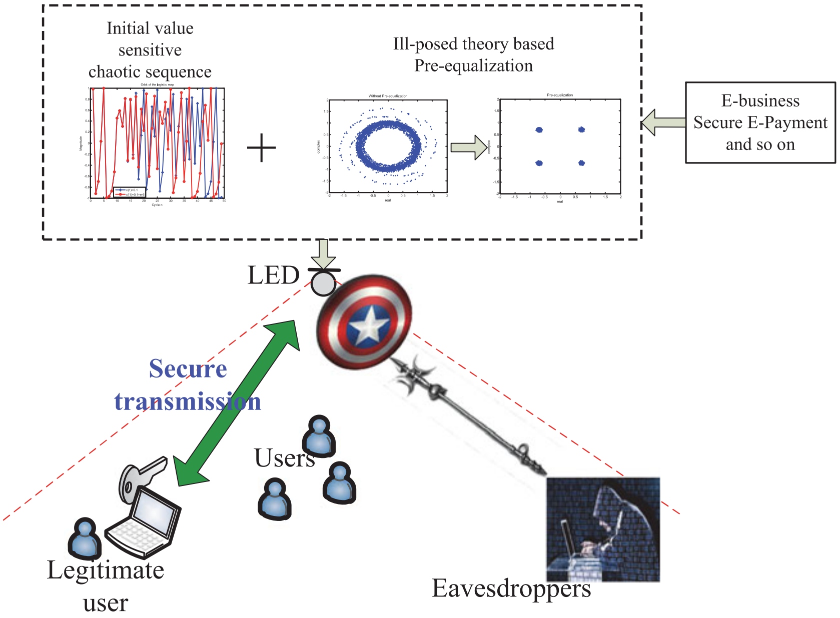
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Design and Analysis of Physical Layer Security Based on Ill-Posed Theory for Optical OFDM-Based VLC System Over Real-Valued Visible Light Channel

Volume 8, Number 6, December 2016

Huaiyin Lu
Lin Zhang, *Member, IEEE*
Wenjun Chen
Zhiqiang Wu, *Senior Member, IEEE*


Initial value sensitive chaotic sequence
+
Ill-posed theory based Pre-equalization
E-business Secure E-Payment and so on
LED
Secure transmission
Users
Legitimate user
Eavesdroppers

DOI: 10.1109/JPHOT.2016.2628800
1943-0655 © 2016 IEEE

Design and Analysis of Physical Layer Security Based on Ill-Posed Theory for Optical OFDM-Based VLC System Over Real-Valued Visible Light Channel

Huaiyin Lu,[1] **Lin Zhang,**[1] ***Member, IEEE*****, Wenjun Chen,**[1]
and Zhiqiang Wu,[2] ***Senior Member, IEEE***

[1]Sun Yat-sen University, Guangzhou 510275, China
[2]Wright State University, Dayton, OH 45435, USA

DOI:10.1109/JPHOT.2016.2628800

Manuscript received July 15, 2016; revised November 8, 2016; accepted November 10, 2016. Date of publication November 15, 2016; date of current version December 6, 2016. This work was supported in part by the National Natural Science Foundation of China under Grant 61602531 and in part by the Science and Technology Program under Project 2014A050503039 of Guangdong Province. Corresponding author: L. Zhang (e-mail: isszl@mail.sysu.edu.cn).

Abstract: Due to the broadcast property of the visible light beam, visible light communication (VLC) systems may suffer from malicious attack or eavesdropping in public area. In this paper, we design and analyze the physical layer security mechanism with the aid of ill-posed theory and present a channel determined subcarrier shifting (CDSS) scheme with pre-equalization. The CDSS scheme exploits the real-valued and location-sensitive channel state information (CSI) of VLC channel and performs sorting operations on the CSI, which formulates a shifting matrix with the aid of chaotic sequences, to dynamically change the available subcarrier for the optical orthogonal frequency division multiplex (OOFDM) aided VLC system. Meanwhile, we combine the CDSS scheme with the preequalization module to further improve the bit error rate (BER) performance for legitimate users. Moreover, the analytical physical layer security model for VLC system is presented using ill-posed theory, which removes the requirements of known CSI and worse channel quality of malicious users when evaluating secrecy capacity. Theoretical and simulation results are provided and compared to prove the benefits achieved by the proposed CDSS scheme, which can enhance the security with no loss of BER, while the secrecy capacity performances are also evaluated to verify the effectiveness of our design.

Index Terms: Optical orthogonal frequency division multiplex (OOFDM)-based visible light communication (VLC), physical layer security, ill-posed theory, real-valued channel state information (CSI), subcarrier shifting, chaotic sequence, pre-equalization.

1. Introduction

Visible light communication (VLC) is a newly developed wireless high-speed data communication technology, which modulates electrical signals to visible light waves with the aid of light emitting diodes (LEDs) as transmitter. Operating over broadband visible light beam, VLC can be further combined with optical orthogonal frequency division multiplex (OOFDM) to provide even higher data rate for the users [1]–[4].

Compared with traditional radio frequency (RF) based systems where signals may penetrate obstacles and thus be easily intercepted by malicious users, VLC's line-of-sight (LOS) transmission property offers a naturally improved security. However, the VLC channel is still of broadcast nature and the interception of the optical signals transmitted in VLC is also possible. That makes VLC links inherently susceptible to eavesdropping by unintended or unauthorized users having access to the physical area illuminated by the data transmitters [5]–[7]. Typical scenarios include public areas such as meeting rooms, libraries, shopping malls etc.

Recently, research has been done in improving physical layer security of VLC system. Rohner *et al.* [8] investigate the issue of security in VLC and outline the research achievements. Sun *et al.* [9] improve secrecy capacity by using orbital angular momentum multiplexing in weak and medium turbulence regimes. Chow *et al.* [10] propose and demonstrate a secure VLC system using data superposition of different LEDs and create a secure VLC zone. Lopez-Martinez *et al.* [11] discuss the implications of physical layer security in the context of free-space optical communications, using the probability of strictly secrecy capacity as performance metric.

Although the secrecy capacity presented by Wyner [12] has been widely exploited for analyzing and improving the security of VLC system [5]–[7], the secrecy capacity evaluation requires that channel state information (CSI) from both legitimate and illegitimate receivers is known to the system, and that the channel quality associated with legitimate receivers should be better than that with eavesdroppers, which may not be always satisfied in practical systems and, therefore, constrains the applicable scope of the secrecy capacity.

On the other hand, little research has been found on combining the physical layer security design with the real-valued transmission over VLC channel. It is well known that due to use of LED, only real-valued signal can be transmitted over the light beam. Compared with the traditional RF channel with complex channel gain coefficient, the real-valued CSI can be sorted, which can be used to scramble the information transmitted. Moreover, considering that CSI information may vary slowly due to the limited coverage of VLC system, we propose to combine the real-valued CSI with chaotic sequences to further improve the security because chaotic sequences also have real value and provides naturally high security due to the property of being sensitive to the initial value and non-periodic, etc. [13].

In order to analyze the security performance, except for the secrecy capacity, recently ill-posed theory has been used for the security performance analysis [14], [15]. Particularly, it may also be applicable to the scenarios where the requirements mentioned above cannot be satisfied. Based on the ill-posed theory, the issue of physical layer security is modelled as the problem of ill-posed equations, and it is naturally required that the system should provide a stable and unique solution for the legitimate receiver, but at the same time unstable and/or non-unique solutions or even unavailable for the malicious users.

Against this background, the main contributions of this paper are that we propose to sort the real-valued CSI of VLC channel, and present the channel determined subcarrier shifting (CDSS) scheme with the aid of pre-equalization for OOFDM-based VLC system. The shifting matrix is determined by the location-sensitive real-valued CSI and the initial value sensitive chaotic sequences, while the security performance analysis is more practical due to the removal of the requirements of known CSI and worse channel quality of malicious channels.

Specifically, with the CDSS scheme, information is modulated at shifted subcarriers according to a shifting matrix determined by sorted real-valued CSI and time varying chaotic sequence, which are transmitted in uncoordinate way [16] to the legitimate users. Since the CSI information is unique for the legitimate users, and only the legitimate users know the key parameters of chaotic sequences transmitted the shared between the transmitters and legitimate receivers, only the legitimate users can retrieve the transmitted information. Furthermore, at the transmitter a pre-equalization module is used, which helps to improve the security performance and to simplify the receiver design, thus improving energy saving for user terminals. With the aid of the proposed CDSS and pre-equalization methods, we contrive a high-security CDSS-VLC design that increases the physical layer security of conventional VLC systems without compromising link bit error rate (BER) performance. Moreover, the issue of physical layer security is modelled as the ill-posed equation, and we propose to exploit the pathological features of redundancy in ill-posed problems for potential

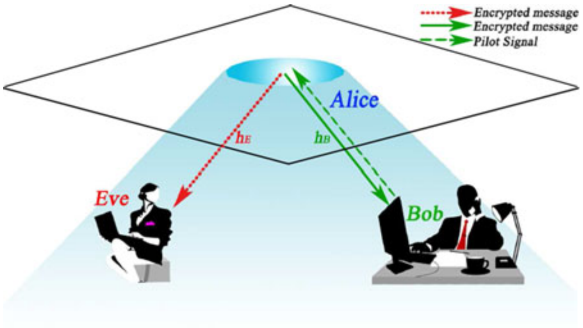


Fig. 1. Model of VLC security communication.

performance enhancement; thus, the requirements of known CSI and worse channel quality from malicious users are removed.

The rest of the paper is organized as follows. We first describe the analytical physical layer security model for OOFDM-based VLC system and the ill-posed theory in Section 2. Then in Section 3, we present details of the proposed CDSS-VLC system including CDSS scheme, pre-equalization scheme, and De-CDSS scheme. In Section 4, we derive the BER expressions, and analyze the security performance of CDSS-VLC system with the aid of the ill-posed theory, notably, we also provide the secrecy capacity performance under the assumption of known CSI to verify the effectiveness of our design. Section 5 provides simulations results of BER and secrecy capacity, and compares them with those in conventional VLC systems. Finally, we conclude our findings in Section 6.

