European Conference on Optical Communication © Optica Publishing Group 2022

An Experimental Demonstration of Secure OFDM-PONs Using Multi-band Chaotic Non-Orthogonal Matrix-Based Encryption

Peiji Song[(1)], Zhouyi Hu[(2)], Chun-Kit Chan[(1)]

[(1)] Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong,
[(2)] Aston Institute of Photonic Technologies, Aston University, Birmingham, B4 7ET, United Kingdom, (z.hu6@aston.ac.uk)

Abstract *We propose and experimentally demonstrate a novel multi-band CNOM-based encryption scheme for secure OFDM-PONs. The proposed method can achieve a huge key space of 9^{768}, and reduce the computational complexity by up to 97% of the original single-band encryption without affecting the transmission performance.*

Introduction

With the advantages of low power consumption, large capacity, and easy maintenance, passive optical network (PON) has been widely deployed over the past decades. It is well-recognized as a promising solution to solve the "last 1-km" bottleneck of the access networks [1]. On the other hand, orthogonal frequency division multiplexing (OFDM) has been widely investigated in PONs thanks to its high spectral efficiency (SE), robustness to channel chromatic dispersion (CD), and flexibility [2]. Nonetheless, most previous studies on OFDM-PONs mainly focused on achieving optimal transmission performance rather than their security issues. In conventional OFDM-PONs, the optical line terminal (OLT) uses a broadcasting way to transmit the downstream data to all optical network units (ONUs), making the transmitted data very susceptible to illegal eavesdropping. To solve this problem, many encryption schemes have been proposed. However, many of these techniques only used primitive permutations for subcarrier or constellation scrambling [3-5], which has high complexity and may cause a time delay and synchronization errors.

In this paper, we propose a novel multi-band non-orthogonal matrix precoding (NOM-p)-based encryption scheme for improving the physical-layer security in OFDM-PONs. In the proposed encryption scheme, the whole bandwidth of the OFDM symbols is first evenly divided into L sub-bands to increase key space and reduce complexity. Then, for each sub-band, we use a set of chaotic non-orthogonal matrices (CNOMs) to do encryption, where faster-than-Nyquist (FTN) signaling [6] and redundant precoding [7] are both utilized. Compared to the single-band CNOM-based encryption scheme previously reported in [8], the proposed multi-band scheme can significantly increase the key space and reduce complexity using the multi-band structure. We, therefore, investigate the impact of the number of sub-bands in the encryption on the transmission and security performance. Our experimental results show that by employing the proposed multi-band CNOM-based encryption scheme, we can realize transmission with higher key space and additional coding gain.

Principle

- Basic principle

Fig. 1 shows the basic principle of multi-band CNOM-based encryption. We first evenly divide the whole bandwidth of OFDM symbols into L sub-bands. Then, for each sub-band, we will use a set of CNOMs to perform encryption. Herein, we use the *l-th* sub-band of the *k-th* OFDM symbol as an example to illustrate the fundamental principle of encryption with CNOM. We first fix the bandwidth of the *l-th* encrypted sub-band at a constant as $\alpha_{lk} B_{\mathrm{OFDM},lk} = \beta$ by jointly controlling the original bandwidth determined by $B_{\mathrm{OFDM},lk}$ and the corresponding scale factors α_{lk}. It should be noted that the constant β is the same for all L sub-bands of all OFDM symbols. The scale factor α_{lk} can be greater or smaller than 1, Fig. 1 shows these three cases of $\alpha_{lk} < 1$, $\alpha_{lk} > 1$, and $\alpha_{lk} = 1$, respectively. In our designed system, the scale factor α_{lk} is determined as $\alpha_{lk} = M/N_{lk}$, where N_{lk} is the original number of subcarriers of the *l-th* sub-band decided by the chaotic system and M is the fixed number of subcarriers. M *is* derived from $M = V/L$, where V is the total number

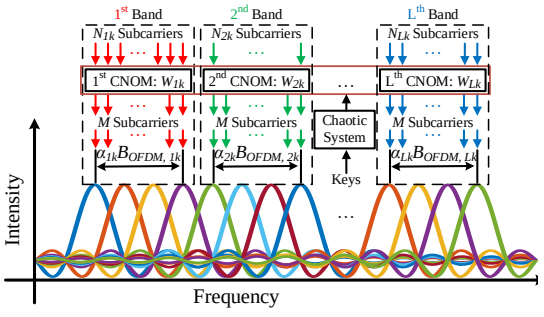

Fig. 1: Principle of multi-band CNOM-based encryption.

