A Novel Approach to Security Enhancement of Chaotic DSSS Systems

Nguyen Xuan Quyen[1], Chuyen T. Nguyen[1], Pere Barlet-Ros[2], and Reiner Dojen[3]

[1]School of Electronics and Telecommunications, Hanoi University of Science and Technology, Vietnam
[2]Department of Computer Architecture, UPC BarcelonaTech, Spain
[3]Department of Electronic and Computer Engineering, University of Limerick, Ireland
[4]Email: {quyen.nguyenxuan, chuyen.nguyenthanh}@hust.edu.vn, pbarlet@ac.upc.edu, reiner.dojen@ul.ie

***Abstract*—In this paper, we propose a novel approach to the enhancement of physical layer security for chaotic direct-sequence spread-spectrum (DSSS) communication systems. The main idea behind our proposal is to vary the symbol period according to the behavior of the chaotic spreading sequence. As a result, the symbol period and the spreading sequence vary chaotically at the same time. This simultaneous variation aims at protecting DSSS-based communication systems from the blind estimation attacks in the detection of the symbol period. Discrete-time models for spreading and despreading schemes are presented and analyzed. Multiple access performance of the proposed technique in the presence of additional white Gaussian noise (AWGN) is determined by computer simulations. The increase in security at the physical layer is also evaluated by numerical results. Obtained results show that our proposed technique can protect the system against attacks based on the detection of the symbol period, even if the intruder has full information on the used chaotic sequence.**

***Index Terms*—Chaotic direct-sequence spread-spectrum (DSSS); Chaos-based spread-spectrum; Physical layer security.**

I. Introduction

In the two last decades, a large number of studies have been devoted to the design and analysis of communication systems based on chaotic direct-sequence spread-spectrum (DSSS) [1]-[5]. The main goal of the application of chaotic sequences to spread-spectrum communications is the enhancement of physical layer security [6]-[9]. However, several recent studies have shown that chaotic sequences can be recovered by different blind detection methods [10]-[13]. A detection method based on nonlinear time series analysis is presented in [10], where mutual information and false nearest neighbor methods are used for establishing optimal embedding parameters for the attractor reconstruction from the experimental time series. The reconstruction of chaotic attractor is also investigated in [11] by exploiting intrinsic geometry of chaotic attractor sets. Based on the reconstructed attractor, the chaotic sequence used can be recovered by an approximation algorithm. The study in [12] shows that the equivariant adaptive separation via independence (EASI) algorithm in fixed-point arithmetic can recover successfully the chaotic sequences. The obtained results of the above studies also pose a new security challenge, that is, if an intruder can recover the chaotic spreading sequence, he will employ the recovered sequence to detect the symbol period [13, 14]. With the recovered sequence and detected period, he can totally recover the original data. It means that the security of chaos-based DSSS systems is totally broken.

This paper proposes a novel chaos-based DSSS technique for overcoming the security weakness aforementioned. In the proposed technique, the period of the data symbol is varied according to the behavior of the chaotic spreading sequence. Because both the spreading sequence and the symbol period vary chaotically at the same time, the bit energy also varies according to the chaotic behavior. As a result, it is not easy for an intruder to detect the symbol period by using energy detection methods [13, 14]. In fact, the idea of chaos-based variation of the symbol period in spread-spectrum communication systems has also been presented in [15] and [16]. However, the spreading sequences investigated in these studies are binary sequences, i.e., PN and NRZ-chaos sequences, which have only two levels, "+1" or "-1". Obtained results point out that the performance of multiple-access system with the simultaneous variation of the symbol period and the spreading sequence gets worse when the variation range of the symbol period is increased. But in return, our technique can protect the system from attacks based on detecting the symbol period at the physical layer, even if the attacker fully knows the chaotic sequence.

The rest of this paper is structured as follows: in Section II, the proposed approach is described via the analysis of discrete-time models for spreading and despreading schemes. Multiple access performance over the AWGN channel is estimated by numerical results in Section III. Section IV presents an investigation using computer simulations on the ability of the proposed technique in resisting the symbol period detection attacks. Finally, our conclusion with remarks is given in Section V.

