IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 20, 2020, accepted June 30, 2020, date of publication July 6, 2020, date of current version July 20, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007429

Improving Availability and Confidentiality via Hyperchaotic Baseband Frequency Hopping Based on Optical OFDM in VLC Networks

YAHYA M. AL-MOLIKI, MOHAMMED T. ALRESHEEDI, AND YAHYA AL-HARTHI
Department of Electrical Engineering, King Saud University, Riyadh 11451, Saudi Arabia

Corresponding author: Mohammed T. Alresheedi (malresheedi@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research (DSR) through the Initiative of Graduate Students Research (GSR) Support.

ABSTRACT The security in visible-light communication (VLC) networks has recently gained attention. This work presents a hyperchaotic baseband frequency hopping method based on optical orthogonal frequency-division multiplexing (Hyperchaos-BB-FH-OOFDM) that can enhance both confidentiality and availability in VLC networks. A four-dimensional hyperchaotic scheme is employed for chaotic mapping. The proposed method exploits the random feature of the input data and chaotic codes to improve the confidentiality against correlation and statistical attacks and to improve the availability against illumination, disguised, and noise jamming. Using the chaotic scheme, the bipolar real OFDM samples are exploited to create dynamic cypher keys and spreading codes that are updated at each frame throughout the entire session, leading to high security against malicious attacks. The proposed method employs a four-fold encryption approach that involves chaotic frequency/time-domain scrambling of OFDM subcarriers, chaotic phase scrambling of frequency-domain subcarriers, and chaotic spreading of the OFDM signals upon transmission. According to the results, in addition to enhancing the confidentiality and availability, the method supports multiplexing, reduces the peak-to-average-power ratio of the OFDM signal, and improves the bit error rate performance for OFDM-based VLC networks.

INDEX TERMS Availability, confidentiality, FH-OOFDM, jamming, visible-light communication.

I. INTRODUCTION

Visible-light communication (VLC) networks are considered to have surpassed the conventional radio-based networks with regard to security, owing to the directivity and high obstacle impermeability of optical signals. This has resulted in the support of a security link for sending data inside indoor environments. However, the broadcast nature of the optical link makes VLC networks susceptible to eavesdropping and jamming. Malicious parties may not only eavesdrop on communication, but also initiate jamming attacks. The security aspects of VLC were reported in [1]–[3]. Physical-layer security has been characterized as an innovative and robust method for enhancing the security of communication [4]. In [5]–[24], authors proposed keyless security techniques as physical-layer security methods for VLC. Despite the confidentiality support, these techniques need to estimate the channel or physical position of the eavesdropper throughout communication, which involves an elaborate implementation. In [25]–[37], authors proposed secret key-based security techniques to enhance the confidentiality of VLC networks. These techniques provide computational security and have lower complexity when compared with keyless security techniques. Although various methods for physical-layer security, reviewed in [4], have been proposed to enhance the confidentiality of VLC to prevent passive eavesdropping [5]–[37], no method has been proposed to enhance the availability of VLC. In this work, we consider also improving the availability of VLC networks to enhance the security against jamming attacks.

Spread spectrum methods are efficient and robust against jamming attacks. In addition to security, they have other application areas, including systems designed to reduce multipath fading and code-division multiple-access systems.

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

Frequency hopping (FH) is one of the spread spectrum methods for providing secure communication in antagonistic environments. It has great rejection to narrowband interferences non-correlated with the spread signal [38]. In VLC, these types of interferences are generated by illumination (sunlight, light-emitting diode, fluorescent, or incandescent lamps) or by rogue transmitters with a directional light source [3]. Delgado *et al.* [39], [40] designed a wireless infrared fast FH spread spectrum method. Although this method reduces the impact of interference and multipath propagation, it is vulnerable to correlation attacks because FH is driven by pseudo-noise (PN) codes generated from linear-feedback shift registers (LFSRs) [41]. There is a high correlation between the PN codes and the output of an LFSR. So, a malicious eavesdropper with a correlation attack capability can estimate the PN codes to follow the FH behavior of the transmitter and consequently eavesdrop on the communication messages, assuming the eavesdropper knows the construction of the PN codes generator [41]. Ling and Li [42] introduced a three-dimensional modulation method called message-driven FH (MDFH). In this method, a portion of the message behaves as the PN code for the choice of the carrier frequency at the transmitting node. This method enhances the spectral efficiency of the system by adding a dimension to the signal space, which is created via transmission through FH control. However, it is susceptible to disguised jamming attacks in cases where the jamming signal has a high correlation with the transmitted signal and a power level equal to or near the power of the transmitted signal. To overcome the deficiency of MDFH, Zhang *et al.* [43] presented an anti-jamming MDFH method in which the transmitting node sends a secure signal identification (ID) code apace with the data, which behaves as a PN code for the selection of the frequency at the transmitting node. The receiving node can use the ID code to detect the valid frequency. The methods in [42] and [43] have high robustness against strong jamming interferences. However, these methods are vulnerable to message eavesdropping, as an eavesdropper can only detect the carrier frequencies to retrieve the message responsible for FH. Wang *et al.* [44] and Sá Sousa and Vilela [45] introduced uncoordinated FH (UFH) methods to enhance the availability [44] and confidentiality [45] of wireless communications. In these methods, the transmitting and receiving nodes jump to arbitrary frequencies to counteract eavesdropping and jamming attacks. The methods based on UFH do not require pre-shared keys or PN codes for the FH scheme during the entire session. However, the transmitting and receiving nodes hop to various random frequencies, depending on the UFH, and the connection among the nodes can only resume if they jump to the same frequency.

Orthogonal frequency-division multiplexing (OFDM) is effective for communication because of its immunity to multipath fading and its high spectral efficiency. Security methods for OFDM based on VLC networks have been proposed in [27]–[37]. Al-Moliki *et al.* [27]–[32] proposed to generate secret keys from the real-valued bipolar samples of the optical OFDM scheme for encrypting the signal upon transmission. Wang and Qiu [33], Wang *et al.* [35], and Wang *et al.* [37] proposed chaotic encryption methods for encrypting the images input type. Yang *et al.* [34] proposed a chaotic encryption method to secure non-orthogonal multiple access (NOMA)-based VLC systems. Security methods for OFDM based on different network technologies such as passive optical network [46], [47] and radio-based network [48], [49] have been proposed in literature. These technologies are out of scope of this paper and we only focus on improving the security for OFDM based on VLC networks.

Methods of FH based on OFDM (FH-OFDM) have been proposed in several works [50]–[53]. These methods can accomplish frequency diversity gain compared with traditional single-carrier frequency OFDM. Scholand *et al.* [50] and Berens *et al.* [51] proposed a radio-frequency (RF) carrier FH OFDM method called RF-FH-OFDM. In this method, the transmitted signal has a steady baseband (BB) signal and a hopping RF carrier. Shi *et al.* [52] introduced a BB-FH-OFDM method. In this method, the transmitted signal has a hopping BB signal and a steady RF carrier. The BB-FH-OFDM method has low hardware complexity compared with RF-FH-OFDM [52]. Despite the contributions of [51] and [52], these works merely focused on the performance of FH-OFDM based on radio channel models [53] as defined by ETSI/ITU and vehicular ad-hoc Network standards [54]. In the present work, a novel FH method based on optical OFDM in VLC networks is proposed. The main contributions of this study are as follows.

1) The chaotic scheme has many advantageous intrinsic properties, such as high sensitivity to the initial conditions, complex dynamic behavior, and distributions that do not satisfy the principle of probability, making them difficult to reconstruct and predict [55]. In this work, we propose for the first time (to our knowledge) a novel hyperchaotic BB FH method based on optical OFDM, which is denoted as hyperchaos-BB-FH-OOFDM. This method can enhance both the confidentiality and availability in VLC networks. In this method, we exploit the random nature of the input data and chaotic codes generated by the hyperchaotic scheme to enhance the confidentiality against correlation and statistical attacks and to enhance the availability against illumination, disguised, and noise jamming. The method produces secret keys and spreading codes from the polarity of the real bipolar time-domain OFDM samples and chaotic scheme. These secret sequences are updated at each frame during the entire session, leading to high security against malicious attacks.
2) The works in [27]–[32] proposed the generation of secret keys from the cyclic prefix (CP) of OFDM samples. These secret keys are exploited to encrypt the time-domain OFDM samples using an element-wise multiplication operation before transmission. Notwithstanding the high security, the multiplication in the time domain by random sequences distorts the time-domain

OFDM subcarriers before transmission, deteriorating the performance of the OFDM method in a noisy channel. In contrast to [27]–[32], instead of implementing polarity scrambling for the time-domain OFDM samples, we propose implementing phase scrambling for the frequency-domain OFDM symbols. Because this operation is implemented before the inverse fast Fourier transform (IFFT) operation, it encrypts the OFDM signals without distorting the time-domain OFDM signal (the actual transmit signal). Additionally, the multiplication of the frequency-domain symbols by a random sequence can make any in-phase frequency-domain OFDM subcarriers out-of-phase. This reduces the peak-to-average-power ratio (PAPR) of the time-domain OFDM signals, improving the performance of the OFDM system [56].

3) In contrast to [27]–[32], we propose a channel coding technique for the secret keys generated from the OFDM samples. This technique can protect the keys included in the signal when the signal travels through jammed channels.

The remaining of this paper is arranged as follows. Section II presents the mechanism of key generation from optical OFDM samples. Section III presents the four dimensional (4D) hyperchaotic scheme. The system design is presented in section IV. Section V presents the security performance of the proposed method. A complexity reduction for our method is presented in section VI. The results are presented in section VII. The paper is concluded in section VIII.

II. KEY GENERATION FROM OPTICAL OFDM SAMPLES [27]

Al-Moliki *et al.* [27] introduced a key-generation encryption mechanism for optical OFDM schemes, as shown in Fig. 1. This mechanism generates private keys from the CP of the real-valued bipolar OFDM samples to encrypt all the time-domain frames during the period of the session. The opening samples of the CP signal have the greatest exposure to the inter-symbol interference (ISI) effect in the multipath-channel scenario. Consequently, the distant samples, i.e., those in the last half, can be applied to extract the private keys [27], as shown in Fig. 2. Assume that $\boldsymbol{S_i}$ is an instant time-domain OFDM signal including two partitions: a data signal $\boldsymbol{S_i^d}$ and a CP signal $\boldsymbol{S_i^c}$, which is a duplication of several last samples of $\boldsymbol{S_i^d}$. The polarity of $\boldsymbol{S_i^c}$ is exploited

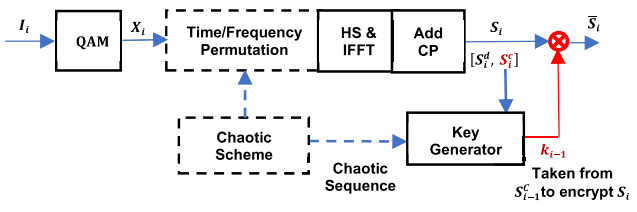

FIGURE 1. Key-generation mechanism in [27] and [29].

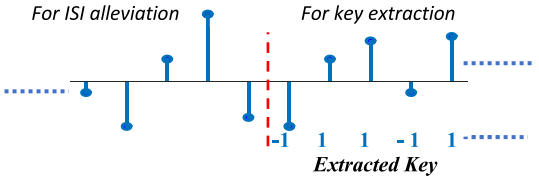

FIGURE 2. Typical CP samples.

to extract a private key $\boldsymbol{k_i}$ for encrypting the posterior time-domain signal $\boldsymbol{S_{i+1}}$. Before the transmission of $\boldsymbol{S_i}$, this signal is encrypted by a private key $\boldsymbol{k_{i-1}}$ extracted from the prior CP samples $\boldsymbol{S_{i-1}^c}$, which was produced during the former time-domain OFDM frame. The encryption operation is expressed as follows:

$$\overline{\boldsymbol{S}}_{\boldsymbol{i}} = \boldsymbol{S_i} \circ \boldsymbol{k_{i-1}}, \tag{1}$$

where the symbol "$\circ$" represents the element-wise multiplication operation (Hadamard product). The key generation and encryption are implemented dynamically throughout the session for encrypting every time-domain OFDM frame with a distinct key. A chaotic scheme can be added to the mechanism to enhance the security [29]. As shown in Fig. 1, a chaotic scheme can be employed to implement the chaotic permutation of subcarrier allocation in the time/frequency domains and the chaotic polarity scrambling of subcarriers [31]. The use of a chaotic scheme in the key generation mechanism proposed in [27] improves the security of the VLC system against several types of malicious attacks, such as known-plaintext attacks (KPAs) and chosen-plaintext attacks (CPAs) [29], [31].

OFDM is susceptible to nonlinearities in the form of signal compression and clipping [57]. In optical OFDM, there are two types of clipping: positive clipping and negative clipping. The positive clipping is to clip the part of positive samples that penetrate the nonlinear region of light-emitting diode (LED) and the negative clipping is to clip the negative samples for intensity modulation and direct detection (IM/DD) scheme. Scrambling of the time-domain samples by random sequences changes randomly the polarity of the samples and consequently the type of clipping (positive or negative) at each sample. This leads to a distortion of the time-domain subcarriers before transmission, and thus the performance of the optical OFDM is deteriorated as shown in the Results section.

