Chaotic Digital Filter-based Physical Layer Security for Heterogeneous Access Networks

Giddings, Roger; He, Jiaxiang; Jin, Wei; Tang, Jianming

Published: 30/09/2024

Peer reviewed version

Chaotic Digital Filter-based Physical Layer Security for Heterogeneous Access Networks

Jiaxiang He
School of Computer Science and Engineering
Bangor University
Bangor, UK
eeu970@bangor.ac.uk

Wei Jin
School of Computer Science and Engineering
Bangor University
Bangor, UK
w.jin@bangor.ac.uk

Roger. P. Giddings*
School of Computer Science and Engineering
Bangor University
Bangor, UK
r.p.giddings@bangor.ac.uk

Jianming Tang
School of Computer Science and Engineering
Bangor University
Bangor, UK
j.tang@bangor.ac.uk

***Abstract*—Resource-constrained devices in security-sensitive applications require security techniques to ensure cyber-resilience, data privacy and integrity, and trust in open networks. To effectively address the above requirement, a physical layer security technique based on chaotic digital filters (CDFs), which have chaotic amplitude and phase frequency responses, is proposed and experimentally demonstrated, for the first time, in an intensity modulation and direct detection intensity (IMDD) 12Gb/s@25km standard single-mode-fiber (SSMF) optical link. The CDF-based technique provides signal protection by directly distorting signals and inducing interferences between data signals. The low-complexity and cost-efficient CDF-based security technique offers salient features of 'security-by-design', 'openness-by-design' and 'dynamic security at the traffic level', which are of great importance for applications in heterogeneous access networks.**

Keywords—Physical layer security, Optical communications, Heterogeneous access networks, Chaotic Digital Filter

I. Introduction

In the 6G era, the Internet of Everything (IoE) with ultra-high connection densities will require cybersecurity techniques to reliably protect data in open networks [1-3]. In addition, resource-constrained devices, such as IoE sensors, also require security techniques with low system complexity and cost-effectiveness. Furthermore, security techniques should be applicable in heterogeneous access networks, i.e., allowing the encrypted signals to seamlessly flow between different types of transmission media, such as fibre and wireless, without changing the applied encryption technique. On the other hand, security techniques based on cryptographic methods at the upper layers only are becoming vulnerable to attacks from artificial intelligence (AI) and quantum computers. Therefore, it is vital to extend security to the physical layer [3] by modifying physical characteristics of the data-carrying signals to realize encryptions/decryptions.

In recent years, several physical layer security techniques have been proposed and developed [4-10]. Quantum key distribution (QKD) requires expansive resources which is unsuitable for heterogeneous access networks with high connection densities. Optical-masking techniques, which mask signals with digital/analogue noise by using devices such as dual-drive Mach-Zehnder modulator (DD-MZM), and optical chaos to realize signal protection, have also been investigated [6-8]. However, these techniques often require highly accurate signal synchronization and/or complex system structures for decryptions. Digital chaos-based systems scramble data signals in multiple dimensions in the digital domain [9,10]. However, they may require additional transmission overheads and DSP complexity. In addition, digital chaos-based systems typically are operable for encrypting signals with particular modulation formats, therefore the lack of signal transparency in the encryption restricts their interoperability between different vendors devices and prohibits to implement open network solutions.

To address the above challenges, a new security technique based on chaotic digital filters (CDFs) is proposed by introducing private security key-dependent instantaneous phase changes into Hilbert-pair digital filters [11], thus resulting in the filters having chaotic amplitude and phase frequency responses. As a direct result, the CDF-based security technique employing private security keys offers signal protection by CDF-induced distortions to data signals, and CDF-induced signal interferences which realize data-assisted protection via using data signals to protect data signals.

The CDF-based security technique is security key-transmission free and has excellent transparency to network design features, such as signal modulation format and protocols, this implies that the technique can be easily and cost-effectively embedded in various DSP-enabled network devices without causing high latency. From the compatibility with existing and future communication technologies point of view, the proposed technique has three salient features: (1) Security-by-Design: the CDFs can be designed and implemented into the individual devices, systems and/or networks from the start due to the wide use of digital filters; (2) Openness-by-Design: ease of interoperability across various vendors' equipment enables open networks solutions; (3) Dynamic security at the traffic level: users can control the CDF characteristics to dynamically enable/disenable the security function depending on the prevailing traffic security requirements.

