

# Secrecy Analysis in Visible Light Communication Systems with Randomly Located Eavesdroppers

Sunghwan Cho, Gaojie Chen, and Justin P. Coon  
Department of Engineering Science,

University of Oxford, OX1 3PJ, United Kingdom.

Email: {sunghwan.cho, gaojie.chen and justin.coon}@eng.ox.ac.uk

**Abstract**—We investigate the secrecy connectivity in visible light communication in the presence of randomly located eavesdroppers. We apply spatial point processes to characterize the unknown eavesdropper locations. The closed-form of the secrecy outage probability is derived as a function of the density of eavesdroppers. The analysis is verified by Monte Carlo simulations. Furthermore, we suggest an LED transmitter selection scheme based on the location of a legitimate user. It is verified that the proposed transmission scheme can significantly improve the secrecy performance as a function of the number of LED transmitters.

**Index Terms**—Physical layer security, visible light communication, stochastic geometry, secrecy connectivity

## I. INTRODUCTION

VISIBLE Light Communication (VLC) is the emerging technology that fulfills wireless communications and provides illumination simultaneously by using light emitting diodes (LEDs). Due to the shortage of the radio frequency spectra and the high efficiency of VLC in the aspects of power consumption and spatial frequency reuse, VLC has been considered as the potential technology to support next generation (5G) mobile networks, Internet of Things (IoT), and Device-to-Device (D2D) communications within buildings [1], [2].

Since visible light, as a communication medium in VLC, cannot penetrate walls and obstacles, VLC can retain higher physical layer security compared to the RF communications [3]. However, VLC is still susceptible to eavesdroppers especially in public places such as libraries, offices, and malls. Recently, Lampe et al have rigorously studied physical layer security in VLC. In [4], [5], they investigated the achievable secrecy rate with several transmission schemes such as robust beamforming and friendly jamming. In [6], Alouini applied the truncated Gaussian input distribution to VLC to enhance the secrecy rate because VLC imposes a peak amplitude constraint on the input distribution. However, these works had been done based on the assumption that the locations of eavesdroppers are known to a transmitter or spatially confined to a certain area, but this may not be a practical assumption in some cases.

To investigate the system-level performance of wireless networks where the nodes are randomly located by a certain distribution, stochastic geometry has been considered widely [7]. Therefore, many researchers have studied the impact of random eavesdroppers' locations on secrecy performance by using the binomial point process (BPP) [8]

and the Poisson point process (PPP) in RF communication system [9]–[11]. Then, the secrecy outage probability (SOP) and the average secrecy capacity (ASC) for VLC with the randomly distributed EDs have been analyzed in [12]. To further enhance the secrecy performance, in this paper, we investigate the secrecy outage probability of the downlink<sup>1</sup> for VLC by using the LED selection scheme when eavesdroppers are randomly distributed and their locations are not known to the transmitters. The contributions of this paper as follows:

- We analyze the SOP when the locations of eavesdroppers are randomly distributed. We apply a PPP model to deal with the randomness of eavesdroppers.
- We consider a few configurations differentiating the distributions and numbers of transmitters and receivers and derive a closed-form for the SOP for each case.
- We propose a simple transmitter selection scheme based on the legitimate user's location to improve the SOP.

The rest of this paper is organized as follows. Section II begins with the system model describing the modulation scheme and channel model in VLC. Section III provides the analysis regarding the SOP, and we propose a transmitter selection scheme. Section IV documents a comparison of theoretical and simulation results. Section V concludes the paper.

## II. SYSTEM MODEL

We consider the DC-biased pulse-amplitude modulation (PAM) VLC scheme as in [5]. The data signal  $s(t) \in \mathbb{R}$  is superimposed on a fixed bias current  $I_{DC} \in \mathbb{R}^+$ , where  $\mathbb{R}$  and  $\mathbb{R}^+$  denote the set of real-valued numbers and non-negative real-valued numbers, respectively. This fixed current is used for its original purpose of light. The modulated signal  $x(t; \alpha)$  of  $s(t)$  can be expressed by  $x(t; \alpha) = \alpha I_{DC} s(t)$ , where  $\alpha \in [0, 1]$  is the modulation index. To maintain linear current-to-light conversion and avoid clipping distortion, the LED transmitter has a constraint on its input power. Since the dynamic range of the LED is  $I_{DC} \pm \alpha I_{DC}$ ,  $x(t; \alpha)$  is subject to the amplitude constraint  $|x(t; \alpha)| \leq \alpha I_{DC}$ . Therefore, the power of the emitted signal from LED can be described as  $P_{TX} = \eta(I_{DC} + x(t; \alpha))$ , where  $\eta$  (W/A) is the current-to-light conversion efficiency. Then, the received power is

<sup>1</sup>In VLC, the uplink is commonly considered as more secure because the receiver directionally transmits its signal to the transmitter normally attached to the ceiling.

