]. While the combination of bit flipping and channel coding (of ciphertext) is used in [11], the combination of chip flipping and (MC) spreading is employed in the proposed system. In addition, the secure MC-CDMA system in this paper is a multiuser system. Thus, there are multiple legitimate transmitters or devices in the system, which results in interuser interference (IUI) that also makes correlation attacks difficult together with random chip flipping as Eve is to receive a superposition of spread signals.

Unfortunately, random chip flipping in spreading sequences can also degrade the detection performance at a legitimate receiver, which is assumed to be a base station (BS) in this paper. Thus, the BS should consider joint optimal detection schemes that can take into account random chip flipping. To this end, the BS can employ the maximum likelihood (ML) detection.

Manuscript received May 26, 2016; revised August 28, 2016; accepted October 28, 2016. Date of publication November 1, 2016; date of current version June 16, 2017. This work was supported by Korea Electric Power Corporation through Korea Electrical Engineering and Science Research Institute under Grant R15XA03-60. This paper was presented in part at the IEEE International Conference on Communications, Kuala Lumpur, Malaysia, May 2016. The review of this paper was coordinated by Prof. C. Zhang.

The authors are with Gwangju Institute of Science and Technology, Gwangju 500712, South Korea (e-mail: jchoi0114@gist.ac.kr; euiseokh@gist.ac.kr).

Digital Object Identifier 10.1109/TVT.2016.2623791

0018-9545 © 2016 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

However, the computational complexity of the ML detection grows exponentially with the processing gain as all the possible combinations of chip flipping in a spreading sequence are to be taken into account to form the likelihood function. To avoid this difficulty, a low-complexity approach based on the expectation-maximization (EM) algorithm [16]–[18] is studied. The resulting method becomes an iterative detector that has a complexity growing linearly with the processing gain. For coded signals, we further extend the EM approach to include channel decoders and derive a low-complexity iterative receiver by employing soft interference cancelation (SIC) [19].

The main contributions of this paper are as follows.

1) A secure multiple access scheme for MTC is proposed using random chip flipping, which makes correlation attacks infeasible.
2) An iterative detection based on the EM algorithm is derived to mitigate the performance degradation at Bob by taking advantage of known unperturbed spreading sequences.
3) Iterative receivers are further derived for coded systems with multiple devices.

It is noteworthy that the proposed scheme in this paper does not provide perfect secrecy, but aims at reducing correlation attacks to brute-force attacks (which might be a best possible secrecy guarantee for the stream ciphers based on pseudorandom sequence generators to generate key sequences) by exploiting the notion of physical layer security. Consequently, the scheme can provide a computational secrecy.

The rest of the paper is organized as follows. In Section II, we present a secure multiple access scheme based on MC-CDMA with random chip flipping. We derive an iterative detection method based on the EM algorithm in Section III for uncoded systems, where we focus on the case of single device. For the case of coded systems with multiple devices, we further extend the EM algorithm with approximations to derive iterative receivers in Section IV. We present simulation results in Section V and conclude the paper with some remarks in Section VI.

Notation: Matrices and vectors are denoted by upper- and lowercase boldface letters, respectively. The superscripts T and H denote the transpose and complex conjugate, respectively. The p-norm of a vector $\mathbf{a}$ is denoted by $||\mathbf{a}||_p$ (if $p = 2$, the norm is denoted by $||\mathbf{a}||$ without the subscript). The superscript † denotes the pseudoinverse. For a vector $\mathbf{a}$, $\text{diag}(\mathbf{a})$ is the diagonal matrix with the diagonal elements from $\mathbf{a}$. For a matrix $\mathbf{X}$ (a vector $\mathbf{a}$), $[\mathbf{X}]_n$ ($[\mathbf{a}]_n$) represents the nth column (element, resp.). If n is a set of indices, $[\mathbf{X}]_n$ is a submatrix of $\mathbf{X}$ obtained by taking the corresponding columns. $\mathbb{E}[\cdot]$ and $\text{Var}(\cdot)$ denote the statistical expectation and variance, respectively. $\mathcal{CN}(\mathbf{a}, \mathbf{R})$ ($\mathcal{N}(\mathbf{a}, \mathbf{R})$) represents the distribution of circularly symmetric complex Gaussian (CSCG) (resp., real-valued Gaussian) random vectors with mean vector $\mathbf{a}$ and covariance matrix $\mathbf{R}$.

II. System Model

In this paper, we consider a multiple access scheme based on the MC-CDMA system [20] using PN sequences to spread signals for uplink transmissions from multiple devices or users[1] to a BS for multiple access in MTC, as shown in Fig 1. Unlike the conventional MC-CDMA systems, each device spreads signals with randomly perturbed PN sequences for secure communications. Note that in MTC, since each device suffers from limited resources (in terms of computing and cost), we consider low-cost hardware-based random number generators.

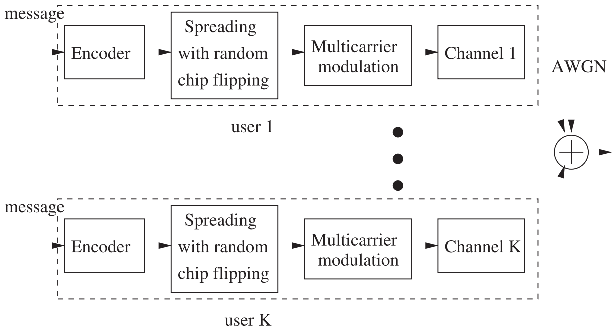


Fig. 1. MC-CDMA system with randomly perturbed spreading.

A. MC Spreading With Perturbed PN Sequences

Suppose that there is a BS, called Bob, and multiple devices or users for uplink transmissions. The number of devices or users is denoted by K. With a processing gain of L, each device, say device k, is to transmit spread signals through MC channels as

$$x_k(Lt + l) = c_k(Lt + l)s_{k;t}, \quad l = 0, \ldots, L - 1 \tag{1}$$

where $c_k(l) \in \{\pm \frac{1}{\sqrt{L}}\}$ denotes the PN sequence, and $s_{k;t} \in \mathcal{S}$ is the tth data symbol of device k. Here, $\mathcal{S}$ represents the signal constellation. Throughout the paper, we assume that $\mathbb{E}[s_{k;t}] = 0$ and $\mathbb{E}[|s_{k;t}|^2] = E_s$, where E_s represents the symbol energy. We discuss the generation of the PN sequence in Section II-B. Let $\mathbf{c}_{k;t} = [c_k(Lt) \ \ldots c_k(Lt + L - 1)]^{\mathrm{T}}$. Then, we can have

$$\begin{aligned} \mathbf{x}_{k;t} &= [x_k(Lt) \ \ldots x_k(Lt + L - 1)]^{\mathrm{T}} \\ &= \mathbf{c}_{k;t} s_{k;t}. \end{aligned} \tag{2}$$

Since the PN sequence is not totally random, Eve may perform an attack to regenerate the PN sequence. In this paper, we use a perturbed version of $c_k(l)$ that can make some known attacks ineffective. For given $\mathbf{c}_{k;t}$, a randomly perturbed version can be given by

$$\bar{\mathbf{c}}_{k;t} = \mathbf{c}_{k;t} \odot \mathbf{u}_{k;t} \tag{3}$$

where $\odot$ represents the elementwise multiplication, and

$$[\mathbf{u}_{k;t}]_i = \begin{cases} 1, & \text{w.p. } q \\ -1, & \text{w.p. } 1 - q. \end{cases} \tag{4}$$

Here, q is referred to as the induced correlation probability (and $p = 1 - q$ becomes the crossover probability of the induced chip flipping BSC) and the elements of $\mathbf{u}_{k;t}$ are independent. For convenience, let $\bar{c}_k(l)$ denote the perturbed version of $c_k(l)$ as in (3). In Fig. 2, we show that how the spread signal $x_k(l)$ can be generated using $\bar{c}_k(l)$, which can be seen as the output of BSC

[1] Throughout the paper, we assume that device and user are interchangeable.