In this study, we modify the mechanism used in [27]–[32] to improve the performance of the OFDM method. Instead of scrambling the time-domain subcarriers, we scramble the frequency-domain subcarriers (phase scrambling) using the private keys generated from the CP signals with the aid of a multidimensional chaotic scheme, as shown in Fig. 3. Along with enhancing the security, randomly scrambling the phase of the frequency-domain OFDM subcarriers can reduce the PAPR of the time-domain OFDM subcarriers. This enhances the performance of the OFDM system, as explained in the Results section.

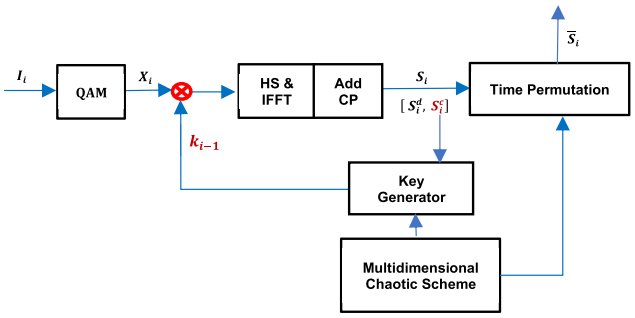

FIGURE 3. Modified key-generation mechanism.

Let $\boldsymbol{X_i}$ represents the frequency-domain signal at the output of quadrature amplitude modulation (QAM). This signal is encrypted by the $\boldsymbol{k_{i-1}}$, which was generated at the $(i-1)_{\text{th}}$ frame from CP samples and chaotic scheme, before the IFFT operation to generate the encrypted version $\overline{\boldsymbol{X}}_{\boldsymbol{i}}$, as follows:

$$\overline{\boldsymbol{X}}_{\boldsymbol{i}} = \boldsymbol{X_i} \circ \boldsymbol{k_{i-1}}. \tag{2}$$

Let $\overline{\boldsymbol{X}}_{\boldsymbol{i}}^{\boldsymbol{H}}$ be the encrypted version after the application of Hermitian symmetry (HS) to $\overline{\boldsymbol{X}}_{\boldsymbol{i}}$. It can be expressed as

$$\overline{\boldsymbol{X}}_{\boldsymbol{i}}^{\boldsymbol{H}} = \left[0, \overline{X}_{i,2}, \overline{X}_{i,3}, \ldots, \overline{X}_{i,\frac{N_d}{2}}, 0, \overline{X}^*_{i,\frac{N_d}{2}+2}, \overline{X}^*_{i,\frac{N_d}{2}+3}, \ldots, \overline{X}^*_{i,N_d}\right], \tag{3}$$

where N_d is the number of time-domain data subcarriers, and $\overline{\boldsymbol{X}}_{\boldsymbol{i,n}}$ is the n_{th} sample of $\overline{\boldsymbol{X}}_{\boldsymbol{i}}$. The time-domain OFDM samples of $\boldsymbol{S_i}$ are generated by the IFFT operation, as follows.

$$S_{i,j} = \frac{1}{N_d} \sum_{n=1}^{N_d} \overline{\boldsymbol{X}}_{i,n}^{\boldsymbol{H}} exp\left(J\frac{2\pi}{N}(n-1)(j-1)\right), \tag{4}$$

where $S_{i,j}$ and $\overline{\boldsymbol{X}}_{i,n}^{\boldsymbol{H}}$ are the j_{th} and n_{th} samples of $\boldsymbol{S_i}$ and $\overline{\boldsymbol{X}}_{\boldsymbol{i}}^{\boldsymbol{H}}$, respectively. Before the transmission of $\boldsymbol{S_i}$, the samples of $\boldsymbol{S_i}$ are permuted by a scrambling matrix generated by the multidimensional chaotic scheme during the session, as shown in Fig. 3. The dynamical scrambling not only improves the security but also enhances the bit error rate (BER) of the optical OFDM method [58].

III. FOUR-DIMENSIONAL (4D) HYPERCHAOTIC SCHEME

Although conventional low-dimensional chaotic schemes are highly effective, they suffer from a small key space and low security. Compared with the low-dimensional chaotic systems, high-dimensional hyperchaotic systems have larger positive Lyapunov exponents (more sensitivity to initial conditions), more complicated and unpredictable dynamic characteristics, and higher randomness [59]. In this study, a 4D hyperchaotic scheme is employed for producing the chaotic quantities for four-fold encryption, which are obtained as follows [60]:

$$\begin{cases} x_{i,j} = a\left(-x_{i,j-1} + y_{i,j-1}\right) + y_{i,j-1}z_{i,j-1}u_{i,j-1} \\ y_{i,j} = b\left(x_{i,j-1} + y_{i,j-1}\right) - x_{i,j-1}z_{i,j-1}u_{i,j-1} \\ z_{i,j} = cy_{i,j-1} - u_{i,j-1} + dx_{i,j-1}y_{i,j-1}u_{i,j-1} \\ u_{i,j} = -eu_{i,j-1} + x_{i,j-1}y_{i,j-1}z_{i,j-1}, \end{cases} \tag{5}$$

where a, b, c, d, and e are real parameters, and $x_{i,j}$ is the j_{th} chaotic quantity of $\boldsymbol{x_i}$ at the i_{th} frame. According to the Lyapunov exponent, if $a = 35, b = 10, c = 80, d = 0.5$, and $e = 10$, the scheme exhibits chaotic features. The approach of Runge–Kutta can be used to solve (5) to obtain the chaotic sequences $\boldsymbol{x_i}, \boldsymbol{y_i}, \boldsymbol{z_i}$, and $\boldsymbol{u_i}$ every frame using a time step of 0.001 s.

After iteration with a certain initial step, digital chaotic quantities with uniform distribution are generated. For instance, Let $\boldsymbol{D_{x,i}}$ be the digitalized chaotic sequence of $\boldsymbol{x_i}$ and it can be obtained as [60]:

$$D_{x,i,j} = mod\left(Extract\left(x_{i,j}, \text{m}, \text{n}, \text{p}\right), M\right), \tag{6}$$

where $D_{x,i,j}$ is the j_{th} chaotic quantity of $\boldsymbol{D_{x,i}}$, (m, n, p) are the first three digits in the decimal portion of $x_{i,j}$, the function $Extract\left(x_{i,j}, \text{m}, \text{n}, \text{p}\right)$ yields an integer that is generated from the m_{th}, n_{th}, and p_{th} digits in the decimal portion of $x_{i,j}$, $mod(\cdot,\cdot)$ is the remainder function, and M is the highest value of the quantity, e.g., 256 in our scheme.

Like $\boldsymbol{D_{x,i}}$, the other digitalized chaotic sequence $\boldsymbol{D_{y,i}}, \boldsymbol{D_{z,i}}$, and $\boldsymbol{D_{u,i}}$ are obtained from $\boldsymbol{y_i}, \boldsymbol{z_i}$, and $\boldsymbol{u_i}$ respectively using (5) and (6). The hyperchaotic quantities generated from the chaotic scheme are highly sensitive to the initial quantities $\left(\sim 1\times10^{-15}\right)$ and have a reliable characteristic of randomness [60], resulting in high security against malicious attacks.

IV. SYSTEM DESIGN

We assume a VLC model, as illustrated in Fig. 4. In this model, a LED lamp is attached to the ceiling to support illumination and to transmit the signal information to legitimate receivers placed within the attocell formed by the radiation pattern of the LED.

Moreover, malicious nodes are placed inside and outside the attocell. These malicious nodes are either: (i) an eavesdropper who eavesdrops on the communication link between legitimates nodes and is located within the attocell or (ii) a jammer who disrupts the VLC link for the legitimate receiving node and may be located outside the attocell. The jamming node may utilize either directed/non-directed line of sight (LOS) or directed/non-directed non-LOS (NLOS) [2], [3]. VLC-based networks contain many independent transmitting nodes to ensure sufficient coverage and capacity. In such settings, the installation of a malicious jamming node may be undetected [3]. In this study, we consider three types of jammers: illumination, disguised, and noise jammers. The illumination jammer (LED, fluorescent,

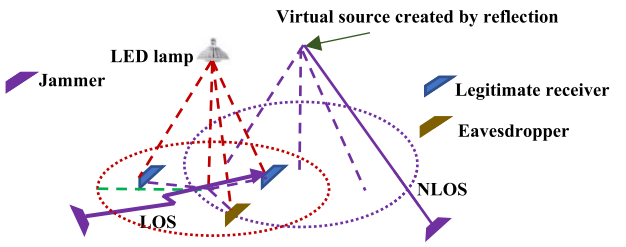

FIGURE 4. System model.

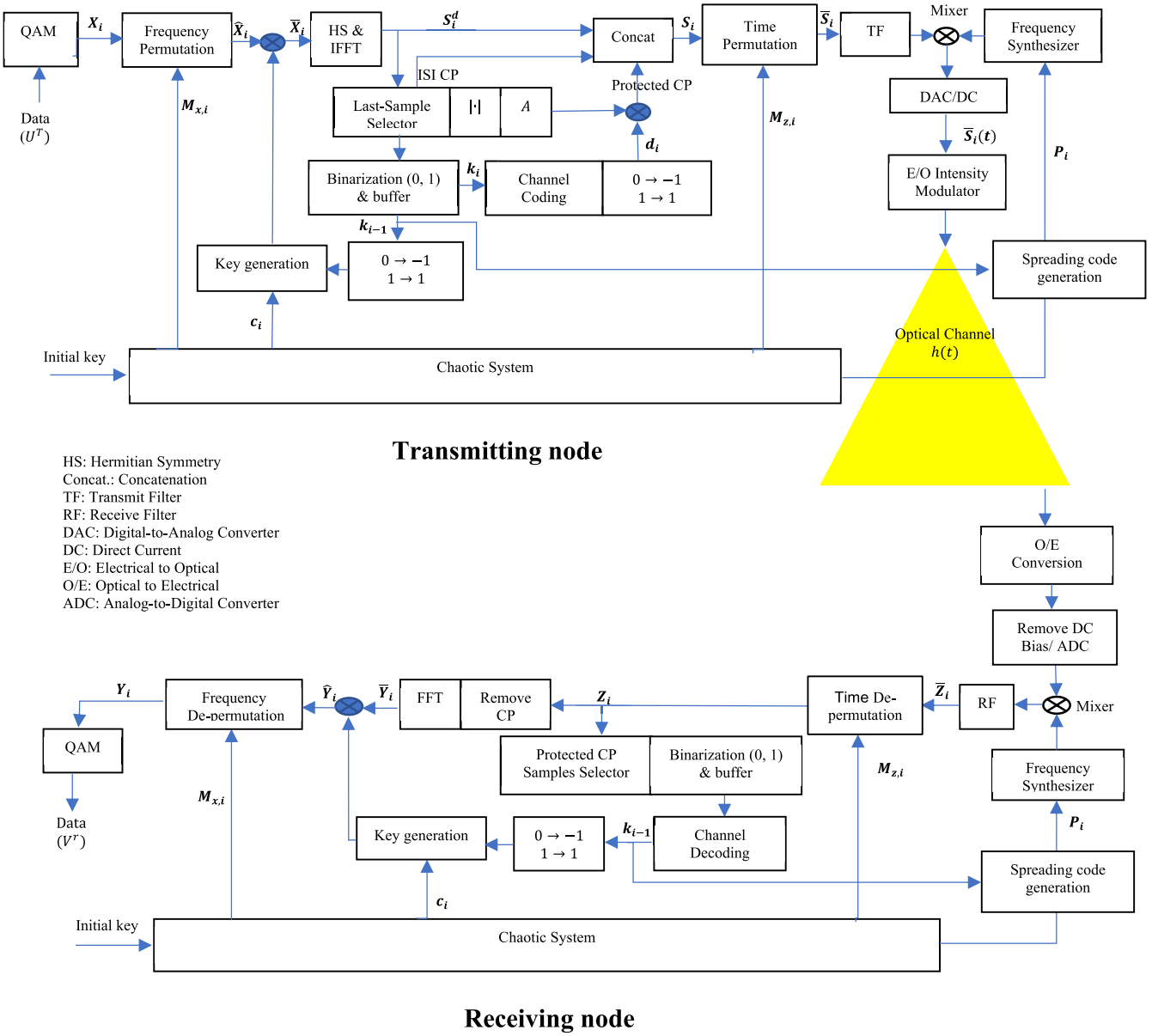

FIGURE 5. Proposed hyperchaos-BB-FH-OOFDM method.

or incandescent lamp) emits a constant illumination average power; the disguised jammer emits a jamming signal that is highly correlated (the same modulation format, number of subcarriers, etc.) with the transmitted signal; and the noise jammer, which was modeled in [61], emits an additive white Gaussian noise (AWGN) signal toward the legitimate node. In this work, we propose a hyperchaos-BB-FH-OOFDM method to mitigate the jamming attacks, as shown in Fig. 5.