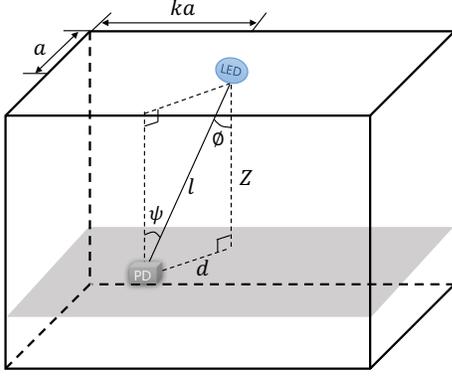


Fig. 1: The visible light communication configuration.

$P_{RX} = GP_{TX}$ , where  $G < 1$  is the path gain. Therefore, the received signal voltage  $y(t)$  after removing the DC bias is given by

$$y(t) = hx(t; \alpha) + w(t) \quad (1)$$

where  $h = \eta GBT$  is the channel gain,  $B$  is the responsivity of a photodiode (PD) ( $A/W$ ),  $T$  is the transimpedance amplifier gain ( $V/A$ ) and  $w(t) \sim \mathcal{N}(0, \sigma^2)$  is a zero-mean additive white Gaussian noise (AWGN) term.

According to [13], the path gain  $G$  corresponding to an LED with a generalized Lambertian emission pattern is given by

$$G = \begin{cases} \frac{1}{2\pi}(m+1)\cos^m(\phi)\frac{A_{RX}}{l^2}\cos(\psi) & \text{for } |\psi| \leq \psi_{FoV} \\ 0 & \text{for } |\psi| > \psi_{FoV} \end{cases} \quad (2)$$

where  $m = -(\ln 2)/(\ln \cos \phi_{1/2})$  is the order of Lambertian emission with the semi-angle  $\phi_{1/2}$  for half illuminance of the LED. As shown in Fig. 1,  $\phi$  is the angle of irradiance,  $\psi$  is the angle of incidence, and  $l$  is the LoS distance between the LED and the photodiode. Also,  $Z$  denotes the vertical distance from the work plane to the ceiling and  $d$  denotes the distance between the transmitter and receiver projected onto the work plane. Throughout this paper, we assume all of the receivers are located on the same work plane. Also,  $A_{RX} = (n^2/\sin^2(\psi_{FoV}))A_{PD}$  is the receiver collection area, where  $n$  is the refractive index of the optical concentrator,  $A_{PD}$  is the PD area and  $\psi_{FoV}$  is the receiver field-of-view (FoV) semi-angle. Note that this channel model considers only LoS propagation and ignores reflections from walls and floors [13].

### III. SECRECY OUTAGE PROBABILITY

In this section, we analyze the SOP when multiple eavesdroppers are randomly distributed. First, we consider a single UE with multiple eavesdroppers distributed according to a PPP. We assume that eavesdroppers act independently of one another (i.e., there is no collusion). We then study the case where transmitter (i.e., LED) selection is employed to enhance secrecy in a Poisson field of eavesdroppers.

#### A. One UE and multiple random PPP eavesdroppers

In the first section, we consider the configuration where one LED transmitter BS transmits the information-bearing

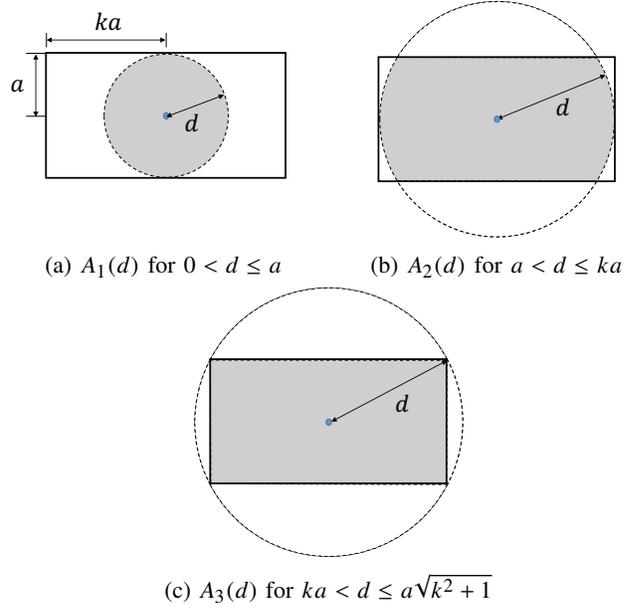


Fig. 2:  $A_i(d)$  for  $i \in \{1, 2, 3\}$

signal to one legitimate receiver UE, and multiple passive eavesdroppers  $E_s$  wiretap the signal. In this paper, we treat each light source as a single LED, however, an LED light may be made up of a series of individual LEDs, called an LED fixture, in practice. The multiple eavesdroppers are distributed according to a PPP  $\Phi_E$  with the density  $\lambda_E$ . As shown Fig. 1, the LED transmitter is attached to the center of a cuboid room's ceiling, where  $a$  denotes the half length of the work plane's width and  $k$  denotes the ratio of length to width of the plane. Also, both the intended receiver and eavesdroppers are assumed to be located on the same work plane [4], [5].

