Enhancing Physical Layer Security of Cognitive Radio Transceiver via Chaotic OFDM

Ali Al-Talabani[1], A. Nallanathan[1], and Huan X. Nguyen[2]
[1]Centre for Telecommunications, Department of Informatics, King's College London, London, WC2R 2LS, UK.
Email: ali.al-talabani@kcl.ac.uk, nallanathan@ieee.org
[2]School of Science and Technology, Middlesex University, The Burroughs, London NW4 4BT, UK.
Email: h.nguyen@mdx.ac.uk

***Abstract*—Due to the enormous potential of improving the spectral utilization by using Cognitive Radio (CR), designing adaptive access system and addressing its physical layer security are the most important and challenging issues in CR networks. Since CR transceivers need to transmit over multiple non-contiguous frequency holes, multi-carrier based system is one of the best candidates for CR's physical layer design. In this paper, we propose a combined chaotic scrambling (CS) and chaotic shift keying (CSK) scheme in Orthogonal Frequency Division Multiplexing (OFDM) based CR to enhance its physical layer security. By employing chaos based third order Chebyshev map which allows optimum bit error rate (BER) performance of CSK modulation, the proposed combined scheme outperforms the traditional OFDM system in overlay scenario with Rayleigh fading channel. Importantly, with two layers of encryption based on chaotic scrambling and CSK modulation, large key size can be generated to resist any brute-force attack, leading to a significantly improved level of security.**

I. Introduction

The radio frequency spectrum is becoming scarce due to the low utilization of the conventional fixed spectrum allocation schemes. According to Federal Communications Commission (FCC), temporal and geographical variations in the utilization of the assigned spectrum range from 15% to 85% [1]. The limited available spectrum and the inefficiency in the spectrum usage necessitate a new communication paradigm as the next generation communication networks to exploit the existing wireless spectrum opportunistically. Opportunistic usage of licensed frequency bands has been proposed as a solution of high demand and scarcity of spectrum resources, by using Cognitive Radio (CR) systems [2]. As an intelligent wireless communication system, CR is aware of the radio frequency environment and often selects the communication parameters such as carrier frequency, bandwidth and transmission power to optimize the spectrum usage, and adapts its transmission and reception accordingly. Developing advanced transceivers for the cognitive physical layer is one of the key objectives in the successful development of CR systems. Spectrum pooling is an opportunistic spectrum access approach that enables public access to the already licensed frequency bands [3], [4]. The basic idea is to merge spectral ranges from different spectrum owners (for example, military radios) into a common pool, from which the secondary users may temporarily rent spectral resources during idle periods of licensed users. In effect, the licensed system does not need to be changed while the secondary users access the unused resources. Among the many possible technologies for unlicensed users transmission in spectrum-pooling radio systems, orthogonal frequency-division multiplexing (OFDM) has already been widely recognized as a highly promising candidate mainly due to its great flexibility in dynamically allocating the unused spectrum among secondary users, as well as its ability to monitor the spectral activities of licensed users at no extra cost [5]. Furthermore, the issue of downlink channel assignment and power control for frequency-division multiple-access-based cognitive networks has been addressed in [6], wherein a set of base stations (BSs) makes opportunistic spectrum access in order to serve the fixed-location wireless users within their cells. To maximize the total number of active users that can be supported while guaranteeing the minimum signal-to-interference-plus-noise ratio (SINR) requirements of secondary users, as well as protecting the primary users, suboptimal schemes are suggested for the formulated mixed integer program. Considering networks with the coexistence of multiple primary and secondary links through an orthogonal frequency-division multiple-access (OFDMA)-based air interface, [7] utilizes the dual framework from [8] to provide centralized and distributed algorithms that improve the total achievable sum rate of secondary networks subject to interference constraints specified at the primary users' receivers. The chaotic signals have been shown to be well suited for spread-spectrum modulation because of their inherent wide band characteristic [9], mitigation of fading channels, jamming resistance and low probability of intercept (LPI) [10]. Furthermore, non-coherent systems are better suited than coherent ones for time and frequency selective channels [11]. Also, chaos based cryptography has attracted significant attention from researchers due to their simplicity of implementation, complex behavior and extreme sensitivity to initial conditions. The scrambling matrix has been considered in [12] which based on a key derived from a one dimensional chaotic nonlinear dynamical system

