Hindawi Publishing Corporation
Abstract and Applied Analysis
Volume 2013, Article ID 764341, 11 pages
http://dx.doi.org/10.1155/2013/764341

Research Article

A Chaos-Based Secure Direct-Sequence/Spread-Spectrum Communication System

Nguyen Xuan Quyen, Vu Van Yem, and Thang Manh Hoang

School of Electronics and Telecommunications, Hanoi University of Science and Technology, 1 Dai Co Viet, Hanoi, Vietnam

Correspondence should be addressed to Thang Manh Hoang; thang@ieee.org

Received 11 October 2012; Revised 7 November 2012; Accepted 21 November 2012

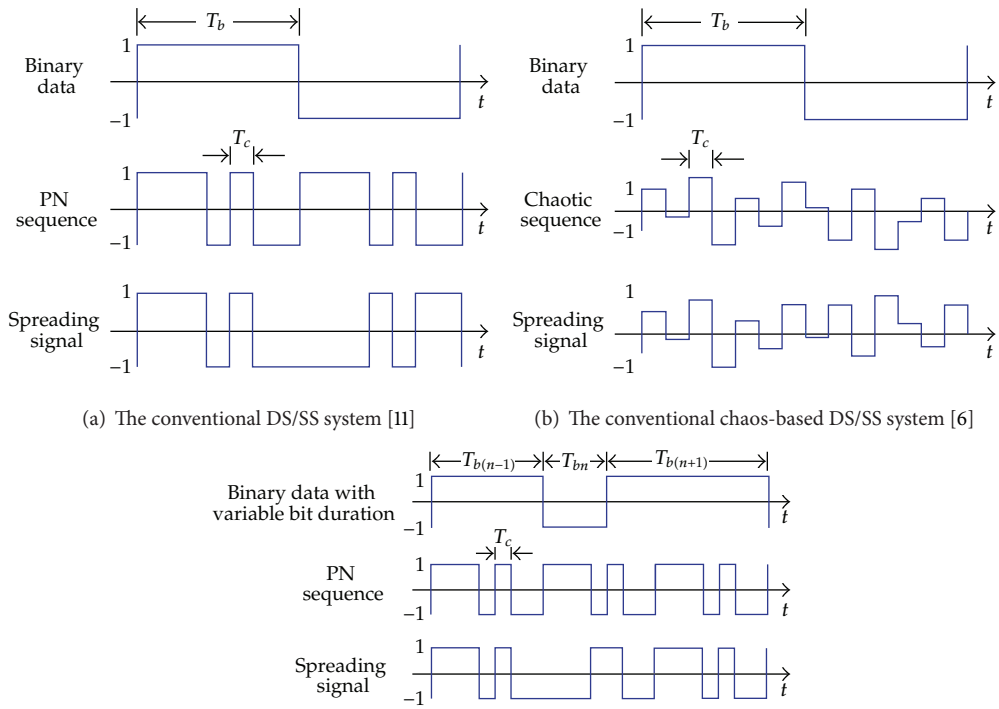
Academic Editor: Ivanka Stamova

This paper proposes a chaos-based secure direct-sequence/spread-spectrum (DS/SS) communication system which is based on a novel combination of the conventional DS/SS and chaos techniques. In the proposed system, bit duration is varied according to a chaotic behavior but is always equal to a multiple of the fixed chip duration in the communication process. Data bits with variable duration are spectrum-spread by multiplying directly with a pseudonoise (PN) sequence and then modulated onto a sinusoidal carrier by means of binary phase-shift keying (BPSK). To recover exactly the data bits, the receiver needs an identical regeneration of not only the PN sequence but also the chaotic behavior, and hence data security is improved significantly. Structure and operation of the proposed system are analyzed in detail. Theoretical evaluation of bit-error rate (BER) performance in presence of additive white Gaussian noise (AWGN) is provided. Parameter choice for different cases of simulation is also considered. Simulation and theoretical results are shown to verify the reliability and feasibility of the proposed system. Security of the proposed system is also discussed.

1. Introduction

Studying the possibilities of using chaotic behavior [1, 2] to improve features of communication systems has received significant attention in the last several years [3–5]. Many chaos-based communication systems were proposed [6, 7] and most of them exploited chaotic behavior to convey information. Communication systems based on combination of direct-sequence/spread-spectrum (DS/SS) and chaos techniques were presented in [8–10]. It is well known that DS/SS is considered as a main technique of spread-spectrum digital communications [11, 12]. The main difference between the conventional and chaos-based DS/SS systems is the use of spreading sequence. Instead of using the pseudonoise (PN) sequence [13, 14] as in the conventional system, the spread- and despread-spectrum processes in the chaos-based system are carried out by multiplying directly the binary data with a chaotic sequence generated by a chaotic map [1, 2, 15, 16]. Time domain signals shown in Figures 1(a) and 1(b) illustrate the difference in the conventional and chaos-based DS/SS systems, where T_b and T_c are fixed bit and chip durations, respectively.

In this paper, we propose a chaos-based secure DS/SS communication system which is the combination of the DS/SS and chaos techniques. Bit duration is varied according to the behavior of chaotic map but always equal to a multiple of the fixed chip duration. Variation in bit duration makes the difference between our proposed system and the conventional ones. The data bits with variable duration are spread in the frequency domain by multiplying directly with the PN sequence and then modulated onto a sinusoidal carrier by means of the binary phase-shift keying (BPSK) [17, 18]. The spread-spectrum process of our proposed chaos-based DS/SS system is illustrated by time domain signals as in Figure 1(c), where T_{bn} is the variable duration of the nth bit. Since the proposed system operates based on the DS/SS using PN sequence, it inherits all advantages such as interference rejection, antijamming, fading reduction, multi-access potential, and low probability of interception from the conventional DS/SS system [11, 12]. In addition, data security



(a) The conventional DS/SS system [11]

(b) The conventional chaos-based DS/SS system [6]

(c) The proposed chaos-based DS/SS system

Figure 1: Time domain signals of the spread-spectrum process in the conventional and proposed DS/SS systems.

is improved significantly since the despread-spectrum and data recovery process needs an identical regeneration of both the PN sequence and chaotic behavior.

In the remainder of the paper, the structure and operation of the proposed communication system is presented in Section 2. Theoretical evaluation of BER performance in presence of additive white Gaussian noise (AWGN) is provided in Section 3. Section 4 presents analysis of parameters choice for the system, based on that specific parameters for different cases of simulation system are chosen with proper values. Simulation results are then shown to verify the theoretical ones. Discussions on security features are presented in Section 5. Finally, the conclusion with some final remarks is given in Section 6.