II. Description of Proposed Approach

A. Spreading Scheme with Variable Bit Period

The block diagram of the spreading scheme is shown in Fig. 1(a). The pulse chain with variable inter-pulse intervals, denoted by $\{p_l\}$ is generated by the variable interval pulse generator (VIPG) whose input is the chaotic sequence $\{x_k\}$. In the VIPG, the input sequence $\{x_k\}$ is sampled at each instance

triggered by the input pulse, i.e.,

$$p_l = P(t - t_l), \tag{1}$$

with

$$P(t) = \begin{cases} 1 & 0 \le t \le \tau, \\ 0 & otherwise, \end{cases} \tag{2}$$

where t_l is the instance to generate the l^{th} pulse. The output sample x_l is then converted into a positive integer β_l by using a transformation function, i.e., $\beta_l = f(x_l)$. Here, the function $f(\cdot)$ is determined so that when the sequence $\{x_l\}$ varies in a known range of $[x_{min}, x_{max}]$, $\{\beta_l\}$ also varies in a corresponding range of $[\beta_{min} = f(x_{min}) = 0, \beta_{max} = f(x_{max}) = \beta_m]$. In order to determine the function $f(\cdot)$, we first choose a fixed value for β_m. The range of $[x_{min}, x_{max}]$ is then divided into (β_m+1) value intervals, i.e., $[x_{min}+j\gamma, x_{min}+(j+1)\gamma]$, with j varying from 0 to β_m. γ is a constant defined by

$$\gamma = (x_{max} - x_{min})/(\beta_m + 1). \tag{3}$$

If the input value x_l falls into the range of $[x_{min}+j\gamma, x_{min}+(j+1)\gamma]$, the corresponding output value β_l is determined by the function $f(\cdot)$ as follows:

$$\beta_l = f(x_l) = \left\lfloor \frac{x_l - x_{min}}{\gamma} \right\rfloor, \tag{4}$$

with $\lfloor \cdot \rfloor$ being the floor function. Depending on the value of β_l, the $(l+1)^{th}$ pulse is generated at the output of VIPG at the instance t_{l+1} given by

$$t_{l+1} = t_l + (\beta + \beta_l)\tau, \tag{5}$$

here τ is chip period of the chaotic sequence $\{x_k\}$ and β is a fixed integer whose value is predetermined. We can see from Eq. (5) that the intervals between inter-pulses of $\{p_l\}$ vary according to the chaotic sample values $\{x_l\}$ and always equal to a multiple of chip period τ.

With the trigger of each pulse of $\{p_l\}$, the data buffer shifts the binary value of next symbol, i.e., $b_l = \{\pm 1\}$, to its output. It means that the period of l^{th} symbol, denoted by T_l, is determined from Eq. (5) as follows:

$$T_{s_l} = t_{l+1} - t_l = (\beta + \beta_l)\tau. \tag{6}$$

The spread-spectrum process is performed by directly multiplying the variable-period bits $\{b_l\}$ with the chaotic sequence $\{x_k\}$. Eq. (6) shows that there are $(\beta+\beta_l)$ chips in the period of l^{th} bit. It means that the sum, i.e., $(\beta + \beta_l)$ is also the spreading factor of the l^{th} bit. In the spreading process, the number of symbol l tends to infinite, β_l varies in the range of $[0, \beta_m]$, thus the spreading factor, $(\beta + \beta_l)$, varies in the range of $[\beta, \beta_m]$. The predetermined constants, β and β_m, are considered as the initial value and the variation width of the spreading factor, respectively.

The output signal of the spreading scheme in the period of the l^{th} bit can be expressed as