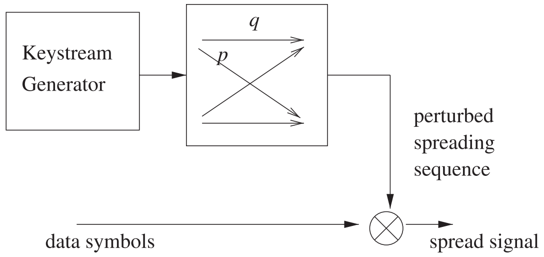


Fig. 2. Generation of spread signals by a perturbed spreading sequence from the keystream generator using chip flipping BSC with the induced correlation probability q.

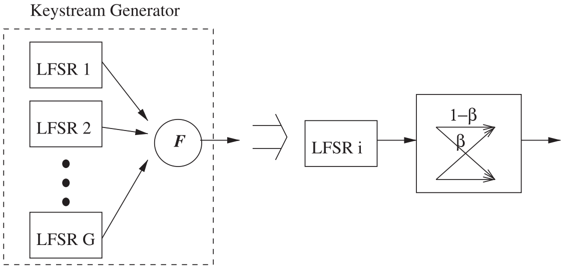


Fig. 3. Keystream generation (the left-hand side) and a model for the correlation attack (the right-hand side).

with input $c_k(l)$. For convenience, the BSC in Fig. 2 is referred to as the chip flipping BSC. Due to this BSC, $\bar{c}_k(l)$ becomes the keystream that Eve is to regenerate for eavesdropping.

Let $\{h_{i,k;t}, i = 0, \ldots, P-1\}$ denote the channel impulse response (CIR) from device k to the BS during symbol duration t, where P is the length of CIR. Then, the channel matrix in the frequency domain is given by

$$\mathbf{H}_{k;t} = \operatorname{diag}\big(H_{0,k;t}, \ldots, H_{L-1,k;t}\big) \tag{5}$$

where $H_{l,k;t} = \sum_{i=0}^{P-1} h_{i,k;t} e^{-j\frac{2\pi i l}{L}}$, $l = 0, \ldots, L-1$. At the BS, the received signal through L MCs is given by

$$\mathbf{y}_t = \sum_{k=1}^{K} \mathbf{H}_{k;t}\bar{\mathbf{c}}_{k;t}s_{k;t} + \mathbf{n}_t, \qquad t = 0, \ldots, T-1 \tag{6}$$

where $\mathbf{n}_t \sim \mathcal{CN}(0, N_0\mathbf{I})$ is the background noise, and T is the length of data packet. Throughout this paper, we assume that $\mathbf{H}_{k;t}$s are known at the BS (i.e., the legitimate receiver).

B. Correlation Attacks

Eve needs to generate the spreading sequences $c_k(l)$ to eavesdrop signals. Suppose that $c_k(l)$ is generated by a combination generator consisting of multiple binary LFSRs and a nonlinear function F, as shown in Fig. 3. It is assumed that Eve knows the structure of the generator (i.e., the polynomials of LFSRs and the nonlinear function), while the initial contents as a shared (private) key are unknown. Since Eve can easily find the initial contents of each LFSR by solving a set of linear equations [21], Eve may consider an attack for each LFSR, say LFSR i, assuming that the output of the nonlinear function F is noisy, which can be modeled by a BSC with crossover probability β, as shown in the right-hand side in Fig. 3. This attack, which is called (fast) correlation[2] attack, is studied in [4], [5], [6] and [11] with computationally efficient methods to estimate the initial contents of a target LFSR from a given (part of) keystream sequence.

In [4], correlation attacks become successful to estimate the initial contents of a target LFSR if $1-\beta$, which is called correlation probability, is sufficiently high. However, if $1-\beta$ is sufficiently low (e.g., $1-\beta \le 0.75$), correlation attacks can be reduced to brute-force attacks for a sufficiently large number of taps of the generator (e.g., more than 10 taps). Clearly, it is crucial to have a low correlation probability.

In our system, we use a randomly perturbed spreading sequence. Thus, Eve observes a noisy keystream. As a result, in correlation attacks, Eve's BSC becomes a tandem connection of two BSCs with crossover probabilities p and β. The resulting BSC has the following crossover probability:

$$p' = p(1-\beta) + (1-p)\beta = p + \beta - 2p\beta. \tag{7}$$

We can also have the following relation: $p = \frac{p'-\beta}{1-2\beta}$. Thus, although $1-\beta$ is not sufficiently low, it is possible to reduce correlation attacks to brute-force attacks using random chip flipping that can effectively lower $1-p'$, which is referred to the overall correlation probability. For example, for the case of $1-\beta = 0.7$ or $\beta = 0.3$, we can have the overall correlation probability $1-p' = 0.6$ (or $p' = 0.4$) if $p = 1/4$. This shows that correlation attacks can be infeasible by introducing random chip flipping in spreading sequences.

Furthermore, if $K > 1$, there is IUI since the spreading codes in the MC-CDMA system illustrated in Fig. 1 are not orthogonal in general (as they are PN sequences generated from LFSRs). If the IUI is taken into account in the BSC model for correlation attacks to estimate the initial vectors of LFSRs by Eve, the overall crossover probability p' may increase and correlation attacks become more difficult. Unfortunately, the performance of the signal detection or decoding at the BS is also degraded due to IUI and random chip flipping. In this paper, we focus on the derivation of iterative receivers that can provide reasonable performances by taking advantage of known spreading sequences and induced correlation probability q at the BS.

It is noteworthy that some bits in $s_{k;t}$ may not be secure although $\bar{\mathbf{c}}_{k;t}$ is not known to Eve. To see this clearly, we consider an example with $K = 1$ and $\mathcal{S} = \{-3, -1, 1, 3\}$ (i.e., 4-ary amplitude-shift keying). Furthermore, consider the following symbol mapping rule:

$$[00] \to -3, [01] \to -1, [11] \to 1, [10] \to 3$$

where the numbers in the bracket represent the bits to be mapped into an element in $\mathcal{S}$. In this example, Eve can decide the second bit from the amplitudes of the received spread signals, while Eve needs to know the spreading sequence to decide the first bit. That is, the second bit is not secure at all. We may avoid this problem by modifying the spreading operation. For example, a binary sequence before modulation can be XORed with a perturbed spreading sequence and the XORed binary sequence can be modulated. In this paper, we do not further consider

[2] For stream ciphers with pseudorandom sequence generators, correlation attacks are well known, and the security of stream cipher can be analyzed by a computational complexity to perform correlation attacks. Since the proposed approach is a variation of stream ciphers, a secrecy analysis is also based on the complexity to perform correlation attacks.

this issue and assume that only one bit per symbol (per device) would be securely transmitted by randomly perturbed spreading sequences, while the other bits are not.

C. Differences From a Similar Approach

As mentioned earlier, the proposed system is based on the approach in [11], where physical-layer security is applied to cryptography. In order to make correlation attacks difficult, error control coding (ECC) is employed under the assumption that the main channel has a higher capacity than the eavesdropper's channel when the channels are modeled by BSCs. Thanks to ECC, Bob can correct errors from the main channel (or has an error-free channel), while Eve still has errors as her channel is worse than the main channel. At Eve, the overall channel is seen as a tandem connection of two BSCs. Due to the increase of the crossover probability, correlation attacks could be reduced to brute-force attacks.

In the proposed system, the role of spreading is similar to that of ECC. In addition, since it is expected that despreading can mitigate random chip flipping in detecting spread signals, the role of despreading is similar to that of decoding in [11].