2. Structure and Operation of Chaos-Based Secure DS/SS Communication System

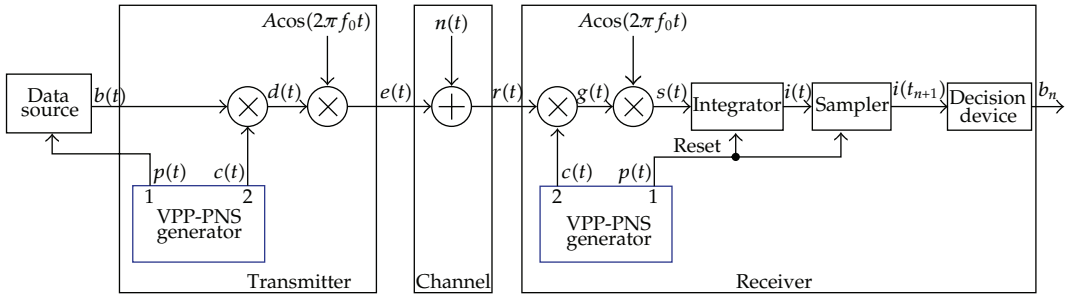
In this section, we present a detailed analysis of the structure and operation of the chaos-based DS/SS communication system proposed. Basically, the proposed system is built around a variable-position pulse and PN sequence (VPP-PNS) generator. Block diagrams of the proposed system and that of the VPP-PNS generator are illustrated in Figures 2(a) and 2(b), respectively.

2.1. VPP-PNS Generator. In the VPP-PNS generator, clock pulses with a fixed frequency, $f_c = 1/T_c$, at the output of the clock generator are fed to the counter and the PN generator. At the initial instance t_0, the clock generator starts working and the sample-and-hold block (S/H as in Figure 2) is loaded initial value X_0. The counter operates in free running mode to produce a discretely increasing signal, $C(t) = m \cdot (t - t_0) = mNT_c$, at its output, where m is count-step (i.e., the increasing value in a clock cycle T_c) and N is the count-number (i.e., the number of input clock pulses from the initial instance). When the signal $C(t)$ reaches the value, $X_1 = F(X_0)$, at the output of the nonlinear converter (i.e., the block $F(\cdot)$ using the one-dimension chaotic map, $X_n = F(X_{n-1})$), the comparator generates a pulse with a fixed width T_c at the instance, $t_1 = t_0 + N_0 T_c$. The position of pulse at the output 2 is determined by the interval, $t_1 - t_0 = \lfloor X_1/m \rfloor$, with $\lfloor \cdot \rfloor$ being the floor function. This pulse simultaneously triggers the PN sequence generator to start working and to allow S/H storing the value X_1. After that it triggers the counter to reset the count-number to zero. New iteration starts and pulses will be generated as in the above description. In general, the pulse train at the output 1 is expressed as follows:

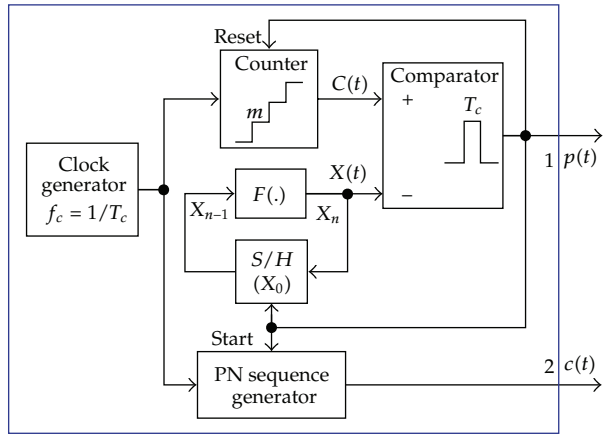
$$p(t) = \sum_{n=1}^{\infty} P_{T_c}(t - t_n), \tag{1}$$

where the nth pulse is generated at the instance

$$t_n = t_{n-1} + N_{n-1} T_c = t_{n-1} + \left\lfloor \frac{X_n}{m} \right\rfloor T_c, \tag{2}$$



(a) The block diagram for the proposed chaos-based DS/SS communication system



(b) The block diagram for the VPP-PNS generator

Figure 2: Structure of the proposed chaos-based DS/SS communication systems.

and its position is determined by the interval

$$t_n - t_0 = \sum_{k=1}^{n} \left\lfloor \frac{X_k}{m} \right\rfloor T_c = \sum_{k=1}^{n} \left\lfloor \frac{F^{(k)}(X_0)}{m} \right\rfloor T_c. \tag{3}$$

$P_{T_c}(t)$ is the rectangular pulse shaping function given by

$$P_{T_c}(t) = \begin{cases} 1, & 0 \le t \le T_c, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

It can be seen that the position of output pulses $p(t)$ varies according to the chaotic signal $X(t)$. With a specific initial instance t_0, (3) points out that variation of position depends on the chaotic map $F(\cdot)$, initial value X_0, and count-step m.

The PN sequence generated at the output 2 with the fixed chip duration of T_c is expressed by a nonreturn-zero (NRZ) pulse train as follows:

$$c(t) = \sum_{n=1}^{\infty} \sum_{k=1}^{N_n} c_k^n P_{T_c}\left(t - t_n - (k-1)T_c\right), \tag{5}$$

where c_k^n and N_n are the binary values (i.e., $\{\pm 1\}$) of the kth chip and the number of chips in the duration of $[t_n, t_{n+1}]$, respectively; the function $P_{T_c}(t)$ is as in (4).

2.2. Transmitter. In the transmitter, each pulse of the train $p(t)$ triggers the data source to shift the data bit to the output. It means that the nth bit is shifted at the instance t_n and its duration is equal to the interval of $[t_n, t_{n+1}]$. Based on (2), the duration of the nth bit is determined by

$$T_{bn} = t_{n+1} - t_n = N_n T_c = \left\lfloor \frac{X_{n+1}}{m} \right\rfloor T_c = \left\lfloor \frac{F^{(n+1)}(X_0)}{m} \right\rfloor T_c. \tag{6}$$

Equation (6) shows that the bit duration varies according to the chaotic signal $X(t)$ and depends on $F(\cdot)$, X_0, and m. With a certain chaotic map $F(\cdot)$, in the iteration process, its output values vary chaotically in the dimensionless range of $[X_{\min}, X_{\max}]$. This leads to the variation in the bit duration within the time range of $[T_{b\min}, T_{b\max}]$ in the communication process. Since the chip duration T_c is fixed, the number of chips per bit, $N_n = T_{bn}/T_c$, called the spreading factor, also varies in the range of $[N_{\min}, N_{\max}]$ what is determined in (6) as

$$N_{\min} = \frac{T_{b\min}}{T_c} = \left\lfloor \frac{X_{\min}}{m} \right\rfloor, \qquad N_{\max} = \frac{T_{b\max}}{T_c} = \left\lfloor \frac{X_{\max}}{m} \right\rfloor. \tag{7}$$

In the design process, the values of the parameters T_c, $N_{\min}$, and $N_{\max}$ are predetermined to guarantee desired specifications of the system such as the bandwidth, average bit rate,

and BER. The chaotic map $F(\cdot)$, the range of $[X_{\min}, X_{\max}]$, and the count-step m are then chosen so as to satisfy (7). The analysis of this choice will be presented in Section 4.1.