$$e_k = b_l x_k. \tag{7}$$

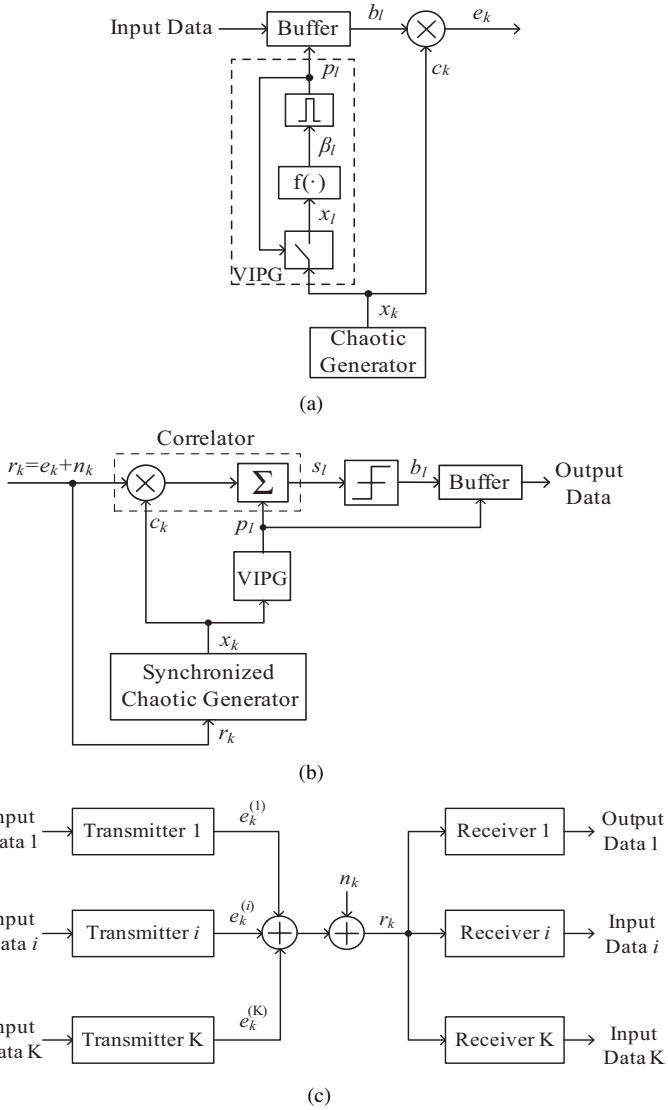


Fig. 1. Block diagrams of (a) Spreading scheme, (b) Despreding scheme, and (c) DS-CDMA system.

It is noted that in the special case of the variation width $\beta_m = 0$, the symbol period $T_s = \beta\tau$ is unvaried in the spreading process. The proposed technique in this case becomes the conventional chaotic DSSS technique.

B. Despreading Scheme

The block diagram of the despreading scheme is displayed in Fig. 1(b). The local chaotic sequence is regenerated and synchronized with the incoming signal by means of the synchronized chaotic generator (SCG) whose scheme is shown in Fig. 1(c). This synchronization scheme relies on the scheme presented in [30] for the conventional chaotic DSSS technique with a modification. In particular, instead of repeating the correlation process after a fixed symbol period as usual, the correlation process is controlled by the trigger pulses from the VIPG. In the SCG, the chaotic generator and the VIPG are identical to those of the spreading scheme. The synchronized

chaotic sequence is used for the despreading process and data recovery.

The incoming signal is the sum of the transmitted signal and the noise of AWGN channel, we have

$$r_k = e_k + n_k, \tag{8}$$

here n_k is an AWGN sample with zero mean and variance $N_0/2$. The despreading process is simply performed by using a correlator. The output signal of the correlator is sampled by the trigger of each pule of $\{p_l\}$. The sample value at the instance t_l is determined by

$$\begin{aligned} s_l &= \sum_{k=1}^{\beta+\beta_l} r_k x_k = \sum_{k=1}^{\beta+\beta_l} (e_k + n_k) x_k \\ &= \sum_{k=1}^{\beta+\beta_l} (b_l x_k + n_k) x_k = b_l \sum_{k=1}^{\beta+\beta_l} (x_k)^2 + \sum_{k=1}^{\beta+\beta_l} n_k x_k. \end{aligned} \tag{9}$$

Based on this sample value s_l, the binary value of l^{th} symbol is recovered by

$$b_l = \begin{cases} 1 & s_l \geq 0, \\ -1 & s_l < 0. \end{cases} \tag{10}$$

At the trigger instance of each pulse of $\{p_l\}$, the recovered bits are shifted into the buffer.

