Secure Multicarrier DS/SS with Induced Random Flipping

Jinho Choi and Euiseok Hwang
Gwangju Institute of Science and Technology (GIST), Korea
Email: {jchoi0114, euiseokh}@gist.ac.kr.

***Abstract*—For secure transmissions, we consider direct sequence/spread spectrum (DS/SS) systems where pseudo-random (PN) sequences are used for spreading. To generate PN sequences, linear feedback shift registers (LFSRs) are employed, which are also used to generate keystreams in stream ciphers. For steam ciphers that use LFSRs, there are known attacks including correlation attacks that can regenerate keystreams. Since those attacks can also be used to regenerate spreading sequences, in this paper, in order to mitigate this problem, we consider induced random (chip) flipping of spreading sequences. While perturbed spreading sequences make correlation attacks infeasible, a legitimate receiver also suffers from random flipping. To take advantage of known spreading sequences for good performances, the maximum likelihood (ML) detection can be used, which is, however, computationally prohibitive as the complexity grows exponentially with the processing gain. To avoid this difficulty, we derive an expectation-maximization (EM) algorithm to perform the ML detection with low computational complexity in this paper.**

***Index Terms*—secure communications, DS/SS, random flipping**

I. Introduction

Stream ciphers are usually fast and require low hardware complexity, which make them suitable for devices of limited computing resources, e.g., sensors in wireless sensor networks. In order to generate a key stream in a stream cipher, linear feedback shift registers (LFSRs) are used. For example, A5/1 cipher in GSM is a stream cipher that uses LFSRs. Since stream ciphers using LFSRs are not immune to correlation attacks, a nonlinear Boolean function is considered in [1], which combines the output sequences of multiple LFSRs to generate a key stream (A5/1 cipher is based on this approach). Since the output of the nonlinear Boolean function can be correlated to the output of an LFSR, it is possible to consider 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 [2], it is shown that there are fast correlation attacks if the lengths of LFSRs are not long and the number of feedback taps is not large.

In [3], the notion of physical layer security [4]–[6] is employed to strengthen the keystream generator based on LFSRs for noisy communication 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. 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. It is shown that correlation attacks can reduce to brute-force attacks if the bit error rate can be sufficiently high.

Motivated by the approach in [3], in this paper, we consider secure multicarrier direct sequence/spread spectrum (DS/SS) that make correlation attack computationally infeasible by inducing random chip flipping in spreading sequences. In the proposed approach, the spread signal is passed through a BSC prior to transmission. As a result, some chips in a spreading sequence for a symbol duration are flipped. There are a few key differences from [3]. Firstly, we do not use any channel coding (however, spreading might be considered a channel coding scheme). Secondly, we include random chip flipping in spreading sequences that can also degrade the detection performance at Bob. That is, induced random flipping results in Eve's computational difficulty in performing correlation attacks at the cost of Bob's performance degradation in the signal detection. Thus, Bob should consider an optimal detection scheme that can take into account random chip flipping. To this end, Bob can employ the maximum likelihood (ML) detection. However, the computational complexity of the ML detection can grow 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. Alternatively, a low complexity approximation can be devised using a Gaussian approximation with the output of the correlator. This approach can take advantage of known spreading sequences and statistical properties of random chip flipping due to BSC at Bob.

Although the complexity of the signal detection with the correlator's output is low, its performance is not close to optimal one. Thus, we still need to consider a low complexity approach to perform the ML detection. To this end, the expectation-maximization (EM) algorithm [7]–[9] is invoked.

Notation: Matrices and vectors are denoted by upper- and lower-case 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 $\dagger$ denotes the pseudo-inverse. For a vector $\mathbf{a}$, $\mathrm{diag}(\mathbf{a})$ 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

978-1-4799-6664-6/16/$31.00 ©2016 IEEE

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 $\mathrm{Var}(\cdot)$ 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 section, we consider a multicarrier DS/SS system using pseudo-noise (PN) sequences to spread signals for a pair of legitimate transmitter and receiver. For secure communications, we consider perturbed PN sequences using BSC.

