A Secure OFDM Transmission Scheme Based on Chaos Mapping

Xiaozhong Zhang, Ying Wang*, Juan Zeng, Yongming Wang
Institute of Information Engineering, Chinese Academy of Sciences, Beijing, 100093, China

***Abstract*—With the wide application of OFDM technology, the security of OFDM system is becoming more and more important. In this paper, we propose a secrecy transmission scheme with phase rotation and sub-carrier mapping based on chaos sequences. The scheme employs the characteristics of pseudo-random and sensitivity to initial conditions of chaos sequences. We have studied on the observed signal features, computational complexity and possible key number, as well as error-correcting performance of proposed scheme. It's shown by simulation results and analysis that the scheme is able to effectively encrypt the information and enhance the randomness of output signals. The malicious receiver cannot estimate the message through the statistic characteristics of received signals, which ensure the aim of secure communication.**

Keywords—Secure communication; Chaos mapping; OFDM; Computational complexity; Anti-eavesdropping

I. INTRODUCTION

In the late 1940s, C. E. Shannon published a foundational paper of cryptography named communication theory of secrecy systems [1-2], in which he proposed a method applying the basic features of chaos theory into cryptography, the features included the sensitivity to initial conditions and initial parameters, and he pointed out two basic principles of cipher design: diffusion and chaos.

Traditional cryptographic algorithm depends on the key transmission and extraction, whereas chaos mapping depends on the initial parameters. The former technique implements diffusion and chaos by increasing the run number of encryption, whereas chaos theory uses inner iteration to spread the initial value into the whole phase space.

The core of encryption based on cryptography is to increase the calculated amount, whose disadvantage is that it works mainly at high layers like network layer and application layer, and the underlying foundation of secure communication is unreliable, which would lead to exposure to DOS-style attacks easily.

There are several applications of the chaos theory in digital cryptosystem, such as stream cipher based on generator of chaos pseudo-random sequence, block cipher based on forward or reverse chaos iteration, and the S-box design of hash function [3]. Some scholars have cracked certain block cipher schemes by chosen-cipher text attack and known-plaintext attack.

Chaos sequence is a typical pseudo random and non-periodic sequence created by nonlinear systems. Once the initial condition is given, the output chaos sequence is determined. The generation procedure of chaos sequence is non-convergent but bounded. It's hypersensitive to initial conditions. Hence chaos sequence is definite but still unpredictable [4]. With these excellent cryptography features, chaos sequence has been adopted in many fields like cipher design, image encryption and secure communication [5-6].

OFDM has high spectral efficiency and favorable bandwidth scalability. Besides, it is robust to multipath fading and it's easy to implement and integrate with MIMO. Since 1990s, OFDM has been introduced by many broadband wireless communication system standards such as DVB, DAB, WLAN, UWB and LTE [7]. Meanwhile, the security of OFDM system is worthy of attention.

The reliability and security of OFDM system can be effectively improved by utilizing the chaos theory. In [8], M. A. Khan proposed chaos based symbol scrambling in OFDM system, where the scrambling acted as random interleaver.

A novel multi-domain jointed dimension-transformed chaotic permutation for physical layer security is proposed in [9] and [10]. The data on both frequency and time domain is permuted through Logistic mapped permutation matrix, which is consisting of mask matrix and permutation vectors for frequency and time domain. The scheme was proved to be effective in resisting hostile attack applied in OFDM passive optical network system and optical coherent OFDM system, respectively.

In [11], a novel chaos modulation scheme based on the symbolic sequence associated to the chaos mapping and backward iteration was proposed, in which the chaos mapping considered has a parameter that allows people to trade security for BER performance. The disadvantage of the scheme is that the improvement of security is at the expense of decreasing the performance.

In this paper, combining the attractive features of chaos sequence and OFDM transmission, we propose a secrecy transmission scheme with phase rotation and sub-carrier mapping based on chaos sequences. Both the system performance and complexity are considered.

At the baseband processing of transmitter, we randomly change the phases of constellation mapping, and randomly select the subcarrier index to carry the data symbols, where the initial conditions of chaos sequence works as keys. In the receiver, legitimate users would demodulate the info with keys from the inverse procedure. The scheme is proved to work efficiently against jammers and eavesdroppers.