II. Operating Principle

The encryption is realized by chaotic shaping filters (CSFs) in the transmitter. The impulse responses of the CSFs consisting of an in-phase (I) filter and a quadrature-phase (Q) filter, can be expressed as:

$$h_{i-I}(t) = p(t)\cos\left(2\pi f_{ci}t + k_i(t)\right) \quad (1)$$
$$h_{i-Q}(t) = p(t)\sin\left(2\pi f_{ci}t + k_i(t)\right) \quad (2)$$

where $p(t)$ is a baseband pulse with square-root raised-cosine form, f_{ci} is the central frequency of the CSFs, which utilise the same chaotic private security key $k_i(t)$ with a noise-like waveform.

Assuming an ideal transmission channel, the encrypted signal can be expressed as:

$$s_{en}(t) = [s_1(t) \otimes h_{i-I}(t)] + [s_2(t) \otimes h_{i-Q}(t)] \quad (3)$$

where $s_1(t)$ and $s_2(t)$ are two parallel signals from a single user, and $\otimes$ represents convolution. The CSF impulse response can be considered as an output of the phase modulation process driven by the security key $k_i(t)$. Accordingly, the CSFs have security key-dependent frequency responses with chaotic phase and amplitude changes, will distort the data signals in both the frequency and time domains, thus resulting in signal protection. The distorted spectrum of the encrypted signal can be represented by the Bessel function of the first kind [12]. Also importantly, the signal interferences due to the chaotic phase rotations in the CSFs achieve enhanced signal protection, i.e., data-assisted protection by using data signals to protect data signals.

In the receiver, the decryption is realized by filtering the received encrypted signal by chaotic matching filters (CMFs) with the same but inverted private security key, their impulse responses are expressed as:

$$g_{i-I}(t) = p(-t)\cos\left(-2\pi f_{ci}t - k_i(t)\right) \quad (4)$$
$$g_{i-Q}(t) = p(-t)\sin\left(-2\pi f_{ci}t - k_i(t)\right) \quad (5)$$

The decrypted signal after CMFs can be expressed as:

$$s_1'(t) = s_{en}(t) \otimes g_{i-I}(t) \quad (6)$$
$$s_2'(t) = s_{en}(t) \otimes g_{i-Q}(t) \quad (7)$$

The CMFs separate and decrypt the data signals with the inverted security key. After the CMFs, residual signal interferences can be further removed by an equalizer based on a 2x2 multi-input, multi-output (MIMO) structure employing the least-mean-squares algorithm and training sequences [13]. If eavesdroppers attempt to recover the signals by applying standard matching filters (MF) or CMFs with incorrect security keys, the interferences between the data signals will be intensified due to further chaotic phase rotations, thus providing additional signal protection.

OFDM signals with noise-like waveforms are highly suited for application as private security keys, offering a theoretically unlimited key space [14] as an OFDM-based private security key is easily manipulated by various parameters such as the input binary data sequences generated by various cryptographic algorithms [15], number of subcarriers, subcarrier modulation format and OFDM symbol manipulations. Before system deployment, two paired transceivers are physically connected back-to-back to securely negotiate the private keys which are thus unique and transmission-free.

The implementation of CDFs in digital hardware is straightforward and their impulse responses can be flexibly and dynamically reconfigured by simply reprograming the tap coefficients of finite impulse response (FIR) filters. The tap coefficients are determined by Eqs. 1-2 and 4-5 which are dependent on the OFDM-based key generation process (KGP).

III. Experimental Demonstration

To experimentally verify the CDF-based security technique, an optical IMDD transmission system is employed, using offline DSP, as shown in Fig. 1 (a). The DSP for encryption in the transmitter is shown in Fig. 1 (b). Firstly, serial to parallel (S/P) conversion is performed on a serial data signal to produce N=16 parallel signals, then each signal is digitally up sampled by a factor M=4. 8 pairs of I/Q CSFs with 8 different OFDM-based private security keys are applied to process 16 signals from one user in parallel, and the two output signals are summed after each pair of CSFs. To allow multiple CSFs to be applied, and to enhance the security level of the system, 8 times oversampling and an 8-bit code division multiplexing process is applied with orthogonal gold codes [16].

