LETTER

Enhanced Secure Transmission for Indoor Visible Light Communications

Sheng-Hong LIN[†,††], **Jin-Yuan WANG**[†,††a)], **Ying XU**[†††], ***Nonmembers***, ***and*** **Jianxin DAI**[††††], ***Member***

SUMMARY This letter investigates the secure transmission improvement scheme for indoor visible light communications (VLC) by using the protected zone. Firstly, the system model is established. For the input signal, the non-negativity and the dimmable average optical intensity constraint are considered. Based on the system model, the secrecy capacity for VLC without considering the protected zone is obtained. After that, the protected zone is determined, and the construction of the protected zone is also provided. Finally, the secrecy capacity for VLC with the protected zone is derived. Numerical results show that the secure performance of VLC improves dramatically by employing the protected zone.

key words: *visible light communications, physical-layer security, secrecy capacity, protected zone*

1. Introduction

As a complement to radio frequency wireless communications (RFWC), visible light communications (VLC) has been regarded as an efficient access solution for future communications. VLC is a kind of optical wireless communication using visible-light spectrum from 380 to 780 nm [1]. VLC transmits data by modulating the intensity emitted by a light emitting diode (LED) at a rate much faster than the persistence of human eye. At the receiver, a photodiode (PD) is employed to perform optical-to-electrical conversion. To be applied into indoor environment, illumination and communication are simultaneously implemented in VLC. Due to the broadcast characteristics, the information security in VLC has become a key issue to be addressed. Recently, physical-layer (PLY) security has emerged as a promising way to improve the security of VLC.

In RFWC, the PLY security was first studied by Shannon [2]. Consider the receiver noise, Wyner proposed the secrecy capacity (SC) over wiretap channels [3]. Therefore, the level of PLY security can be measured by the SC [4]. For indoor VLC, by using a truncated generalized normal distribution for the input signal, the SC was investigated in [5]. By optimizing the input distribution, tighter bounds on the SC for VLC were further obtained in [6].

After deriving the SC, the next step is to exploit the PLY security improvement schemes. In [7] and [8], the optimal and robust secure beamforming schemes for VLC were studied. By using the jamming scheme, the PLY security of VLC was improved in [9]. In [10], an artificial noise-aided precoding scheme was proposed in an VLC wiretap channel. A Polar code based secure coding scheme was proposed in [11] to improve the PLY security of VLC. In [12], the protected zone was utilized to improve the secure performance of RFWC. By using the protected zone, the attacks at close quarters can be prevented and the secure performance can be improved. As it is known, the signal constraints and channel model in VLC are quite different from that in RFWC [6]. To the best of our knowledge, the protected zone based PLY security for indoor VLC has not been discussed.

Motivated by the above literature, this letter considers an indoor VLC network including a transmitter Alice, a legitimate receiver Bob and a passive eavesdropper Eve. Considering the characteristics of VLC, the non-negativity and the dimmable average optical intensity constraint are considered. Based on our previous work [6], the lower bound on the SC for VLC is obtained. By employing the protected zone, the SC for indoor VLC is further derived. When Bob and Eve are not located in the same receiver plane, the derived protected zone can be determined by the positions of Alice and Bob. Specially, when Bob and Eve are located in the same receiver plane, the protected zone is a disk whose center is the projection point of Alice and radius is the distance between Bob and the projection point of Alice. Finally, numerical results verify the effectiveness of the VLC system with the protected zone.

2. System Model

Consider a classic three-node indoor VLC system as shown in Fig. 1, which consists of a transmitter Alice, a legitimate receiver Bob and a passive eavesdropper Eve. The room size is $J \times K \times L$. Alice is installed on the ceiling, Bob and Eve can be deployed in any possible positions of the room. The position set for Bob and Eve is denoted as $\mathcal{S}$. The coordinates of Alice, Bob and Eve are denoted as (a, b, c), $(x_{\mathrm{B}}, y_{\mathrm{B}}, z_{\mathrm{B}})$ and $(x_{\mathrm{E}}, y_{\mathrm{E}}, z_{\mathrm{E}})$, respectively. At the transmitter, Alice is equipped with an LED to transmit the optical signal. At the receiver, a PD is individually employed at Bob and Eve to transform the optical signal to electrical signal. When

Manuscript received November 19, 2019.
Manuscript publicized February 25, 2020.