The received signals at the UE and  $E_e$  for  $e \in \Phi_E$  are given by

$$y_{BU}(t) = \alpha I_{DC} h_{BU} s(t) + n_U(t), \quad (3a)$$

$$y_{BE_e}(t) = \alpha I_{DC} h_{BE_e} s(t) + n_{E_e}(t) \quad (3b)$$

where  $h_{BU}$  and  $h_{BE_e}$  are the channel gains from transmitter to UE and  $E_e$ , respectively, and  $n_U$  and  $n_{E_e}$  are the zero-mean AWGN at the UE and  $E_e$  with variance  $\sigma^2$ , respectively. From (2), by assuming a receiver's PD faces up perpendicular to a work plane, the channel gain can be simplified as

$$\begin{aligned} h &= \frac{\eta}{2\pi}(m+1)\cos^m(\phi)\frac{A_{RX}}{l^2}\cos(\psi)BT \\ &= \frac{\eta}{2\pi}(m+1)\left(\frac{Z}{l}\right)^m\frac{A_{RX}}{l^2}\left(\frac{Z}{l}\right)BT \\ &= Kl^{-(m+3)} \end{aligned} \quad (4)$$

where  $K = (\eta(m+1)Z^{m+1}A_{RX}BT)/2\pi$ . The trigonometric functions in (4) can be simplified with  $Z$  and  $l$ . Note that the channel gain depends only on the distance between the transmitter and receivers when other parameters are fixed. Therefore, the signal-to-noise ratio (SNR) at UE and  $E_e$  can

be described as

$$\gamma_{BU} = \frac{\alpha^2 I_{DC}^2 |h_{BU}|^2}{\sigma^2}, \quad (5a)$$

$$\gamma_{BE_e} = \frac{\alpha^2 I_{DC}^2 |h_{BE_e}|^2}{\sigma^2} \quad (5b)$$

respectively.

1) *Fixed UE*: First, we investigate the SOP when the UE's location is fixed. Given the UE's location, the distance in the work plane between BS and UE,  $d_{BU}$ , is also fixed. Therefore, the SOP for a fixed UE and multiple random eavesdroppers is given by

$$P_{SO} = \mathbb{P}(\gamma_{BU} < \max_{e \in \Phi_E} \gamma_{BE_e}) \stackrel{(a)}{=} \mathbb{P}(\min_{e \in \Phi_E} d_{BE_e} < d_{BU})$$

$$\stackrel{(b)}{=} \begin{cases} 1 - e^{-\lambda_E A_1(d_{BU})} & \text{for } 0 < d_{BU} \leq a \\ 1 - e^{-\lambda_E A_2(d_{BU})} & \text{for } a < d_{BU} \leq ka \\ 1 - e^{-\lambda_E A_3(d_{BU})} & \text{for } ka < d_{BU} \leq a\sqrt{k^2 + 1} \end{cases} \quad (6)$$

where (a) holds due to the assumption that the receivers are located on the same work plane and (b) holds due to the distribution of the contact distance to the nearest point of the PPP [14]. Note that the probability distribution of the contact distance is identical to the probability distribution that there is no eavesdropper in the given area  $A_i(d)$  for  $i \in \{1, 2, 3\}$ , which is the area of a circle bounded by the rectangle for the different regions of  $d$  as shown in Fig. 2, i.e., the shaded area. These areas are given by,

$$A_1(d) = \pi d^2, \quad (7a)$$

$$A_2(d) = \pi d^2 - 2 \left( d^2 \arccos\left(\frac{a}{d}\right) - a\sqrt{d^2 - a^2} \right), \quad (7b)$$

$$A_3(d) = \pi d^2 - 2 \left( d^2 \arccos\left(\frac{a}{d}\right) - a\sqrt{d^2 - a^2} \right) - 2 \left( d^2 \arccos\left(\frac{ak}{d}\right) - ak\sqrt{d^2 - (ak)^2} \right). \quad (7c)$$

Note that the secrecy outage occurs only when the E's location is closer to BS than UE.

2) *Random BPP UE*: From the previous result, we can also calculate the SOP when we do not condition on the intended user's location, i.e., the location of the legitimate user is random, distributed according to a BPP with a single point. The cumulative distribution function (CDF) of  $d_{BU}$  is

$$F_{d_{BU}}(d) = \begin{cases} \frac{A_1(d)}{4ka^2} & \text{for } 0 < d \leq a \\ \frac{A_2(d)}{4ka^2} & \text{for } a < d \leq ka \\ \frac{A_3(d)}{4ka^2} & \text{for } ka < d \leq a\sqrt{k^2 + 1}. \end{cases} \quad (8)$$

Therefore, the probability density function (PDF) of  $d_{BU}$  can be easily calculated by differentiating (8) to give (9) at the top of the next page.

