Physical-Layer Security of Visible Light Communications with Jamming

Dinghui Tian[1], Wensheng Zhang[1], Jian Sun[1], and Cheng-Xiang Wang[2,3]
[1]School of Information Science and Engineering, Shandong Provincial Key Lab of Wireless Communication Technologies, Shandong University, Qingdao, Shandong, 266237, China.
[2]National Mobile Communications Research Laboratory, School of Information Science and Engineering, Southeast University, Nanjing, 210096, China.
[3]Purple Mountain Laboratories, Nanjing, 211111, China.
Email: tiandinghui1994@126.com, zhangwsh@sdu.edu.cn, sunjian@sdu.edu.cn, chxwang@seu.edu.cn

***Abstract*—Visible light communication (VLC) is a burgeoning field in wireless communications as it considers illumination and communication simultaneously. The broadcast nature of VLC makes it necessary to consider the security of underlying transmissions. A physical-layer security (PLS) scheme by introducing jamming LEDs is considered in this paper. The secrecy rate of an indoor VLC system with multiple LEDs, one legitimate receiver, and multiple eavesdroppers is investigated. Three distributions of input signal are assumed, i.e., truncated generalized normal distribution (TGN), uniform distribution, and exponential distribution. The results show that jamming can improve the secrecy performance efficiently. This paper also demonstrates that when the numbers of LEDs transmitting information-bearing signal and jamming signal are equal, the average secrecy rate can be maximized.**

***Index Terms*—visible light communication, physical-layer security, secrecy rate, jamming.**

I. Introduction

In the past thirty years, wireless communications have made enormous progresses [1]. Optical wireless communication (OWC) becomes an indispensable part of wireless communication in order to reduce spectrum stress. VLC technology uses visible light as carriers to transfer information. The spectrum of visible light is approximately $4 \times 10^{14} \sim 7.9 \times 10^{14}$ Hz, so it has no interference to radio frequency (RF) systems. VLC technology is one of the potential key technologies of the sixth generation (6G) mobile communication systems. It has attracted more and more attentions of researchers [2]–[6].

Physical-layer security enhances the security performance of the communication systems by using interference and channel randomness to reduce the information received and correctly detected by unauthorized eavesdroppers. Many technologies have been utilized to improve the security performance of VLC systems. In [8], polar codes was introduced into indoor VLC system to achieve secrecy rate. In [9]–[11], chaotic sequences were applied to distinguish the legitimate users because only the legitimate users can detect the information according to the known chaotic pseudo-random code. A key generation mechanism was designed for VLC orthogonal frequency division multiplexing (OFDM) systems in [12], and improved system robustness. The authors designed a disk-shaped secrecy protected zone around the legitimate receiver to enhance the secrecy performance in [13]. In [14], the authors proposed a receiving scheme using the angular diversity technology to improve the accuracy of detection. Friendly jamming namely artificial noise has been proposed into wireless communications since 2008 [15], and it was been introduced into VLC systems to degrade eavesdropper channels [16].

C. Shannon has laid the foundation of information theory, and showed that the perfect secrecy requires keys having the same number of messages [17]. D. Wyner proposed the Wyner wiretap Gaussian channel model based on discrete memoryless channels and came out the concept of secrecy capacity [18]. Secrecy capacity is defined as the maximum transmit rate that the system can reach under the condition that eavesdroppers can not detect any information. Based on Wyner wiretap channel model, the authors in [19], [20] proposed the mathematical expression of secrecy capacity. They described the physical meaning of secrecy capacity the difference between the channel capacity of legitimate channel and wiretap channel. They also put up that secrecy capacity is the upper bound of secrecy rate. From then on, many researchers began to study the secrecy capacity and secrecy rate of different communication systems. The closed-form secrecy capacity expression of RF systems have been proposed, but it cannot be utilized in VLC systems directly, because some of the characteristics of VLC systems are different from those of RF systems. The input signal of RF systems is bipolar while the input signal of VLC systems is nonnegative. In RF systems, the variance of input signal is important to be considered, but in VLC systems, the mean is also necessary. Some forms of the bound on the secrecy capacity on VLC were derived [21]–[23]. In [21], the authors used three methods to derive the lower bound and upper bound of an indoor VLC system with typical wiretap channel. Ref. [22] used tight upper bound and lower bound to express the closed-form secrecy capacity. In [23], the achievable secrecy rate was given for different input distributions: TGN distribution and uniform distribution. A securing VLC links with friendly jammers was proposed in [**?**], [23], [24], and the closed-form secrecy rate expression for the systems was derived. To the best of our knowledge, no one investigated the ratio of information-bearing signal and jamming signal among these papers using artificial noise. This

paper aims to fill the above research gaps.