The binary data with variable bit duration at the output of the data source is formatted in NRZ pulses and expressed by

$$b(t) = \sum_{n=1}^{\infty} b_n P_{T_{bn}}(t - t_n), \tag{8}$$

where b_n is the binary value (i.e., $\{\pm 1\}$) of the nth bit, and $P_{T_{bn}}(t)$ is the rectangular pulse shaping function defined by

$$P_{T_{bn}}(t) = \begin{cases} 1, & 0 \le t \le T_{bn}, \\ 0, & \text{otherwise.} \end{cases} \tag{9}$$

The spectrum spreading process is carried out by multiplying the data $b(t)$ with the PN sequence $c(t)$. The spreading signal $d(t)$ is then modulated onto a sinusoidal carrier by means of BPSK, producing the DS/SS-BPSK signal given by

$$e(t) = Ab(t)\, c(t) \cos(2\pi f_0 t), \tag{10}$$

with A and f_0 being the amplitude and frequency of the carrier, respectively. The resulting signal $e(t)$ is transmitted at the output of the transmitter.

2.3. Receiver. The VPP-PNS generators in the transmitter and receiver are designed to work as digital modules which can be implemented on the programmable devices such as the field programmable gate array (FPGA), digital signal processing (DSP), and microprocessor (MP). In practice, this design can be guaranteed such that there is nearly no parameters mismatch between the VPP-PNS generators. It means that the variable-position pulse train and PN sequence regenerated in the receiver are identical to those in the transmitter. Therefore, we can apply the available synchronization methods of the conventional DS/SS system [11, 12, 18] for the proposed system. Here, for simplicity, the operation of the receiver assumes that the synchronization in the sinusoidal carrier, variable-position pulse train, and PN sequence is established and maintained.

The received signal $r(t)$ at the input is the sum of the transmitted signal $e(t)$ and channel noise $n(t)$. Firstly, the received signal is multiplied with the PN sequence as follows:

$$\begin{aligned} g(t) &= r(t)\, c(t) = (e(t) + n(t))\, c(t) \\ &= Ab(t)\, c^2(t) \cos(2\pi f_0 t) + n(t)\, c(t) \\ &= Ab(t) \cos(2\pi f_0 t) + n(t)\, c(t), \end{aligned} \tag{11}$$

and then the resulting signal $g(t)$ is mixed with the sinusoidal carrier by

$$\begin{aligned} s(t) &= Ag(t) \cos(2\pi f_0 t) \\ &= Ab(t) \cos^2(2\pi f_0 t) + An(t)\, c(t) \cos(2\pi f_0 t) \\ &= \frac{A^2}{2} b(t) + \frac{A^2}{2} b(t) \cos(4\pi f_0 t) \\ &\quad + An(t)\, c(t) \cos(2\pi f_0 t). \end{aligned} \tag{12}$$

The signal $s(t)$ is fed to the integrator whose output is reset to zero by the trigger of each pulse of the train $p(t)$. It means that the integration period of each bit is equal to the corresponding interpulse interval which is also the corresponding bit duration. Before each reset instance, the output signal of the integrator, $i(t)$, is sampled. The output value of the sampler at the instance t_{n+1} is determined by

$$\begin{aligned} i(t_{n+1}) &= \int_{t_n}^{t_{n+1}} s(t)\, dt \\ &= \int_0^{T_{bn}} \frac{A^2}{2} b(t)\, dt + \int_0^{T_{bn}} \frac{A^2}{2} b(t) \cos(4\pi f_0 t)\, dt \\ &\quad + \int_0^{T_{bn}} An(t)\, c(t) \cos(2\pi f_0 t)\, dt \\ &= \frac{A^2}{2} b_n T_{bn} + 0 + \int_0^{T_{bn}} An(t)\, c(t) \cos(2\pi f_0 t)\, dt, \end{aligned} \tag{13}$$

where $(A^2/2b_n)T_{bn}$ is the energy of the desired signal; $\int_0^{T_{bn}} (A^2/2b)(t) \cos(4\pi f_0 t) dt$ equal to zero because the period T_{bn} is a multiple of the carrier cycle (i.e., $T_0 = 1/f_0$); $\int_0^{T_{bn}} An(t)c(t) \cos(2\pi f_0 t) dt$ is the energy produced by the channel noise. It is noted that the correlation between $c(t)$ and $An(t) \cos(2\pi f_0 t)$ is very low and hence the noise energy is much less than the signal energy. Finally, the resulting sample is fed to the decision device to recover the binary value of the nth bit as follows:

$$b_n = \begin{cases} 1, & i(t_{n+1}) \ge 0, \\ 0, & i(t_{n+1}) < 0. \end{cases} \tag{14}$$

3. Theoretical Evaluation of BER Performance

In this section, BER performance of the proposed communication system with the channel noise being AWGN is evaluated theoretically. In the receiver, at each sampling instance, an error decision leading to an error bit occurs when the noise energy exceeds the signal energy in the opposite direction. Therefore, signal-to-noise ratio (SNR) of each output sample is a key parameter for estimating the BER of the system. Let us consider the value of the $(n+1)$th sample with two energy component as given in (13). The first component is the signal energy whose absolute magnitude is determined by

$$S_n = \left| \frac{A^2}{2} b_n T_{bn} \right| = \frac{A^2}{2} T_{bn}. \tag{15}$$

The second one is the noise energy which is a random variable depending on the zero-mean Gaussian noise $n(t)$ and thus

its mean is also zero, while its variance can be calculated as follows:

$$\sigma_n^2 = E\left[\left(\int_0^{T_{bn}} An(t)\,c(t)\cos\left(2\pi f_0 t\right)\right)^2\right] = \frac{A^2N_0}{2}\int_0^{T_{bn}} c^2(t)\cos^2\left(2\pi f_0 t\right)dt = \frac{A^2T_{bn}N_0}{4}, \tag{16}$$

where $E[\cdot]$ is the statistical expectation and N_0 is the noise power spectral density. The SNR of the $(n+1)$th sample, SNR_n, is determined as the absolute magnitude of the signal energy, S_n, divided by the root-mean-square noise $\sqrt{\sigma_n^2}$ [19], so we have

$$\mathrm{SNR}_n = \frac{S_n}{\sqrt{\sigma_n^2}} = \sqrt{\frac{A^2T_{bn}}{N_0}} = \sqrt{\frac{A^2N_nT_c}{N_0}} = \sqrt{2N_n\left(\frac{E_c}{N_0}\right)}, \tag{17}$$