Also, the CDF of the minimum distance of multiple eavesdroppers, i.e.,  $d_{BE}^* = \min_{e \in \Phi_E} d_{BE_e}$ , is given by

$$F_{d_{BE}^*}(d) = \begin{cases} 1 - e^{-\lambda_E A_1(d)} & \text{for } 0 < d \leq a \\ 1 - e^{-\lambda_E A_2(d)} & \text{for } a < d \leq ka \\ 1 - e^{-\lambda_E A_3(d)} & \text{for } ka < d \leq a\sqrt{k^2 + 1} \end{cases} \quad (10)$$

similarly to (6). Then, the SOP can be calculated by using the PDF and CDF as shown in the first line of (13) at the next page. However, to the best of our knowledge, it is impossible to calculate the closed-form of the SOP due to the  $\arccos(\cdot)$  power term of the exponential function. To release this restriction, we apply a piecewise approximation to express  $A_i(d)$  for  $i \in \{2, 3\}$  in the polynomial form, which are given by

$$\hat{A}_2(d) = K_1 d^3 + K_2 d^2, \quad (11a)$$

$$\hat{A}_3(d) = K_3 d^3 + K_4 d^2 \quad (11b)$$

where  $\hat{A}_i(d)$  for  $i \in \{2, 3\}$  denotes the approximated area of  $A_i(d)$ . The approximation constants  $K_i$  for  $i \in \{1, 2, 3, 4\}$  are given by

$$K_1 = \frac{(2\sqrt{k^2 - 1}/k^2 - 2 \arccos(\frac{1}{k}))}{a(k - 1)},$$

$$K_2 = \pi - aK_1,$$

$$K_3 = 2 \left( \arccos\left(\frac{1}{k}\right) - \arccos\left(\frac{1}{\sqrt{k^2 + 1}}\right) - \arccos\left(\frac{k}{\sqrt{k^2 + 1}}\right) + \frac{2k}{k^2 + 1} - \frac{\sqrt{k^2 - 1}}{k^2} \right) / \left( a(\sqrt{k^2 + 1} - k) \right),$$

$$K_4 = \pi - 2 \left( \arccos\left(\frac{1}{k}\right) - \frac{\sqrt{k^2 - 1}}{k^2} \right) - kaK_3. \quad (12)$$

For more details, please see the Appendix. Therefore, the closed-form of the SOP can be calculated to yield (13) on the next page.

## B. Transmitter selection and PPP eavesdroppers

In this subsection, we propose a transmitter selection scheme in which the intended receiver selects LED transmitter among multiple transmitters based on the location of the legitimate receiver, i.e., the nearest transmitter from UE is chosen to send the information-bearing signal. The channel gain in VLC is mainly determined by the LoS component, thus the nearest transmitter can be easily chosen by comparing the received SNRs at the legitimate receiver. In practice, multiple LEDs are uniformly and widely distributed to evenly illuminate the entire room within the lighting standards, e.g., from 400 to 1000 lux for a typical office [15]. We use the rectangular arrangement for LED transmitters satisfying the light requirement as shown in Fig. 3,

In this scenario, one legitimate receiver and multiple eavesdroppers are distributed by the BPP and PPP models, the latter with the density  $\lambda_E$ , respectively. Since the transmitter is selected based on the distance to UE, the coverage area of

$$f_{d_{BU}}(d) = \begin{cases} d\pi/(2a^2k) & \text{for } 0 < d \leq a \\ d \left( \pi - 2 \arccos\left(\frac{a}{d}\right) \right) / (2a^2k) & \text{for } a < d \leq ka \\ d \left( \pi - 2 \arccos\left(\frac{a}{d}\right) - 2 \arccos\left(\frac{ak}{d}\right) \right) / (2a^2k) & \text{for } ka < d \leq a\sqrt{k^2+1} \end{cases} \quad (9)$$

$$\begin{aligned} P_{SO} &= \mathbb{P}(d_{BE}^* < d_{BU}) = \int_0^{a\sqrt{k^2+1}} \mathbb{P}(d_{BE}^* < d_{BU} | d_{BU} = d) f_{d_{BU}}(d) dd \\ &= \frac{1}{4ka^2} \left( \int_0^a (1 - e^{-\lambda_E A_1(d)}) (2\pi d) dd + \int_a^{ka} (1 - e^{-\lambda_E \hat{A}_2(d)}) \hat{A}'_2(d) dd + \int_{ka}^{a\sqrt{k^2+1}} (1 - e^{-\lambda_E \hat{A}_3(d)}) \hat{A}'_3(d) dd \right) \\ &= \frac{1}{4ka^2} \left( \pi a^2 - \frac{e^{-\lambda_E \pi a^2} - 1}{\lambda_E} + K_1 a^3 (k^3 - 1) + K_2 a^2 (k^2 - 1) + \frac{e^{-\lambda_E a^2 k^2 (K_1 ak + K_2)} - e^{-\lambda_E a^2 (K_1 a + K_2)}}{\lambda_E} \right. \\ &\quad \left. + K_3 a^3 \left( (1 + k^2) \sqrt{1 + k^2} - k^3 \right) + K_4 a^2 + \frac{e^{-\lambda_E a^2 (1+k^2) (K_3 a \sqrt{1+k^2} + K_4)} - e^{-\lambda_E a^2 k^2 (K_3 ak + K_4)}}{\lambda_E} \right) \end{aligned} \quad (13)$$

