THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

Physical-Layer Security in Multiuser Visible Light Communication Networks

Citation for published version:
Yin, L & Haas, H 2017, 'Physical-Layer Security in Multiuser Visible Light Communication Networks', *IEEE Journal on Selected Areas in Communications*, pp. 162 - 174. https://doi.org/10.1109/JSAC.2017.2774429

Digital Object Identifier (DOI):
10.1109/JSAC.2017.2774429

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
IEEE Journal on Selected Areas in Communications

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

OPEN ACCESS

Download date: 27. Apr. 2024

Physical-Layer Security in Multiuser Visible Light Communication Networks

Liang Yin and Harald Haas, *Senior Member, IEEE*

***Abstract*— In this paper, we study the physical-layer security in a 3-D multiuser visible light communication (VLC) network. The locations of access points (APs) and mobile users are modeled as two 2-D, independent and homogeneous Poisson point processes at distinct heights. Using mathematical tools from stochastic geometry, we provide a new analytical framework to characterize the secrecy performance in multiuser VLC networks. Closed-form results for the outage probability and the ergodic secrecy rate are derived for networks without AP cooperation. Considering the cooperation among APs, we give tight lower and upper bounds on the secrecy outage probability and the ergodic secrecy rate. To further enhance the secrecy performance at the legitimate user, a disk-shaped secrecy protected zone is implemented in the vicinity of the transmit AP. Based on the obtained results, it is shown that cooperating neighboring APs in a multiuser VLC network can bring performance gains on the secrecy rate, but only to a limited extent. We also show that building an eavesdropper-free protected zone around the AP significantly improves the secrecy performance of legitimate users, which appears to be a promising solution for the design of multiuser VLC networks with high security requirements.**

***Index Terms*— Visible light communication, secrecy capacity, physical-layer security, poisson point process, stochastic geometry.**

I. Introduction

BY UTILIZING the existing lighting infrastructure and shifting the communication frequency to the visible spectrum, visible light communication (VLC) [1]–[3] has recently emerged as a promising candidate for future high-speed broadband communications, which could effectively alleviate the spectrum congestion issue in current radio frequency (RF) based wireless systems. Recent advances have also led to the standardization of short-range wireless optical communication using VLC for local and metropolitan area networks [4], which serves as a major step towards its commercialization in the near future. Compared to RF communication, VLC has the following main advantages: 1) VLC builds upon existing lighting devices and operates on the license-free spectrum so that it has lower implementation cost; 2) VLC can operate safely in electromagnetic sensitive areas, where RF is intrinsically prohibited; 3) VLC networking can be designed in addition to existing heterogeneous wireless networks because it receives zero interference from, and adds zero interference to its RF counterparts; 4) Based on the property that visible light does not penetrate through opaque objects, the communication bandwidth in one room can be efficiently reused in other rooms to obtain a high frequency reuse factor and hence a high area spectral efficiency; 5) Indoor VLC typically achieves higher physical-layer security since the transmitted signal is confined within the room.

The broadcast property of VLC has been utilized in many novel designs of multiuser VLC networks [5]–[7]. However, it also causes potential concerns to legitimate users and network administrators regarding the information privacy and confidentiality, especially in public areas, such as train stations and libraries. From an information-theoretic point of view, the physical-layer security was pioneered by Wyner for proposing the wiretap channel [8]: a channel in which an eavesdropper receives a degraded version of the transmitted signal. The degraded wiretap channel was later extended to the non-degraded broadcast channel by Csiszár and Körner [9]. In their seminal work, it is shown that perfect secrecy can be achieved as long as the legitimate user has a less degraded channel than the eavesdropper, and the secrecy capacity is derived as the difference between the information capacity for the two users. Typical security enhancement techniques that are implemented at upper layers of the communication chain include password protection and user admission control. Physical-layer security, on the other hand, exploits the randomness of the noise and the wireless communication channel to limit the amount of legitimate information to be detected by unauthorized eavesdroppers [8], [9].

Different from point-to-point communication, studying the secrecy performance in a large-scale wireless network requires not only the knowledge of locations of legitimate users but also the knowledge of locations of eavesdropping users that may interact with legitimate users. Initial works that characterize the secrecy performance in multiuser wireless networks rely on the secrecy graph model to study the node connectivity [10], [11] and the maximum secrecy rate [12], from an information-theoretic perspective. Following these works, the secrecy rate per source-destination pair was investigated in [13] by characterizing the secrecy capacity scaling laws in a wireless network. Moving from network information theory, recent works have evaluated the secrecy performance in multiuser wireless networks using mathematical tools from stochastic geometry [14], [15]. It should be noted that works in [8]–[15] are all focused on RF based wireless networks.

Manuscript received February 22, 2017; revised July 15, 2017; accepted September 16, 2017. This work was supported by the U.K. Engineering and Physical Sciences Research Council under Grant EP/K008757/1. *(Corresponding author: Liang Yin.)*

The authors are with the School of Engineering, Institute for Digital Communications, Li-Fi Research and Development Centre, University of Edinburgh, Edinburgh EH9 3JL, U.K. (e-mail: l.yin@ed.ac.uk; h.haas@ed.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSAC.2017.2774429

0733-8716 © 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

IEEE Proof

Different from RF communication, which is typically modeled as a Gaussian broadcast channel with an average power constraint at the transmitter side, VLC typically uses intensity modulation and direct detection (IM/DD) due to the use of inexpensive light-emitting diodes (LEDs) and photodiodes (PDs) as the optical transmitter and receiver, respectively. In VLC, since the signal is modulated onto the intensity of the emitted light, it must satisfy average, peak as well as non-negative amplitude constraints, that are imposed by the dynamic range of typical LEDs and practical illumination requirements [6], [16]–[18]. Although typical LEDs have a nonlinear electrical-to-optical (E/O) transfer characteristic, this nonlinearity can be successfully compensated by pre-distortion techniques [19]. Also, since the wavelength of visible light is hundreds of nanometers while the detection area of a typical PD is millions of square wavelengths, this spatial diversity essentially prevents the "multipath fading" effect in the VLC channel. Due to these fundamental differences, results on the secrecy capacity obtained for RF networks can not be directly applied to VLC networks.

Since the secrecy capacity is related to the information capacity of the communication channel [8], [9], before determining the secrecy capacity in VLC networks it is essential to obtain the information capacity of the VLC channel with average, peak and non-negative constraints. However, to the best of authors' knowledge, the exact information capacity of the VLC channel with such constraints still remains unknown, even for the simplest single-input single-output (SISO) case, despite some lower and upper bounds have been derived [16]–[18]. By considering one transmitter, one legitimate user and one eavesdropper in a VLC system, lower and upper bounds on the secrecy capacity of the amplitude-constrained Gaussian wiretap channel was recently studied in [20], with the use of the derived capacity lower and upper bounds in [16]. In the same work [20], beamforming was also utilized to improve the secrecy capacity for the multiple-input single-output (MISO) VLC channel. Following this, the optimal beamformer design problem subject to amplitude constraints was further studied in [21]. The secrecy performance in a single-cell VLC system with only one AP was studied in [22]. However, the randomness of legitimate users as well as eavesdroppers and, more importantly, the interactions between them, have not been fully characterized when analyzing the secrecy performance in a random multiuser VLC network.

A. Approaches and Contributions

In this work, we aim to characterize the secrecy performance in an indoor multiuser VLC network by considering the unique properties of the VLC channel as well as the network layout, that differ from typical RF networks. Our approach builds upon a proposed three-dimensional network model with two independent random topologies for the VLC APs and mobile users. Specifically, the VLC APs are modeled by a two-dimensional homogeneous Poisson point process (PPP) in the ceiling, while the locations of users, that include both legitimate users and eavesdroppers, are modeled by another independent two-dimensional homogeneous PPP at the user plane. To separate eavesdroppers from legitimate users, the locations of random eavesdroppers are obtained from a thinned PPP. Despite the grid-like deployment of LEDs in typical offices, the following observations indicate that a stochastic model may be required to accurately capture the distribution of APs in a VLC network. First, more and more LEDs with built-in motion-detection sensors are deployed in public spaces in order to reduce energy consumption. In this case, some of the LEDs will be temporally switched off when they are not required to provide illumination. Second, the distribution of ceiling lights is not necessarily equivalent to the distribution of APs in a VLC network because not necessarily all of the ceiling lights are simultaneously operating in the communication mode, i.e., some of the ceiling lights may operate in the illumination mode only when no data traffic is demanded from them. In these scenarios, the distribution of APs can not be accurately modeled by the grid model. Instead, a stochastic thinning process built upon the grid-like deployment of LEDs is more accurate, where the activeness/idleness of each AP is determined by a time-varying probability distribution function (PDF). However, finding the PDF of activeness/idleness of the LED requires full knowledge of the users' movement and handover characteristics, which is generally complicated and not analytically tractable. In order to derive analytically tractable results, the PPP model is assumed in this work. For completeness, we also compare the secrecy performance between the PPP model and the grid model and provide a method of applying the derived analytical results to estimate the secrecy performance in a conventional grid-like VLC network.

The main contributions of this paper are as follows:

1) When the legitimate user is served by the nearest AP in its vicinity, we derive the distribution function of the secrecy rate of a typical legitimate user, based on which secrecy outage probability and ergodic secrecy rate are obtained. To provide further insights into the secrecy performance with different network parameters, lower and upper bounds on the secrecy outage probability as well as on the ergodic secrecy rate are given.
2) We enhance the secrecy performance by implementing AP cooperation in a multiuser VLC network, and give lower and upper bounds on the secrecy outage probability and the ergodic secrecy rate. The derived analytical bounds are found to be reasonably tight in general and become tighter when the density of eavesdroppers becomes larger.
3) To further enhance the secrecy performance for legitimate users, we introduce a disk-shaped secrecy protected zone around the AP in a multiuser VLC network, in which the presence of eavesdroppers is prohibited. In this scenario, the secrecy outage probability and the ergodic secrecy rate are derived. The impact of designing the protected zone with different sizes on the secrecy performance is also investigated.

The remainder of this paper is organized as follows. In Section II, we introduce a three-dimensional link model for multiuser VLC networks and formulate the information-theoretic secrecy rate expression based on a close

IEEE Proof

approximation of the channel capacity. The secrecy outage probability and the ergodic secrecy rate with/without the AP cooperation are derived in Section III. We extend the analysis on the secrecy performance in Section IV by implementing a disk-shaped protected zone. Simulation results and discussions are provided in Section V. Finally, concluding remarks are given in Section VI.

II. System Model

A. Poisson Network Model

We consider a downlink transmission scenario of a multiuser VLC network with the presence of both legitimate users and eavesdroppers inside a three-dimensional space. The VLC APs are vertically fixed, since they are attached to the room ceiling, and their horizontal positions are modeled by a two-dimensional homogeneous PPP Φ_{a} with density λ_{a}, in nodes per unit area. Similarly, mobile users are assumed to be at a fixed height and their horizontal positions are modeled by another independent two-dimensional homogeneous PPP Φ_{u} with density λ_{u}. The vertical distance between the AP plane and the user plane is denoted by L. After adding an additional user at the room center,[1] the new point process for mobile users becomes $\Phi_{\mathrm{u}} \bigcup \{0\}$. Slivnyak's theorem states that adding a user into Φ_{u} is equivalent to conditioning Φ_{u} on the added point, and this process does not change the distribution of Φ_{u} [23]. Therefore, the added user at the origin can be treated as the *typical* legitimate user in the study since it can reflect the spatial average of the performance of all legitimate users in the network. Among all of the users, there exist malicious eavesdroppers that could compromise the transmission privacy of ongoing legitimate links, due to the broadcast nature of the VLC channel. Since eavesdroppers typically disguise as legitimate users, it is uncertain whether a random user $u \in \Phi_{\mathrm{u}}$ is a legitimate user or an eavesdropper. Therefore, it is assumed that u is an eavesdropper with probability p_{e} and that u is a legitimate user with probability $1 - p_{\mathrm{e}}$. This thinned realization of Φ_{u} gives the point process for eavesdroppers, Φ_{e}, which is also a homogeneous PPP whose density can be found as $\lambda_{\mathrm{e}} = p_{\mathrm{e}}\lambda_{\mathrm{u}}$ [23]. Furthermore, it is assumed that eavesdroppers do not collude with each other so that each eavesdropper needs to decode any confidential messages sent to legitimate users individually. An example of the described multiuser VLC network is depicted in Fig. 1.

A complete VLC channel includes both the line-of-sight (LOS) link and non-line-of-sight (NLOS) links, that are caused by light reflections from interior surfaces. However, in a typical indoor lighting environment, the sum signal power carried by NLOS components is significantly weaker than that carried by the LOS link [1], [24], [25]. Therefore, we will only focus on the LOS link in the following analysis in order to obtain tractable analytical results. The VLC APs are assumed to have a Lambertian radiation profile whose Lambertian order is $m = -1/\log_2(\cos\ (\Phi_{1/2}))$, where $\Phi_{1/2}$ denotes the semi-angle of the LED. The PD equipped at each user is assumed to be facing vertically upwards with a field-of-view (FOV) of Ψ_{fov}. For each VLC link, the optical channel direct current (DC) gain is given by [26]:

$$h = \frac{(m+1)A\eta}{2\pi d^2}\cos^m(\phi)T(\psi)g(\psi)\cos(\psi), \qquad (1)$$

where A denotes the effective detection area of the PD; η is the responsivity of the PD; ϕ and ψ are the angle of irradiance and the angle of incidence of the optical link, respectively; $T(\psi)$ represents the gain of the optical filter used at the receiver; and $g(\psi)$ represents the gain of the optical concentrator. The optical concentrator gain is given by [26]:

$$g(\psi) = \begin{cases} \dfrac{n^2}{\sin^2(\Psi_{\mathrm{fov}})}, & 0 \le \psi \le \Psi_{\mathrm{fov}} \\ 0, & \psi > \Psi_{\mathrm{fov}} \end{cases}, \qquad (2)$$

where n is the reflective index of the optical concentrator, and it is defined as the ratio of the speed of light in vacuum and the phase velocity of light in the optical material. For visible light, the typical value for n varies between 1 and 2.