A. DS/SS with Perturbed Spreading Sequences

Suppose that the processing gain is L and the DS/SS signal to be transmitted through multicarrier channels from the legitimate transmitter, called Alice, is given by

$$x(Lt+l) = c(Lt+l)s_t,\ l = 0, \ldots, L-1, \tag{1}$$

where $c(l) \in \{\pm\frac{1}{\sqrt{L}}\}$ denotes the PN sequence and $s_t \in \mathcal{S}$ is the tth data symbol. Here, $\mathcal{S}$ represents the signal constellation. We discuss the generation of the PN sequence in Subsection II-B. Let $\mathbf{c}_t = [c(Lt)\ \ldots c(Lt+L-1)]^{\mathrm{T}}$. Then, we can have

$$\begin{aligned}\mathbf{x}_t &= [x(Lt)\ \ldots x(Lt+L-1)]^{\mathrm{T}} \\ &= \mathbf{c}_t s_t.\end{aligned} \tag{2}$$

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 $c(l)$ that can make some known attack ineffective. For given $\mathbf{c}_t$, a perturbed version can be given by

$$\bar{\mathbf{c}}_t = \mathbf{c}_t \odot \mathbf{u}_t, \tag{3}$$

where $\odot$ represents the elementwise multiplication and

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

Here, q is referred to as the induced correlation probability (and $p = 1-q$ becomes the crossover probability) and the elements of $\mathbf{u}_t$ are independent. For convenience, $\bar{c}(l)$ denotes the perturbed version of $c(l)$ as in (3). In Fig. 1, we show that how the spread signal, $x(l)$, can be generated using $\bar{c}(l)$, which can be considered as the output of BSC with input $c(l)$. For convenience, the BSC in Fig. 1 is referred to as the chip flipping BSC. Due to this BSC, $\bar{c}(l)$ becomes the keystream which Eve is to regenerate for eavesdropping.

Let $\{h_i, i = 0, \ldots, P-1\}$ denote the channel impulse response (CIR) from Alice to the legitimate receiver, called Bob, where P is the length of CIR. Then, the channel matrix in the frequency domain is given by

$$\mathbf{H} = \mathrm{diag}(H_0, \ldots, H_{L-1}), \tag{5}$$

where $H_l = \sum_{i=0}^{P-1} h_i e^{-j\frac{2\pi i l}{L}},\ l = 0, \ldots, L-1$. At Bob, the received signal through L multicarriers is given by

$$\mathbf{y}_t = \mathbf{H}\bar{\mathbf{c}}_t s_t + \mathbf{n}_t,\ t = 0, \ldots, T-1, \tag{6}$$

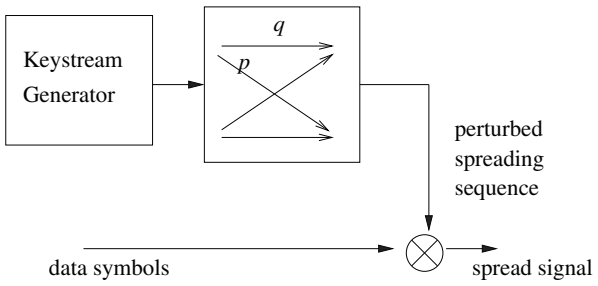

Fig. 1. Generation of spread signals by a perturbed spreading sequence from the keystream generator using chip flipping BSC with the induced correlation probability q.

where $\mathbf{n}_t \sim \mathcal{CN}(0, N_0\mathbf{I})$ is the background noise and T is the length of data packet.

B. Correlation Attack

Suppose that that $c(l)$ is generated by a combination generator consisting of multiple binary LFSRs and a nonlinear function, F, as shown in Fig. 2. Since Eve can easily find the initial contents of each LFSR by solving a set of linear equations [10], 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. 2. This attack, which is called (fast) correlation attack, is studied in [2], [3], [11] with computationally efficient methods to estimate the initial contents of a target LFSR from a given (part of) keystream sequence.