The proposed hyperchaos-BB-FH-OOFDM implements chaotic encryption on four principal stages, as follows. The first stage is the permutation of frequency-domain OFDM symbols and is defined by the sequence $\boldsymbol{D_{x,i}}$. The second stage is the phase scrambling of frequency-domain OFDM symbols and is defined by the sequence $\boldsymbol{D_{y,i}}$ and the secret key generated from the CP samples. The third stage is the permutation of time-domain OFDM samples and is defined by the sequence $\boldsymbol{D_{z,i}}$. The last stage is the generation of the chaotic spreading codes and is defined by the sequence $\boldsymbol{D_{u,i}}$ and the secret key generated from the CP samples, for FH operation. The details of the encryption method are as follows.

The first sequence $\boldsymbol{D_{x,i}}$ is employed for frequency-domain permutation of OFDM symbols, as shown in Fig. 5. In accordance with the order of the digital values in $\boldsymbol{D_{x,i}}$, a scrambling matrix $\boldsymbol{M_{x,i}}$ is created. Let $\mathbf{r_{x,i}}$ be a permutation vector with a length of $\frac{N_f}{2}$, where N_f is the number of frequency-domain subcarriers, this vector is expressed as follows.

$$\boldsymbol{r_{x,i}} = \left[D_{x,i,1}, D_{x,i,2}, \ldots, D_{x,i,\frac{N_f}{2}} \right]^T. \tag{7}$$

Let $\boldsymbol{r}^{s}_{\boldsymbol{x},\boldsymbol{i}}$ be the ascending sorted form of $\boldsymbol{r}_{\boldsymbol{x},\boldsymbol{i}}$, an $\frac{N_f}{2} \times \frac{N_f}{2}$ matrix $\boldsymbol{B}_{\boldsymbol{x},\boldsymbol{i}}$ is computed as

$$\boldsymbol{B}_{\boldsymbol{x},\boldsymbol{i}} = \boldsymbol{I}\left(\boldsymbol{r}^{s}_{\boldsymbol{x},\boldsymbol{i}}\left[\boldsymbol{r}^{-1}_{\boldsymbol{x},\boldsymbol{i}}\right]^{T}\right), \tag{8}$$

where $\boldsymbol{r}^{-1}_{\boldsymbol{x},\boldsymbol{i}} = \left[\frac{1}{D_{x,i,1}}, \frac{1}{D_{x,i,2}}, \ldots, \frac{1}{D_{x,i,\frac{N_f}{2}}}\right]^{T}$, $\boldsymbol{I}(\cdot)$ is given as

$$\boldsymbol{I}(\boldsymbol{Y}) = \boldsymbol{Z} \rightarrow Z_{m,n} = \begin{cases} 1 & \text{for } Y_{m,n} = 1 \\ 0 & \text{else,} \end{cases} \tag{9}$$

where $\boldsymbol{Z}$ and $\boldsymbol{Y}$ are the output and input matrices of $\boldsymbol{I}$ respectively. An $N_f \times N_f$ scrambling matrix is computed as follows.

$$\boldsymbol{M}_{\boldsymbol{x},\boldsymbol{i}} = \begin{bmatrix} \boldsymbol{B}_{\boldsymbol{x},\boldsymbol{i}} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{B}^{r}_{\boldsymbol{x},\boldsymbol{i}} \end{bmatrix}, \tag{10}$$

where $\boldsymbol{B}^{r}_{\boldsymbol{x},\boldsymbol{i}}$ indicates the rotation process of $\boldsymbol{B}_{\boldsymbol{x},\boldsymbol{i}}$ and it is obtained by

$$\boldsymbol{B}^{r}_{\boldsymbol{x},\boldsymbol{i}} = \boldsymbol{r}\boldsymbol{B}_{\boldsymbol{x},\boldsymbol{i}}\boldsymbol{r}, \tag{11}$$

where $\boldsymbol{r}$ is an $\frac{N_f}{2} \times \frac{N_f}{2}$ anti-diagonal matrix and it is obtained by

$$\boldsymbol{r} = \begin{bmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{bmatrix}. \tag{12}$$

The scrambling matrix $\boldsymbol{M}_{\boldsymbol{x},\boldsymbol{i}}$ contains one entry of 1 in each row and each column and 0s elsewhere. After the generation, the scrambling matrix is employed to implement permutation for frequency-domain OFDM symbols:

$$\widehat{\boldsymbol{X}}_{\boldsymbol{i}} = \boldsymbol{M}_{\boldsymbol{x},\boldsymbol{i}}\boldsymbol{X}_{\boldsymbol{i}}, \tag{13}$$

where $\widehat{\boldsymbol{X}}_{\boldsymbol{i}}$ represents the permuted frequency-domain OFDM symbols.

The second sequence $\boldsymbol{D}_{\boldsymbol{y},\boldsymbol{i}}$ is utilized for the phase scrambling of $\widehat{\boldsymbol{X}}_{\boldsymbol{i}}$. A private key $\boldsymbol{c}_{\boldsymbol{i}}$ is generated from $\boldsymbol{D}_{\boldsymbol{y},\boldsymbol{i}}$ using binarization process as

$$c_{i,j} = \begin{cases} -1 & for\ D_{y,i,j} \leq \dfrac{M}{4} \\ +1 & for\ D_{y,i,j} > \dfrac{M}{4}, \end{cases} \quad 1 \leq j \leq N_f \tag{14}$$

where $c_{i,j}$ and $D_{y,i,j}$ are the j_{th} elements of $\boldsymbol{c}_{\boldsymbol{i}}$ and $\boldsymbol{D}_{\boldsymbol{y},\boldsymbol{i}}$ respectively and $M = 256$ in our scheme. This key is employed to perform phase scrambling for frequency-domain OFDM symbols. Let $\boldsymbol{k}_{\boldsymbol{i}}$ be a secret key generated from the polarity of the CP samples of time-domain OFDM signal at the i_{th} frame (see Fig. 5 and (18)), the phase scrambling operation is implemented as follows.

$$\overline{\boldsymbol{X}}_{\boldsymbol{i}} = \widehat{\boldsymbol{X}}_{\boldsymbol{i}} \circ \boldsymbol{c}_{\boldsymbol{i}} \circ \boldsymbol{k}_{\boldsymbol{i-1}}, \tag{15}$$

where $\boldsymbol{k}_{\boldsymbol{i-1}}$ is a private key generated from the CP samples of the time-domain signal during the previous frame, with index $(i-1)_{\text{th}}$, and $\overline{\boldsymbol{X}}_{\boldsymbol{i}}$ represents the encrypted OFDM symbols. Concatenated copies of $\boldsymbol{k}_{\boldsymbol{i-1}}$ are generated to produce a key with the same length as $\widehat{\boldsymbol{X}}_{\boldsymbol{i}}$.

Let $\boldsymbol{S}^{\boldsymbol{d}}_{\boldsymbol{i}}$ represents the current real bipolar OFDM samples at the output of the IFFT operation at the time of communication. This signal is produced by applying the HS to the subcarriers in the frequency domain using (3) and (4). The CP samples $\boldsymbol{S}^{\boldsymbol{c}}_{\boldsymbol{i}}$ are appended to $\boldsymbol{S}^{\boldsymbol{d}}_{\boldsymbol{i}}$ to create the total OFDM samples $\boldsymbol{S}_{\boldsymbol{i}}$. The $\boldsymbol{S}^{\boldsymbol{c}}_{\boldsymbol{i}}$ samples are created from the last several samples of $\boldsymbol{S}^{\boldsymbol{d}}_{\boldsymbol{i}}$, as follows:

$$\boldsymbol{S}^{\boldsymbol{c}}_{\boldsymbol{i}} = [\underbrace{S^{d}_{i,(N_d-l_I)}, \ldots, S^{d}_{i,N_d}}_{ISI\ CP}, \underbrace{A_i.*d_{i,1}, \ldots, A_i.*d_{i,l_p}}_{Protected\ CP}], \tag{16}$$

$$A_i = \frac{1}{l_I}\sum_{j=N_d-l_I}^{N_d}\left|S^{d}_{i,j}\right|, \tag{17}$$

where $S^{d}_{i,j}$ is the j_{th} sample of $\boldsymbol{S}^{\boldsymbol{d}}_{\boldsymbol{i}}$ at the i_{th} frame, (l_I, l_p) are the lengths of the ISI and protected CP samples, A_i is the average of the absolute values of the last several selected samples of $\boldsymbol{S}^{\boldsymbol{d}}_{\boldsymbol{i}}$ and it is significantly higher than the channel noise owing to the requirement of illumination [27], and $d_{i,j}$ is the j_{th} element of a vector $\boldsymbol{d}_{\boldsymbol{i}}$, where $\boldsymbol{d}_{\boldsymbol{i}}$ is produced from the last several samples of $\boldsymbol{S}^{\boldsymbol{d}}_{\boldsymbol{i}}$ after binarization and channel coding operations, the first part of $\boldsymbol{S}^{\boldsymbol{c}}_{\boldsymbol{i}}$ is utilized for ISI absorption, and the second part contains the CP key $\boldsymbol{k}_{\boldsymbol{i}}$ that is generated from the last several samples of $\boldsymbol{S}^{\boldsymbol{d}}_{\boldsymbol{i}}$ as follows.

$$k_{i,j} = \begin{cases} -1 & for\ S^{d}_{i,j} \leq 0 \\ +1 & for\ S^{d}_{i,j} \geq 0, \end{cases} \quad N_d - Rl_p \leq j \leq N_d \tag{18}$$

where $k_{i,j}$ is the j_{th} element of $\boldsymbol{k}_{\boldsymbol{i}}$, and R is the code rate of the channel coder that encodes $\boldsymbol{k}_{\boldsymbol{i}}$. The key $\boldsymbol{k}_{\boldsymbol{i}}$ is exploited to encrypt $\widehat{\boldsymbol{X}}_{\boldsymbol{i+1}}$ during the next frame, with index $(i+1)_{\text{th}}$, using (15). After the total OFDM signal $\boldsymbol{S}_{\boldsymbol{i}}$ is generated from $\boldsymbol{S}^{\boldsymbol{d}}_{\boldsymbol{i}}$ and $\boldsymbol{S}^{\boldsymbol{c}}_{\boldsymbol{i}}$, the third sequence $\boldsymbol{D}_{\boldsymbol{z},\boldsymbol{i}}$ is employed for time-domain permutation of the OFDM samples $\boldsymbol{S}_{\boldsymbol{i}}$. Let $\left(N = N_d + l_I + l_p\right)$ be the total number of time-domain subcarriers, In accordance with the order of the digital values in $\boldsymbol{D}_{\boldsymbol{z},\boldsymbol{i}}$, an $N \times N$ scrambling matrix $\boldsymbol{M}_{\boldsymbol{z},\boldsymbol{i}}$ is created using the same procedure as $\boldsymbol{M}_{\boldsymbol{x},\boldsymbol{i}}$ is created (see (7) to (12)). This scrambling matrix is employed to implement permutation for the time-domain OFDM samples, as follows:

$$\overline{\boldsymbol{S}}_{\boldsymbol{i}} = \boldsymbol{M}_{\boldsymbol{z},\boldsymbol{i}}\boldsymbol{S}_{\boldsymbol{i}}, \tag{19}$$

where $\overline{\boldsymbol{S}}_{\boldsymbol{i}}$ represents the permuted time-domain OFDM samples.

Suppose that N_c is the number of usable carrier frequency channels $\{f_1, f_2, \ldots, f_{N_c}\}$. Assuming that N_c is a power of 2, the number of bits utilized to determine a specific channel is $\log_2 N_c$.

Let T_s represents the period of the OFDM symbol and T_h represents the hop period. Then, the number of hops per OFDM symbol duration is given as $N_h = \frac{T_s}{T_h}$. For fast FH method, N_h is an integer equal to or greater than 1. Both the final chaotic sequence $\boldsymbol{D}_{\boldsymbol{u},\boldsymbol{i}}$ and the CP key $\boldsymbol{k}_{\boldsymbol{i-1}}$, which was generated during the $(i-1)_{\text{th}}$ frame, are employed to generate the spreading vector $\boldsymbol{P}_{\boldsymbol{i}} = \{p_{i,1}, p_{i,2}, \ldots, p_{i,N_h}\}$ using

binarization process for FH, where $p_{i,j}$ is the j_{th} spreading code generated during the current frame. Let $\boldsymbol{b_i}$ be a private key generated from $\boldsymbol{D_{u,i}}$ using binarization process as

$$b_{i,j} = \begin{cases} -1 & for\ D_{u,i,j} \le \dfrac{M}{4} \\ +1 & for\ D_{u,i,j} > \dfrac{M}{4}, \end{cases} \quad 1 \le j \le N_h \log_2 N_c \quad (20)$$

where $b_{i,j}$ and $D_{u,i,j}$ are the j_{th} elements of $\boldsymbol{b_i}$ and $\boldsymbol{D_{u,i}}$ respectively. The spreading vector $\boldsymbol{P_i}$ can be computed as follows:

$$\boldsymbol{P_i} = \boldsymbol{b_i} \circ \boldsymbol{k_{i-1}}. \quad (21)$$

A truncated portion of $\boldsymbol{k_{i-1}}$ with a length of $N_h \log_2 N_c$ is obtained to generate $\boldsymbol{P_i}$ using (21).

