Computer Networks 000 (2016) 1–9

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Chaotic direct-sequence spread-spectrum with variable symbol period: A technique for enhancing physical layer security

Nguyen Xuan Quyen[a], Trung Q. Duong[b,c,*], Nguyen-Son Vo[c], Qingqing Xie[d], Lei Shu[d]

[a] Hanoi University of Science and Technology, Hanoi, Vietnam
[b] Queen's University Belfast, Belfast, United Kingdom
[c] Duy Tan University, Da Nang, Vietnam
[d] Guangdong University of Petrochemical Technology, Guangdong, China

ARTICLE INFO

Article history:
Received 24 October 2015
Revised 25 February 2016
Accepted 18 June 2016
Available online xxx

Keywords:
Chaos
Chaotic sequences
Chaos-based digital communications
Chaotic DSSS
Chaos-based DS-CDMA
Physical layer security

ABSTRACT

In chaotic direct-sequence spread-spectrum (DSSS) technique, chaotic sequences with typical properties such as aperiodic variation, wideband spectrum, good correlation, and initial condition sensitivity have been used as spreading codes in order to improve the security at physical layer. However, a number of recent studies have proved that an intruder can recover chaotic sequences by blind estimation methods and use the sequences to detect symbol period, which will result in the original data being exposed. To overcome this security weakness, this paper proposes a novel chaotic DSSS technique, where the symbol period is varied according to behavior of the chaotic spreading sequence in the communication process. The data with variable symbol period is multiplied with the chaotic sequence to perform the spread-spectrum process. Discrete-time models for the spreading scheme with variable symbol period and the despreading scheme with sequence synchronization are presented and analyzed. Multiple-access performance of the proposed technique in the presence of the additional white Gaussian noise (AWGN) is calculated by means of both theoretical derivation and numerical computation. Computer simulations are carried out and simulated performances are shown to verify the estimated ones. Obtained results point out that our proposed technique can protect the DSSS systems against the detection of symbol period from the intruder, even if he has full information on the used chaotic sequence.

1. Introduction

The use of chaotic sequences as a secure alternative to pseudo-noise (PN) sequences in direct-sequence spread-spectrum (DSSS) communication systems has been widely studied during the two last decades [1,2]. This alternative is due to the advantages that chaotic sequences can offer, such as non-periodic variation with an infinite number of states [3], wideband with good correlation [4], support of multiple access operation [5], robustness in multi-path environments [6], resistance to jamming [7], low probability of interception [8], and transmission security at physical layer [9]. Multiple studies have been devoted to the design and analysis of chaos-based DSSS technique, which can be divided into two main categories, i.e., (i) design [10], optimization [11], synchronization [12–14] of chaotic spreading sequences, and (ii) theoretical and numerical analysis of the BER performance for chaos-based direct sequence/code division multiple access (DS/CDMA) communication systems under different transmission channels [15–19].

Among all the aforementioned advantages, the main goal of the application of chaotic sequences to spread-spectrum communications is the enhancement of physical layer security [1,2]. However, several recent studies have proved that chaotic sequences can be recovered by blind detection methods [20–22]. In [20], a detection method based on nonlinear time series analysis is presented, 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 [21] by exploiting intrinsic geometry of chaotic attractor sets. Based on the reconstructed attractor, the used chaotic sequence can be recovered by an approximation algorithm. Another method for recovering chaotic sequences is proposed in [22], where 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

[*] Corresponding author.
E-mail addresses: quyen.nguyenxuan@hust.edu.vn (N.X. Quyen), trung.q.duong@qub.ac.uk (T.Q. Duong), vonguyenson@gmail.com (N.-S. Vo), qingqing.xie@outlook.com (Q. Xie), lei-shu@outlook.com (L. Shu).

http://dx.doi.org/10.1016/j.comnet.2016.06.022
1389-1286/© 2016 Elsevier B.V. All rights reserved.

sequence, he then use the recovered sequence in detecting symbol period [23,24]. With the recovered sequence and detected period, he can totally recover the original data and breaks the security of chaos-based DSSS systems.

