Implementation of Digital Chaotic Encryption in THz Wireless Communication

Feng Wang[1], Bowen Zhu[1], Cuiwei Liu[1], Kaihui Wang[1], Jiao Zhang[2], Junjie Ding[1], Junting Shi[1], Chen Wang[1], Li Zhao[1], Miao Kong[1], Yanyi Wang[1], Wen Zhou[1], Min Zhu[2], Jianguo Yu[3], Feng Zhao[4], and Jianjun Yu[1*]

[1] *Fudan University, Shanghai, 200433, China * jianjun@fudan.edu.cn*

[2]*Purple Mountain Laboratories and National Mobile Communications Research Laboratory, Southeast University, Nanjing, 210096, China*

[3]*Beijing University of Posts and Telecommunications, Beijing, 100876, China*

[4]*School of Electronic Engineering, Xi'an University of Posts and Telecommunications, Xi'an, 710121, China*

Abstract: We implement a digital chaos-based encryption scheme in a photonics-aided terahertz radio-over-fiber (ROF) system operating at 340 GHz. The encrypted PS-64QAM-OFDM signal is successfully transmitted over 20 km SSMF and 54 m wireless link.

1. Introduction

With the rapid development and deployment of wireless communication systems, there is an increasing demand for higher data rate in wireless access networks in order to keep up with the unprecedented growth of data traffic. Terahertz (THz) frequency band (0.1-10 THz) is regarded as the last piece of radio frequency (RF) spectrum, which has received widespread attention in the research community [1]. However, due to the complex structure, dynamic topology, and open characteristics of the wireless communication network, the signal beams broadcast to the free space are vulnerable to eavesdropping. Security strategies based on traditional cryptography at the upper layers are gradually insufficient to ensure the information security of wireless networks in today's era. Since the physical layer is the bottom of network, more comprehensive protection for the transmitted data can be provided at this layer. The chaotic systems have attracted widespread attention due to its good pseudo-random, unpredictability, and extreme sensitivity to the initial conditions and control parameters. Many properties of chaotic systems are consistent with the paradigm of traditional cryptography and have great potential for encryption. In particular, digital chaos is an alternative approach to the design of cryptosystems to avoid implementation difficulty [2]. Moreover, the physical layer encryption method based on the digital chaos combined with flexible DSP in the electric domain has a great application prospect for the future THz communication. Furthermore, considering the frequency selective fading in the wireless link, OFDM is a better choice because of its robustness. Therefore, the blend of OFDM and physical layer encryption scheme will be a promising direction in wireless transmission system.

In this paper, a physical layer encryption scheme based on a three-dimensional digital multi-scroll chaotic system is proposed and implemented in a ROF transmission system at THz band to enhance the security of communication. Additionally, the PS technique is incorporated into the encrypted THz wave wireless transmission system as mentioned in Ref. [3]. Finally, we successfully demonstrated the transmission of encrypted 16-QAM-OFDM and PS-64QAM-OFDM signals over 20 km SSMF and 25/54 m wireless transmission distance, respectively.

2. Operation principle

Fig. 1 depicts the schematic diagram of physical layer encryption scheme using a three-dimensional digital chaotic system in the OFDM wireless system. Firstly, we use a three-dimensional multi scroll chaotic system based on jerk model to obtain a set of chaotic sequences (x, y, z) in this encryption scheme. The chaotic system can be described as a group of ordinary differential equations (ODEs):

$$\begin{cases} \dfrac{dx}{dt} = y - sign(y) \\ \dfrac{dy}{dt} = z \\ \dfrac{dz}{dt} = -a(x + y + z - sign(x) - sign(y)) \end{cases} \tag{1}$$

where x, y, z are three state variables, a is a constant system parameter. When a = 0.6 is taken, the multi-scroll system exhibits hyper-chaotic behavior. The initial values $\{x_0, y_0, z_0\}$ of the digital chaotic system can be acted as the secret keys, which are shared between the transmitter and legitimate receiver. The Eq. (1) can be solved by Runge-Kutta method with a time step of $\Delta t = 0.01$ to generate three independent chaotic sequences $\{x\}$, $\{y\}$, $\{z\}$. The

output sequences of the three-dimensional multi-scroll chaotic system, are shown in Fig. 2(a) and (b).