C. Multiple-access Operation

Fig. 1(c) shows a typical DS-CDMA communication system based on the proposed DSSS technique. K users are distinguished from each other by different chaotic sequences, which can be produced by using the same chaotic map with different initial values. At the input of the i^{th} receiver, the incoming signal is expressed as

$$r_k = \sum_{i=1}^{K} e_k^{(i)} + n_k = \sum_{i=1}^{K} b_l^{(i)} x_k^{(i)} + n_k \tag{11}$$

The correlation value at output of the sampler is given by

$$\begin{aligned} s_l^{(i)} &= \sum_{k=1}^{\beta+\beta_l} r_k x_k^{(i)} \\ &= \sum_{k=1}^{\beta+\beta_l} \left(\sum_{i=1}^{K} e_k^{(i)} + n_k \right) x_k^{(i)} \\ &= \sum_{k=1}^{\beta+\beta_l} \left(\sum_{i=1}^{K} b_l^{(i)} x_k^{(i)} + n_k \right) x_k^{(i)} \\ &= b_l^{(i)} \sum_{k=1}^{\beta+\beta_l} (x_k^{(i)})^2 + \sum_{k=1}^{\beta+\beta_l} \sum_{i=1, i\neq j}^{K} b_l^{(i)} x_k^{(i)} x_k^{(j)} + \sum_{k=1}^{\beta+\beta_l} n_k x_k^{(i)} \end{aligned} \tag{12}$$

Similarly, based on this sample value $s_l^{(i)}$, the value of $b_l^{(i)}$ is recovered by the comparison as in Eq. (10).

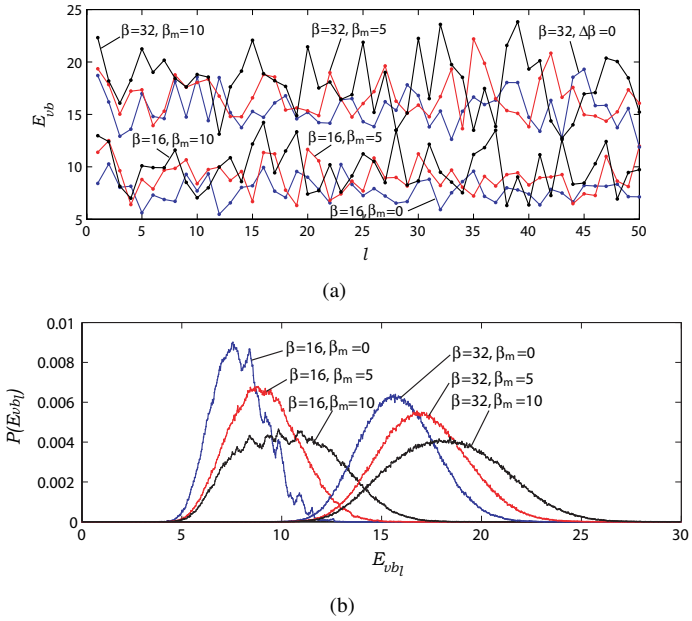


Fig. 2. Results obtained by numerical computation: (a) Variation of symbol energy, (b) Histograms of symbol energy distribution.

III. Simulation Results

In this section, PC simulations for the chaotic DS-CDMA system based on the proposed DSSS technique are carried out with different system parameters. The chaotic map used for generating chaotic sequences is the Chebyshev polynomial function of order 2 given by

$$x_k = f(x_{k-1}) = 2x_{k-1}^2 - 1, \tag{13}$$

with $[x_{min}, x_{max}] = [-1, 1]$ and

$$E_c = E\left[x_k^2\right] = \int_{-\infty}^{\infty} x^2 \rho(x) dx = \int_{-1}^{1} x^2 \frac{1}{\pi\sqrt{1-x^2}} dx = \frac{1}{2}, \tag{14}$$

Fig. 2(a) and Fig. 2(b) show respectively the variation of bit energy and the histograms of the bit energy distribution, obtained by numerical computations for cases of $\beta = 16, 32$ with $\beta_m = 0, 5, 10$. Each histogram is plotted by means of 1000 classes which are calculated statistically from 100000 samples of bit energy. It can be clearly observed that the bit energy varies aperiodically, where the average energy increases along with the increment of the initial spreading factor β, and the variation range of the bit energy becomes wider with the increment of variation width β_m.