The encrypted signal is formed by the summation of the CDM-encoded signals, which is upload to a 64 GS/s arbitrary waveform generator (AWG). The AWG's embedded channel pre-compensation function is employed to flatten the transmission system frequency response. Then, a 1550 nm MZM-based 35 GHz optical transmitter performs electrical-to-optical conversion. After a 25 km SSMF, a variable optical attenuator (VOA) is employed to adjust the received optical signal's power. Then, a 40 GHz PIN performs optical-to-electrical conversion, and a 64 GS/s digital sampling oscilloscope (DSO) captures the encrypted signal for offline DSP processing.

The DSP for the decryption performs the inverse of the encryption process by demultiplexing the received encrypted signal with correct CDM codes and applying CMFs at the receiver end, as shown in Fig. 1 (c). Any two parallel signals from the same pair of CMFs are down sampled by a factor of M=4 and then processed by an equalizer based on a 2x2 MIMO structure to remove residual signal interferences. The P/S conversion on the decrypted 16 parallel data signals produces a serial data signal.

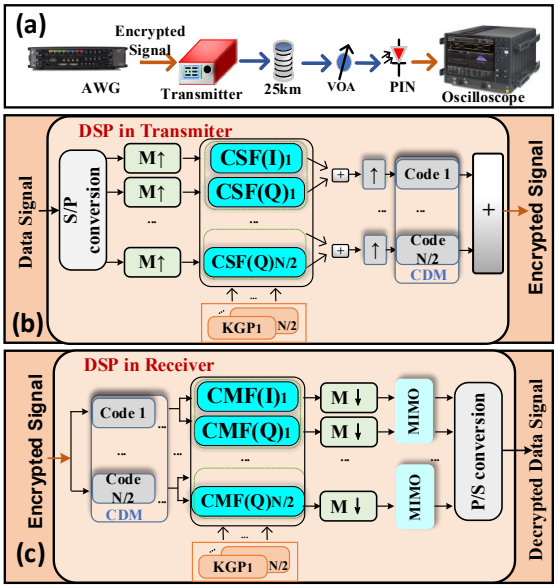

Fig. 1. (a). Experiment setup. (b). DSP flow at the transmitter side. (c) DSP flow at the receiver side.

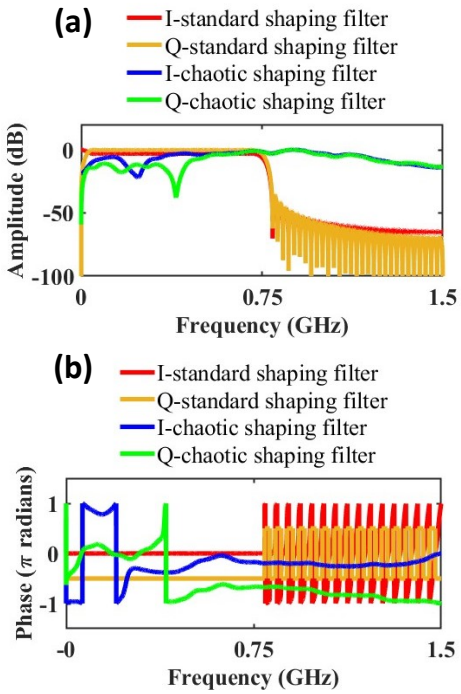

Fig. 2. (a). Amplitude frequency response of one pair of the I/Q SFs and CSFs. (b). Phase frequency response of I/Q SFs and CSFs.

All CDFs' central frequencies are taken to be 0.375GHz. The roll-off coefficient is fixed at 0.1. The serial data signal is a polar non-return-to-zero signal with a bit rate of 12 Gb/s and the effective encrypted signal bandwidth after the transmitter is 12 GHz. The OFDM-based security keys are produced by a KGP with randomly generated bit sequences, 15 subcarriers, IFFT size of 32, modulation format of 16QAM, CP length of 1/16 and a clipping ratio of 8 dB. The adopted properties for the security key are security key amplitude k_{pk}=0.8π (the peak value of $k_i(t)$), key-to-signal bandwidth ratio R_b=0.75 (the ratio between the bandwidth of the security key and the effective baseband signal bandwidth), key normalization block length L_n=32 (the security key is divided into multiple blocks of length L_n samples before applying amplitude normalisation, this eliminates the low power regions of the key due to high peak-to-average power). In this paper, the illegal decryptions are assumed to apply correct CDM codes and standard MFs.