Ying Wang*:the corresponding author.E-mail:wangying@iie.ac.cn
The research was supported by National Natural Science Foundation of China with Grant 61501459.

978-1-4673-8590-9/15/$31.00 ©2015 IEEE

The remainder of the paper is organized as follows. The principle of logistic chaos mapping is depicted in the section II. Section III presents the structure of system model of chaos based secrecy OFDM transmission and the implementation of the secure scheme proposed. In section IV, some interesting results are shown to illustrate the security level and system performance. In Section V, some conclusions and main work are summarized.

II. Basic Principles of Logistic Chaos Mapping

Logistic chaos mapping is widely studied, as it has relatively simple expression and favorable characteristic of pseudorandom. It is defined as

$$X_{n+1} = \mu \times X_n \times (1 - X_n), \quad n = 1,2,3 \ldots \ldots \tag{1}$$

Where $0<X_n<1$, $1 \le \mu \le 4$, μ is the fractal parameter. System works in the chaos state when $3.56994... \le \mu \le 4$. X_n is randomly distributed, which is non-periodic and non-convergent. The closer to 4 μ is, the better the random feature the chaos system will have. Nevertheless, logistic chaos mapping will surely converge to a fixed value after several iterations, that is, the system cannot work in chaos state if μ falls outside the range [3.56994…, 4].

To verify the randomness of logistic chaos mapping, we firstly transform the chaos sequence X_n into binary sequence A_n, here $A_n \in \{0,1\}$. The conversion formula expresses as

$$A_n = \begin{cases} 0, & 0 \le X_n \le 0.5 \\ 1, & 0.5 \le X \le 1_n \end{cases}, \quad n = 1,2 \ldots \tag{2}$$

Assumed that the length of X_n is N, thus the length of A_n is N. J and K denote the number of 0 and 1 of A_n respectively. Hence the balance degree of binary sequences is defined as [12]

$$\mathrm{E(N)} = \frac{|J - K|}{N} \tag{3}$$

Fig. 1 shows the test result of balance degree of logistic chaos mapping, where μ=4, N=10000. As shown in Fig.1, whatever the value of X_0 is, the results of balance degree always close to 0, which illustrates that the randomness of logistic chaos mapping is good, and the number of 0 and 1 element is almost the same.

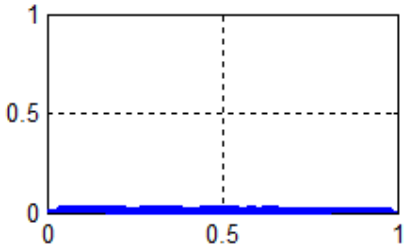

Fig. 1. Balance degree for chaos mapping

Another chaos mapping called segmented logistic chaos mapping is proposed in [13], the definition is depicted as

$$Y_{n+1} = \begin{cases} 4 \times \mu \times Y_n \times (0.5 - Y_n), 0 \le Y_n < 0.5 \\ 1 - 4 \times \mu \times (1 - Y_n) \times (Y_n - 0.5), 0.5 \le Y_n \le 1 \end{cases} \tag{4}$$

Where $3.56994... \le \mu \le 4$, $0<Y_n<1$. Experiment result s show that segmented logistic chaos mapping has the similar characteristics to logistic chaos mapping. Compared with logistic chaos mapping, segmented logistic chaos mapping shows unstable motion trajectory and fast adjacent track separation.

The focus of this article is not on the design of chaos sequence. Hence we take logistic chaos mapping and segmented logistic chaos mapping as example, which are used to produce phase rotation factor and sub-carrier mapping factor respectively. It's important to note that the proposed scheme is not limited to these two kinds of chaos mapping.

