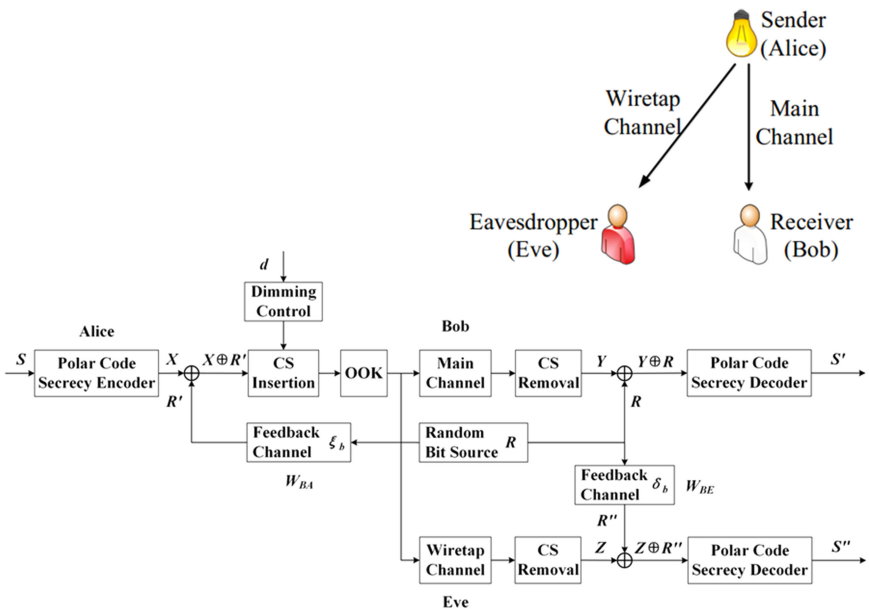
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

A Physical-Layer Secure Coding Scheme for Indoor Visible Light Communication Based on Polar Codes

Volume 10, Number 5, September 2018

Zhen Che
Junbin Fang
Zoe Lin Jiang
Jin Li
Shancheng Zhao
Yongchun Zhong
Zhe Chen



DOI: 10.1109/JPHOT.2018.2869931
1943-0655

A Physical-Layer Secure Coding Scheme for Indoor Visible Light Communication Based on Polar Codes

Zhen Che,[1] Junbin Fang,[2] Zoe Lin Jiang,[3] Jin Li,[2] Shancheng Zhao,[1] Yongchun Zhong,[2] and Zhe Chen[2]

[1]College of Information Science and Technology, Jinan University, Guangzhou 510632, China
[2]Guangdong Provincial Engineering Technology Research Center on VLC, Guangzhou Municipal Key Laboratory of Engineering Technology on VLC, and Department of Optoelectronic Engineering, Jinan University, Guangzhou 510632, China
[3]Harbin Institute of Technology Shenzhen Graduate School, Shenzhen 518055, China

DOI:10.1109/JPHOT.2018.2869931

Manuscript received August 14, 2018; revised September 4, 2018; accepted September 9, 2018. Date of publication September 13, 2018; date of current version September 26, 2018. This work was supported in part by the National Natural Science Foundation of China under Grant 61771222 and Grant 61475066; in part by the Science and Technology Projects of Guangdong Province under Grant 2016A010101017, Grant 2016A010119093, Grant 2014B010120002, and Grant 2016A030311019; in part by the Project of Guangdong High Education under Grant YQ2015018; in part by the Science and Technology Project of Guangzhou under Grant 201707010253, Grant 201803020023, Grant 201704030105, Grant 201605030002, and Grant 201604040005; in part by the Science and Technology Projects of Shenzhen under Grant JSGG20160427185010977, Grant JCYJ20170815145900474, and Grant JCYJ20160318094015947; in part by the Joint Fund of Pre-Research for Equipment, Ministry of Education of China under Grant 6141A02022124; and in part by the Rail Transit Healthy Operation Cooperative Innovation Center of Zhuhai under Grant 55560307. This paper was presented in part at the 12th Conference on Lasers and Electro-Optics Pacific Rim, Singapore, July 31–August 4, 2017. Corresponding authors: Junbin Fang and Zoe Lin Jiang (e-mail: junbinfang@gmail.com; zoeljiang@gmail.com).

Abstract: Visible light communication (VLC) can provide short-range optical wireless communication together with illumination using LED lightings. Since VLC channel is an open wireless channel, physical-layer security is desirable in order to hide secret information from unauthorized receivers, without reliance on upper-layer cryptographic techniques. In this paper, a secure coding scheme based on polar codes is proposed to simultaneously achieve physical-layer security and transmission reliability for indoor VLC systems under Wyner's wiretap model. An indoor VLC degraded wiretap channel model and an indoor VLC undegraded wiretap model are analyzed to estimate the corresponding secrecy capacity with typical indoor VLC scenarios considering the requirements of illumination and reliable transmission. Then, a physical-layer secure coding scheme and an enhanced scheme are designed to provide securely reliable communication without sacrificing the illumination functionality. Numerical results show that for VLC degraded wiretap channel, the proposed coding scheme can reduce the bit error rate (BER) of main channel to nearly 0 and increase that of wiretap channel to 0.5. Therefore, the mutual information between the sender and the eavesdropper and the BER of the legitimate receiver are both decreased to nearly 0. Both the security and reliability of VLC are guaranteed by the proposed coding scheme. And the practical secrecy rate reaches 85.96% at some positions when codeword length is 2 048 bits. Furthermore, an enhanced coding scheme with a feedback channel is proposed to handle the case that the wiretap channel is not degraded with respect to the main channel. With the feedback channel, the wiretap channel can be equivalently degraded and the security can

be increased gradually with the increment of the degradation level of the wiretap channel. Meanwhile, the secrecy capacities can be asymptotically achieved for indoor VLC systems.

Index Terms: Visible light communication, polar codes, physical-layer security, secrecy capacity.