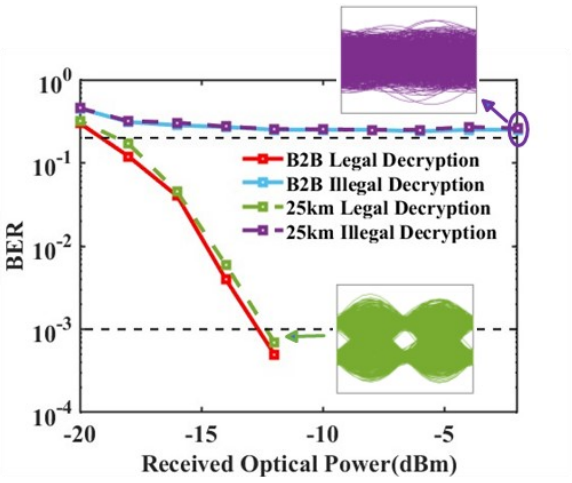

Fig. 3. BER performances of SSMF and optical B2B transmission with legal and illegal decryptions. Inset: Eye diagrams after SSMF transmission with legal and illegal decryptions when the received optical power is -2dBm.

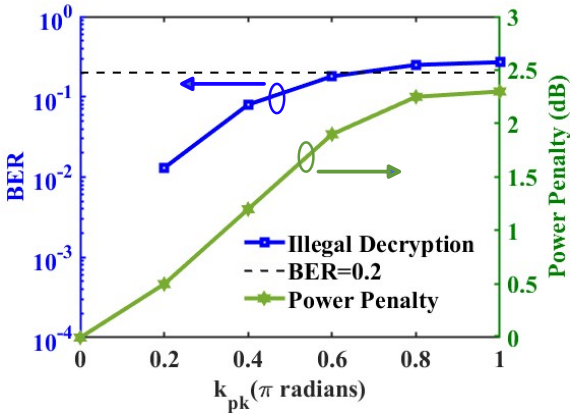

Fig. 4. The BER of illegal detections and power penalty induced by encryption with different security key amplitude k_{pk}.

As shown in Fig.2 (a) and (b), compared to the standard SFs, the frequency responses of one pair of the adopted CDFs have chaotic amplitude and phase changes which cause the data signals to be distorted in both the time and frequency domains.

A. Secure Optical Transmission Performances

The BER performances of legal decryption and illegal decryption, over an optical back-to-back (B2B) and 25 km SSMF are shown in Fig. 3. The receiver sensitivity of legal detections for the optical B2B and 25 km transmission system is ~13 dBm and ~12.5 dBm respectively at the adopted forward error correction (FEC) threshold of 1×10^{-3}, which indicates that the power penalty induced by the fibre is only ~0.5 dB. The BERs of illegal detections for both SSMF transmission and optical B2B are all >0.2, indicating that eavesdroppers cannot recover the data. Meanwhile, the eye diagrams for legal and illegal decryption are shown as insets in Fig. 3, the eye for the legal (illegal) decryption is open (completely closed).

B. Trade off between the legal transmission performances and BERs of illegal decryptions

The range of instantaneous phase changes in the CDF is determined by the security key amplitude k_{pk}, which influences the effectiveness of the encryption and then the BERs of the illegal decryptions. Furthermore, the legal decryption performance is also influenced by k_{pk} due to the residual interferences after decrypting by CMFs and the aliasing effect induced by the filter bandwidth expansions. It is therefore essential to explore the trade-off between the BERs of illegal decryptions and the power penalty for legal decryption performances as a function of k_{pk}. The power penalty at a specific k_{pk} value is measured as the reduction in receiver sensitivity relative to the corresponding case of k_{pk}= 0. As shown in Fig.4, with increasing k_{pk}, the BER of illegal detections increases, while the power penalty induced by the CDF-based encryption also increases. When k_{pk}=0.8π, the BER of illegal detections is >0.2 which is considered secure, and the corresponding power penalty is ~2.2 dB.

IV. Conclusion

In this paper, a low-cost physical layer security technique employing CDFs has been proposed and experimentally demonstrated, for the first time, in a 25 km SSMF IMDD-based 12 Gb/s NRZ optical communication system. Suitable transmission performances are achieved with a fibre-induced power penalty of ~0.5 dB and an encryption-induced power penalty of ~2.2 dB. The CDF-enabled security technique with low DSP complexity and inherent qualities of security-by-design, openness-by-design and dynamic security at the traffic level, has significant potential for providing a cost-effective physical layer security solution for heterogeneous access networks.