Consider the communication link from an AP $x \in \Phi_{\mathrm{a}}$ to an eavesdropper $e \in \Phi_{\mathrm{e}}$. Based on the geometry [7] of the VLC link, it is easy to obtain $d = \sqrt{\|e-x\|^2 + L^2}$, $\cos(\phi) = L/\sqrt{\|e-x\|^2+L^2}$ and $\cos(\psi) = L/\sqrt{\|e-x\|^2+L^2}$. Therefore, the received optical power at eavesdropper e from AP x can be written as:

$$\begin{aligned} P_{\mathrm{rx}}(x,e) &= hP_{\mathrm{tx}} \\ &= \frac{(m+1)A\eta T(\psi)g(\psi)L^{m+1}}{2\pi(\|e-x\|^2+L^2)^{\frac{m+3}{2}}}P_{\mathrm{tx}}, \qquad (3) \end{aligned}$$

where P_{tx} denotes the transmit optical power of the AP. Similarly, the received signal power at the legitimate user can be written as $P_{\mathrm{rx}}(x,o)$, where o representing the origin is the location of the typical user of interest.

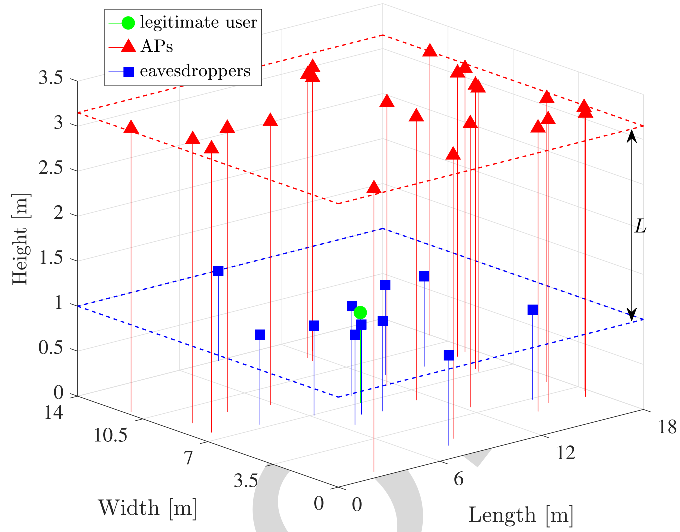

Fig. 1. Random network model: the legitimate user of interest is placed at the room center; VLC APs are randomly distributed in the ceiling according to a homogeneous PPP Φ_{a}; and eavesdroppers are randomly distributed on the same plane as the legitimate user, following a homogeneous PPP Φ_{e}. In this example, an indoor VLC network of size $18 \times 14 \times 3.5$ m^3 is shown.

[1]The room center is also called the origin. We use both expressions interchangeably throughout the paper since the room center has more geographical meanings while the origin has more mathematical meanings when we apply stochastic geometry tools in the theoretical analysis.

B. Secrecy Capacity Formulation

The classic Shannon equation does not apply to VLC because of the average, peak and non-negative constraints on the modulated optical signal. Although the exact capacity of the VLC channel remains unknown, several upper and lower bounds have been derived [16]–[18]. Based on the capacity lower bound derived in [16], the exact channel capacity of VLC can be written as:

$$C = \frac{1}{2}\log_2\left(1 + \frac{\exp(1)P_{\mathrm{rx}}^2}{2\pi\sigma_{\mathrm{n}}^2}\right) + \epsilon\left(\frac{P_{\mathrm{rx}}}{\sigma_{\mathrm{n}}}\right), \tag{4}$$

where ϵ, as a function of the received optical-signal-to-noise ratio (OSNR) $P_{\mathrm{rx}}/\sigma_{\mathrm{n}}$, represents a positive capacity gap between the exact channel capacity and the analytical lower bound [16], and σ_{n}^2 represents the total power of noise processes at the receiver. Note that inside the receiver circuit the dominant noise sources are the thermal noise and shot noise [1], [25]. The thermal noise is mainly caused by the preamplifier circuits while the shot noise originates mainly from the ambient light and/or other light sources. The signal-dependent shot noise, on the other hand, is relatively small, and hence its effect can be ignored. The overall noise process is generally well modeled as the additive white Gaussian noise (AWGN) [1], [25]. As the legitimate user and eavesdroppers may use different grades of receivers, for example, PDs with different detection areas and/or bandwidths, they are subject to different levels of receiver noise and are capable of detecting signals with different amplifying gains. Without loss of generality, the choice of different grades of receivers can be accounted for in the system model by assigning different noise variances at the legitimate user and the eavesdropper. Based on this, we denote by σ_{nb}^2 and σ_{ne}^2 the noise variance at the legitimate user and the noise variance at the eavesdropper, respectively. Unlike RF channels whose input signals are subject to an average power constraint [29], VLC channels require the input signals to satisfy a peak amplitude (optical power) constraint. This makes it challenging to obtain closed-form expressions for the secrecy capacity of a VLC link, even for the simplest SISO case [20], [30]. Therefore, in the following analysis we focus on a tight achievable lower bound on the secrecy capacity [20]:

$$C_{\mathrm{s}} \ge [C_{\mathrm{b}} - C_{\mathrm{e}}]^+ = \underline{C}_{\mathrm{s}}, \tag{5}$$

where $[a]^+ = \max\{a, 0\}$; C_{s} represents the exact secrecy capacity; $\underline{C}_{\mathrm{s}}$ represents the tight lower bound on the secrecy capacity given by the right-hand side of (5); C_{b} is the channel capacity of the legitimate link; and C_{e} is the channel capacity of the eavesdropper's link.

III. Secrecy Rate in Random VLC Networks

A. Nearest AP to Serve the Legitimate User

Without AP cooperation, the nearest AP is typically assumed to serve a mobile user in the VLC network in order to maximize the information rate of the communication link. As a result, based on (4), the capacity of the legitimate link can be written as $C_{\mathrm{b}} = \max_{x\in\Phi_{\mathrm{a}}} \frac{1}{2}\log_2(1+\exp(1)P_{\mathrm{rx}}^2(x,o)/2\pi\sigma_{\mathrm{nb}}^2) + \epsilon\left(P_{\mathrm{rx}}(x,o)/\sigma_{\mathrm{nb}}\right) = \frac{1}{2}\log_2(1+\exp(1)P_{\mathrm{rx}}^2(x_0,o)/2\pi\sigma_{\mathrm{nb}}^2) + \epsilon\left(P_{\mathrm{rx}}(x_0,o)/\sigma_{\mathrm{nb}}\right)$, where x_0 represents the location of the nearest AP to the origin. Since it is assumed that eavesdroppers do not collude, the secrecy performance of the legitimate user is limited by the eavesdropper with the highest OSNR. Therefore, the lower bound on the secrecy capacity at the typical legitimate user is formulated as:

$$\begin{aligned}\underline{C}_{\mathrm{s}} = \Bigg[&\frac{1}{2}\log_2\left(1 + \frac{\exp(1)P_{\mathrm{rx}}^2(x_0,o)}{2\pi\sigma_{\mathrm{nb}}^2}\right) \\ &- \frac{1}{2}\log_2\left(1 + \frac{\exp(1)P_{\mathrm{rx}}^2(x_0,e^*(x_0))}{2\pi\sigma_{\mathrm{ne}}^2}\right) \\ &+ \epsilon\left(\frac{P_{\mathrm{rx}}(x_0,o)}{\sigma_{\mathrm{nb}}}\right) - \epsilon\left(\frac{P_{\mathrm{rx}}(x_0,e^*(x_0))}{\sigma_{\mathrm{ne}}}\right)\Bigg]^+, \end{aligned} \tag{6}$$

where $e^*(x_0)$ denotes the horizontal distance from AP x_0 to the nearest eavesdropper. Given that the legitimate user is connected to AP x, the general solution for $e^*(x)$, denoting the horizontal distance between AP x and the strongest eavesdropper, can be obtained by finding the location of the eavesdropper $e \in \Phi_{\mathrm{e}}$ that receives the strongest signal power:

$$\begin{aligned} e^*(x) &= \arg\max_{e\in\Phi_{\mathrm{e}}} P_{\mathrm{rx}}(x,e) \\ &= \arg\min_{e\in\Phi_{\mathrm{e}}} \|e - x\|, \end{aligned} \tag{7}$$

where the last step is obtained based on the monotonic property of (3). By utilizing fractional frequency reuse [28] or orthogonal multiple access techniques, the achievable data rate can be quantified through the received signal-to-noise ratio (SNR) without the side effect of co-channel interference (CSI). As a result, OSNR of $P_{\mathrm{rx}}/\sigma_{\mathrm{n}} > 30$ dB can be achieved at typical illumination levels [25], [27], where $\epsilon(P_{\mathrm{rx}}/\sigma_{\mathrm{n}})$ is found to be comparatively small [16]–[18]. Therefore, we focus on the high OSNR regime, where $\epsilon(P_{\mathrm{rx}}(x_0,o)/\sigma_{\mathrm{nb}}) \ll 1/2\log_2(\exp(1)P_{\mathrm{rx}}^2(x_0,o)/2\pi\sigma_{\mathrm{nb}}^2)$ and $\epsilon(P_{\mathrm{rx}}(x_0,e^*(x_0))/\sigma_{\mathrm{ne}}) \ll 1/2\log_2(\exp(1)P_{\mathrm{rx}}^2(x_0,e^*(x_0))/2\pi\sigma_{\mathrm{ne}}^2)$. Based on this, (6) can be further approximated to:

$$\underline{C}_{\mathrm{s}} \approx \left[\frac{1}{2}\log_2\left(\frac{P_{\mathrm{rx}}^2(x_0,o)}{P_{\mathrm{rx}}^2(x_0,e^*(x))}\right) + \log_2\left(\frac{\sigma_{\mathrm{ne}}}{\sigma_{\mathrm{nb}}}\right)\right]^+ = R_{\mathrm{s}}. \tag{8}$$

To distinguish from the exact secrecy capacity, we define in (8) R_{s} as the achievable secrecy rate. Due to the lack of the complete knowledge of the exact secrecy capacity C_{s}, the secrecy rate R_{s} is of interest in this paper. It is shown in (8) that a non-negative secrecy rate can only be achieved when the legitimate user achieves a higher SNR than the strongest eavesdropper. In the case that a eavesdropper receives signals from a less-degraded link than the legitimate user, the achievable secrecy rate drops to zero. It can also be seen from (8) that when the legitimate user and the eavesdropper use different grades of receivers, the achieved secrecy capacity at the legitimate user is offset by a constant, whose value is proportional to the logarithm of $\sigma_{\mathrm{ne}}/\sigma_{\mathrm{nb}}$. Therefore, without loss of generality, $\sigma_{\mathrm{nb}} = \sigma_{\mathrm{ne}}$ is assumed in the following analysis.

Theorem 1: When the legitimate user is served by the nearest AP in its vicinity, the cummulative distribution function (CDF) of the secrecy rate R_{s} is given by:

$$F_{R_{\mathrm{s}}}(\upsilon) = 1 - \frac{1}{1 + \frac{\lambda_{\mathrm{e}}}{\lambda_{\mathrm{a}}}4^{\frac{\upsilon}{m+3}}}\exp\left(-\pi\lambda_{\mathrm{e}}\left(4^{\frac{\upsilon}{m+3}} - 1\right)L^2\right), \tag{9}$$

where $\upsilon \ge 0$.

IEEE Proof

Proof: According to (8), we have $R_s \geq 0$. Therefore, the CDF of the secrecy rate R_s can be calculated by:

$$\begin{aligned} F_{R_s}(\upsilon) &= \mathbb{P}\left[R_s \leq \upsilon\right] \\ &= \mathbb{P}\left[\frac{P_{rx}^2(x_0, o)}{P_{rx}^2(x_0, e^*(x_0))} \leq 4^{\upsilon}\right] \\ &= \mathbb{P}\left[\|e^*(x_0) - x_0\| \leq \sqrt{\beta x_0^2 + (\beta - 1)L^2}\right], \end{aligned} \quad (10)$$

where $\beta = 4^{\upsilon/(m+3)}$. Since the legitimate user is served by the nearest AP, the PDF of x_0 is [31]:

$$f_{x_0}(x_0) = 2\pi\lambda_a x_0 \exp\left(-\pi\lambda_a x_0^2\right). \quad (11)$$

When conditioned on distance x_0, (10) is the probability that no eavesdroppers exist within a circle, which is centered at x_0 and has a radius of $\sqrt{\beta x_0^2 + (\beta - 1)L^2}$. Such probability can be calculated using the void probability of PPP [32]. As a result, (10) can be calculated as:

$$\begin{aligned} &F_{R_s}(\upsilon) \\ &= \mathbb{E}_{x_0}\left[\mathbb{P}\left[\|e^*(x_0) - x_0\| \leq \sqrt{\beta x_0^2 + (\beta - 1)L^2}\,\middle|\, x_0\right]\right] \\ &= \int_0^\infty \mathbb{P}\left[\|e^*(x_0) - x_0\| \leq \sqrt{\beta x_0^2 + (\beta - 1)L^2}\,\middle|\, x_0\right] f_{x_0}(x_0)\mathrm{d}x_0 \\ &= \int_0^\infty \left(1 - \exp\left(-\pi\lambda_e\left(\beta x_0^2 + (\beta - 1)L^2\right)\right)\right) 2\pi\lambda_a x_0 \\ &\quad \times \exp\left(-\pi\lambda_a x_0^2\right)\mathrm{d}x_0 \\ &= 1 - \frac{1}{1 + \frac{\lambda_e}{\lambda_a}\beta}\exp\left(-\pi\lambda_e(\beta - 1)L^2\right). \end{aligned} \quad (12)$$

After plugging $\beta = 4^{\upsilon/(m+3)}$ into (12), we obtain (9). ■

Corollary 1: When the legitimate user is served by the n-th nearest AP in its vicinity, the CDF of the secrecy rate is:

$$F_{R_s}(\upsilon) = 1 - \left(\frac{1}{1 + \frac{\lambda_e}{\lambda_a}4^{\frac{\upsilon}{m+3}}}\right)^n \exp\left(-\pi\lambda_e\left(4^{\frac{\upsilon}{m+3}} - 1\right)L^2\right), \quad (13)$$

where $\upsilon \geq 0$.