A key difference from the approach in [11] is that we consider a multiple access scheme where multiple devices transmit signal simultaneously, while the approach in [11] is for point-to-point communications. Due to randomly perturbed spreading sequences, Bob cannot successfully mitigate IUI using a conventional approach, which is different from the case in [11] where there is no IUI. In order to minimize the impact of randomly perturbed spreading sequences on the performances at Bob, we may need to employ optimal detection/decoding approaches that are usually computationally prohibitive. In other words, randomly perturbed spreading sequences can result in computational difficulties at both Eve and Bob. However, since the original spreading sequences are available at Bob, Bob can use them to derive low-complexity approaches for signal detection/decoding, as will discussed in Sections III and IV.

III. Detection of Uncoded Signals

In this section, we study the signal detection at the BS in the presence of random chip flipping and derive a low-complexity detection method by taking advantage of known unperturbed spreading sequences $\{c_k(l)\}$ and induced correlation probability q.

A. Optimal Detection

For convenience, we omit the time index t and let $\mathbf{s}_k = [s_1 \ \dots \ s_K]^{\mathrm{T}}$, $\mathbf{U} = [\mathbf{u}_1 \ \dots \ \mathbf{u}_K]$, and $\mathbf{C} = [\mathbf{c}_1 \ \dots \ \mathbf{c}_K]$. For the optimal signal detection, we consider the ML criterion. For given $\mathbf{y}$, the ML function of $\mathbf{s}$ can be given by

$$\begin{aligned} f(\mathbf{y}|\mathbf{s}) &= \sum_{\mathbf{U}\in\mathcal{U}^K} f(\mathbf{y},\mathbf{U}|\mathbf{s}) \\ &= \sum_{\mathbf{U}\in\mathcal{U}^K} f(\mathbf{y}|\mathbf{U},\mathbf{s})\Pr(\mathbf{U}|s) \\ &= \sum_{\mathbf{U}\in\mathcal{U}^K} f(\mathbf{y}|\mathbf{U},\mathbf{s})\Pr(\mathbf{U}) \end{aligned} \tag{8}$$

where $\mathcal{U}$ represents the set of all possible chip flipping vectors $\mathbf{u}_k$, and $\mathcal{U}^K$ is the Cartesian product of K $\mathcal{U}$s. The signal detection can be carried out as follows:

$$\hat{\mathbf{s}} = \underset{\mathbf{s}\in\mathcal{S}^K}{\operatorname{argmax}} f(\mathbf{y}|\mathbf{s}). \tag{9}$$

Note that if $\mathbf{C}$ is not known (which is the case of Eve), the ML function becomes

$$\begin{aligned} f(\mathbf{y}|\mathbf{s}) &= \sum_{\mathbf{C}\in\mathcal{C}^K}\sum_{\mathbf{U}\in\mathcal{U}^K} f(\mathbf{y},\mathbf{U},\mathbf{C}|\mathbf{s}) \\ &= \sum_{\mathbf{C}\in\mathcal{C}^K}\sum_{\mathbf{U}\in\mathcal{U}^K} f(\mathbf{y}|\mathbf{U},\mathbf{C},\mathbf{s})\Pr(\mathbf{U},\mathbf{C}|s) \\ &= \sum_{\mathbf{C}\in\mathcal{C}^K}\sum_{\mathbf{U}\in\mathcal{U}^K} f(\mathbf{y}|\mathbf{U},\mathbf{C},\mathbf{s})\Pr(\mathbf{U})\Pr(\mathbf{C}) \end{aligned} \tag{10}$$

where $\mathcal{C}$ represents the set of all possible spreading vectors $\mathbf{c}_k$, and $\mathcal{C}^K$ is the Cartesian product of K $\mathcal{C}$s. Clearly, we have $|\mathcal{U}| = 2^L$ and $|\mathcal{U}^K| = 2^{\mathrm{KL}}$. In addition, $|\mathcal{C}| = 2^L$ and $|\mathcal{C}^K| = 2^{\mathrm{KL}}$. For the optimal signal detection in (9), we need to find $f(\mathbf{y}|\mathbf{s})$, which is a sum of 2^{KL} terms. Thus, the computational complexity to perform the optimal detection grows exponentially with KL at Bob. Similarly, at Eve, the computational complexity to perform the optimal detection becomes $O(2^{2KL})$.

At Bob, since the elements of $\mathbf{u}_k$ are not equally likely when $p < \frac{1}{2}$, we may approximate $f(\mathbf{y}|\mathbf{s})$ in (9) with a subset of $\mathcal{U}^K$. If the number of the elements in the subset is small, the complexity of the approximate ML detection can be low. Another approach to perform the (approximate) ML detection with low complexity at Bob is to use the EM approach [16], [17], which will be explained in Section III-B. As will be shown later, the complexity of the EM approach becomes linear in L. On the other hand, at Eve, the complexity to perform the ML detection is still proportional to 2^L unless correlation attacks succeed. Furthermore, even if it is possible to obtain the likelihood function in (10), the performance of the signal detection would be limited due to the uncertainty of $\mathbf{C}$. Thus, in the rest of the paper, we do not consider the signal recovery at Eve but focus on the signal recovery at the BS or Bob with random chip flipping.

B. EM Algorithm

In (8), $f(\mathbf{y}|\mathbf{U},\mathbf{s})$ is written as

$$f(\mathbf{y}|\mathbf{U},\mathbf{s}) = C\exp\left(-\frac{1}{N_0}||\mathbf{y} - \sum_k \mathbf{H}_k(\mathbf{c}_k\odot\mathbf{u}_k)s_k||^2\right) \tag{11}$$

where C is a constant. Suppose that $\{\mathbf{U},\mathbf{s}\}$ is the complete data, while $\{\mathbf{s}\}$ is the incomplete data. Then, the E-step is given by

$$\begin{aligned} Q(\mathbf{s}|\hat{\mathbf{s}}^{(m)}) &= \mathbb{E}\left[\ln f(\mathbf{U},\mathbf{y}|\mathbf{s})|\mathbf{y},\hat{\mathbf{s}}^{(m)}\right] \\ &= \mathbb{E}\left[\ln f(\mathbf{y}|\mathbf{U},\mathbf{s})\Pr(\mathbf{U}|\mathbf{s})|\mathbf{y},\hat{\mathbf{s}}^{(m)}\right] \\ &= \mathbb{E}\left[\ln f(\mathbf{y}|\mathbf{U},\mathbf{s})|\mathbf{y},\hat{\mathbf{s}}^{(m)}\right] + \mathbb{E}\left[\ln\Pr(\mathbf{U})|\mathbf{y},\hat{\mathbf{s}}^{(m)}\right] \\ &= -\frac{1}{N_0}\mathbb{E}\left[||\mathbf{y} - \sum_k \mathbf{H}_k(\mathbf{c}_k\odot\mathbf{u}_k)s_k||^2|\mathbf{y},\hat{\mathbf{s}}^{(m)}\right] \\ &\quad + C' \end{aligned} \tag{12}$$

where C' is a constant, and $\hat{\mathbf{s}}^{(m)}$ is the estimate of $\mathbf{s}$ at the mth iteration. Throughout this paper, m is used to represent the EM iteration index. Note that one EM iteration consists of one E-step and one M-step.