using logistic map. In this paper, we propose a security mechanism for OFDM based CR network, which provides two layers of security. In the first layer, the constellation symbols are dynamically scrambled using a scrambling matrix that is generated based on the mixing property of the chaotic dynamical systems (chaos based logistic map). The second layer uses the third order Chebyshev map to carry out chaotic shift keying (CSK) modulation that allows spreading of each frame of the scrambled data with specific initial condition. The proposed method provides extreme sensitivity of the initial conditions in generating the chaotic sequence, hence a slight difference in initial condition of the chaotic sequences between transmitter and receiver results in almost a completely different position matrix, leading to failure in decrypt the data signal. This guarantees security of the system. We select Chebyshev map to generate chaotic reference sequence which is used in CSK because this map satisfies the necessary conditions for optimum bit error rate (BER) in chaotic OFDM (COFDM). The proposed scheme not only show an enhanced level of security (with two layers of scrambling and modulation) but also provide a significant improvement in overall BER performance.

II. System Model and Proposed CR Architecture

The proposed architecture of CR network with two primary users, two secondary (unlicensed) users, a primary (licensed) base-station and a secondary (unlicensed) base-station is presented in Fig. 1. The primary users have a license to operate in a certain spectrum band while the primary base-station is a fixed infrastructure network component which has a spectrum license such as base-station transceiver system (BTS) in a cellular system. The secondary base-station is a fixed infrastructure that can provide single hop connection to secondary users without spectrum access license.

A. Transmitter

The OFDM-CSK system benefits from the non-coherent advantages of differential chaotic shift keying (DCSK) and the spectral efficiency of multi-carrier modulation. Here, we consider OFDM-CSK system using discrete chaotic sequence for modulation. For mathematical simplification, we describe mathematical model for one user only. As shown in Fig. 2, for each user, a reference chaotic code is generated and used as a reference and spreading code. The input information sequence is first converted into U parallel data sequences with each bit being of equal probability of +1 and -1.

Let $\mathbf{S}$ of size $U \times U$ denote the scrambling matrix. This scrambling matrix is generated based on the chaotic sequence $\mathbf{x}_c$ generated from the chaotic signal generator. We also denote $\mathbf{s} = [s_1,\ s_2, \cdots, s_U]^T$ and $\mathbf{s}_e = [s_{e,1},\ s_{e,2}, \cdots, s_{e,U}]^T$ as the data vectors before and after

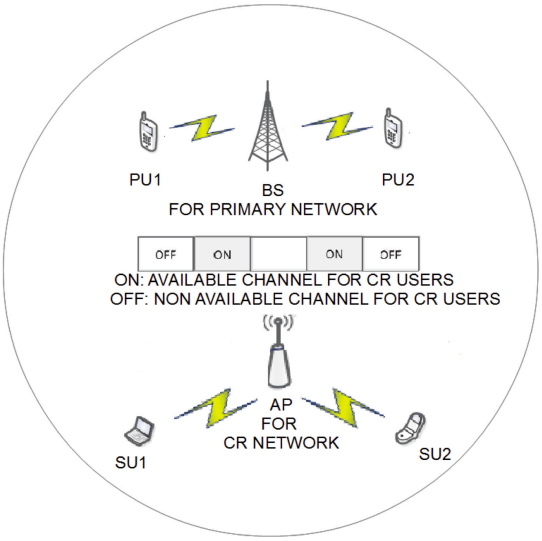

Fig. 1. Cognitive radio architecture.