1. Introduction

Visible light communication (VLC) has attracted increasing attention as a novel short-range wireless communication technology since it can provide both illumination and communication service simultaneously [1]. The IEEE 802.15.7 standard, released in 2011 [2], is a major step towards the widespread deployment of VLC networks. Secure transmission of private message over an open channel is a critical issue in wireless communication due to the broadcast nature of wireless. Taking advantage of the line-of-sight (LoS) propagation and non-penetrating nature of light waves through opaque surfaces, VLC is more secure than its radio frequency (RF) counterpart. However, as an open wireless channel, VLC is still vulnerable to eavesdropping by unauthorized users illuminated by the data transmitters. Physical-layer security has emerged as a promising complement to conventional encryption techniques to counter eavesdropping [3].

Several physical-layer security schemes for VLC systems have been proposed [3]–[10]. Most of them are based on signal control techniques such as beamforming and jamming. For example, two jamming schemes were introduced to send jamming signals and optimize the jamming beamformer such that the VLC secrecy rate can be maximized [4], [5]. Furthermore, Mostafa and Lampe utilized beamforming to obtain achievable secrecy rates and proposed a practical robust beamforming scheme for the multiple-input, single-output (MISO) VLC wiretap channel [6], [7]. On this basis, Ma *et al.* designed both the optimal and robust secrecy beamformers for indoor MISO VLC systems [8]. And, Shen *et al.* devised a minorization-maximization algorithm to find the optimal transmit beamformer and jamming precoder that maximize receiver's signal-to-noise ratio (SNR) satisfying eavesdropper's SNR constraints and LED optical power constraints [9]. In addition, Mukherjee *et al.* proposed a two-stage beamforming design to examine secret key agreement for MISO VLC systems [3]. Beamforming techniques require the cooperation of multiple transmitters and then increase the hardware design complexity of transmitters. Furthermore, it may cause a non-uniform illumination. On the other hand, Al-Moliki proposed a new security approach for VLC links based on an encryption key-generation method (secret key based secrecy) suitable for optical OFDM system in VLC to provide high spectral efficiency and to overcome inter-symbol interference (ISI) [10]. Besides, in the Media Access Control (MAC) layer, Mousa *et al.* proposed a secure MIMO-VLC system that relied on the position of the user by incorporating a new modified version of the Rivest-Shamir-Adleman (RSA) technique for encrypting the transmitted data [11]. For this category of physical-layer security techniques, pre-shared keys are required and key management may not be convenient.

In this paper, instead of relying on signal control techniques or key-based techniques, we propose a secure keyless coding scheme based on polar codes, a novel forward error correction (FEC) codes, to simultaneously achieve physical-layer security and transmission reliability for indoor VLC systems with binary discrete memoryless channels (BDMCs) under Wyner's wiretap model [12]. In 1975, Wyner proved that secret messages can be transmitted securely and reliably via FEC codes as long as the eavesdropper's channel is degraded with respect to the receiver's channel. Polar codes are the first deterministic construction of capacity-achieving FEC codes for symmetric BDMCs [13]. In our previous work [14], we firstly proposed a polar codes-based FEC coding scheme for dimmable VLC systems to increase transmission efficiency and reliability and to fulfill two lighting related requirements, i.e., flicker mitigation and dimming support, as suggested in IEEE Standard 802.15.7 [2]. In this paper, we further utilize polar codes to provide physical-layer security and transmission reliability together for VLC systems with one coding scheme.

The main contributions of this paper are as follows: First, two typical indoor VLC scenarios, i.e., single-input single-output (SISO) VLC and MISO VLC, are analyzed to build two VLC wiretap

channel models based on the basic propagation model of indoor VLC channel and Wyner's wiretap model, with the considerations of uniform illumination and reliable transmission. Therefore, the secrecy capacities of the two wiretap channel models are estimated. Secondly, a polar codes-based physical-layer secure coding scheme is proposed for indoor VLC degraded wiretap channel model to simultaneously achieve transmission security and reliability with one coding scheme. For VLC degraded wiretap channel model, where the wiretap channel is regarded as a degraded version of the main channel, the proposed coding scheme can be applied directly to provide the functionalities of security and reliability simultaneously. Thirdly, for a more complicated case that the wiretap channel is not degraded, we propose an enhanced VLC coding scheme with a feedback channel to degrade the wiretap channel equivalently, and provide physically secure transmission. Finally, numerical results show that for VLC degraded wiretap channel, the proposed coding scheme can reduce the bit error rate (BER) of main channel to nearly 0 and increase that of wiretap channel to 0.5. Therefore, the mutual information between the sender and the eavesdropper and the BER of the legitimate receiver are both decreased to nearly 0. Both the security and reliability of VLC are guaranteed by the proposed coding scheme. And the practical secrecy rate reaches 85.96% at some positions when codeword length is 2,048 bits. A higher practical secrecy rate can be achieved with a longer codeword length. As for the VLC undegraded wiretap model, with the enhanced coding scheme, the wiretap channel can be equivalently degraded and the security can be increased gradually with the increment of the degradation level of the wiretap channel. Meanwhile, the secrecy capacities can be asymptotically achieved for indoor VLC systems.

The rest of this paper is organized as follows. The basic VLC model, the SISO and MISO wiretap channel models are introduced in Section 2. And the proposed physical-layer secure coding schemes are proposed with the numerical results in Section 3. Section 4 concludes the paper.

2. Indoor VLC Wiretap Channel Model

First, the basic indoor VLC channel model is introduced, as well as Wyner's wiretap model. And then, a SISO indoor VLC wiretap channel model is analyzed and its secrecy capacity with a set of typical parameters for indoor illumination is numerically estimated. Based on this, a more complicated VLC wiretap channel model, MISO indoor VLC wiretap channel, is analyzed and estimated assuming that the wiretap channel may not be degraded with respect to main channel.