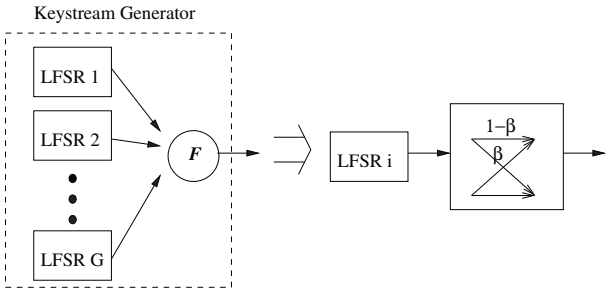

Fig. 2. Keystream generation (the left-hand side) and a model for the correlation attack (the right-hand side).

In [2], correlation attacks can be 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 reduce 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 perturbed spreading sequence. Thus, Eve can observe 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 $p = \frac{1}{4}$.

III. Signal Detection at Bob

In Subsection II-B, we show that correlation attacks can be ineffective by introducing random chip flipping in spreading sequences. However, the detection performance at Bob can also be degraded due to random chip flipping. In this section, we study the signal detection at Bob in the presence of random chip flipping under the assumption that the original spreading sequence, $\{c(l)\}$, and the induced correlation probability, q, are known.

A. Optimal Detection

For convenience, we omit the time index t. For the optimal signal detection, we consider the ML criterion from $\mathbf{y}$. For given $\mathbf{y}$, the ML function of s can be given by

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

where $\mathcal{U}$ represents the set of all possible chip flipping vectors, $\mathbf{u}$. Clearly, we have $|\mathcal{U}| = 2^L$. For a given $\mathbf{u}$, let m denote the number of -1 in $\mathbf{u}$. Since m is a binomial random variable, we have

$$\Pr(\mathbf{u}) = P_m = \binom{L}{m}(1-q)^m q^{L-m}. \tag{9}$$

The signal detection can be carried out as follows:

$$\hat{s} = \underset{s\in\mathcal{S}}{\operatorname{argmax}}\, f(\mathbf{y}|s). \tag{10}$$

For the optimal signal detection in (10), we need to find $f(\mathbf{y}|s)$ which is a sum of 2^L terms. Thus, we can see that the computational complexity to perform the optimal detection grows exponentially with L. To avoid this difficulty, we consider the EM approach in Section IV. For comparison purposes, in the next subsection, we also consider a low-complexity approach with despread signals, which results in a detection method.

B. Correlator Detector

In this subsection, in order to lower the computational complexity in signal detection, we use the correlator to detect the signal.

Since Bob knows the spreading sequence, $c(l)$, and statistical properties of the chip flipping BSC, he can take advantage of them. At Bob, the despread signal or the output of the correlator with $c(l)$, not $\bar{c}(l)$, is given by

$$\begin{aligned} r &= \mathbf{c}^{\mathrm{T}}\mathbf{H}^{\mathrm{H}}\mathbf{y} \\ &= \sum_{l=0}^{L-1} |H_l|^2\alpha_l s + n, \end{aligned} \tag{11}$$

where $\alpha_l = c(l)\bar{c}(l) \in \{\pm\frac{1}{L}\}$ and $n = \mathbf{c}^{\mathrm{T}}\mathbf{H}^{\mathrm{H}}\mathbf{n} \sim \mathcal{N}(0,\sigma^2)$. Here, $\sigma^2 = A_2 N_0$, where $A_2 = \frac{\sum_l |H_l|^2}{L}$. In (11), although $\{\alpha_l\}$ are unknown at Bob and considered random variables, the statistical properties are known. Thus, for given r, the ML function can be found as

$$\begin{aligned} f(r|s) &= \sum_{\{\alpha_l\}} f(r|\alpha_0,\ldots,\alpha_{L-1},s)\Pr(\alpha_0,\ldots,\alpha_{L-1}) \\ &= \sum_{\{\alpha_l\}} e^{-\frac{|r-Z(\alpha_0,\ldots,\alpha_{L-1})s|^2}{\sigma^2}} \Pr(\alpha_0,\ldots,\alpha_{L-1}), \end{aligned} \tag{12}$$

where

$$Z(\alpha_0,\ldots,\alpha_{L-1}) = \sum_{l=0}^{L-1} |H_l|^2\alpha_l$$

and $\Pr(\alpha_0,\ldots,\alpha_{L-1}) = P_m$ with m that is the number of the α_l's of value $-\frac{1}{L}$. From $f(r|s)$, the signal detection is carried out by

$$\hat{s} = \underset{s\in\mathcal{S}}{\operatorname{argmax}}\, f(r|s). \tag{13}$$