2. Analytic Model for Physical Layer Security in VLC System

2.1. Physical Layer Security Model for VLC System

Fig. 1 illustrates a typical scenario for indoor VLC system security analysis. In this model, Alice is the transmitter, Bob is the legitimate receiver, Eve is the malicious eavesdropper, and they share the same VLC network in public scenario. We assume that Eve's physical location is sufficiently far from Bob's, and thus the VLC channel between Alice and Eve is uncorrelated with that between Alice and Bob.

Assume that there exists only one legitimate receiver, namely Bob, in the VLC system. The signal received by Bob is expressed as

$$\mathbf{r}_{\mathbf{Bob}} = \mathbf{h}_{\mathbf{Bob}}\text{diag}_N(\mathbf{p})\mathbf{x} + \mathbf{n}_{\mathbf{Bob}}, \tag{1}$$

where $\mathbf{h}_{\mathbf{Bob}}$ is the $N \times N$ channel matrix between Alice and Bob, $\mathbf{p}$ is an $N \times 1$ precoding vector for Bob, $\text{diag}_N(\mathbf{p})$ is an $N \times N$ diagonal matrix with its main diagonal entries extracted from vector $\mathbf{p}$, $\mathbf{n}_{\mathbf{Bob}}$ is the additive white Gaussian noise (AWGN) vector with zero mean and a variance of $\frac{N_0}{2}$, $\mathbf{x}$ is the $N \times 1$ signal vector, and N is the inverse fast Fourier transform (IFFT) size for the orthogonal frequency division multiplexing (OFDM) modem. In this paper, we adopt the well known channel model of [17]. On the other hand, the signal received by Eve is

$$\mathbf{r}_{\mathbf{Eve}} = \mathbf{h}_{\mathbf{Eve}}\text{diag}_N(\mathbf{p})\mathbf{x} + \mathbf{n}_{\mathbf{Eve}}, \tag{2}$$

where $\mathbf{h}_{\mathbf{Eve}}$ is the $N \times N$ channel matrix between Alice and Eve, and $\mathbf{n}_{\mathbf{Eve}}$ is the AWGN vector having same statistical properties as $\mathbf{n}_{\mathbf{Bob}}$.

The security performance of the VLC system illustrated in Fig. 1 has been analyzed using the secrecy capacity [5]–[7] presented by Wyner [12]; however, the secrecy capacity evaluation requires that the value of both $\mathbf{h}_{\mathbf{Bob}}$ and $\mathbf{h}_{\mathbf{Eve}}$ is known to Alice and that the channel quality between Alice and Bob should be better that between Alice and Eve, which may not be always satisfied. We here propose to analyze the security performance with the ill-posed theory given as below.

2.2. Review of Ill-posed Theory

If the solution of a problem is unstable, non-unique, or not existing under perturbation on data, it is considered as an ill-posed problem [18]. Assuming that **x** and **b** are $N \times 1$ vectors, while **A** is an $N \times N$ matrix, we have a common expression as

$$\mathbf{A}\mathbf{x} = \mathbf{b} \tag{3}$$

where **b** denotes the observation vector, **x** represents the parameter vector to be calculated, **A** is an operator mapping **x** to **b**. Let B be the space of observation vector and X be the space of parameter vector, respectively. We may calculate **x** by

$$\mathbf{x} = f(\mathbf{b}), \mathbf{b} \in B, \mathbf{x} \in X \tag{4}$$

where $f(\cdot)$ is an operator that maps **b** to **x**. The uniqueness of the solutions for (3) or (4) depends on the singularity of the coefficient matrix as follows:

- *Situation 1 (S1)*: If **A** is singular, then the solution to (3) is not unique or does not exist.
- *Situation 2 (S2)*: If **A** is nonsingular, then the solution to (3) is unique.

According to [18], $S1$ is an ill-posed problem. In $S2$, we may rewrite (4) as

$$\mathbf{x} = \mathbf{A}^{-1}\mathbf{b}, \mathbf{b} \in B, \mathbf{x} \in X. \tag{5}$$

Let $\mathbf{W} = \mathbf{A}^{-1}$, while $\delta\mathbf{b}$ and $\delta\mathbf{W}$ represent small perturbations to **b** and **W**, respectively. Then, if we change **b** to $(\mathbf{b} + \delta\mathbf{b})$ and **W** to $(\mathbf{W} + \delta\mathbf{W})$ in (5), the resultant solution becomes $(\mathbf{W} + \delta\mathbf{W})(\mathbf{b} + \delta\mathbf{b})$. With $(\mathbf{x} + \delta\mathbf{x})$ being the corresponding changed solution, we have

$$\mathbf{x} + \delta\mathbf{x} = (\mathbf{W} + \delta\mathbf{W})(\mathbf{b} + \delta\mathbf{b}). \tag{6}$$

If $\delta\mathbf{x}$ changes dramatically when both $\delta\mathbf{W}$ and $\delta\mathbf{b}$ are small, then the solution is considered as unstable. In this case, $S2$ becomes an ill-posed problem.

In this paper, we are interested in the ill-posed problem, in which the unstable solutions are expected to be provided for the malicious users. That is to say, the malicious users have to retrieve the effective data from the numerous solutions since they could hardly get all the same parameters as the the legitimate users.

The definition of the unstable ill-posed problem is captured below [14].

Definition: Assume that (X, ρ_X) and (B, ρ_B) are spaces of solutions and parameters, respectively, while ρ_X and ρ_B represent the metric operators in X and B which are denoted by $\rho_X{:}X \to R$ and $\rho_B{:}B \to R$, respectively, where R is the space of real numbers. Then, when **A** is nonsingular and the solution to $\mathbf{A}\mathbf{x} = \mathbf{b}$ is unique, for $\forall \varepsilon > 0$, $\exists \delta > 0$, where ε is a small positive real number and δ is any positive real number, we call it an unstable ill-posed problem, if we have

$$\rho_X(\mathbf{x}_1, \mathbf{x}_2) = \|\mathbf{x}_1 - \mathbf{x}_2\| > \delta, \tag{7}$$

where $\mathbf{x}_1, \mathbf{x}_2 \in X$, $\mathbf{A}\mathbf{x}_1 = \mathbf{b}_1$, $\mathbf{A}\mathbf{x}_2 = \mathbf{b}_2$, subjected to

$$\rho_B(\mathbf{b}_1, \mathbf{b}_2) = \|\mathbf{b}_1 - \mathbf{b}_2\| \leq \varepsilon, \mathbf{b}_1, \mathbf{b}_2 \in B. \tag{8}$$

In simple words, the above definition implies that if a small change from $\mathbf{b}_1$ to $\mathbf{b}_2$ would lead to a large change from $\mathbf{x}_1$ to $\mathbf{x}_2$, then it is referred to as an unstable ill-posed problem.

2.3. Ill-posed Problem of Physical Layer Security for VLC channel

As mentioned above, in order to ensure secure signal transmission for legitimate users, it requires that the combination of the channel and the signal processing module constitutes an ill-posed problem.

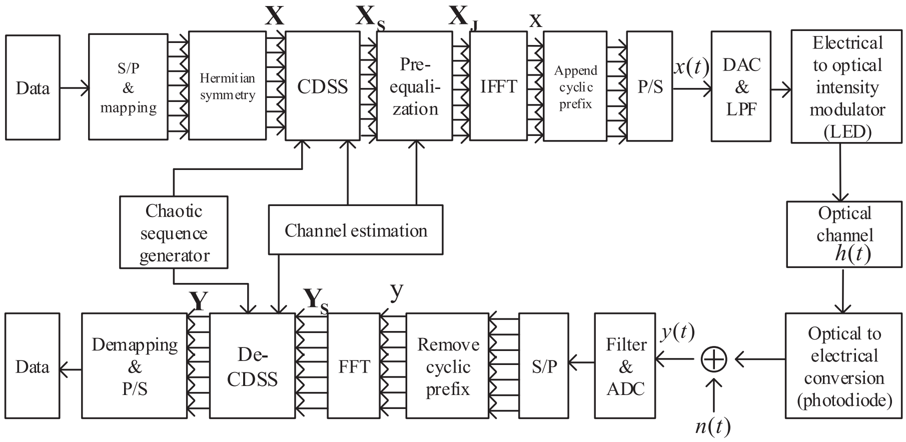


Fig. 2. Proposed CDSS-VLC system model.

Specifically, for combating eavesdroppers, following the ill-posed theory reviewed in Section 2.2, it requires that the equivalent channel between Alice and Eve, namely $\mathbf{h}_{\mathbf{Eve}}\mathrm{diag}_N(\mathbf{p})$, should vary as dramatically and randomly as possible, such that the probability of successful decoding is minimized. Noting (6) and that $\mathrm{diag}_N(\mathbf{p})$ is the solution to (10), we formulate

$$\mathrm{diag}_N(\mathbf{p}) + \Delta\mathrm{diag}_N(\mathbf{p}) = (\mathbf{h}_{\mathbf{Bob}} + \Delta\mathbf{h}_{\mathbf{Bob}})^{-1}(\mathbf{U} + \Delta\mathbf{U}), \tag{9}$$

where $\Delta\mathrm{diag}_N(\mathbf{p})$ denotes a change to $\mathrm{diag}_N(\mathbf{p})$, while $\Delta\mathbf{h}_{\mathbf{Bob}}$ and $\Delta\mathbf{U}$ represent a change to the channel matrix $\mathbf{h}_{\mathbf{Bob}}$ and to the constant matrix $\mathbf{U}$, respectively.

More explicitly, note that $\Delta\mathbf{h}_{\mathbf{Bob}}$ represents the difference between the CSI obtained at the transmitter and that estimated at the receiver. Assuming perfect channel estimation and CSI feedback, we have $\Delta\mathbf{h}_{\mathbf{Bob}} = 0$ for the legitimate users. However, it is difficult for the eavesdroppers to get the exact values of $\mathbf{h}_{\mathbf{Bob}}$ even with perfect CSI estimator and feedback, due to the fact that their physical locations differ from that of the legitimate user. For secure transmissions of legitimate users, based on the ill-posed equations (10) and (9), $\Delta\mathrm{diag}_N(\mathbf{p})$ should change dramatically with the changes of $\Delta\mathbf{h}_{\mathbf{Bob}}$ and $\Delta\mathbf{U}$. That is to say, $\mathrm{diag}_N(\mathbf{p})$ must have a redundant solution set that helps to randomize Eve's received signals and hence favourably formulates an unstable ill-posed problem, as described in *S*2 for eavesdroppers.