Proof: The distance distribution of the legitimate user to the n-th nearest AP is given by [31]:

$$f_{x_n}(x_n) = \frac{2(\pi\lambda_a x_n^2)^n}{x_n\Gamma(n)}\exp\left(-\pi\lambda_a x_n^2\right). \quad (14)$$

By using (14) and following similar steps as in (12), (13) can be obtained. ■

The secrecy outage probability, denoted by p_{so}, is defined as the probability that the secrecy rate is below a target secrecy rate $\bar{R}_s$. Mathematically, it is formulated as:

$$p_{so} = \mathbb{P}\left[R_s \leq \bar{R}_s\right] = F_{R_s}(\bar{R}_s), \quad (15)$$

which can be obtained directly from Theorem 1.

Corollary 2: When the legitimate user is served by the nearest AP in its vicinity, the secrecy outage probability is lower bounded by:

$$p_{so}^{LB} = 1 - \exp\left(-\pi\lambda_e\left(4^{\frac{\bar{R}_s}{m+3}} - 1\right)L^2\right), \quad (16)$$

when the density of VLC APs approaches infinity.

Proof: (16) can be obtained from $p_{so}^{LB} = \lim_{\lambda_a\to\infty} p_{so}$. ■

Theorem 1 and Corollary 2 provide an important guideline for the design of VLC networks: installing more VLC APs can help decrease the secrecy outage probability of a typical legitimate user; however, when the density of APs reaches a certain level, further increasing the density of APs is not meaningful since it can no longer enhance the secrecy performance. In other words, it is impossible for a legitimate user in the network to simultaneously achieve a target secrecy rate $\bar{R}_s$ and have an outage probability lower than $p_{so}^{LB}(\bar{R}_s)$. Given a target secrecy rate $\bar{R}_s$ and a target outage probability $\bar{p}_{so} > p_{so}^{LB}(\bar{R}_s)$, this requirement can be achieved by installing more APs in the network so that the density of APs satisfies $\lambda_a \geq \lambda_e(1 - \bar{p}_{so})4^{\bar{R}_s/(m+3)} \big/ \left(\bar{p}_{so} - p_{so}^{LB}(\bar{R}_s)\right)$. From (9) and (16), it is shown that reducing the semi-angle of the LED, or equivalently increasing the Lambertian order, can also help improve the secrecy performance of the network. Nevertheless, the actual choice of the semi-angle of the LED should also satisfy the illumination requirement.

Theorem 2: When the legitimate user is served by the nearest AP in its vicinity, the ergodic secrecy rate at the legitimate user is:

$$\begin{aligned} \mathbb{E}[R_s] = \frac{m+3}{\ln(4)}\Big[&\exp\left(\pi(\lambda_e + \lambda_a)L^2\right)\mathrm{Ei}\left(-\pi(\lambda_e + \lambda_a)L^2\right) \\ &- \exp\left(\pi\lambda_e L^2\right)\mathrm{Ei}\left(-\pi\lambda_e L^2\right)\Big], \end{aligned} \quad (17)$$

where $\mathrm{Ei}(a) = -\int_{-a}^{\infty}\exp(-t)/t\,\mathrm{d}t$ is the exponential integral function [33].

Proof: The ergodic secrecy rate can be calculated based on the CDF of R_s:

$$\begin{aligned} \mathbb{E}[R_s] &= \int_0^\infty \left(1 - F_{R_s(\upsilon)}\right)\mathrm{d}\upsilon \\ &= \frac{m+3}{\ln(4)}\int_1^\infty \frac{1}{\beta\left(1 + \frac{\lambda_e}{\lambda_a}\beta\right)}\exp\left(-\pi\lambda_e(\beta - 1)L^2\right)\mathrm{d}\beta \\ &= \frac{m+3}{\ln(4)}\Bigg[\int_1^\infty \frac{\exp\left(-\pi\lambda_e(\beta - 1)L^2\right)}{\beta}\mathrm{d}\beta \\ &\quad - \int_1^\infty \frac{\exp\left(-\pi\lambda_e(\beta - 1)L^2\right)}{\beta + \frac{\lambda_a}{\lambda_e}}\mathrm{d}\beta\Bigg], \end{aligned} \quad (18)$$

where the integration variable has been changed from υ to β. After applying [33, eq. 3.351.5], the first integration in (18) can be calculated as:

$$\int_1^\infty \frac{\exp\left(-\pi\lambda_e(\beta - 1)L^2\right)}{\beta}\mathrm{d}\beta = -\exp\left(\pi\lambda_e L^2\right)\mathrm{Ei}\left(-\pi\lambda_e L^2\right). \quad (19)$$

After applying [33, eq. 3.352.2], the second integration in (18) can be calculated as:

$$\begin{aligned} &\int_1^\infty \frac{\exp\left(-\pi\lambda_e(\beta - 1)L^2\right)}{\beta + \frac{\lambda_a}{\lambda_e}}\mathrm{d}\beta \\ &\quad = -\exp\left(\pi(\lambda_e + \lambda_a)L^2\right)\mathrm{Ei}\left(-\pi(\lambda_e + \lambda_a)L^2\right). \end{aligned} \quad (20)$$

After plugging (19) and (20) into (18), (17) is obtained. ■

IEEE Proof

Corollary 3: When the legitimate user is served by the nearest AP in its vicinity, the ergodic secrecy rate at the legitimate user is upper bounded by:

$$R_{\mathrm{s}}^{\mathrm{UB}} = \frac{m+3}{\ln(4)} \left(-\exp\left(\pi\lambda_{\mathrm{e}} L^2\right) \mathrm{Ei}\left(-\pi\lambda_{\mathrm{e}} L^2\right)\right). \tag{21}$$

Proof: The upper bound on the secrecy rate can be obtained from $R_{\mathrm{s}}^{\mathrm{UB}} = \lim_{\lambda_{\mathrm{a}}\to\infty} \mathbb{E}[R_{\mathrm{s}}]$. Based on the equality

$$\lim_{\lambda_{\mathrm{a}}\to\infty} \exp\left(\pi(\lambda_{\mathrm{e}}+\lambda_{\mathrm{a}})L^2\right) \mathrm{Ei}\left(-\pi(\lambda_{\mathrm{e}}+\lambda_{\mathrm{a}})L^2\right) = 0, \tag{22}$$

we obtain (21). ■

Theorem 2 and Corollary 3 indicate that increasing the density of VLC APs can help enhance the ergodic secrecy rate of a typical legitimate user. However, when the density of APs exceeds a certain level, installing more APs can not enhance the ergodic secrecy rate any further. While satisfying the illumination requirement, using LEDs with a smaller semi-angle can increase the ergodic secrecy rate of a typical user. Specifically, it can be seen from (17) and (21) that a linear relationship exists between the ergodic secrecy rate and the Lambertian order m. Given the choice of LEDs, the maximum ergodic secrecy rate can not exceed the upper bound given in (21). To achieve a target ergodic secrecy rate $\bar{R}_{\mathrm{s}}$, whose value is smaller than $R_{\mathrm{s}}^{\mathrm{UB}}$, the density of APs needs to exceed λ_{a}^*, where λ_{a}^* is the numerical solution for λ_{a} to equation $\exp\left(\pi\ (\lambda_{\mathrm{e}}+\lambda_{\mathrm{a}})L^2\right) \mathrm{Ei}\left(-\pi\ (\lambda_{\mathrm{e}}+\lambda_{\mathrm{a}})L^2\right) = \ln(4)\bar{R}_{\mathrm{s}}/(m+3) + \exp\left(\pi\lambda_{\mathrm{e}}L^2\right)\mathrm{Ei}\left(-\pi\lambda_{\mathrm{e}}L^2\right)$.

B. Optimal AP to Serve the Legitimate User

Due to the randomness of eavesdroppers, it is not always optimal to serve the legitimate user with the nearest AP. For example, if the eavesdropper is close to the nearest AP around the legitimate user but far away from the second nearest AP around the legitimate user, selecting the second nearest AP to serve the legitimate user may yield a higher secrecy rate. Therefore, with the cooperation among APs, the secrecy performance at legitimate users can be further enhanced. However, it should be noted that selecting the optimal AP to serve legitimate users requires the knowledge of the location information of all eavesdroppers at the central controller, which can be achieved with indoor sensing and localization technologies. Despite the additional implementation and computation complexity, this optimal scheme yields an enhanced secrecy rate, which is useful for network designers to quantify the secrecy performance provided by the nearest AP and optimal AP and to decide which scheme is more suitable for practical implementations. When the optimal AP is selected to serve the legitimate user, the secrecy rate is formulated as:

$$R_{\mathrm{s}} = \left[\max_{x\in\Phi_{\mathrm{a}}} \left\{\frac{1}{2}\log_2\left(\frac{P_{\mathrm{rx}}^2(x,o)}{P_{\mathrm{rx}}^2(x,e^*(x))}\right)\right\}\right]^+. \tag{23}$$

Due to the intractability of the secrecy rate expression given in (23), the distribution function of R_{s} is hard to obtain. In the following, we provide two analytical bounds on the CDF of the secrecy rate.

Corollary 4: With the cooperation among VLC APs, the CDF of the secrecy rate at the typical legitimate user is lower bounded by:

$$F_{R_{\mathrm{s}}}(\upsilon) \ge \exp\left(-\frac{\lambda_{\mathrm{a}}}{\lambda_{\mathrm{e}}} 4^{-\frac{\upsilon}{m+3}} \exp\left(-\pi\lambda_{\mathrm{e}}\left(4^{\frac{\upsilon}{m+3}}-1\right)L^2\right)\right), \tag{24}$$

and is upper bounded by:

$$F_{R_{\mathrm{s}}}(\upsilon) \le 1 - \frac{1}{1+\frac{\lambda_{\mathrm{e}}}{\lambda_{\mathrm{a}}}4^{\frac{\upsilon}{m+3}}} \exp\left(-\pi\lambda_{\mathrm{e}}\left(4^{\frac{\upsilon}{m+3}}-1\right)L^2\right). \tag{25}$$

Proof: With the cooperation of VLC APs, the CDF of the secrecy rate can be calculated with the help of the probability generating functional (PGFL) of the PPP [23]:

$$\begin{aligned}
&F_{R_{\mathrm{s}}}(\upsilon) \\
&= \mathbb{P}\left[\max_{x\in\Phi_{\mathrm{a}}}\left\{\frac{1}{2}\log_2\left(\frac{P_{\mathrm{rx}}^2(x,o)}{P_{\mathrm{rx}}^2(x,e^*(x))}\right)\right\} \le \upsilon\right] \\
&= \mathbb{P}\left[\frac{1}{2}\log_2\left(\frac{P_{\mathrm{rx}}^2(x,o)}{P_{\mathrm{rx}}^2(x,e^*(x))}\right) \le \upsilon, \forall x\in\Phi_{\mathrm{a}}\right] \\
&= \mathbb{E}_{\Phi_{\mathrm{e}}}\left[\mathbb{E}_{\Phi_{\mathrm{a}}}\left[\prod_{x\in\Phi_{\mathrm{a}}} \mathbf{1}\left(\|e-x\| \le \sqrt{\beta l^2+(\beta-1)L^2}\right)\right]\right] \\
&= \mathbb{E}_{\Phi_{\mathrm{e}}}\left[\exp\left[-\lambda_{\mathrm{a}}\int_{\mathbb{R}^2} \mathbf{1}\left[\|e-x\| > \sqrt{\beta l^2+(\beta-1)L^2}\,\middle|\, x\right]\mathrm{d}x\right]\right],
\end{aligned} \tag{26}$$

where $\mathbf{1}(\mathcal{A}) = 1$ with event $\mathcal{A}$ being true, and zero otherwise. Based on Jensen's inequality, the lower bound can be calculated as:

$$F_{R_{\mathrm{s}}}(\upsilon) \ge \exp\left[-2\pi\lambda_{\mathrm{a}}\int_0^\infty \mathbb{P}\left[\|e-x\| > \sqrt{\beta x^2+(\beta-1)L^2}\,\middle|\, x\right] \times x\,\mathrm{d}x_0\right]. \tag{27}$$

After calculating the integration part in (27), the lower bound result in Corollary 4 is obtained. The upper bound can be obtained straightforwardly from the following inequality:

$$\left[\max_{x\in\Phi_{\mathrm{a}}}\left\{\log_2\left(\frac{P_{\mathrm{rx}}^2(x,o)}{P_{\mathrm{rx}}^2(x,e^*(x))}\right)\right\}\right]^+ \ge \left[\log_2\left(\frac{P_{\mathrm{rx}}^2(x_0,o)}{P_{\mathrm{rx}}^2(x_0,e^*(x_0))}\right)\right]^+. \tag{28}$$

In other words, choosing the nearest AP to serve the legitimate user is sub-optimal, which gives an upper bound on the CDF of the secrecy capacity. Therefore, the upper bound expression shown in (25) can be obtained directly from Theorem 1. ■