where $E_c = A^2T_c/2$ is fixed, and called the energy per chip; the ratio E_c/N_0 is known as the SNR per chip. It can be seen from (17) that the SNR of each output sample depends on the ratio E_c/N_0 and the corresponding spreading factor N_n. Therefore, the SNR for general case of the spreading factor being equal to N is given by

$$\mathrm{SNR}_{N,E_c/N_0} = \sqrt{2N\left(\frac{E_c}{N_0}\right)}. \tag{18}$$

In our proposed system, since the spreading factor varies from $N_{\min}$ to $N_{\max}$ in the communication process, the BER is estimated approximately by

$$\mathrm{BER}_{[N_{\min},N_{\max}],E_c/N_0} = \sum_{N=N_{\min}}^{N_{\max}} p_N \mathrm{BER}_{N,E_c/N_0}, \tag{19}$$

where p_N is the probability to the spreading factor being equal to N, and $\mathrm{BER}_{N,E_c/N_0}$ is the BER of the system for case of the spreading factor being equal to N. Assume that the chaotic values distribute uniformly in $[X_{\min}, X_{\max}]$. It means that the probability p_N is the same for all values of $N \in [X_{\min}, X_{\max}]$, so we have

$$p_N = \frac{1}{\left(N_{\max} - N_{\min} + 1\right)}. \tag{20}$$

Based on the evaluation result of the error probability for the conventional DS/SS-BPSK system as mentioned in [20, 21], the $\mathrm{BER}_{N,E_c/N_0}$ is determined according to the $\mathrm{SNR}_{N,E_c/N_0}$ by

$$\mathrm{BER}_{N,E_c/N_0} = Q\left[\mathrm{SNR}_{N,E_c/N_0}\right] \quad \text{with } Q[x] = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-u^2/2}du. \tag{21}$$

From the obtained results in (18), (19), (20), and (21), the theoretical evaluation of the BER performance for the proposed communication system is given by the following:

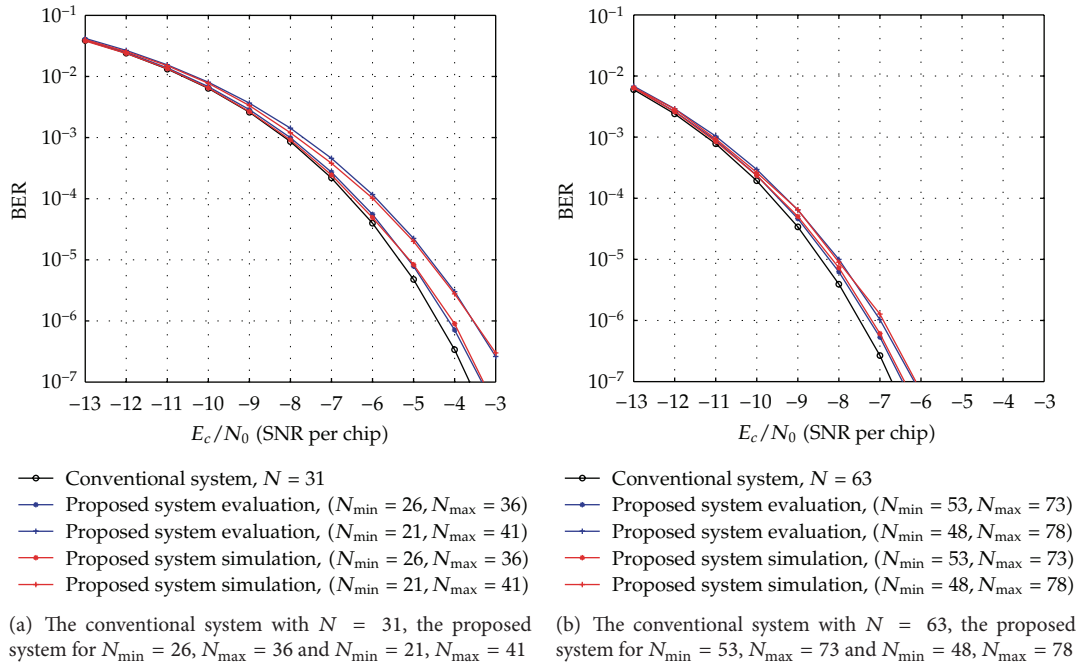
$$\mathrm{BER}_{[N_{\min},N_{\max}],E_c/N_0} = \frac{1}{\left(N_{\max} - N_{\min} + 1\right)}\sum_{N=N_{\min}}^{N_{\max}} Q\left[\sqrt{2N\left(\frac{E_c}{N_0}\right)}\right]. \tag{22}$$

The evaluation BER performances according to (22) for different cases of $[N_{\min}, N_{\max}]$ with the same average spreading factor as well as their comparison with the performance of the equivalent conventional system are shown in Figure 3. With the above assumption of the uniformly distributed chaotic values, the average spreading factor and average bit rate are determined by $N_{\mathrm{av}} = (N_{\min} + N_{\max})/2$ and $\mathrm{BR}_{\mathrm{av}} = 2/((N_{\min} + N_{\max})T_c)$, respectively. In Figure 3(a), the performances of the proposed system for the cases of $[N_{\min} = 26, N_{\max} = 36]$ and $[N_{\min} = 21, N_{\max} = 41]$, are compared to each other and to that of the conventional system [21] which has a fixed spreading factor, $N = N_{\mathrm{av}} = 31$. It can be seen that the proposed system with the case of $[N_{\min} = 26, N_{\max} = 36]$ performs slightly worse than the conventional system with $N = 31$ and better than the $[N_{\min} = 21, N_{\max} = 41]$ case. Similarly, we can observe from Figure 3(b) that the performance of $[N_{\min} = 53, N_{\max} = 73]$ case is between those of the conventional system with $N = 63$ and the case of $[N_{\min} = 48, N_{\max} = 78]$. It is clear that the performance of the proposed system with $[N_{\min}, N_{\max}]$ is poorer than that of conventional system with $N = N_{\mathrm{av}}$. In addition, the difference between the performance of the proposed system and that of conventional one tends to diminish as the average value $(N_{\min} + N_{\max})/2$ gets closer to $N = N_{\mathrm{av}}$.

4. Parameter Choice and Simulation Results

This section presents the analysis of parameter choice for the proposed system. Based on the analysis, the specific parameters for different cases of the simulation system are chosen with proper values. The simulation results are then shown in order to verify all the theoretical analyses and results obtained.