To obtain $Q(\mathbf{s}|\hat{\mathbf{s}}^{(m)})$, $\Pr(u_{l,k}|\mathbf{y}, \mathbf{s}^{(m)})$ is required. To this end, we can show that

$$\begin{aligned}\Pr\left(\mathbf{U}|\mathbf{y}, \hat{\mathbf{s}}^{(m)}\right) &\propto f\left(\mathbf{y}|\mathbf{U}, \hat{\mathbf{s}}^{(m)}\right) \Pr\left(\mathbf{U}, \hat{\mathbf{s}}^{(m)}\right) \\ &\propto \left(\prod_l e^{-\frac{1}{N_0}|y_l - \sum_k c_{l,k} u_{l,k} H_{l,k} \hat{s}_k^{(m)}|^2}\right) \Pr(\mathbf{U}) \\ &= \prod_l \phi_l(\mathbf{a}_l) \qquad (13)\end{aligned}$$

where $\mathbf{a}_l = [u_{l,1} \, \ldots \, u_{l,K}]^{\mathrm{T}}$ (i.e., $\mathbf{a}_l^{\mathrm{T}}$ is the lth row of $\mathbf{U}$), and

$$\phi_l(\mathbf{a}_l) = e^{-\frac{1}{N_0}|y_l - \sum_k c_{l,k} u_{l,k} H_{l,k} \hat{s}_k^{(m)}|^2} \Pr(\mathbf{a}_l). \qquad (14)$$

Here, $c_{l,k}$ and $u_{l,k}$ denote the lth elements of $\mathbf{c}$ and $\mathbf{u}$, respectively, and $\Pr(\mathbf{a}_l) = \prod_{k=1}^{K} \Pr(u_{l,k})$. As shown in (13), $\mathbf{a}_l$s are independent. Thus, for each l, we can find $\Pr(u_{l,k}|\mathbf{y}, \mathbf{s}^{(m)})$, $k = 1, \ldots, K$, from $\phi(\mathbf{a}_l)$.

As shown in (14), the computational complexity to obtain $\phi_l(\mathbf{a}_l)$ for all l is $O(L2^K)$ that is lower than the computational complexity for the optimal detection in Section III-A, which is $O(2^{\mathrm{KL}})$. However, the computational complexity of the EM algorithm is still high for a large K as it grows exponentially with K. Thus, we now focus on the case of $K = 1$ (i.e., a single-device system). We will discuss the case of $K > 1$ with channel coding in Section IV.

Suppose that $K = 1$. From (4), we have $\Pr(u_{l,1} = +1) = q$ and $\Pr(u_{l,1} = -1) = 1 - q$. Let $\kappa = 1 - q/q$. Then, it can be shown that

$$\begin{aligned}\bar{u}_{l,1}^{(m)} &= \mathbb{E}\left[u_{l,1}|\mathbf{y}, \hat{s}_1^{(m)}\right] \\ &= \frac{\phi_l(u_{l,1} = 1) - \phi_l(u_{l,1} = -1)}{\phi_l(u_{l,1} = 1) + \phi_l(u_{l,1} = -1)} \\ &= \frac{1 - \kappa e^{-\frac{4}{N_0}\Re(y_l^* c_{l,1} H_{l,1} \hat{s}_1^{(m)})}}{1 + \kappa e^{-\frac{4}{N_0}\Re(y_l^* c_{l,1} H_{l,1} \hat{s}_1^{(m)})}}. \qquad (15)\end{aligned}$$

Since

$$\begin{aligned}||\mathbf{y} - \mathbf{H}_1(\mathbf{c}_1 \odot \mathbf{u}_1)s_1||^2 &= ||\mathbf{y}||^2 + |s_1|^2 ||\mathbf{H}_1(\mathbf{c}_1 \odot \mathbf{u}_1)||^2 \\ &\quad - 2\Re(\mathbf{y}^{\mathrm{H}} \mathbf{H}_1(\mathbf{c}_1 \odot \mathbf{u}_1)s_1) \\ &= ||\mathbf{y}||^2 + A|s_1|^2 \\ &\quad - 2\Re(\mathbf{y}^{\mathrm{H}} \mathbf{H}_1(\mathbf{c}_1 \odot \mathbf{u}_1)s_1) \qquad (16)\end{aligned}$$

where $A = \frac{\sum_l |H_{l,1}|^2}{L}$, we have

$$\begin{aligned}&\mathbb{E}\left[||\mathbf{y} - \mathbf{H}_1(\mathbf{c}_1 \odot \mathbf{u}_1)s_1||^2|\mathbf{y}, \hat{s}_1^{(m)}\right] \\ &= ||\mathbf{y}||^2 + A|s|^2 - 2\Re\left(\mathbf{y}^{\mathrm{H}} \mathbf{H}_k\left(\mathbf{c}_k \odot \bar{\mathbf{u}}_1^{(m)}\right)s_1\right) \qquad (17)\end{aligned}$$

where $\bar{\mathbf{u}}_1^{(m)} = \mathbb{E}[\mathbf{u}_1|\mathbf{y}, \hat{s}_1^{(m)}]$, which is available from (15). Finally, the M-step is given by

$$\begin{aligned}\hat{s}_1^{(m+1)} &= \operatorname*{argmax}_{s_1 \in \mathcal{S}} Q(s_1|\hat{s}_1^{(m)}) \\ &= \operatorname*{argmin}_{s_1 \in \mathcal{S}} A|s_1|^2 - 2\Re\left(\mathbf{y}^{\mathrm{H}} \mathbf{H}(\mathbf{c}_1 \odot \bar{\mathbf{u}}_1^{(m)})s_1\right). \qquad (18)\end{aligned}$$

If $|\mathcal{S}| = M$ is small, we can use an exhaustive search to find $\hat{s}_1^{(m+1)}$.

In summary, the EM algorithm for the ML detection for a single-device system (i.e., $K = 1$) can be shown as follows.

A0) Let $m = 0$ and $[\bar{\mathbf{u}}_1^{(m)}]_i = 1$ for all i.

A1) Perform the M-step in (18) with $\bar{\mathbf{u}}_1^{(m)}$ and find $\hat{s}_1^{(m+1)}$.

A2) Update $m \leftarrow m + 1$ and perform the E-step in (15) with $\hat{s}_1^{(m)}$ and find $\bar{\mathbf{u}}_1^{(m)}$.

A3) If $||\bar{\mathbf{u}}_1^{(m-1)} - \bar{\mathbf{u}}_1^{(m)}|| \leq \epsilon$, stop. Otherwise, move A1).

The complexity of the EM algorithm is linear in L, as shown in (15) and (18). Note that it is not always guaranteed that the EM algorithm converges to the ML solution [17]. In particular, it is important to have a good initial solution in the EM algorithm. At Bob, the initial vectors of $\{\mathbf{u}_k\}$ can be all one vectors if p is not too large, i.e., the unperturbed spreading sequences can be used as the initial spreading sequences. This initial setup can provide good performances of the EM algorithm as shown in Section V-A, which implies that Bob can take advantage of known unperturbed spreading sequences that are used as good initial spreading sequences.

IV. Iterative Receivers for Coded Multiuser Systems With Approximations

In Section III, we consider the signal detection for uncoded systems and focus on the EM algorithm as a low-complexity detection algorithm when there is a single device transmitting signal. However, in multiple access, there are multiple devices that transmit signals simultaneously. In this section, we consider an approximation to lower complexity for the case of $K > 1$ and derive iterative receivers for the coded system that is illustrated in Fig. 1.

A. Approximation of $\bar{u}_{l,k}^{(m)}$

Since the complexity to find $\bar{u}_{l,k}^{(m)}$ is high for a large K, we consider an approximation in this section.

For convenience, let $\mathbf{s} = \hat{\mathbf{s}}^{(m)}$, which is assumed to be known. In order to estimate $\bar{u}_{l,k}^{(m)}$, we can consider an iterative approach based on the Gaussian approximation.