III. System Model of Chaos Based Secrecy OFDM Transmission

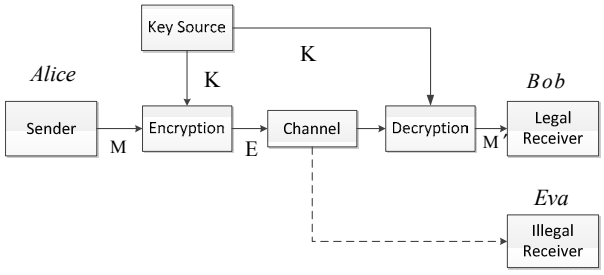

Fig. 2. Simplified model for secrecy transmission system

Fig. 2 shows the simplified secrecy communication system. As what we can see, the information sequence, called M, is encrypted in the sending end through certain encryption method. The cipher key is K. E denotes the cipher text. The legitimate receiver recovers the information M' with the inverse process of encryption. Due to the openness of wireless transmission, there are illegal receivers who can eavesdrop or actively interfere the regular communication of legal receiver.

The system model of chaos based secrecy OFDM transmission is shown in Fig. 3. There are two main modules which is different with traditional OFDM system, that is phase chaos rotation module and sub-carrier chaos mapping module, which respectively correspond to key K_1 and K_2. The received signals after wireless channel are recovered with key K_1 and K_2. The following discussion adopts QPSK as default digital modulation. Key transmission and distribution is not our focus, and we suppose the keys are known only by Alice and Bob.

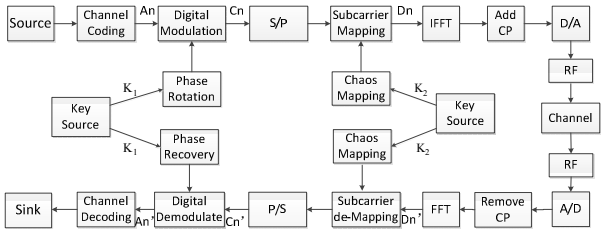

Fig. 3. Schematic diagram for chaos based secrecy OFDM transmission system

In Fig. 3, A_n is the output code word after channel coding, the length of which is N. B_n is used to denote complex signal produced by A_n through digital modulation, which has four states: {-1-i, -1+i, 1-i, 1+i}. Phase rotation factor is created by logistic chaos mapping. First chaos mapping produces chaos sequence with the length of m×N. Then the binary signal is created by chaos sequence, every sequential m-bit binary of which form a number, so that a sequence W_n is constituted with the length of N, called phase rotation factor sequence. Here, $W_n \in [0, 2^m - 1]$. The relationship of state transition is formulated as

$$C_n = B_n \exp\left(j2\pi \frac{W_n}{2^m}\right), \quad n = 1,2 \ldots \tag{5}$$

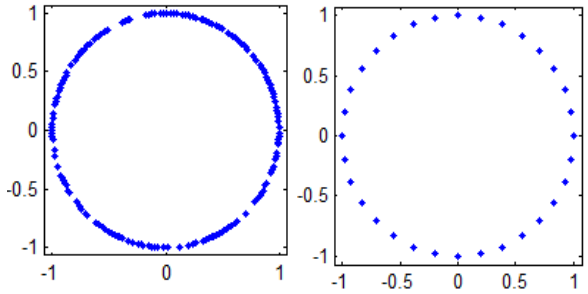

Fig. 4. Comparison of constellation for different modulation order

Fig. 4 shows the comparison of constellation between m=8 and m=5.With m increasing, the constellation after phase rotation converts gradually to a circle. It will surely converts to a hazily closed circle when m is large enough and the number of data is big enough. This would change the symbols' phase and lead to phase ambiguity. The eavesdropper can wiretap the message, but it's hard to demodulate the data from the constellation. The scheme of phase chaos rotation applies to PSK modulations and can be extended to QAM modulations.

The phase rotation is the first security measure, the following will discuss the second security measure, called sub-carrier chaos mapping. Before the sequence C_n is mapped to sub-carrier, the binary sequence created by chaos sequence is used to randomly disrupt the order of sub-carrier mapping. To increase the security level, the segmented logistic chaos mapping is adopted. It's initial condition and input parameter constitutes the key K_2.