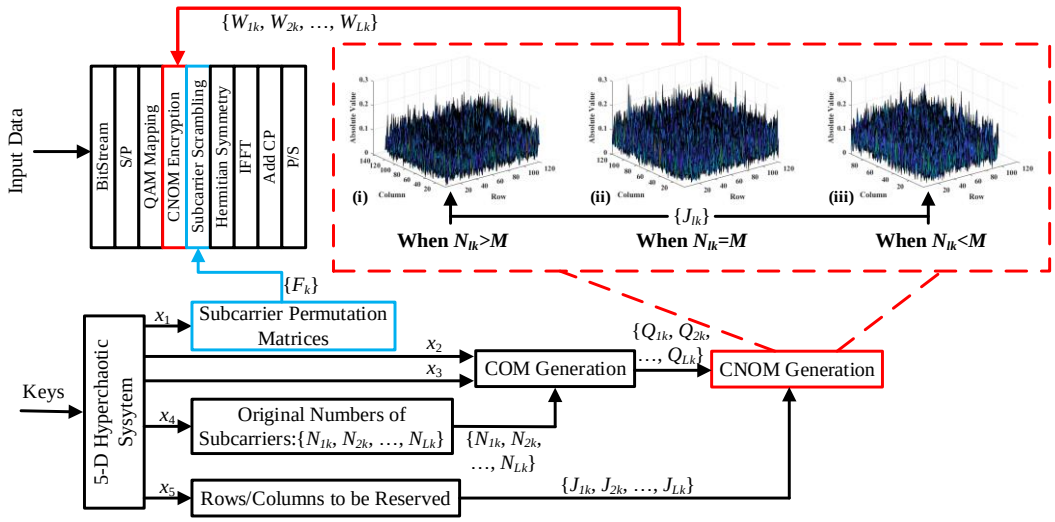

Fig. 2: Block diagram of the proposed secure PON based on multi-band CNOM encryption. Insets (i) - (iii): CNOMs $\{W_{lk}\}$ after rows/columns selection according to $\{J_{lk}\}$.

of subcarriers after encryption. Based on the value of α_{lk}, we can classify the encryption into three cases: (1) When $\alpha_{lk} < 1$, the encryption precoding matrix W_{lk} is a CNOM, and the encryption is equivalent to applying FTN precoding [6]. An additional soft-decision decoder is needed at the receiver to eliminate inter-carrier interference (ICI) [9]; (2) When $\alpha_{lk} = 1$, W_{lk} is a COM [10], the encryption will not introduce any penalty; (3) When $\alpha_{lk} > 1$, the encryption becomes as redundant precoding and the system robustness to channel impairments can be increased in this case.

The encryption can be described as $X_{lk} = W_{lk}S_{lk}$, where S_{lk} is an $N_{lk}\times1$ vector representing the original data loaded over N_{lk} subcarriers, W_{lk} is an $M\times N_{lk}$ CNOM generated by the chaotic system, and X_{lk} is an $M\times1$ vector denoting the encrypted data re-allocated over M subcarriers. The encrypted subcarriers will then be combined and scrambled by another permutation matrix F_k which is different for different OFDM symbols.

- Encryption process

Fig. 2 shows the transmitter DSP of our designed secure OFDM-PONs. Here, we use a 5-D hyperchaotic system whose state equation can be found in Ref. [11] (Eq. (15)).

The detailed encryption process is then given as follows,

Step 1: Iterate the state equation of this 5-D hyperchaotic system by Runge-Kutta 4th-order method to obtain the five chaotic sequences of x_1, x_2, x_3, x_4, and x_5.

Step 2: Generate the subcarrier permutation matrices $\{F_k\}$ from x_1 [12].

Step 3: Generate the COM $\{Q_{lk}\}$ from the chaotic sequences of x_2 and x_3, as well as the corresponding original number of subcarriers $\{N_{lk}\}$ from x_4 in a similar way in [8]. Herein, N_Q=max(N_{lk}, M). N_{min}, which is the minimum value of N_{lk} is set to be $0.8M$, and the maximum value of N_{lk} is $1.2M$ to keep the overall SE fixed in this work. Thus, the dynamic range D of N_{lk} is $2(M\text{-floor}(0.8M))$.

Step 4: Determine the rows/columns, i.e., $\{J_{lk}\}$, that should be reserved according to x_5 and N_{lk} as the process in [8]. As shown in insets (i)-(iii) of Fig. 2, we reserve or discard some rows or columns of Q_{lk} according to J_{lk}, to generate the corresponding CNOM W_{lk} with a size of $N_{lk}\times M$.

- Key space analysis

The number of all possible combinations of $\{W_{lk}\}$ for all L sub-bands against the exhaustive search attack can be calculated as,

$$KS = (((M - floor(0.8M))\times2+1)^P)^L = (((\frac{V}{L} - floor(0.8\frac{V}{L}))\times2+1)^P)^L, \quad (1)$$

where P is the frame size. We can see that the key space will increase as L increases. In addition, the chaotic behavior of CNOMs and the subcarrier scrambling matrices $\{F_k\}$ can provide additional security enhancement. However, it is noted that L should be chosen appropriately. It is because although key space will increase with L, the transmission performance and flexibility will decrease due to the inherent constraints of multi-band precoding and the FTN signaling. We will analyze the choice of L in the next section.