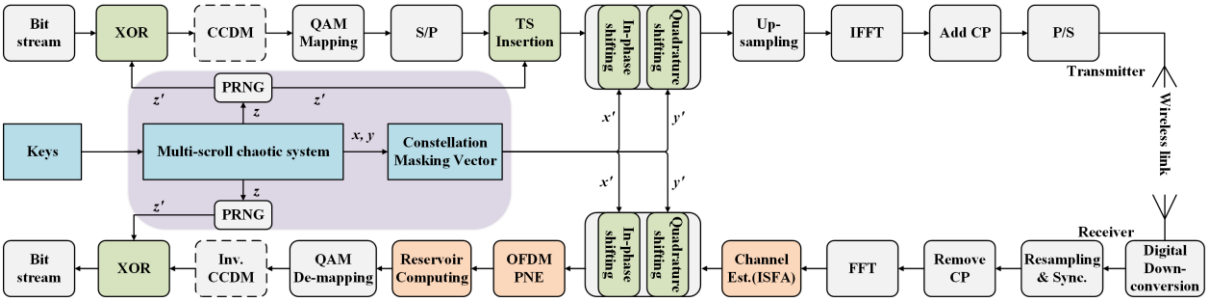

Fig. 1. Schematic diagram of proposed physical layer encryption scheme in the OFDM wireless system.

At the transmitter, original data is generated by PRBS. The chaotic sequence $\{z\}$ is used to generate $\{z'\}$ through a PRNG. The PRNG is demonstrated by the $z_i' = \mathrm{mod}(Extract(z_i, m), 2)$ where $Extract(z_i, m)$ outputs an integer, which is obtained by the *m-th* digit in the decimal part of z_i. The XOR operation is performed with the $\{z'\}$ to encrypt the original data, which can be expressed by $PRBS' = PRBS \oplus z'$. Where $\oplus$ represents the XOR operation, *PRBS* and $PRBS'$ are respectively the original and encrypted bit stream. Then, the encrypted bit stream is mapped into QAM symbols. After accomplishing S/P conversion, the training sequence (TS) is inserted that is generated by the part of the sequence $\{z'\}$. Then, the second-pass encryption is applied to change the position of the QAM constellation points by $S' = (real[S] + k \cdot x') + j(imag[S] + k \cdot y')$, where S and S' are the original and encrypted modulated QAM symbols, respectively. $\{x'\}$ and $\{y'\}$ are the sequences obtained after whitening the chaotic sequences $\{x\}$ and $\{y\}$, and k is the coefficient that controls the value range of $\{x'\}$ and $\{y'\}$. It is noted that the TS is not only used for signal synchronization, but also for channel estimation. So, the TS is not encrypted in this procedure. The original 16 QAM constellation diagram is shown in Fig. 3(c), and the encrypted noise-like 16 QAM constellation diagram is shown in Fig. 3(d). After the IFFT operation, a cyclic prefix (CP) is appended. Subsequently, the encrypted OFDM symbols are converted into a time serial sequence and sent to the free space.

At the receiver end, the IF signal is firstly down-converted to baseband, and the additional CP is removed after TS synchronization. The FFT is used to convert the baseband signal to the frequency domain, and the following channel estimation based on ISFA is implemented to smooth the estimated channel response. For the legitimate receiver, the same sequences $\{x'\}$ and $\{y'\}$ can be reproduced with the correct key, so the introduced artificial noise has no influence on the performance. However, the introduced artificial noise will cause estimation error for the illegal receiver channel, thus preventing eavesdroppers from stealing information. After the phase noise of OFDM signals is estimated by using the decision-directed-free (DDF) blind phase noise estimation (PNE) technique [4], the reservoir computing (RC) based equalization is a new machine learning method can further compensate for the signal impairments and improve the system performance [5]. Finally, the original bit is recovered by XOR operation.