Suppose the number of sub-carrier is N, the length of C_n is N. Every sequential $\log_2 N$-bit binary of binary sequence forms a number, so that a sequence V_n is constituted with the length N, called sub-carrier mapping factor sequence. Since chaos mapping has good ergodicity, V_n can traversal every value from 0 to N-1. D_n denotes the sequence that has been disrupted. D_n is decided by

$$\begin{cases} D_n = C_{\hat{n}} \\ V_{\hat{n}} = n - 1 \end{cases} \tag{6}$$

It is able to attain the goal of security transmission by transmitting the signals after mapping D_n to sub-carriers. The base band signal of OFDM is

$$x(t) = \sum_{i=-\frac{N}{2}}^{\frac{N}{2}} D_{i+\frac{N}{2}} \exp\left(j2\pi \frac{i}{T} t\right) \tag{7}$$

The demodulation process in the legitimate receiver is right the inverse process of modulation process in the sending end. System sends key K_1 and K_2 to the legitimate receiver which will recover the phase rotation factor sequence and sub-carrier mapping factor sequence and then decipher with the sequences.

To simplify the description, we suppose that the channel model is AWGN channel. The signals received by the legitimate receiver can be expressed by

$$r(t) = x(t) + n(t) \tag{8}$$

Where n(t) denotes additive white Gaussian noise. Utilizing the orthogonal property of sub-carriers, we can use one sub-carrier to demodulate the data on the sub-carrier with the same frequency. Take the k'th sub-carrier for example, here we don't consider the channel disturbance. The process can be described as:

$$\frac{1}{T}\int_{\tau}^{\tau+T} \exp\left(-j2\pi \frac{k}{T} t\right)\left[\sum_{i=-\frac{N}{2}}^{\frac{N}{2}-1} D_{i+\frac{N}{2}} \exp\left(j2\pi \frac{i}{T} t\right)\right] dt$$

$$= \sum_{i=-\frac{N}{2}}^{\frac{N}{2}-1} \frac{1}{T} D_{i+\frac{N}{2}} \int_0^T \exp\left(j2\pi \frac{i-k}{T} t\right) = D_{k+\frac{N}{2}} \tag{9}$$

The demodulation sequence, denoted by D'_n, can be obtained by demodulate the N sub-carriers respectively. If the channel model is multi-path fading channel, ISI will be brought in and the above method cannot recover the original signals. In order to alleviate and eliminate the influence of multi-path fading channel, equalization like zero-forcing and minimum mean squared error should be adopted.

According to the sub-carrier chaos mapping factor, the legitimate receiver should recover the original sub-carrier index. The procedure is denoted by

$$\begin{cases} C'_n = D'_{\hat{n}} \\ V_n = \hat{n} - 1 \end{cases}, \quad n = 1,2,3 \ldots \tag{10}$$

To eliminate the influence of phase chaos rotation, the key K_1 should be employed. It's described as

$$A'_n = C'_n \exp\left(-j2\pi \frac{W_n}{2^m}\right), \quad \nu = 1,2,3 \ldots \tag{11}$$

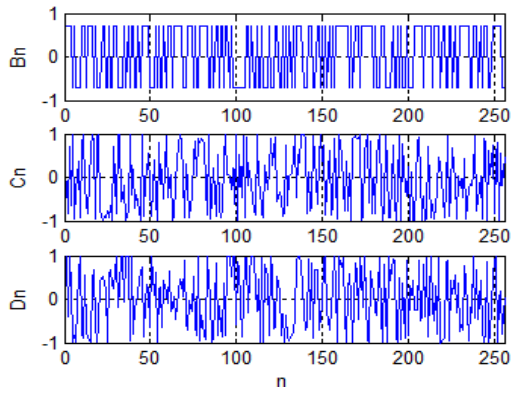

Fig. 5. Envelope of waveforms for different module

At last, the original signals can be recovered by the legitimate receiver normally.

Fig. 5 shows the envelopes of the real part of waveform of B_n, C_n and D_n. Here N=256. We can see that the envelopes of the waveform have good randomness after sub-carrier chaos mapping.

IV. Simulation Results

A. The observed signal features

The comparison of transmitted time domain signals with or without secure transmission scheme is depicted in Fig. 6. The difference between the two kinds of waveforms is random. The proposed scheme shows good random encryption feature.