As in (13), since $\mathbf{a}_l$s are independent, we consider a specific $\mathbf{a}_l$ omitting the index l for notational convenience. Then, $y_l = y$ can be written as

$$y = \sum_k c_k H_k s_k u_k + n. \qquad (19)$$

Let $b_k = c_k H_k s_k$, which is known. Furthermore, suppose that we have prior information of u_k as follows:

$$\mathbb{E}[u_k] = \bar{u}_k \text{ and } \mathrm{Var}(u_k) = 1 - \bar{u}_k^2.$$

Note that the variance of u_k is due to the fact that $u_k \in \{-1, +1\}$. With the *a priori* probability of $\{u_1, \ldots, u_{k-1}, u_{k+1}, \ldots, u_K\}$, we can update the mean of u_k. However, since u_k is binary, this updating may require a high complexity. To avoid it, we can consider a Gaussian approximation as follows:

$$y = b_k u_k + \sum_{k' \neq k} b_{k'} u_{k'} + n = b_k u_k + n_k \tag{20}$$

where $n_k = n + \sum_{k' \neq k} b_{k'} u_{k'}$ is assumed to be Gaussian. That is, we assume that $n_k \sim \mathcal{CN}(\mu_{-k}, \sigma_{-k}^2)$, where

$$\mu_{-k} = \sum_{k' \neq k} b_{k'} \bar{u}_{k'} \text{ and } \sigma_{-k}^2 = N_0 + \sum_{k' \neq k} |b_{k'}|^2 \big(1 - \bar{u}_{k'}^2\big). \tag{21}$$

Based on this Gaussian approximation, the mean of u_k is updated as

$$\bar{u}'_k(\bar{\mathbf{u}}_{-k}) = \frac{1 - \kappa e^{-\frac{4}{\sigma_{-k}^2}\Re(\hat{y}_{-k}^* b_k)}}{1 + \kappa e^{-\frac{4}{\sigma_{-k}^2}\Re(\hat{y}_{-k}^* b_k)}} \tag{22}$$

where $y_{-k} = y - \mu_{-k}$, and $\bar{\mathbf{u}}_{-k} = [\bar{u}_1, \ldots, \bar{u}_{k-1}, \bar{u}_{k+1}, \ldots, \bar{u}_K]^{\mathrm{T}}$.

In summary, we can consider an iterative method, which is referred to as the Gaussian approximation based iterative method (GAIM) to estimate $\bar{u}_k$ as follows.

I0) Let $i = 0$ (here, i is used as the GAIM iteration index) and

$$\bar{u}_k^{(0)} = \Pr(u_k = 1) - \Pr(u_k = -1) = 1 - 2p, \quad \text{for all } k.$$

I1) Update the mean value of u_k as in (22), i.e.,

$$\bar{u}_k^{(i+1)} = \bar{u}'_k\big(\bar{\mathbf{u}}_{-k}^{(i)}\big), \quad \text{for all } k.$$

I2) Stop if $\sum_k |\bar{u}_k^{(i+1)} - \bar{u}_k^{(i)}| \le \epsilon$ or $i \ge I_{\max}$, where ϵ and $I_{\max}$ are a small constant and the maximum number of iterations, respectively. Otherwise, $l \leftarrow l + 1$ and move to I1).

Note that there is no guarantee that the GAIM converges.

B. Case of Coded Systems With Multiple Devices

In Section III-B, we only consider the M-step for uncoded single-device systems. In this section, we extend it to the case of coded systems with multiple active devices transmitting signals simultaneously.

It can be shown that

$$\begin{aligned}||\mathbf{y} - \sum_k \mathbf{H}_k(\mathbf{c}_k \odot \mathbf{u}_k)s_k||^2 &= ||\mathbf{y} - \sum_k \mathbf{v}_k s_k||^2 \\ &= ||\mathbf{y}||^2 + \mathbf{s}^{\mathrm{H}}\mathbf{V}^{\mathrm{H}}\mathbf{V}\mathbf{s} \\ &\quad - 2\Re(\mathbf{y}^{\mathrm{H}}\mathbf{V}\mathbf{s})\end{aligned} \tag{23}$$

where $\mathbf{v}_k = \mathbf{H}_k(\mathbf{c}_k \odot \mathbf{u}_k)$, and $\mathbf{V} = [\mathbf{v}_1 \ \ldots \ \mathbf{v}_K]$. Let $\bar{\mathbf{V}}^{(m)} = \mathbb{E}[\mathbf{V}|\mathbf{y}, \hat{\mathbf{s}}^{(m)}]$ and $\mathbf{\Phi}^{(m)} = \mathbb{E}[\mathbf{V}^{\mathrm{H}}\mathbf{V}|\mathbf{y}, \hat{\mathbf{s}}^{(m)}]$. Then, we have

$$\begin{aligned}&\mathbb{E}[||\mathbf{y} - \mathbf{V}\mathbf{s}||^2 \,|\, \mathbf{y}, \hat{s}^{(m)}] \\ &\quad = ||\mathbf{y}||^2 + \mathbf{s}^{\mathrm{H}}\mathbf{\Phi}^{(m)}\mathbf{s} - 2\Re\left(\mathbf{y}^{\mathrm{H}}\bar{\mathbf{V}}^{(m)}\mathbf{s}\right)\end{aligned} \tag{24}$$

It can be shown that $\bar{\mathbf{V}}^{(m)} = [\bar{\mathbf{v}}_1^{(m)} \ \ldots \ \bar{\mathbf{v}}_K^{(m)}]$, where

$$\big[\bar{\mathbf{v}}_k^{(m)}\big]_l = H_{l,k} c_{l,k} \mathbb{E}\big[u_{l,k}|\mathbf{y}, \mathbf{s}^{(m)}\big] = H_{l,k} c_{l,k} \bar{u}_{l,k}^{(m)}. \tag{25}$$

Here, $\bar{u}_{l,k}^{(m)} = \mathbb{E}[u_{l,k}|\mathbf{y}, \mathbf{s}^{(m)}]$. We can also show that

$$\begin{aligned}\big[\mathbf{\Phi}^{(m)}\big]_{k',k} &= \mathbb{E}\big[\mathbf{v}_{k'}^{\mathrm{H}}\mathbf{v}_k\big] \\ &= \sum_l H_{l,k'}^* H_{l,k} c_{l,k'} c_{l,k} \mathbb{E}\big[u_{l,k'} u_{l,k}|\mathbf{y}, \mathbf{s}^{(m)}\big] \\ &= \begin{cases}(\bar{\mathbf{v}}_{k'}^{(m)})^{\mathrm{H}}\bar{\mathbf{v}}_k^{(m)}, & \text{if } k' \neq k \\ A_k, & \text{if } k' = k\end{cases}\end{aligned} \tag{26}$$

where $A_k = \frac{1}{L}\sum_k |H_{l,k}|^2$. Thus, once we estimate $\bar{u}_{l,k}^{(m)}$ using the GAIM, $\mathbf{v}_k$ can be found as in (25). Finally, the M-step is given by

$$\begin{aligned}\mathbf{s} &= \operatorname*{argmax}_{\mathbf{s} \in \mathcal{S}^K} Q\big(\mathbf{s}|\hat{\mathbf{s}}^{(m)}\big) \\ &= \operatorname*{argmin}_{\mathbf{s} \in \mathcal{S}^K} \mathbf{s}^{\mathrm{H}}\mathbf{\Phi}^{(m)}\mathbf{s} - 2\Re\big(\mathbf{y}^{\mathrm{H}}\bar{\mathbf{V}}^{(m)}\mathbf{s}\big).\end{aligned} \tag{27}$$

This M-step is to be generalized for coded signals.