In Fig. 3(a), we evaluate the effect of two parameters, i.e., β and β_m, on the performance of the mono-user system under the same value of $\frac{E_{ab}}{N_0} = 9dB$. We can find that the calculated results totally agree with the simulated ones. Both of them point out that the system performance increases with the value of β. For example with the same $\beta_m = 10$, when β increases from 4 to 64, the BER value reduces from $2 \cdot 10^{-3}$ to $6 \cdot 10^{-5}$, respectively. In contrast, when β_m increases, the system performance gets worse. Specifically, at the same

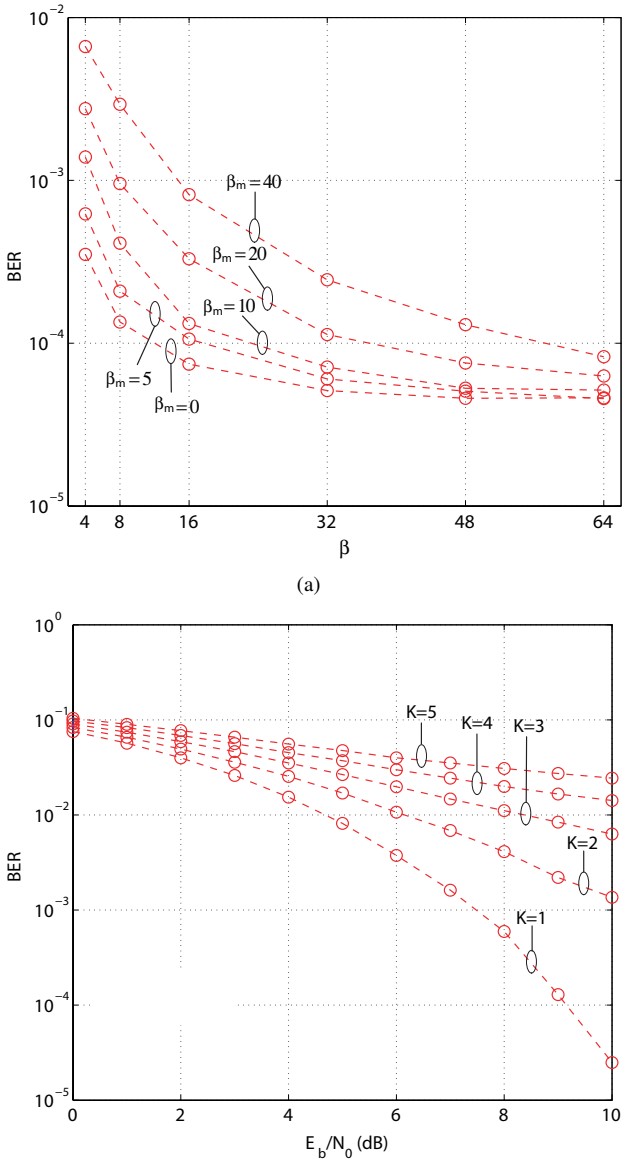


Fig. 3. BER performance of the DS-CDMA system using the proposed DSSS technique: (a) Mono-user system with increment of β and β_m at the same $E_{ab}/N_0 = 9dB$; (b) Multi-user system with increment of K at $\beta = 16$ and $\beta_m = 10$.

$\beta = 16$, the BER value increases from $8 \cdot 10^{-5}$ to 10^{-3} corresponding to β_m varying from 0 to 40. In return, the increment of β_m contributes to enhance the system security at the physical layer. This enhancement will be analyzed in Section IV.

The dependence of the system performance upon the number of users K for $\beta = 16$, $\beta_m = 10$ is displayed in Fig. 3(b). It can be clearly observed that the system performs worse with the increment of K. For example with the same value of $\frac{E_{ab}}{N_0} = 10dB$, the BER value increases from $3 \cdot 10^{-5}$ to $6 \cdot 10^{-2}$ corresponding to K increasing from 1 to 5.