In this paper, the secrecy rate of an indoor VLC system using jamming is analyzed. The information sender equipped with multiple LEDs to transmit signal is set on the ceiling of the room, including information-bearing signal and jamming signal. A legitimate receiver and eavesdroppers are on the floor of the same room with their own photodetectors, and there is no collusion between eavesdroppers. The noise is assumed to be Gaussian and input-independent. Legitimate channel and eavesdropper channels have the same variance value. The information-bearing signal and jamming signal are assumed to follow the same distribution. The input signal is assumed to be TGN distributed, uniformly distributed, and exponential distributed, respectively. It is found that TGN distribution performs best among the three distributions, and exponential distribution performs worst when they have the same variance. Moreover, the average secrecy rate can achieve maximum value when half LEDs are used for jamming signal and other LEDs for information-bearing signal.

The rest of the paper is organized as follows: Section II describes the system model. The formula analysis is demonstrated in Section III. The simulation results are shown in Section IV, and Section V is the conclusion.

Notation: In this paper, $\mathbb{R}^M$ means the set of M-dimensional column vectors consisting of real numbers. $I[\cdot;\cdot]$ is the mutual information and $H(\cdot)$ is the entropy. Moreover, $var(\cdot)$ means the variance of a random variable, $\max[\cdot,\cdot]$ is a function that returns the bigger one between two numbers.

II. System Model

There are N LEDs (N is a constant) on the ceiling of an indoor environment with fixed positions, one legitimate user with known position information and channel response information, and multiple eavesdroppers with unknown positions. The system model is shown in Fig. 1.

Since the position of the legitimate user B (named Bob) is known to information sender A (named Alice), the channel gains between A and B: $h_{B_1}, h_{B_2}, ..., h_{B_N}$ can be perfectly known. But neither the position nor the number of eavesdroppers E (named Eve) are uncertain, the channel gains between A and E are unknown. The channel gain between A and the $k-th$ eavesdropper can be expressed as: $h_{E,k_1}, h_{E,k_2}, ..., h_{E,k_N}$. According to [2], [7], the ceiling, floor, and other objects can absorb a large part of light, reflect and diffuse a small part, so in this paper, only the line-of-sight (LoS) component is considered. The channel gain between transmitter and photodetector is given by [7]

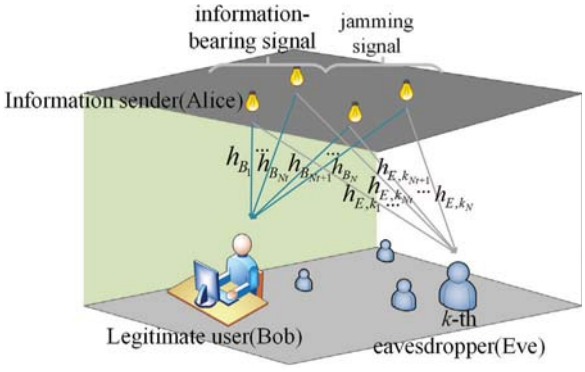

Fig. 1. System model.

$$h_i = \begin{cases} \dfrac{(n+1)A}{2\pi {d_i}^2} cos^n(\varphi_i) T_f(\psi_i) g(\psi_i) cos(\psi_i), & 0 \le \psi_i \le \psi_{FoV} \\ 0, & \psi_i > \psi_{FoV} \end{cases} \quad (1)$$

where $n = \frac{-ln2}{ln(\theta_{0.5})}$ is Lambertian order of LED, $\theta_{0.5}$ represents the half-angle at which half of the peak optical power is emitted, d_i is the distance between LED and photodetector, φ_i is the angle of incidence, ψ_i is the angle of irradiated light, ψ_{FoV} is the field of view (FoV) of photodetector, A is the area of photodetector, $T_f(\psi_i)$ is the gain of the filter at receiver side, $g(\psi_i)$ is the concentration gain.