In (12), we can see that the complexity to find $f(r|s)$ exponentially grows with L. However, for a large L, we may consider a Gaussian approximation. Suppose that Z can be approximated by a real-valued Gaussian random variable, i.e.,

$$Z \sim \mathcal{N}\left(\mathbb{E}[Z], \mathrm{Var}(Z)\right), \tag{14}$$

where the mean, $\mathbb{E}[Z]$, and the variance, $\mathrm{Var}(Z)$, can be found from (9) as

$$\begin{aligned} \mathbb{E}[Z] &= (2q-1)A_2 \\ \mathrm{Var}(Z) &= \sum_l |H_l|^4(\mathbb{E}[\alpha_l^2] - \mathbb{E}[\alpha_l]^2) \\ &= 4q(1-q)A_4, \end{aligned} \tag{15}$$

where $A_4 = \frac{\sum_l |H_l|^4}{L^2}$. Then, after some manipulations, $f(r|s)$ in (12) can be approximated as

$$\begin{aligned} f(r|s) &= C\mathbb{E}\left[\exp\left(-\frac{1}{N_0}|r-Zs|^2\right)\right] \\ &\approx C'\int e^{-\frac{|y-xs|^2}{N_0}} e^{-\frac{(x-\mathbb{E}[Z])^2}{2\mathrm{Var}(Z)}}\,dx \\ &\propto \frac{1}{\sqrt{a}}\exp\left(\frac{b^2}{a} - \frac{|r|^2}{N_0} - \frac{\mathbb{E}[Z]}{2\mathrm{Var}(Z)}\right), \end{aligned} \tag{16}$$

which has a closed-form expression. Here, C and C' are constant, and we have

$$a = \frac{|s|^2}{N_0} + \frac{1}{2\mathrm{Var}(Z)} \text{ and } b = \frac{\Re(r^*s)}{N_0} + \frac{\mathbb{E}[Z]}{2\mathrm{Var}(Z)}.$$

The resulting detector is referred to the correlator detector.

IV. EM Algorithm

As shown in Subsection III-A, the computational complexity to perform the optimal detection is prohibitively high when L is sufficiently large. In this section, we consider the EM algorithm for the optimal detection, which is computationally efficient.

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

$$f(\mathbf{y}|s,\mathbf{u}) = C\exp\left(-\frac{1}{N_0}||\mathbf{y}-\mathbf{H}(\mathbf{c}\odot\mathbf{u})s||^2\right), \quad (17)$$

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

$$\begin{aligned} Q(s|\hat{s}^{(l)}) &= \mathbb{E}[\ln f(\mathbf{u},\mathbf{y}|s)|\mathbf{y},\hat{s}^{(l)}] \\ &= \mathbb{E}[\ln f(\mathbf{y}|\mathbf{u},s)\Pr(\mathbf{u}|s)|\mathbf{y},\hat{s}^{(l)}] \\ &= \mathbb{E}[\ln f(\mathbf{y}|\mathbf{u},s)|\mathbf{y},\hat{s}^{(l)}] + \mathbb{E}[\ln\Pr(\mathbf{u})|\mathbf{y},\hat{s}^{(l)}] \\ &= -\frac{1}{N_0}\mathbb{E}[||\mathbf{y}-\mathbf{H}(\mathbf{c}\odot\mathbf{u})s||^2|\mathbf{y},\hat{s}^{(l)}] + C', \quad (18) \end{aligned}$$

where C' is constant and $\hat{s}^{(l)}$ is the estimate of s at the lth iteration. Since