On the other hand, for the legitimate channel with known $\mathbf{p}$, it should arrive at

$$\mathbf{h}_{\mathbf{Bob}}\mathrm{diag}_N(\mathbf{p}) = \mathbf{U} \tag{10}$$

where $\mathbf{U}$ is a constant matrix. Referring to (3), we note that (10) constitutes an ill-posed problem from the system design perspective. Assuming that an optical OOFDM system is employed in the VLC system considered, the channel impulse responses (CIR) can be considered as statistically independent [19]–[21]. Then the channel matrix $\mathbf{h}_{\mathbf{Bob}}$ is nonsingular and $\mathrm{diag}_N(\mathbf{p})$ in (10) can be calculated with the aid of (5).

3. CDSS scheme with aid of Pre-equalization Scheme

3.1. Pre-equalization Aided CDSS-VLC System Model

Recall from Section 1 that we propose to enhance the security of VLC system with CDSS scheme with pre-equalization, which exploits the real-valued $\mathbf{h}_{\mathbf{Bob}}$ of VLC channel and the chaotic sequences. As an example application, direct current (DC) biased optical OFDM (DCO-OFDM) [22] is assumed.

As illustrated inFig. 2, at the transmitter side, we apply the CDSS and pre-equalization functions between the Hermitian symmetry and the IFFT modules. The complex data signal stream, which is

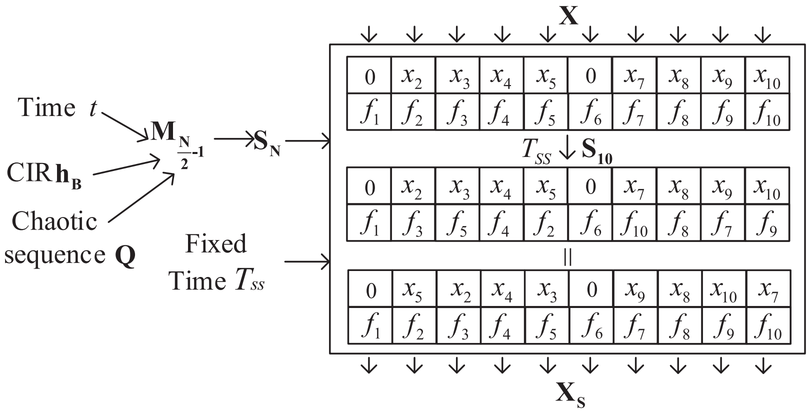

X
Time t
$\mathbf{M}_{\frac{N}{2}-1}$
$\mathbf{S}_N$
CIR $\mathbf{h_B}$
Chaotic sequence $\mathbf{Q}$
Fixed Time T_{ss}
0 x_2 x_3 x_4 x_5 0 x_7 x_8 x_9 x_{10}
f_1 f_2 f_3 f_4 f_5 f_6 f_7 f_8 f_9 f_{10}
T_{SS} $\mathbf{S}_{10}$
0 x_2 x_3 x_4 x_5 0 x_7 x_8 x_9 x_{10}
f_1 f_3 f_5 f_4 f_2 f_6 f_{10} f_8 f_7 f_9
||
0 x_5 x_2 x_4 x_3 0 x_9 x_8 x_{10} x_7
f_1 f_2 f_3 f_4 f_5 f_6 f_7 f_8 f_9 f_{10}
$\mathbf{X_S}$

Fig. 3. Proposed CDSS scheme.

denoted by $\mathbf{X} = [X_0, X_1, \ldots, X_{N-1}]$, is first processed by the CDSS operation, resulting in $\mathbf{X_S}$ as the input to the pre-equalization block, where a pre-equalized complex data signal $\mathbf{X_J}$ will be generated.

Due to the requirement of intensity modulation/direct detection (IM/DD) and LED transmitter, the output signal after IFFT should have real value, hence $\mathbf{X}$ should be Hermitian symmetric and satisfy

$$X_m = X^*_{N-m}, 0 < m < \frac{N}{2} \tag{11}$$

where $(\cdot)^*$ denotes the conjugate operation and we have $X_0 = X_{\frac{N}{2}} = 0$ and N should be an even number. Furthermore, the process of CDSS and pre-equalization must maintain the Hermitian symmetry property, as will be detailed in Sections 3.2 and 3.3, respectively. After IFFT, $\mathbf{X_J}$ is converted to a real signal $\mathbf{x}$. The k^{th} time-domain sample of $\mathbf{x}$ is given by

$$x_k = \frac{1}{N} \sum_{m=0}^{N-1} X_{J,m} \exp\left(\frac{j2\pi km}{N}\right) \tag{12}$$

where $X_{J,m}$ is the sample associated with the m^{th} subcarrier of $\mathbf{X_J}$. After cyclic prefix extension, parallel-to-serial (P/S) conversion, digital-to-analog conversion (DAC) and low pass filtering (LPF), $\mathbf{x}$ is transformed to $x(t)$, as seen in Fig. 2. Following the processes of DC bias addition, zero clipping and electrical-to-optical conversion, the resultant visible light signal is transmitted through a VLC channel.

At the receiver side, after optical-to-electrical conversion, cyclic prefix removal and fast Fourier transform (FFT), the De-CDSS operation is applied to the received signal to generate the complex signal $\mathbf{Y}$ with the aid of the CSI between transmitter and legitimate receiver associated with locally regenerated chaotic sequences. Finally, the transmitted data can be recovered.

3.2. CDSS Design

As mentioned in Section 3.1, the data samples are mapped to the shifted subcarriers designated by the CDSS scheme, which is illustrated in Fig. 3. More specifically, the shifting rule is determined by a shifting matrix based on real-valued CSI between transmitter and legitimate user associated with time-varying chaotic sequence, which can be regenerated at the legitimate receiver for assisting in the subcarrier de-shifting operation. As the CIR can be considered as statistically independent at different receivers [19]–[21], the CSI between transmitter and legitimate user would not be available at the eavesdropper, thus transmission security can be improved compared with systems dispensing with the employment of CDSS.

In practical VLC scenarios, transmit CSI is needed for the CDSS and may be acquired through feedback channels from the receiver, exploiting for example conventional RF techniques or infrared communication in the uplink [23]. For simplicity, in this paper we assume that perfect transmit CSI is available. Let $l_{CP} = l_{ht} < N$, where l_{CP} and l_{ht} are the lengths in terms of samples of cyclic prefix and time-domain CIR, respectively. The CIR between the transmitter and a legitimate user is defined by a $l_{CP} \times 1$ vector as

$$\mathbf{h_B} = [h_{B,0}, h_{B,1}, \ldots, h_{B,l_{CP}-1}]^T \tag{13}$$

where $h_{B,l_{CP}-1}$ denotes the nonzero-gain channel tap associated with the maximum path delay.

The shifting matrix $\mathbf{S_N}$ is applied on the basis of a given time period T_{SS}, where N is the length of $\mathbf{X}$. It is constructed by utilizing a $(\frac{N}{2}-1)\times(\frac{N}{2}-1)$ matrix $\mathbf{M_{\frac{N}{2}-1}}$, which is determined by CIR associated with chaotic sequence. The chaotic sequence is constructed by the chaotic sequence generator, where the easy-to-realize method using a logistic map with control parameter β is adopted, as

$$Q(k) = \beta Q(k-1) - \beta Q^2(k-1), k = 1, 2, \ldots, \tag{14}$$

where $Q(i) \in (0, 1)$ $(i = 0, 1, \ldots)$ is the i^{th} element of $\mathbf{Q}$. In our system, $\beta = 4$ is assumed. Associate with chaotic sequence, the multiplied CIR vector is defined as

$$\mathbf{h_{BM}} = \left[Q(0)\mathbf{h_B}^T, Q(1)\mathbf{h_B}^T, \ldots, Q(i)\mathbf{h_B}^T, \ldots\right]^T. \tag{15}$$

For generating matrix $\mathbf{M_{\frac{N}{2}-1}}$, $\mathbf{h_{BM}}$ is divided into several $(\frac{N}{2}-1)\times 1$ vectors $\mathbf{h_{BM,k}}$

$$\mathbf{h_{BM,k}} = \left[h_{BM}\left(k\left(\frac{N}{2}-1\right)\right), \ldots, h_{BM}\left(k\left(\frac{N}{2}-1\right)+\left(\frac{N}{2}-2\right)\right)\right], k = 1, 2, \ldots \tag{16}$$

where $h_{BM}(i)\,(i = 0, 1, \ldots)$ is the i^{th} element of $\mathbf{h_{BM}}$ and $\mathbf{h_{BM,k}}$ indicates the k^{th} vector used in the k^{th} shifting period.

As the CIR of VLC channels $\mathbf{h_B}$ and chaotic sequence $\mathbf{Q}$ are real-valued, unlike the complex RF channel, here sorting operations are allowed to be performed on $\mathbf{h_{BM,k}}$ in VLC system. Note that in each row and each column of the matrix $\mathbf{M_{\frac{N}{2}-1}}$, there is only one "1" and all other elements are "0." Thus, $\mathbf{M_{\frac{N}{2}-1}}$ in fact exercises a sorting operation on $\mathbf{h_{BM,k}}$ in an ascending order using any sorting algorithm. Without loss of generality, let the $(\frac{N}{2}-1)\times 1$ vector $\mathbf{h_{BMS,k}}$ be the sorted version of $\mathbf{h_{BM,k}}$. Then, $\mathbf{M_{\frac{N}{2}-1}}$ may be seen as a transformed identity matrix and can be calculated as

$$\mathbf{M_{\frac{N}{2}-1}} = f_S\left(\mathbf{h_{BMS,k}}\,[\mathbf{h_{BM,k}}]^{-1}\right) \tag{17}$$

where $[\mathbf{h_{BM,k}}]^{-1} = \left[\frac{1}{h_{BM,k}(1)}, \frac{1}{h_{BM,k}(2)}, \ldots, \frac{1}{h_{BM,k}(\frac{N}{2}-1)}\right]$, and $f_S(\cdot)$ is a function defined by

$$\mathbf{V} = f_S(\mathbf{U}) \rightarrow V_{i,j} = \begin{cases} 1, & \text{if} \quad U_{i,j} = 1 \\ 0, & \quad\;\; \text{else} \end{cases} \tag{18}$$

where the $N \times N$ matrices $\mathbf{V}$ and $\mathbf{U}$ are the output and the input parameters of function f_S, respectively. Then, $\mathbf{S_N}$ may be generated through (17) as

$$\mathbf{S_N} = \begin{bmatrix} 0 & & & \\ & \mathbf{M_{\frac{N}{2}-1}} & & \\ & & 0 & \\ & & & \mathbf{M^R_{\frac{N}{2}-1}} \end{bmatrix} \tag{19}$$

where $\mathbf{M_{\frac{N}{2}-1}}$ and $\mathbf{M^R_{\frac{N}{2}-1}}$ locate at the main diagonal of $\mathbf{S_N}$, and $(\cdot)^R$ denotes the rotating operation defined by

$$\mathbf{Z}^R = \mathbf{RZR} \tag{20}$$

where $\mathbf{Z}$ is the matrix to be rotated, while $\mathbf{R}$ is a $(\frac{N}{2}-1)\times(\frac{N}{2}-1)$ matrix with all elements on its counter diagonal being 1 and is given by

$$\mathbf{R}=\begin{bmatrix} & & 1\\ & \vdots & \\ 1 & & \end{bmatrix}. \tag{21}$$

To elaborate a little further, let us consider an example as follows.