Let $\boldsymbol{f_i}$ be the carrier-frequency vector corresponding to $\boldsymbol{P_i}$. Suppose $N_c = 64$ channels with carrier frequencies of {10, 12, 14, . . . , 132, 134, and136} MHz, in accordance with [39], $\boldsymbol{f_i}$ can be computed as follows:

$$\boldsymbol{f_i} = \left\{2 \cdot B2D(\boldsymbol{P_i}) + 10\right\} \times 10^6, \quad (22)$$

where $B2D$ is the binary-to-decimal conversion. After $\boldsymbol{f_i}$ is generated, the transmitted signal is expressed as follows:

$$\begin{aligned} &\overline{\boldsymbol{S}}_i(t) \\ &= \sqrt{2} Re\left\{\sum_{j=1}^{N} \overline{S}_{i,j} \cdot [g(t-(j-1)T_h)] \cdot e^{J2\pi f_{i,j} t}\right\} + i_{bias} \\ &= \sqrt{2} Re\left\{\sum_{j=1}^{N}\sum_{m=1}^{N_c} \alpha_{m,j} \overline{S}_{i,j} \cdot [g(t-(j-1)T_h)] \cdot e^{J2\pi f_m t}\right\} + i_{bias}, \end{aligned} \quad (23)$$

$\alpha_{m,j}$ is given as

$$\alpha_{m,j} = \begin{cases} 1 & \text{if } f_{i,j} = f_{\boldsymbol{m}} \\ 0 & \text{otherwise}, \end{cases}$$

where $\overline{S}_{i,j}$ is the j_{th} sample of $\overline{\boldsymbol{S}}_{\boldsymbol{i}}$, $f_{i,j}$ is the j_{th} carrier frequency, i_{bias} is the direct-current bias added to the signal for IM/DD in the VLC system [27], and $g(t)$ is a pulse-shaping filter given by [62] as

$$g(t) = \frac{\sin[\pi t(1-\gamma)/\ell T_s] + 4\gamma t \cos[\pi t(1+\gamma)/\ell T_s]/\ell T_s}{\pi t[1-(4\gamma t/\ell T_s)^2]/T_s}, \quad (24)$$

where γ and ℓ are the roll-off and oversampling factors respectively.

The random feature of the input data is exploited to create dynamic cyphertexts. From (15), (21), (23), and Fig. 5, to detect the current OFDM frame $\mathrm{S}_i(t)$, with index i_{th}, Eavesdropper requires to detect the previous OFDM frame $\mathrm{S}_{i-1}(t)$, with index $(i-1)_{\text{th}}$, to generate $\boldsymbol{k_{i-1}}$ which was employed to encrypt and spread the current OFDM frame $\mathrm{S}_i(t)$, accordingly, the complete historical OFDM signals are required to detect the subsequent signal. Unlike the methods in [33]–[37], where they provide static chaotic keys with statistical characteristics that are helpful for the malicious nodes, our method provides dynamic cypher keys, associated with the random input data, that can destroy this type of statistics, therefore our method supports high security against statistical attacks.

Remarks: In a wireless optical-based network, the wavelength hopping method [63], which is implemented in the optical domain, cannot be used to overcome jamming interference. This is because the malicious node can simply emit white light, which contains nearly all wavelengths, as a jamming interference to disrupt any wavelength agreed upon legitimate nodes in each hop period. Thus, similar to [39], we choose the FH method, which is implemented in the electrical domain, to overcome jamming interference.

Herein, we assume that the initial key of the hyperchaotic scheme that is used to generate the initial chaotic sequences $(\boldsymbol{D_{x,1}}, \boldsymbol{D_{y,1}}, \boldsymbol{D_{z,1}}, \boldsymbol{D_{u,1}})$, which are employed to encrypt and spread the first frame during the session, is exchanged securely and reliably between the transmitter and receiver during the connection setup phase. In [25], the feasibility of implementing a secret key in VLC channels was investigated, and a secure beamforming design for the multi-input single-output scenario was introduced for the exchange of this key. In [27], a handshaking protocol was introduced for the exchange of the initial key. In [29], the authors introduced a chaotic key creation protocol that utilized the location-sensitive and real-valued channel state information of the VLC channel to create the initial key.

At the receiving node, the received signal is given by

$$\overline{Z}_i(t) = h(t) \otimes \left(r \cdot \overline{S}_i(t)\right) + J(t) + n(t), \quad (25)$$

where r is the photodetector responsivity, $J(t)$ is the jamming signal produced from a malicious node, $n(t)$ represents thermal and shot noises and is modeled as an AWGN process, the operator $\otimes$ indicates convolution, and $h(t)$ is the channel impulse response.

In case of line-of-sight channel with no reflection, the time-domain channel impulse response is roughly a scaled and delayed Dirac delta function as [64]

$$h^0(t; \mathrm{S}, \mathrm{R}) = \frac{(m+1)A_{pd}}{2\pi \mathrm{D}^2} \cos^m(\emptyset) \cos(\varphi) \cdot rect\left(\frac{\varphi}{FOV}\right) \delta\left(t - \frac{\mathrm{D}}{c}\right), \quad (26)$$

where S is a particular source, R is a particular receiver, m signifies the order of Lambertian emission $\left(m = -\frac{\ln(2)}{\ln(\cos(\emptyset_{1/2}))}\right)$, $\emptyset_{1/2}$ stands for the half power semi-angle of the LED, D is the Euclidean distance between the transmitter and receiver, $\emptyset$ is the radiance angle, φ is the incident angle, FOV is the field of view of the receiver, c is the speed of light, and the rectangular function is given by

$$rect(v) = \begin{cases} 1, & \text{for } |v| \le 1 \\ 0, & \text{for } |v| > 1. \end{cases} \quad (27)$$

In case of multipath channel with κ reflections, the time-domain impulse response of the optical channel was obtained

in [64] as

$$h\left(t;\mathrm{S},\mathrm{R}\right)=\sum_{\kappa=0}^{\infty}h^{\kappa}\left(t;\mathrm{S},\mathrm{R}\right), \tag{28}$$

where $h^{\kappa}\left(t;\mathrm{S},\mathrm{R}\right)$ is the light response experiencing precisely κ reflections. The response $h^{0}\left(t\right)$, $\kappa=0$, is obtained by (26) and the higher-order impulse responses $h^{\kappa}\left(t\right)$, $\kappa>0$, are computed by [64]:

$$\begin{aligned}&h^{\kappa}\left(t;\mathrm{S},\mathrm{R}\right)\\&=\frac{m+1}{2\pi}\sum_{i=1}^{\mathbb{N}}\frac{\rho_i\cos^{m}(\emptyset)\cos(\varphi)}{\mathrm{D}^2}\\&\quad\cdot rect\left(\frac{2\varphi}{\pi}\right).h^{\kappa-1}\left(t-\frac{\mathrm{D}}{c};\{\mathbf{r},\widehat{\boldsymbol{n}},\mathbf{1}\},\mathrm{R}\right)\cdot\Delta A,\end{aligned} \tag{29}$$

where $\mathbb{N}$ is the overall number of reflecting parts in a room, $\widehat{\boldsymbol{n}}$ is the normal to the source surface S at position $\mathbf{r}$, ρ_i is the element reflectivity at position $\mathbf{r}$, ΔA is the area of the small reflecting elements, D is the Euclidean distance ($\mathrm{D}=\|\mathbf{r}-\mathbf{r}_s\|$), $\cos\left(\emptyset\right)=\widehat{\boldsymbol{n}}_s\cdot(\mathbf{r}-\mathbf{r}_s)/\mathrm{D}$, $\cos\left(\varphi\right)=\widehat{\boldsymbol{n}}\cdot(\mathbf{r}_s-\mathbf{r})/\mathrm{D}$, $\widehat{\boldsymbol{n}}_s$ is the orientation of the source S, and $\mathbf{r}_s$ is the position of the source.

Assuming perfect synchronization, after the removal of the direct-current bias from $\overline{Z}_i\left(t\right)$, $\overline{Z}_i\left(t\right)$ is down-converted back to the BB by the carrier-frequency vector $\boldsymbol{f_i}$, which is generated using $\boldsymbol{D_{u,i}}$ and $\boldsymbol{k_{i-1}}$ (produced from CP samples during the $(i-1)_{\text{th}}$ frame, see Fig. 5). Then, the low-pass pulse-shaping filter is applied to $\overline{Z}_i\left(t\right)$ for down-sampling and reducing the high-frequency components. For any jamming attacks, as the FH pattern of the jamming signal does not match with the FH pattern, described by $\boldsymbol{f_i}$, that is generated from the proposed scheme, the received jamming signal is shifted to the high frequency regions at the output of the mixer and it will be filtered out by the low-pass pulse-shaping filter of the receiver as shown in figure 5.

We assume that a zero-forcing (ZF) equalizer [62] is used to eliminate the effect of multipath fading. Let $\boldsymbol{h_j}$ be the equivalent discrete-time impulse response ($\boldsymbol{h_j}=h\left(t;\mathrm{S},\mathrm{R}\right)|_{t=jT_s}$), After supplementing zeros to $\boldsymbol{h_j}$ up to N, $\boldsymbol{h_j}=[h_1,h_2,\ldots,h_l,0,0,\ldots,0]$, where l is the maximum path delay, an N-point fast Fourier transform (FFT) can be applied to $\boldsymbol{h_j}$ to obtain the equivalent frequency-domain channel transfer function vector $\boldsymbol{H_n}=[H_1,H_2,\ldots,H_N]$ as follows:

$$H_n=\sum_{j=1}^{N}h_j\cdot e^{\left(-J\frac{2\pi}{N}(n-1)(j-1)\right)}. \tag{30}$$

Let $\boldsymbol{H_n^{-1}}=\left[\frac{1}{H_1},\frac{1}{H_2},\ldots,\frac{1}{H_N}\right]$ be the inverse frequency-domain vector, the impulse response of the equalizer, $\boldsymbol{h_j^{-1}}=\left[h_1^{-1},h_2^{-1},\ldots,h_N^{-1}\right]$ is obtained as follows:

$$h_j^{-1}=\frac{1}{N}\sum_{n=1}^{N}H_n^{-1}\cdot e^{\left(J\frac{2\pi}{N}(n-1)(j-1)\right)}. \tag{31}$$

In case of line-of-sight channel ($\kappa=0$), common case, $\boldsymbol{H_n}$ represents the direct current (DC) gain H_n^0 from transmitting node to receiving node and it is expressed as follows:

$$H_n^0=\frac{(m+1)\,A_{pd}}{2\pi\mathrm{D}^2}\cos^{m}\left(\emptyset\right)\cos\left(\varphi\right). \tag{32}$$

In this case, the impulse response $\boldsymbol{h_j^{-1}}$ can be obtained as

$$h_j^{-1}=\frac{1}{H_n^0}\delta_{k-\frac{D}{C}}. \tag{33}$$

After equalization, the output of a sampled filter is given as

$$\overline{\boldsymbol{Z}}_{\boldsymbol{i}}=r\cdot\overline{\boldsymbol{S}}_{\boldsymbol{i}}+\boldsymbol{h_j^{-1}}\otimes\mathbf{J}+\boldsymbol{h_j^{-1}}\otimes\boldsymbol{n}. \tag{34}$$

The components $\boldsymbol{h_j^{-1}}\otimes\mathbf{J}$ and $\boldsymbol{h_j^{-1}}\otimes\boldsymbol{n}$ have a large impact only at the beginning of $\overline{Z}_{\boldsymbol{i}}$, which can be eliminated by removing the ISI CP samples [27]. Let $\overline{Z}_{i,m,j}$ be the sampled filter output at the j_{th} hopping period, for $m=1,\ldots,N_c$, the received symbol can be expressed as

$$\overline{Z}_{i,m,j}=r\cdot\alpha_{m,j}\overline{S}_{i,j}+\beta_{m,j}\mathrm{j}_{m,j}+\sigma_{m,j}, \tag{35}$$

where $\mathrm{j}_{m,j}$ and $\sigma_{m,j}$ represent the jamming interference and the noise after equalization, respectively. $\alpha_{m,j}$, $\beta_{m,j}\in\{0,1\}$ are binary numbers indicating the existence of the transmitted signal and the interference jamming signal, respectively.