Among N LEDs, N_t LEDs are used to transmit the information-bearing signal and the other $(N - N_t)$ LEDs are used to transmit jamming signal. It is assumed that $\mathbf{s} = [s_1, s_2, ..., s_{N_t}] \in \mathbb{R}^{N_t}$ is information-bearing signal and jamming signal is $\mathbf{w} = [w_1, w_2, ..., w_{N-N_t}] \in \mathbb{R}^{N-N_t}$, $\mathbf{h}_{B1} = [h_{B_1}, h_{B_2}, ..., h_{B_{N_t}}]^{\mathrm{T}} \in \mathbb{R}^{N_t}$ represents the vectors consisted the channel gains between Bob and the N_t LEDs transmitting information-bearing signal, $\mathbf{h}_{E,k,1} = [h_{E,k_1}, h_{E,k_2}, ..., h_{E,k_{N_t}}]^{\mathrm{T}} \in \mathbb{R}^{N_t}$ represents the vectors consisted the channel gains between the $k-th$ Eve and the N_t LEDs transmitting information-bearing signal, and $\mathbf{h}_{B2} = [h_{B_{N_t+1}}, h_{B_{N_t+2}}, ..., h_{B_N}]^{\mathrm{T}} \in \mathbb{R}^{N-N_t}$, $\mathbf{h}_{E,k,2} = [h_{E,k_{N_t+1}}, h_{E,k_{N_t+2}}, ..., h_{E,k_N}]^{\mathrm{T}} \in \mathbb{R}^{N-N_t}$ represent the vectors consisting of the channel gains of jammers–B links and jammers–$k-th$ Eve links, respectively. Since The jamming signal is generated from the nullspace of the channel response information between Alice and Bob, $\mathbf{w}$ is orthogonal to $\mathbf{h}_{B2}$, i.e.,

$$\mathbf{h}_{B2}^{\mathrm{T}} \mathbf{w} = 0. \quad (2)$$

The received signals can be given by

$$\begin{aligned} y_B &= \mathbf{h}_{B1}^{\mathrm{T}} \mathbf{s} + n_B \\ y_{E,k} &= \mathbf{h}_{E,k,1}^{\mathrm{T}} \mathbf{s} + \mathbf{h}_{E,k,2}^{\mathrm{T}} \mathbf{w} + n_{E,k} \end{aligned} \quad (3)$$

where $n_B \sim N(0, \sigma_B^2)$ and $n_{E,k} \sim N(0, \sigma_{E,k}^2)$ represent the input-independent Gaussian noise, and σ_B^2 and $\sigma_{E,k}^2$ are the variances of the noise of legitimate channel and $k-th$ eavesdropper channel, respectively.

In this system, Bob can detect and discard the jamming signal, and only receive and process the information-bearing signal. Eve receives all signals sent by N LEDs and cannot detect the jamming signal. Theoretically, the system can enhance secrecy performance of the system by decreasing signal to noise ratio (SNR) of Eve. Jamming signal disturbs

and confuses eavesdroppers. SNR of legitimate channel and eavesdropper channel can be expressed as

$$\begin{aligned} SNR_B &= \frac{\mathbf{h}_{B1}^{\mathrm{T}}\mathbf{s}\mathbf{s}^{\mathrm{T}}\mathbf{h}_{B1}}{\sigma_B^2} \\ SNR_{E,k} &= \frac{\mathbf{h}_{E,k,1}^{\mathrm{T}}\mathbf{s}\mathbf{s}^{\mathrm{T}}\mathbf{h}_{E,k,1}}{\mathbf{h}_{E,k,2}^{\mathrm{T}}\mathbf{w}\mathbf{w}^{\mathrm{T}}\mathbf{h}_{E,k,2}+\sigma_{E,k}^2}. \end{aligned} \tag{4}$$

III. Secrecy Rate Analysis

A. Secrecy Rate of the System

The expression of secrecy capacity for wireless communication given by [19], [20] is

$$C_S^+ = \max[\max_{f_X(x)} \{I[x;y_B] - I[x;y_E]\}, 0] = \max[C_S, 0]. \tag{5}$$

Here $f_X(x)$ is the probability density function (PDF) of input signal. Because secrecy capacity is a nonnegative value, secrecy capacity equals zero when C_S is negative. For our model, the input is determined, so C_S can be rewritten as

$$\begin{aligned} C_S &= \max \min_k \{I[\mathbf{s};y_B] - I[\mathbf{s};y_{E,k}]\} \\ &\geq \min_k \{I[\mathbf{s};y_B] - I[\mathbf{s};y_{E,k}]\} \\ &\geq \min_k \{H(y_B) - H(y_B|\mathbf{s}) - H(y_{E,k}) + H(y_{E,k}|\mathbf{s})\}. \end{aligned} \tag{6}$$