4.1. Parameter Choice. In order to guarantee the desired specifications of the system such as the bandwidth (i.e., $\mathrm{BW} = 1/T_c$), average bit rate (i.e., $\mathrm{BR}_{\mathrm{av}} = 2/((N_{\min} + N_{\max})T_c)$, and BER (i.e., $\mathrm{BER}_{[N_{\min},N_{\max}],E_c/N_0}$ according to (22)), the values of parameters $T_c, N_{\min}$, and $N_{\max}$ are predetermined. The chaotic behavior of the chaotic map $F(\cdot)$ is based on that of a conventional chaotic map, $x_n = f(x_{n-1})$, denoted by $f(\cdot)$, whose output values vary in a known range of $[x_{\min}, x_{\max}]$. The parameters $T_c, N_{\min}$, and $N_{\max}$ and the map $f(\cdot)$ are considered as the predetermined parameters of the system.



(a) The conventional system with $N = 31$, the proposed system for $N_{min} = 26$, $N_{max} = 36$ and $N_{min} = 21$, $N_{max} = 41$

(b) The conventional system with $N = 63$, the proposed system for $N_{min} = 53$, $N_{max} = 73$ and $N_{min} = 48$, $N_{max} = 78$

FIGURE 3: BER performances obtained from the theoretical evaluation and numerical simulation for different cases of the proposed system in comparison to those of the equivalent conventional system.

Using these predetermined parameters, the count-step m and the chaotic map $F(\cdot)$ are chosen as follows:

$$m = \frac{x_{max} - x_{min}}{N_{max} - N_{min}},$$

$$X_n = x_n + d = f(x_{n-1}) + d = f(X_{n-1} - d) + d = F(X_{n-1}). \quad (23)$$

It is easy to find that the output value of the chaotic map $F(\cdot)$ varies chaotically in the range of $[X_{min} = x_{min} + d, X_{max} = x_{max} + d]$ and thus the initial value X_0 will be chosen in this range. Here, d is a shift value chosen to satisfy (7) as follows:

$$N_{min}m - x_{min} \le d < (N_{min} + 1)m - x_{min}. \quad (24)$$

The count-step m and the parameters d, X_0 of the map $F(\cdot)$ are called the chosen parameters of the system.

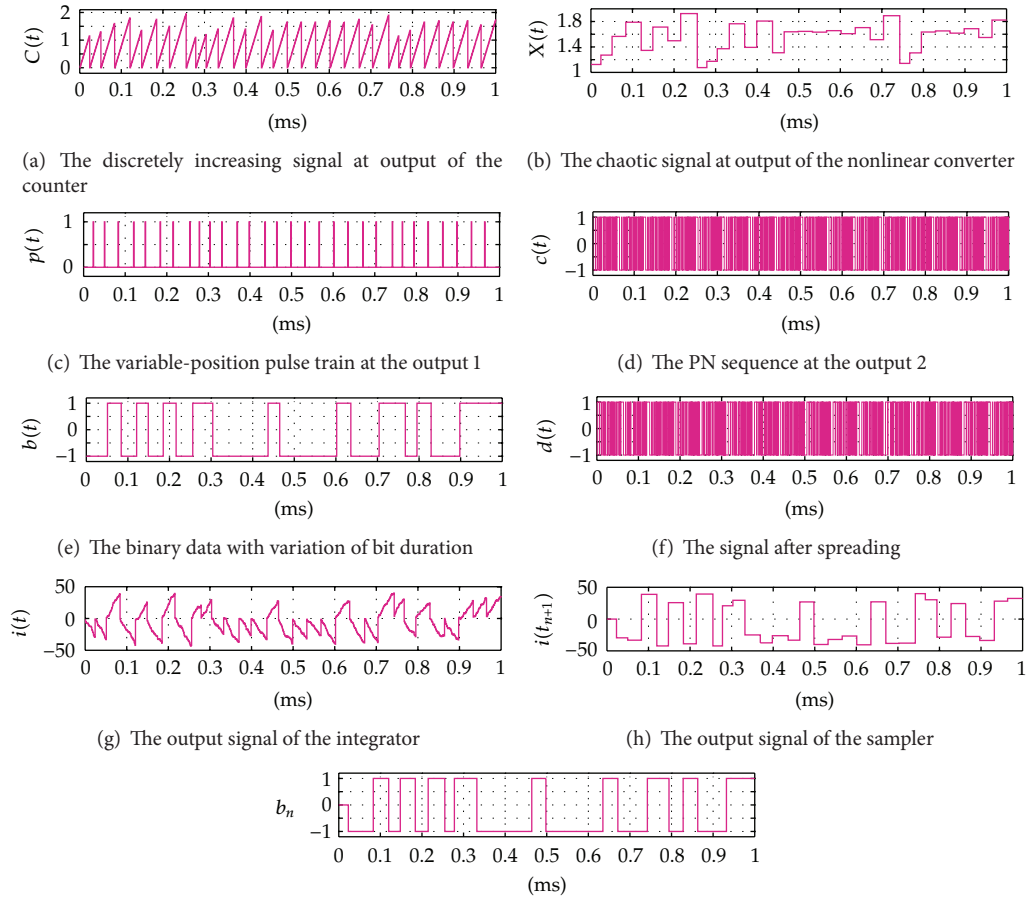
4.2. Simulation Results. Numerical simulations for different cases of the proposed system with the specific parameters are carried out in Simulink. The values of the predetermined parameters of the simulation system are given as follows: $T_c = 1\ \mu s$; four cases of $[N_{min}, N_{max}] = [26, 36], [21, 41], [53, 73]$, and $[48, 78]$; three conventional chaotic maps simulated in turn are Tent map, Logistic map, and Bernoulli map [1, 2, 15, 16], whose output values vary chaotically in $[x_{min} = 0, x_{max} = 1]$. Based on the choice analysis above, the values of the specifications and chosen parameters of the simulation system corresponding to the different cases of $[N_{min}, N_{max}]$ are determined and shown as in Table 1.

Time domain signals obtained from the simulation system using Tent map for the case of $[N_{min} = 21, N_{max} = 41]$ within duration from the starting time 0 to $1000\ \mu s$ are presented in Figure 4. When the synchronization state of system is established and maintained, the signals of the VPP-PNS generators in the transmitter and receiver are identical and shown as in Figures 4(a)–4(d). The baseband signals in the transmitter and receiver are given in Figures 4(e)-4(f) and Figures 4(g)–4(i), respectively. The chaotic behavior the nonlinear converter $F(\cdot)$ is seen by the attractor diagram in Figure 5(a). It is clear that this is the attractor of Tent map after being shifted with a positive value, $d = 1.075$. The variation in bit duration according to the chaotic behavior is given in the diagram as in Figure 5(b), where each point expresses the relation between the duration of previous bit and that of the present one. It can be seen that the bit duration varies in the range of $[T_{b\,min} = 21\ \mu s, T_{b\,max} = 41\ \mu s]$.