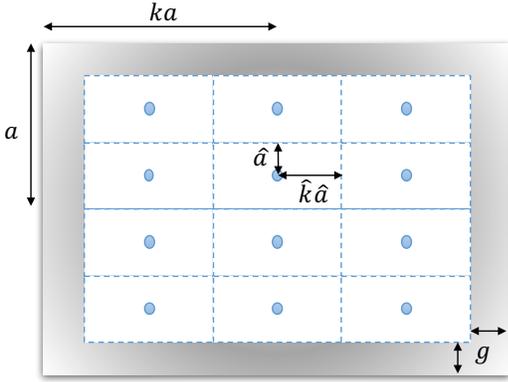


Fig. 3: A rectangular LED arrangement example for the LED transmitter selection, where  $N_r \times N_c = 4 \times 3$ .

each transmitter become a small rectangle. Let  $\hat{a}$  denote the half length of the rectangular coverage's width and  $\hat{k}$  denote the ratio of length to width of the coverage. We assume that the UE does not locate at the edge of the room, which is the shaded area in Fig. 3, while eavesdroppers can locate anywhere within the room. By defining the number of rows and columns of the LED arrangement as  $N_r$  and  $N_c$ , respectively, we can note  $\hat{a} = (a-g)/N_r$  and  $\hat{k} = (ka-g)/(N_c \hat{a})$ , where  $g$  denotes the thickness of the edge. We also assume that there are  $L = N_r \times N_c$  transmitters uniformly distributed and attached to the ceiling in which each transmitter has the equal transmission coverage area.

Since one legitimate receiver and multiple eavesdroppers are randomly and uniformly distributed, we can scale down this multiple transmitters configuration to only one rectangular coverage area. In other words, wherever the UE locates, due to the uniformly distributed transmitters, it should be in the coverage of a certain transmitter and the distance in the work plane between the selected transmitter BS and UE cannot exceed  $\hat{a}\sqrt{\hat{k}^2+1}$ . Therefore, the PDF of the distance in the work plane between the selected transmitter BS and UE, i.e.,

$d_{B^*U} = \min_{i \in \{1,2,\dots,L\}} d_{B_iU}$  is identical to (9) by changing from  $a$  and  $k$  to  $\hat{a}$  and  $\hat{k}$ .

We also define  $d_{BE}^*$  to be the distance in the work plane between the selected transmitters and the nearest eavesdropper, i.e.,  $d_{BE}^* = \min_{e \in \Phi_E} d_{B^*E_e}$ . The CDF of  $d_{BE}^*$  can be similarly calculated as in (10). However, the possible locations of eavesdroppers are slightly different. For the previous rectangular room, the eavesdroppers are assumed not to exist outside of the cuboid space, on the other hand, when we consider a certain rectangular coverage, the eavesdroppers can locate even outside of the rectangular region. As long as the thickness of the edge  $g$  is greater than  $\hat{a}(\sqrt{\hat{k}^2+1}-1)$ , the CDF of  $d_{BE}^*$  does not have different expressions according to the region of  $d$  unlike (10). Therefore, the CDF of  $d_{BE}^*$  is simply calculated to be  $F_{d_{BE}^*}(d) = 1 - \exp(-\lambda_E \pi d^2)$  for  $0 < d \leq \hat{a}\sqrt{\hat{k}^2+1}$ . Using these distribution functions, the SOP can be calculated to yield (14) at the top of the next page, where the upper incomplete gamma function is defined by  $\Gamma(s, z) = \int_z^\infty t^{s-1} e^{-t} dt$  and the exponential integral function  $\text{Ei}(x) = \int_{-x}^\infty e^{-t}/t dt$ . For (a) in (14), we apply the truncated Taylor expansion of  $\arccos(\cdot)$ :

$$\arccos(x) \approx P_K(x) = \frac{\pi}{2} - \sum_{n=0}^{K-1} \frac{(2n)!}{4^n (n!)^2 (2n+1)} x^{2n+1} \quad (15)$$

where  $P_K(x)$  is the  $K$ th order Taylor polynomial. By using the remainder theorem of Taylor polynomials [16], we can note that the 10th order Taylor polynomial of  $\arccos(x)$  has the remainder less than  $10^{-8}$  at  $x = 0.5$  and  $0.18$  at  $x = 1$ , respectively, which is considered as small enough to validate our analysis.