If $N_h>1$, the system supports frequency diversity, and the multiple received copies of $\overline{\boldsymbol{S}}_{\boldsymbol{i}}$ are combined to produce the OFDM signal $\overline{\boldsymbol{Z}}_{\boldsymbol{i}}$, as follows:

$$\overline{\boldsymbol{Z}}_{\boldsymbol{i}}=r.\sum_{j=1}^{N}\sum_{m=1}^{N_c}\left(\alpha_{m,j}\overline{S}_{i,j}+\beta_{m,j}\mathrm{j}_{m,j}+\sigma_{m,j}\right). \tag{36}$$

The components $\mathrm{j}_{m,j}$ and $\sigma_{m,j}$ are very small compared with $\overline{S}_{i,j}$ owing to the low-pass filtering and the requirement of illumination, respectively. After $\overline{\boldsymbol{Z}}_{\boldsymbol{i}}$ is received, the samples are de-permuted by the scrambling matrix $\boldsymbol{M_{z,i}}$ generated from $\boldsymbol{D_{z,i}}$, as follows:

$$\boldsymbol{Z_i}=\boldsymbol{M_{z,i}^{T}}\overline{\boldsymbol{Z}}_{\boldsymbol{i}}, \tag{37}$$

where $\boldsymbol{M_{z,i}^{T}}$ is the transpose of $\boldsymbol{M_{z,i}}$, $\boldsymbol{Z_i}$ is the received de-permuted OFDM signal at the i_{th} frame. This signal consists of an OFDM data signal $\boldsymbol{Z_i^d}$ and a CP signal $\boldsymbol{Z_i^c}$. The protected CP samples of $\boldsymbol{Z_i^c}$ are exploited to generate the CP key $\boldsymbol{k_i}$ that is used to decrypt and de-spread the received OFDM signal $\overline{Z}_{i+1}\left(t\right)$ at the $(i+1)_{\text{th}}$ frame. After $\boldsymbol{k_i}$ is generated, $\boldsymbol{Z_i^c}$ is removed, and $\boldsymbol{Z_i^d}$ is added to the FFT to generate the phase-scrambled signal $\overline{\boldsymbol{Y}}_{\boldsymbol{i}}$, which is the received version of $\overline{\boldsymbol{X}}_{\boldsymbol{i}}$. This signal is de-scrambled using both the key $\boldsymbol{k_{i-1}}$ generated from the CP samples $\boldsymbol{Z_{i-1}^c}$ during the $(i-1)_{\text{th}}$ frame and $\boldsymbol{c_i}$ generated from $\boldsymbol{D_{y,i}}$ using the binarization operation (see (14) and (18)), as follows:

$$\widehat{\boldsymbol{Y}}_{\boldsymbol{i}}=\overline{\boldsymbol{Y}}_{\boldsymbol{i}}\circ\boldsymbol{c_i}\circ\boldsymbol{k_{i-1}}, \tag{38}$$

where $\widehat{\boldsymbol{Y}}_{\boldsymbol{i}}$ is the output of the phase-scrambling operation and is the received version of $\widehat{\boldsymbol{X}}_{\boldsymbol{i}}$. The symbols of $\widehat{\boldsymbol{Y}}_{\boldsymbol{i}}$ are then de-permuted by the scrambling matrix $\boldsymbol{M}_{\boldsymbol{x},\boldsymbol{i}}$ generated from $\boldsymbol{D}_{\boldsymbol{x},\boldsymbol{i}}$ as follows:

$$\boldsymbol{Y}_{\boldsymbol{i}} = \boldsymbol{M}_{\boldsymbol{x},\boldsymbol{i}}^{\boldsymbol{T}} \widehat{\boldsymbol{Y}}_{\boldsymbol{i}}, \tag{39}$$

where $\boldsymbol{M}_{\boldsymbol{x},\boldsymbol{i}}^{\boldsymbol{T}}$ is the transpose of $\boldsymbol{M}_{\boldsymbol{x},\boldsymbol{i}}$, $\boldsymbol{Y}_{\boldsymbol{i}}$ is the de-permuted frequency-domain OFDM signal, which is the received version of $\boldsymbol{X}_{\boldsymbol{i}}$. Finally, a QAM demodulator is applied to $\boldsymbol{Y}_{\boldsymbol{i}}$ for recovering the information data.

The total key space of the introduced method can be computed as follows. The time/frequency domain permutations of OFDM symbols will produce two separate key space of $N!$ and $N_f!$, the chaotic phase scrambling of frequency-domain OFDM symbols can produce another key space of 10^{15}, and the chaotic spreading codes for FH will increase the key space by a factor of N_c. Suppose $N_d = 512$, $l_I = l_p = \frac{N_d}{8}$, $N = (N_d + l_I + l_p) = 640$, $N_f = \frac{N_d}{2} = 256$, and $N_c = 64$, a total key space of $(N! \times N_f! \times N_c \times 10^{15} = 640! \times 256! \times 64 \times 10^{15} \sim 10^{2043})$ is achieved. Since the present fastest computing speed is $3.18 \times 10^{17} 1/s$ [46], it takes $\sim 10^{2017}$ years to obtain the user data, which reveals that the introduced method supports high security against any type of brute-force attack.

V. THE SECURITY PERFORMANCE OF THE PROPOSED METHOD

The security of our method can be evaluated quantitatively by obtaining the information leakage. According to [31] and [65], the information leakage, assuming that each transmitted bits '0' and '1' are equally likely, is calculated as

$$\begin{aligned} L &= I\left(V^E; U^T\right) \\ &= H(V^E) - H(V^E|U^T), \\ &= 1 + P_e \log_2 P_e + (1 - P_e) \log_2 (1 - P_e), \end{aligned} \tag{40}$$

where U^T is the data transmitted by the transmitter, V^E is the data retrieved by the eavesdropper, P_e implies the bit-error-rate (BER) of the eavesdropper, I is the mutual information, and H is the operation of entropy. Subsequently, we attain the secrecy capacity of data with our method as

$$\begin{aligned} C_d &= max[I(U^T; V^r) - I(U^T; V^E)] \\ &\geq H(V^r) - H(V^r|U^T) - \left(H(V^E) - H(V^E|U^T)\right) \\ &= P_r \log_2 P_r + (1 - P_r) \log_2 (1 - P_r) - P_e \log_2 P_e \\ &\quad - (1 - P_e) \log_2 (1 - P_e), \end{aligned} \tag{41}$$

where V^r is the data retrieved by the legitimate receiver and P_r implies the BER of the legitimate receiver. In [30], the CP keys are found to have equal probability of bits on an average. Thus, the secrecy capacity of the CP keys is obtained as

$$\begin{aligned} C_k &= KMR_r \log_2 KMR_r + (1 - KMR_r) \\ &\quad \cdot \log_2 (1 - KMR_r) - KMR_e \log_2 KMR_e \\ &\quad - (1 - KMR_e) \cdot \log_2 (1 - KMR_e), \end{aligned} \tag{42}$$

where KMR_r and KMR_e are the key-mismatch rate of the CP keys at the legitimate receiver and eavesdropper respectively.

VI. COMPLEXITY REDUCTION AND INTERNET-OF-THINGS (IoT) APPLICATIONS

IoT machines are amongst the communication structures that are not supplied with processors that can carry out processes that involve very complicated computations and significant time delays. IoT machines utilized in areas like smart homes, smart buildings, smart healthcare, ...etc., are typically wireless sensors that connect to servers. Encrypting information picked up by these sensors is a critical issue as the communication channel from the sensor to the database server is possibly susceptible to eavesdropping particularly in a wireless scenario. Nevertheless, traditional standard encryption methods, like the Advanced Encryption Standard (AES), cannot be employed in IoT applications because of their disadvantages that do not fit the restricted memory and computational capacities of IoT machines [66]. These challenges can be met by suggesting lightweight encryption methods for these resource-restricted machines (see e.g., [67]–[72]). As an example, Matalgah and Magableh [72] suggested to utilize the conventional encryption simply for the first block of data in a particular frame (or superframe) being sent. All the residual information in the frame is sent securely through the wireless channel without the requirement to utilize strong conventional encryption. This method has been shown to attain lower complexity and higher data transmission rates.

In our method, the complexity comes from the operations of generating secret (CP) keys, $\boldsymbol{k}_{\boldsymbol{i}}$, from the OFDM samples and the signal processing accompanying it that are implemented each frame throughout the entire session for the purpose of dynamic cyphertexts generation, as shown in Fig. 5. To reduce the complexity for lightweight encryption, the CP key can be generated once every several frames, e.g. every $T_k = 10, 20, \ldots, 100$ frames, etc., instead of every frame throughout the session depending on the computational capabilities of IoT devices, where T_k is the period of the CP key generation. The period T_k can be exchanged securely between transmitter and receiver at the connection setup to further enhance the security. This modified method can reduce the processing time delay and complexity, leading to improving the throughput of the communication system. In addition, the hopping rate can be reduced, e.g. several OFDM symbols are transmitted by one frequency hop, according to the computational capabilities of IoT devices. This leads to reducing the computational complexity and relaxing the synchronization at the receiver with the incoming signals. Preamble sequence inserted in time-domain and pilot subcarriers inserted in frequency-domain can be used for synchronization and channel estimation.

Ignoring the complexity that comes during the periods of CP key generation, the method only involves a two-matrix multiplication to accomplish the frequency/time permutations besides the IFFT, phase scrambling, and FH operations. The IFFT requires $\frac{N_d}{2} \log_2 N_d$ complex multiplication and $N_d \log_2 N_d$ complex addition, the frequency and time permutation require N_f and N_d interleaving respectively,

the phase scrambling requires N_f complex multiplication, and the FH requires $\ell N_d N_h$ multiplication. Therefore, the total complexity is $\left(\frac{N_d}{2}\log_2 N_d + N_f + \ell N_d N_h\right)$ multiplication, $\left(N_d \log_2 N_d\right)$ addition, and $\left(N_f + N_d\right)$ interleaving operations.

Besides the complexity reduction, the low-complexity method has the following properties:

- In terms of KPAs and CPAs, it has lower security than the introduced method shown in Fig. 5. However, since it still generates dynamic cyphertexts every T_k frames associated with the random input data, it supports higher security than the methods in [33]–[37] that provide static chaotic keys with statistical characteristics that are helpful for the malicious nodes. The generation of dynamic cyphertexts by this method can destroy this type of statistics. Therefore, the low-complexity method provides the capability against KPAs and CPAs.
- It is an adaptable method. The parameters T_k and T_h can be adapted according to the computational capabilities of IoT devices, throughput needs, and security requirements in the communication environment.

A comprehensive study on the area of IoT applications is out of scope of this paper and is left for a future work.

VII. RESULTS

A Monte Carlo simulation was performed for designing our hyperchaos-BB-FH-OOFDM method, as shown in Fig. 5. We used 32-QAM as a modulation technique; $l_I = l_p = \frac{N_d}{8}$ for the ISI and protected CP samples, respectively ;$N_d = 512$; Reed Solomon coding $RS(16, 8)$ as a channel-coding method for protecting the CP secret key $\boldsymbol{k_i}$; and $N_c = 64$ channels with carrier frequencies of {10, 12, 14, . . . , 132, 134, and 136} MHz, in accordance with [39]. We selected the square-root-raised-cosine filter as the pulse-shaping and matched filters at the transmitter and receiver with a roll-off factor of 0.2, a filter span of 8 samples, and a gain of 0.3578. The multipath VLC channel was modeled as in [64]. The room dimensions were 5m × 5 m × 3 m, with reflection coefficients of 0.8, 0.8, and 0.3 for the walls, ceilings, and floor, respectively, and the maximum order of reflection is 3. The center of the room was given by the coordinate (2.5, 2.5). A ZF equalizer at the receivers was used to relieve the multipath fading.

Fig 6 shows the simulation of the bit-error rate (BER) performance of our hyperchaos-BB-FH-OOFDM method using the phase-scrambling operation (the operation proposed in this work), and using polarity scrambling, i.e., the scrambling operation employed in [27]–[32]. The results were compared with those of conventional BB-FH-OOFDM. i.e. the method in [52] but with using optical OFDM, such as DCO-OFDM [73], instead of the ordinary OFDM [74]. In the simulation, we used one legitimate transmitter at (2.5, 2.5, 3) with a half-power semi-angle of 70° and a power of 1 W, one legitimate receiver at (1.5, 1.5, 0) with a half-angle *FOV* of 85°, and one jammer at (1.5, 1.5, 3) with a half-power semi-angle of 70°.

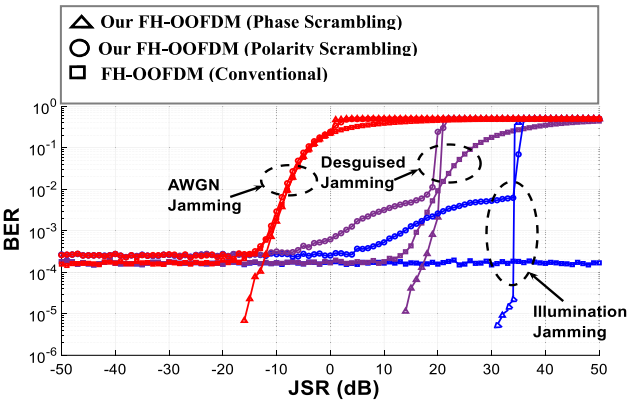

FIGURE 6. BER of the hyperchaos-BB-FH-OOFDM with phase scrambling (this work) and polarity scrambling [29] operations, for $N_h = 2$.