2.1 Basic Indoor VLC Channel

Basically, VLC channel is characterized by LED lights' properties and a light propagation model. LED lights mainly have two basic properties, LED's luminous intensity and transmitted optical power. In general, light signal is propagated through LoS and diffused paths. For most indoor scenarios wherein light fixtures are attached to the ceiling and facing down, reflections are significantly weaker than LoS components [15], [16]. As shown in Fig. 1, the propagation model of VLC channel focuses more on LoS path. Therefore, considering the illumination of LED lighting, the luminous intensity in angle ϕ is given by

$$I(\phi) = I(0)\cos^m(\phi), \tag{1}$$

where $I(0)$ is the center luminous intensity of an LED, m is the order of Lambertian emission, and is given by the semiangle at half illuminance of an LED $\phi_{1/2}$ as $m = log2/log(\cos\phi_{1/2})$. A horizontal illuminance E_{hor} at position (x, y) (the origin (0, 0) corresponds to the LED light source) is given by [15]

$$E_{hor} = I(0)\cos^m(\phi)/d^2 \cdot \cos(\psi), \tag{2}$$

where ϕ is the angle of irradiance, ψ is the angle of incidence, and d is the distance between an LED and a detector's surface.

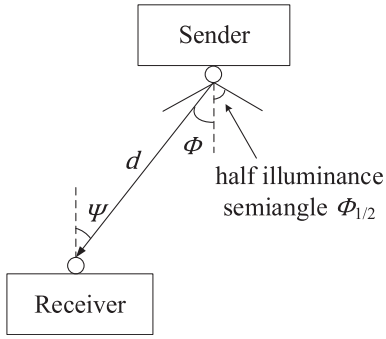


Fig. 1. Propagation model of LoS path.

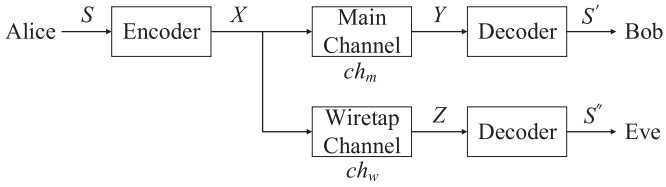


Fig. 2. The diagram of a generic wiretap-channel system.

In an LoS link, the channel gain is given as [15]:

$$G = \begin{cases} \frac{(m+1)A_{RX}n_i^2}{2\pi d^2 \sin^2\psi_c}\cos^m(\phi)T_s(\psi)\cos(\psi), & |\psi| \le \psi_c \\ 0, & |\psi| > \psi_c \end{cases} \tag{3}$$

where A_{RX} is the receiver collection area of the detector in a PD. ψ_c denotes the receiver field-of-view (FoV) semiangle, n_i denotes the refractive index, and $T_s(\psi)$ is the gain of an optical filter. Consequently, the received optical power P_r is derived by the transmitted optical power P_t, as [17]

$$P_r = \alpha R G P_t, \tag{4}$$

where α is the modulation index, and R is the responsivity of a PD.

2.2 Wyner's Wiretap Channel Model

We briefly recap Wyner's wiretap channel model with the illustration in Fig. 2. A n-symbol sequence X, which is encoded from a k-bit message S input by a sender (Alice), is transmitted to a legitimate receiver (Bob) across a BDMC, the main channel (ch_m). Meanwhile, the transmission is eavesdropped by an eavesdropper (Eve) through another BDMC, the wiretap channel (ch_w). Therefore, after the transmission, Bob receives the transmitted sequence as Y, while Eve gets an eavesdropped symbol sequence as Z. Finally, by using decoders, Bob and Eve map Y and Z into estimates S' and S'' of the original message (S), respectively.

In this model, the capacity of the main channel is the mutual information between Alice and Bob:

$$C(ch_m) = I(S;S') = H(S) - H(S|S') = 1 - H(p_{bob}), \tag{5}$$

where $H(\cdot)$ denotes binary entropy function $H(x) = -xlog_2(x) - (1-x)log_2(1-x)$, and p_{bob} is the BER of Bob's output. Note that the source message S is assumed to have a binary uniform distribution and $H(S) = H(0.5) = 1$. For simplicity, the channel is assumed to be a binary symmetric channel (BSC) and the mutual information can be represented by Bob's channel BER.

Similarly, the capacity of the wiretap channel is the mutual information between Alice and Eve:

$$C(ch_w) = I(S;S'') = H(S) - H(S|S'') = 1 - H(p_{eve}), \tag{6}$$

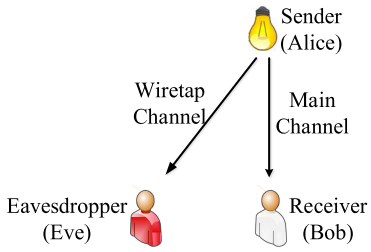


Fig. 3. The SISO indoor VLC wiretap channel model.

where p_{eve} is the BER of Eve's output.

Actually, the mutual information between Alice and Eve is the eavesdropped information of Eve. Wyner proved that such a system is characterized by a single constant C_{sec}, called the secrecy capacity [12], which is calculated as:

$$C_{sec} = C(ch_m) - C(ch_w) = (1 - H(p_{bob})) - (1 - H(p_{eve})) = H(p_{eve}) - H(p_{bob}), \tag{7}$$

given that ch_w is degraded with respect to ch_m, i.e., $C(ch_m) > C(ch_w) \geq 0 \leftrightarrow p_{bob} < p_{eve} \leq 0.5$.

Wyner also proved that secret messages can be transmitted secure and reliable via FEC codes as long as the eavesdropper's channel is degraded with respect to the receiver's channel. Security is usually measured in terms of the mutual information between the original message S and Eve's observations S''. Specifically, the security condition is as the following:

$$\textbf{Security condition}: \quad \lim_{k\to\infty} I(S; S'') = 0. \tag{8}$$

Reliability is measured in terms of the probability of error bits in recovering the message. Specifically, the reliability condition is:

$$\textbf{Reliability condition}: \quad \lim_{k\to\infty} Pr\{S' \neq S\} = 0, \tag{9}$$

According to (6), (8) can be rewritten as:

$$\textbf{Security condition}: \quad \lim_{k\to\infty} Pr\{i \in [k] : S''_i \neq S_i\} = 0.5, \tag{10}$$

Therefore, to design a coding scheme to communicate both securely and reliably, it should be able to make the BER of Bob's estimation (S') nearly 0, while keep the BER of Eve's estimation (S'') nearly 0.5.