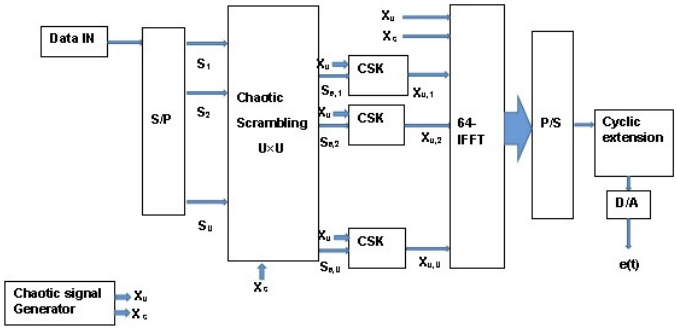

Fig. 2. Block diagram of MC-CSK(OFDM-CSK) transmitter

scrambling, respectively. We have

$$\mathbf{s}_e = \mathbf{s} \times \mathbf{S}. \tag{1}$$

Then, the u^{th} sub stream is spread due to multiplication in time (we now add time index t to the equations) with the chaotic spreading code $\mathbf{x}_u = [x_{u,1},\ x_{u,2}, \cdots, x_{u,\beta}]$ (generated by the same chaotic signal generator)

$$x_u(t) = \sum_{k=1}^{\beta} x_{u,k} h(t - kT_c), \tag{2}$$

where $h(t)$ is the square-root-raised-cosine filter and T_c is the chip duration. This filter is band-limited and is normalized to have unit energy. Let $H(f) = F(h(t))$, where F denotes the Fourier transform. It is assumed that $H(f)$ is limited to $[-B_c/2,\ B_c/2]$ which satisfies the Nyquist criterion with a roll off factor α $(0 < \alpha < 1)$. Here, $B_c = (1+\alpha)/T_c$. Note that the first two subcarriers are used to modulate the reference signals $x_u(t)$ and $x_c(t)$. The remaining subcarriers are used to carry data. Therefore, the

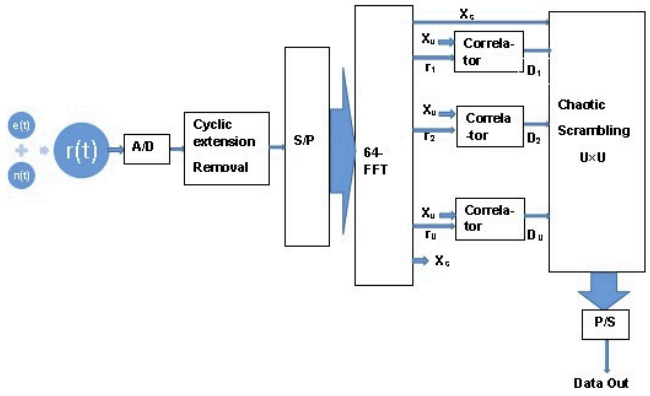

Fig. 3. Block diagram of OFDM-CSK receiver

transmitted signal of the single-user OFDM-CSK is given by

$$e(t) = x_u(t)\cos(2\pi f_1 t + \varphi_1) + x_c(t)\cos(2\pi f_2 t + \varphi_2) + \sum_{i=1}^{U} s_{e,i}(t)x_u(t)cos(2\pi f_{i+2}t + \varphi_{i+2}), \quad (3)$$

where φ_i represents the phase angle introduced in the carrier modulation process of the ith subcarrier. In this paper, we normalize the transmitted energy in every subcarrier.

B. Receiver

The block diagram of the OFDM-CSK receiver is illustrated in Fig. 3. We consider a set of correlators, each demodulating the desired signal of the corresponding carrier frequencyf_i. The signals are then sampled every kT_c seconds. Assuming that perfect symbol and carrier synchronization of OFDM are realized at the receiver, we assume that our channel is Additive White Gaussian Noise (AWGN). In addition, we assume that there is no interference between subcarriers. In this case, we evaluate the received signal for one user [13], [14], which is

$$r(t) = e(t) + n(t), \quad (4)$$

where $n(t)$ is an AWGN noise with zero mean and power spectral density of $N_0/2$. After doing FFT on the received signal, the output at subcarrier i is given by

$$r_i = y_i + v_i, \quad (5)$$

where $y_i = s_i x_i$ and v_i is the additive Gaussian noise. The output of each matched filter is given by

$$U_i = \sum_{k=1}^{\beta} r_{i,k}x_k = s_i \sum_{k=1}^{\beta} x_k^2 + V_i \quad (6)$$