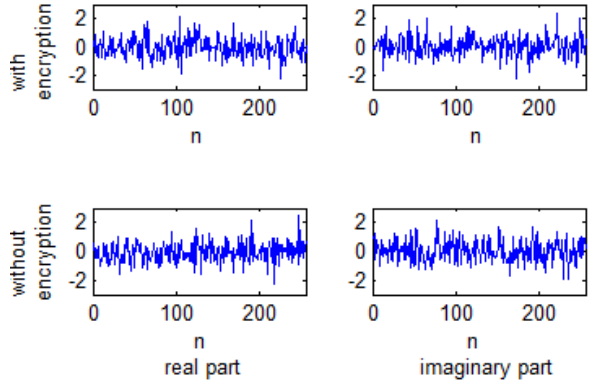

Fig. 6. Comparison of the time domain signals

In Fig. 7, it shows the received constellations of legitimate receiver (the left) and illegal receiver (the right). The signal-to-noise ratio is 10dB in Fig. 7(a), which adopts QPSK modulate technique. In Fig. 7(b), the signal-to-noise ratio is 15dB, the modulate mode is 16QAM. We can see that data symbols' phase of illegal receiver is ambiguous. They cannot demodulate the original information if they can't find out the right encryption keys.

B. Computational complexity and key number

Chaos sequence has favorable sensitivity to initial conditions and parameters. Experiments results show that when system initial condition or parameter changes with the magnitude of 10^{-10}, the number of iterations when two adjacent tracks separate completely is 30~35. Assumed that the magnitude that can maintain the sensitivity of initial condition X_0 and parameter μ is 10^{-10}, the total number of combine-keys using logistic chaos mapping is 1.8×10^{39}.

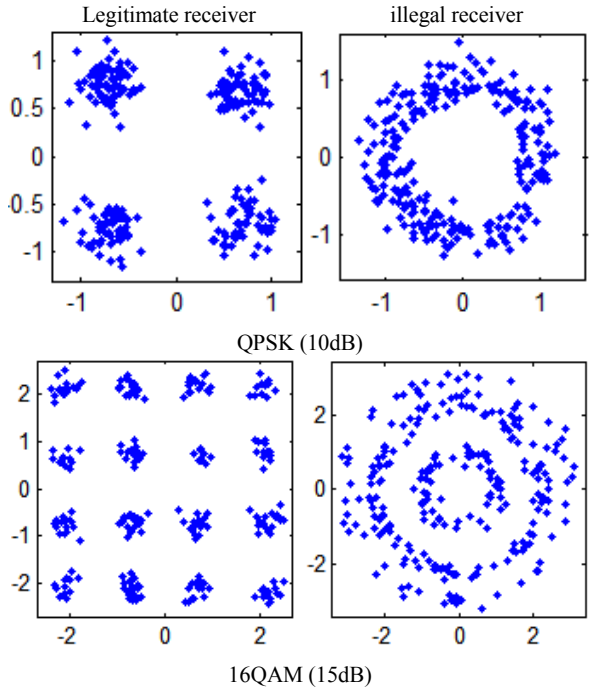

Fig. 7. Constellation received by legitimate receiver and illegal receiver

Assumed that chaos mapping can traverse from 0 to N-1 once, the calculation complexity when illegal receivers wiretap the data transmitted, would be $mN^2log_2N \times 1.8 \times 10^{39}$ at the worst condition that they have no prior information. The time they require when using the exhaustive key search is $mN^2log_2N \times 5.7 \times 10^{22}$ years if the speed of calculation is 10^6 decryptions/ms. When m=8, N=256, the time is 2.4×10^{29} years.

TABLE I. Required Decryption Time Comparison

Approach	Method	Number of secret keys	Time required
RF fingerprint	24-bit DES	1.7×10^8	8.4milliseconds
IS-95 CDMA	42-bit LFSR	4.4×10^{12}	2.2seconds
AES CDMA	128-bit AES	3.4×10^{38}	5.4×10^{18}years
Rand-MIMO	Random matrix	3.4×10^{38}	5.4×10^{18}years
Chaos based OFDM	Two-stage chaos mapping	1.8×10^{39}	2.4×10^{29}years

In [14], it compared several common encryption measures with the number of cipher keys and the required decryption time. TABLE I makes a comparison among the proposed scheme with other approaches such as radio frequency (RF) fingerprint, AES-CDMA method, randomization of MIMO transmission coefficients. Here, the speed of calculation is 10^6 decryptions/ms.