$$\begin{aligned} ||\mathbf{y}-\mathbf{H}(\mathbf{c}\odot\mathbf{u})s||^2 &= ||\mathbf{y}||^2 + |s|^2||\mathbf{H}(\mathbf{c}\odot\mathbf{u})||^2 \\ &\quad - 2\Re(\mathbf{y}^{\mathrm{H}}\mathbf{H}(\mathbf{c}\odot\mathbf{u})s) \\ &= ||\mathbf{y}||^2 + A_2|s|^2 \\ &\quad - 2\Re(\mathbf{y}^{\mathrm{H}}\mathbf{H}(\mathbf{c}\odot\mathbf{u})s), \quad (19) \end{aligned}$$

we have

$$\begin{aligned} &\mathbb{E}[||\mathbf{y}-\mathbf{H}(\mathbf{c}\odot\mathbf{u})s||^2|\mathbf{y},\hat{s}^{(l)}] \\ &= ||\mathbf{y}||^2 + A_2|s|^2 - 2\Re\left(\mathbf{y}^{\mathrm{H}}\mathbf{H}(\mathbf{c}\odot\bar{\mathbf{u}}^{(l)})s\right), \quad (20) \end{aligned}$$

where $\bar{\mathbf{u}}^{(l)} = \mathbb{E}[\mathbf{u}|\mathbf{y},\hat{s}^{(l)}]$. To find $\bar{\mathbf{u}}^{(l)}$, we need to derive $\Pr(\mathbf{u}|\mathbf{y},\hat{s}^{(l)})$. We assume that each element of $\mathbf{u}$ is independent. Then, it can be shown that

$$\begin{aligned} \Pr(\mathbf{u}|\mathbf{y},\hat{s}^{(l)}) &\propto f(\mathbf{y}|\mathbf{u},\hat{s}^{(l)})\Pr(\mathbf{u},\hat{s}^{(l)}) \\ &\propto \left(\prod_i e^{-\frac{1}{N_0}|y_i - c_i u_i H_i \hat{s}^{(l)}|^2}\right)\Pr(\mathbf{u}) \\ &= \prod_i \phi_i(u_i) \quad (21) \end{aligned}$$

where $\phi_i(u_i) = e^{-\frac{1}{N_0}|y_i - c_i u_i H_i \hat{s}^{(l)}|^2}\Pr(u_i)$. From (4), we have $\Pr(u_i=+1) = q$ and $\Pr(u_i=-1) = 1-q$. Let $\kappa = \frac{1-q}{q}$. Then, it can be shown that

$$\begin{aligned} [\bar{\mathbf{u}}^{(l)}]_i &= \mathbb{E}[u_i|\mathbf{y},\hat{s}^{(l)}] \\ &= \frac{\phi_i(1)-\phi_i(-1)}{\phi_i(1)+\phi_i(-1)} \\ &= \frac{1-\kappa e^{-\frac{4}{N_0}\Re(y_i^* c_i H_i \hat{s}^{(l)})}}{1+\kappa e^{-\frac{4}{N_0}\Re(y_i^* c_i H_i \hat{s}^{(l)})}}. \quad (22) \end{aligned}$$

The M-step is given by

$$\begin{aligned} \hat{s}^{(l+1)} &= \underset{s\in\mathcal{S}}{\operatorname{argmax}}\, Q(s|\hat{s}^{(l)}) \\ &= \underset{s\in\mathcal{S}}{\operatorname{argmin}}\, A_2|s|^2 - 2\Re\left(\mathbf{y}^{\mathrm{H}}\mathbf{H}(\mathbf{c}\odot\bar{\mathbf{u}}^{(l)})s\right). \quad (23) \end{aligned}$$

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

In summary, the EM algorithm for the ML detection can be shown as follows:

A0) Let $l=0$ and $[\bar{\mathbf{u}}^{(l)}]_i = 1$ for all i.
A1) Perform the M-step in (23) with $\bar{\mathbf{u}}^{(l)}$ and find $\hat{s}^{(l+1)}$.
A2) Update $l \leftarrow l+1$ and perform the E-step in (22) with $\hat{s}^{(l)}$ and find $\bar{\mathbf{u}}^{(l)}$.
A3) If $||\bar{\mathbf{u}}^{(l-1)} - \bar{\mathbf{u}}^{(l)}|| \le \epsilon$, stop. Otherwise, move A1).