In order to explain the M-step for coded signals, we need to include the time index t. Suppose that for each device $\{s_{k;0}, \ldots, s_{k,T-1}\} \in \mathcal{C}_k$ is a coded signal sequence that is a code word in the codebook $\mathcal{C}_k$ for device k. Let $\mathbf{s}_t = [s_{1;t} \ \ldots \ s_{K;t}]^{\mathrm{T}}$, $\mathbf{v}_{k;t} = \mathbf{H}_{k;t}(\mathbf{c}_{k;t} \odot \mathbf{u}_{k;t})$, and $\mathbf{V}_t = [\mathbf{v}_{1;t} \ \ldots \ \mathbf{v}_{K;t}]$. Furthermore, let $\bar{\mathbf{V}}_t^{(m)} = \mathbb{E}[\mathbf{V}_t|\mathbf{y}_t, \hat{\mathbf{s}}_t^{(m)}]$ and $\mathbf{\Phi}_t^{(m)} = \mathbb{E}[\mathbf{V}_t^{\mathrm{H}} \mathbf{V}_t|\mathbf{y}_t, \hat{\mathbf{s}}_t^{(m)}]$. Then, the M-step is given by

$$\{\mathbf{s}_t\} = \operatorname*{argmin}_{\{\mathbf{s}\} \in \mathcal{C}} \sum_t \mathbf{s}_t^{\mathrm{H}}\mathbf{\Phi}_t^{(m)}\mathbf{s} - 2\Re\big(\mathbf{y}_t^{\mathrm{H}}\bar{\mathbf{V}}_t^{(m)}\mathbf{s}_t\big) \tag{28}$$

where $\mathcal{C} = \mathcal{C}_1 \times \cdots \times \mathcal{C}_K$. This shows that the M-step is joint decoding for K coded signals, which is computationally prohibitive. Thus, we need to resort to any suboptimal approaches.

The first suboptimal approach is based on the correlator. To the channel decoder for each device, the output of the correlator with the estimated perturbed spreading sequence can be used, which is given by

$$z_k^{(m)} = \sum_{l=0}^{L-1} y_l H_{l,k}^* c_{l,k} \bar{u}_{l,k}^{(m)} = \big(\bar{\mathbf{v}}_k^{(m)}\big)^{\mathrm{H}}\mathbf{y} \tag{29}$$

where the time index t is omitted for notational convenience. If K is small and L is large, the correlator can reasonably mitigate interference from the other devices. The hard decision of the output of a channel decoder becomes $\hat{\mathbf{s}}^{(m+1)}$. The resulting approach is referred to as the iterative receiver with correlator.

Another approach is based on the minimum mean squared error (MMSE) with SIC [19]. In each iteration, the interference from the other devices is to be mitigated by SIC. At the mth iteration, we decompose $\mathbf{V}$ as $\mathbf{V} = \bar{\mathbf{V}} + \tilde{\mathbf{V}}$, where $\bar{\mathbf{V}} = \bar{\mathbf{V}}^{(m)}$. Here, we omit the EM iteration index m for notational convenience. To decide a soft decision of s_k as an input to a channel decoder, $\mathbf{y}$ is to be rewritten as

$$\begin{aligned}\mathbf{y} &= \bar{\mathbf{V}}\mathbf{s} + \tilde{\mathbf{V}}\mathbf{s} + \mathbf{n} \\ &= \bar{\mathbf{v}}_k s_k + \sum_{q \neq k} \mathbf{v}_q s_q + \tilde{\mathbf{V}}\mathbf{s} + \mathbf{n}. \end{aligned} \tag{30}$$

From the previous EM iteration, suppose that the mean values of $\{s_q\}$, $q \neq k$ are available. Then, the SIC can be carried out as follows:

$$\mathbf{y}_k = \mathbf{y} - \sum_{q \neq k} \bar{\mathbf{v}}_q \bar{s}_q = \bar{\mathbf{v}}_k s_k + \mathbf{w}_k \tag{31}$$

where $\mathbf{w}_k = \sum_{q \neq k} \bar{\mathbf{v}}_q \tilde{s}_q + \tilde{\mathbf{V}}\mathbf{s} + \mathbf{n}$. The covariance matrix of $\mathbf{w}_k$ can be obtained as

$$\begin{aligned}\boldsymbol{\Sigma}_k &= \mathbb{E}\left[\mathbf{w}_k \mathbf{w}_k^{\mathrm{H}}\right] \\ &= \sum_{q \neq k} \bar{\mathbf{v}}_q \bar{\mathbf{v}}_q^{\mathrm{H}} \tilde{\sigma}_q^2 + E_s \mathbb{E}\left[\tilde{\mathbf{V}}\tilde{\mathbf{V}}^{\mathrm{H}}\right] + N_0 \mathbf{I}. \end{aligned} \tag{32}$$

It can be shown that

$$\begin{aligned}\left[\mathbb{E}\left[\tilde{\mathbf{V}}\tilde{\mathbf{V}}^{\mathrm{H}}\right]\right]_{l,l'} &= \left(\frac{1}{L}\sum_{k=1}^{K} |H_{l,k}|^2 \mathbb{E}\left[|u_{l,k} - \bar{u}_{l,k}|^2\right]\right)\delta_{l,l'} \\ &= \left(\frac{1}{L}\sum_{k=1}^{K} |H_{l,k}|^2 (1 - \bar{u}_{l,k}^2)\right)\delta_{l,l'}. \end{aligned} \tag{33}$$

The MMSE estimate of s_k after SIC is finally given by

$$z_k = \boldsymbol{\Sigma}_k^{-1} \bar{\mathbf{v}}_k^{\mathrm{H}} \mathbf{y}_k. \tag{34}$$

This becomes the input to the channel decoder for device k. The output of the channel decoder becomes the output of the M-step, i.e., $\hat{s}_k^{(m+1)} = [\hat{\mathbf{s}}^{(m+1)}]_k$. The resulting approach is referred to as the iterative receiver with MMSE-SIC detector.

V. Simulation Results

In this section, we present simulation results with 64-quadrature amplitude modulation. Each tap of the CIR $h_{i,k;t}$ is assumed to be an independent zero-mean CSCG random variable with variance $1/P$ with $P = 6$ (i.e., Rayleigh fading is assumed). In Sections V-A and V-B, we discuss simulation results of uncoded cases of $K = 1$ and coded cases of $K \geq 1$, respectively.

A. Simulation Results of Uncoded Systems With $K = 1$

In this section, we consider uncoded systems with $K = 1$ with a processing gain of $L = 64$. The signal-to-noise ratio (SNR) is given by SNR $= E_s/N_0$.

Fig. 4 shows the symbol error rate (SER) for various SNRs with $p = 0.25$. For the initialization of the EM algorithm, we assume that $\bar{u}_{l,1}^{(0)} = 1$. The performance after the first iteration is poor as the estimation of $u_{l,1}$ is not satisfactory. However, after the second iteration, we can see that the performance is significantly improved at a high SNR and a better performance can be achieved with more iterations.

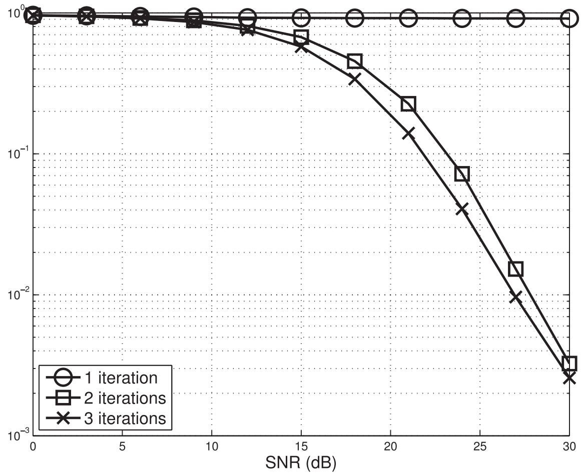


Fig. 4. SER versus SNR ($L = 64$ and $p = 0.25$).

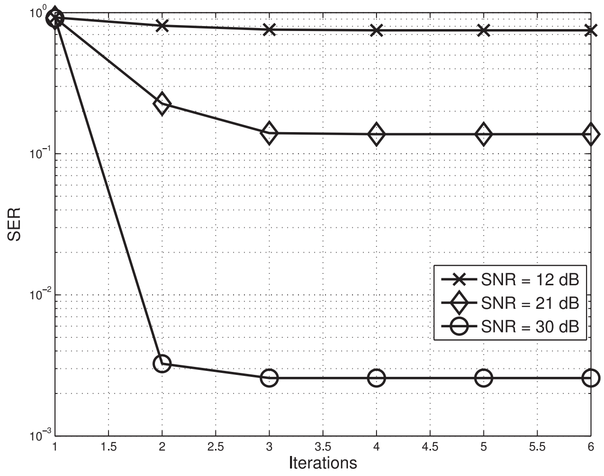


Fig. 5. SER over iterations ($L = 64$ and $p = 0.25$).