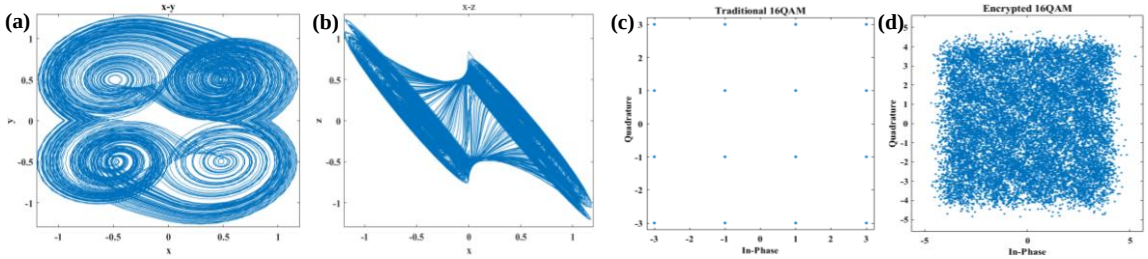

Fig. 2 (a) *x-y* phase diagram, (b) *x-z* phase diagram, (c) the traditional 16 QAM constellation, (d) after I/Q encrypted 16 QAM constellation.

3. Experimental setup and results

Fig. 3(a) illustrates the experimental setup of our demonstrated a photonics-aided terahertz wireless transmission system to evaluate the proposed encryption scheme. At the transmitter, the encrypted 16 Gbaud 16-QAM-OFDM and PS-64-QAM-OFDM (5.5 bit/symbol) are generated by using the method mentioned in the previous section. The TS is inserted every 15 OFDM symbols and the FFT size of OFDM is set to 4096, among which 1024 subcarriers are used to carry data. The TS is inserted every 15 OFDM symbols, and then a CP of size 128 is configured. Fig. 3(b)

shows the measured optical OFDM THz-wave signal spectrum after PM-OC corresponding 340 GHz. Fig. 3(c) illustrates the experimental photographs of the 54 m indoor THz wave wireless transmission.

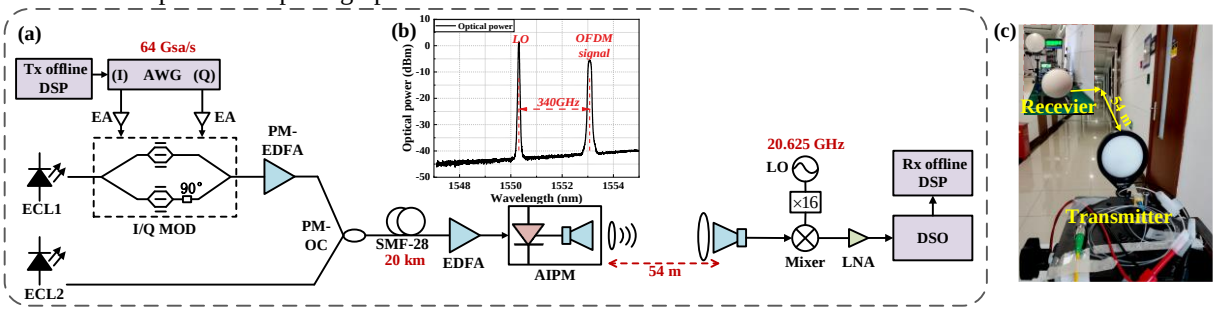

Fig. 3 (a) Experimental setup of photonics-based THz wireless transmission system, (b) the optical spectra after PM-OC corresponding to 340 GHz, (c) the experimental photographs of the 54 m indoor THz wave wireless transmission.