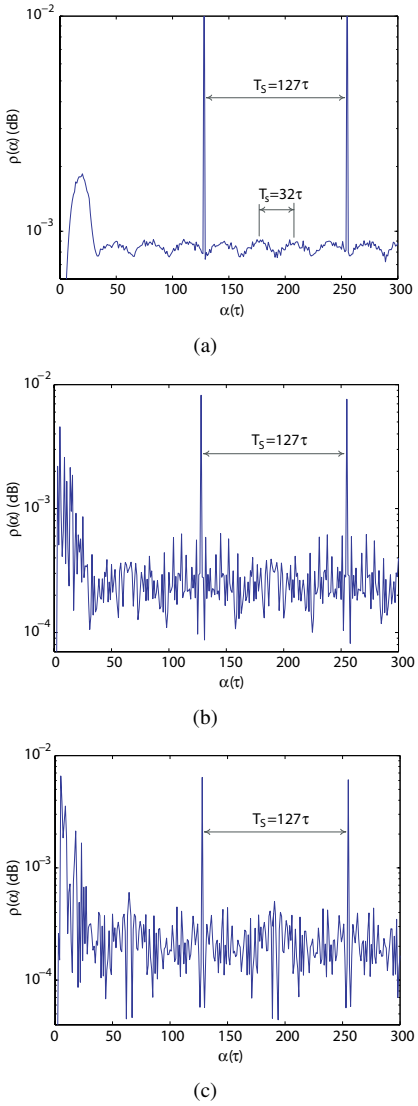
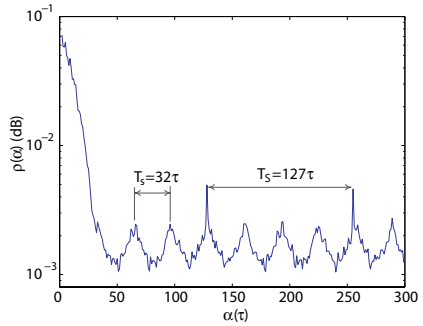


Fig. 4. Fluctuation graphs obtained by PC simulations for the first scenario in cases of (a) PN-DSSS technique, (b) Chaotic DSSS technique, and (c) Proposed DSSS technique.

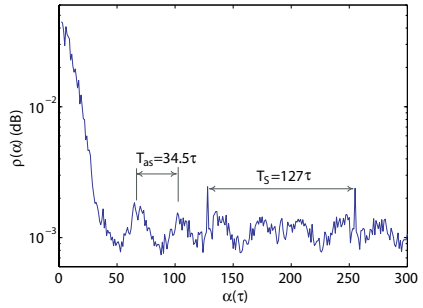
IV. Improvement of Physical Layer Security

In this section, we investigate the security ability of the proposed chaos-based DSSS technique by means of PC simulations. Let's suppose that an intruder uses the well-known attack method proposed in [13, 14] to detect the typical parameters, i.e, symbol period T_s and sequence period T_S, of the spreading sequence from the received signal $r(t)$. The attack method used relies on the computation of the fluctuation of the auto-correlation value. In order to compute the fluctuations, the received signal is divided into L temporal windows with W being the window width. By applying an autocorrelation estimator to each window, the correlation value is computed by

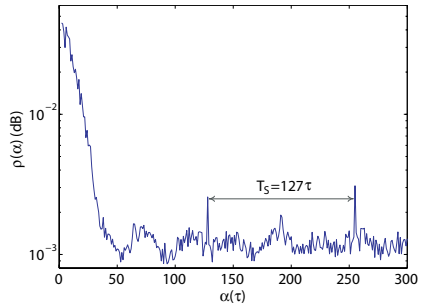
$$\widehat{R^n_{rr}(\alpha)} = \frac{1}{W} \int_0^W r(t) r^*(t-\alpha) dt, \qquad (15)$$



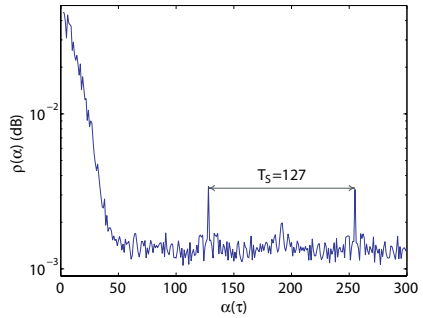
(a)



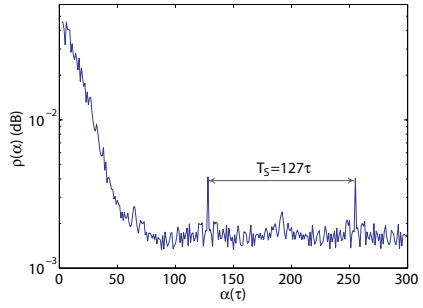
(b)



(c)



(d)



(e)

Fig. 5. Fluctuation graphs obtained by PC simulations for the second scenario in cases of (a) Chaotic DSSS technique, (b) Proposed DSSS technique with $\beta_m = 5$, (c) Proposed DSSS technique with $\beta_m = 10$, (d) Proposed DSSS technique with $\beta_m = 20$, (b) Proposed DSSS technique with $\beta_m = 40$.