In order to see the performance of the EM algorithm over iterations, we show the SERs for various numbers of iterations in Fig. 5 with $p = 0.25$. It is shown that three EM iterations might be sufficient for reasonable performances.

Fig. 6 shows the SERs for various values of p. As mentioned earlier, it is desirable to have a high crossover probability p of the chip flipping BSC to make correlation attacks computationally infeasible, which can also result in a degraded detection performance at Bob as shown in Fig. 6. However, it is shown that at a high p, Bob can still have a reasonable SER with the EM algorithm (after three iterations).

B. Simulation Results of Coded Systems With $K \geq 1$

In this section, we present simulation results of coded systems with $K \geq 1$ where each device employs a rate-half convolutional code with a random bit interleaver. The generator polynomial of the convolutional code is $(5, 7)$ in octal. At the receiver, we use the BCJR algorithm [22] to provide soft decision for the MMSE-SIC detector. For coded systems, we consider E_b/N_0 for the SNR, which is given by

$$\frac{E_{\mathrm{b}}}{N_0} = \frac{E_s}{N_0 R_{\mathrm{c}} \log_2 M}$$

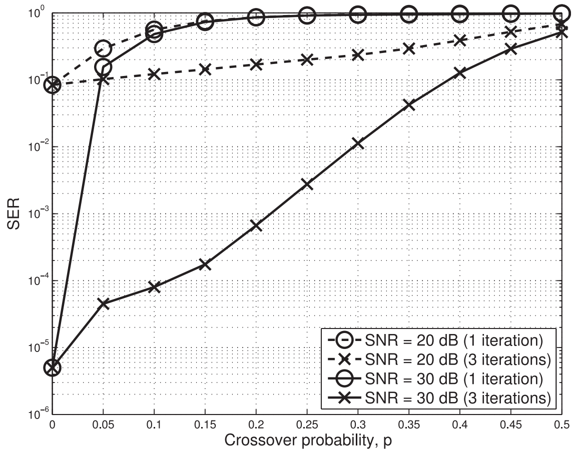


Fig. 6. Performances of SER for various values of p.

where R_c denotes the code rate (which is 1/2). In each EM iteration, the maximum number of GAIM iterations is set to 20 in all the simulations in this section.

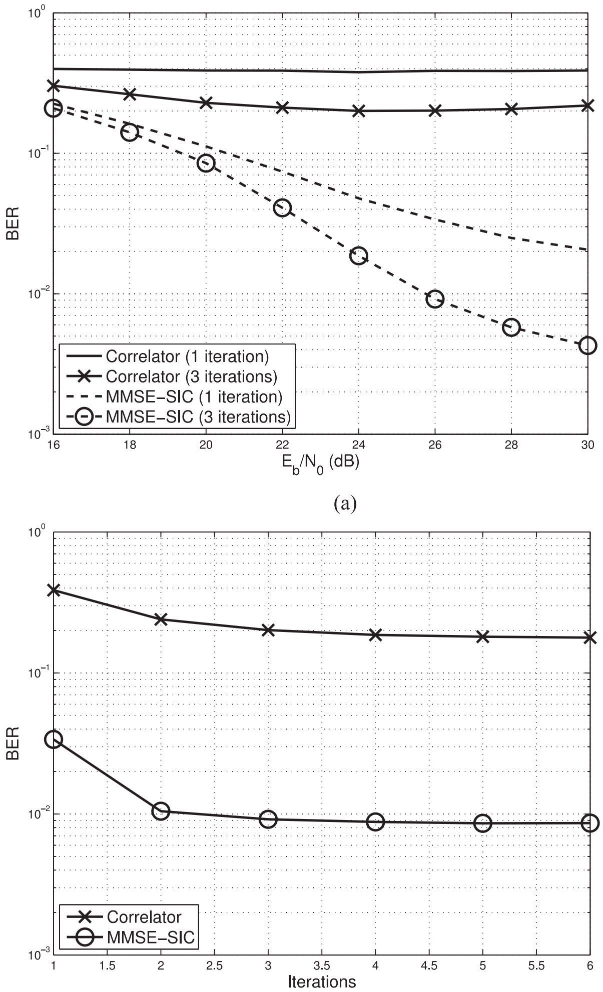
Fig. 7 shows the performances of the iterative receivers with correlator and MMSE-SIC detector when $L = 64$, $p = 0.1$, and $K = 4$. As shown in Fig. 7(a), the iterative receiver with MMSE-SIC detector performs better than that with correlator as the IUI can be suppressed by SIC using the soft decisions from the previous EM iteration. We can also see that the performance can be improved with more iterations, as shown in Fig. 7(b). We may need three iterations for reasonable performances.

It is noteworthy that as shown in Fig. 7(a), the performance of the coded systems with $K \geq 1$ is not significantly improved as the SNR increases, which is different from that of uncoded systems with $K = 1$ shown in Fig. 4. This difference results from the existence of IUI and errors in estimating $\bar{\mathbf{u}}_k$ in the case of $K > 1$. Thus, a better performance could be obtained if a better estimator of $\bar{\mathbf{u}}_k$ can be employed.

Fig. 8 shows the performances for various values of p when $L = 64$, $E_b/N_0 = 30$ dB, and $K = 4$. It is shown that the performance is quickly degraded as p increases. Note that as mentioned earlier, the overall crossover probability p' can effectively increase due to IUI in the multiuse case. Thus, a small value of the crossover probability of the induced chip flipping BSC p could be sufficient to reduce Eve's correlation attacks to brute-force attacks, and Bob can have reasonably good performances (e.g., if $p = 0.1$, the coded BER of the iterative receiver with MMSE-SIC is around 3×10^{-3} after three iterations).

The impact of K on the performance is shown in Fig. 9 when $L = 64$, $E_b/N_0 = 30$ dB, and $p = 0.1$. If K is small (e.g., $K = 2$), we can see that a low BER (less than 10^{-4}) can be achieved by the iterative receiver with MMSE-SIC. For a small K, since the IUI is limited, a good estimate of $\bar{\mathbf{u}}_k$ can be obtained, which results in a better mitigation performance of the other spread signals by the MMSE-SIC detector. From this, a low-coded BER can be obtained for a small K.

Fig. 10 shows the performance for various values of L when $K = 4$, $E_b/N_0 = 30$ dB, and $p = 0.1$. It is shown that as L increases, the Bob's performance can be improved, and the



(a)

(b)

Fig. 7. Performances of the iterative receivers with the correlator and MMSE-SIC detector when $L = 64$, $p = 0.1$, and $K = 4$. (a) Coded BER versus E_b/N_0. (b) coded BER versus iterations.

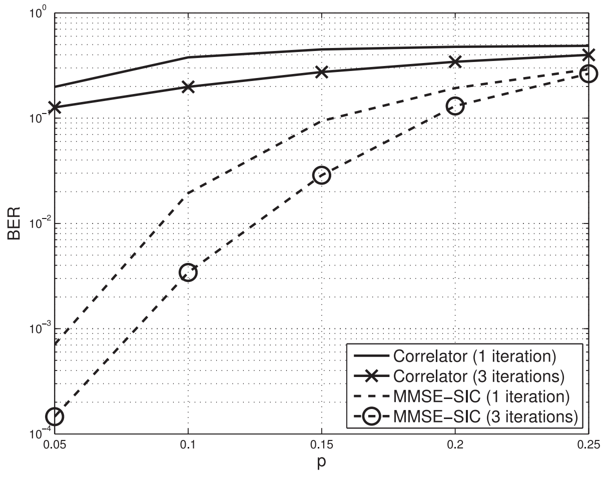


Fig. 8. Performances of coded BER for various values of p when $L = 64$, $E_b/N_0 = 30$ dB, and $K = 4$.