Given $N=10$, $l_{ht}=3$, the chaotic sequence $\mathbf{Q}=[0.80, 0.64]$, and $\mathbf{h_B}=10^{-5}*[0.15, 0.99, 0.45]^T$, we have $\mathbf{h_{BM,1}}=10^{-5}*[0.120, 0.792, 0.360, 0.096]^T$ and $\mathbf{h_{BMS,1}}=10^{-5}*[0.096, 0.120, 0.360, 0.792]^T$ which is sorted on $\mathbf{h_{BM,1}}$ in an ascending order. Then, using (17) and (18), we can get

$$\mathbf{M_4}=\begin{bmatrix} 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 \end{bmatrix}. \tag{22}$$

Hence, $\mathbf{S_{10}}$ can be generated as

$$\mathbf{S_{10}}=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 & 0 & 0 & 0\\ 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 0 & 0 & 0\\ 0 & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 0 & 0 & 0 & 0\\ 0 & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0}\\ 0 & 0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0}\\ 0 & 0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1}\\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}. \tag{23}$$

If the input data stream is $\mathbf{X}=[0, x_2, x_3, x_4, x_5, 0, x_7, x_8, x_9, x_{10}]^T$, where due to Hermitian symmetry we have $x_2=x_{10}^*$, $x_3=x_9^*$, $x_4=x_8^*$, $x_5=x_7^*$, then we arrive at

$$\mathbf{X_S}=\mathbf{S_{10}X}=[0, x_5, x_2, x_4, x_3, 0, x_9, x_8, x_{10}, x_7,]^T, \tag{24}$$

as demonstrated in Fig. 3. Note, particularly that the CDSS-processed data stream $\mathbf{X_S}$ in (24) maintains the Hermitian symmetry property. The general expression of the proposed CDSS procedure can be formulated as

$$\mathbf{X_S}=\mathbf{S_N X}. \tag{25}$$

It is worth pointing out that $\mathbf{h_B}$ can be dynamically updated according to time varying CSI and chaotic sequence $\mathbf{Q}$ can be also dynamically updated, for instance from one shifting period to another through (14), such that the generated shifting matrix $\mathbf{S_N}$ changes accordingly and is therefore not trackable by eavesdroppers. This enhances security for data transmissions. The pattern of $\mathbf{Q}$ for different shifting periods may follow a predefined codebook shared between transmitters and receivers, or may be dynamically signalled to receivers through encrypted control channels.

3.3. Pre-equalization

In order to enhance the security communication without imposing excessive complexity at the receivers, a pre-equalization scheme is employed at the transmitter.

As we define CIR vector $\mathbf{h_B}$ in Section 3.2, after appending zeros to $\mathbf{h_B}$ up to N, N-point FFT can be invoked on $\mathbf{h_B}$, resulting in the corresponding frequency-domain channel transfer function vector

$$\mathbf{H_B} = [H_{B,0}, H_{B,1}, \ldots, H_{B,N-1}]^T. \tag{26}$$

The pre-equalized signal vector $\mathbf{X_J}$ can be generated by

$$\mathbf{X_J} = \mathbf{J X_S} \tag{27}$$

where $\mathbf{X_S}$ is given by (25) and the pre-equalization matrix $\mathbf{J}$ is defined as

$$\mathbf{J} = \text{diag}_N\left(\mathbf{H_B^{-1}}\right) \tag{28}$$

where $\mathbf{H_B^{-1}} = \left[\frac{1}{H_{B,0}}, \frac{1}{H_{B,1}}, \ldots, \frac{1}{H_{B,N-1}}\right]$.

As we discuss in Section 3.2 that both $\mathbf{X_S}$ and $\mathbf{H_B}$ are Hermitian symmetric, $\mathbf{X_J}$ of (27) also fulfils the Hermitian symmetry requirement in OOFDM-VLC systems.

3.4. De-CDSS Procedure

Using the same CSI between transmitter and legitimate receiver as well as chaotic sequences, as shown in Fig. 3, the legitimate receiver is capable of regenerating $\mathbf{M_{\frac{N}{2}-1}}$ according to (17) and (18), and thus recovers the transmitted information. More specifically, the $N \times N$ channel determined subcarrier de-shifting matrix at the legitimate receiver is given by

$$\mathbf{G_N} = \begin{bmatrix} 0 & & & \\ & \mathbf{M_{\frac{N}{2}-1}^{-1}} & & \\ & & 0 & \\ & & & \left(\mathbf{M_{\frac{N}{2}-1}^{-1}}\right)^R \end{bmatrix} \tag{29}$$

where both $\mathbf{M_{\frac{N}{2}-1}^{-1}}$ and $(\mathbf{M_{\frac{N}{2}-1}^{-1}})^R$ are located at the main diagonal of $\mathbf{G_N}$ in a way similar to (19). Using (29), in the same example provided in Section 3.2, we will have the corresponding channel determined subcarrier de-shifting matrix $\mathbf{G_{10}}$ as

$$\mathbf{G_{10}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & 0 & 0 & 0 & 0 \\ 0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ 0 & 0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ 0 & 0 & 0 & 0 & 0 & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix} \tag{30}$$

which is then exploited to facilitate the channel determined subcarrier de-shifting operation on the received signal at the legitimate receiver, as exemplified in Fig 4.

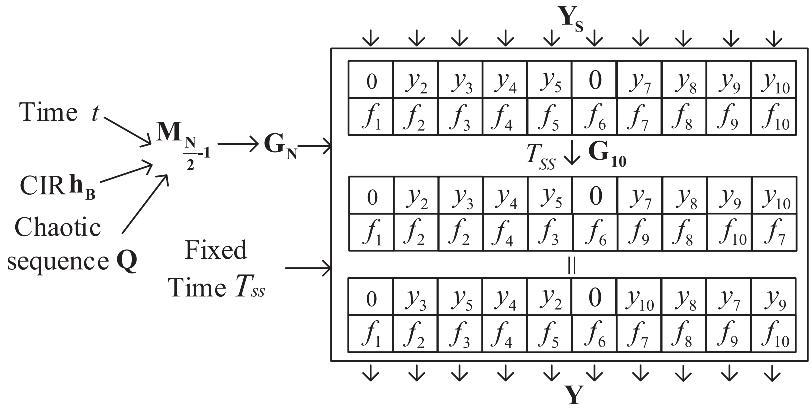

$\mathbf{Y_S}$
0 y_2 y_3 y_4 y_5 0 y_7 y_8 y_9 y_{10}
f_1 f_2 f_3 f_4 f_5 f_6 f_7 f_8 f_9 f_{10}
Time t
$\mathbf{M}_{\frac{N}{2}-1}$
$\mathbf{G_N}$
CIR $\mathbf{h_B}$
Chaotic sequence $\mathbf{Q}$
Fixed Time T_{ss}
T_{SS}
$\mathbf{G_{10}}$
0 y_2 y_3 y_4 y_5 0 y_7 y_8 y_9 y_{10}
f_1 f_2 f_2 f_4 f_3 f_6 f_9 f_8 f_{10} f_7
||
0 y_3 y_5 y_4 y_2 0 y_{10} y_8 y_7 y_9
f_1 f_2 f_3 f_4 f_5 f_6 f_7 f_8 f_9 f_{10}
$\mathbf{Y}$

Fig. 4. Channel determined subcarrier de-shifting procedure.

Thus, the received signal $\mathbf{Y_S}$ indicated in Fig. 4 can be de-shifted to

$$\mathbf{Y} = \mathbf{G_N}\mathbf{Y_S} \tag{31}$$

where we have $\mathbf{Y} = [0, y_3, y_5, y_4, y_2, 0, y_{10}, y_8, y_7, y_9]^T$. Since the eavesdroppers are unable to track and obtain the time varying location-related CSI or time-varying chaotic sequences between transmitter and legitimate receiver, they cannot derive $\mathbf{M}_{\frac{N}{2}-1}$ and $\mathbf{G_N}$. This therefore helps to improve the achievable security performance of the VLC system.

4. Theoretical Performance Analysis

4.1. Analysis Based on the Ill-posed Theory

Based on the ill-posed theory described in 2.3, the security mechanism is expected to provide stable and unique solutions for legitimate users, but unstable and/or non-unique solutions forxbrk eavesdroppers.