Illumination, disguised, and noise (AWGN) jamming were considered in the simulation. The jammer existed by itself or as a virtual source at (1.5, 1.5, 3). The virtual source can be created by a jammer with a directed NLOS configuration, as shown in Fig. 1.

The jammer used a chaotic generator with the same hop rate as the legitimate transmitter for hopping randomly among the 64 channels. The power of the jammer was adjusted in which the ratio of the transmitted jamming signal power to the legitimate signal power (*JSR*) was changed from −50 to 50 dB and the signal-to-noise ratio E_b/N_0 was 30 dB. As shown in Fig. 6, the performance of hyperchaos-BB-FH-OOFDM with phase scrambling was better than that of hyperchaos-BB-FH-OOFDM with polarity scrambling in all *JSR* regions owing to the distortion of the time-domain OFDM subcarriers in the case of polarity scrambling. Additionally, Fig. 6 shows that the performance of hyperchaos-BB-FH-OOFDM with phase scrambling was better than that of conventional BB-FH-OOFDM in some ranges of *JSR* values, because of the scrambling. When the *JSR* value exceeded a high specific value depending on the type of jamming (1 dB in the case of noise jamming, 20 dB in the case of disguised jamming, and 34 dB in the case of illumination jamming), the key-mismatch rate (KMR) of the CP keys between the transmitting and receiving nodes became higher than zero, as shown in Fig. 7. Consequently, the BER of hyperchaos-BB-FH-OOFDM suddenly increased to approximately 0.5, as shown in Fig. 6. In the case of noise jamming, the hyperchaos-BB-FH-OOFDM approximately followed the conventional method for KMR > 0. For disguised and illumination jamming, for KMR > 0, the performance of our method was worse than that of the conventional one. Although the conventional BB-FH-OOFDM is more robust than our hyperchaos-BB-FH-OOFDM in the very high *JSR* region for disguised and illumination jamming, it is vulnerable to several confidential attacks, such as correlation attacks, KPAs, and CPAs. The exploitation of the random feature of input data (OFDM samples) to generate secret keys, i.e., our hyperchaos-BB-FH-OOFDM method, can provide high confidentiality against such attacks [29], [31], [75].

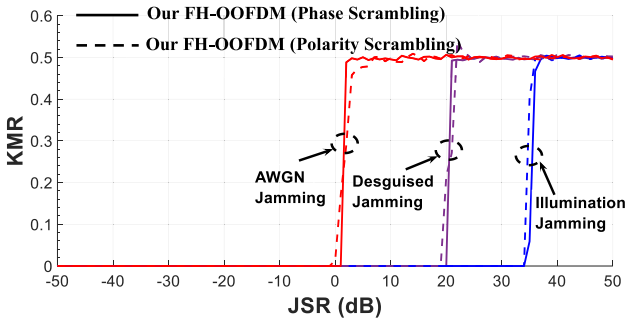

FIGURE 7. KMR of the hyperchaos-BB-FH-OOFDM with phase scrambling (this work) and polarity scrambling [29] operations at the session phase, for $N_h = 2$.

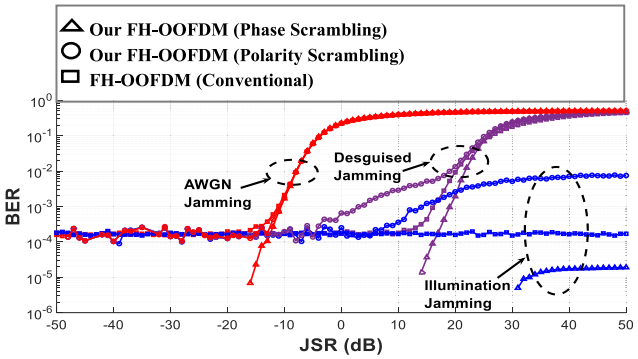

FIGURE 8. BER of the independent-input hyperchaos-BB-FH-OOFDM with phase scrambling (this work) and polarity scrambling [29] operations, for $N_h = 2$.

Furthermore, because the optical channel is visible, the very high jamming power is easily detected by the user. Thus, the user can change his/her location or even locate the jamming node to turn it off. Another technique, our hyperchaos-BB-FH-OOFDM in Fig. 5 can work independently of the input (CP samples). The method can only use the secret quantities generated from the hyperchaotic scheme for encrypting and spreading the signals in the very high *JSR* scinareo. In this case, the CP samples are not required to generate CP keys for the phase scrambling and spreading operations. As shown in Fig. 8, hyperchaos-BB-FH-OOFDM with phase scrambling outperforms either hyperchaos-BB-FH-OOFDM with polarity scrambling or the conventional BB-FH-OOFDM at all *JSR* regions especially at illumination jamming.

Fig. 9 shows the performance of the OOFDM method, where no FH was utilized, with both phase and polarity scrambling. As shown, compared with hyperchaos-BB-FH-OOFDM, OOFDM was defenseless to jamming attacks. This indicates that the proposed hyperchaos-BB-FH-OOFDM improves the availability against malicious jamming.

Figs. 10 (a) and (b) show the simulation results for the performance of our hyperchaos-BB-FH-OOFDM and OOFDM with both phase and polarity scrambling, as well as the conventional BB-FH-OOFDM, in a multi-user scenario. In this simulation, a transmitter was equipped with four LEDs located at $(2, 2, 3)$, $(2, 3, 3)$, $(3, 2, 3)$, and $(3, 3, 3)$. We assumed that each LED emitted at the same wavelength

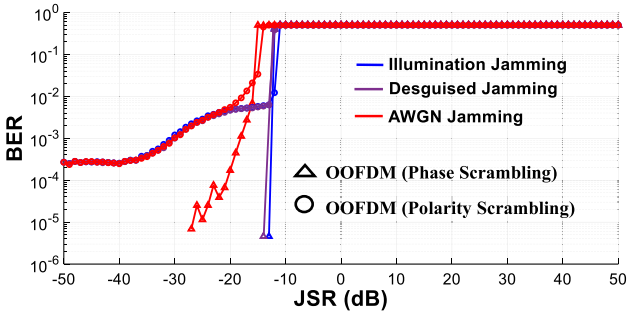

FIGURE 9. BER of the OOFDM without FH and with phase scrambling (this work) and polarity scrambling [29] operations, for $N_h = 2$.

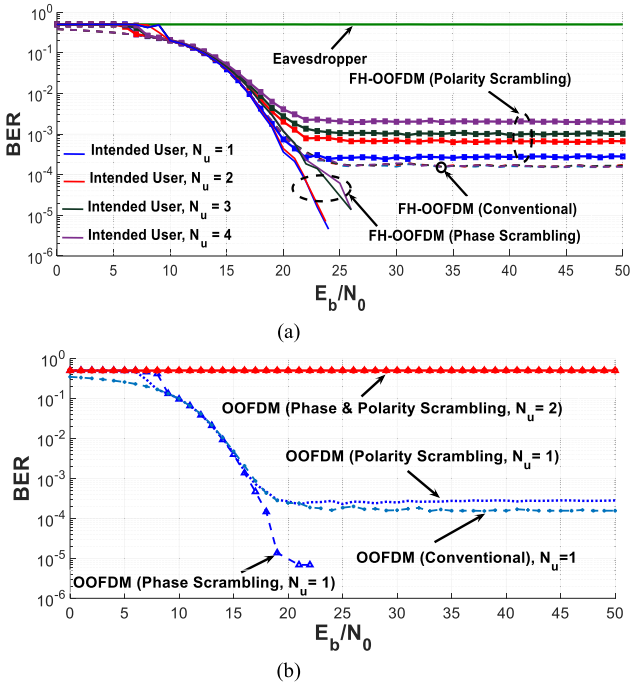

FIGURE 10. Performance of (a) hyperchaos-BB-FH-OOFDM and (b) OOFDM without FH, in the multi-user case at the session phase, for 32-QAM and $N_h = 1$. Here, N_u represents the number of users.

and color, with a half-power semi-angle of 70°. We assumed four users located at $(2.5, 2.5, 0)$, $(2, 3, 0)$, $(3, 2, 0)$, and $(3, 3, 0)$ with a half-angle *FOV* of 85°. Each user was served by an independent LED. Figs. 10 (a) and (b) show the performance of "user 1" located at $(2.5, 2.5, 0)$, which was the "worst-case" position, served by the source located at $(2, 2, 3)$.

As shown in Fig. 10 (a), the FH-OOFDM methods for user 1 relieved the interference effect of the neighboring sources, even if the other three users were active. As shown in Fig. 10 (b), although the OOFDM methods for user 1 outperformed the FH-OOFDM methods in the case of no interference, they could not retrieve the transmitted information when only one other neighboring user was active. This indicates that the FH-OOFDM methods support multiplexing for a VLC system. They support multiple channels in the electrical domain, in addition to the 12 channels provided in the optical domain [76]. Also, Fig. 10 (a) shows that

our hyperchaos-BB-FH-OOFDM with phase scrambling outperformed both the conventional BB-FH-OOFDM (owing to scrambling) and the hyperchaos-BB-FH-OOFDM with polarity scrambling (owing to the distortion of the time-domain OFDM subcarriers when polarity scrambling in the time domain was used instead of phase scrambling in the frequency domain). Fig. 10 (a) also shows the performance of an eavesdropper located at (1.5, 1.5, 0). Because the eavesdropper did not know the secret keys generated from the input data and hyperchaotic scheme, he/she could not retrieve the transmitted information. Fig. 11 shows the constellation diagrams at 30 dB for a transmitted 32-QAM modulated signal, received hyperchaos-BB-FH-OOFDM signals with phase and polarity scrambling at user 1, and a received signal at the eavesdropper. As shown in Figs. 11 (b) and (c), the hyperchaos-BB-FH-OOFDM method with phase scrambling improved the BER performance when compared with the method with polarity scrambling. Also, Fig. 11 (d) shows the eavesdropper could not detect the information data.

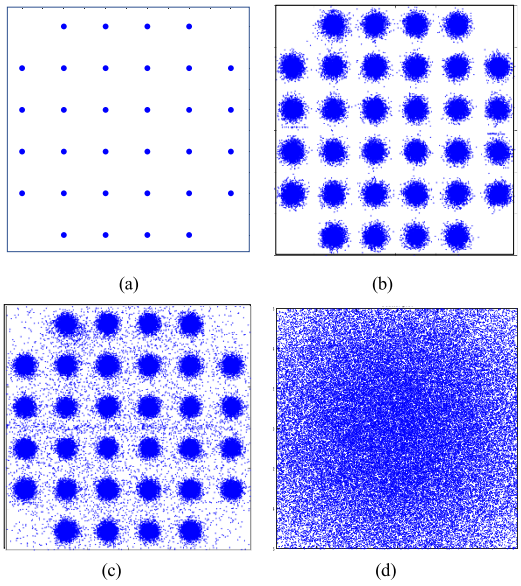

FIGURE 11. Constellation diagrams at 30 dB for (a) transmitted signal, (b) received signal with phase scrambling at user 1, (c) received signal with polarity scrambling at user 1, and (d) received signal at the eavesdropper.

Figs. 12 (a) and (b) show the KMR of the CP keys at "user 1" for our hyperchaos-BB-FH-OOFDM and OOFDM methods at the session phase in the multi-user scenario. As shown in Fig 12 (a), in case of phase scrambling, the hyperchaos-BB-FH-OOFDM method achieved zero KMR at 8 dB and 9 dB with $N_u = 1$ and 4, respectively, and in case of polarity scrambling, it achieved zero KMR at 9 dB and 10 dB with $N_u = 1$ and 4, respectively. From Figs 10 (a) and 12 (a), our hyperchaos-BB-FH-OOFDM method achieved zero KMR before the target performance of the system (i.e., BER of 3×10^{-3} at 20 dB). Thus, in the multi-user case, the legitimate user could retrieve the transmitted data utilizing

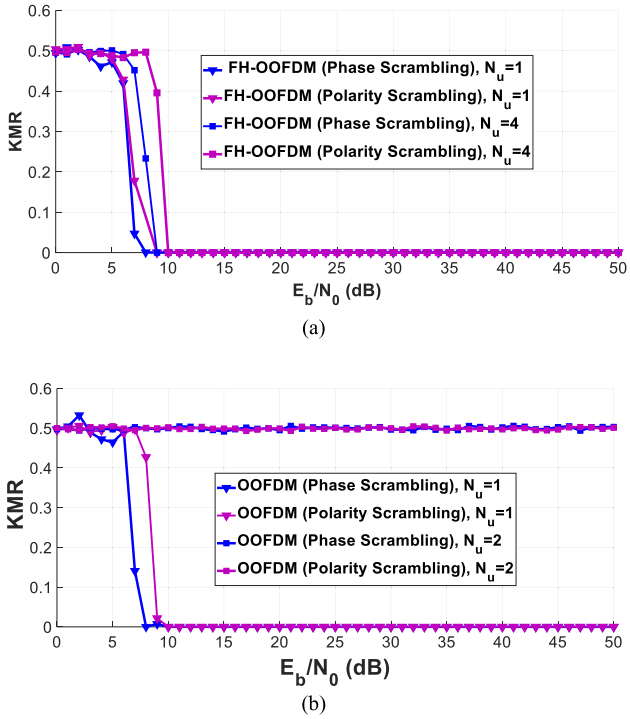

FIGURE 12. KMR of (a) hyperchaos-BB-FH-OOFDM and (b) OOFDM without FH, in the multi-user case at the session phase, for 32-QAM and $N_h = 1$. Here, N_u represents the number of users.

the corresponding decryption keys. From Fig. 12 (b), with $N_u = 1$, OOFDM method achieved zero KMR at 8 dB and 10 dB in case of phase scrambling and polarity scrambling respectively. However, with $N_u = 2$, the KMR of OOFDM was approximately 0.5, the highest probability of error, due to the interference effect from the neighboring channel. From Figs 10 (b) and 12 (b), although the OOFDM achieved zero KMR before the target performance of the system (i.e., BER of 3×10^{-3} at around 15 dB) in the one-user case, it achieved 0.5 KMR in the multi-user case, even with $N_u = 2$. Therefore, in the multi-user case, the legitimate user could not retrieve the transmitted data in case of OOFDM method.