BER performance of the simulation system using Tent map for the cases of $[N_{min} = 26, N_{max} = 36]$, $[N_{min} = 21, N_{max} = 41]$, $[N_{min} = 53, N_{max} = 73]$, $[N_{min} = 48, N_{max} = 78]$ is presented in Figure 3 to compare with the corresponding theoretical performance. In order to investigate the performance of the proposed system with different chaotic maps, the simulation systems using Tent, Logistic, and Bernoulli maps for the cases of $[N_{min} = 21, N_{max} = 41]$ and $[N_{min} = 26, N_{max} = 36]$ are carried out and the result is as shown in Figure 6. Here, the simulation BERs are calculated as the number of error bits divided by the total number of 10^8 bits transmitted and the channel noise is AWGN. It can be seen from Figure 3, for each case, that the simulation and corresponding evaluation curves are nearly the same. Also, Figure 6 shows that there is a slight difference in the simulation curves of the different chaotic maps. These prove

Table 1: Specific parameters of the simulation system for cases of $[N_{\min}, N_{\max}] = [26, 36], [21, 41], [53, 73], [48, 78]$.

Predetermined parameters			Specifications of system			Chosen parameters			
T_c	$[N_{\min}, N_{\max}]$	$f(\cdot) : x_n = f(x_n - 1)$ $[x_{\min} = 0, x_{\max} = 1]$	BW	BR_{av}	BER	m	Chaotic map $F(\cdot) : X_n = F(X_{n-1})$ $[X_{\min} = d, X_{\max} = d + 1]$	d	X_0
$1\,\mu$s	$[26, 36]$	Tent map: $x_n = 2\,\lvert 0.5 - \lvert 0.5 - x_{n-1}\rvert\rvert$	1 MHz	32.25 Kbps	Blue lines in Figure 2(a)	$0.1/\mu$s	$X_n = 2\,\lvert 0.5 - \lvert 0.5 - (X_{n-1} - d)\rvert + d\rvert$	2.65	2.7
	$[21, 41]$	Logistic map: $x_n = 4x_{n-1}(1 - x_{n-1})$				$0.05/\mu$s	$X_n = 4(X_{n-1} - d)(1 - (X_{n-1} - d)) + d$	1.075	1.1
	$[53, 73]$	Bernoulli map: $x_n = (2x_{n-1}) \bmod 1$		15.87 Kbps	Blue lines in Figure 2(b)	$0.05/\mu$s	$X_n = ((2(X_{n-1} - d)) \bmod 1) + d$	2.675	2.7
	$[48, 78]$					$0.033/\mu$s		1.616	1.7



(a) The discretely increasing signal at output of the counter

(b) The chaotic signal at output of the nonlinear converter

(c) The variable-position pulse train at the output 1

(d) The PN sequence at the output 2

(e) The binary data with variation of bit duration

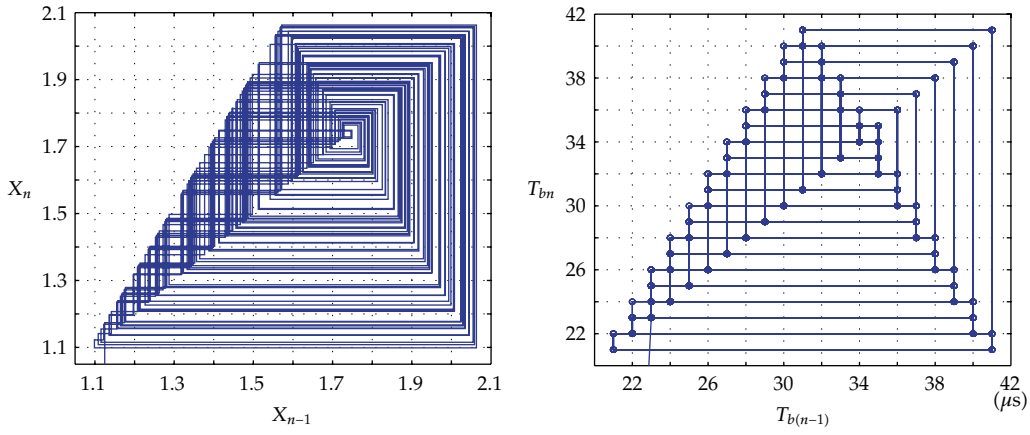
(f) The signal after spreading

(g) The output signal of the integrator

(h) The output signal of the sampler

(i) The recovered data bits at output of the decision device

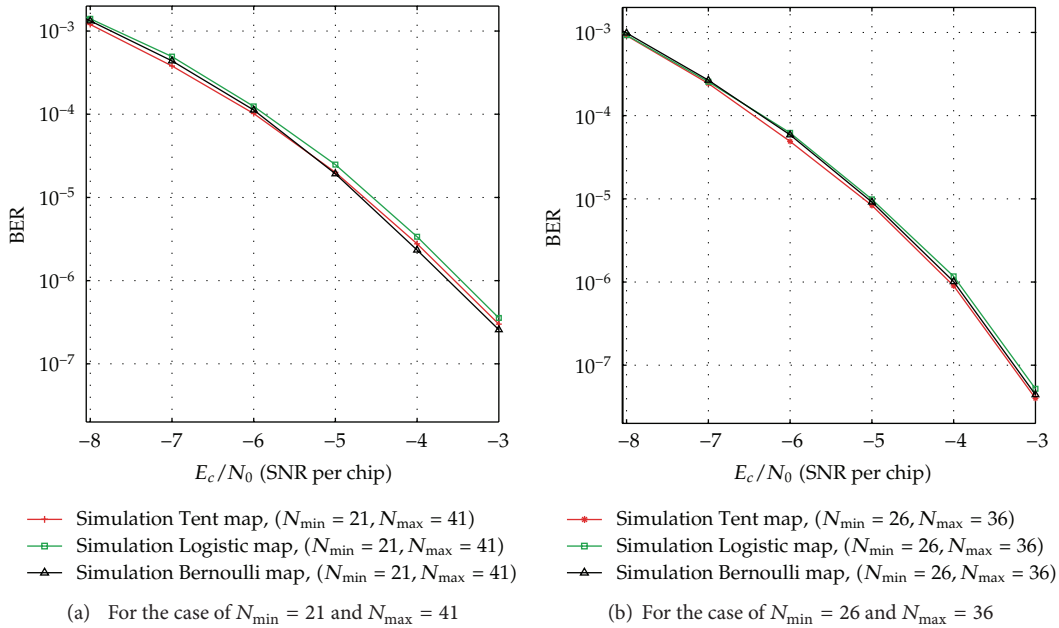
FIGURE 4: Time domain signals of the simulation system using Tent map for case of $[N_{\min} = 21, N_{\max} = 41]$.



(a) The attractor diagram of the chaotic map $F(\cdot)$

(b) The variation diagram of bit duration

FIGURE 5: The variation of bit duration according to the chaotic behavior.



(a) For the case of N_{min} = 21 and N_{max} = 41

(b) For the case of N_{min} = 26 and N_{max} = 36

Figure 6: Simulation BER performances with different chaotic maps.