[†]The authors are with College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, China.
[††]The authors are also with Shandong Key Laboratory of Optical Communication Science and Technology, Liaocheng University, China.
[†††]The author is with Engineering Training Center, Nantong University, China.
[††††]The author is with School of Science, Nanjing University of Posts and Telecommunications, China.
a) E-mail: jywang@njupt.edu.cn

DOI: 10.1587/transinf.2019EDL8202

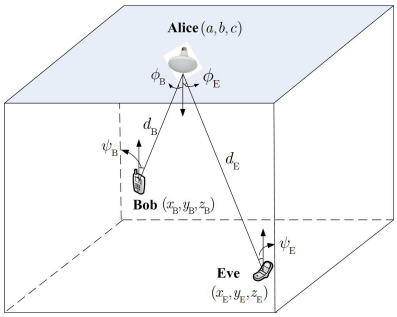


Fig. 1 An indoor VLC network.

Alice transmits information to Bob, Eve can also receive the information. Therefore, the received electrical signals at Bob and Eve can be written as

$$\begin{cases} Y_{\mathrm{B}} = H_{\mathrm{B}}X + Z_{\mathrm{B}} \\ Y_{\mathrm{E}} = H_{\mathrm{E}}X + Z_{\mathrm{E}} \end{cases}, \tag{1}$$

where X is the transmitted optical intensity signal. $Z_{\mathrm{B}} \sim N(0,\sigma_{\mathrm{B}}^2)$ and $Z_{\mathrm{E}} \sim N(0,\sigma_{\mathrm{E}}^2)$ are Gaussian noises at Bob and Eve, where σ_{B}^2 and σ_{E}^2 are noise variances.

In (1), X is the instantaneous optical intensity emitted by the LED, which should be non-negative, i.e.,

$$X \geq 0. \tag{2}$$

To satisfy the illumination requirement, the average optical intensity constraint for VLC is given by

$$E(X)=\xi P, \tag{3}$$

where $0 < \xi \leq 1$ denotes the dimming target, and P denotes the nominal optical intensity of the LED.

In (1), the channel coefficient H_k (k = B for Bob; k = E for Eve) can be written as

$$H_k = \frac{(m+1)A}{2\pi d_k^2} T_s g \cos^m(\phi_k)\cos(\psi_k)\mathrm{rect}\left(\frac{\psi_k}{\Psi}\right), \tag{4}$$

where d_k and ϕ_k denote the distance and the irradiance angle between Alice and Bob (or Eve); A denotes the area of PD, m is the order of Lambertian emission, g is the concentrator coefficient of the PD, and T_s is the optical filter gain, Ψ is the field of view of the PD, rect$(\cdot)$ represents the rectangular function.

Assume that the normal vectors of the transceiver planes are perpendicular to the ceiling, we have $\cos(\phi_k) = \cos(\psi_k) = |c - z_k| / d_k$. Submitting it into (4), the channel coefficient is further expressed as

$$H_k = \Xi \frac{|c - z_k|^{m+1}}{\left[(a-x_k)^2 + (b-y_k)^2 + (c-z_k)^2\right]^{\frac{m+3}{2}}}, \tag{5}$$

where $\Xi \triangleq (m+1)AT_s g/(2\pi)$.

3. Secrecy Performance Enhancement Scheme

From *Theorem 1* in [6], a lower bound of the SC for VLC with constraints (2) and (3) is given by

$$C_{\mathrm{s}} = \begin{cases} \frac{1}{2}\ln\left(\frac{\sigma_{\mathrm{E}}^2}{2\pi\sigma_{\mathrm{B}}^2}\cdot\frac{e\xi^2P^2H_{\mathrm{B}}^2+2\pi\sigma_{\mathrm{B}}^2}{H_{\mathrm{E}}^2\xi^2P^2+\sigma_{\mathrm{E}}^2}\right), & \text{if } \frac{H_{\mathrm{B}}}{\sigma_{\mathrm{B}}} \geq \frac{H_{\mathrm{E}}}{\sigma_{\mathrm{E}}} \\ 0, & \text{if } \frac{H_{\mathrm{B}}}{\sigma_{\mathrm{B}}} < \frac{H_{\mathrm{E}}}{\sigma_{\mathrm{E}}} \end{cases}$$
$$\text{s.t.} \quad (x_{\mathrm{E}}, y_{\mathrm{E}}, z_{\mathrm{E}}) \in \mathcal{S}. \tag{6}$$

In (6), when given the positions of Alice and Bob, the SC varies with Eve's position. When Eve moves close to Alice, the SC may be zero, and thus the secure transmission cannot be guaranteed.