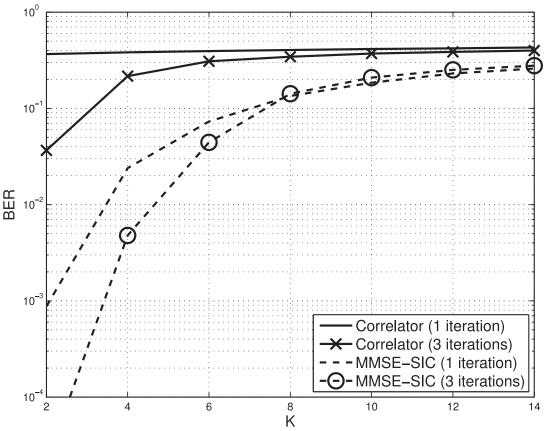


Fig. 9. Performances of coded BER for various values of K when $L = 64$, $E_b/N_0 = 30$ dB, and $p = 0.1$.

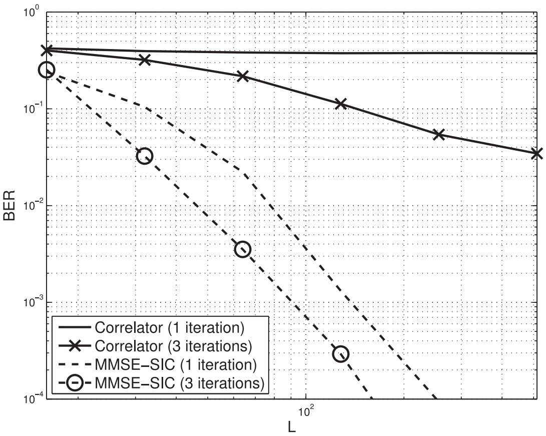


Fig. 10. Performances of coded BER for various values of L when $K = 4$, $E_b/N_0 = 30$ dB, and $p = 0.1$.

iterative receivers with correlator and MMSE-SIC detector can provide better performances through iterations. It is noteworthy that although L increases, the transmission power remains unchanged as the norm of spreading sequence is normalized. From this, we can see that reliable transmissions can be achieved at the cost of lower data rate or wider bandwidth.

VI. Concluding Remarks

We studied induced random chip flipping for secure multiple access based on the MC-CDMA system that uses PN sequences from LFSRs for spreading, which is suitable for MTC as PN sequences can be generated by low-cost hardware at devices. Since PN sequences are vulnerable to correlation attacks, spreading sequences are deliberatively perturbed by random chip flipping to make correlation attacks computationally infeasible. However, the detection performance at a legitimate receiver, i.e., Bob, could also be severely degraded if unperturbed spreading sequences are used for signal detection. To mitigate the performance degradation, the optimal ML detection was formulated to take into account random chip flipping, which is, however, computationally prohibitive as the complexity grows exponentially with the processing gain. Thus, in order to avoid a high computational complexity, the EM algorithm was derived. In particular, for the case of multiple devices transmitting signals simultaneously, we considered coded systems and derived iterative receivers based on the EM algorithm to mitigate IUI using the correlator and MMSE-SIC detector. The iterative receiver with MMSE-SIC detector can exploit the previous decoding result and provides a better performance than that with correlator. Through the simulations, we saw that the EM algorithm can perform well with a high crossover probability (e.g., an SER of 10^{-2} can be achieved with a crossover probability of $p = 0.3$) for the case of $K = 1$. For the case of coded systems with $K \geq 1$, the iterative receiver with MMSE-SIC provided good performances for a large processing gain.

References

[1] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. New York, NY, USA: Springer, 2010.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC, 1996.

[3] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications (corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 5, pp. 776–780, Sep. 1984.

[4] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," *J. Cryptol.*, vol. 1, no. 3, pp. 159–176, 1989.

[5] W. Meier, "Fast correlation attacks: Methods and countermeasures," in *Fast Software Encryption (Lecture Notes in Computer Science)*, vol. 6733, A. Joux, Ed. Berlin, Germany: Springer, 2011, pp. 55–67.

[6] T. Johansson and F. Jonsson, "Theoretical analysis of a correlation attack based on convolutional codes," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2173–2181, Aug. 2002.

[7] *Study on RAN Improvements for Machine-Type Communications, 3GPP TR 37.868 V11.0*, Oct. 2011.

[8] *Overview of the Internet of things, ITU-T Y.2060*, 2012.

[9] M. Hasan, E. Hossain, and D. Niyato, "Random access for machine-to-machine communication in LTE-advanced networks: Issues and approaches," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 86–93, Jun. 2013.

[10] F. Ghavimi and H.-H. Chen, "M2M communications in 3GPP LTE/LTE-A networks: Architectures, service requirements, challenges, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 525–549, Apr.–Jun. 2015.

[11] W. Harrison and S. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–5.

[12] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[13] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[14] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[15] R. Vaidyanathaswami and A. Thangaraj, "Robustness of physical layer security primitives against attacks on pseudorandom generators," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 1070–1079, Mar. 2014.

[16] A. P. Dempster, N. M. Laird, and D. B. Rubin, "Maximum likelihood from incomplete data via the em algorithm," *J. Roy. Statist. Soc. B*, vol. 39, no. 1, pp. 1–38, 1977.

[17] G. McLachlan and T. Krishnan, *The EM Algorithm and Extensions*. Hoboken, NJ, USA: Wiley, 1997.

[18] J. Choi, *Adaptive and Iterative Signal Processing in Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2006.

[19] X. Wang and H. Poor, "Iterative (turbo) soft interference cancellation and decoding for coded CDMA," *IEEE Trans. Commun.*, vol. 47, no. 7, pp. 1046–1061, Jul. 1999.

[20] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM Wireless Communications With MATLAB*. Hoboken, NJ, USA: Wiley-IEEE Press, 2010.

[21] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. IT-15, no. 1, pp. 122–127, Jan. 1969.

[22] L. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 2, pp. 284–287, Mar. 1974.

Jinho Choi (SM'02) was born in Seoul, South Korea. He received the B.E. (*magna cum laude*) degree in electronics engineering in 1989 from Sogang University, Seoul, and the M.S.E. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 1991 and 1994, respectively.

He is currently with Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea, where he is a Professor. Prior to joining GIST in 2013, he was with the College of Engineering, Swansea University, Swansea, U.K., where he was a Professor/Chair in wireless. His research interests include wireless communications and array/statistical signal processing. He authored two books published by Cambridge University Press in 2006 and 2010.

Prof. Choi received the 1999 Best Paper Award for Signal Processing from EURASIP and the 2009 Best Paper Award at the WPMC Conference. He is currently an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and had served as an Associate Editor or Editor of other journals, including the IEEE COMMUNICATIONS LETTERS, the *Journal of Communications and Networks*, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and the *ETRI Journal*.

Euiseok Hwang (M'08) received the B.S. and M.S. degrees from the School of Engineering, Seoul National University, Seoul, South Korea, in 1998 and 2000 and the M.S. and Ph.D. degrees in electrical and computer engineering from Carnegie Mellon University, Pittsburgh, PA, USA, in 2010 and 2011, respectively.

He was with Daewoo Electronics, Co., Ltd., South Korea, from 2000 to 2006 and with LSI Corporation (now Broadcom), San Jose, CA, USA, from 2011 to 2014. He is currently an Assistant Professor with the School of Mechatronics, Gwangju Institute of Science and Technology, Gwangju, South Korea. He has more than 60 journal and conference papers on various channel data processing issues, in addition to 18 granted U.S. patents. His research interests include channel coding and signal processing for data storage and communication systems and emerging large-scale information processing applications.