Based on the upper bound on the CDF of the secrecy rate, a lower bound on the ergodic secrecy rate can be obtained, as given in (17). An upper bound on the ergodic secrecy rate can be obtained by integrating the complement of the CDF of R_{s}:

$$\begin{aligned}
&\mathbb{E}[R_{\mathrm{s}}] \\
&= \int_0^\infty \left(1-F_{R_{\mathrm{s}}(\upsilon)}\right)\mathrm{d}\upsilon \\
&\le \frac{m+3}{\ln(4)}\int_1^\infty \left(1-\exp\left(-\frac{\lambda_{\mathrm{a}}}{\lambda_{\mathrm{e}}\beta}\exp\left(-\pi\lambda_{\mathrm{e}}(\beta-1)L^2\right)\right)\right)\frac{1}{\beta}\mathrm{d}\beta.
\end{aligned} \tag{29}$$

IEEE Proof

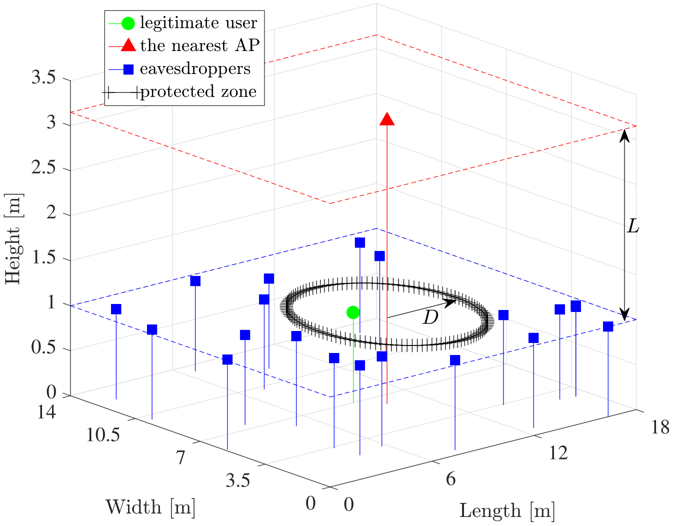

Fig. 2. Random network model with a secrecy protected zone. In this model, each VLC AP has a disk-shaped protected zone, which is centered around the AP and has a radius of D on the user plane. For simplicity, only the protected zone around the nearest AP is drawn.

Because of the nested exponential function in (29), a closed-form expression is not available. However, (29) can be efficiently calculated using numerical methods.

IV. Enhancing Secrecy Rate in VLC Networks With a Protected Zone

In order to further enhance the secrecy performance of legitimate users in VLC networks, a strategy named the "protected zone" [34] can be implemented. As depicted in Fig. 2, a protected zone is an eavesdropper-free area (on the user plane), which allows only legitimate users to enter. If any eavesdropper enters the protected zone, such behavior will be made aware to the AP, and the AP will notify the legitimate user and temporarily stop the communication. A practical implementation of the protected zone in VLC networks can be achieved with motion sensors that are already built in modern energy-efficient lighting devices. We acknowledge that there might be means to break the suggested enforcement of the protected zone. However, a deeper investigation of this aspect is outside the scope of this work. A secrecy protected zone can be completely described by its center, i.e., its associated AP, and a security radius D. The security radius is defined as the smallest horizontal distance between the AP and any eavesdroppers that are undetectable.

Lemma 1: Given that the horizontal distance between the nearest AP to the legitimate user is x_0, the PDF of the horizontal distance between this AP and the nearest eavesdropper, that is outside the protected zone, is:

$$f_{\|e^*(x_0)-x_0\|}(\alpha) = 2\pi\lambda_e\alpha\exp\left(-\pi\lambda_e(\alpha^2 - D^2)\right), \quad (30)$$

for $\alpha \geq D$, and zero otherwise.

Proof: (30) can be obtained using the void probability of PPP [32]. ■

With Lemma 1, we are ready to obtain the CDF of the secrecy rate enhanced by the protected zone.

Corollary 5: When the legitimate user is served by the nearest AP in its vicinity, which has a protected zone with radius D, the CDF of the enhanced secrecy rate is given by:

$$F_{R_s}(\upsilon) = 1 - \frac{\exp\left(-\pi\lambda_e\left(\left(4^{\frac{\upsilon}{m+3}} - 1\right)L^2 - D^2\right)\right)}{1 + \frac{\lambda_e}{\lambda_a}4^{\frac{\upsilon}{m+3}}}, \quad (31)$$

for $\upsilon \geq \frac{m+3}{2}\log_2\left(D^2/L^2 + 1\right)$, and

$$F_{R_s}(\upsilon) = \frac{\exp\left(-\pi\lambda_a\left(D^2 - \left(4^{\frac{\upsilon}{m+3}} - 1\right)L^2\right)4^{-\frac{\upsilon}{m+3}}\right)}{1 + \frac{\lambda_a}{\lambda_e}4^{-\frac{\upsilon}{m+3}}}, \quad (32)$$

for $0 \leq \upsilon < \frac{m+3}{2}\log_2\left(D^2/L^2 + 1\right)$.

Proof: Since the protected zone has a radius D, the minimum distance between the nearest eavesdropper and the AP is D. Therefore,

$$e^*(x_0) = \arg\min_{e\in\Phi_e, e\notin\mathcal{B}(x_0,D)} \|e - x_0\|, \quad (33)$$

where $\mathcal{B}(x_0, D)$ denotes the disk-shaped area centered at x_0 with radius D. Due to the exclusive region in (33), the derivation of the CDF of the enhanced secrecy rate needs to be separated into two scenarios. First, when $\sqrt{(\beta-1)L^2} \geq D$, i.e., $\upsilon \geq \frac{m+3}{2}\log_2\left(D^2/L^2+1\right)$, the CDF of the enhanced secrecy rate can be calculated as:

$$F_{R_s}(\upsilon) = \int_0^\infty\left(1 - \exp\left(-\pi\lambda_e\left(\beta x_0^2 + (\beta-1)L^2 - D^2\right)\right)\right) \times 2\pi\lambda_a x_0\exp\left(-\pi\lambda_a x_0^2\right)\mathrm{d}x_0, \quad (34)$$

which gives the result in (31). Second, when $\sqrt{(\beta-1)L^2} < D$, i.e., $0 \leq \upsilon < \frac{m+3}{2}\log_2\left(D^2/L^2+1\right)$, the CDF of the enhanced secrecy rate can be calculated as:

$$\begin{aligned}F_{R_s}(\upsilon) = &\int_{\sqrt{\frac{D^2-(\beta-1)L^2}{\beta}}}^\infty 2\pi\lambda_a x_0\exp\left(-\pi\lambda_a x_0^2\right)\\ &\times\left(1 - \exp\left(-\pi\lambda_e\left(\beta x_0^2 + (\beta-1)L^2 - D^2\right)\right)\right)\mathrm{d}x_0\\ &+\int_0^{\sqrt{\frac{D^2-(\beta-1)L^2}{\beta}}} 2\pi\lambda_a x_0\exp\left(-\pi\lambda_a x_0^2\right)\\ &\times\mathbb{P}\left[e^*(x_0)\in\mathcal{B}(x_0,D)\right]\mathrm{d}x_0, \quad (35)\end{aligned}$$

in which the critical point $x_0 = \sqrt{(D^2-(\beta-1)L^2)/\beta}$ is found by solving $\sqrt{\beta x_0^2 + (\beta-1)L^2} = D$. Since $e^*(x_0) \notin \mathcal{B}(x_0, D)$, $\mathbb{P}\left[e^*(x_0)\in\mathcal{B}(x_0,D)\right] = 0$, and the second integration in (35) reduces to zero. After calculating the first integration in (35), we obtain (32). To this end, the proof is completed. ■

It can be seen from Corollary 5 that the radius of the protected zone has a strong impact on the CDF of the secrecy rate and on the secrecy outage probability. On the one hand, if the radius of the protected zone is small enough so that the target secrecy rate satisfies $\bar{R}_s \geq \frac{m+3}{2}\log_2\left(D^2/L^2+1\right)$, given a fixed density of eavesdroppers, the secrecy outage probability is lower bounded by:

$$p_{so}^{LB} = 1 - \exp\left(-\pi\lambda_e\left(\left(4^{\frac{\bar{R}_s}{m+3}} - 1\right)L^2 - D^2\right)\right), \quad (36)$$

IEEE Proof

which is obtained when the density of the APs goes to infinity. On the other hand, if the radius of the protected zone is large enough so that the target secrecy rate satisfies $\bar{R}_\mathrm{s} < \frac{m+3}{2}\log_2\left(D^2/L^2+1\right)$, increasing the density of VLC APs can efficiently reduce the secrecy outage probability, and the worst-case scenario of the secrecy outage probability is upper bounded by:

$$p_\mathrm{so}^\mathrm{UB} = \exp\left(-\pi\,\lambda_\mathrm{a}\left(D^2-\left(4^{\frac{\bar{R}_\mathrm{s}}{m+3}}-1\right)L^2\right)4^{-\frac{\bar{R}_\mathrm{s}}{m+3}}\right), \quad (37)$$

which is obtained by letting λ_e approach infinity.

Corollary 5 provides an essential guideline to network designers so that they can design a suitable protected zone around each VLC AP in order to provide legitimate users with guaranteed secrecy service. Specifically, for legitimate users to achieve a target secrecy rate $\bar{R}_\mathrm{s}$ with a target secrecy outage probability $\bar{p}_\mathrm{so}$, network designers can set up the protected zone with radius no smaller than D^*, where $D^* = ((4^{\bar{R}_\mathrm{s}/(m+3)}-1)L^2 + (\ln(1-\bar{p}_\mathrm{so}) + \ln(1+4^{\bar{R}_\mathrm{s}/(m+3)}\lambda_\mathrm{e}/\lambda_\mathrm{a}))/\pi\,\lambda_\mathrm{e})^{1/2}$ for $\bar{p}_\mathrm{so} \geq 1-(1+4^{\bar{R}_\mathrm{s}/(m+3)}\lambda_\mathrm{e}/\lambda_\mathrm{a})^{-1}$, and $D^* = ((4^{\bar{R}_\mathrm{s}/(m+3)}-1)L^2 - (\ln\bar{p}_\mathrm{so} + \ln(1+4^{-\bar{R}_\mathrm{s}/(m+3)}\lambda_\mathrm{a}/\lambda_\mathrm{e}))4^{\bar{R}_\mathrm{s}/(m+3)}/\pi\,\lambda_\mathrm{a})^{1/2}$ for $\bar{p}_\mathrm{so} < 1-(1+4^{\bar{R}_\mathrm{s}/(m+3)}\lambda_\mathrm{e}/\lambda_\mathrm{a})^{-1}$. Also, it is evident that a more stringent secrecy requirement with a larger $\bar{R}_\mathrm{s}$ and/or a smaller $\bar{p}_\mathrm{so}$ requires the implementation of a larger secrecy protected zone.

Theorem 3: When the legitimate user is served by the nearest AP in its vicinity, which has a protected zone with radius D, the enhanced ergodic secrecy rate at the typical legitimate user is:

$$\begin{aligned}
&\mathbb{E}[R_\mathrm{s}]\\
&= \frac{m+3}{\ln(4)}\Bigg[-\exp\left(\pi\,\lambda_\mathrm{e}\left(L^2+D^2\right)\right)\mathrm{Ei}\left(-\pi\,\lambda_\mathrm{e}\left(L^2+D^2\right)\right)\\
&\quad+\ln\left(\frac{D^2}{L^2}+1\right)\Bigg] + \frac{m+3}{\ln(4)}\exp\left(\pi\,\lambda_\mathrm{a}L^2\right)\Bigg[\mathrm{Ei}\left(-\pi\,\lambda_\mathrm{a}L^2\right)\\
&\quad+\exp\left(\pi\,\lambda_\mathrm{e}\left(L^2+D^2\right)\right)\mathrm{Ei}\left(-\pi\left(\lambda_\mathrm{a}+\lambda_\mathrm{e}\right)\left(L^2+D^2\right)\right)\\
&\quad-\mathrm{Ei}\left(-\pi\,\lambda_\mathrm{a}\left(L^2+D^2\right)\right)\Bigg]. \qquad (38)
\end{aligned}$$

Proof: Based on Corollary 5, the enhanced ergodic rate can be calculated by integrating the complement of the CDF. Since the CDF has different expressions at different regions, the integration should be separated into two parts:

$$\begin{aligned}
&\mathbb{E}[R_\mathrm{s}]\\
&= \frac{m+3}{\ln(4)}\int_1^{\frac{D^2}{L^2}+1}\left(1-\frac{\exp\left(\frac{-\pi\,\lambda_\mathrm{a}\left(D^2-(\beta-1)L^2\right)}{\beta}\right)}{1+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}\frac{1}{\beta}}\right)\frac{1}{\beta}\mathrm{d}\beta\\
&\quad+\frac{m+3}{\ln(4)}\int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\,\lambda_\mathrm{e}\left((\beta-1)\,L^2-D^2\right)\right)}{\beta+\frac{\lambda_\mathrm{e}}{\lambda_\mathrm{a}}\beta^2}\mathrm{d}\beta, \qquad (39)
\end{aligned}$$

where for simplicity the variable of integration has been changed from υ to β. The first integration in (39) can be simplified to:

$$\begin{aligned}
&\int_1^{\frac{D^2}{L^2}+1}\left(1-\frac{\exp\left(\frac{-\pi\,\lambda_\mathrm{a}\left(D^2-(\beta-1)L^2\right)}{\beta}\right)}{1+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}\frac{1}{\beta}}\right)\frac{1}{\beta}\mathrm{d}\beta\\
&\qquad= \ln\left(\frac{D^2}{L^2}+1\right)+\exp\left(\pi\,\lambda_\mathrm{a}L^2\right)\\
&\qquad\quad\times\int_1^{\frac{D^2}{L^2}+1}\frac{\exp\left(-\frac{\pi\,\lambda_\mathrm{a}\left(L^2+D^2\right)}{\beta}\right)}{\beta+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}}\mathrm{d}\beta, \qquad (40)
\end{aligned}$$

in which the integration part can be obtained as:

$$\begin{aligned}
&\int_1^{\frac{D^2}{L^2}+1}\frac{\exp\left(-\frac{\pi\,\lambda_\mathrm{a}\left(L^2+D^2\right)}{\beta}\right)}{\beta+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}}\mathrm{d}\beta\\
&= \mathrm{Ei}\left(-\pi\,\lambda_\mathrm{a}L^2\right)-\mathrm{Ei}\left(-\pi\,\lambda_\mathrm{a}\left(L^2+D^2\right)\right)\\
&\quad+\exp\left(\pi\,\lambda_\mathrm{e}\left(L^2+D^2\right)\right)\mathrm{Ei}\left(-\pi\left(\lambda_\mathrm{a}+\lambda_\mathrm{e}\right)\left(L^2+D^2\right)\right)\\
&\quad-\exp\left(\pi\,\lambda_\mathrm{e}\left(L^2+D^2\right)\right)\mathrm{Ei}\left(-\pi\,\lambda_\mathrm{a}L^2-\pi\,\lambda_\mathrm{e}\left(L^2+D^2\right)\right). \qquad (41)
\end{aligned}$$