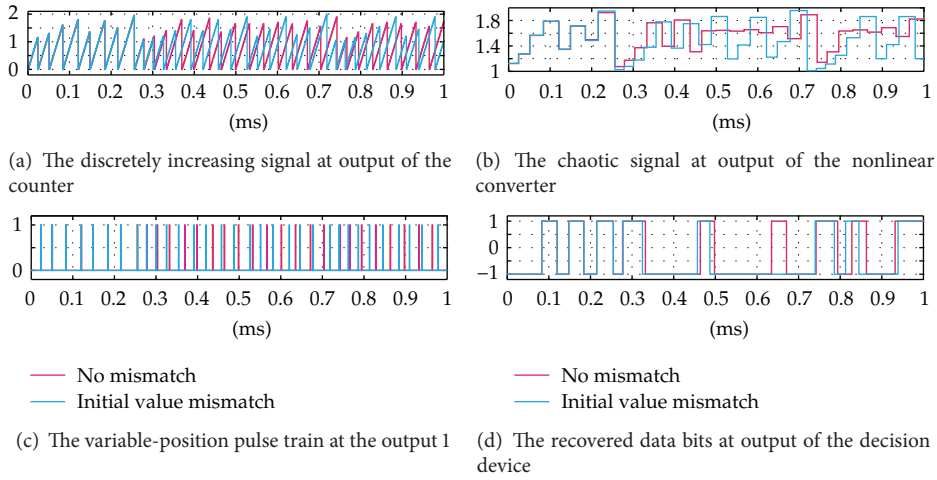
that the theoretical analysis and the result are reasonable and the proposed communication system is totally feasible.

5. Discussion on Security

It is clear that the conventional DS/SS-BPSK system, an intruder can break the security and recover successfully the original data if he detects correctly the PN sequence and the integration period which is equal to bit rate. Since the bit duration is the same and fixed in the observation process, it is not difficult for the intruder to detect exactly bit rate. Several detection methods of bit rate have been presented in [22, 23]. It means that the security of the conventional system mainly depends on the complication of PN sequence.

Since our proposed system is combined by the DS/SS technique using PN sequence and chaotic modulation, the data transmitted by using the proposed system must be more secure from eavesdroppers than that in case of using individual methods. In other words, the security has been compromised by burying chaotic modulation in the conventional DS/SS technique. With the presence of the conventional DS/SS technique in the proposed system, the transmitted signal has properties like random noise and occupies a wide bandwidth with a very low power spectral density on the transmission channel. It means that the proposed system inherits the security advantages from the conventional method such as the anti jamming capability and low probability of detection and interception [24, 25]. In addition, with the variation of bit duration according to the chaotic behavior, the capability to protect data against unauthorized accesses is improved significantly.

More specifically, the data security of the proposed system is dependent on not only on the complication of PN sequence but also on the variation of the integration period (i.e., the bit duration) according to the chaotic behavior. It is seen that the generation of the chaotic behavior is quite simple for the transmitter and the authorized receiver which has full information on the structure, the value of parameters and functions. In fact, the exact regeneration of chaotic behavior in the proposed system is very difficult for intruders trying to detect them in the context that the chaotic system is covered by the PN sequence generator. Due to the sensitive dependence of the chaotic behavior on the initial value, a very slight error in its detection leads to exponentially increasing errors in the regeneration. In such case, the detection of the variation of bit duration is completely incorrect and the receiver operates in the desynchronization state. As a result, BER will be very high and thus the unauthorized access is failed. These are proved by simulation results in Figures 7 and 8, where the time domain signals and BER performances of the receiver in the case of initial value mismatch (with a very small difference, $\Delta X_0 = 0.0001$) are shown and compared with those in the case of no mismatch. We can observe that after about 0.2 ms from the starting time, the mismatch signals become totally different from the corresponding no-mismatch signals. The BER performance with the mismatch is much worse than that of the cases with no-mismatch. Particularly, although the ratio E_c/N_0 increases gradually, the mismatches in BER are nearly unvaried and approximately equal to 1.6 10^{-1}. It is noticed that the set of values of m, X_0, and $F(\cdot)$ is considered as a secret key. It is hard for the intruder to recover correctly the data without having full information on the structure of the system, the PN sequence, and this secret key. Furthermore, the generation of the chaotic values can easily be made as complicated as is desired. For example, instead of the one-dimension maps, we can use multidimension chaotic ones. Also, several chaotic maps may be combined to increase the number of parameters involved.



(a) The discretely increasing signal at output of the counter

(b) The chaotic signal at output of the nonlinear converter

(c) The variable-position pulse train at the output 1

(d) The recovered data bits at output of the decision device

FIGURE 7: Time domain signals in the receiver of the simulation system using Tent map for case of $[N_{\min} = 21, N_{\max} = 41]$ with no mismatch and with initial value mismatch ($\Delta X_0 = 0.0001$).

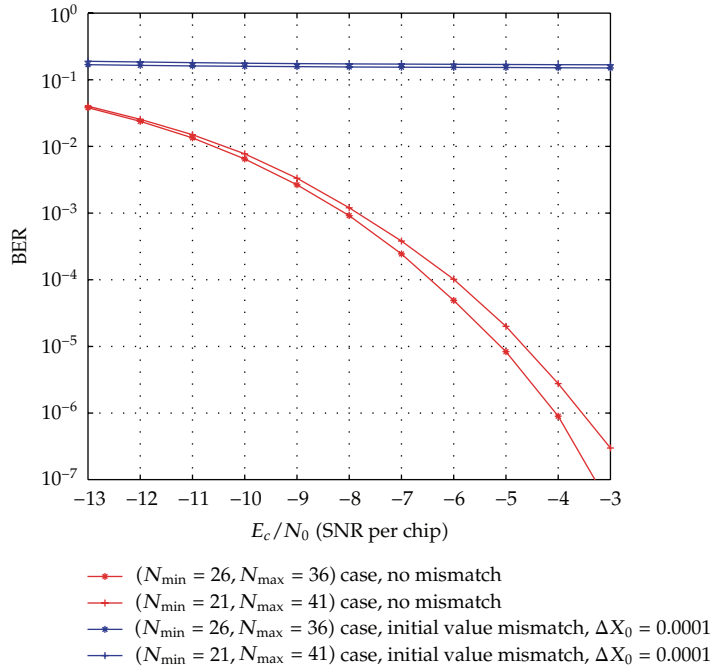


FIGURE 8: BER performances of the simulation system using Tent map for cases of $[N_{\min} = 26, N_{\max} = 36]$ and $[N_{\min} = 21, N_{\max} = 41]$ with no mismatch and with initial value mismatch ($\Delta X_0 = 0.0001$).

The initial value can be changed for different communication sessions. All these will improve significantly the security of the proposed method.