Experimental setup and results

Fig. 3 shows the schematic diagram of this experiment. V and P were set to 120 and 128 in this experiment, respectively. Initial binary bits after serial to parallel conversion were first mapped onto 4-QAM symbols, then divided into L sub-bands, and each sub-band was encrypted by $\{W_{lk}\}$. After Hermitian symmetry for intensity modulation, we use IFFT with a size of 256 to generate the real-valued signal, where its 1/16 was set as the cyclic prefix (CP). At the OLT, the

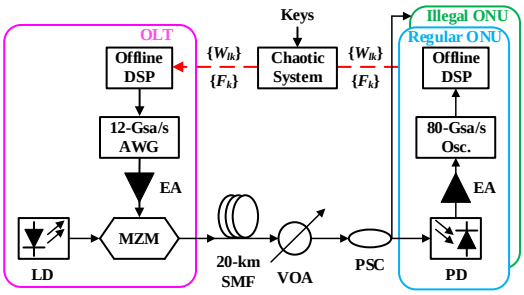

Fig. 3: Proof-of-concept experimental setup for verifying the proposed secure OFDM-PON.

generated real-valued digital signal was transformed into analog signal by using an arbitrary waveform generator (AWG) working at 12-GSample/s. As a result, the data rate excluding the CP was about 10.6 Gb/s (=12G×2×120/256×16/17). The analog signal was then amplified by an electrical amplifier (EA). Next, a Mach-Zehnder modulator (MZM) together with a laser diode (LD) centered at 1550nm converted the electrical signal into the optical domain. After 20-km standard single-mode fiber (SSMF) transmission, a variable optical attenuator (VOA) was employed to set different received optical power (ROP) values. The encrypted signal was simultaneously sent to a regular ONU and an illegal ONU using a 50:50 power splitter/coupler (PSC). After detection by a photodiode (PD), the received data was captured by an 80-GSample/s real-time oscilloscope. Finally, the detected data were restored by using right and wrong keys at two ONUs, respectively.

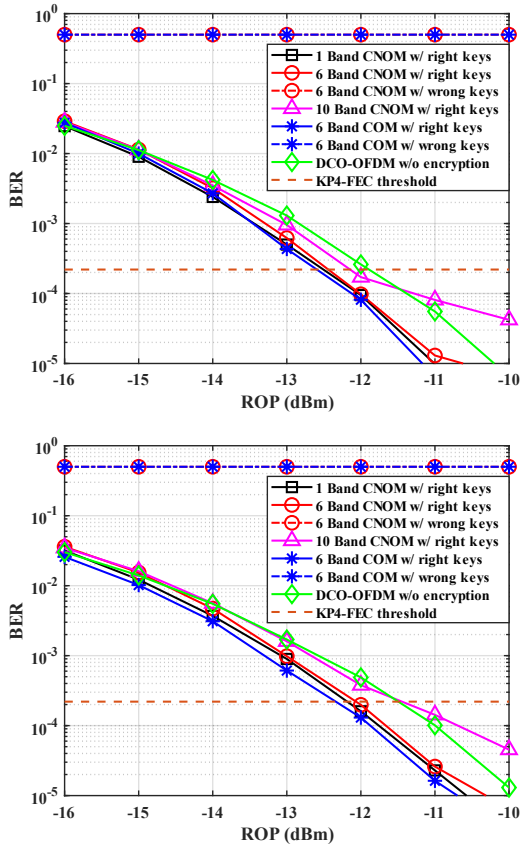

Fig. 4: Measured transmission and security performance at (a) BTB transmission, and (b) 20-km SSMF.

The experimental results are presented in Fig. 4. We first study the effect of choosing different Ls on the system performance. We can see from the figure that compared with single-band encryption, i.e., $L = 1$, the performance penalty is negligible when L increases to 6. However, the system performance will sharply deteriorate when L further increases, for instance, $L = 10$. Therefore, $L = 6$ was chosen for encryption in this work.

For $L = 6$, we can see that compared to encryption with 6-band COM, 6-band CNOM encryption only shows a slight penalty, whereas it can provide an enormous increase of key space ($(9^6)^{128}=9^{768}$ times) based on (1), where single-band CNOM encryption can only provide 49^{128} times which is very small relative to 6-band CNOM encryption. Meanwhile, both 6-band COM and 6-band CNOM encryption outperform the conventional DC-biased optical (DCO-) OFDM signal without encryption, this can be attributed to their coding gain. It can also be seen from the figure that the bit-error-rate (BER) rises sharply to 0.5 when there is only a tiny perturbation of the initial value ($\Delta x_2(0)=1\times10^{-15}$), which means no information can be eavesdropped at the illegal ONU. Moreover, we found that the total computational complexity of the proposed scheme is approximately proportional to $(N_Q)^2$. When $L = 1$, N_Q is 144, while only 24 for $L = 6$. Thus, we can reduce the complexity by up to 97% of single-band encryption using this proposed multi-band encryption.