where $i = 1, 2, 3, \ldots, U$ and

$$Vi = \sum_{k=1}^{\beta}[x_k v_{k,i} + s_{-i}x_{-k}x_k] \quad (7)$$

where $s_{-i}x_{-k}$ represents interference from other secondary users. We use an equal gain combining as an equalizer in the receiver side with equalization coefficients as follows

$$E_\varphi = \frac{(H_\varphi)^\bigstar}{|H_\varphi|} \quad (8)$$

where H_φ is transfer function of channel, ($\bigstar$) represents conjunction relation and $|H_\varphi|$ is the amplitude of transfer function. This equalization method corrects the phase shift due to channel. We can recover the information bit a_i of ith correlation detector from (9) after equalization, as

$$a_i = sign(U_i). \quad (9)$$

Then apply descrambling process with same initial condition of transmitter on a_i to detect the transmitted bits.

C. Design of Chaotic Scrambling and CSK Modulation

Enhancing the physical layer security is the important goal of our proposed system. As shown later in Eq. (17), chaotic map parameter and initial condition of chaotic sequence have reasonable impact on the overall BER. Therefore, we propose two layers of encryption by combining chaotic modulation and scrambling to improve diffusion property of the encrypted data. The scrambling matrix represents the first layer of encryption and is generated by the following algorithm: A new position matrix $\mathbf{P}$ of the same size $U \times U$ as in (1) is generated, where position elements signify the location of 1 in the scrambling matrix $\mathbf{S}$. The design methodology of position matrix is based on the so-called mixing property of the chaotic dynamical systems. The mixing property is defined in the following way [15]: For any two open intervals I and J (which can be arbitrarily small, but must have a nonzero length) one can find initial values in I which, when iterated, will eventually lead to points in J. Each sub-domain chaotic map is sequentially numbered from 0 to $U-1$.

The scrambling matrix design is in such a way that each row has one '1' and rest of the elements are zero and no two rows are the same. For each scrambling matrix, a new key is used, where each key entails mapping to a unique combination. The matrix when multiplied with constellation symbols scrambles the position of the elements. It is difficult to recover the data with different key. Due to the characteristic of CR like wireless LAN, attackers can store and sniff all the traffic of CR. Therefore, the chaotic scrambling will be useful to provide each frame encrypted with specific initial condition. Let the scrambled version of the first frame F_1 with length U be denoted by $S_1 = CS(F_1, ch(IC_1))$, where CS is chaotic scrambling process as described above, $ch1$ is the logistic chaotic function and IC_1 is initial condition of chaotic map for the first frame. In general, for the nth frame:

$$S_n = CS(F_n, ch1(IC_n)), \quad (10)$$

$$ch1(t+1) = r \times ch1(t)(1 - ch1(t)), \quad (11)$$

where $3.75 \leq r \leq 4$, and $ch1(t+1)$ is the current state of the chaotic map while $ch1(t)$ is its previous state. Note that $ch1(t)$ has a value between [0, 1].

The second layer of encryption is represented by CSK modulation which provides random sequences of samples that modulate and spread each frame of output scrambled data $s_{e,u}$ with specific initial condition according to the following formula

$$x_u = CSK(s_{e,u}, ch2(IC_u)), \tag{12}$$

where CSK is the chaotic shift keying modulating function, $ch2(\cdot)$ is selected as the third order Chebyshev map because this map satisfies the necessary conditions of optimum BER, which is shown later in the next section. In our proposed system, the characteristic of the third order Chebyshev map is written as follows

$$g_3(cos\phi) = 4(cos\phi)^3 - 3cos\phi, \tag{13}$$

$$ch2(t+1) = 4ch2^3(t) - 3ch2(t), \tag{14}$$

where the current state of chaotic signal is $ch2(t+1) = g_3(\cos\phi)$ and the previous state of chaotic map is $ch2(t) = cos\phi$. Note that $c_1 = 4$ and $c_2 = 3$ are the chaotic map parameters. $ch2(t)$ has values between [-1, 1]. Thus, the eavesdropper needs to have the same initial condition and chaotic map parameters to be able to decrypt data.