#### IV. THEORETICAL AND SIMULATION RESULTS

In this section, theoretical and simulation results are given to validate our analysis. The simulation results are obtained by averaging over  $10^5$  independent Monte Carlo trials. We set  $a = 4$  m,  $k = 1.5$ ,  $g = 0.8$  m and  $Z = 3$  m, and assume the

$$\begin{aligned}
P_{SO} &= \mathbb{P}(d_{BE}^* < d_{B^*U}) = \int_0^{\hat{a}\sqrt{\hat{k}^2+1}} \mathbb{P}(d_{BE}^* < d_{B^*U} | d_{B^*U} = d) f_{d_{B^*U}}(d) dd \\
&= \int_0^{\hat{a}} (1 - e^{-\lambda_E \pi d^2}) \left( \frac{d\pi}{2\hat{a}^2 \hat{k}} \right) dd + \int_{\hat{a}}^{\hat{a}\hat{k}} (1 - e^{-\lambda_E \pi d^2}) \left( \frac{d(\pi - 2 \arccos(\frac{\hat{a}}{d}))}{2\hat{a}^2 \hat{k}} \right) dd \\
&\quad + \int_{\hat{a}\hat{k}}^{\hat{a}\sqrt{\hat{k}^2+1}} (1 - e^{-\lambda_E \pi d^2}) \left( \frac{d(\pi - 2 \arccos(\frac{\hat{a}}{d}) - 2 \arccos(\frac{\hat{a}\hat{k}}{d}))}{2\hat{a}^2 \hat{k}} \right) dd \\
&\stackrel{(a)}{=} \frac{(e^{-\lambda_E \pi \hat{a}^2} - 1)/(\lambda_E \hat{a}^2) + \pi}{4\hat{k}} + \sum_{n=0}^K \left( \frac{(2n)!}{4^n (n!)^2 (2n+1)} \left( \frac{\hat{k}^{-2n} - \hat{k}^{-1}}{1-2n} - \frac{\text{Ei}(n + \frac{1}{2}, \lambda_E \pi \hat{a}^2)}{2\hat{k}} + \frac{\text{Ei}(n + \frac{1}{2}, \lambda_E \pi (\hat{a}\hat{k})^2)}{2\hat{k}^{2n}} \right) \right) \\
&\quad + \frac{(e^{\lambda_E \pi \hat{a}^2} - 1) e^{-\lambda_E \pi \hat{a}^2 (1+\hat{k}^2)} - \pi \lambda_E \hat{a}^2}{4\lambda_E \hat{a}^2 \hat{k}} + \sum_{n=0}^K \left( \frac{(2n)!}{4^n (n!)^2 (2n+1)} \frac{\hat{a}^{-1+2n} (1 + \hat{k}^{1+2n})}{\hat{k}} \right. \\
&\quad \left. \cdot \left( \frac{\hat{a}^{1-2n} (\hat{k}^{1-2n} - (1 + \hat{k}^2)^{\frac{1}{2}-n})}{-1+2n} + \frac{(\lambda_E \pi)^{n-\frac{1}{2}}}{2} \left( -\Gamma\left(\frac{1}{2} - n, \lambda_E \pi (\hat{a}\hat{k})^2\right) + \Gamma\left(\frac{1}{2} - n, \lambda_E \pi \hat{a}^2 (1 + \hat{k}^2)\right) \right) \right) \right) \quad (14)
\end{aligned}$$

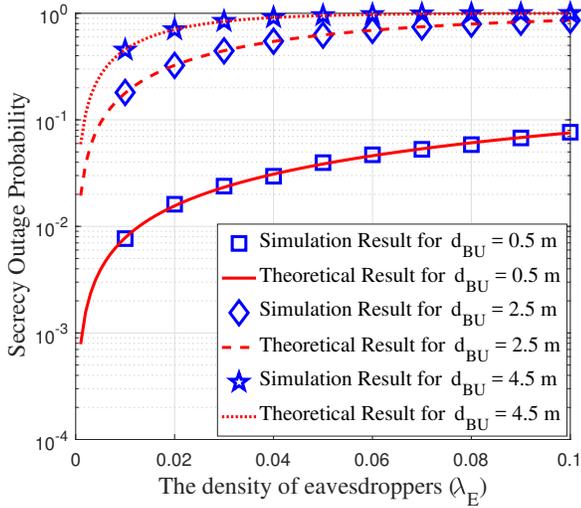


Fig. 4: Theoretical vs simulation secrecy outage probabilities for one fixed UE and multiple eavesdroppers with different density  $\lambda_E$ , where  $a = 4$  m and  $k = 1.5$ .

LED half luminous intensity semi-angle as  $\phi_{1/2} = 60^\circ$  and the receiver field of view as  $\psi_{Fov} = 60^\circ$  as in [5]. The theoretical results referred to in this section are corresponding to (6), (13), and (14).

Fig. 4 shows the simulation and theoretical results for the configuration of fixed UE and PPP Es. It shows that the secured connection is difficult to be established with a single LED transmitter when the legitimate user locates somewhat far away from the transmitter even with a tiny density. Note that, for the the given room size of  $4ka^2 = 96$  m<sup>2</sup>, at the upper end of the density range in the plot, i.e.,  $\lambda_E = 0.1$ , there are averagely 10 eavesdroppers located in the room. Also, one or no eavesdropper is located for the density less than  $\lambda_E = 0.01$ .