Conclusions

In this paper, we have proposed a novel multi-band CNOM-based encryption scheme for secure OFDM-PONs. Since there is a trade-off between transmission performance and key space, depending on the sub-band number L, we optimize the choice of L via experimental results. The experimental results have shown that the optimal value of L is 6 in this system. By utilizing this 6-band structure, we can greatly increase the key space, and reduce the total computational complexity to 1/36 of the conventional single-band encryption without affecting the transmission performance. The results indicated the great potential of the proposed multi-band CNOM-based encryption in future high-security and high-speed PONs.

Acknowledgements

The work was partially supported by the General Research Fund (Project No. 14205820) of Hong Kong Research Grants Council.

References

[1] N. Cvijetic, “OFDM for next-generation optical access networks,” *Journal of Lightwave Technology*, vol. 30, no. 4, pp. 384–398, 2012.
DOI: 10.1109/JLT.2011.2166375.

[2] Z. Zhu, W. Lu, L. Zhang, and N. Ansari, "Dynamic Service Provisioning in Elastic Optical Networks with Hybrid Single-/Multi-Path Routing," *Journal of Lightwave Technology*, vol. 31, no. 1, pp. 15–22, 2013.
DOI: 10.1109/JLT.2012.2227683.

[3] Y. Xiao, Y. Chen, C. Long, J. Shi, J. Ma, and J. He, ‘‘A novel hybrid secure method based on DNA encoding encryption and spiral scrambling in chaotic OFDM-PON,’’ *IEEE Photonics Journal*, vol. 12, no. 3, 7201215, 2020.
DOI: 10.1109/JPHOT.2020.2987317.

[4] T. Wu, C. Zhang, H. Wei, and K. Qiu, “PAPR and security in OFDM-PON via optimum block dividing with dynamic key and 2D-LASM,” *Optics Express,* vol. 27, no. 20, pp. 27946–27961, 2019.
DOI: 10.1364/OE.27.027946.

[5] M. Li, B. Liu, R. Ullah, J. Ren, Y. Mao, S. Han, J. Zhao, R. Tang, S. Chen, and J. Ling, “5D data iteration in a multi-wavelength OFDM-PON using the hyperchaotic system,” *Optics Letters,* vol. 45, no. 17, 4960-4963, 2020.
DOI: 10.1364/OL.402734.

[6] Z. Hu and C. K. Chan, “Non-orthogonal matrix precoding based faster-than-Nyquist signaling over optical wireless communications,” *in Optical Fiber Communication Conference*, San Diego, California, 2020.
DOI: 10.1364/OFC.2020.M1J.5.

[7] S. Ohno and G. B. Giannakis, “Optimal training and redundant precoding for block transmissions with application to wireless OFDM,” *IEEE Transactions on Communications,* vol. 50, no. 12, pp. 2113–2123, 2002.
DOI: 10.1109/TCOMM.2002.806547.

[8] Z. Hu, P. Song, and C. K. Chan, “Chaotic Non-Orthogonal Matrix-Based Encryption for Secure OFDM-PONs,” *IEEE Photonics Technology Letters*, vol. 33, no. 20, pp. 1127–1130, 2021.
DOI: 10.1109/LPT.2021.3109029.

[9] Z. Hu and C. K. Chan, “A novel baseband faster-than-Nyquist non-orthogonal FDM IM/DD system with block segmented soft-decision decoder,” *Journal of Lightwave Technology*, vol. 38, no. 3, pp. 632–641, 2020.
DOI: 10.1109/JLT.2019.2947176.

[10] Z. Hu and C. K. Chan, “A real-valued chaotic orthogonal matrix transform-based encryption for OFDM-PON,” *IEEE Photonics Technology Letters*, vol. 30, no. 16, pp. 1455–1458, 2018.
DOI: 10.1109/LPT.2018.2853155.

[11] C. Shen, S. Yu, J. Lu, and G. Chen, “A systematic methodology for constructing hyperchaotic systems with multiple positive Lyapunov exponents and circuit implementation,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 3, pp. 854–864, 2014.
DOI: 10.1109/TCSI.2013.2283994.

[12] Z. Hu and C. K. Chan, “A 7-D hyperchaotic system-based encryption scheme for secure fast-OFDM-PON,” *Journal of Lightwave Technology*, vol. 36, no. 16, pp. 3373–3381, 2018.
DOI: 10.1109/JLT.2018.2841042..