The complexity of the EM algorithm is linear in L as shown in (22) and (23). Note that it is not always guaranteed that the EM algorithm converges to the ML solution [8].

V. Simulation Results

For simulations, we consider 64-quadrature amplitude modulation (QAM) and a processing gain of $L=64$. Each tap of the CIR, h_i, is assumed to be an independent zero-mean CSCG random variable with variance $1/P$ with $P=6$ (i.e., Rayleigh fading is assumed). The signal-to-noise ratio (SNR) is given by

$$\mathrm{SNR} = \frac{\mathbb{E}[|s|^2]}{N_0}. \quad (24)$$

Fig. 3 shows the symbol error rate (SER) for various SNRs with $p=0.25$. It is shown that a better performance of the correlator detector can be obtained as the SNR increases. However, the EM algorithm can provide a better performance than the correlator detector after 3 iterations and the performance gap becomes wider as the SNR increases.

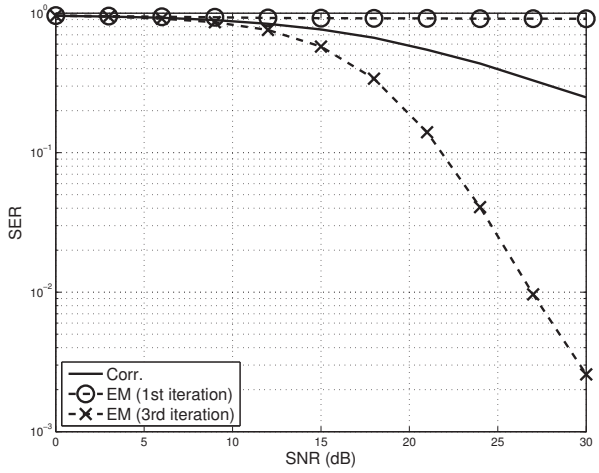

Fig. 3. Symbol error rate versus SNR ($L=64$ and $p=0.25$).

In order to see the performance of the EM algorithm over iterations, we show the SERs for various numbers of iterations in Fig. 4 with $p=0.25$. It is shown that 3 iterations might be sufficient for reasonable performances.

Fig. 5 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

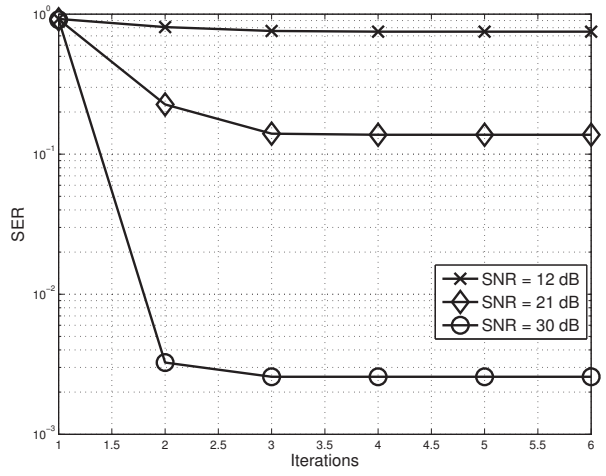

Fig. 4. Symbol error rate over iterations ($L = 64$ and $p = 0.25$).

detection performance at Bob as shown in Fig. 5. However, it is shown that at a high p, Bob can still have a reasonable SER with the EM algorithm (after 3 iterations). That is, at p of 0.3 and 0.4, we can have SERs of 10^{-2} and 10^{-1}, respectively. Thus, we believe that the proposed approach is promising for stream ciphers that can be used wireless devices (especially, transmitters) of limited computing power.