Moreover, $H(y_B|\mathbf{s})$ can be expressed as

$$H(y_B|\mathbf{s}) = H(n_B) = \frac{1}{2}\ln(2\pi e\sigma_B^2). \tag{7}$$

In the following derivation, the entropy power inequality is used. The entropy power of a random variable X is defined as $N(X) = \frac{1}{2\pi e}e^{2H(X)}$. Let X and Y be independent random variables, then we can get $e^{2H(X+Y)} \geq e^{2H(X)} + e^{2H(Y)}$. Associating with entropy power inequality and (3), $H(y_B)$ can be written as

$$\begin{aligned} H(y_B) &= H(\mathbf{h}_{B1}^{\mathrm{T}}\mathbf{s} + n_B) \\ &\geq \frac{1}{2}\ln\left(e^{2H(\mathbf{h}_{B1}^{\mathrm{T}}\mathbf{s})} + e^{2H(n_B)}\right) \\ &= \frac{1}{2}\ln\left(e^{2H\left(\sum_{i=1}^{N_t} h_{B_i}s_i\right)} + e^{2H(n_B)}\right) \\ &\geq \frac{1}{2}\ln\left(\sum_{i=1}^{N_t} e^{2H(h_{B_i}s_i)} + 2\pi e\sigma_B^2\right) \\ &= \frac{1}{2}\ln\left(\sum_{i=1}^{N_t} e^{2H(s_i)+2\ln(h_{B_i})} + 2\pi e\sigma_B^2\right) \\ &= \frac{1}{2}\ln\left(\mathbf{h}_{B1}^{\mathrm{T}}\mathbf{h}_{B1}e^{2H(s_i)} + 2\pi e\sigma_B^2\right). \end{aligned} \tag{8}$$

Similarly, $H(y_{E,k}|\mathbf{s})$ can be written as

$$\begin{aligned} H(y_{E,k}|\mathbf{s}) &= H(\mathbf{h}_{E,k,2}^{\mathrm{T}}\mathbf{w} + n_{Ek}) \\ &= \frac{1}{2}\ln\left(\mathbf{h}_{E,k,2}^{\mathrm{T}}\mathbf{h}_{E,k,2}e^{2H(w_i)} + 2\pi e\sigma_{Ek}^2\right). \end{aligned} \tag{9}$$

$H(y_{E,k})$ can be calculated as follows

$$H(y_{E,k}) = \frac{1}{2}\ln[2\pi e var(y_{E,k})]. \tag{10}$$

Here, $var(y_{E,k})$ can be calculated as

$$\begin{aligned} var(y_{E,k}) &= var(\mathbf{h}_{E,k,1}^{\mathrm{T}}\mathbf{s} + \mathbf{h}_{E,k,2}^{\mathrm{T}}\mathbf{w} + n_{E,k}) \\ &= var\left(\sum_{i=1}^{N_t} h_{E,k,1_i}s_i\right) + var\left(\sum_{i=1}^{N-N_t} h_{E,k,2_i}w_i\right) + var(n_{E,k}) \\ &= \sum_{i=1}^{N_t} h_{E,k,1_i}^2 var(s_i) + \sum_{i=1}^{N-N_t} h_{E,k,2_i}^2 var(w_i) + \sigma_{E,k}^2 \\ &= \mathbf{h}_{Ek}^{\mathrm{T}}\mathbf{h}_{Ek}var(s_i) + \sigma_{E,k}^2. \end{aligned} \tag{11}$$

It should be mentioned that $var(s_i) = var(w_i)$ is used.

Substituting (7)–(11) to (6), the lower bound of secrecy capacity can be shown as

$$C_S \geq \frac{1}{2}\ln\frac{(\mathbf{h}_{B1}^{\mathrm{T}}\mathbf{h}_{B1}e^{2H(s_i)} + 2\pi e\sigma_B^2)(\mathbf{h}_{E,k,2}^{\mathrm{T}}\mathbf{h}_{E,k,2}e^{2H(w_i)} + 2\pi e\sigma_{Ek}^2)}{(2\pi e)^2\sigma_B^2[\mathbf{h}_{Ek}^{\mathrm{T}}\mathbf{h}_{Ek}var(s_i) + \sigma_{E,k}^2]}. \tag{12}$$