Similarly, the second integration in (39) can be simplified to:

$$\begin{aligned}
&\int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\,\lambda_\mathrm{e}\left((\beta-1)\,L^2-D^2\right)\right)}{\beta+\frac{\lambda_\mathrm{e}}{\lambda_\mathrm{a}}\beta^2}\mathrm{d}\beta\\
&\quad= \exp\left(\pi\,\lambda_\mathrm{e}\left(L^2+D^2\right)\right)\Bigg[\int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\,\lambda_\mathrm{e}\beta L^2\right)}{\beta}\mathrm{d}\beta\\
&\qquad-\int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\,\lambda_\mathrm{e}\beta L^2\right)}{\beta+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}}\mathrm{d}\beta\Bigg]. \qquad (42)
\end{aligned}$$

Applying [33, eq. 3.352.2], the two integrations in (42) can be calculated as:

$$\int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\,\lambda_\mathrm{e}\beta L^2\right)}{\beta}\mathrm{d}\beta = -\mathrm{Ei}\left(-\pi\,\lambda_\mathrm{e}\left(L^2+D^2\right)\right), \quad (43)$$

and

$$\begin{aligned}
&\int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\,\lambda_\mathrm{e}\beta L^2\right)}{\beta+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}}\mathrm{d}\beta\\
&\quad= -\exp\left(\pi\,\lambda_\mathrm{a}L^2\right)\mathrm{Ei}\left(-\pi\,\lambda_\mathrm{e}L^2\left(\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}+\frac{D^2}{L^2}+1\right)\right). \qquad (44)
\end{aligned}$$

Combining (40) – (44) gives the result shown in (38), which completes the proof. ■

Note that the expression for the ergodic secrecy rate in Theorem 3 can be simplified to the one given in Theorem 2 when $D = 0$. Also, it is shown in Theorem 3 that the ergodic secrecy rate scales linearly with the Lambertian order m, regardless of the size of the protected zone. Given the choice of LEDs, the density of APs and the density of eavesdroppers, a target ergodic secrecy capacity $\bar{R}_\mathrm{s}$ can be achieved through the implementation of a protected zone with radius D^*, where

IEEE Proof

TABLE I
SIMULATION PARAMETERS

Parameter	value
Room dimensions	$18 \times 14 \times 3.5$ m^3
Height of VLC APs	3.15 m
Height of mobile users	1 m
Semi-angle of VLC APs, $\Phi_{1/2}$	30°
Transmit optical power of VLC APs, $P_{\rm tx}$	1 W
Receiver detection area, A	1 cm^2
Receiver responsivity, η	0.4 A/W
Reflective index of the optical concentrator, n	1.5
Optical filter gain, T	1
Receiver FOV, $\Psi_{\rm fov}$	90°
Receiver noise power, $\sigma^2_{\rm nb} = \sigma^2_{\rm ne}$	−103.98 dBm

D^* is the numerical solution for D by letting (38) equal $\bar{R}_{\rm s}$. Since the expression in (38) monotonically increases with respect to D, the numerical solution for D^* is unique.

V. SIMULATION RESULTS AND DISCUSSIONS

A. Results Based on the PPP Model

In this section, we use a MATLAB implementation to validate the derived results. Simulation results are obtained by averaging 20, 000 realizations of Monte Carlo simulations. A typical office of size $18 \times 14 \times 3.5$ m^3 is considered, as illustrated in Figs. 1 and 2. If not otherwise specified, the network parameters used for the simulation setup are described in Table I.

First, we consider the scenario where the legitimate user is served by the nearest AP in its vicinity, without the implementation of the secrecy protected zone. Therefore, malicious eavesdroppers can be horizontally as close as possible to the AP that serves the legitimate user. By fixing the density of eavesdroppers ($\lambda_{\rm e} = 0.2$), the secrecy outage probability at the typical legitimate user is evaluated at different values of the AP density, as shown in Fig. 3. It can be seen that, when $\lambda_{\rm a}$ is small, increasing the density of VLC APs can efficiently reduce the secrecy outage probability at the legitimate user. However, when $\lambda_{\rm a}$ is large, further increasing the density of VLC APs only slightly reduces the secrecy outage probability. For example, given that the target secrecy rate is $\bar{R}_{\rm s} = 1$ bit/s/Hz, increasing $\lambda_{\rm a}$ from 0.1 to 1 can cause the secrecy outage probability to drop by 0.3. In comparison, when $\lambda_{\rm a}$ is increased from 1 to 10, the secrecy outage probability only drops by 0.1. Also, it is shown that a lower bound on the secrecy outage probability exists even if the density of VLC APs approaches infinity. This result is in agreement with Corollary 2. In Fig. 4, the ergodic secrecy rate is plotted against the density of APs. It is shown that the ergodic secrecy rate at the legitimate user drops when the density of eavesdroppers increases. Given a fixed density of eavesdroppers, increasing the density of VLC APs can efficiently enhance the ergodic secrecy rate when $\lambda_{\rm a}$ is small. However, the ergodic secrecy rate of the legitimate user tends to saturate at high AP densities. As a result, increasing the density of VLC APs when $\lambda_{\rm a}$ is large does not bring a significant incrementation to the ergodic secrecy rate. Instead, increasing the density of APs when $\lambda_{\rm a}$ is small is more meaningful.

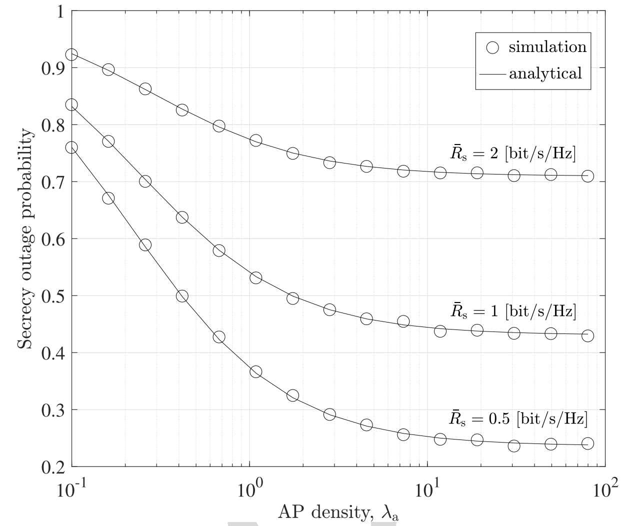

Fig. 3. Secrecy outage probability versus VLC AP density. The legitimate user is served by the nearest AP in its vicinity. $\lambda_{\rm e} = 0.2$.

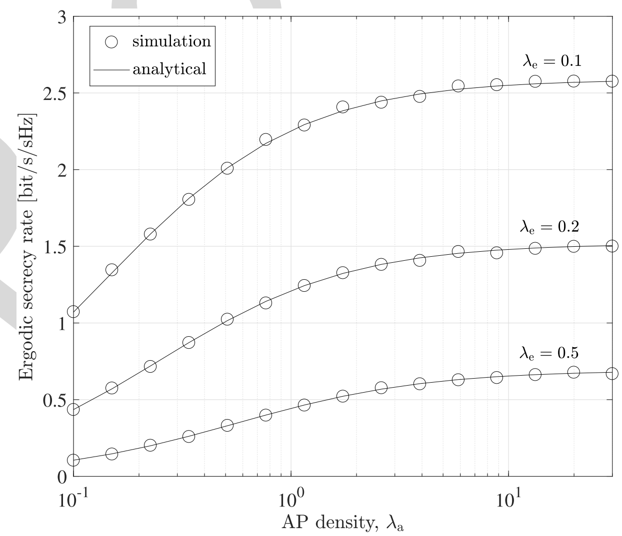

Fig. 4. Ergodic secrecy rate versus VLC AP density. The legitimate user is served by the nearest AP in its vicinity.

Second, we consider the scenario where the legitimate user is served by the optimal AP when APs are cooperated in the network. For the typical legitimate user, the optimal AP is not necessarily the nearest one, depending on the locations of potential eavesdroppers. With the cooperation among VLC APs, the optimal AP that brings the highest secrecy rate to the legitimate user is selected. For Monte Carlo simulations, the optimal AP is found out through the exhaustive search method. In Fig. 5, the secrecy outage probability is plotted against different eavesdropper densities, and it can be seen that the simulation results are well bounded by the derived analytical results. On the one hand, by assuming that the optimal AP is the nearest one, we underestimate the secrecy rate at the legitimate user. As a result, this assumption leads to an upper bound on the secrecy outage probability. On the other hand, the lower bound on the secrecy outage probability is

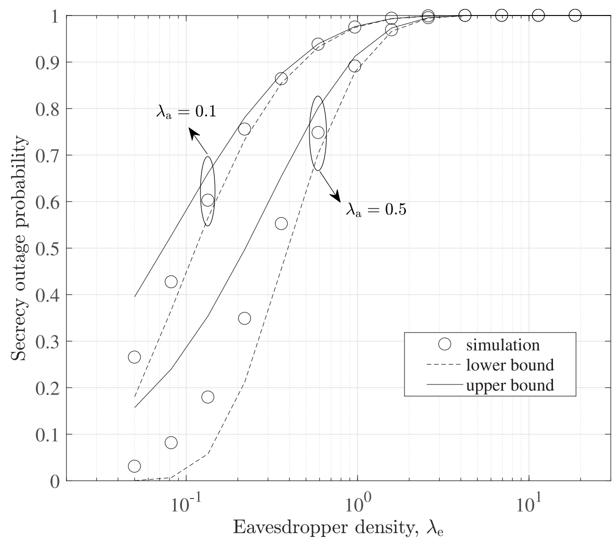

Fig. 5. Secrecy outage probability versus eavesdropper density. The legitimate user is served by the optimal AP. $\bar{R}_s = 0.5$ bit/s/Hz.

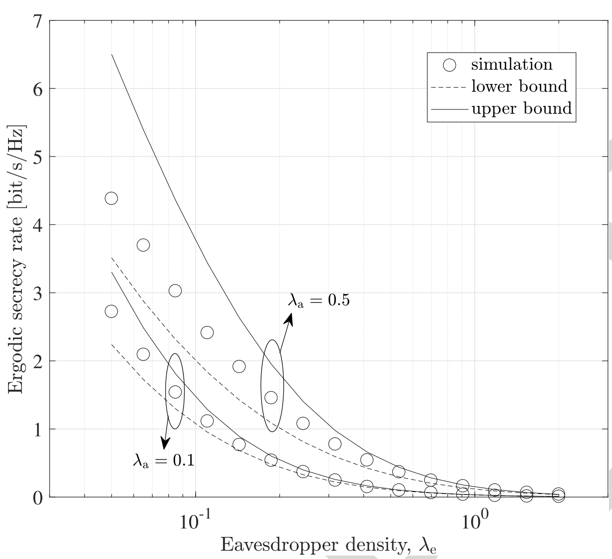

Fig. 6. Ergodic secrecy rate versus eavesdropper density. The legitimate user is served by the optimal AP.

obtained from Jensen's inequality, as described in Corollary 4. Comparing the lower bound with the upper bound, it can be seen that the lower bound is closer to the simulation results. It is also shown in Fig. 5 that both theoretical bounds on the secrecy outage probability are reasonably tight when the eavesdropper density is large. In Fig. 6, the ergodic secrecy rate at the legitimate user is computed for different values of the eavesdropper density. It should be noted that assuming the optimal AP is the nearest one gives the lower bound on the ergodic secrecy rate in Fig. 6, which corresponds to the upper bound on the secrecy outage probability in Fig. 5. Again, both analytical bounds become tighter as the eavesdropper density increases. Based on the results shown in Fig. 5 and Fig. 6, we can conclude that the optimal AP that maximizes the secrecy performance at the legitimate user is not necessarily the nearest one. To investigate deeper, we show in Fig. 7

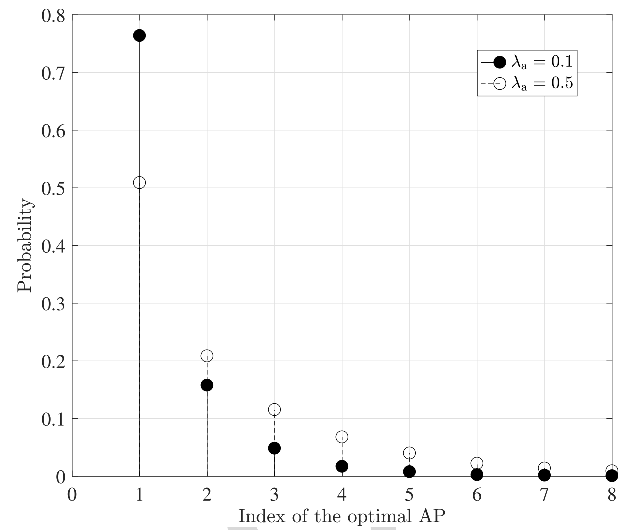

Fig. 7. Probability mass function (PMF) of the index of the optimal AP. $\lambda_e = 0.2$.

the probability mass function (PMF) of the index of the optimal AP that maximizes the secrecy rate at the legitimate user. Index i relates to the i-th nearest neighboring AP to the legitimate user. For example, index 1 corresponds to the nearest AP, index 2 corresponds to the second nearest AP, and so on. It is shown in Fig. 7 that, compared to other neighboring APs, the nearest AP is most likely the optimal one. However, it is also possible that the optimal AP is the second nearest, third nearest, etc. Fig. 7 also shows that with a smaller value of λ_a, it is more likely that the nearest AP is the optimal one, which therefore explains why the analytical bounds are tighter for smaller values of λ_a, as observed in Fig. 5 and Fig. 6.