In the present encrypted scheme, an illegal receiver is unable to obtain correct information without the correct key normally. The number of possible secret keys is closely related to the security level. The scheme has a larger key size, which make it more difficult for the eavesdropper to decrypt the data.

C. *Error-correcting performance*

Fig. 8 shows the BER performance demodulated by legitimate receiver and illegal receiver in the AWGN channel. The BER performance of legal receiver is almost the same as the theoretical QPSK performance for the legitimate receiver, which illustrates that the security measure doesn't influent the receiver performance of OFDM system. And the BER performance improves a lot after using channel coding. For the illegal user, the BER curve can't drop-off as it can't decrypt the data without the two secret keys.

Fig. 9 shows the BER curve of legitimate receiver and illegal receiver in the fast Rayleigh fading channel. When zero-forcing equalization is adopted, the BER performance is worse than theoretical performance of one-fold receiving diversity in Rayleigh channel. As for the minimum mean squared error equalization, the slope of BER curve is close to theoretical performance of ten-fold receiving diversity.

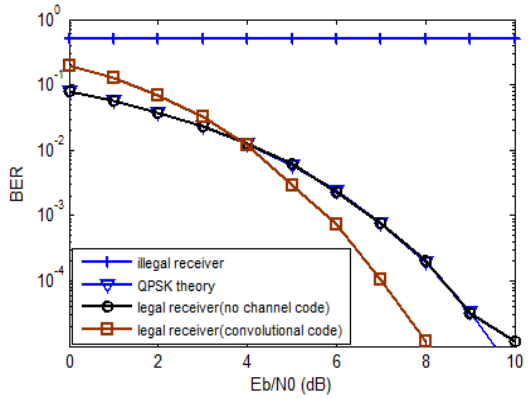

Fig. 8. BER curve for AWGN channel

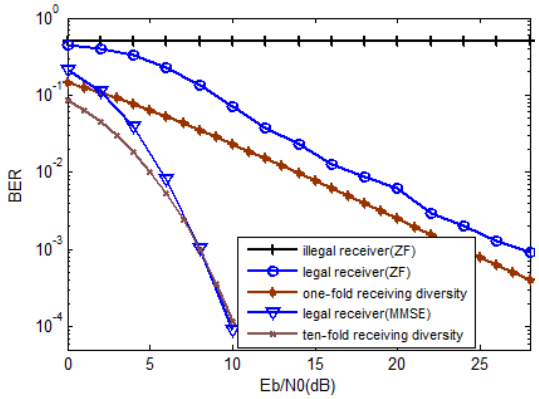

Fig. 9. BER curve for fast Rayleigh fading channel

Fig. 10 shows the BER curve of legitimate receiver and illegal receiver under the 3GPP SCME channel model with the Urban Macro scenario. The vehicle speed is 0/60/120 km/h. For the legitimate user, BER performance has a little loss at the high E_b/N_0 region, when the speed increases to 60km/h.

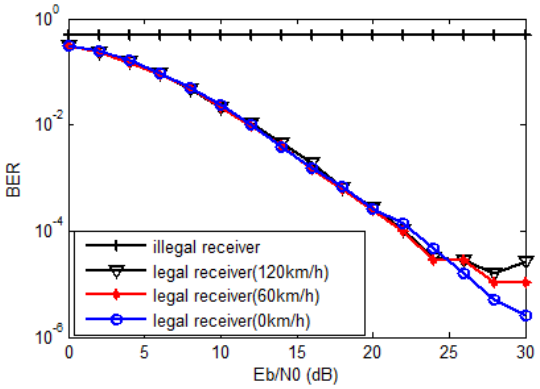

Fig. 10. BER curve for 3GPP SCME (Urban Macro) channel model

In the three channel models, illegal receiver cannot demodulate out the correct data if they don't know the right encryption keys. It's shown that the proposed scheme can work against the fading and enhance both the reliability and security of wireless data transmission. The parameters used in the simulations are listed in TABLE II.