Acknowledgment

This work has been partly funded by the North Wales Growth Deal through Ambition North Wales, the UK GOV DSIT (FONRC) project REASON and the Engineering and Physical Sciences Research Council Project TITAN [EP/Y037243/1].

References

[1] Y. Siriwardhana, P. Porambage, M. Liyanage and M. Ylianttila, "AI and 6G security: opportunities and challenges," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), 2021.

[2] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, S. B. Taher, M. Kabir, S. M. Muyeem and A. H. Gandomi, "Toward a secure 5G-Enabled Internet of Things: A Survey on Requirements, Privacy, Security, Challenges, and Opportunities," IEEE Access, vol. 12, pp. 13125-13145, Jan. 2024.

[3] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R. A. Stoica, G. Abreu and H. Haas, "Physical-layer security in 6G networks," IEEE Open Journal of the Communications Society, vol. 2, pp. 1901-1914, Aug. 2021.

[4] J. Liu, Z. Lin, D. Liu, X. Feng, F. Liu, K. Cui, Y. Huang and W. Zhang, "High-dimensional quantum key distribution using energy-time entanglement over 242 km partially deployed fiber," Quantum Science and Technology, vol. 9, Oct. 2023.

[5] Z. Gao, Q. Wu, L. Liao, B. Su, X. Gao, S. Fu, Z. Li, Y. Wang and Y. Qin, "Experimental demonstration of synchronous privacy enhanced chaotic temporal phase en/decryption for high speed secure optical communication," Optics Express, vol. 30, pp. 31209-31219, Aug. 2022.

[6] L. Liu, S. Xiao, L. Zhang, M. Bi, Y. Zhang, J. Fang, W. Hu, "Digital chaos-masked optical encryption scheme enhanced by two-dimensional key space," Optics Communications, vol. 398, pp. 62-66, Apr. 2017.

[7] L. Zheng, Z. Zhang, M. P. Fok, Z. Liu and S. Xiao, "Optical analog noise encryption with adaptive recovery of two-dimensional keys," IEEE Photonics Technology Letters, vol. 33, no. 21, pp. 1185-1188, Nov. 2021.

[8] L. Jiang, Y. Pan, A. Yi, J. Feng, W. Pan, L. Yi, et al, "Trading off security and practicability to explore high-speed and long-haul chaotic optical communication," Opt. Express, vol. 29, pp. 12750-12762, Apr. 2021.

[9] X. Liang, C. Zhang, Y. Luo, X. Wang and K. Qiu, "Secure encryption and key management for OFDM-PON based on chaotic hilbert Motion," Journal of Lightwave Technology, vol. 41, no. 6, pp. 1619-1625, Mar. 2023.

[10] S. Wei, Y. Li, W. Wei, K. Zhu, M. Zhang, Y. Li, Y. Zhao and J. Zhang, "Probabilistic shaping probability distribution scrambling based on chaotic system for security enhancement in DFTs-OFDM," 49th European Conference on Optical Communications, Glasgow, UK, 2023, pp. 932-935.

[11] M. Bolea, R. P. Giddings and J. M. Tang, "Digital orthogonal filter-enabled optical OFDM channel multiplexing for software-reconfigurable elastic PONs," Journal of Lightwave Technology, vol. 32, no. 6, pp. 1200-1206, Mar. 2014.

[12] B. P. Lathi, Modern Digital and Analog Communications Systems, 3rd ed. Oxford University Press, Inc.1998.

[13] Y. Han and G. Li, "Coherent optical communication using polarization multiple-input-multiple-output," Optics Express, vol. 13, pp. 7527-7534, Sept. 2005.

[14] J. He, R. Giddings, W. Jin and J. Tang, "DSP-based physical layer security for coherent optical communication systems," in IEEE Photonics Journal, vol. 14, no. 5, pp. 1-11, Oct. 2022.

[15] S. Chandra, S. Paira, S. S. Alam and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), 2014

[16] X. Liu, L. Dai, C. Huang, M. Cheng, Q. Yang, M. Tang, D. Liu and L. Deng, "245Gb/s P2MP mobile fronthaul downstream transmission using code-division multiplexing and self-homodyne coherent technologies," IEEE Photonics Journal, vol. 14, no. 6, pp. 1-9, Dec. 2022.