Third, we consider the scenario where the legitimate user is served by the nearest AP in its vicinity, with the implementation of a secrecy protected zone. It is assumed that any malicious eavesdroppers that are inside the protected zone can be detected by the AP so that these eavesdroppers do not cause any secrecy information loss at the legitimate user. As a result, the secrecy information loss at the legitimate user is caused by the eavesdroppers that are outside the protected zone only. In Fig. 8, the secrecy outage probability is plotted against the density of VLC APs. It is shown that, for a given target secrecy rate, the secrecy outage probability decreases as the AP density increases. However, when λ_a is large, further increasing the density of VLC APs only slightly reduces the secrecy outage probability. Also, it is shown that there exists a lower bound on the secrecy outage probability when λ_a approaches infinity. After implementing a secrecy protected zone with radius D, the secrecy outage probability is reduced significantly. More specifically, when $\lambda_a = 1$, $\lambda_e = 0.2$ and the target secrecy rate is $\bar{R}_s = 2$ bit/s/Hz, implementing a secrecy protected zone with radius $D = 1$ m reduces the secrecy outage probability by 0.2. If the secrecy protected zone has a radius of $D = 2$ m, the secrecy outage probability can be reduced to nearly zero. It is also shown in Fig. 8 that, with a sufficiently large protected area, the secrecy outage probability is no longer bounded at the lower end, i.e., increasing the density of VLC

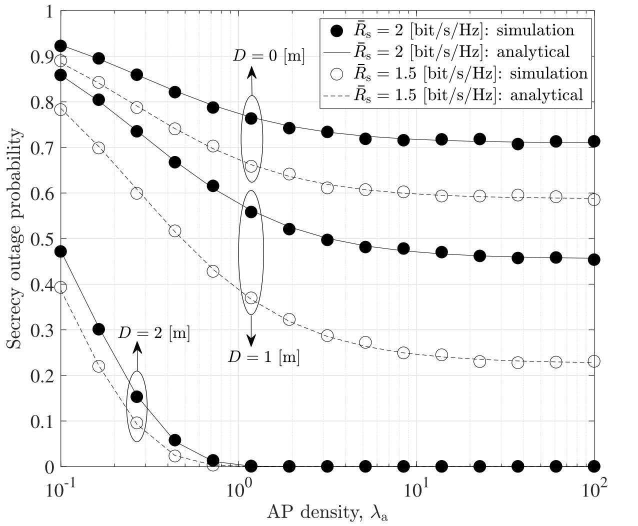

Fig. 8. Secrecy outage probability versus VLC AP density. The legitimate user is served by the nearest AP in its vicinity, and eavesdroppers are outside the protected zone with radius D. $\lambda_e = 0.2$.

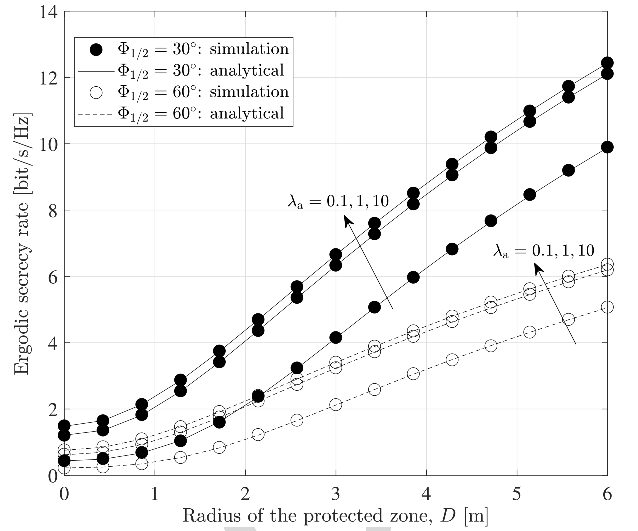

Fig. 10. Ergodic secrecy rate versus the radius of the protected zone. The legitimate user is served by the nearest AP in its vicinity. $\lambda_e = 0.2$.

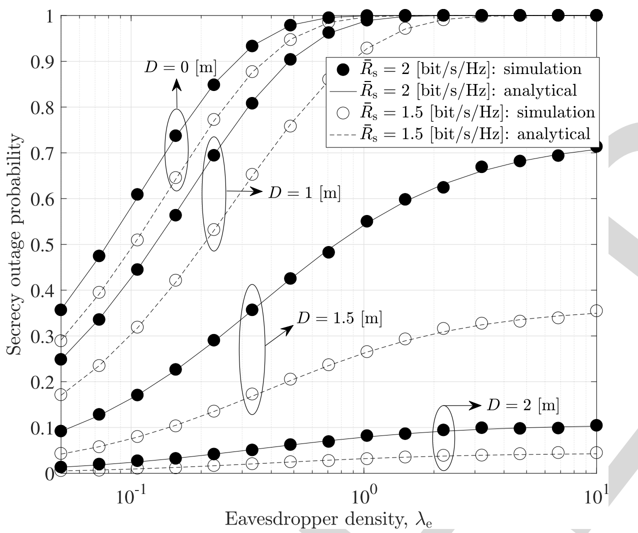

Fig. 9. Secrecy outage probability versus eavesdropper density. The legitimate user is served by the nearest AP in its vicinity, and eavesdroppers are outside the protected zone with radius D. $\lambda_a = 0.5$.

APs can efficiently reduce the secrecy outage probability to zero. In Fig. 9, we fix $\lambda_a = 0.5$ and evaluate the impact of the eavesdropper density on the secrecy outage probability. It can be seen that, without the protected zone, the secrecy outage probability can be as large as one if the eavesdropper density is sufficiently high. However, with the implementation of a protected zone, the worst-case scenario of the secrecy outage probability can be limited below a certain level. For example, when the target secrecy rate is $\bar{R}_s = 2$ bit/s/Hz and the protected zone has a radius of $D = 2$ m, the worst-case secrecy outage probability at the legitimate user does not exceed 0.12, regardless of the eavesdropper density. To further investigate the impact of the protected zone, we show in Fig. 10 the ergodic secrecy rate against the radius of the protected zone while fixing the eavesdropper density to $\lambda_e = 0.2$. The slope of the curve shows that a very small protected area brings only marginal improvement on the secrecy performance. However, by increasing the size of the protected zone further, the secrecy performance at the legitimate user can be enhanced significantly. Specifically, when $\lambda_a = 1$ and $\Phi_{1/2} = 30°$, increasing the radius of the protected zone from 0 to 1 m increases the ergodic secrecy rate by 0.6 bit/s/Hz. In contrast, increasing the radius of the protected zone from 1 to 2 m can increase the ergodic secrecy rate by 1.9 bit/s/Hz. In Fig. 10, it is also shown that using more directional LEDs, i.e., LEDs with a smaller semi-angle, enhances the secrecy performance at the legitimate user. However, the actual choice of LEDs should also take practical illumination requirements into consideration.

B. PPP Model vs. Grid Model

In the following, we compare the secrecy performance between the stochastic PPP model and the deterministic grid model. For the grid model, it implicitly assumes that the number of APs, as well as their locations in the network, are fixed and known. As shown in Fig. 11 and Fig. 12, we use a hexagonal-shaped grid to model the locations of APs within the same indoor space. A total number of 31 APs (represented by red triangles) are considered, and without loss of generality the secrecy performance is studied by focusing on the central hexagonal cell. A legitimate user (represented by the green circle) is randomly distributed within the central cell and is served by the central AP. The eavesdroppers (represented by blue squares) are assumed to follow a Poisson distribution with intensity λ_e. To allow for a fair comparison between the PPP model and the grid model, the density of APs in the PPP model is set to 0.12 so that the expected number of APs in the PPP model equals the total number of APs in the grid model. It can be seen from Fig. 11 that the PPP model and the grid model yield similar results for the secrecy outage probability. Both curves have similar shapes and trends, especially for higher target secrecy rates and with larger eavesdropper densities. In general, the grid model

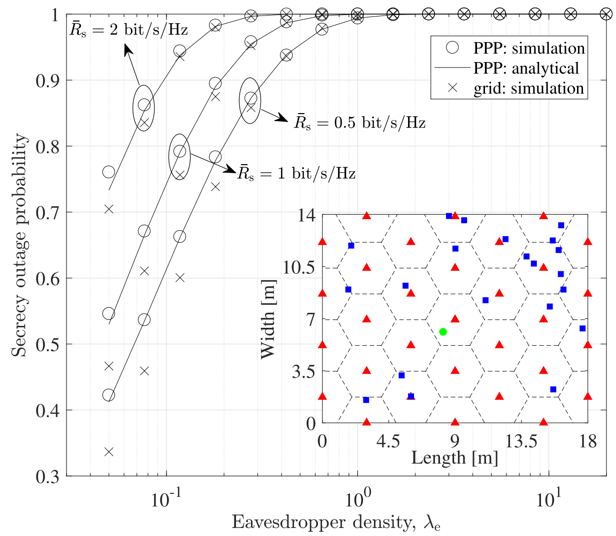

Fig. 11. Secrecy outage probability comparison between the PPP model and the grid model. $\lambda_a = 0.12$.

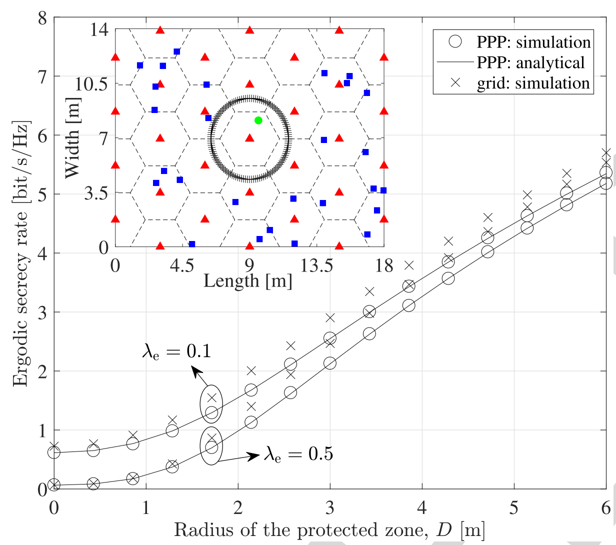

Fig. 12. Ergodic secrecy rate comparison between the PPP model and the grid model. $\lambda_a = 0.12$.

provides slightly superior coverage performance than the PPP model because of its more regularized cell shapes. With the implementation of a secrecy protected zone, we compare in Fig. 12 the achieved ergodic secrecy rate between the PPP model and the grid model. The configuration of the grid model in Fig. 12 is the same as that in Fig. 11, except that the eavesdroppers are prohibited in the circular protected zone centered around the central AP. Results show that both models yield close ergodic secrecy rates, especially for networks with more populated eavesdroppers.

VI. Conclusion

In this work, we studied the performance of physical-layer secrecy in a three-dimensional multiuser VLC network. With the use of mathematical tools from stochastic geometry, analytical expressions for the secrecy outage probability, the ergodic secrecy rate, as well as their lower and upper bounds, are derived in tractable forms and verified through Monte Carlo simulations. Impacts of AP cooperation and the implementation of a secrecy protected zone on the secrecy performance have also been investigated. Results show that cooperating neighboring APs can enhance the secrecy performance of VLC networks, but only to a limited extent. We also show that building a secrecy protected zone around the AP significantly improves the network secrecy performance.

Justifying the application of the PPP model to the performance analysis of VLC networks is an important research direction. Also, improved stochastic models may be developed in the future to more accurately capture the spatial distribution of APs in a real network deployment.

References

[1] 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.

[2] S. Dimitrov and H. Haas, *Principles of LED Light Communications: Towards Networked Li-Fi*. Cambridge, U.K.: Cambridge Univ. Press, 2015.

[3] H. Haas, L. Yin, Y. Wang, and C. Chen, "What is LiFi?" *J. Lightw. Technol.*, vol. 34, no. 6, pp. 1533–1544, Mar. 15, 2016.

[4] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.7: Short-Range Wireless Optical Communication Using Visible Light*, IEEE Computer Society, IEEE Standard 802.15.7-2011, 2011.

[5] X. Li, F. Jin, R. Zhang, J. Wang, Z. Xu, and L. Hanzo, "Users first: User-centric cluster formation for interference-mitigation in visible-light networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 39–53, Jan. 2016.

[6] H. Ma, L. Lampe, and S. Hranilovic, "Coordinated broadcasting for multiuser indoor visible light communication systems," *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3313–3324, Sep. 2015.

[7] L. Yin, W. O. Popoola, X. Wu, and H. Haas, "Performance evaluation of non-orthogonal multiple access in visible light communication," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5162–5175, Dec. 2016.

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

[9] I. Csiszär and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[10] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 539–543.

[11] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[12] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.

[13] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[14] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[15] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, Jun. 2013.

[16] A. Lapidoth, S. M. Moser, and M. A. Wigger, "On the capacity of free-space optical intensity channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4449–4461, Oct. 2009.