VI. Concluding Remarks

We proposed a secure multicarrier DS/SS system where the notion of stream cipher is employed with induced random chip flipping using a BSC to make correlation attacks computationally infeasible. Since spreading sequences became perturbed by random chip flipping, the detection performance at a legitimate receiver could also be degraded. To keep good performances, the optimal ML detection was considered at Bob. However, it was shown that its complexity grows exponentially with the processing gain. To avoid a high computational complexity, the output of the correlator was considered for the signal detection. In addition, the EM algorithm was employed to perform the ML detection. Through the simulations, we saw that the EM algorithm can perform well with a high crossover probability (e.g., a SER of 10^{-2} can be achieved with a crossover probability of $p = 0.3$).

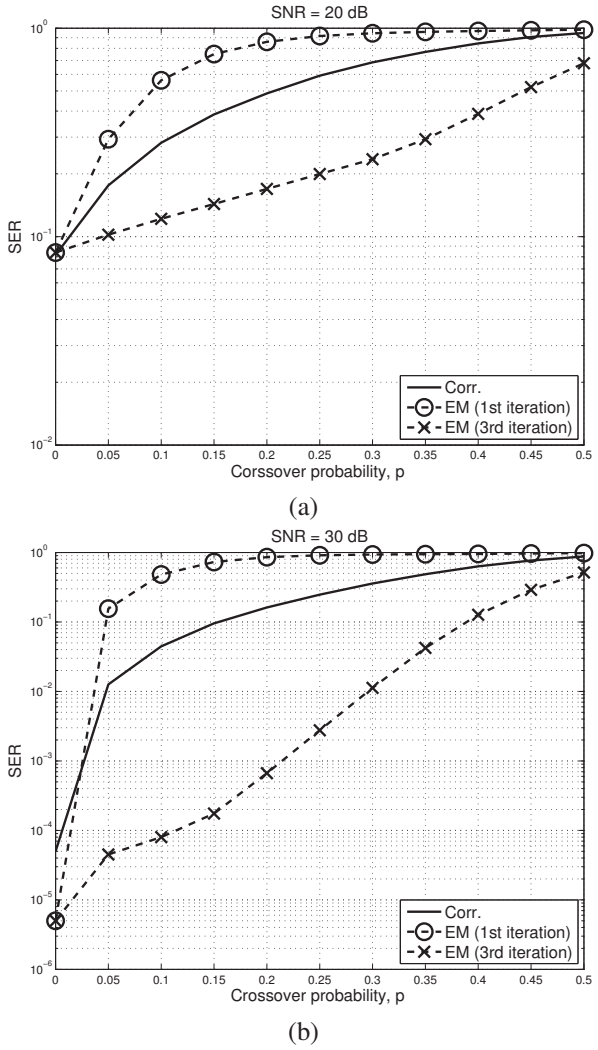

Fig. 5. Performances of symbol error rate for various values of p: (a) SNR = 20 dB; (b) SNR = 30 dB.

References

[1] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications (corresp.)," *IEEE Trans. Inf. Theory*, vol. 30, pp. 776–780, Sep 1984.

[2] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," *Journal of Cryptology*, vol. 1, no. 3, pp. 159–176, 1989.

[3] W. Harrison and S. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *Communications, 2009. ICC '09. IEEE International Conference on*, pp. 1–5, June 2009.

[4] Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2470 –2492, June 2008.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2515–2534, June 2008.

[6] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[7] A. P. Dempster, N. M. Laird, and D. B. Rubin, "Maximum likelihood from incomplete data via the em algorithm," *J. of The Royal Statistical Society, Series B*, vol. 39, no. 1, pp. 1–38, 1977.

[8] G. McLachlan and T. Krishnan, *The EM Algorithm and Extensions*. John Wiley & Sons, 1997.

[9] J. Choi, *Adaptive and Iterative Signal Processing in Communications*. Cambridge University Press, 2006.

[10] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. 15, pp. 122–127, Jan 1969.

[11] T. Johansson and F. Jonsson, "Theoretical analysis of a correlation attack based on convolutional codes," *IEEE Trans. Inf. Theory*, vol. 48, pp. 2173–2181, Aug 2002.