III. Analysis of BER Performance

In this section we derive analytical expressions for BER of OFDM-based CSK scheme. We will present the analysis for the discrete-time case. By applying Gaussian approximation and the central limit theorem, we get approximate analytical expressions of the BER for sufficiently large spreading factor. It can be seen that all sum items in Eq. (6) can be regarded as zero-mean Gaussian random variable. So decision parameter of y_i in Eq. (6) can be obtained as

$$y_i = D_i \sum_{k=1}^{\beta} x_k^2 + \sum_{j=1, j\neq i}^{N} D_j \sum_{k=1}^{\beta} x_k x_{k,j} + \sum_{k=1}^{\beta} x_k v_i \tag{15}$$

where D_j and $x_{k,j}$ are the transmitted data and spreading sequence respectively of other secondary users. N is the number of secondary users. From an independence feature between chaotic sequences, both $cov[x_k^2, x_{k,j}^2]$ and $E[x_k, x_{k,j}]$ need to be equal to zero. According to this assumption, the variance of y_i is equal to

$$var[U_i] = \beta(var\left[x^2\right] + E[x_k^2] \sum_{j=1, j\neq i}^{N} E[x_{k,j}^2] + E[x_k^2] N_0/2) \tag{16}$$

where $E[.]$ represents the expectation operator, $N_0/2$ is the power spectral density of Gaussian noise, and $var[.]$ denotes the variance operator. Each correlation detection output U_i could be regarded as independent Gaussian variable for large β. Thus, the overall optimum BER can be achieved as [16], [17]

$$BER(i) = \frac{1}{2} erfc((\frac{2\nu}{\beta} + \frac{2(N-1)}{\beta} + (\frac{E_b}{N_o})^{-1})^{-1/2}) \tag{17}$$

where E_b/N_0 is the SNR per bit, $\nu = var[x_k^2]/P_s^2$, $P_s = E[x_k^2]$ and ν needs to be same for all users. However, the above BER performance is achieved only if the chaotic map satisfies the following conditions:

c1) Different users have chaotic sequences with very low cross correlations even for a finite length, i.e., $cov[x_k^2, x_m^2] = 0$ where x_k and x_m are different chaotic sequences.
c2) The bit energy is kept constant for each user.
c3) $E[x_k, x_m] = 0$

In the following, we will show that the chaos based Chebychev map will satisfy these three conditions. In general, we can show that for the Chebyshev map of degree N is

$$g_N^k(\cos\varphi) = \cos(N^k\varphi) \tag{18}$$

Moreover, the invariant probability density function (pdf) of $\cos\varphi$ can be shown equal to:

$$\sigma(x) = \begin{cases} \frac{1}{\pi sin\varphi} & \text{if } 0 \leq x \leq \pi \\ 0 & \text{otherwise} \end{cases} \tag{19}$$

- *Proof of condition (c1) and (c2)*: We have

$$cov\left[x_k^2, x_m^2\right] = E[x_k^2, x_m^2] - E\left[x_k^2\right] E\left[x_m^2\right] \tag{20}$$

We consider the case where $k \neq m$. Without loss of generality, we assume $k = n + m$ for some positive integer. Then

$$E[x_k^2, x_m^2] = \int_{-\infty}^{\infty} x^2 \left(g_m^n(x)\right)^2 \rho(x) dx = \int_{-1}^{1} x^2 \left(g_m^n(x)\right)^2 \frac{1}{\sqrt{1-x^2}} dx \tag{21}$$

Using (18) and $x = \cos\varphi$, Eq. (21) can be written as follows

$$E[x_k^2, x_m^2] = \frac{1}{\pi} \int_0^{\pi} cos^2(\varphi) \left(g_m^n(cos\varphi)\right)^2 d\varphi = \frac{1}{4}. \tag{22}$$

Also, we can derive $E\left[x_k^2\right]$ as

$$E\left[x_k^2\right] = \int_{-\infty}^{\infty} x^2 \rho(x) dx = \int_{-1}^{1} x^2 \frac{1}{\pi\sqrt{1-x^2}} dx = \frac{1}{2} \tag{23}$$

Combining Eq. (20), (22) and (23), we obtain $cov\left[x_k^2, x_m^2\right] = 0$.