As shown in Fig. 2, utilizing (25) and (27), we have

$$\mathbf{x} = \sqrt{N}\mathbf{D_N}^{-1}\mathbf{X_J} = \sqrt{N}\mathbf{D}_N^{-1}\mathbf{J}\mathbf{S_N}\mathbf{X} \tag{32}$$

where $\sqrt{N}$ is the power normalization factor, and $\mathbf{D_N}$ is the $N \times N$ discrete Fourier transform (DFT) matrix given by [24]

$$\mathbf{D_N} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & W_N^1 & W_N^2 & \cdots & W_N^{N-1} \\ 1 & W_N^2 & W_N^4 & \cdots & W_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & W_N^{N-1} & W_N^{2(N-1)} & \cdots & W_N^{(N-1)(N-1)} \end{bmatrix} \tag{33}$$

where $W_N^i = \exp(\frac{-2\pi j}{N} \cdot i)$ with $j = \sqrt{-1}$ and $i = 1, 2, \ldots, (N-1)^2$. The received signal after removing cyclic prefix is

$$\mathbf{y} = \mathbf{h}\mathbf{x} + \mathbf{n} \tag{34}$$

where $\mathbf{n}$ is the $N \times 1$ AWGN vector with zero mean and a variance of $\frac{N_0}{2}$, while $\mathbf{h}$ is the $N \times N$ time-domain convolutional CIR matrix defined by

$$\mathbf{h} = \begin{bmatrix} h_0 & 0 & \cdots & 0 & h_{l_{CP}-1} & h_{l_{CP}-2} & \cdots & h_2 & h_1 \\ h_1 & h_0 & \cdots & 0 & 0 & h_{l_{CP}-1} & \cdots & h_3 & h_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & h_{l_{CP}-2} & h_{l_{CP}-3} & h_{l_{CP}-4} & \cdots & h_0 & 0 \\ 0 & 0 & \cdots & h_{l_{CP}-1} & h_{l_{CP}-2} & h_{l_{CP}-3} & \cdots & h_1 & h_0 \end{bmatrix}. \tag{35}$$

The elements of $\mathbf{h}$ in (35) can be generated by exploiting (13) as

$$h_{i,j} = \begin{cases} h_{B,\lfloor(i-j+N)\rfloor_N}, & \text{if} \quad \lfloor(i-j+N)\rfloor_N \in [0, l_{cp}-1] \\ 0, & \text{else} \end{cases} \tag{36}$$

where $i, j = 0, \ldots, N-1$ and $\lfloor\cdot\rfloor_N$ denotes the modulo-N operation.

4.1.1 Analysis for Legitimate Receivers: The signal received by the legitimate receiver Bob is

$$\mathbf{y_{Bob}} = \mathbf{h_{Bob}x} + \mathbf{n_{Bob}} \tag{37}$$

where $\mathbf{h_{Bob}}$ in the form of (35) is the convolutional CIR matrix associated with the channel link between Alice and Bob, and $\mathbf{n_{Bob}}$ is the AWGN noise at Bob. After FFT and the De-CDSS operation described in Section 3.4, the OFDM-demodulated signal can be derived with the aid of (32) and (37), as

$$\begin{aligned} \mathbf{Y_{Bob}} &= \mathbf{G_{Bob}} \cdot \sqrt{N}\mathbf{D_N} \cdot \mathbf{y_{Bob}} \\ &= \mathbf{G_{Bob}} \cdot \sqrt{N}\mathbf{D_N} \cdot \mathbf{h_{Bob}x} + \mathbf{G_{Bob}} \cdot \sqrt{N}\mathbf{D_N} \cdot \mathbf{n_{Bob}} \\ &= N\mathbf{G_{Bob}D_N h_{Bob} D_N^{-1} J S_N X} + \sqrt{N}\mathbf{G_{Bob}D_N n_{Bob}} \end{aligned} \tag{38}$$

where $\mathbf{G_{Bob}}$ is the channel determined subcarrier de-shifting matrix in the form of (29). Define the $N \times N$ matrix $\mathbf{A_{Bob}}$ as Bob's equivalent channel matrix formulated by

$$\mathbf{A_{Bob}} = N\mathbf{G_{Bob}D_N h_{Bob} D_N^{-1} J S_N}. \tag{39}$$

Then, according to the ill-posed theory discussed in Section 2.2, (38) may be reformulated as an ill-posed problem represented by

$$\mathbf{X} + \triangle\mathbf{X} = \left\{\mathbf{A_{Bob}^{-1}} + \triangle\left[\mathbf{A_{Bob}^{-1}}\right]\right\}\left\{\mathbf{Y_{Bob}} + \triangle\mathbf{Y_{Bob}}\right\}, \tag{40}$$

where the $\triangle(\cdot)$ operator denotes a change of the corresponding variable.

Now, we want to prove that the solution to $\mathbf{X}$ in (40) is stable. we have the following theorem:

Theorem 1: In the proposed CDSS-VLC system, the equivalent channel between the transmitter and the legitimate user remains constant. Thus, the solution to the legitimate user's information vector is stable.

Proof: Exploiting $\mathbf{D_N}$ of (33) and $\mathbf{h_{Bob}}$ of (37), we have

$$\mathbf{D_N h_{Bob}} = \begin{bmatrix} H_{B,0} & H_{B,0}W_N^{0\cdot 1} & \cdots & H_{B,0}W_N^{0\cdot(N-1)} \\ H_{B,1} & H_{B,1}W_N^{1\cdot 1} & \cdots & H_{B,1}W_N^{1\cdot(N-1)} \\ H_{B,2} & H_{B,2}W_N^{2\cdot 1} & \cdots & H_{B,2}W_N^{2\cdot(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ H_{B,N-1} & H_{B,N-1}W_N^{(N-1)\cdot 1} & \cdots & H_{B,N-1}W_N^{(N-1)^2} \end{bmatrix} \tag{41}$$

where $H_{B,k}(k = 0, 1, \ldots N-1)$ are defined in (26). Then multiply (41) with $N\mathbf{D_N^{-1}}$ to obtain

$$\mathbf{K_{Bob}} = N\mathbf{D_N h_{Bob} D_N^{-1}} = \mathrm{diag}_N(\mathbf{H_B}). \tag{42}$$

Utilizing (28), we arrive at

$$\mathbf{K_{Bob} J} = \mathbf{E_N} \tag{43}$$

where $\mathbf{E_N}$ is the identity matrix of dimension N. Then, (39) reduces to

$$\mathbf{A_{Bob}} = \mathbf{G_{Bob} S_N}. \tag{44}$$

Next, exploiting (19) and (29), we further simplify (44) to

$$\mathbf{A_{Bob}} = \begin{bmatrix} 0 & & & \\ & \mathbf{E_{\frac{N}{2}-1}} & & \\ & & 0 & \\ & & & \mathbf{E_{\frac{N}{2}-1}} \end{bmatrix} = \mathbf{E_N^o} \tag{45}$$

where $\mathbf{E_{\frac{N}{2}-1}}$ is the identity matrix of dimension $(\frac{N}{2}-1)$, and $\mathbf{E_N^o}$ is the $N \times N$ optical identical matrix, which is obtained by setting the 1^{st} and the $(\frac{N}{2}+1)^{th}$ rows of $\mathbf{E_N}$ to zeros. Under the assumption that both channel estimation and feedback are perfect, $\mathbf{A_{Bob}}$ in (45) becomes a constant matrix which does not change as the channel changes. Therefore, we have $\triangle[\mathbf{A_{Bob}^{-1}}] = 0$, and (40) reduces to

$$\mathbf{X} + \triangle\mathbf{X} = \left\{\mathbf{A_{Bob}^{-1}}\right\}\left\{\mathbf{Y_{Bob}} + \triangle\mathbf{Y_{Bob}}\right\}, \tag{46}$$

which implies that $\triangle\mathbf{X}$ is bounded when $\triangle\mathbf{Y}$ is bounded. According to (9), a stable system is defined as a system that has a bounded output given a bounded input [25]. Thus, based on (46), we conclude that the CDSS-VLC system is stable for legitimate users. The proof completes.

Subsequently, exploiting $X_0 = X_{\frac{N}{2}} = 0$ and the Hermitian symmetry property of $\mathbf{X}$, we insert (39) into (38) to obtain

$$\begin{aligned} \mathbf{Y_{Bob}} &= \mathbf{A_{Bob}X} + \sqrt{N}\mathbf{G_{Bob}D_N n_{Bob}} \\ &= \mathbf{X} + \sqrt{N}\mathbf{G_{Bob}D_N n_{Bob}}. \end{aligned} \tag{47}$$

4.1.2 Analysis for Eavesdroppers: The received signal at the eavesdropper is

$$\mathbf{y_{Eve}} = \mathbf{h_{Eve}x} + \mathbf{n_{Eve}}, \tag{48}$$

where $\mathbf{h_{Eve}}$ in the form of (35) is the convolutional CIR matrix associated with the channel link between Alice and Eve, and $\mathbf{n_{Eve}}$ is the AWGN vector at Eve. Similar to the case of Bob, the data demodulated by Eve is derived as

$$\begin{aligned} \mathbf{Y_{Eve}} &= \mathbf{G_{Eve}} \cdot \sqrt{N}\mathbf{D_N} \cdot \mathbf{y_{Eve}} \\ &= N\mathbf{G_{Eve}D_N h_{Eve} D_N^{-1} J S_N X} + \sqrt{N}\mathbf{G_{Eve}D_N n_{Eve}} \end{aligned} \tag{49}$$

with an ill-posed equation of

$$\mathbf{A_{Eve}} = N\mathbf{G_{Eve}}\mathbf{D_N}\mathbf{h_{Eve}}\mathbf{D_N^{-1}}\mathbf{JS_N} \tag{50}$$

where $\mathbf{G_{Eve}}$ is the subcarrier de-shifting matrix invoked by Eve, and $\mathbf{A_{Eve}}$ is Eve's equivalent channel matrix. We may define

$$\mathbf{K_{Eve}} = N\mathbf{D_N}\mathbf{h_{Eve}}\mathbf{D_N^{-1}} = \mathrm{diag}_N(\mathbf{H_E}) \tag{51}$$

where $\mathbf{H_E} = [H_{E,0}, H_{E,1}, \ldots, H_{E,N-1}]^T$ is the frequency domain channel transfer functions between Alice and Eve.

Compared with Bob who knows his de-shifting matrix $\mathbf{G_{Bob}}$, however, Eve has to employ brute force methods for deriving the unknown $\mathbf{G_{Eve}}$. Furthermore, since the pre-equalization matrix $\mathbf{J}$ is constructed according to the channel between Alice and Bob, the signal received by Eve will be distorted by her own channel. Hence, $\mathbf{A_{Eve}}$ would not be a constant matrix and, as a result, the equivalent channel between the transmitter and the eavesdropper will dramatically and randomly vary. Due to such unstable characteristics, $\mathbf{Y_{Eve}}$ in (49) is not determinable. Therefore, in the proposed CDSS-VLC system, eavesdroppers are unlikely able to decode the information transmitted to legitimate users. A higher transmission security can then be achieved in comparison to conventional VLC systems.