The BER performance is gradually better with the increase of optical power into AIPM, and the RC shows a significant performance improvement as demonstrated in Fig. 4(a). Fig. 4(b) depicts the BER curves of the 16-QAM-OFDM and PS-64-QAM-OFDM signals after 20 km SSMF and 25/54 m wireless transmission. From the result, it can be observed that the encryption method causes little distortion of transmission performance compared with the traditional OFDM signal. Considering the SD-FEC threshold of 4.2×10^{-2} with 25% overhead, the maximum net bit rate of the experiment system can be calculated as 16 Gbaud × 5.5 bit/symbol × 14/15 × (4096/(4096+128)) /1.25 ≈ 63.7 Gbit/s. At last, we analyze the security property of encryption scheme. The confidentiality of OFDM signal transmission in our proposed THz system can be greatly enhanced by implementing multi-fold encryption. At the receiver, we try to use the different keys with a small difference compared to the initial values, such as $\{x_0+\Delta x_0, y_0, z_0\}$, to decrypt the signals. The BER performance with respect to the initial value error is shown in Fig. 4(c). A very tiny deviation of 1×10^{-15} from the correct key leads to serious decryption errors, and the BER is around 0.5. According to Kerckhoff's principle, we assume that the eavesdropper masters the encryption skill based on the digital chaos well, except the secure keys $\{x_0, y_0, z_0\}$. When the parameters of the digital 3-D multi-scroll chaotic system are not considered, the total key space can reach $10^{15}\times10^{15}\times10^{15}=10^{45}$ for a conservative consideration. Consequently, the encryption method based on digital chaos can provide a huge key space, which is enough to resist exhaustive attacks. In addition, in the presence of In-phase/Quadrature encryption by inducing artificial noise for the QAM constellation, the eavesdropping channel is always at a very low SNR. Given that, even if the powerful FEC approaches are used, the eavesdropper cannot receive the transmitted data correctly.

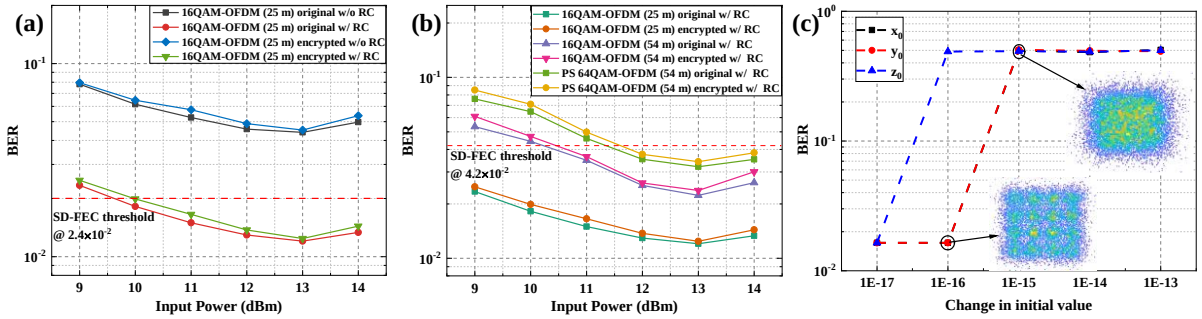

Fig. 4 (a) and (b) BER curves of the traditional/encrypted 16 Gbaud 16 QAM-OFDM and PS 64 QAM-OFDM signals after 20 km SSMF and 25/54 m wireless transmission with/without RC. (c) BER performances versus the initial value error.

4. Conclusions

In this paper, an improved physical layer encryption scheme based on a digital three-dimensional multi-scroll chaotic system is implemented to enhance the security of ROF communication. We experimentally demonstrated the encrypted PS-64QAM-OFDM signal (63.7 Gbit/s net bit rate) is successfully transmitted over 20 km SSMF and 54 m wireless link at 340 GHz. The experiment results indicate that the proposed encrypted algorithm can successfully protect against the eavesdroppers, and there is only a slight penalty in the transmission performance.

5. References

[1] Elayan, Hadeel, et al. IEEE OJ-COMS 1 (2019): 1-32.

[2] Alvarez, G, et al. Int. J. Bifurcation Chaos Appl. Sci. Eng. 16.08 (2006): 2129-2151.

[3] Zhu B, et al. IEEE Photonics Technol. Lett., 2021, 33(8): 383-386.

[4] Le, Son Thai, et al. J. Lightwave Technol. 2015, 34(2): 745-753.

[5] Sorokina M, et al. ECOC. IEEE, 2018: 1-3.