where $\widehat{R^n_{rr}(\alpha)}$ is the correlation value of the n^{th} window, $r^*(t-\alpha)$ is the complex conjugate of $r(t-\alpha)$, and α is the shifted duration. The fluctuation value is then determined as follows:

$$\rho(\alpha) = \widehat{E}\left\{\left|\widehat{R^n_{rr}(\alpha)}\right|^2\right\} = \frac{1}{L}\sum_{0}^{L-1}\left|\widehat{R^n_{rr}(\alpha)}\right|^2. \qquad (16)$$

By plotting the graph of $\rho(\alpha)$ versus α, called fluctuation graph, the symbol period or sequence period can be determined by measuring the duration between peak values in the graph.

To compare the security level, we simulate the attack process of the intruder with respect to three techniques, i.e., PN-DSSS, chaotic DSSS, and chaotic DSSS with variable symbol period. The simulation parameters are chosen as follows: fixed spreading factor $\beta = 32$ for the cases of PN and chaotic DSSS techniques, $\beta = 32$ and $\beta_m = 5, 10, 20, 40$ for the case of the proposed technique, sequence period $T_S = 127\tau$, window width $W = 1000\tau$, and window number $L = 4000$. Here, the attack simulations are carried out for two scenarios: (1) the intruder has no information about the transmitting side. He performs a blind detection using the aforementioned method; (2) the intruder has full information on the spreading sequence. The received signal is multiplied with this known sequence. The output product is then used as the input signal of the detection method above.

Fluctuation graphs obtained by the simulations for the first scenario are shown in Fig. 5. For the case of the PN-DSSS technique, by measuring the cycle of periodic the curve of the graph in Fig. 4(a), the intruder can easily detect the symbol period, $T_s = 32\tau$, and the sequence period, $T_S = 127\tau$. With respect to the cases of the chaotic DSSS and our proposed techniques with $\beta_m = 10$, Fig. 4(b) and Fig. 4(c) clearly show that the intruder just detects the sequence period $T_S = 127\tau$ and there is no sign of the symbol period. These results point out an important feature, that is, the DSSS systems are protected from the attack method described above by replacing PN sequences by chaotic ones.

Fig. 5 presents the simulated fluctuation graphs for the second scenario. We can see from Fig. 5(a) that the intruder can detect both of the symbol and sequence periods in the case of the conventional chaotic DSSS technique. For the case of the proposed DSSS technique, Fig. 5(b), Fig. 5(c), Fig. 5(d), and Fig. 5(e) show that the intruder can detect the sequence period $T_S = 127\tau$ but cannot detect exactly the variation of the symbol period. With respect to the case of $\beta_m = 5$, the intruder may detect the average symbol period, i.e., $T_{as} = (\beta + \beta_m/2)\tau = 34.5\tau$, even so this average value is not enough to recover the original data. For the case of $\beta_m = 10$, the sign of the average period starts to disappear. There is no sign of the symbol period for the cases of $\beta_m = 20$ and $\beta_m = 40$. It means that our technique can hide the information of the symbol period, thus its security cannot be broken by the intruder who has full information on the chaotic sequence used.

V. CONCLUSIONS

This study has proposed and investigated a novel chaos-based DSSS technique, where the symbol period is varied according to the behavior of the chaotic spreading sequence used. Mathematical models in discrete time domain for the spreading scheme with variable symbol period and the despreading scheme with sequence synchronization are presented and analyzed. The BER performance of the proposed technique in DS-CDMA communication systems over an AWGN channel is estimated with the use of numerical simulation. The robustness against the attack of symbol period detection of the proposed technique in comparison with that of the conventional techniques is evaluated in two different scenarios by means of the numerical simulations. The obtained results show that: (1) the use of chaotic sequences instead of PN sequences helps to protect DSSS-based communication systems from blind estimation attacks to detect the symbol period; (2) the multiple access performance gets better when the initial spreading factor β is increased. With the chip period being fixed, this increment leads to the reduction of the symbol rate. On the other hand, the increment of variation width of the spreading factor, i.e., β_m, makes the performance worse, but in return the physical layer security is enhanced significantly. Therefore, the values of β and β_m have to be properly predetermined to guarantee the trade-off between performance, data rate and security of the system; (3) it is clear that the spreading, despreading and synchronization schemes of the proposed technique are more complicated than those of the conventional ones and they operate based on the process of discrete-sample processing. Therefore, these schemes are suitable to be implemented easily on high speed programmable integrated circuits. All the noticeable remarks above make the chaos-based DSSS with variable symbol period be a promising and robust technique for enhancing the physical layer security of DS-CDMA communication systems.