4.2. BER Analysis

Over AWGN channel, similar to RF systems, the theoretical electrical BER of the prosed CDSS-VLC system with M-ary quadrature amplitude modulation (QAM), may be developed from the well known BER expression of M-QAM system under high signal-to-noise ratio (SNR), which is given by [26]

$$P_b = \frac{\sqrt{M}-1}{\sqrt{M}\log_2\sqrt{M}}\mathrm{erfc}\left[\sqrt{\frac{3\log_2 M E_b}{2(M-1)N_0}}\right] = \frac{\sqrt{M}-1}{\sqrt{M}\log_2\sqrt{M}}\mathrm{erfc}\left[\sqrt{\frac{3E_s}{2(M-1)N_0}}\right] \tag{52}$$

where the value of the signal symbol energy E_s is dependent on both the VLC channel coefficients and the corresponding bit energy for legitimate receivers or eavesdroppers.

Based on (52), we can derive the BER expressions for legitimate receivers and eavesdroppers, respectively.

4.2.1 BER for Legitimate Users: For the legitimate receiver, E_s is calculated by

$$E_{s,Bob} = E[\|\mathbf{A_{Bob}X}\|^2] = E[\|\mathbf{X}\|^2] \tag{53}$$

Utilizing (47) and (52), as we define the variance of AWGN noise $\frac{N_0}{2}$ in (34), the BER expression of the legitimate user Bob is formulated as

$$P_{b,Bob} = \frac{\sqrt{M}-1}{\sqrt{M}\log_2\sqrt{M}}\mathrm{erfc}\left[\sqrt{\frac{3E_{s,Bob}}{(M-1)N_0}}\right]. \tag{54}$$

4.2.2 BER for Eavesdroppers: Similar to (53), E_s for the eavesdropper Eve can be calculated by

$$E_{s,Eve} = E[\|\mathbf{A_{Eve}X}\|^2] = E[\mathbf{X}^H\mathbf{A_{Eve}^H}\mathbf{A_{Eve}X}] \tag{55}$$

where $(\cdot)^H$ denotes the Hermitian transpose operator, and $\mathbf{A_{Eve}}$ is given in (50). Then we have

$$\begin{aligned}\mathbf{A_{Eve}^H}\mathbf{A_{Eve}} &= (N\mathbf{G_{Eve}}\mathbf{D_N}\mathbf{h_{Eve}}\mathbf{D_N^{-1}}\mathbf{JS_N})^H(N\mathbf{G_{Eve}}\mathbf{D_N}\mathbf{h_{Eve}}\mathbf{D_N^{-1}}\mathbf{JS_N})\\ &= (\mathbf{G_{Eve}}\mathbf{K_{Eve}}\mathbf{JS_N})^H(\mathbf{G_{Eve}}\mathbf{K_{Eve}}\mathbf{JS_N})\\ &= \mathbf{S_N^H}\mathbf{J}^H\mathbf{K_{Eve}^H}\mathbf{G_{Eve}^H}\mathbf{G_{Eve}}\mathbf{K_{Eve}}\mathbf{JS_N}\end{aligned} \tag{56}$$

where $\mathbf{K_{Eve}}$ is defined in (51).

Note that the value of (56) is dependent on how much information the eavesdropper knows about the transmission scheme, where we have two cases:

- *Case 1 (C1)*: The eavesdropper is not aware of the existence of CDSS.
- *Case 2 (C2)*: The eavesdropper knows the rules of shifting matrix generation specified in (29) but does not know the CSI between transmitter and legitimate receiver or the key parameters of chaotic sequences, namely the initial value and the logistic map of (14).

In $C1$, since CDSS is not considered at the eavesdropper, (56) can be simplified with $\mathbf{G}_{\mathbf{Eve}}$ reduced to $\mathbf{E}_{\mathbf{N}}$, resulting in

$$\begin{aligned}(\mathbf{A}^H_{\mathbf{Eve}}\mathbf{A}_{\mathbf{Eve}})_{C1} &= \mathbf{S}^H_{\mathbf{N}}\mathbf{J}^H\mathbf{K}^H_{\mathbf{Eve}}\mathbf{K}_{\mathbf{Eve}}\mathbf{J}\mathbf{S}_{\mathbf{N}} \\ &= \mathbf{S}^H_{\mathbf{N}}\mathbf{J}^H\operatorname{diag}_N(|\mathbf{H}_{\mathbf{E}}|^2)\mathbf{J}\mathbf{S}_{\mathbf{N}}\end{aligned} \tag{57}$$

where $|\mathbf{H}_{\mathbf{E}}|^2 = [|H_{E,0}|^2, |H_{E,1}|^2, \ldots, |H_{E,N-1}|^2]^T$.

In $C2$, when knowing the rules of shifting matrix generation without the CSI between transmitter and legitimate receiver or the key parameters of chaotic sequences, the eavesdropper has to traverse all possible combinations of $\mathbf{G}_{\mathbf{Eve}}$ to identify the correct $\mathbf{G}_{\mathbf{N}}$. Since $\mathbf{G}_{\mathbf{Eve}}$ is a subcarrier de-shifting matrix in the form of (29), for every possible $\mathbf{G}_{\mathbf{Eve}}$, we have $\mathbf{G}^H_{\mathbf{Eve}}\mathbf{G}_{\mathbf{Eve}} = \mathbf{E}^{\mathbf{o}}_{\mathbf{N}}$. We may simplify (56) to

$$\begin{aligned}(\mathbf{A}^H_{\mathbf{Eve}}\mathbf{A}_{\mathbf{Eve}})_{C2} &= \mathbf{S}^H_{\mathbf{N}}\mathbf{J}^H\mathbf{K}^H_{\mathbf{Eve}}\mathbf{E}^{\mathbf{o}}_{\mathbf{N}}\mathbf{K}_{\mathbf{Eve}}\mathbf{J}\mathbf{S}_{\mathbf{N}} \\ &= \mathbf{S}^H_{\mathbf{N}}\mathbf{J}^H\operatorname{diag}_N(|\mathbf{H}^{\mathbf{o}}_{\mathbf{E}}|^2)\mathbf{J}\mathbf{S}_{\mathbf{N}}\end{aligned} \tag{58}$$

where $\mathbf{H}^{\mathbf{o}}_{\mathbf{E}}$ is defined by

$$|\mathbf{H}^{\mathbf{o}}_{\mathbf{E}}|^2 = [0, |H_{E,1}|^2, \ldots, |H_{E,\frac{N}{2}-1}|^2, 0, |H_{E,\frac{N}{2}+1}|^2, \ldots, |H_{E,N-1}|^2]^T \tag{59}$$

Recall from Section 3.1 that we have $X_0 = X_{\frac{N}{2}} = 0$ in $\mathbf{X}$. Thus, we arrive at

$$\mathbf{X}^H(\mathbf{A}^H_{\mathbf{Eve}}\mathbf{A}_{\mathbf{Eve}})_{C1}\mathbf{X} = \mathbf{X}^H(\mathbf{A}^H_{\mathbf{Eve}}\mathbf{A}_{\mathbf{Eve}})_{C2}\mathbf{X}. \tag{60}$$

Based on (60), we can rewrite (55) as

$$E_{s,Eve} = E[\mathbf{X}^H\mathbf{S}^H_{\mathbf{N}}\mathbf{J}^H\operatorname{diag}_N(|\mathbf{H}_{\mathbf{E}}|^2)\mathbf{J}\mathbf{S}_{\mathbf{N}}\mathbf{X}], \text{ for } \mathrm{C}_1, \mathrm{C}_2. \tag{61}$$

Since the CIRs are assumed to be statistically independent [19]–[21], the cross-correlation between $\mathbf{H}_{\mathbf{E}}$ and $\mathbf{H}_{\mathbf{B}}$ is very low, provided that the locations of the two users are sufficiently far away. Thus, the term of $\{\mathbf{J}^H\operatorname{diag}_N(|\mathbf{H}_{\mathbf{E}}|^2)\mathbf{J}\}$ in (61) is expected to have a very small value, where $\mathbf{J}$ is defined by (28). This implies that $E_{s,Eve}$ of (61) is dramatically smaller than $E_{s,Bob}$ of (53). Furthermore, its value also changes randomly due to the effect of $\mathbf{S}_{\mathbf{N}}$ seen in (61).

Utilizing (52) and (61), the BER expression of the eavesdropper Eve is formulated as

$$P_{b,Eve} = \frac{\sqrt{M}-1}{\sqrt{M}\log_2\sqrt{M}}\operatorname{erfc}\left[\sqrt{\frac{3E[\|\mathbf{X}^H\mathbf{S}^H_{\mathbf{N}}\mathbf{J}^H\operatorname{diag}_N(|\mathbf{H}_{\mathbf{E}}|^2)\mathbf{J}\mathbf{S}_{\mathbf{N}}\mathbf{X}\|]}{(M-1)N_0}}\right]. \tag{62}$$

4.3. Secrecy Capacity of CDSS-VLC system

In order to investigate the effectiveness of our security mechanism design and security performance analysis for VLC system, here, we derive the secrecy capacity for our presented system with the aid of [7], under the assumption that the channel conditions of malicious user channel are known to Alice, namely the transmitter, and that the channel conditions between Bob and Alice are better than those between Eve and Alice.