[17] J.-B. Wang, Q.-S. Hu, J. Wang, M. Chen, and J.-Y. Wang, "Tight bounds on channel capacity for dimmable visible light communications," *J. Lightw. Technol.*, vol. 31, no. 23, pp. 3771–3779, Dec. 1, 2013.

[18] A. Chaaban, J. M. Morvan, and M. S. Alouini, "Free-space optical communications: Capacity bounds, approximations, and a new sphere-packing perspective," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1176–1191, Mar. 2016.

IEEE Proof

[19] S. Dimitrov and H. Haas, "Information rate of OFDM-based optical wireless communication systems with nonlinear distortion," *J. Lightw. Technol.*, vol. 31, no. 6, pp. 918–929, Mar. 15, 2013.

[20] 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.

[21] 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.

[22] G. Pan, J. Ye, and Z. Ding, "On secure VLC systems with spatially random terminals," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 492–495, Mar. 2016.

[23] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and its Applications*, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.

[24] L. Zeng *et al.*, "High data rate multiple input multiple output (MIMO) optical wireless communications using white LED lighting," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1654–1662, Dec. 2009.

[25] J. Grubor, S. Randel, K. D. Langer, and J. W. Walewski, "Broadband information broadcasting using LED-based interior lighting," *J. Lightw. Technol.*, vol. 26, no. 24, pp. 3883–3892, Dec. 15, 2008.

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

[27] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless," *Proc. IEEE*, vol. 100, pp. 1853–1888, May 2012.

[28] C. Chen, S. Videv, D. Tsonev, and H. Haas, "Fractional frequency reuse in DCO-OFDM-based optical attocell networks," *J. Lightw. Technol.*, vol. 33, no. 19, pp. 3986–4000, Oct. 1, 2015.

[29] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[30] O. Ozel, E. Ekrem, and S. Ulukus, "Gaussian wiretap channel with an amplitude constraint," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Sep. 2012, pp. 139–143.

[31] M. Haenggi, "On distances in uniformly random networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3584–3586, Oct. 2005.

[32] S. Srinivasa and M. Haenggi, "Distance distributions in finite uniformly random networks: Theory and applications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 940–949, Feb. 2010.

[33] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

[34] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2013.

Liang Yin received the B.Eng. degree (Hons.) in electronics and electrical engineering from the University of Edinburgh, Edinburgh, U.K., in 2014, where he is currently pursuing the Ph.D. degree in electrical engineering. His research interests are in visible light communication and positioning, multiuser networking, and wireless network performance analysis. He received the Class Medal Award and IET Prize Award from the University of Edinburgh.

Harald Haas (S'98–AM'00–M'03–SM'17) received the Ph.D. degree from the University of Edinburgh in 2001. He currently holds the Chair of mobile communications with the University of Edinburgh, and is the Initiator, Co-Founder, and the Chief Scientific Officer of pureLiFi Ltd and the Director of the LiFi Research and Development Center, University of Edinburgh. He has authored 400 conference and journal papers including a paper in Science and co-authored a book entitled *Principles of LED Light Communications Towards Networked Li-Fi* (Cambridge University Press, 2015). His main research interests are in optical wireless communications, hybrid optical wireless and RF communications, spatial modulation, and interference coordination in wireless networks. He first introduced and coined spatial modulation and LiFi. LiFi was listed among the 50 best inventions in TIME Magazine 2011. He was an invited speaker with TED Global 2011, and his talk on Wireless Data from Every Light Bulb has been watched online over 2.4 million times. He gave a second TED Global lecture in 2015 on the use of solar cells as LiFi data detectors and energy harvesters. This has been viewed online over 1.8 million times. He was elected as a Fellow of the Royal Society of Edinburgh in 2017. In 2012 and 2017, he was the recipient of the prestigious Established Career Fellowship from the Engineering and Physical Sciences Research Council (EPSRC) within Information and Communications Technology in the U.K. In 2014, he was selected by EPSRC as one of ten Recognising Inspirational Scientists and Engineers Leaders in the U.K. He was the co-recipient of the EURASIP Best Paper Award for the *Journal on Wireless Communications and Networking* in 2015, and co-recipient of the Jack Neubauer Memorial Award of the IEEE VEHICULAR TECHNOLOGY SOCIETY. In 2016, he was a recipient of the outstanding achievement award from the International Solid State Lighting Alliance. He was the co-recipient of recent Best Paper Awards at VTC, 2013, VTC 2015, ICC 2016, and ICC 2017. He is currently an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE JOURNAL OF LIGHTWAVE TECHNOLOGIES.

IEEE Proof

Physical-Layer Security in Multiuser Visible Light Communication Networks

Liang Yin and Harald Haas, *Senior Member, IEEE*

***Abstract*— In this paper, we study the physical-layer security in a 3-D multiuser visible light communication (VLC) network. The locations of access points (APs) and mobile users are modeled as two 2-D, independent and homogeneous Poisson point processes at distinct heights. Using mathematical tools from stochastic geometry, we provide a new analytical framework to characterize the secrecy performance in multiuser VLC networks. Closed-form results for the outage probability and the ergodic secrecy rate are derived for networks without AP cooperation. Considering the cooperation among APs, we give tight lower and upper bounds on the secrecy outage probability and the ergodic secrecy rate. To further enhance the secrecy performance at the legitimate user, a disk-shaped secrecy protected zone is implemented in the vicinity of the transmit AP. Based on the obtained results, it is shown that cooperating neighboring APs in a multiuser VLC network can bring performance gains on the secrecy rate, but only to a limited extent. We also show that building an eavesdropper-free protected zone around the AP significantly improves the secrecy performance of legitimate users, which appears to be a promising solution for the design of multiuser VLC networks with high security requirements.**

***Index Terms*— Visible light communication, secrecy capacity, physical-layer security, poisson point process, stochastic geometry.**

I. Introduction

BY UTILIZING the existing lighting infrastructure and shifting the communication frequency to the visible spectrum, visible light communication (VLC) [1]–[3] has recently emerged as a promising candidate for future high-speed broadband communications, which could effectively alleviate the spectrum congestion issue in current radio frequency (RF) based wireless systems. Recent advances have also led to the standardization of short-range wireless optical communication using VLC for local and metropolitan area networks [4], which serves as a major step towards its commercialization in the near future. Compared to RF communication, VLC has the following main advantages: 1) VLC builds upon existing lighting devices and operates on the license-free spectrum so that it has lower implementation cost; 2) VLC can operate safely in electromagnetic sensitive areas, where RF is intrinsically prohibited; 3) VLC networking can be designed in addition to existing heterogeneous wireless networks because it receives zero interference from, and adds zero interference to its RF counterparts; 4) Based on the property that visible light does not penetrate through opaque objects, the communication bandwidth in one room can be efficiently reused in other rooms to obtain a high frequency reuse factor and hence a high area spectral efficiency; 5) Indoor VLC typically achieves higher physical-layer security since the transmitted signal is confined within the room.

The broadcast property of VLC has been utilized in many novel designs of multiuser VLC networks [5]–[7]. However, it also causes potential concerns to legitimate users and network administrators regarding the information privacy and confidentiality, especially in public areas, such as train stations and libraries. From an information-theoretic point of view, the physical-layer security was pioneered by Wyner for proposing the wiretap channel [8]: a channel in which an eavesdropper receives a degraded version of the transmitted signal. The degraded wiretap channel was later extended to the non-degraded broadcast channel by Csiszár and Körner [9]. In their seminal work, it is shown that perfect secrecy can be achieved as long as the legitimate user has a less degraded channel than the eavesdropper, and the secrecy capacity is derived as the difference between the information capacity for the two users. Typical security enhancement techniques that are implemented at upper layers of the communication chain include password protection and user admission control. Physical-layer security, on the other hand, exploits the randomness of the noise and the wireless communication channel to limit the amount of legitimate information to be detected by unauthorized eavesdroppers [8], [9].

Different from point-to-point communication, studying the secrecy performance in a large-scale wireless network requires not only the knowledge of locations of legitimate users but also the knowledge of locations of eavesdropping users that may interact with legitimate users. Initial works that characterize the secrecy performance in multiuser wireless networks rely on the secrecy graph model to study the node connectivity [10], [11] and the maximum secrecy rate [12], from an information-theoretic perspective. Following these works, the secrecy rate per source-destination pair was investigated in [13] by characterizing the secrecy capacity scaling laws in a wireless network. Moving from network information theory, recent works have evaluated the secrecy performance in multiuser wireless networks using mathematical tools from stochastic geometry [14], [15]. It should be noted that works in [8]–[15] are all focused on RF based wireless networks.

Manuscript received February 22, 2017; revised July 15, 2017; accepted September 16, 2017. This work was supported by the U.K. Engineering and Physical Sciences Research Council under Grant EP/K008757/1. *(Corresponding author: Liang Yin.)*

The authors are with the School of Engineering, Institute for Digital Communications, Li-Fi Research and Development Centre, University of Edinburgh, Edinburgh EH9 3JL, U.K. (e-mail: l.yin@ed.ac.uk; h.haas@ed.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSAC.2017.2774429

0733-8716 © 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

IEEE Proof

Different from RF communication, which is typically modeled as a Gaussian broadcast channel with an average power constraint at the transmitter side, VLC typically uses intensity modulation and direct detection (IM/DD) due to the use of inexpensive light-emitting diodes (LEDs) and photodiodes (PDs) as the optical transmitter and receiver, respectively. In VLC, since the signal is modulated onto the intensity of the emitted light, it must satisfy average, peak as well as non-negative amplitude constraints, that are imposed by the dynamic range of typical LEDs and practical illumination requirements [6], [16]–[18]. Although typical LEDs have a nonlinear electrical-to-optical (E/O) transfer characteristic, this nonlinearity can be successfully compensated by pre-distortion techniques [19]. Also, since the wavelength of visible light is hundreds of nanometers while the detection area of a typical PD is millions of square wavelengths, this spatial diversity essentially prevents the "multipath fading" effect in the VLC channel. Due to these fundamental differences, results on the secrecy capacity obtained for RF networks can not be directly applied to VLC networks.

Since the secrecy capacity is related to the information capacity of the communication channel [8], [9], before determining the secrecy capacity in VLC networks it is essential to obtain the information capacity of the VLC channel with average, peak and non-negative constraints. However, to the best of authors' knowledge, the exact information capacity of the VLC channel with such constraints still remains unknown, even for the simplest single-input single-output (SISO) case, despite some lower and upper bounds have been derived [16]–[18]. By considering one transmitter, one legitimate user and one eavesdropper in a VLC system, lower and upper bounds on the secrecy capacity of the amplitude-constrained Gaussian wiretap channel was recently studied in [20], with the use of the derived capacity lower and upper bounds in [16]. In the same work [20], beamforming was also utilized to improve the secrecy capacity for the multiple-input single-output (MISO) VLC channel. Following this, the optimal beamformer design problem subject to amplitude constraints was further studied in [21]. The secrecy performance in a single-cell VLC system with only one AP was studied in [22]. However, the randomness of legitimate users as well as eavesdroppers and, more importantly, the interactions between them, have not been fully characterized when analyzing the secrecy performance in a random multiuser VLC network.

A. Approaches and Contributions

In this work, we aim to characterize the secrecy performance in an indoor multiuser VLC network by considering the unique properties of the VLC channel as well as the network layout, that differ from typical RF networks. Our approach builds upon a proposed three-dimensional network model with two independent random topologies for the VLC APs and mobile users. Specifically, the VLC APs are modeled by a two-dimensional homogeneous Poisson point process (PPP) in the ceiling, while the locations of users, that include both legitimate users and eavesdroppers, are modeled by another independent two-dimensional homogeneous PPP at the user plane. To separate eavesdroppers from legitimate users, the locations of random eavesdroppers are obtained from a thinned PPP. Despite the grid-like deployment of LEDs in typical offices, the following observations indicate that a stochastic model may be required to accurately capture the distribution of APs in a VLC network. First, more and more LEDs with built-in motion-detection sensors are deployed in public spaces in order to reduce energy consumption. In this case, some of the LEDs will be temporally switched off when they are not required to provide illumination. Second, the distribution of ceiling lights is not necessarily equivalent to the distribution of APs in a VLC network because not necessarily all of the ceiling lights are simultaneously operating in the communication mode, i.e., some of the ceiling lights may operate in the illumination mode only when no data traffic is demanded from them. In these scenarios, the distribution of APs can not be accurately modeled by the grid model. Instead, a stochastic thinning process built upon the grid-like deployment of LEDs is more accurate, where the activeness/idleness of each AP is determined by a time-varying probability distribution function (PDF). However, finding the PDF of activeness/idleness of the LED requires full knowledge of the users' movement and handover characteristics, which is generally complicated and not analytically tractable. In order to derive analytically tractable results, the PPP model is assumed in this work. For completeness, we also compare the secrecy performance between the PPP model and the grid model and provide a method of applying the derived analytical results to estimate the secrecy performance in a conventional grid-like VLC network.

The main contributions of this paper are as follows:

1) When the legitimate user is served by the nearest AP in its vicinity, we derive the distribution function of the secrecy rate of a typical legitimate user, based on which secrecy outage probability and ergodic secrecy rate are obtained. To provide further insights into the secrecy performance with different network parameters, lower and upper bounds on the secrecy outage probability as well as on the ergodic secrecy rate are given.
2) We enhance the secrecy performance by implementing AP cooperation in a multiuser VLC network, and give lower and upper bounds on the secrecy outage probability and the ergodic secrecy rate. The derived analytical bounds are found to be reasonably tight in general and become tighter when the density of eavesdroppers becomes larger.
3) To further enhance the secrecy performance for legitimate users, we introduce a disk-shaped secrecy protected zone around the AP in a multiuser VLC network, in which the presence of eavesdroppers is prohibited. In this scenario, the secrecy outage probability and the ergodic secrecy rate are derived. The impact of designing the protected zone with different sizes on the secrecy performance is also investigated.