2.3 SISO Indoor VLC Wiretap Channel

An example of indoor VLC wiretap channel is shown in Fig. 3. It includes a main channel between a sender (Alice) and a legitimate receiver (Bob), and a wiretap channel between the sender (Alice) and an eavesdropper (Eve). This model corresponds to a realistic scenario that information is sent from only one LED luminaire. Since the channel is single-input and single-output, this model is regarded as a SISO indoor VLC wiretap channel and it can be applied to several point-to-point VLC applications such as indoor VLC, vehicle-to-vehicle VLC, underwater VLC and etc.

In this model, since Bob and Eve are at different locations, their received light signal powers are also different, as well as the signal-to-noise ratio (SNR). As most of indoor VLC systems are using on-off keying (OOK) modulation and the communication links can be regarded as BDMCs, given the SNR at the receiver, the BERs are approximated by $OOK : Q(\sqrt{SNR})$ for OOK modulation assuming a rectangular pulse shape whose duration equals the bit period [15]. Therefore, according to the secrecy capacity of this SISO VLC model is:

$$C_{sec} = C(ch_w) - C(ch_m) = H(p_{eve}) - H(p_{bob}) = H(Q(\sqrt{SNR_{eve}})) - H(Q(\sqrt{SNR_{bob}})), \tag{11}$$

TABLE 1
Simulation Parameters for an Indoor VLC Channel [7]

Room dimensions $(W \times L \times H)$	$5 \times 5 \times 3$ m^3
Light fixture height	3 m
Receivers height	0.85 m
Average optical power per LED	1 W
LED center luminous intensity $I(0)$	30 cd
LED half luminous intensity semi-angle	60°
the modulation index α	10%
Receiver FOV	60°
Lens refractive index n_i	1.5
PD geometrical area A_{RX}	1 cm^2
PD responsivity R	0.54 A/W
Average electrical noise power σ^2	-98.82 dBm

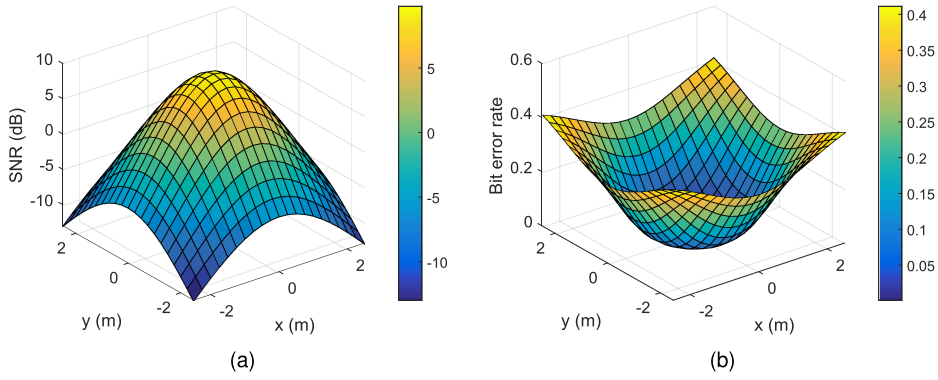


Fig. 4. The spatial distributions of (a) the SNR and (b) the BER in the SISO VLC model.

where p_{Bob}, p_{Eve} are the BERs of Bob's receiver and Eve's receiver, respectively. Thus, to estimate the secrecy capacity of a SISO VLC system, the light signal powers at Bob and Eve should be calculated first.

The parameters shown in Table 1 are used to numerically calculate the light signal power at receiver [7]. Assuming the room dimensions are 5 $\times$ 5 $\times$ 3 m^3, and one LED light luminaire (VLC transmitter) is fixed on the center of the ceiling. The receivers are at a height of 0.85 m, and their FOVs are 60°. Besides, the average electrical noise power is set as -98.82 dBm. A Cartesian coordinate system (x, y) is used at the receivers' height to identify their locations, and the origin (0, 0) corresponds to the center of the room. Since the received light signal power is related to position, the spatial distribution of SNR and BER at the receivers level (0.85 m above the floor level) are shown in Fig. 4.

As shown in Fig. 4(a), the SNR decreases from 9.77 to -12.98 dB versus the distance between Bob and Eve. In contrast, the BER increases from 0.001 to 0.411, as shown in Fig. 4(b).

The distribution of theoretical secrecy capacity for Bob at position (0, 0) against Eve is calculated as shown in Fig. 5. The range of theoretical secrecy capacity is from 0 when Eve is at the center to 0.965 when Eve is at the corners.

2.4 MISO Indoor VLC Wiretap Channel

In general, multiple lighting luminaires are usually deployed for indoor illumination to fulfill indoor lighting standards, e.g., the requirement of an uniform indoor illumination. In this case, information

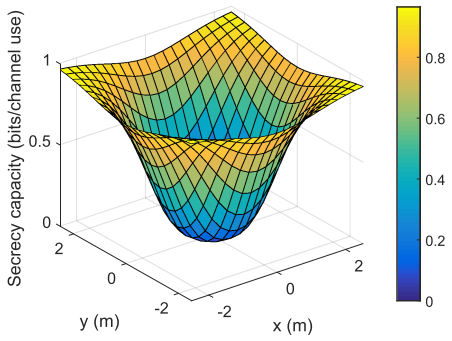


Fig. 5. The distribution of theoretical secrecy capacity in SISO indoor VLC wiretap channel model.

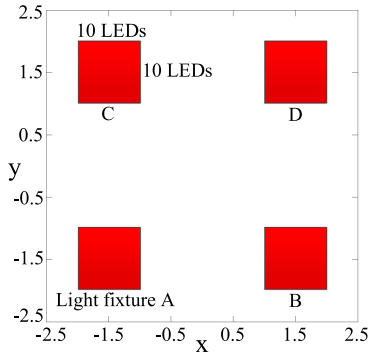


Fig. 6. The positions of four LED luminaires in the room.