Figs 13 (a) and (b) illustrate the secrecy capacity of data and CP keys at "user 1" in the multi-user scenario. As shown, in case of hyperchaos-BB-FH-OOFDM method with either phase or polarity scrambling, the secrecy capacities C_d and C_k increased with the increase of E_b/N_0 until they reached the maximum value even with $N_u = 4$. In case of OOFDM method with either phase or polarity scrambling and $N_u = 1$, C_d and C_k also increased with the increase of E_b/N_0 and reached the maximum value in a faster manner than hyperchaos-BB-FH-OOFDM method. This is because the BER of the OOFDM is better than that of hyperchaos-BB-FH-OOFDM in the one-user scenario, $N_u = 1$, as shown in Fig. 10. However, in the multi-user scenario, even with $N_u = 2$, no secrecy capacity of data and secret keys was achieved. This is because the BER of OOFDM is high in the multi-user scenario as shown in Fig. 10.

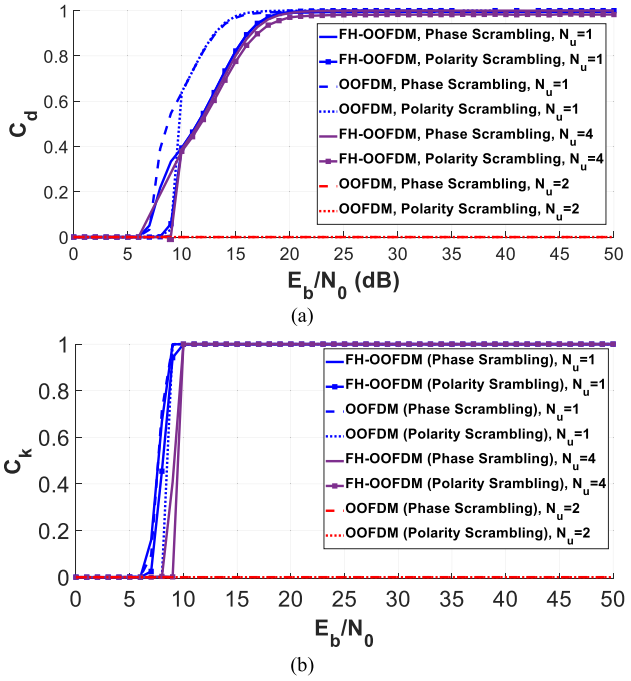

FIGURE 13. Secrecy capacity of (a) data C_d and (b) key C_k.

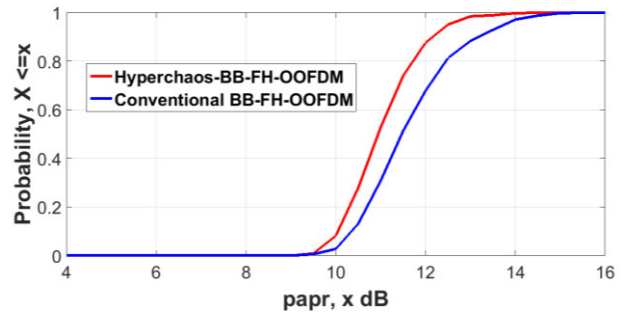

FIGURE 14. PAPR of the BB-FH-OOFDM methods.

The PAPR of the time-domain OFDM signal $\boldsymbol{S_i}$ was computed as

$$PAPR_i = \frac{max_{k=1,\ldots,\ell N} \left|S_{i,k}\right|^2}{\frac{1}{\ell N}\sum_{k=1}^{\ell N}\left|S_{i,k}\right|^2} = \frac{\|\boldsymbol{S_i}\|_\infty^2}{\frac{1}{\ell N}\|\boldsymbol{S_i}\|_2^2}, \qquad (43)$$

According to (4) and (43), high peaks in the time-domain OFDM samples occur when the subcarriers of the frequency-domain OFDM symbols are in-phase or approximately in-phase. Assuming that the original input data are images, the images have a large amount of correlation pixels. After encoding and modulation, there is a high probability that several resultant subcarriers of the frequency-domain OFDM symbols are in-phase or nearly in-phase. Thus, the time-domain signals generated from the conventional OFDM systems have a high PAPR value. With the phase scrambling in the proposed method, the possibility of frequency-domain OFDM subcarriers being in-phase or nearly in-phase is reduced. This leads to a reduction in the PAPR of the time-domain OFDM signal, enhancing the performance of the OFDM system. Fig. 14 shows that our hyperchaos-BB-FH-OOFDM method enhanced the PAPR performance of the signal compared with the conventional BB-FH-OOFDM.

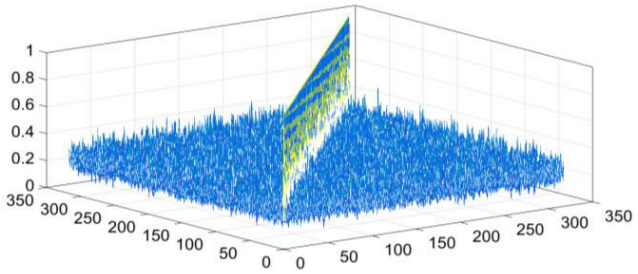

FIGURE 15. Correlation matrix of the CP keys c_i.

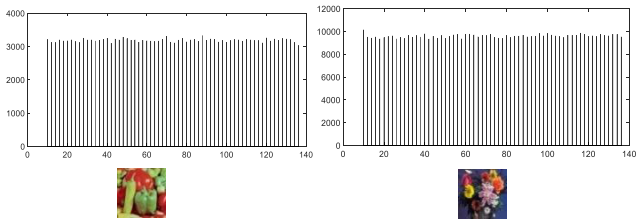

FIGURE 16. Histogram of carrier frequencies from different inputs.

Fig. 15 illustrates the normalized correlation matrix for the 318 dynamic CP keys extracted during the entire session. As shown, a peak of correlation was demonstrated merely among every key and itself, and a slight correlation was observed between the diverse keys. Thus, our method creates uncorrelated keys that are updated at each frame throughout the entire session. Therefore, our method provides strong confidentiality against correlation attacks.

Correlation attacks exploit the statistical weakness of PN and the chaotic generator of conventional FH methods. Fig. 16 presents a histogram of the generated carrier frequencies from our method for different input data. As shown in Fig. 5, from the CP samples and the hyperchaotic scheme, our method generates dynamic cypher keys that are updated at each frame and generates a roughly uniform distribution of FH carrier frequencies during the session as depicted in Fig. 16. Therefore, our method provides high confidentiality against correlation and statistical attacks.

VIII. CONCLUSION

We introduce a hyperchaos-BB-FH-OOFDM method that provides both confidentiality and availability in VLC networks. This method exploits the random characteristics of the input data and chaotic quantities of the hyperchaotic scheme to enhance the confidentiality against correlation and statistical attacks and to enhance the availability against illumination, disguised, and noise jamming. Using the hyperchaotic

scheme, the polarity of bipolar real OFDM samples is exploited to generate dynamic cypher keys and spreading codes. These secret quantities are updated at each frame throughout the entire session, providing high security against malicious attacks. In addition to enhancing the security, our method provides multiplexing, reduces the PAPR of the OFDM signal, and enhances the BER performance for OFDM-based VLC networks. In the future work, we will implement experimentally a hyperchaos-BB-FH-OOFDM system with the capability of enhancing both confidentiality and availability in VLC networks.

ACKNOWLEDGMENT

The authors would like to thank Deanship of Scientific Research (DSR) in King Saud University for funding and supporting this research through the initiative of Graduate Students Research (GSR) Support.

REFERENCES

[1] C. Rohner, S. Raza, D. Puccinelli, and T. Voigt, "Security in visible light communication: Novel challenges and opportunities," *Sensors Transducers*, vol. 192, no. 9, pp. 9–15, Sep. 2015.
[2] G. Blinowski, "Security issues in visible light communication systems," in *Proc. 13th IFAC and IEEE Conf. Program. Devices Embedded Syst.*, vol. 48, Sep. 2015, pp. 234–239.
[3] G. J. Blinowski, "The feasibility of launching rogue transmitter attacks in indoor visible light communication networks," *Wireless Pers. Commun.*, vol. 97, no. 4, pp. 5325–5343, Dec. 2017.
[4] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.
[5] H. Le Minh, A. T. Pham, Z. Ghassemlooy, and A. Burton, "Secured communications-zone multiple input multiple output visible light communications," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2014, pp. 505–511.
[6] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2014, pp. 524–529.
[7] A. Mostafa and L. Lampe, "Pattern synthesis of massive LED arrays for secure visible light communication links," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, Jun. 2015, pp. 1350–1355.
[8] H. Zaid, Z. Rezki, A. Chaaban, and M. S. Alouini, "Improved achievable secrecy rate of visible light communication with cooperative jamming," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Dec. 2015, pp. 1165–1169.
[9] T. V. Pham and A. T. Pham, "On the secrecy sum-rate of MU-VLC broadcast systems with confidential messages," in *Proc. 10th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Jul. 2016, pp. 1–6.
[10] H. Shen, Y. Deng, W. Xu, and C. Zhao, "Secrecy-oriented transmitter optimization for visible light communication systems," *IEEE Photon. J.*, vol. 8, no. 5, pp. 1–14, Oct. 2016.
[11] S. Ma, Z.-L. Dong, H. Li, Z. Lu, and S. Li, "Optimal and robust secure beamformer for indoor MISO visible light communication," *J. Lightw. Technol.*, vol. 34, no. 21, pp. 4988–4998, Nov. 1, 2016.
[12] A. Mostafa and L. Lampe, "Optimal and robust beamforming for secure transmission in MISO visible-light communication links," *IEEE Trans. Signal Process.*, vol. 64, no. 24, pp. 6501–6516, Dec. 2016.
[13] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the secrecy capacity of MISO visible light communication channels," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–7.
[14] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the input distribution and optimal beamforming for the MISO VLC wiretap channel," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Dec. 2016, pp. 970–974.
[15] X. Liu, X. Wei, L. Guo, Y. Liu, and Y. Zhou, "A new eavesdropping-resilient framework for indoor visible light communication," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.
[16] G. Pan, J. Ye, and Z. Ding, "On secure VLC systems with spatially random terminals," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 492–495, Mar. 2017.
[17] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 1, pp. 162–174, Jan. 2018.
[18] X. Zhao, H. Chen, and J. Sun, "On physical-layer security in multiuser visible light communication systems with non-orthogonal multiple access," *IEEE Access*, vol. 6, pp. 34004–34017, Jun. 2018.
[19] Z. Che, J. Fang, Z. L. Jiang, J. Li, S. Zhao, Y. Zhong, and Z. Chen, "A physical-layer secure coding scheme for indoor visible light communication based on polar codes," *IEEE Photon. J.*, vol. 10, no. 5, pp. 1–13, Oct. 2018.
[20] M. Soltani and Z. Rezki, "Optical wiretap channel with input-dependent Gaussian noise under peak- and average-intensity constraints," *IEEE Trans. Inf. Theory*, vol. 64, no. 10, pp. 6878–6893, Oct. 2018.
[21] Z. Chen and X. Wang, "A method for improving physical layer security in visible light communication networks," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2018, pp. 1–5.
[22] J.-Y. Wang, C. Liu, J.-B. Wang, Y. Wu, M. Lin, and J. Cheng, "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6423–6436, Dec. 2018.
[23] T. V. Pham, T. Hayashi, and A. T. Pham, "Artificial-noise-aided precoding design for multi-user visible light communication channels," *IEEE Access*, vol. 7, pp. 3767–3777, 2019.
[24] S. Cho, G. Chen, and J. P. Coon, "Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2633–2648, Oct. 2019.
[25] A. Mukherjee, "Secret-key agreement for security in multi-emitter visible light communication systems," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1361–1364, Jul. 2016.
[26] B. Chen, L. Zhang, and H. Lu, "High security differential chaos-based modulation with channel scrambling for WDM-aided VLC system," *IEEE Photon. J.*, vol. 8, no. 5, pp. 1–13, Oct. 2016.
[27] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Robust key generation from optical OFDM signal in indoor VLC networks," *IEEE Photon. Technol. Lett.*, vol. 28, no. 22, pp. 2629–2632, Nov. 15, 2016.
[28] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Secret key generation protocol for optical OFDM systems in indoor VLC networks," *IEEE Photon. J.*, vol. 9, no. 2, pp. 1–15, Apr. 2017.
[29] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Physical-layer security against known/chosen plaintext attacks for OFDM-based VLC system," *IEEE Commun. Lett.*, vol. 21, no. 12, pp. 2606–2609, Dec. 2017.
[30] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Randomness evaluation of key generation based on optical OFDM system in visible light communication networks," *Electron. Lett.*, vol. 53, no. 24, pp. 1594–1596, Nov. 2017.
[31] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Chaos-based physical-layer encryption for OFDM-based VLC schemes with robustness against known/chosen plaintext attacks," *IET Optoelectron.*, vol. 13, no. 3, pp. 124–133, Jun. 2019.
[32] Y. Al-Moliki, M. Alresheedi, and Y. Al-Harthi, "Design of physical layer key generation encryption method using ACO-OFDM in VLC networks," *IEICE Trans. Commun.*, vol. E103-B, no. 9, pp. 1–10, 2020.
[33] Z. Wang and W. Qiu, "Secure image transmission over DFT-precoded OFDM-VLC systems based on chebyshev chaos scrambling," *Opt. Commun.*, vol. 397, pp. 84–90, Aug. 2017.
[34] Y. B. Yang, C. Chen, W. Zhang, X. Deng, P. F. Du, H. L. Yang, W.-D. Zhong, and L. Y. Chen, "Secure and private NOMA VLC using OFDM with two-level chaotic encryption," *Opt. Express*, vol. 26, no. 26, pp. 34031–34042, Dec. 2018.
[35] Z. Wang, F. Chen, W. Qiu, S. Chen, and D. Ren, "A two layer chaotic encryption scheme of secure image transmission for DCT precoded OFDM-VLC transmission," *Opt. Commun.*, vol. 410, pp. 94–101, Mar. 2018.
[36] M. Gao, C. Li, and Z. Xu, "Performance enhancement of LED-based indoor OFDM-VLC system using digital chaotic scheme," *Opt. Commun.*, vol. 439, pp. 21–26, May 2019.