Fig. 5 shows the SOP for the configuration of BPP UE and PPP Es as the density of multiple eavesdroppers  $\lambda_E$  increases. As can be seen, the SOP is very high with a single transmitter, on the other hand, the secrecy performance with

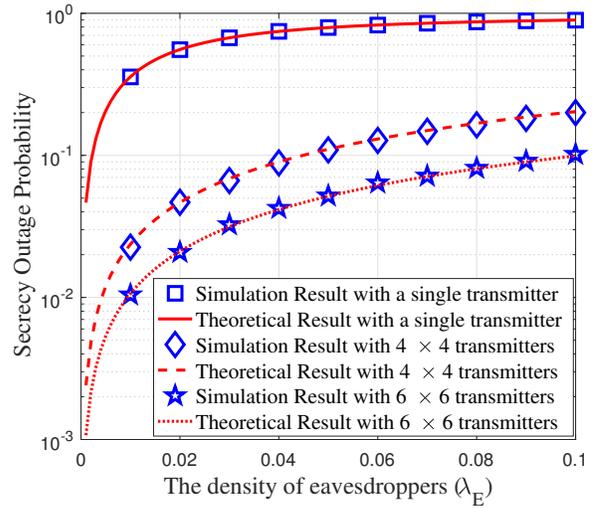


Fig. 5: Theoretical vs simulation secrecy outage probabilities for one BPP UE and multiple eavesdroppers with different density  $\lambda_E$ , where  $a = 4$  m,  $k = 1.5$  and  $g = 0.8$  m. For the transmitter selection scheme with  $4 \times 4$  and  $6 \times 6$  transmitters,  $\hat{a} = 0.8$  m,  $\hat{k} = 1.625$  and  $\hat{a} = 0.53$  m,  $\hat{k} = 1.625$  are used, respectively.

the transmitter selection scheme can be significantly improved. More specifically, the  $P_{SO}$  for  $\lambda_E = 0.05$  is about 0.79 without the transmitter selection scheme, while the  $P_{SO}$  with the transmitter selection scheme of  $4 \times 4$  LEDs for the same density is only about 0.11. Also, we can note that the secrecy performance can be more improved with a larger number of transmitters. This proposed transmitter selection scheme would be practical especially in a wide open space such as malls and large office. In such a large space, there might be so many transmitters spread out widely to illuminate the large space evenly. However, from the communication point of view, only the nearest one might be the main contributor for the receiver's SNR. It might be unnecessary for all the transmitters to transmit the signal to the intended user, since it could help eavesdroppers wiretap the signal more easily.

TABLE I: Secrecy Outage Probability for the different ratio  $\hat{k}$ 

$N_r \times N_c$	$12 \times 12$	$16 \times 9$	$18 \times 8$	$24 \times 6$
Theoretical $P_{so}$	0.029	0.034	0.038	0.059
Simulation $P_{so}$	0.029	0.034	0.038	0.059
$\hat{a}$ (m)	0.375	0.281	0.250	0.188
$\hat{k}$	1	1.78	2.25	4.00
$L = 144, 4\hat{k}\hat{a}^2 = 0.563 \text{ m}^2, a = 5 \text{ m}, k = 1, g = 0.5 \text{ m}$				

Table. I shows the SOP according to the different ratio  $\hat{k}$  while maintaining the coverage area  $4\hat{k}\hat{a}^2$  and the room configuration, i.e.,  $a$  and  $k$ . To change  $\hat{k}$ , we apply different  $N_r \times N_c$  combinations for a given number of transmitters. The result shows that the outage probability slightly increases as  $\hat{k}$  increases. The square, i.e.,  $\hat{k} = 1$ , has the lowest SOP. These results can be interpreted as that since eavesdroppers are uniformly distributed throughout the work plane, minimizing the expected distance between the transmitter and the legitimate user, i.e.,  $\mathbb{E}[d_{B^*U}]$ , would result in the minimum SOP. Thus, this result can be used to design an LED arrangement to maximize the secrecy performance given the number of transmitters and the room standard.

## V. CONCLUSION

In this paper, the SOP was derived as a function of the density of eavesdroppers and geometric factors related to the indoor VLC environment. To deal with the randomly located receivers, we applied the stochastic geometry such as BPP and PPP models to represent E and UE spatial locations. This analysis was validated via theoretical and simulation results. Furthermore, we verified that a transmitter selection scheme could significantly reduce the SOP.