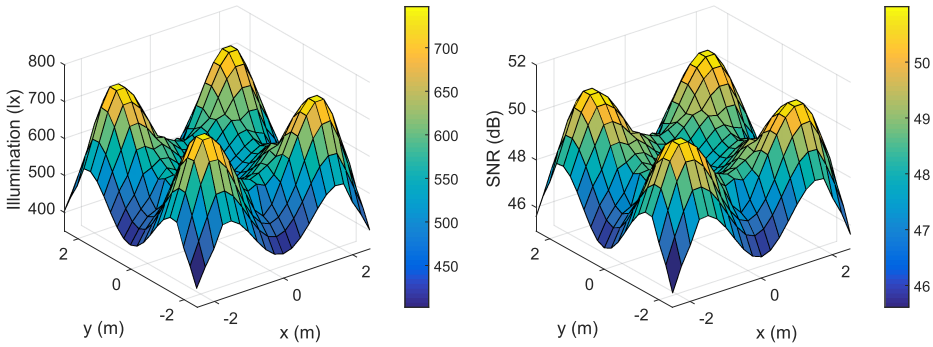


Fig. 7. The distribution of (a) illumination and (b) SNR in the MISO VLC model.

can be sent by multiple LED luminaires for VLC to increase signal power and transmission performance. Therefore, the indoor VLC channel model becomes a MISO VLC model.

To numerically simulate a MISO VLC channel, the parameters for calculation are set as the same as those in Table 1, except that four down-facing LED luminaires are fixed on the ceiling of the room as VLC transmitters, with the positions as shown in Fig. 6. Besides, each luminaire consists 10 $\times$ 10 LEDs, each of which radiates 1 W optical power and its center luminous intensity is 30 cd. The half-illuminance semiangle of each LED is 60°, which is a typical value for commercially-available high-brightness LEDs.

As shown in Fig. 7(a), the horizontal illuminance at any position inside the room varies from 402 to 583 lx, and the uniformity of illuminance is 0.7, as required by CIE/ISO lighting standard for indoor

work places [18]. Since VLC signal power is closely related to illuminance, the corresponding distribution of SNR can be numerically estimated. As shown in Fig. 7(b), the SNR reaches its maximum value (50.99 dB) at the position right under each luminaire, and decreases to its minimum value (45.61 dB) at the corners, while the SNR at the room center is to 47.61 dB. Therefore, the corresponding BER at any position is nearly 0 for OOK modulation because even the minimum value in the SNR distribution is relatively high (45.61 dB).

As we mentioned above, MISO indoor VLC could provide more reliable communication with a uniform illumination. However, for security consideration, according to (11), even Bob is at the position right under a luminaire with the highest SNR, the theoretical secrecy capacity can only reach its maximum value $C_{sec} = H(Q(\sqrt{45.61})) - H(Q(\sqrt{50.99})) = 2.58 \times 10^{-10}$, which is still too close to 0, when Eve is at the corners. It means that an eavesdropper at any position in the room can have a wiretap channel, which is nearly not degraded with respect to the main channel. Thus, the MISO indoor VLC wiretap channel model is more complicated. Note that the SISO indoor VLC wiretap channel model may also have this problem when Bob is not at the position with the highest SNR. For simplicity, we take the SISO model and the MISO model as the example for a degraded VLC wiretap channel and an undegraded VLC wiretap channel, respectively.

3. Physical-Layer Secure Coding Schemes for VLC Wiretap Channel

In this section, a polar codes-based secure coding scheme is first proposed for the degraded VLC wiretap channel model to achieve physical-layer security and transmission reliability simultaneously. Then, an enhanced secure coding scheme with a feedback channel is proposed for the case that the wiretap channel is not degraded. The numerical models of SISO and MISO in Section 2 are used as typical examples to examine the performances of the proposed coding schemes.

3.1 Polar Codes-Based Secure Coding Scheme for VLC Degraded Wiretap Channel

Polar codes are the first deterministic construction of capacity-achieving codes for symmetric BDMCs proposed by Arikan [13]. In 2011, Mahdavifar and Vardy proved that the secrecy capacity of wiretap channels could be achieved using polar codes [19]. The basic concept is to utilize the gap of channel polarization for main channel and wiretap channel. As the wiretap channel is degraded with respect to the main channel, the good bit-channels it has are more than that of the main channel when both of them go through the processes of channel splitting and channel combination.

In details, given Bob's main channel $ch_m = \langle \{0, 1\}, Y, W_m \rangle$ and Eve's wiretap channel $ch_w = \langle \{0, 1\}, Z, W_w \rangle$, and ch_w is degraded with respect to ch_m. W_m and W_w are the matrices of transition probabilities of the main channel and the wiretap channel, respectively. Formally, we define three subsets based on the set of bit-channels $[n]$ as follows:

$$R \overset{def}{=\!=} \mathscr{G}_n(W_w, \beta) \tag{12}$$

$$A \overset{def}{=\!=} \mathscr{G}_n(W_m, \beta) \backslash \mathscr{G}_n(W_w, \beta) \tag{13}$$

$$B \overset{def}{=\!=} \mathscr{B}_n(W_m, \beta) \tag{14}$$

Notice that the sets R, A, B are disjoint and $R \cup A \cup B = [n]$.

Then, as illustrated in Fig. 8, secret transmission can be achieved by transmitting random bits over those bit-channels R that are good for both Eve and Bob, transmitting information bits over those bit-channels A that are good for Bob but bad for Eve, and transmitting frozen bits over those bit-channels B that are bad for both Bob and Eve. Let $[n] = \{1, 2, ..., n\}$, and let $\beta < 1/2$ be a fixed

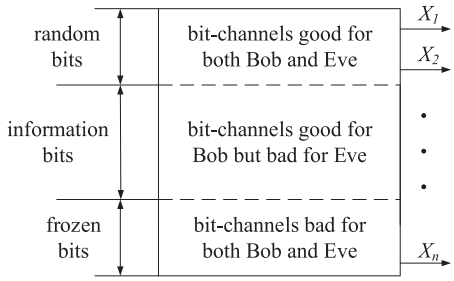


Fig. 8. The polar codes-based secure coding scheme.