Secrecy capacity is the maximum secrecy rate that can be achieved, so this lower bound of secrecy capacity can be used to express the secrecy rate. There are two extreme cases: one is that no LEDs transmit jamming signal, i.e., $N_t = N$. In this case, the secrecy rate denotes $R_{S(N)}$ can be written as

$$R_{S(N_t=N)} = \frac{1}{2}\ln\frac{2\pi e\sigma_{E,k}^2(\mathbf{h}_B^{\mathrm{T}}\mathbf{h}_B e^{2H(s_i)} + 2\pi e\sigma_B^2)}{(2\pi e)^2\sigma_B^2(\mathbf{h}_{Ek}^{\mathrm{T}}\mathbf{h}_{Ek}var(s_i) + \sigma_{E,k}^2)}. \tag{13}$$

Another case is that all LEDs transmit jamming signal, i.e., $N_t = 0$. Then the secrecy rate denotes $R_{S(0)}$ is

$$R_{S(N_t=0)} = \frac{1}{2}\ln\frac{2\pi e\sigma_B^2(\mathbf{h}_E^{\mathrm{T}}\mathbf{h}_E e^{2H(w_i)} + 2\pi e\sigma_{Ek}^2)}{(2\pi e)^2\sigma_B^2(\mathbf{h}_{Ek}^{\mathrm{T}}\mathbf{h}_{Ek}var(s_i) + \sigma_{E,k}^2)}. \tag{14}$$

What can be seen from (14) is that when the input signal follows Gaussian distribution, the power entropy can achieve the maximum value, i.e. $H(w_i) = \frac{1}{2}\ln[2\pi e var(w_i)]$. At this time, $R_{S(N_t=0)}$ has the maximum value zero. For other distributions, $R_{S(N_t=0)}$ are lesser than zero certainly. So the secrecy rate is equal to zero for $N_t = 0$, which means when all LEDs are used for jamming signal, neither the legitimate user nor the eavesdroppers can get any information in this system.

B. Truncated Generalized Normal Distribution

In the systems of [**?**], [**?**], [23], TGN distribution were considered. TGN distribution is physically realizable, and it is flexible to determine the interval of the random variable [**?**]. Suppose that random variable $X \sim N_A(0, \sigma^2)$ is truncated normal distributed and lies in the interval (a, b). Then the PDF of X can be given by

$$f_X(x) = \frac{\phi(\frac{x}{\sigma})}{\sigma\left(\Phi(\frac{b}{\sigma}) - \Phi(\frac{a}{\sigma})\right)} \tag{15}$$

where $\phi(\cdot)$ and $\Phi(\cdot)$ are PDF and cumulative distribution function (CDF) of standard Gaussian distribution, respectively. The entropy of TGN can be expressed as

$$H(x) = \frac{1}{2}\ln(2\pi e\sigma^2 Z^2) + \gamma. \tag{16}$$

Here some symbols are used for convenience, $\alpha = a/\sigma$, $\beta = b/\sigma$, $Z = \Phi(\beta) - \Phi(\alpha)$, and $\gamma = \frac{\alpha\phi(\alpha)-\beta\phi(\beta)}{2Z}$.

The secrecy rate for TGN distribution can be expressed as

$$\begin{aligned} R_S^{TGN} = & \frac{1}{2}\ln(\mathbf{h}_{B1}^{\mathrm{T}}\mathbf{h}_{B1}\sigma^2 Z^2 e^{2\gamma} + \sigma_B^2) \\ & + \frac{1}{2}\ln(\mathbf{h}_{E,k,2}^{\mathrm{T}}\mathbf{h}_{E,k,2}\sigma^2 Z^2 e^{2\gamma} + \sigma_{Ek}^2) \\ & - \frac{1}{2}\ln\left[\mathbf{h}_{E,k}^{\mathrm{T}}\mathbf{h}_{E,k}\sigma^2\left(1 + 2\gamma - \left(\frac{\phi(\alpha)-\phi(\beta)}{Z}\right)^2\right) + \sigma_{Ek}^2\right] \\ & - \frac{1}{2}\ln(\sigma_B^2). \end{aligned} \tag{17}$$

C. Uniform Distribution

Uniform distribution is simple and generally used in some communication systems. Uniform distribution was utilized in [16]. In [16], the authors derived a formula of achievable secrecy rate as a function of Bob's position.