To improve the secure performance of VLC, an eavesdropper-free area, the protected zone is employed for the area that the SC is zero. Here, the set of the protected zone is defined as

$$\mathcal{P} = \left\{(x_{\mathrm{E}}, y_{\mathrm{E}}, z_{\mathrm{E}}) \middle| H_{\mathrm{B}} \leq \frac{\sigma_{\mathrm{B}}}{\sigma_{\mathrm{E}}} H_{\mathrm{E}}\right\}. \tag{7}$$

Submitting (5) into (7), the protected zone is given by

$$\mathcal{P} = \left\{(x,y,z) \middle| \left|\frac{c-z_{\mathrm{B}}}{c-z}\right|^{m+1} \leq \frac{\sigma_{\mathrm{B}}}{\sigma_{\mathrm{E}}} \times \left[\frac{(a-x_{\mathrm{B}})^2+(b-y_{\mathrm{B}})^2+(c-z_{\mathrm{B}})^2}{(a-x)^2+(b-y)^2+(c-z)^2}\right]^{\frac{m+3}{2}}\right\}. \tag{8}$$

Therefore, Eve cannot be deployed in $\mathcal{P}$, i.e., $(x_{\mathrm{E}}, y_{\mathrm{E}}, z_{\mathrm{E}}) \in \mathcal{S} \setminus \mathcal{P}$, where $\mathcal{S} \setminus \mathcal{P}$ denotes the set of elements of $\mathcal{S}$ which are not in $\mathcal{P}$.

Remark 1: (Position information acquisition at Alice) Before constructing the protected zone, Alice needs to know the position of Bob. In the considered VLC system, the reverse link can be established by using infrared, Wi-Fi, or RF technologies [13]. As a legitimate receiver, Bob can actively report his position to Alice through the reverse link. However, Eve is an eavesdropper, who will hide her location. Actually, to construct the protected zone, Alice does not need to know Eve's position but needs the ability to remove her when Eve is located in the protected zone.

Remark 2: (The method of detecting Eve) Before transmission, Alice can construct the protected zone according to (8). Alice scans and detects the nearby bugging devices via various detecting devices (such as a metal detector, evolved heat detector, x-ray detector, or the leaked local oscillator power detector). As the passive eavesdropper, Eve has no information about the protected zone. If Eve is located out of the protected zone, she cannot be detected by Alice and thus is covert. However, if Eve is located in the protected zone, she will be detected by Alice and then be cleared out of the protected zone.

Remark 3: (Construction method of the protected zone) The protected zone can be constructed either inherently or intentionally. When the transmission nodes are deployed in restricted-access areas (such as equipment rooms, the top of communication towers or on roofs), so this physical layout inherently defines a protected zone. When no

protected zone physically exists, we may also wish to intentionally deploy a security perimeter to achieve a given level of secrecy. The derived protected zone in (9) is meaningful and gives us insights to improve PLY security of the VLC system.

Remark 4: (Special Case) If Bob and Eve are located in the same receiver plane, i.e., $z_B = z_E = z_0$, the set of the protected zone in (8) reduces to

$$\mathcal{P} = \left\{(x, y) \middle| (x-a)^2 + (y-b)^2 \le \Lambda \right\}, \tag{9}$$

where Λ is defined as

$$\Lambda = \frac{(a-x_B)^2+(b-y_B)^2+(c-z_0)^2}{\left(\frac{\sigma_E}{\sigma_B}\right)^{\frac{2}{m+3}}} - (c-z_0)^2. \tag{10}$$

This indicates that, when Bob and Eve are deployed in the same plane, the protected zone is a disk with center (a, b) and radius $\sqrt{\Lambda}$. More specifically, if $\sigma_B = \sigma_E$, the protected zone in (9) becomes a disk with center (a, b) and radius $\sqrt{(a-x_B)^2 + (b-y_B)^2}$.

According to (6) and (8), the SC for VLC with the protected zone is given by

$$C_s = \begin{cases} \frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2} \cdot \frac{e\xi^2 P^2 H_B^2 + 2\pi\sigma_B^2}{H_E^2\xi^2P^2+\sigma_E^2}\right), & \text{if } \frac{H_B}{\sigma_B} \ge \frac{H_E}{\sigma_E} \\ 0, & \text{if } \frac{H_B}{\sigma_B} < \frac{H_E}{\sigma_E} \end{cases}$$
$$\text{s.t. } (x_E, y_E, z_E) \in \mathcal{S} \setminus \mathcal{P}. \tag{11}$$

Therefore, the protected zone based scheme contributes to secrecy by preventing attacks at close quarters.