TABLE 2
Practical Secrecy Rate Achieved in the SISO VLC Degraded Wiretap Channel Model

Eve's position	BER of Eve (p_{eve})	Code rate (R_c)	Secrecy capacity (C_{sec})	R_c/C_{sec}
(2.5, 2.5)	0.411	0.83	0.9656	85.96%
(1.75, 2.0)	0.315	0.71	0.8875	80%
(1.5, 1.5)	0.215	0.52	0.7395	70.32%
(1.25, 1.0)	0.101	0.25	0.4607	54.26%

positive constant. Then the index sets of the good and bad channels are given by [13]

$$\mathscr{G}_n(W,\beta) \overset{def}{=\!=} \left\{ \sum_{i\in[n]} Z(W_i) \le 2^{-n^\beta} \right\} \tag{15}$$

$$\mathscr{B}_n(W,\beta) \overset{def}{=\!=} [n]\backslash\mathscr{G}_n(W,\beta) \tag{16}$$

where $Z(W)$ is Bhattacharyya parameter defined as:

$$Z(W) \overset{def}{=\!=} \sum_{y\in\mathscr{Y}} \sqrt{W(y|0)W(y|1)} \tag{17}$$

The coding scheme was implemented in Matlab and tested using the SISO indoor VLC channel described in Section 2.3 as a typical example of VLC degraded wiretap channel model. The length of codewords was set to $n = 2,048 = 2^{11}$ bits. Note that the position of Bob is at (0, 0) and the BER of the main channel is $p_{bob} = 0.001$ according to Fig. 4(b). Then, the performance of the coding scheme was evaluated with several positions of Eve, as well as the corresponding channel BERs, as shown in Table 2. Therefore, given the BERs of the main channel and the wiretap channels, the Bhattacharyya parameters for the main channel and the wiretap channels were calculated. According to the calculated Bhattacharyya parameters, we selected appropriate bit-channels to design the subsets of R, A, and B for a target BER of 10^{-9} and a security mutual information of 10^{-30}. Then, a series of numerical simulations were carried out to simulate light signal transmission and the implemented coding scheme was used to correct the error bits introduced during transmission. Numerical results show that the decoder output of Bob has BERs lower than 10^{-9} and the decoder output of Eve has BERs nearly 0.5. It means that the conditions in (9) and (10) are fulfilled and the proposed coding scheme can guarantee security and reliability for the communication between Alice and Bob. For the given positions of Eve, the practical code rate and the practical secrecy rate (R_c/C_{sec}) achieved using the proposed coding scheme are shown in Table 2. For Eve's position at room corners where Eve has the lowest SNR of received signal, the theoretical secrecy capacity is $C_{sec} = H(0.411) - H(0.001) = 0.9656$. Since the practical code rate is 0.83, the practical secrecy rate achieved by the proposed coding scheme is $0.83/0.9656 = 0.8596 = 85.96\%$. For Eve's position near to Bob, e.g. (1.25, 1.0), the theoretical secrecy capacity

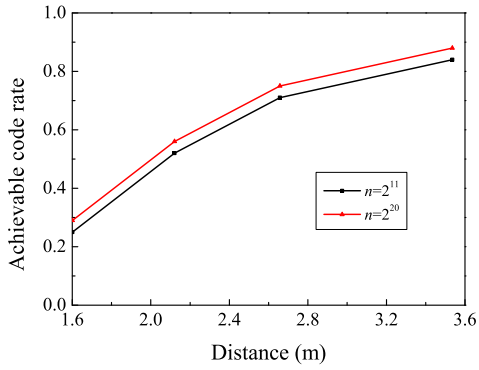


Fig. 9. Practical secrecy code rate versus Eve's distance from the center.

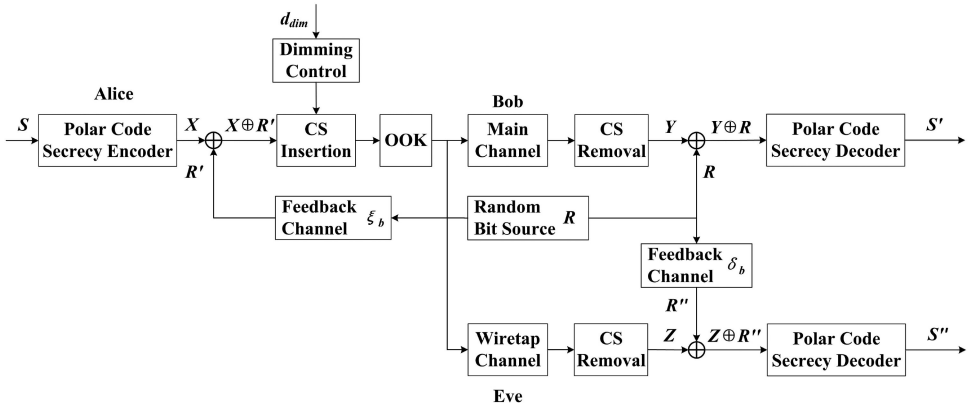


Fig. 10. The enhanced polar codes-based physical-layer secure coding scheme with a feedback channel.

decreases to $C_{sec} = H(0.101) - H(0.001) = 0.4607$ and the practical secrecy rate also decreases to 54.26%. The decrement of practical secrecy rate is due to the finite length effect and the secrecy capacity can be asymptotically achieved.

The achievable secrecy code rates shown in Table 2 are also plotted with square markers in Fig. 9 as a function of Eve's distance from the center at a height of 0.85 m. As a comparison, the achievable secrecy code rates when codeword length is 2^{20} bits are also plotted with dot markers in Fig. 9. It can be seen that the achievable secrecy code rate increases when Eve is away from the center.