- *Proof of condition (c3)*: With $k \neq m$ and some positive integer n, and replacing $x = \cos\varphi$, then we achieve the cross correlation $E[x_k x_m]$ as

$$E[x_k x_m] = \int_{-\infty}^{\infty} x \left(g_m^n(x)\right) \rho(x) dx = \frac{1}{\pi} \int_0^{\pi} \cos\varphi \left(g_m^n(\cos\varphi)\right) d\varphi = 0.$$

IV. Simulation Results and Discussion

The CR based chaotic OFDM-CSK system uses a Chebyshev map to generate chaotic sequence. The system is applied in spectrum overlay, or opportunistic spectrum access (OSA), where secondary users aim to exploit frequency bands that are not used by primary users in a particular geographical area. In this scheme, there is no restriction on power limits of secondary users because no interference to primary users.

In our system simulation, we consider the following parameters: 2 secondary users, 2 primary users, data rate: 10kbps, symbol period T_b = 100μsec, spreading factor (β): 12, 25, and 50, FFT length: 64, data subcarriers: 52, Rayleigh fading channel with AWGN. Number of taps for Rayleigh fading channel in the comparison between traditional OFDM and chaotic OFDM is 10 in overlay spectrum access.

Figure 4 indicates BER performance of CR based MC-CSK for different lengths of spreading codes in overlay scenario. We can see from this figure that BER is improved by using longer spreading code according to (17). Fig. 5 represents BER of both the proposed system and the CR based OFDM system with BPSK and QPSK modulations for single user transmission in overlay spectrum access. Figure 5 indicates that the proposed system outperforms the traditional OFDM based CR system.

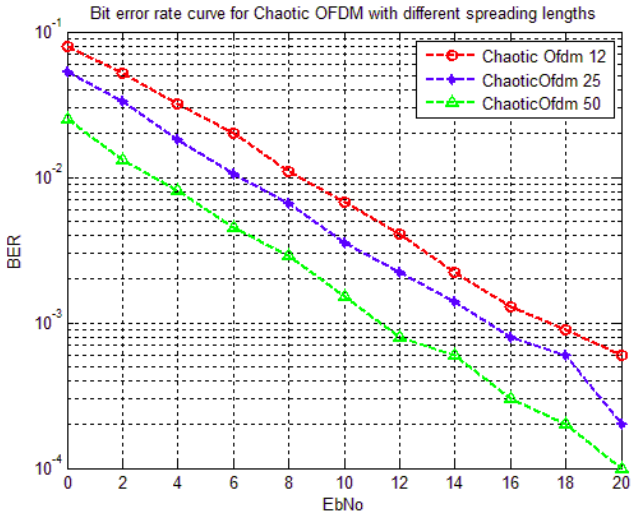

Fig. 4. BER performance of the proposed system for different lengths of spreading code in CR based overlay spectrum access.

Regarding to scrambling and CSK process, when the same data is recovered with slightly different initial condition of chaos generator between transmitter and receiver, almost all the constellation symbols are in error. The probability of error is uniformly distributed in symbols. The effect of chaotic scrambling/modulation is tested into two scenarios as detailed below:

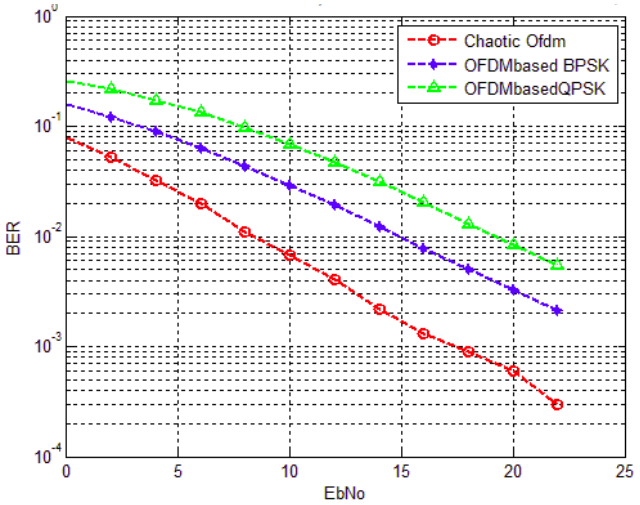

Fig. 5. BER performance comparison: The proposed system with spreading length($\beta = 12$) versus OFDM-PSK in CR based overlay spectrum access.