4. Numerical Results

Here, the secrecy performance will be evaluated. The main simulation parameters are given in Table 1.

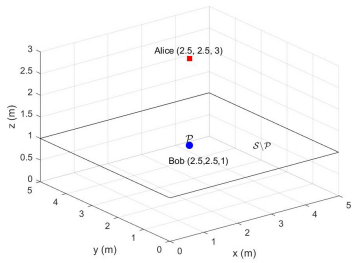
Figure 2(a) shows the protected zone when $(x_B, y_B) = (2.5\text{m}, 2.5\text{m})$ and $z_B = z_E = 1\text{m}$. In the simulation, Bob and Eve are located in the same receiver plane, and Bob is located below Alice. The zone $\mathcal{P}$ is the position of Bob, and the other positions of the receiver plane belong to zone $\mathcal{S}\setminus\mathcal{P}$. This indicates that the secure transmission can be guaranteed as long as Eve is not located at the position of Bob. Figure 2(b) shows the protected zone when $(x_B, y_B) = (2\text{m}, 1\text{m})$ and $z_B = z_E = 1\text{m}$. In this figure, Bob is far away from the projection point of Alice on the receiver plane. Compared with Fig. 2(a), the protected zone $\mathcal{P}$ in Fig. 2(b) enlarges. In Fig. 2(b), the protected zone is a disk whose center is the projection point of Alice and radius is the distance between Bob and the projection point of Alice, which coincides with that in *Remark 4*.

Table 1 Main simulation parameters

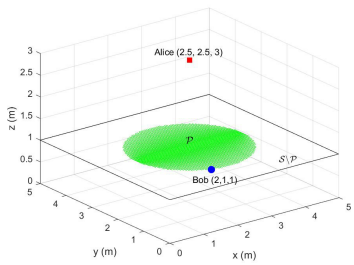
Description	Symbol	Value
Room size	$J \times K \times L$	$5\text{m} \times 5\text{m} \times 3\text{m}$
Position of Alice	(a, b, c)	(2.5m, 2.5m, 3m)
Noise variances	σ_B^2, σ_E^2	0 dB
Lambertian emission order	m	1

Figure 3 shows the average SC for VLC with and without the protected zones when Bob and Eve are located in the same plane. As can be seen, when Bob is just located below Alice, the SC does not improve at all. This is because the protected zone is small enough to be ignored. However, when Bob is located at (2 m,1 m,1 m), the secrecy performance improves by using the protected zone. That is, when Bob is far away from the projection point of Alice, the protected zone based scheme is an efficient method to improve PLY security.

In practice, Bob and Eve are not necessarily located on the same receiver plane. For an arbitrarily located Eve, Figs. 4(a) and 4(b) show the protected zones when $(x_B, y_B, z_B) = (2.5\text{m}, 2.5\text{m}, 1\text{m})$ and $(x_B, y_B, z_B) = (2\text{m}, 1\text{m}, 1\text{m})$, respectively. For these two cases, the protected zones are large and look like ellipsoids. As can be found, the protected zone is almost determined by the rel-



(a) $(x_B, y_B) = (2.5\text{m}, 2.5\text{m})$



(b) $(x_B, y_B) = (2\text{m}, 1\text{m})$

Fig. 2 The protected zone when $z_B = z_E = 1\text{m}$.

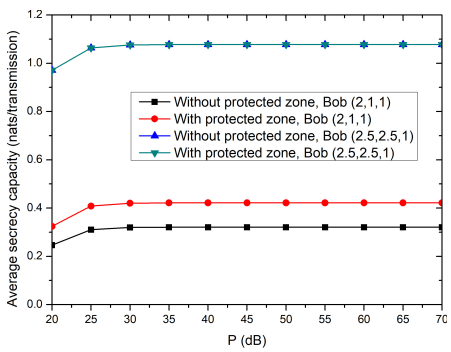
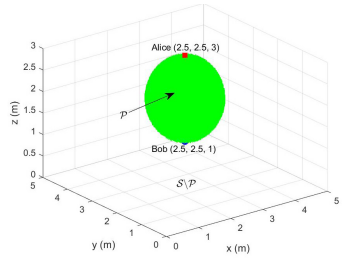
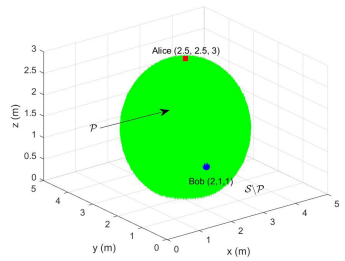


Fig. 3 Average SC when $z_B = z_E = 1\text{m}$.