3.2 Enhanced Physical-Layer Secure Coding Scheme with a Feedback Channel for VLC Undegraded Wiretap Channel

To achieve secure transmission against VLC undegraded wiretap channel, where the wiretap channel ($A \rightarrow E$) is not degraded with respect to the main channel ($A \rightarrow B$), an enhanced secure coding scheme is proposed by introducing a feedback channel to degrade the wiretap channel equivalently [20].

Fig. 10 shows the structure of the enhanced coding scheme. The key element is the feedback channel from Bob to Alice ($B \rightarrow A$) with a crossover probability of ξ_b. For each communication, Bob feeds back a n-bit Bernoulli random sequence R with the expectation of $E[R] = 0.5$. Note that the feedback channel is not error free and Alice receives the feedback sequence R as R'.

Therefore, for the communication between Alice and Bob, if Alice wants to send message S securely to Bob, she first encodes S into an n-bit sequence X using the polar code secrecy encoder,

and then uses exclusive or operations to combine the encoded sequence X with the received feedback sequence R' as $X \oplus R'$. Before Alice sends the encoded codeword $X \oplus R'$ to Bob, she needs to insert some compensation symbols (CSs) according to dimming ratio d_{dim} to fulfill the requirement of dimmable illumination, as suggested in [21]. And then, the encoded codeword with inserted CSs is transmitted to Bob via OOK modulation.

At the receiver's side, Bob first demodulate the transmitted light signals and remove the inserted CSs to extract the transmitted codeword Y. Note that the OOK demodulation module is not shown in this figure for simplicity. Then, Bob uses exclusive or operations to combine Y with the local random sequence R as $Y \oplus R$ and try to decode $Y \oplus R$ and recover S using the polar code secrecy decoder. The main task of the decoder is to correct the error bits in $Y \oplus R$, which include two parts, i.e., the error bits introduced by the feedback channel (denoted as $e_{b\to a}$) and those introduced by the main channel (denoted as $e_{a\to b}$). Since $X \oplus R' = X \oplus R \oplus e_{b\to a}$, and $Y = (X \oplus R') \oplus e_{a\to b}$ Therefore, $Y \oplus R$ can be rewritten as $Y \oplus R = (X \oplus R \oplus e_{b\to a} \oplus e_{a\to b}) \oplus R = X \oplus e_{b\to a} \oplus e_{a\to b}$. Denote $X' = X \oplus e_{b\to a} \oplus e_{a\to b}$. Using the polar code secrecy decoder optimized to handle the bit error pattern $X' \oplus X$, Bob can successfully recover $S' = S$ from X'.

As for the eavesdropper, Eve may also wiretap the feedback channel with a crossover probability of δ_b and get a wiretapped feedback sequence R''. Then, for each transmission over the main channel, Eve first wiretaps the transmitted symbols and do the same operations as Bob to extract an eavesdropped sequence as Z. Eve also uses exclusive or operations to combine Z with the wiretapped feedback sequence R'' as $Z \oplus R''$ and try to recover S from it. However, $Z \oplus R''$ includes three parts of error bits, i.e., the error bits introduced by the feedback channel (denoted as $e_{b\to a}$), the error bits introduced by the wiretap feedback channel (denoted as $e_{b\to e}$) and those introduced by the wiretap channel (denoted as $e_{a\to e}$). And $Z \oplus R''$ can be rewritten as $Z \oplus R'' = X \oplus e_{b\to a} \oplus e_{b\to e} \oplus e_{a\to e}$. Denote $X'' = X \oplus e_{b\to a} \oplus e_{b\to e} \oplus e_{a\to e}$. Eve may try to recover $S'' = S$ from X''. However, since the parameters of the enhanced coding scheme is optimized for the bit error pattern $X' \oplus X$ instead of the bit error pattern $X'' \oplus X$, Eve's decoder cannot successfully correct the error bits in X''. The worse, it introduces more error bits into S'' due to the error propagation mechanism of the successive cancellation decoding algorithm of polar codes. For security consideration, the parameters of the enhanced coding scheme can be carefully designed to fulfill the security condition (10).

In this paper, MISO indoor VLC channel is taken as an example of VLC undegraded wiretap channel model. As analyzed in Section 2.4, both the main channel and the wiretap channel are nearly error free. With the introduced feedback channel, the equivalent BER of Bob is $\xi_{bob} = \xi_b$, while the equivalent BER of Eve is

$$\xi_{eve} = \xi_b + \delta_b - 2\xi_b\delta_b. \tag{18}$$

Therefore, Eve's wiretapping is degraded with the a reliability gap

$$\xi_{eve} - \xi_{bob} = \delta_b(1 - 2\xi_b) \geq 0, \tag{19}$$

and the gap can be utilized to achieve secure transmission using the coding scheme proposed in Section 3.1. And in theory, the secrecy capacity is

$$C_{sec} = H(\xi_{eve}) - H(\xi_{bob}) = H(\xi_b + \delta_b - 2\xi_b\delta_b) - H(\xi_b). \tag{20}$$

In practice, the feedback channel can be a weak visible light uplink from Bob toward one LED luminaire fixed on room's ceiling. Since the uplink light signal is weak and has a LoS propagation nature, Eve's wiretapped feedback channel is degraded with respect to Alice's feedback channel.