## APPENDIX

### THE PIECEWISE APPROXIMATION OF THE BOUNDED CIRCLE

The bounded circle  $A_i(d)$  for  $i \in \{1, 2, 3\}$  in (7) can be described in the form of  $A_i(d) = C_i(d) \cdot d^2$ , where  $C_i(d)$  for  $i \in \{1, 2, 3\}$  are given by

$$\begin{aligned} C_1(d) &= \pi, \\ C_2(d) &= \pi - 2 \left( \arccos\left(\frac{a}{d}\right) - \frac{a\sqrt{d^2 - a^2}}{d^2} \right), \\ C_3(d) &= \pi - 2 \left( \arccos\left(\frac{a}{d}\right) - \frac{a\sqrt{d^2 - a^2}}{d^2} \right) \\ &\quad - 2 \left( \arccos\left(\frac{ak}{d}\right) - \frac{ak\sqrt{d^2 - (ak)^2}}{d^2} \right). \end{aligned}$$

Here, we approximate  $C_i(d)$  for  $i \in \{2, 3\}$  with a linear function of  $d$ , i.e.,  $\hat{C}_2(d) = K_1d + K_2$  and  $\hat{C}_3(d) = K_3d + K_4$ , respectively. To find the optimal  $K_i$  for  $i \in \{1, 2, 3, 4\}$ , we evaluate three coordinates  $C_1(a)$ ,  $C_2(ak)$ , and  $C_3(a\sqrt{k^2 + 1})$  as shown in Fig. 6. Using these values, we can easily calculate the approximation constants as in (12).

## ACKNOWLEDGMENT

The work was supported in part by EPSRC grant number EP/N002350/1 (“Spatially Embedded Networks”).

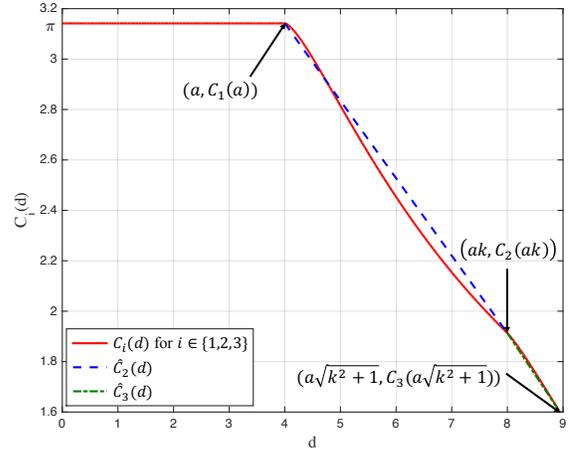


Fig. 6: An example of  $\hat{C}_2(d)$  and  $\hat{C}_3(d)$  for  $a = 4 \text{ m}$ ,  $k = 2$ . Note  $ak = 8 \text{ m}$  and  $a\sqrt{k^2 + 1} = 8.94 \text{ m}$ .

## REFERENCES

- [1] S. Wu, H. Wang, and C. H. Youn, “Visible light communications for 5G wireless networking systems: from fixed to mobile communications,” *IEEE Network*, vol. 28, no. 6, pp. 41–45, Nov. 2014.
- [2] H. Elgala, R. Mesleh, and H. Haas, “Indoor optical wireless communication: potential and state-of-the-art,” *IEEE Commun. Magazine*, vol. 49, no. 9, pp. 56–62, Sep. 2011.
- [3] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, “Visible light communication, networking, and sensing: A survey, potential and challenges,” *IEEE Commun. Surveys Tutorials*, vol. 17, no. 4, pp. 2047–2077, 2015.
- [4] A. Mostafa and L. Lampe, “Securing visible light communications via friendly jamming,” in *IEEE Globecom Workshops in Austin, USA*, Dec. 2014.
- [5] —, “Physical-layer security for MISO visible light communication channels,” *IEEE Journal on Selected Areas in Commun.*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.
- [6] H. Zaid, Z. Rezki, A. Chaaban, and M. S. Alouini, “Improved achievable secrecy rate of visible light communication with cooperative jamming,” in *2015 IEEE GlobalSIP in Orlando, USA*, Dec. 2015.
- [7] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, “Stochastic geometry and random graphs for the analysis and design of wireless networks,” *IEEE Journal on Selected Areas in Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.
- [8] G. Chen, J. P. Coon, and M. D. Renzo, “Secrecy enhancement by antenna selection and FD communication with randomly located eavesdroppers,” in *IEEE GLOBECOM in Washington D.C., USA*, Dec. 2016.
- [9] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, “On the throughput cost of physical layer security in decentralized wireless networks,” *IEEE Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
- [10] T. X. Zheng, H. M. Wang, and Q. Yin, “On transmission secrecy outage of a multi-antenna system with randomly located eavesdroppers,” *IEEE Commun. Lett.*, vol. 18, no. 8, pp. 1299–1302, Aug. 2014.
- [11] G. Chen, J. P. Coon, and M. D. Renzo, “Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1195–1206, May 2017.
- [12] G. Pan, J. Ye, and Z. Ding, “On secure VLC systems with spatially random terminals,” *IEEE Commun. Lett.*, to appear, 2017.
- [13] T. Komine and M. Nakagawa, “Fundamental analysis for visible-light communication system using LED lights,” *IEEE Consumer Electronics*, vol. 50, no. 1, pp. 100–107, Feb. 2004.
- [14] A. Baddeley, E. Rubak, and R. Turner, *Spatial point patterns: methodology and applications with R*. CRC Press, 2015.
- [15] *Lighting of Indoor Work Places*, European Stand. EN 12464-1, 2003.
- [16] T. Apostol, *Calculus: One-variable calculus, with an introduction to linear algebra*, ser. Calculus. Wiley, 1967.