[37] Z. Wang, Z. Wang, and S. Chen, "Encrypted image transmission in OFDM-based VLC systems using symbol scrambling and chaotic DFT precoding," *Opt. Commun.*, vol. 431, pp. 229–237, Jan. 2019.
[38] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum Communications–A tutorial," *IEEE Trans. Commun.*, vol. 30, no. 5, pp. 855–884, May 1982.
[39] F. Delgado, R. Perez-Jimenez, J. A. Rabadan, and F. J. Lopez-Hernandez, "Design of fast frequency-hopping spread-spectrum system for wireless infrared communications," *Electron. Lett.*, vol. 36, no. 17, pp. 1510–1512, Aug. 2000.
[40] F. Delgado, R. Prez-Jimenez, J. Rabadan, M. A. Bacallado, and F. J. Lopez-Hernandez, "Experimental characterization of a low-cost fast frequency-hopping spread-spectrum system for wireless in-house optical communications," *IEEE Trans. Consum. Electron.*, vol. 48, no. 1, pp. 10–16, Feb. 2002.
[41] J. Choi and E. Hwang, "Secure multiple access based on multicarrier CDMA with induced random flipping," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5099–5108, Jun. 2017.
[42] Q. Ling and T. Li, "Message-driven frequency hopping: Design and analysis," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1773–1782, Apr. 2009.
[43] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping—Part I: System design," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 70–79, Jan. 2013.
[44] Q. Wang, P. Xu, K. Ren, and X.-Y. Li, "Towards optimal adaptive UFH-based anti-jamming wireless communication," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 1, pp. 16–30, Jan. 2012.
[45] J. Sá Sousa and J. P. Vilela, "Uncoordinated frequency hopping for wireless secrecy against non-degraded eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 143–155, Jan. 2018.
[46] Y. Xiao, Z. Wang, J. Cao, R. Deng, Y. Liu, J. He, and L. Chen, "Time-frequency domain encryption with SLM scheme for physical-layer security in an OFDM-PON system," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 10, no. 1, pp. 46–51, Jan. 2018.
[47] 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 Photon. J.*, vol. 12, no. 3, pp. 1–15, Jun. 2020.
[48] Z. Liu, L. Zhang, and Z. Wu, "Reliable and secure pre-coding OFDM-DCSK design for practical cognitive radio systems with the carrier frequency offset," *IEEE Trans. Cognit. Commun. Netw.*, vol. 6, no. 1, pp. 189–200, Mar. 2020.
[49] Z. Liu, L. Zhang, Z. Wu, and J. Bian, "A secure and robust frequency and time diversity aided OFDM–DCSK modulation system not requiring channel state information," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1684–1697, Mar. 2020.
[50] T. Scholand, T. Faber, A. Seebens, J. Lee, J. Cho, Y. Cho, H. W. Lee, and P. Jung, "Fast frequency hopping OFDM concept," *Electron. Lett.*, vol. 41, no. 13, p. 748, 2005.
[51] F. Berens, A. Rüegg, T. Scholand, A. Hessamian-Alinejad, and P. Jung, "Fast frequency hopping diversity scheme for OFDM-based UWB systems," *Electron. Lett.*, vol. 43, no. 1, p. 41, 2007.
[52] Q. Shi, Z. Yang, L. He, and K. Peng, "All digital baseband frequency hopping OFDM system," in *Proc. 11th IEEE Singap. Int. Conf. Commun. Syst.*, Guangzhou, China, Nov. 2008, pp. 661–665.
[53] A. Molisch, J. Foerster, and M. Pendergrass, "Channel models for ultrawideband personal area networks," *IEEE Wireless Commun.*, vol. 10, no. 6, pp. 14–21, Dec. 2003.
[54] J. Ntaganda, E. Ntagwirumugara, and R. Musabe, "Bit error rate mitigation in VANETs using FFH-OFDM pre-coding approach," in *Proc. Int. Conf. Intell. Innov. Comput. Appl. (ICONIC)*, Dec. 2018, pp. 1–8.
[55] M. Cheng, L. Deng, X. Gao, H. Li, M. Tang, S. Fu, P. Shum, and D. Liu, "Security-enhanced OFDM-PON using hybrid chaotic system," *IEEE Photon. Technol. Lett.*, vol. 27, no. 3, pp. 326–329, Feb. 1, 2015.
[56] Y. Wang, Y. Wang, and Q. Shi, "Optimized signal distortion for PAPR reduction of OFDM signals with IFFT/FFT complexity via ADMM approaches," *IEEE Trans. Signal Process.*, vol. 67, no. 2, pp. 399–414, Jan. 2019.
[57] T. Rouphael, "Common digital modulation methods," in *RF and Digital Signal Processing for Software-Defined Radio*. Newnes, NSW, Australia: Elsevier, 2009, ch. 3, pp. 25–85.
[58] B. Liu, L. Zhang, X. Xin, and J. Yu, "Physical layer security in CO-OFDM transmission system using chaotic scrambling," *Opt. Commun.*, vol. 291, pp. 79–86, Mar. 2013.
[59] S. M. Salman and A. A. Elsadany, "On the bifurcation of Marotto's map and its application in image encryption," *J. Comput. Appl. Math.*, vol. 328, pp. 177–196, Jan. 2018.
[60] X. Hu, X. Yang, Z. Shen, H. He, W. Hu, and C. Bai, "Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 27, no. 23, pp. 2429–2432, Dec. 1, 2015.
[61] J. J. Kang and K. C. Teh, "Performance of coherent fast frequency-hopped spread-spectrum receivers with partial-band noise jamming and AWGN," *IEE Proc.-Commun.*, vol. 152, no. 5, pp. 679–685, Oct. 2005.
[62] J. Proakis, *Digital Communications*, 3rd ed. New York, NY, USA: McGraw-Hill, 1995.
[63] Y.-T. Chang, H.-C. Cheng, and Y.-X. Zheng, "Wireless wavelength hopping with AWG/optical switch implemented secure audio/digital signals," in *Proc. 27th Wireless Opt. Commun. Conf. (WOCC)*, Hualien, Taiwan, Apr. 2018, pp. 1–3.
[64] J. R. Barry, J. M. Kahn, W. J. Krause, E. A. Lee, and D. G. Messerschmitt, "Simulation of multipath impulse response for indoor wireless optical channels," *IEEE J. Sel. Areas Commun.*, vol. 11, no. 3, pp. 367–379, Apr. 1993.
[65] H. Li, X. Wang, and Y. Zou, "Dynamic subcarrier coordinate interleaving for eavesdropping prevention in OFDM systems," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1059–1062, Jun. 2014.
[66] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things," *IEEE Security Privacy*, vol. 13, no. 1, pp. 14–21, Jan. 2015.
[67] S. Roy, U. Rawat, and J. Karjee, "A lightweight cellular automata based encryption technique for IoT applications," *IEEE Access*, vol. 7, pp. 39782–39793, 2019.
[68] S.-Y. Tan, K.-W. Yeow, and S. O. Hwang, "Enhancement of a lightweight attribute-based encryption scheme for the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6384–6395, Aug. 2019.
[69] M. A. Habib, M. Ahmad, S. Jabbar, S. H. Ahmed, and J. J. P. C. Rodrigues, "Speeding up the Internet of Things: LEAIoT: A lightweight encryption algorithm toward low-latency communication for the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 7, no. 6, pp. 31–37, Nov. 2018.
[70] V. Dahiphale, G. Bansod, and J. Patil, "ANU-II: A fast and efficient lightweight encryption design for security in IoT," in *Proc. Int. Conf. Big Data, IoT Data Sci. (BID)*, Dec. 2017, pp. 130–137.
[71] S. Koteshwara and A. Das, "Comparative study of authenticated encryption targeting lightweight IoT applications," *IEEE Des. Test.*, vol. 34, no. 4, pp. 26–33, Aug. 2017.
[72] M. M. Matalgah and A. M. Magableh, "Simple encryption algorithm with improved performance in wireless communications," in *Proc. IEEE Radio Wireless Symp.*, Jan. 2011, pp. 215–218.
[73] S. D. Dissanayake and J. Armstrong, "Comparison of ACO-OFDM, DCO-OFDM and ADO-OFDM in IM/DD systems," *J. Lightw. Technol.*, vol. 31, no. 7, pp. 1063–1072, Apr. 2013.
[74] L. L. Hanzo, M. Münster, B. J. Choi, and T. Keller, "OFDM system design," in *OFDM and MC-CDMA for Broadband Multi-User Communications, WLANs and Broadcasting*. 2003, ch. 2, pp. 21–49.
[75] X. Yang, Z. Shen, X. Hu, and W. Hu, "Chaotic encryption algorithm against chosen-plaintext attacks in optical OFDM transmission," *IEEE Photon. Technol. Lett.*, vol. 28, no. 22, pp. 2499–2502, Nov. 15, 2016.
[76] L. Cui, Y. Tang, H. Jia, J. Luo, and B. Gnade, "Analysis of the multichannel WDM-VLC communication system," *J. Lightw. Technol.*, vol. 34, no. 24, pp. 5627–5634, Dec. 15, 2016.

YAHYA M. AL-MOLIKI received the B.Sc. degree in electrical engineering from Sana'a University, Sana'a, Yemen, in 2007, the M.Sc. degree (Hons.) in engineering from the University of Malaya, Malaysia, in 2012, and the Ph.D. degree in electrical engineering from King Saud University, Riyadh, Saudi Arabia, in 2019. His research interests include physical-layer security for indoor VLC networks and OFDM-based optical systems.

MOHAMMED T. ALRESHEEDI received the B.Sc. degree (Hons.) in electrical engineering from King Saud University, Riyadh, Saudi Arabia, in 2006, and the M.Sc. degree (Hons.) in communication engineering and the Ph.D. degree in electronic and electrical engineering from Leeds University, U.K., in 2009 and 2014, respectively. He is currently an Associate Professor with the Electrical Engineering Department, King Saud University. His research interests include adaptation techniques for OW, OW systems design, indoor OW networking, and visible-light communications.

YAHYA AL-HARTHI received the B.Sc. degree from the King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, in 2000, the M.Sc. degree from The George Washington University, Washington, DC, USA, in 2002, and the Ph.D. degree from the University of Minnesota, Minneapolis, MN, USA, in 2005, all in electrical engineering. He is currently an Associate Professor with the Electrical Engineering Department, King Saud University. His research interests lie in the general area of communication theory, with a current focus on wireless ad hoc networks, adaptive modulation schemes, and multiuser and cooperative diversity techniques.