To address the aforementioned security challenge, in this paper, we propose a novel chaos-based DSSS technique in which the period of data symbol is varied according to the chaotic behavior of the spreading sequence. Owing to both the spreading sequence and symbol period varying chaotically in the same time, the bit energy also varies according to the chaotic behavior. This simultaneous variation makes the unauthorized detection of the symbol period using the energy detection methods [23,24] become more and more difficult. Previously, the study in [25] proved that the random variation of symbol duration can remove the cyclostationary properties [26] of transmitted signal in chaos-based symbolic dynamics modulation systems [27]. The ideal of chaos-based variation of the symbol period in spread-spectrum communication systems has been presented in [28] and [29]. 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”. To the best of our knowledge, ours is the first work to investigate a chaotic DSSS technique with variable symbol period. The obtained results point out that the performance of the multiple-access system using the proposed technique gets worse when the variation range of symbol period is spanned. But in return, our technique can protect the system from the attacks of detecting symbol period at physical layer, even if the attacker fully knows the used chaotic sequence.

The remaining sections of this paper are organized as follows. In Section 2, the proposed technique is described by means of the analysis of discrete-time models for spreading scheme despreading scheme. The multiple access performance over the additional white Gaussian noise (AWGN) channel is calculated in Section 3 with the use of the theoretical derivation and numerical integration. The results obtained by PC simulations are shown in comparison with the calculated ones in Section 4. Section 5 presents a numerical investigation on the possibility of the proposed technique in resisting the attack of symbol period detection. Finally, our conclusion with noticeable points is given in Section 6.

2. Proposed chaotic DSSS technique

2.1. Spreading scheme with variable bit period

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 lth 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 $(\beta_m + 1)$ value intervals, i.e., $[x_{min} + j\gamma, x_{min} + (j+1)\gamma]$, with j varying from 0 to β_m and γ being a constant defined by

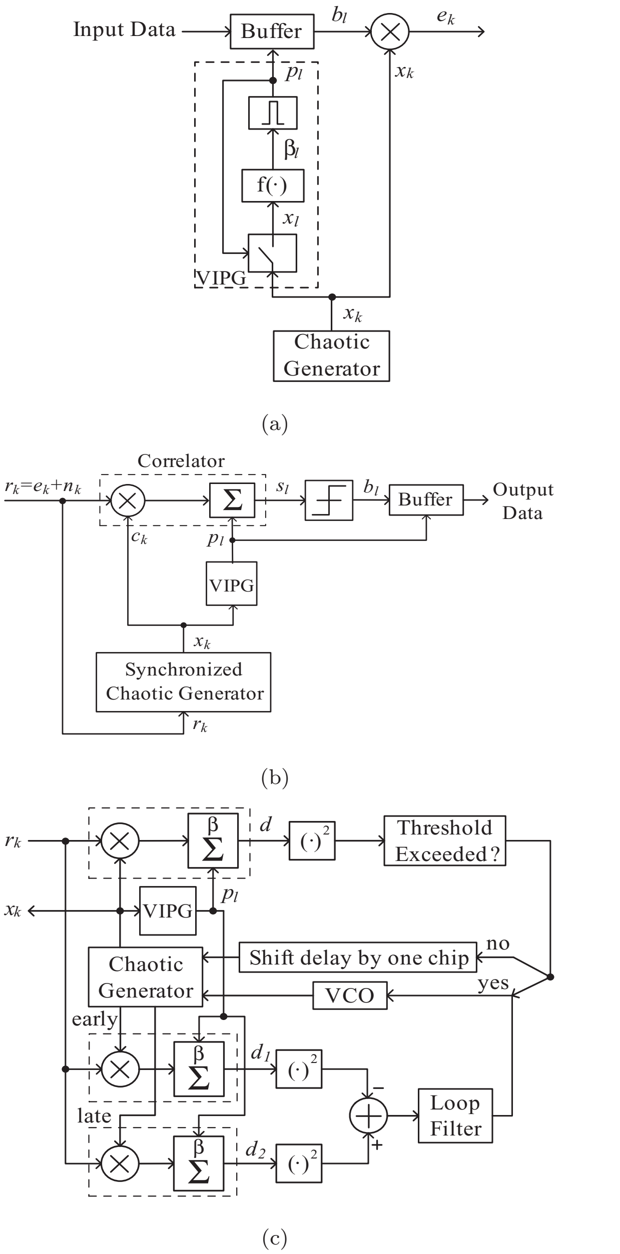

Fig. 1. Block diagrams of (a) Spreading scheme, (b) Despreding scheme, and (c) Synchronization scheme.

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

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 the chip period of the chaotic sequence $\{x_k\}$ and β is a fixed integer whose value is predetermined. We can see from