For our model, the secrecy rate for uniform distribution lying in the interval $[-a, a]$ can be given by

$$\begin{aligned} R_S^U = & \frac{1}{2}\ln(4a^2\mathbf{h}_{B1}^{\mathrm{T}}\mathbf{h}_{B1} + 2\pi e\sigma_B^2) + \frac{1}{2}\ln(4a^2\mathbf{h}_{E,k,2}^{\mathrm{T}}\mathbf{h}_{E,k,2} + 2\pi e\sigma_{Ek}^2) \\ & - \frac{1}{2}\ln(2\pi e\mathbf{h}_{E,k}^{\mathrm{T}}\mathbf{h}_{E,k}\frac{a^2}{3} + 2\pi e\sigma_{Ek}^2) - \frac{1}{2}\ln(2\pi e\sigma_B^2). \end{aligned} \tag{18}$$

D. Exponential Distribution

Exponential distribution was proved to be optimal to maximize the lower bound on the secrecy capacity of dimmable VLC system with average optical intensity constraint [21]. If we apply exponential distribution with parameter λ, the secrecy rate can be expressed as

$$\begin{aligned} R_S^{\exp} = & \frac{1}{2}\ln(\mathbf{h}_{B1}^{\mathrm{T}}\mathbf{h}_{B1}e^2\frac{1}{\lambda^2} + 2\pi e\sigma_B^2) + \frac{1}{2}\ln(\mathbf{h}_{E,k,2}^{\mathrm{T}}\mathbf{h}_{E,k,2}e^2\frac{1}{\lambda^2} + 2\pi e\sigma_{Ek}^2) \\ & - \frac{1}{2}\ln(\mathbf{h}_{E,k}^{\mathrm{T}}\mathbf{h}_{E,k}\frac{2\pi e}{\lambda^2} + 2\pi e\sigma_{Ek}^2) - \frac{1}{2}\ln(2\pi e\sigma_B^2). \end{aligned} \tag{19}$$

IV. Simulation Results

The simulation parameters are set as follows: the variance of both legitimate channels' noise and eavesdroppers channels' noise are 10^{-13}. For the sake of fairness, we use the same variance for all three distributions. For TGN distribution, $\sigma^2 = 0.1225$, $a = -0.1$, $b = 0.1$. For uniform distribution, $a = 0.1$. For exponential distribution, $\lambda = 0.055$.

Fig. 2 shows the relationship between secrecy rate of the form part and the proportion of information-bearing signal. The details of the part circled by rectangle in Fig. 2 can be seen in Fig. 3. It is worth mentioning that during simulation we calculate secrecy rate as $R_S^+ = \max[R_S, 0]$ because secrecy rate should not be negative like secrecy capacity. According to Fig. 2, the system can perform well except there is no jamming or all jamming transmitted. This indicates that using jamming can improve the secrecy performance of VLC systems. When the system has the same proportion of information-bearing signal, the system can have the highest secrecy rate if both information-bearing signal and jamming signal follow TGN

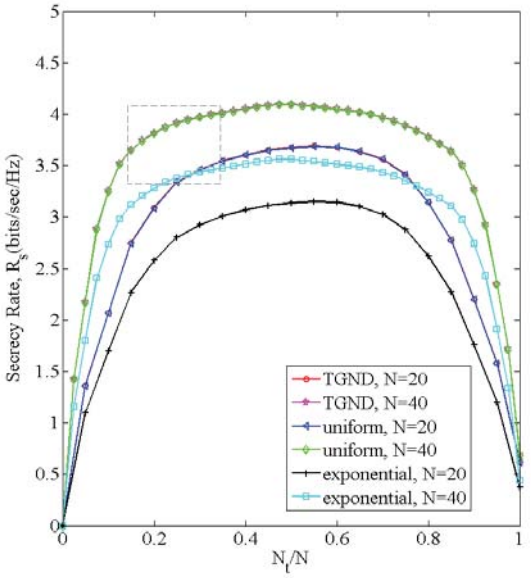

Fig. 2. Secrecy rates for different distributions.