TABLE II. SYSTEM PARAMETERS FOR SIMULATIONS

Parameter	AWGN channel	Fast Rayleigh fading channel	3GPP SCME (Urban Macro) channel
Modulation	QPSK	QPSK	QPSK
Channel Coding	(2,1,2) Convolutional code	(2,1,2) Convolutional code	(2,1,2) Convolutional code
Equalization	none	ZF/MMSE	ZF
Length of Frame	256	256	256
Number of Frames	2000	2000	2000
Number of Subcarrier	256	256	256

V. CONCLUSION

To ensure the secrecy transmission of OFDM system, this paper proposes a chaos based OFDM transmission scheme with phase chaos rotation and sub-carrier chaos mapping. The proposed secure transmission scheme has the following advantages:

- The scheme uses the principle of chaos mapping to enhance the communication security of OFDM transmission system, which can not only work effectively against multipath fading and interference, but also resist attacks like eavesdropping, traffic analysis.
- The scheme adopts two kinds of chaos mapping at the baseband signal processing. The message can't be decrypted without known the two secret keys K_1, K_2.
- The secret keys used in the scheme are lightweight, and they depend on the initial value and initial parameter of

chaos mapping. Moreover, the possible number of secret keys is large enough to resist the normal attacks.

- Compared with traditional OFDM system, the proposed scheme maintains the error-correcting performance, with a little price on the complexity. It increases the complexity that is linear with the data amount, which is acceptable for regular secrecy communications.

REFERENCES

[1] Shannon C. E.. "Communication theory of secrecy systems" [J]. *Bell Syst. Tech. J.*, vol.28, pp.656-715, 1949.

[2] Shannon C. E.. "Science of chaos and cryptology" [J]. *Bell Syst. Tech. J*., 28: 656, 1949.

[3] Dachselt F., Schwarz W.. "Chaos and cryptography" [J]. *IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1498-1509, 2001.

[4] Sarkar M., Chaudhuri R. R., Chowdhury S. D., et al. "Onset of chaos for different non linear systems by varying system parameters" [M]. *Advances in Optical Science and Engineering*. Springer India, pp. 383-396, 2015.

[5] Zhang H., Wang X. F., Li Z. H., et al. "A new image encryption algorithm based on chaos system" [C]. *Proc. of IEEE International Conference on Robotics, Intelligent Systems and Signal Processing*, vol.2, pp. 778-782, 2003.

[6] Alvarez G., Montoya F., Romera M., et al. "Breaking two secure communication systems based on chaotic masking" [J]. *IEEE transactions on circuits and systems-II* , vol. 51, no. 10, pp. 505-506, 2004.

[7] Ozdemir M. K., Arslan H.. "Channel estimation for wireless ofdm systems" [J]. *IEEE Communications Surveys & Tutorials*, vol. 9, no. 2, pp. 18-48, 2007.

[8] Khan M. A., Asim M., Jeoti V., et al. "Chaos based constellation scrambling in OFDM systems: Security & interleaving issues" [C]. *Proc. of IEEE International Symposium on Information Technology*, pp. 1 – 7, 2008.

[9] Liu B., Zhang L., Xin X., et al. "Physical layer security in OFDM-PON based on dimension-transformed chaotic permutation" [J]. *IEEE Photonics Technology Letters*, vol. 26, no. 2, pp. 127-130, 2014.

[10] Lijia Zhang, et al. "Theory and performance analyses in secure CO-OFDM transmission system based on two-dimensional permutation" [J]. *IEEE Photonics Technology Letters*, vol. 31, no. 1, pp. 74 -80, 2013.

[11] Luengo D., Santamaria I.. "Secure communications using OFDM with chaotic modulation in the subcarriers" [C]. *Proc. of IEEE Vehicular Technology Conference*, vol. 2, pp. 1022-1026, 2005.

[12] Liao Ni-huan, et al. "The chaotic spreading sequences generated by the extended chaotic map and tis performance analysis" [J]. *Journal of Electronics & Information Technology*, vol. 28, no. 7, pp. 1255-1257, 2006. (In Chinese)

[13] Fan Jiu-lun, et al. "Piecewise Logistic Chaotic Map and Its Performance Analysis" [J]. *Acta Electronica Sinica,* vol. 37, no. 4, pp. 720-725, 2009. (In Chinese)

[14] Shiu Y. S., Chang S. Y., Wu H. C., et al. "Physical layer security in wireless networks: a tutorial" [J]. *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66-74, 2011.