i) Scenario 1: We applied proposed chaotic scrambling in OFDM with QPSK. It is assumed that initial condition value of chaotic map in legal receiver is 0.095 while the eavesdropper with illegal receiver has an initial condition value of same chaotic map of 0.095000001. The simulation results of BER are shown in Fig. 6. It confirms that with the slightly different initial conditions of around 10^{-9} between the legal and illegal receivers, the illegal receiver yields a much higher BER in the case of using the proposed chaotic scrambling than the case of using the time domain scrambling implemented in [18]. Therefore, this result confirms the enhancement in low data interception feature because the proposed system encrypts each frame with specific initial condition of chaotic scrambling. Also, it is difficult for passive attacker to sniff encrypted frames with different chaotic initial conditions.

ii) Scenario 2: We investigated the effect of slight error in parameter of chaotic map that generates chaotic signal for CSK on BER performance of the illegal COFDM based receiver (no error in scrambling process). Fig. 7 shows that the illegal receiver still has very high BER compared to that of the legal COFDM receiver.

From the above scenarios, the chaotic scrambling and CSK modulation are useful to generate large key space to resist brute-force attack and provide low interception feature.

V. Conclusion

In this paper, OFDM-CSK based CR system with chaotic scrambling is proposed. OFDM-CSK is a non-coherent system which does not require reproduction of the chaotic signal in the receiver in comparison with the traditional CSK. A security mechanism is proposed to provide two layers of security. In the first layer, the constellation symbols are dynamically scrambled using a scrambling matrix that

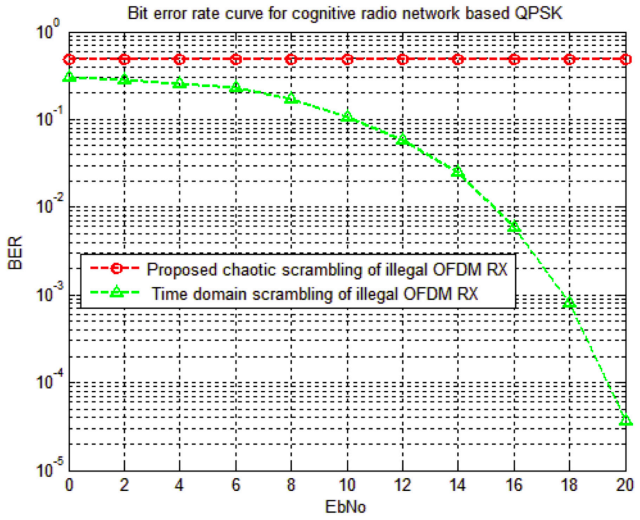

Fig. 6. Effect of slight error of initial condition for chaotic scrambling on BER of the illegal reciever.

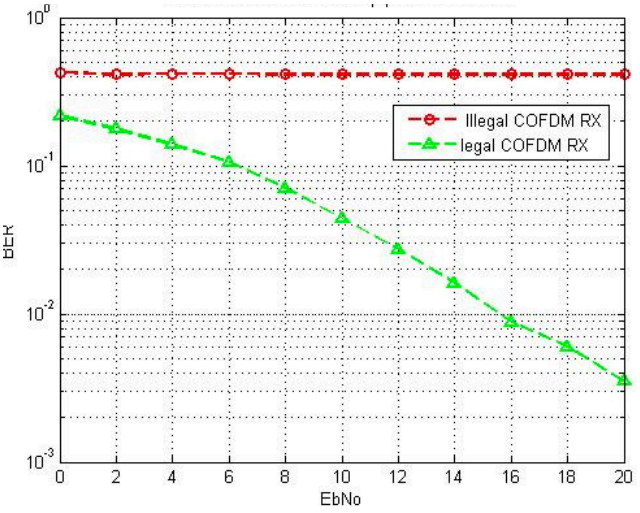

Fig. 7. Effect of slight error in parameters of chaotic modulation on performance of the illegal receiver.

is generated based on the chaos logistic map. In the second layer, the Chebyshev map based CSK allows spreading of each frame of the scrambled data with specific initial condition and mapping parameters. Simulation results indicate that two security layers provide low interception property and that it is difficult for passive attackers to process different frames with different initial conditions or different values of chaotic map parameters. This feature provides the large key space for chaotic scrambling and chaotic modulation to resist malicious attacks. Furthermore, the proposed system is applied in overlay scenarios of CR, where simulation results show that the proposed system outperform the traditional OFDM based CR in terms of BER performance.