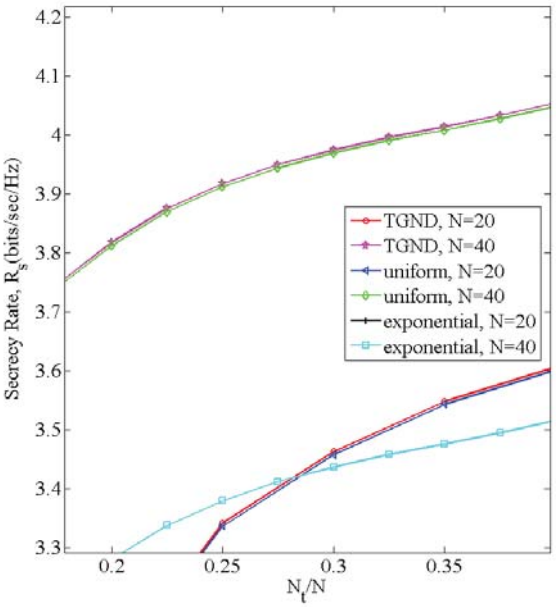

Fig. 3. Detail of the part circled by rectangle in Fig. 2.

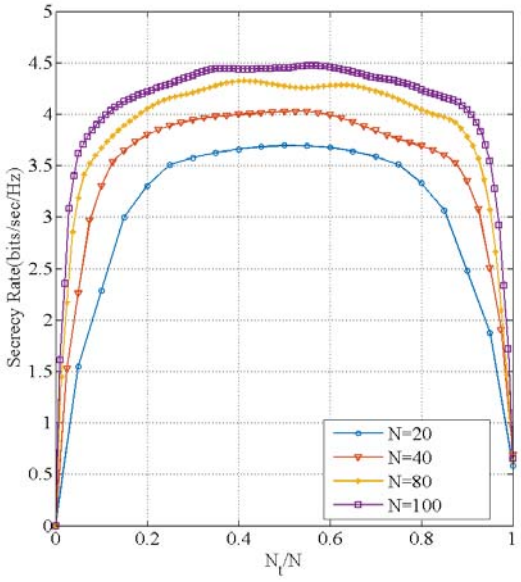

Fig. 4. Secrecy rates with different total numbers of LEDs (TGN distribution).

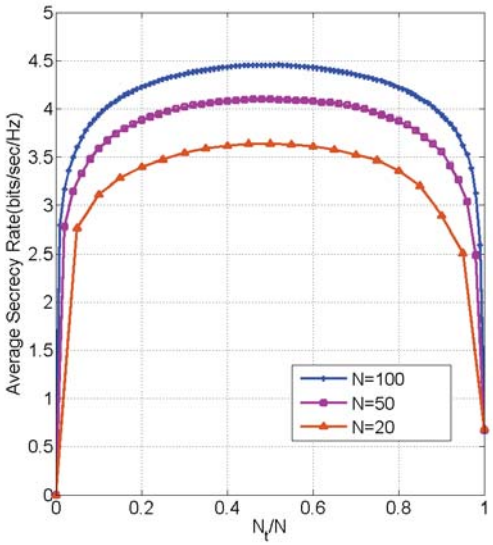

Fig. 5. Average secrecy rate (TGN distribution).

distribution. Uniform distribution takes second place, and exponential distribution performs worst. Fig. 3 shows that TGN distribution performs better than uniform distribution. Fig. 4 shows the relationship between the total number of LEDs and secrecy rate taking TGN distribution as an example. It can be seen clearly that the more LEDs, the better secrecy performance. More LEDs means stronger intensity of light.

We change Bob's and Eve's locations by Monte-Carlo simulations. It is found that the optimal proportion of information-bearing signal is not a fixed value. However, we take average of all simulation results, and then plot the diagram of the average secrecy rate and proportion of information-bearing signal as shown in Fig. 5. It is found that when half of the LEDs transmit information-bearing signal, namely $N_t = \frac{1}{2}N$, the system can reach the highest average secrecy rate.

V. Conclusions

In this paper, an indoor VLC system with the help of jamming has been investigated. In this system, the legitimate user and eavesdroppers are exposed in Gaussian noise channel with the same variance. Three distributions for both information-bearing signal and jamming signal have been considered, and expressions of the secrecy rate for each distribution have been derived. Through simulations, it is demonstrated that TGN distribution is the best choice among three distributions. To the best of our knowledge, this is the first time to consider the effect of ratio between information senders and jammers to VLC systems with jamming. It contributes to the designing, security performance optimization, and system deployment of VLC systems. We will research on tradeoff between security performance and data transmission efficiency in the future.

Acknowledgment

This work was supported by Shandong Provincial Natural Science Foundation (ZR2017MF012), Key Research and Development Program of Shandong Province (2016GGX101014), Fundamental Research Funds of Shandong University (2017JC029), Taishan Scholar Program of Shandong Province, Science and Technology Project of Guangzhou (201704030105), EU H2020 RISE TESTBED Project (734325), Natural Science Foundation of China (No. 61771293), and Fundamental Research Funds for the Central Universities (2242019R30001).