(a) $(x_{\mathrm{B}}, y_{\mathrm{B}}, z_{\mathrm{B}}) = (2.5\mathrm{m}, 2.5\mathrm{m}, 1\mathrm{m})$



(b) $(x_{\mathrm{B}}, y_{\mathrm{B}}, z_{\mathrm{B}}) = (2\mathrm{m}, 1\mathrm{m}, 1\mathrm{m})$

Fig. 4 The protected zone when Eve is arbitrarily deployed.

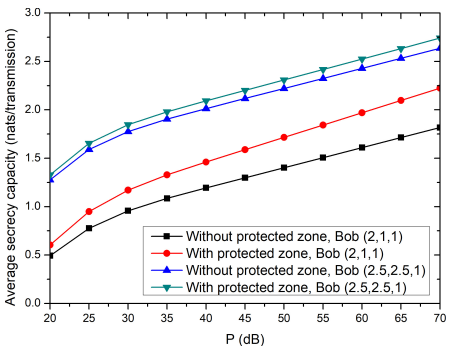


Fig. 5 Average SC when Bob and Eve are not located in the same receiver plane.

ative positions of Alice and Bob. In other words, the protected zone enlarges with the increase of the distance between Alice and Bob.

Without the constraint that Bob and Eve are located in the same receiver plane, Fig. 5 shows the average SC for the VLC with and without the protected zone. As is seen, the average SC improves by using the protected zone. Moreover, the performance improvement is observed to be more prominent for large distance between Alice and Bob. This indicates that it is necessary to employ the protected zone for VLC.

5. Conclusions

In this letter, the protected zone based PLY security improvement scheme is proposed for VLC. The derived protected zone can be directly determined according to the geometrical relationship between Alice and Bob, which is quite different from that for RFWC. By employing the protected zone, the secure performance of the VLC improves dramatically.

Acknowledgements

This work has been supported by National Natural Science Foundation of China (61701254), the fund of the Shandong Key Laboratory of Optical Communication Science and Technology in Liaocheng University (SDOC201901), and Natural Science Foundation of Jiangsu Province (BK20170901).

References

[1] J. Luo, L. Fan, and H. Li, "Indoor positioning systems based on visible light communication: State of the art," IEEE Commun. Sur. & Tutor., vol.19, no.4, pp.2871–2893, 2017.
[2] C.E. Shannon, "Communication theory of secrecy systems," Bell Labs Tech. J., vol.28, no.4, pp.656–715, Oct. 1949.
[3] A.D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol.54, no.8, pp.1355–1387, Oct. 1975.
[4] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," Proc. IEEE, vol.103, no.10, pp.1814–1825, Oct. 2015.
[5] M.A. Arfaoui, Z. Rezki, A. Ghrayeb, and M.-S. Alouini, "On the secrecy capacity of MISO visible light communication channels," Proc. IEEE GLOBECOM, Washington, DC, USA, 2016.
[6] J.-Y. Wang, C. Liu, J.-B. Wang, Y. Wu, M. Lin, and J. Cheng, "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," IEEE Trans. Commun., vol.66, no.12, pp.6423–6436, 2018.
[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, Sept. 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. Lightwave Technol., vol.34, no.21, pp.4988–4998, Nov. 2016.
[9] F. Wang, C. Liu, Q. Wang, J. Zhang, R. Zhang, L.-L. Yang, and L. Hanzo, "Optical jamming enhances the secrecy performance of the generalized space-shift-keying-aided visible-light downlink," IEEE Trans. Commun., vol.66, no.9, pp.4087–4102, Sept. 2018.
[10] T.V. Pham, T. Hayashi, and A.T. Pham, "Artificial-noise-aided precoding design for multi-user visible light communication channels," Proc. IEEE ICC Workshops, Kansas City, MO, USA, 2018.
[11] Z. Che, J. Fang, Z.L. Jiang, J. Li, S. Zhao, Y. Zhong, and Z. Chen, "A physical-layer secure coding scheme for indoor visible light communication based on Polar codes," IEEE Photon. J., vol.10, no.5, pp.1–13, Oct. 2018.
[12] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," IEEE Trans. Veh. Technol., vol.65, no.8, pp.6146–6158, Aug. 2016.
[13] M.T. Alresheedi, A.T. Hussein, and J.M.H. Elmirghani, Uplink design in VLC systems with IR sources and beam steering, IET Commun., vol.11, no.3, pp.311–317, 2017.