REFERENCES

[1] FCC, ET Docket No 03-222, "Notice of proposed rule making and order," Dec. 2003.

[2] S. Hakin, "Cognitive radio: Brain-empowered wireless communications", *IEEE J. Select Areas in Commun.*, vol.23, no.2, pp. 201-220, Feb 2005.

[3] T. Weiss and F. Jondral, "Spectrum pooling: An innovative strategy for the enhancement of spectrum efficiency," *IEEE Commun. Mag.*, vol. 42, no. 3, pp. 8-14, Mar. 2004.

[4] U. Berthold, F. Jondral, S. Brandes, and M. Schnell, "OFDM-based overlay systems: A promising approach for enhancing spectral efficiency [Topics in radio communications]," *IEEE Commun. Mag.*, vol. 45, no. 12, pp. 52-58, Dec. 2007.

[5] S. Chuprun, J. Kleider, and C. Bergstrom, "Emerging software defined radio architectures supporting wireless high data rate OFDM," in *Proc. IEEE RAWCON*, 1999, pp. 117-120.

[6] A. T. Hoang and Y.-C. Liang, "Downlink channel assignment and power control for cognitive networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 8, pp. 3106-3117, Aug. 2008.

[7] P. Cheng, Z. Zhang, H.-H. Chen, and P. Qiu, "Optimal distributed joint frequency, rate and power allocation in cognitive OFDMA systems," *IET Commun.*, vol. 2, no. 6, pp. 815-826, Jul. 2008.

[8] W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1310-1322, Jul. 2006.

[9] F. C. M. Lau and C. K. Tse, *Chaos-based digital communication systems*, Springer-Verlag, 2003.

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

[11] B. Le Saux, M. Helard, and P.-J. Bouvet, "Comparison of coherent and non-coherent space time schemes for frequency selective fast-varying channels," in *Proc. 2nd Int. Symp. on Wireless Communication Systems*, Sep. 2005, pp. 32-36.

[12] M. A. Khan, M. Asim, V. Jeoti, and R. S. Manzoor, "On secure OFDM system: Chaos based constellation scrambling," in *Proc. Int. Conf. on Intelligent and Advanced Systems*, 2007.

[13] G. Kaddoum, F. Gagnon, and F.-D. Richardson, "Design of a secure Multi-Carrier DCSK system," in *Proc. the Ninth Int. Symp. on Wireless Communication Systems*, Jun. 2012.

[14] G. Kaddoum, M. Vu, and F. Gagnon, "Performance analysis of differential chaotic shift keying communications in mimo systems," in *Proc. IEEE Int. Symp. on Circuits and Systems (ISCAS)*, 2011, pp. 1580-1583.

[15] H.-O. Peitgen, H. Jrgens, and D. Saupe, *Chaos and fractals-new frontiers of science*, 2nd Edition, Springer-Verlag, 2004.

[16] Wai M. Tam, F. C. M. Lau, C. K. Tse, and A. J. Lawrance, "Exact analytical bit error rates for multiple access chaos-based communication systems," *IEEE Trans. Circuits and Systems*, vol. 51, no. 9, Sep. 2004.

[17] A. J. Lawrance and G. Ohama "Exact calculation of bit error rates in communication systems with Chaotic modulation," *IEEE Trans. on Circuits and Systems*, vol. 50, no. 11, Nov. 2003.

[18] H. Li, X. Wang, and W. Hou, "Secure transmission in OFDM systems by using time domain scrambling," in *Proc. 13th Canadian Workshop on Information Theory (CWIT)*, 2013.