Utilizing equation (47) and (49), we have the SNR of Bob and Eve

$$SNR_{Bob} = \frac{E_{s,Bob}}{\sigma_n^2} = \frac{E[\|\mathbf{X}\|^2]}{\frac{N_0}{2}}, SNR_{Eve} = \frac{E_{s,Eve}}{\sigma_n^2} = \frac{E[\|\mathbf{A}_{\mathbf{Eve}}\mathbf{X}\|^2]}{\frac{N_0}{2}}. \tag{63}$$

TABLE 1
Simulation parameters

Parameters	Value
Size of room ($L \times W \times H$)	$5 \times 5 \times 3$ m^3
Length range of room	$[-2.5, 2.5]$
Width range of room	$[-2.5, 2.5]$
Height range of room	[0, 3]
Reflection coefficient (wall/ceiling/floor)	(0.8, 0.8, 0.3)
Size of small optical reflation elements (wall/ceiling/floor)	0.01 m^2
Maximum reflection order	4
LED transmitter location	(0, 0, 3)
Transmit power	1 W
Physical area of PD	1 cm^2
Semi-half power angle	60°
Field of view	85°
Position of legitimate user	$(-2, -1.5, 0)$
Position of eavesdropper	(1, 1, 0)
DC bias	13 dB
Cyclic prefix length	$N/8$

Then, the secrecy capacity for an single input single output(SISO) VLC system C_s is found by [27] and [28]

$$C_s = \max[R_{Bob} - R_{Eve}]^+ \tag{64}$$

where $[x]^+ = \max(x, 0)$ and variable R indicates achievable rate. According to [7], the upper bound secrecy capacity of CDSS-VLC system is

$$C_s = \frac{1}{2} \max\left[\log_2(1 + SNR_{Bob}) - \log_2(1 + SNR_{Eve})\right]^+ . \tag{65}$$

5. Simulation

In this section, the performances of the proposed DCO-OFDM aided CDSS-VLC system are evaluated. The performances of conventional DCO-OFDM scheme are also provided as reference. It is assumed that there are one transmitter, one legitimate user, and one eavesdropper who is under the $C2$ scenario described in Section 4.2.2. The typical scenario for indoor VLC system illustrated in [17] is adopted for performance comparison in this paper and the main simulation parameters are summarizedin Table 1. Since perfect channel estimation is assumed and the pre-equalization scheme provides nice channel equalization, the multipath channel impulse response can be eliminated and the parameters such as size of room and the field of view do not cause significant impact to communication performance. The transmit power of LED source is set to $1W$ in general which can be change according to specific SNR.

First, the comparison of theoretical and simulated BER performances of the legitimate user is provided in Fig. 5, where the theoretical results were generated by (54). As indicated in [26], the BER formula of (52) is valid only in high SNR area. From Fig. 5, we can see the theoretical and the simulation results beyond $E_b/N_0 = 20$ dB match well. When we have $E_b/N_0 < 20$ dB, however,

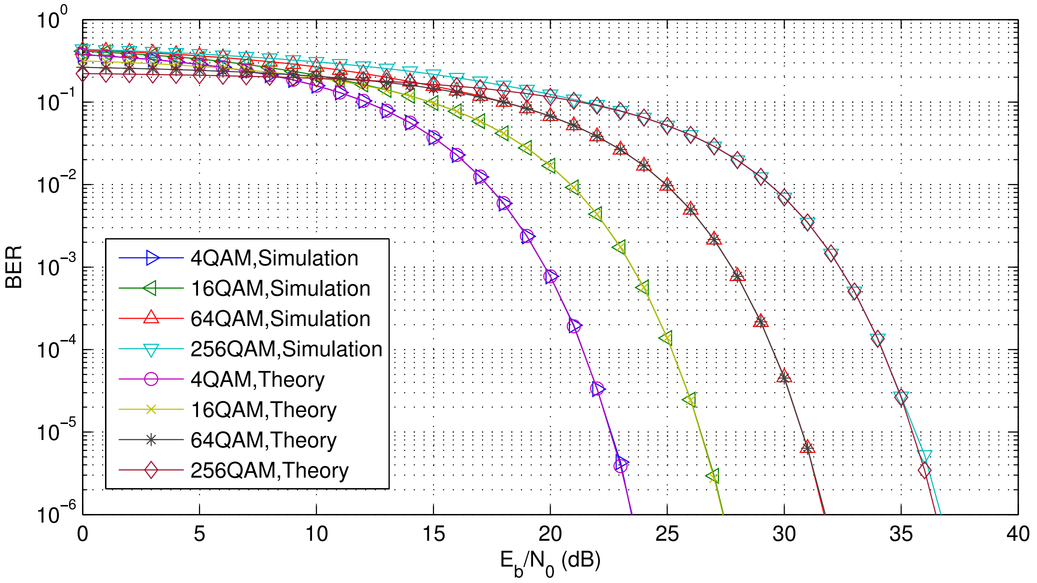


Fig. 5. Theoretical versus simulated BER performances of the legitimate user in the CDSS-VLC system.

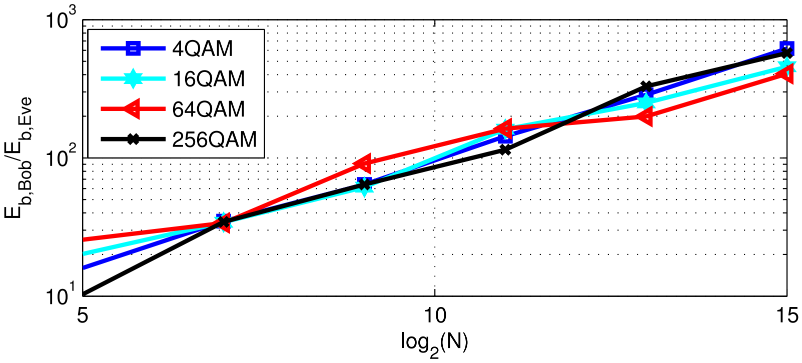


Fig. 6. Ratio between $E_{b,Bob}$ and $E_{b,Eve}$ versus different values of subcarrier number N in the CDSS-VLC system.

there exist noticeable differences between the two groups of results, due to the approximation of (52) under low SNRs.

Next, in Fig. 6, we show the relative energy difference between the legitimate user and the eavesdropper, based on the ratio between $E_{s,Bob}$ of (53) and $E_{s,Eve}$ of (61). As seen in Fig. 6, assuming the system's transmit power remains unchanged, a significantly higher signal energy ratio can be achieved when the number of subcarriers N increases. Based on ill-posed theory, the CDSS and pre-equalization techniques offer remarkably more stable equivalent channel to Bob (45) than Eve (50), which results in a substantially lower SNR of the eavesdropper than that of the legitimate user, hence effectively helps to improve the security performance of the VLC system. More explicitly, the large energy gap at an order of 10 to 10^3 indicates a dramatic difference between the BER performances of the legitimate user and the eavesdropper, as evidenced in Fig. 7, where the configurations of $N = \{512, 2048, 8192\}$ were simulated under 16QAM. From Fig. 7, it can be observed that the BER of the eavesdropper remains to be the prohibitively high value of 0.5 regardless of the value of N, implying the fact that it is not possible for the eavesdropper to retrieve any useful information from the received signal. In contrast, the BERs of the legitimate user protected by the

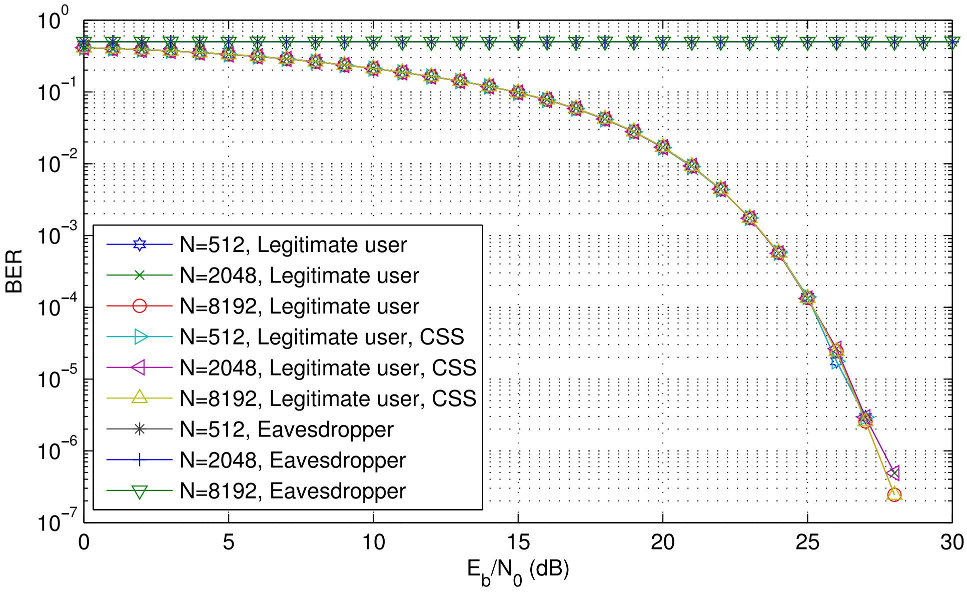


Fig. 7. BER performance comparison of the VLC systems with different values of subcarrier number N assuming the use of 16 QAM.

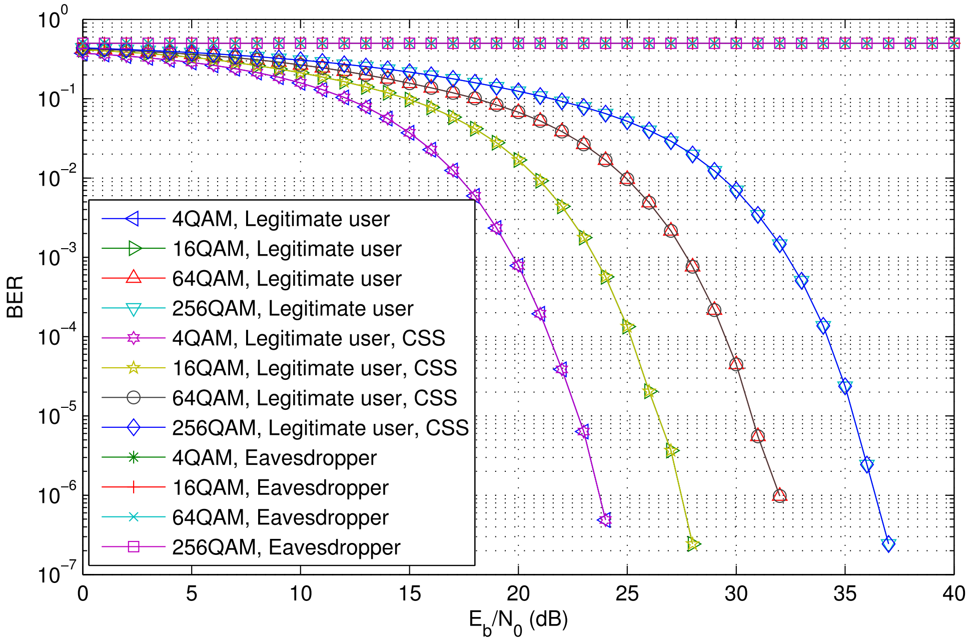


Fig. 8. BER performance comparison of the VLC systems with different QAM schemes assuming $N = 512$.

proposed CDSS scheme are almost the same as the conventional DCO-OFDM-VLC benchmarks. This proves that the proposed techniques would not degrade the achievable conventional BER performances, while at the same time offering improved security to signal transmissions.