REFERENCES

[1] C. C. Chong and S. K. Yong, "UWB direct chaotic communication technology for low-rate WPAN applications," *IEEE Trans. Veh. Technol.*, vol. 57, no. 3, pp. 1527-1536, 2008.

[2] G. Kaddoum, P. Charge, and D.Roviras, "A generalized methodology for bit-error-rate prediction in correlation-based communication schemes using chaos," *IEEE Comm. Letters*, vol. 13, no. 8, pp. 567-569, 2009.

[3] N. X. Quyen, L. V. Cong, N. H. Long, V. V. Yem, "An OFDM-based chaotic DSSS communication system with MPSK modulation," *Proc. Int. Conf. Communications and Electronics (ICCE'14)*, Danang-Vietnam, 2014, pp. 106-111.

[4] S. M. Berber, "Probability of error derivatives for binary and chaos-based CDMA systems in wide-band channels," *IEEE Trans. Wirel. Commun.*, vol. 13, no. 10, pp. 5596-5606, 2014.

[5] M. K. Patel, , S. M. Berber, K. W. Sowerby, "Adaptive RAKE receiver in chaos based pilot-added DS-CDMA system," *Physical Communication*, vol. 16, pp. 37-42, 2015.

[6] N. X. Quyen, V. V. Yem, T. M. Hoang, and K. Kyamakya, "MxN-ary chaotic pulse-width-position modulation: An effective combination method for improving bit rate," *Int. Jour. for Computation and Mathematics in Electrical and Electronic Engineering*, vol. 32, no. 3, pp. 776-793, 2013.

[7] J. Yu and Y.-D. Yao, "Detection performance of chaotic spreading LPI waveforms," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 390-396, 2005.

[8] A. N. Miliou, I. P. Antoniades, S. G. Stavrinides, A. N. Anagnostopoulos, "Secure communication by chaotic synchronization: Robustness under noisy conditions," *Nonlinear Analysis: Real World Applications*, vol.8, no. 3, pp. 1003-2012, 2007.

[9] N. X. Quyen, T. Q. Duong, A. Nallanathan, "Modeling, analysis and performance comparison of two direct sampling DCSK receivers under frequency nonselective fading channels," *IET Communications*, doi: 10.1049/iet-com.2015.1103, 2016.

[10] S. Kodba, M. Perc, and M. Marhl, "Detecting chaos from a time series," *Europen Journal of Physics*, vol. 26, pp. 205-215, 2005.

[11] G. K. Rohdea, J. M. Nichols, and F. Bucholtz, "Chaotic signal detection and estimation based on attractor sets: Applications to secure communications," *Chaos: An Interdis. Jour. of Nonli. Science*, vol. 18, 013114, 2008.

[12] S-J. Kimy, K. Umenoyz, and R. Takahashiz, "Recovery of chaotic signals using on-line ICA algorithm," *2007 Int. Symp. on Nonli. Theory and its Appli. (NOLTA'07)*, Vancouver-Canada, Sept. 2007, pp. 192-195.

[13] G. Burel, "Detection of spread spectrum transmissions using fluctuations of correlation estimators," *IEEE-ISPACS*, Nov. 2000, pp. B8.2.5.1-B8.2.5.6.

[14] H. Xu, Z. Huang, Y. Zhou, "Blind estimation of the symbol period of a long-code DS-SS signal," *Int. Conf. on Micro.and Milli. Wave Techno. (ICMMT'07)*, Changsha-China, Apr. 2004, pp.1-4.

[15] N. X. Quyen, V. V. Yem, T. M. Hoang, "A chaos-based secure direct-sequence/spread-spectrum communication system," *Abstract and Applied Analysis*, 11 pages, doi: 10.1155/2013/764341, 2013.

[16] N. X. Quyen, V. V. Yem, T. Q. Duong, "Design and analysis of a spread-spectrum communication system with chaos-based variation of both phase-coded carrier and spreading factor," *IET Communications*, vol. 9, no. 12, pp. 1466-1473, 2015.