3.3 Performance of The Enhanced Coding Scheme

A series of numerical simulations were conducted under the MISO VLC undegraded wiretap model to evaluate the performances of the enhanced physical-layer secure coding scheme with a feedback channel. In the simulations, the crossover probability of the feedback channel $B \to A$ (ξ_b) was fixed as 0.01, and the equivalent BER of Bob (ξ_{bob}) is 0.01. The crossover probabilities of the feedback

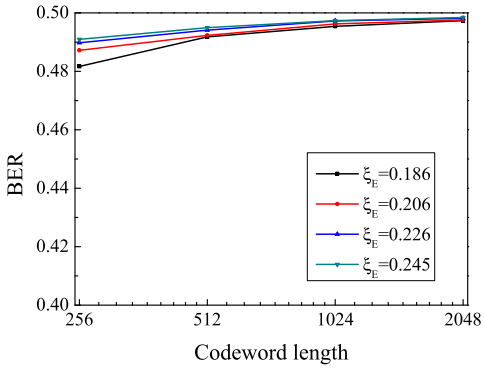


Fig. 11. The BER of Eve's output in the MISO VLC wiretap model.

channel $B \rightarrow E$ (δ_b) were vaired from 0.18 to 0.24 with a step-length of 0.02. After being calculated, the equivalent BERs of Eve (ξ_{eve}) are 0.186, 0.206, 0.226, and 0.245, and the theoretical secrecy capacities are 0.6122, 0.6530, 0.6902 and 0.7225, respectively. The codeword lengths were set from 256-bit to 2048-bit. Considering the illumination requirements [14], we selected a typical code rate of 0.5 for our numerical simulations. For each codeword length, 10,000 data frames were tested using the polar code secrecy en/decoder.

Numerical results show that the BER and frame error rate (FER) of Bob's output are both nearly 0 since the parameters of the enhanced coding scheme have been optimized for ξ_{bob}. Therefore, the reliability condition for data transmission is satisfied. Contrarily, Eve has relatively high BERs and FERs, as shown in Fig. 11. With the increment of codeword length, the BERs and FERs of Eve's output grow to nearly 0.5 and 1, respectively. It indicates that the conditions in (9) and (10) are simultaneously fulfilled and the secret messages sent from Alice can be hided to the unauthorized receiver Eve using the enhanced coding scheme. Furthermore, with the same code rate and codeword length, the BER of Eve's output is increased as the equivalent BER ξ_{eve} rises. It means that the security of the VLC system can be further enhanced with the degradation level of the wiretap channel increasing gradually.

Consequently, for undegraded VLC wiretap channel, the enhanced coding scheme can provide security and reliability simultaneously without the limitation on receiver's position, and the security can be increased with the increment of the degradation level of the wiretap channel. In addition, the secrecy capacity of the MISO VLC wiretap system can be asymptotically achieved for transmitting secret information.

4. Conclusion

Visible light communication (VLC) has attracted increasing attention as it can simultaneously provide illumination and communication services. Since the broadcast nature of the VLC channel makes VLC links inherently susceptible to eavesdropping by unauthorized users. In this paper, a polar codes-based secure coding scheme is proposed to provide the physical-layer security for indoor VLC systems, as well as the reliability. The secrecy capacities of two indoor VLC wiretap channel models are analyzed considering the requirements of illumination and reliable communication. Numerical results show that for VLC degraded wiretap channel model, the proposed coding scheme can be applied directly to provide the functionalities of security and reliability simultaneously. Furthermore, an enhanced coding scheme with a feedback channel is proposed to handle the more complicated case that the wiretap channel is not degraded with respect to the main channel. With the feedback channel, the wiretap channel can be equivalently degraded, and the security can be achieved and increased gradually with the increment of the degradation level of the wiretap channel without the limitation on receiver's position, as well as reliability. Meanwhile, the secrecy

capacities can be asymptotically achieved for the indoor VLC systems. Besides, taking advantages of polar codes' good performances on error correction, DC-balanced and run-length limited without additional techniques, our proposed coding scheme can also fulfill the lighting related requirements and can be generalized to dimmable VLC systems for their secure and reliable communications.

References

[1] A. Jovicic, J. Li, and T. Richardson, "Visible light communication: Opportunities, challenges and the path to market," *IEEE Commun. Mag.*, vol. 51, no. 12, pp. 26–32, Dec. 2013.

[2] *IEEE Standard for Local and Metropolitan Area Networks-part 15.7: Short-Range Wireless Optical Communication Using Visible Light*, IEEE Std. 802.15.7-2011, 2011.

[3] 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.

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

[5] 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.*, 2015, pp. 1165–1169.

[6] 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.

[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] 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, 2016.

[9] 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, Oct. 2016, Art. no. 7905914.

[10] 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. 2016.

[11] F. I. K. Mousa, N. A. S. Almaadeed, K. K. Busawon, A. Bouridane, and R. Binns, "Secure MIMO visible light communication system based on user's location and encryption," *J. Lightw. Technol.*, vol. 35, no. 24, pp. 5324–5334, 2017.

[12] A. D. Wyner, "The wire-tap channel," *Bell Labs Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[13] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[14] J. Fang *et al.*, "An efficient flicker-free FEC coding scheme for dimmable visible light communication based on polar codes," *IEEE Photon. J.*, vol. 9, no. 3, Jun. 2017, Art. no. 7903310.

[15] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 100–107, Feb. 2004.

[16] A. Al-Kinani, C.-X. Wang, H. Haas, and Y. Yang, "Characterization and modeling of visible light communication channels," in *Proc. IEEE 83rd Veh. Technol. Conf.*, 2016, pp. 1–5.

[17] J. M. Kahn and J. R. Barry, "Wireless infrared communications," *Proc. IEEE*, vol. 85, no. 2, pp. 265–298, Feb. 1997.

[18] *008/e-2001: Lighting of Indoor Work Places*, ISO8995, Vienna, Austria, CIE, pp. 5–6, 2001.

[19] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[20] G. T. Amariucai and S. Wei, "Feedback-based collaborative secrecy encoding over binary symmetric channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 8, pp. 5248–5266, Aug. 2012.

[21] S. H. Lee, S.-Y. Jung, and J. K. Kwon, "Modulation and coding for dimmable visible light communication," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 136–143, Feb. 2015.

[22] Z. Che, J. Fang, Z. L. Jiang, X. Yu, G. Xi, and Z. Chen, "A physical-layer secure coding scheme for visible light communication based on polar codes," in *Proc. IEEE Conf. Lasers Electro-Optics Pac. Rim*, 2017, pp. 1–2.