Subsequently, we compare the BERs of the VLC systems under different modulation orders inFig. 8 with $N = 512$. Again, it can be seen that the BER performances of the legitimate user are

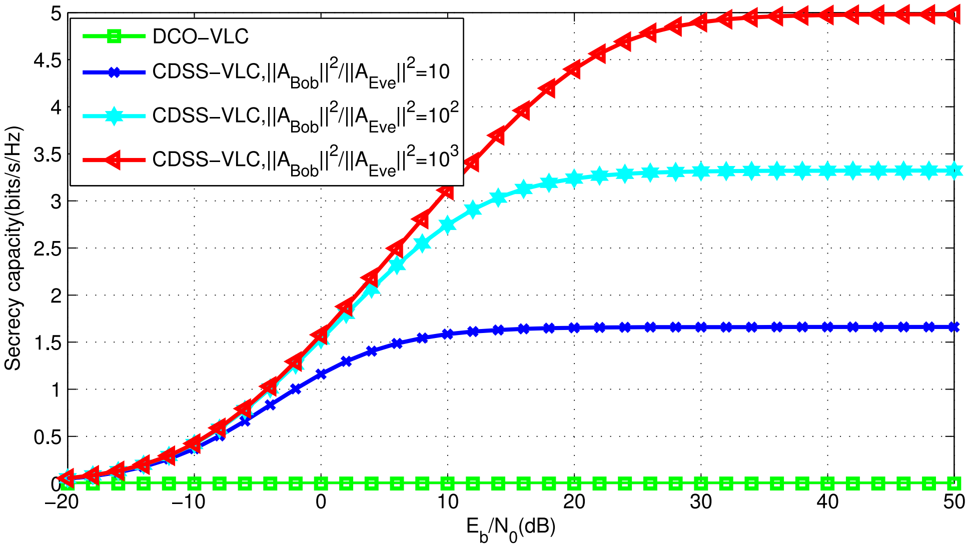


Fig. 9. Secrecy capacity of CDSS-VLC.

not affected by CDSS with different QAM schemes. Furthermore, it is noticeable that when using the same QAM scheme, the performance of the proposed DCO-OFDM based CDSS-VLC system under fading channel is identical to that of the conventional DCO-OFDM-VLC system over AWGN channel, which can be found in [29, Fig. 2]. This indicates that the proposed CDSS-VLC scheme is capable of eliminating the impact of fading channel and approaching AWGN performance. This is an expected result according to (47), given the assumption that perfect CSI is available for constructing the pre-equalization matrix **J** at the transmitter. On the contrary, similar to the trend observed in Fig. 7, the BERs of the eavesdropper with different modulation schemes remain as high as 0.5, as seen in Fig. 8.

Last but not least, in Fig. 9, assuming the average channel gains of Bob and Eve are equal, i.e. $E[\|\mathbf{h}_{\mathbf{Bob}}\|^2] = E[\|\mathbf{h}_{\mathbf{Eve}}\|^2]$, we simulate the secrecy capacity performances of conventional DCO-OFDM-VLC and the proposed CDSS-DCO-OFDM-VLC systems based on (65). In the conventional system, channel equalization is typically implemented at receiver, implying that if the eavesdropper is aware of transmitted pilot signals, the associated CSI can be estimated and used for assisting in data demodulation. In such a scenario without the protection of the proposed CDSS and pre-equalization schemes, the secrecy capacity remains to be zero for all SNR level. By contrast, in the proposed system, however, the secrecy capacity increase as SNR increase before the limit value which is consistent with the result in [7]. Thanks to the employment of our tailored CDSS and pre-equalization techniques based on the ill-posed theory, the secrecy capacity C_s increase as the value of $\frac{\|\mathbf{A}_{\mathbf{Bob}}\|^2}{\|\mathbf{A}_{\mathbf{Eve}}\|^2}$ increases although the average channel gains of Bob and Eve remain the same, which indicates that secure transmission can be achieved.

6. Conclusion

In this paper, exploiting the real-valued CSI of VLC channel and chaotic sequences, and practical ill-posed theory, we present chaotic CDSS scheme with pre-equalization to enhance the physical layer security of the DCO-OFDM aided VLC system. The sorting operations are allowed in real domain to be performed on the CSI of VLC channel, and together with the combination with chaotic sequences and pre-equalization, the CDSS aided VLC system can provide high security transmission for the users. Moreover, we conduct an analytical derivation on the formulations of the equivalent channels for legitimate receivers and eavesdroppers, as well as the associated BER equations. Further, we provide secrecy capacity to verify the effectiveness of our design and analysis based on ill-posed theory. Both theoretical and simulation results are offered to validate the proposed system design, demonstrating that our scheme can improve the achievable security performance of the OOFDM-based VLC system without compromising its BER.

References

[1] J. Grubor, S. C. J. Lee, K.-D. Langer, T. Koonen, and J. W. Walewski, “Wireless high-speed data transmission with phosphorescent white-light LEDs,” in *Proc. 33rd Eur. Conf. Exhib. Opt. Commun.*, 2007, Paper PD3.6.

[2] S. Hranilovic, *Wireless Optical Communication Systems*. New York, NY, USA: Springer, 2006.

[3] R. Mesleh, H. Elgala, and H. Haas, “On the performance of different OFDM based optical wireless communication systems,” *IEEE/OSA J. Opt. Commun. Netw.*, vol. 3, no. 8, pp. 620–628, Aug. 2011.

[4] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, *Optical Wireless Communications: System and Channel Modelling with MATLAB*. Boca Raton, FL, USA: CRC, 2012.

[5] A. Mostafa and L. Lampe, “Physical-layer security for indoor visible light communications,” in *Proc. IEEE Int. Conf. Commun.*, 2014, pp. 3342–3347.

[6] A. Mostafa and L. Lampe, “Securing visible light communications via friendly jamming,” in *Proc. Globecom Workshops*, 2014, pp. 524–529.

[7] A. Mostafa and L. Lampe, “Physical-Layer security for MISO visible light communication channels,” *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.

[8] C. Rohner, S. Raza, D. Puccinelli, and T. Voigt, “Security in visible light communication: Novel challenges and opportunities,” *Sensors Transducers*, vol. 192, pp. 9–15, Sep. 2015.

[9] X. Sun and I. Djordjevic, “Physical-layer security in orbital angular momentum multiplexing free-space optical communications,” *IEEE Photon. J.*, vol. 8, no. 1, pp. 1–10, Feb. 2016.

[10] C. Chow, Y. Liu, C. Yeh, C. Chen, C. Lin, and D. Hsu, “Secure communication zone for white-light LED visible light communication,” *Opt. Commun.*, vol. 344, pp. 81–85, 2015.

[11] F. Lopez-Martinez, G. Gomez, and J. Garrido-Balsells, “Physical-layer security in free-space optical communications,” *IEEE Photon. J.*, vol. 7, no. 2, pp. 1–14, Apr. 2015.

[12] A. D. Wyner, “The Wire-tap Channel,” *Bell Syst. Tech. J.,* vol. 54, pp. 1355–1387, Oct. 1975.

[13] T. Yang, “A survey of chaotic secure communication systems,” *Int. J. Comput. Cognition*, vol. 2, no. 2, pp. 81–130, 2004.

[14] X. Xu, W. Luo, H. Song, and L. Zhang, “Enhancing wireless security with theory of Ill-posed problem: A novel physical-layer encryption mechanism,” in *Proc. Int. Conf. Inf. Sci. Technol.*, Mar. 2013, pp. 1606–1609.

[15] H. Lu, L. Zhang, Z. Zhang, and Z. Wu, “The practical use of Ill-Posed theory: Improved dynamic subcarrier coordinated interleaving OFDM system with pre-equalization,” in *Proc. IEEE/CIC Int. Conf. Commun. China*, Nov. 2015, pp. 585–589.

[16] M. Strasser, C. Pöpper, S. Capkun, and M. Cagalj, “Jamming-resistant key establishment using uncoordinated frequency hopping,” in *Proc. IEEE Symp. Security Privacy*, May 2008, pp. 64–78.

[17] J. B. 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.

[18] P. C. Hansen, *Rank-deficient and Discrete Ill-posed Problems: Numerical Aspects of Linear Inversion*, 4th ed. Philadelphia, PA, USA: SIAM, 1998.

[19] B. E. I. Wong, “Optimal resource allocation in the OFDMA downlink with imperfect channel knowledge,” *IEEE Trans. Commun.*, vol. 57, no. 1, pp. 232–241, Jan. 2009.

[20] S. K. Hashemi, Z. Ghassemlooy, L. Chao, and D. Benhaddou, “Channel estimation for indoor diffuse optical OFDM wireless communications,” in *Proc. IEEE 5th Int. Conf. Broadband Commun., Netw. Syst.*, Sep. 2008, pp. 431–434.

[21] W. Shieh, H. Bao, and Y. Tang, “Coherent Optical OFDM: Theory and Design,” *Opt. Exp.*, vol. 16, no. 2, pp. 841–859, 2008.

[22] 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.

[23] D. Karunatilaka, F. Zafar, V. Kalavally, and R. Parthiban, “LED based indoor visible light communications: State of the art,” *IEEE Commun. Surveys Tut.*, vol. 17, no. 3, pp. 1649–1678, Aug. 2015.

[24] N. Ahmed and S. M. Cheng, “On matrix partitioning and a class of algorithms,” *IEEE Trans. Edu.*, vol. 13, no. 2, pp. 103–105, Aug. 1970.

[25] A. Oppenheim and A. Willsky, *Signals and Systems*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 1996.

[26] K. Cho and D. Yoon, “On the general BER expression of one- and two-dimensional amplitude modulations,” *IEEE Trans. Commun.*, vol. 50, no. 7, pp. 1074–1080, Jul. 2002.

[27] O. Ozel, E. Ekrem, and S. Ulukus, “Gaussian wiretap channel with an amplitude constraint,” in *Proc. IEEE Inf. Theory Workshop*, Sep. 2012, pp. 139–143.

[28] Y. Zou, X. Wang, and W. Shen, “Physical-Layer security with multiuser scheduling in cognitive radio networks,” *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[29] J. Armstrong and B. J. C. Schmidt, “Comparison of asymmetrically clipped optical OFDM and DC-Biased optical OFDM in AWGN,” *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 343–345, May 2008.