Most of the attack methods are proposed in order to break the chaotic communication systems [26–29] operated based on exploiting properties such as waveform, spectrum, and attractor of the chaotic signal which masks the information and is transmitted directly on the channel. In the proposed system, the signal transmitted on the channel is totally the same as that of the conventional system and without any trace of the chaotic behavior; thus, the existing attack methods are inapplicable to the proposed system. It means that no chance for the intruder to be able to detect the variation of bit duration from the physical signal on the channel. It is also clear that the conventional detection methods of bit rate mentioned above cannot detect in detail this variation. They may detect the variation range and average value of bit duration, but this is not sufficient for a successful access.

6. Conclusion

This study has presented a chaos-based secure DS/SS communication system which is based on a novel combination of the conventional DS/SS and chaos techniques. The structure,

operation, and BER performance of the proposed system are described and investigated by means of the theoretical analysis and numerical simulation. The simulation result agrees with the theoretical analysis. The discussion shows the potential of security improvement. It can be seen from the obtained results, that is, (1) the proposed system inherits all the advantages from the conventional system such as the interference rejection, antijamming, fading reduction, multiaccess capability, and low probability of interception due to its operation also based on the DS/SS using PN sequence and BPSK technique; (2) with the variation of bit duration according to the chaotic behavior in the communication process, the proposed system not only still maintains an approximately good performance but also achieves significant improvement on the data security in comparison with the equivalent conventional system. All these features make the proposed system feasible and robust for the security required and DS/SS-based digital communication system.

Acknowledgment

This work is supported by the Vietnam's National Foundation for Science and Technology Development (NAFOSTED) under Grant no. 102.02-2012.34.

References

[1] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*, Westview Press, 2001.

[2] R. C. Hilborn, *Chaos and Nonlinear Dynamics: An introduction for Scientists and Engineer*, The Clarendon Press Oxford University Press, 2001.

[3] M. P. Kennedy, R. Rovatti, and G. Setti, *Chaotic Electronics in Telecommunications*, CRC Press, 2000.

[4] M. P. Kennedy and G. Kolumbán, "Special issue on noncoherent chaotic communications," *IEEE Transactions on Circuits and Systems I* , vol. 47, no. 12, pp. 1661–1662, 2000.

[5] A. Abel and W. Schwarz, "Chaos communications—Principles, schemes, and system analysis," *Proceedings of the IEEE*, vol. 90, no. 5, pp. 691–710, 2002.

[6] F. C. M. Lau and C. K. Tse, *Chaos-Based Digital Communication Systems: Operating Principles, Analysis Methods, and Performance Evaluation*, Springer, 2003.

[7] P. Stavroulakis, *Chaos Applications in Telecommunications*, CRC Press, 2005.

[8] G. Heidari-bateni and C. D. McGillem, "Chaotic direct-sequence spread-spectrum communication system," *IEEE Transactions on Communications*, vol. 42, no. 2, pp. 1524–1527, 1994.

[9] G. Heidari-Bateni and C. D. McGillem, "Chaotic sequences for spread spectrum: an alternative to PN-sequences," in *Proceedings of the IEEE International Conference on Selected Topics in Wireless Communications*, pp. 437–440, Vancouver, Canada, June 1992.

[10] A. P. Kurian, S. Puthusserypady, and S. M. Htut, "Performance enhancement of DS/CDMA system using chaotic complex spreading sequence," *IEEE Transactions on Wireless Communications*, vol. 4, no. 3, pp. 984–989, 2005.

[11] R. L. Peterson, R. E. Zeimer, and D. E. Borth, *Introduction to Spread Spectrum Communications*, Prentice Hall, New York, NY, USA, 1995.

[12] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, Computer Science Press, 1985.

[13] E. H. Dinan and B. Jabbari, "Spreading codes for direct sequence CDMA and wideband CDMA cellular networks," *IEEE Communications Magazine*, vol. 36, no. 9, pp. 48–54, 1998.

[14] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proceedings of the IEEE*, vol. 68, no. 5, pp. 593–619, 1980.

[15] R. L. Devaney, *An Introduction to Chaotic Dynamica Systems*, Addison-Wesley, Reading, Mass, USA, Second edition, 1989.

[16] H. G. Schuster, *Deterministic Chaos, an Introduction*, Physick, Weinheim, Germany, 1984, D-6940.

[17] R. L. Frank and S. A. Zadoff, "Phase shift pulse codes with good periodic correlation properties," *IRE Transactions on Information Theory*, vol. 8, pp. 381–382, 1962.

[18] J. Proakis, *Digital Communications*, McGraw-Hill, New York, NY, USA, 4th edition, 2000.

[19] M. B. Pursley, "Performance evaluation for phase-coded spread-spectrum multiple-access communication—part I: system Analysis," *IEEE Transactions on Communications*, vol. 25, no. 8, pp. 795–799, 1977.

[20] R. K. Morrow and J. S. Lehnert, "Bit-to-bit error dependence in slotted DS/SSMA packet systems with random signature sequences," *IEEE Transactions on Communications*, vol. 37, no. 10, pp. 1052–1061, 1989.

[21] J. M. Holtzman, "A simple, accurate method to calculate spread-spectrum multiple-access error probabilities," *IEEE Transactions on Communications*, vol. 40, no. 3, pp. 461–464, 1992.

[22] D. E. Reed, "Comparison of symbol-rate detector and radiometer intercept receiver performances in a nonstationary environment," in *Proceedings of the IEEE Military Communications Conference*, vol. 1, pp. 1951–1955, Boston, Mass, USA, October 1989.

[23] G. Burel, C. Bouder, and O. Berder, "Detection of direct sequence spread spectrum transmissions without prior knowledge," in *Proceedings of the IEEE Global Telecommunicatins Conference*, pp. 236–239, November 2001.

[24] R. A. Dillard, "Detectability of spread-spectrum signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 15, no. 4, pp. 526–537, 1979.

[25] R. Schoolcraft, "Low probability of detection communications–LPD waveform design and detection techniques," in *Proceedings of the Military Communications Conference*, vol. 2, pp. 3531–3539, McLean, Va, USA, November 1991.

[26] K. M. Short, "Steps toward unmasking secure communication," *International Journal of Bifurcation and Chaos*, vol. 4, no. 4, pp. 959–977, 1994.

[27] K. M. Short, "Unmasking a modulated chaotic communications scheme," *International Journal of Bifurcation and Chaos*, vol. 6, no. 2, pp. 611–615, 1996.

[28] M. I. Sobhy and A. R. Shehata, "Methods of attacking chaotic encryption and countermeasures," in *Proceedings of the IEEE Interntional Conference on Acoustics, Speech, and Signal Processing*, vol. 2, pp. 1001–1004, May 2001.

[29] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Breaking parameter modulated chaotic secure communication system," *Chaos, Solitons and Fractals*, vol. 21, no. 4, pp. 783–787, 2004.