References

[1] C.-X. Wang, J. Bian, J. Sun, W. Zhang, and M. Zhang, "A survey of 5G channel measurements and models," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3142–3168, 4th Quart., 2018.

[2] D. Karunatilaka, F. Zafar, V. Kalavally, and R. Parthiban, "LED based indoor visible light communications: State of the art," *IEEE Commun. Surveys Tutotials*, vol. 17, no. 3, pp. 1649–1678, third quarter 2015.

[3] A. Al-Kinani, J. Sun, C.-X. Wang, W. Zhang, X. Ge, and H. Haas, "A 2D non-stationary GBSM for vehicular visible light communication channels," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 7981–7992, Dec. 2018.

[4] A. Al-Kinani, C.-X. Wang, L. Zhou, and W. Zhang, "Optical wireless communication channel measurements and models," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1939–1962, 3rd Quart., 2018.

[5] L. Zhou, C.-X. Wang, A. Al-Kinani, and W. Zhang, "Visible light communication system evaluations with integrated hardware and optical parameters," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 4059–4073, Sept. 2018.

[6] J. Wang, A. Al-Kinani, W. Zhang, C.-X. Wang, and L. Zhou, "A general channel model for visible light communications in underground mines," *China Commun.*, vol. 15, no. 9, pp. 95–105, Sept. 2018.

[7] P. H. Pathak, X. T. Feng, P. F. Hu, and P. Mohapatra, "Visible light communication, networking, and sensing: A survey, potential and challenges," *IEEE Commun. Surveys Tutotials*, vol. 17, no. 4, pp. 2047–2077, forth quarter 2015.

[8] Z. Che, J. Fang, Z. L. Jiang, X. Yu, G. Xi, and Z. Chen, "A physical-layer secure coding schcme for visible light communication based on polar codes," in *Proc. CLEO-PR'17*, Singapore, Aug. 2017, pp. 1–2.

[9] D. Li, L. Zhang, and J. Qiu, "High security chaotic multiple access scheme for VLC systems," in *Proc. ITNAC'16*, Dunedin, Dec. 2016, pp. 133–135.
[10] H. Lu, L. Zhang, and X. Liu, "High-security colour shift keying modulation scheme with chaos-based constellation rotation for VLC system," in *Proc. ASID'16*, Xiamen, Sept. 2016, pp. 20–24.
[11] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Physical-layer security against known/chosen plaintext attacks for OFDM-based VLC system," *IEEE Commun. Lett.*, vol. 21, no. 12, pp. 2606–2609, Dec. 2017.
[12] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Robust key generation from optical OFDM signal in indoor VLC networks," *IEEE Photon. Techn. Lett.*, vol. 28, no. 22, pp. 2629–2632, Nov. 2016.
[13] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 1, pp. 162–174, 2018.
[14] P. Fahamuel, J. Thompson, and H. Haas, "Improved indoor VLC MIMO channel capacity using mobile receiver with angular diversity detectors," in *Proc. IEEE GlobeCom'14*, Austin, TX, Dec. 2014, pp. 2060–2065.
[15] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2190, Jun. 2008.
[16] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," in *Proc. GC Wkshps'14*, Austin, TX, Dec. 2014, pp. 524–529.
[17] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[18] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[19] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, Jul. 1978.
[20] I. Csiszui and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May. 1978.
[21] C. Liu, J. Wang, J. Wang, J. Zhu, and M. Chen, "Three lower bounds on secrecy capacity for indoor visible light communications," in *Proc. WCSP'17*, Nanjing, China, Oct. 2017, pp. 1–5.
[22] J. Wang, S. Lin, C. Liu, J. Wang, B. Zhu, and Y. Jiang, "Secrecy capacity of indoor visible light communication channels," in *Proc. ICC Workshops'18*, Kansas City, MO, May 2018, pp. 1–6.
[23] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the secrecy capacity of MISO visible light communication channels," in *Proc. GLOBECOM'16*, Washington, DC, Dec. 2016, pp. 1–7.
[24] S. Ma, Z. Dong, H. Li, Z. Lu, and S. Li, "Optimal and robust secure beamformer for indoor MISO visible light communication," *J. of Lightw. Technol.*, vol. 34, no. 21, pp. 4988–4998, Nov. 2016.