The remainder of this paper is organized as follows. In Section II, we introduce a three-dimensional link model for multiuser VLC networks and formulate the information-theoretic secrecy rate expression based on a close approximation of the channel capacity. The secrecy outage probability and the ergodic secrecy rate with/without the AP cooperation are derived in Section III. We extend the analysis on the secrecy performance in Section IV by implementing a disk-shaped protected zone. Simulation results and discussions are provided in Section V. Finally, concluding remarks are given in Section VI.

II. System Model

A. Poisson Network Model

We consider a downlink transmission scenario of a multiuser VLC network with the presence of both legitimate users and eavesdroppers inside a three-dimensional space. The VLC APs are vertically fixed, since they are attached to the room ceiling, and their horizontal positions are modeled by a two-dimensional homogeneous PPP Φ_{a} with density λ_{a}, in nodes per unit area. Similarly, mobile users are assumed to be at a fixed height and their horizontal positions are modeled by another independent two-dimensional homogeneous PPP Φ_{u} with density λ_{u}. The vertical distance between the AP plane and the user plane is denoted by L. After adding an additional user at the room center,[1] the new point process for mobile users becomes $\Phi_{\mathrm{u}} \bigcup \{0\}$. Slivnyak's theorem states that adding a user into Φ_{u} is equivalent to conditioning Φ_{u} on the added point, and this process does not change the distribution of Φ_{u} [23]. Therefore, the added user at the origin can be treated as the *typical* legitimate user in the study since it can reflect the spatial average of the performance of all legitimate users in the network. Among all of the users, there exist malicious eavesdroppers that could compromise the transmission privacy of ongoing legitimate links, due to the broadcast nature of the VLC channel. Since eavesdroppers typically disguise as legitimate users, it is uncertain whether a random user $u \in \Phi_{\mathrm{u}}$ is a legitimate user or an eavesdropper. Therefore, it is assumed that u is an eavesdropper with probability p_{e} and that u is a legitimate user with probability $1 - p_{\mathrm{e}}$. This thinned realization of Φ_{u} gives the point process for eavesdroppers, Φ_{e}, which is also a homogeneous PPP whose density can be found as $\lambda_{\mathrm{e}} = p_{\mathrm{e}}\lambda_{\mathrm{u}}$ [23]. Furthermore, it is assumed that eavesdroppers do not collude with each other so that each eavesdropper needs to decode any confidential messages sent to legitimate users individually. An example of the described multiuser VLC network is depicted in Fig. 1.

A complete VLC channel includes both the line-of-sight (LOS) link and non-line-of-sight (NLOS) links, that are caused by light reflections from interior surfaces. However, in a typical indoor lighting environment, the sum signal power carried by NLOS components is significantly weaker than that carried by the LOS link [1], [24], [25]. Therefore, we will only focus on the LOS link in the following analysis in order to obtain tractable analytical results. The VLC APs are assumed to have a Lambertian radiation profile whose Lambertian order is $m = -1/\log_2(\cos\ (\Phi_{1/2}))$, where $\Phi_{1/2}$ denotes the semi-angle of the LED. The PD equipped at each user is assumed to be facing vertically upwards with a field-of-view (FOV) of Ψ_{fov}. For each VLC link, the optical channel direct current (DC) gain is given by [26]:

[1]The room center is also called the origin. We use both expressions interchangeably throughout the paper since the room center has more geographical meanings while the origin has more mathematical meanings when we apply stochastic geometry tools in the theoretical analysis.

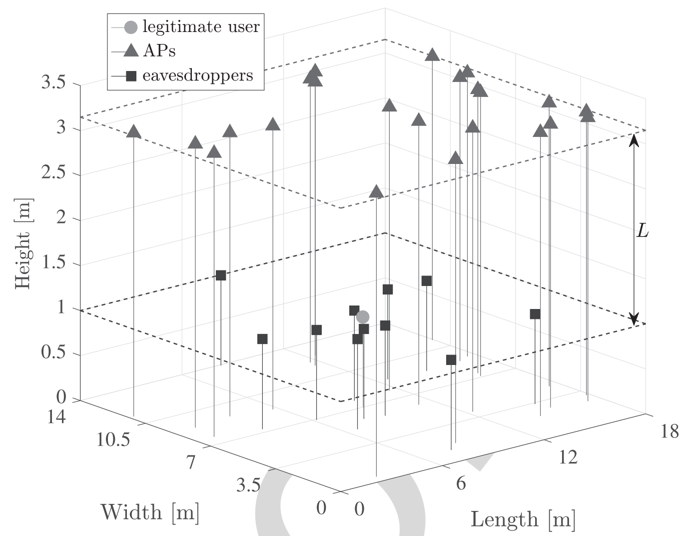

Fig. 1. Random network model: the legitimate user of interest is placed at the room center; VLC APs are randomly distributed in the ceiling according to a homogeneous PPP Φ_{a}; and eavesdroppers are randomly distributed on the same plane as the legitimate user, following a homogeneous PPP Φ_{e}. In this example, an indoor VLC network of size $18 \times 14 \times 3.5$ m^3 is shown.

$$h = \frac{(m+1)A\eta}{2\pi d^2}\cos^m(\phi)T(\psi)g(\psi)\cos(\psi), \qquad (1)$$

where A denotes the effective detection area of the PD; η is the responsivity of the PD; ϕ and ψ are the angle of irradiance and the angle of incidence of the optical link, respectively; $T(\psi)$ represents the gain of the optical filter used at the receiver; and $g(\psi)$ represents the gain of the optical concentrator. The optical concentrator gain is given by [26]:

$$g(\psi) = \begin{cases} \dfrac{n^2}{\sin^2(\Psi_{\mathrm{fov}})}, & 0 \le \psi \le \Psi_{\mathrm{fov}} \\ 0, & \psi > \Psi_{\mathrm{fov}} \end{cases}, \qquad (2)$$

where n is the reflective index of the optical concentrator, and it is defined as the ratio of the speed of light in vacuum and the phase velocity of light in the optical material. For visible light, the typical value for n varies between 1 and 2.

Consider the communication link from an AP $x \in \Phi_{\mathrm{a}}$ to an eavesdropper $e \in \Phi_{\mathrm{e}}$. Based on the geometry [7] of the VLC link, it is easy to obtain $d = \sqrt{\|e - x\|^2 + L^2}$, $\cos(\phi) = L/\sqrt{\|e - x\|^2 + L^2}$ and $\cos(\psi) = L/\sqrt{\|e - x\|^2 + L^2}$. Therefore, the received optical power at eavesdropper e from AP x can be written as:

$$\begin{aligned} P_{\mathrm{rx}}(x, e) &= hP_{\mathrm{tx}} \\ &= \frac{(m+1)A\eta T(\psi)g(\psi)L^{m+1}}{2\pi(\|e - x\|^2 + L^2)^{\frac{m+3}{2}}}P_{\mathrm{tx}}, \end{aligned} \qquad (3)$$

where P_{tx} denotes the transmit optical power of the AP. Similarly, the received signal power at the legitimate user can be written as $P_{\mathrm{rx}}(x, o)$, where o representing the origin is the location of the typical user of interest.

B. Secrecy Capacity Formulation

The classic Shannon equation does not apply to VLC because of the average, peak and non-negative constraints on the modulated optical signal. Although the exact capacity of the VLC channel remains unknown, several upper and lower bounds have been derived [16]–[18]. Based on the capacity lower bound derived in [16], the exact channel capacity of VLC can be written as:

$$C = \frac{1}{2}\log_2\left(1 + \frac{\exp(1) P_{\rm rx}^2}{2\pi\sigma_{\rm n}^2}\right) + \epsilon\left(\frac{P_{\rm rx}}{\sigma_{\rm n}}\right), \qquad (4)$$

where ϵ, as a function of the received optical-signal-to-noise ratio (OSNR) $P_{\rm rx}/\sigma_{\rm n}$, represents a positive capacity gap between the exact channel capacity and the analytical lower bound [16], and $\sigma_{\rm n}^2$ represents the total power of noise processes at the receiver. Note that inside the receiver circuit the dominant noise sources are the thermal noise and shot noise [1], [25]. The thermal noise is mainly caused by the preamplifier circuits while the shot noise originates mainly from the ambient light and/or other light sources. The signal-dependent shot noise, on the other hand, is relatively small, and hence its effect can be ignored. The overall noise process is generally well modeled as the additive white Gaussian noise (AWGN) [1], [25]. As the legitimate user and eavesdroppers may use different grades of receivers, for example, PDs with different detection areas and/or bandwidths, they are subject to different levels of receiver noise and are capable of detecting signals with different amplifying gains. Without loss of generality, the choice of different grades of receivers can be accounted for in the system model by assigning different noise variances at the legitimate user and the eavesdropper. Based on this, we denote by $\sigma_{\rm nb}^2$ and $\sigma_{\rm ne}^2$ the noise variance at the legitimate user and the noise variance at the eavesdropper, respectively. Unlike RF channels whose input signals are subject to an average power constraint [29], VLC channels require the input signals to satisfy a peak amplitude (optical power) constraint. This makes it challenging to obtain closed-form expressions for the secrecy capacity of a VLC link, even for the simplest SISO case [20], [30]. Therefore, in the following analysis we focus on a tight achievable lower bound on the secrecy capacity [20]:

$$C_{\rm s} \geq [C_{\rm b} - C_{\rm e}]^+ = \underline{C}_{\rm s}, \qquad (5)$$

where $[a]^+ = \max\{a, 0\}$; $C_{\rm s}$ represents the exact secrecy capacity; $\underline{C}_{\rm s}$ represents the tight lower bound on the secrecy capacity given by the right-hand side of (5); $C_{\rm b}$ is the channel capacity of the legitimate link; and $C_{\rm e}$ is the channel capacity of the eavesdropper's link.

III. Secrecy Rate in Random VLC Networks

A. Nearest AP to Serve the Legitimate User

Without AP cooperation, the nearest AP is typically assumed to serve a mobile user in the VLC network in order to maximize the information rate of the communication link. As a result, based on (4), the capacity of the legitimate link can be written as $C_{\rm b} = \max_{x\in\Phi_{\rm a}} \frac{1}{2}\log_2(1+\exp(1)P_{\rm rx}^2(x,o)/2\pi\sigma_{\rm nb}^2) + \epsilon\left(P_{\rm rx}(x,o)/\sigma_{\rm nb}\right) = \frac{1}{2}\log_2(1 + \exp(1)P_{\rm rx}^2(x_0,o)/2\pi\sigma_{\rm nb}^2) + \epsilon\left(P_{\rm rx}(x_0,o)/\sigma_{\rm nb}\right)$, where x_0 represents the location of the nearest AP to the origin. Since it is assumed that eavesdroppers do not collude, the secrecy performance of the legitimate user is limited by the eavesdropper with the highest OSNR. Therefore, the lower bound on the secrecy capacity at the typical legitimate user is formulated as:

$$\begin{aligned}\underline{C}_{\rm s} = \Bigg[&\frac{1}{2}\log_2\left(1 + \frac{\exp(1)P_{\rm rx}^2(x_0,o)}{2\pi\sigma_{\rm nb}^2}\right) \\ &- \frac{1}{2}\log_2\left(1 + \frac{\exp(1)P_{\rm rx}^2(x_0,e^*(x_0))}{2\pi\sigma_{\rm ne}^2}\right) \\ &+ \epsilon\left(\frac{P_{\rm rx}(x_0,o)}{\sigma_{\rm nb}}\right) - \epsilon\left(\frac{P_{\rm rx}(x_0,e^*(x_0))}{\sigma_{\rm ne}}\right)\Bigg]^+, \qquad (6)\end{aligned}$$

where $e^*(x_0)$ denotes the horizontal distance from AP x_0 to the nearest eavesdropper. Given that the legitimate user is connected to AP x, the general solution for $e^*(x)$, denoting the horizontal distance between AP x and the strongest eavesdropper, can be obtained by finding the location of the eavesdropper $e \in \Phi_{\rm e}$ that receives the strongest signal power:

$$\begin{aligned}e^*(x) &= \arg\max_{e\in\Phi_{\rm e}} P_{\rm rx}(x,e) \\ &= \arg\min_{e\in\Phi_{\rm e}} \|e - x\|, \qquad (7)\end{aligned}$$

where the last step is obtained based on the monotonic property of (3). By utilizing fractional frequency reuse [28] or orthogonal multiple access techniques, the achievable data rate can be quantified through the received signal-to-noise ratio (SNR) without the side effect of co-channel interference (CSI). As a result, OSNR of $P_{\rm rx}/\sigma_{\rm n} > 30$ dB can be achieved at typical illumination levels [25], [27], where $\epsilon(P_{\rm rx}/\sigma_{\rm n})$ is found to be comparatively small [16]–[18]. Therefore, we focus on the high OSNR regime, where $\epsilon(P_{\rm rx}(x_0,o)/\sigma_{\rm nb}) \ll 1/2\log_2(\exp(1)P_{\rm rx}^2(x_0,o)/2\pi\sigma_{\rm nb}^2)$ and $\epsilon(P_{\rm rx}(x_0,e^*(x_0))/\sigma_{\rm ne}) \ll 1/2\log_2(\exp(1)P_{\rm rx}^2(x_0,e^*(x_0))/2\pi\sigma_{\rm ne}^2)$. Based on this, (6) can be further approximated to:

$$\underline{C}_{\rm s} \approx \left[\frac{1}{2}\log_2\left(\frac{P_{\rm rx}^2(x_0,o)}{P_{\rm rx}^2(x_0,e^*(x))}\right) + \log_2\left(\frac{\sigma_{\rm ne}}{\sigma_{\rm nb}}\right)\right]^+ = R_{\rm s}. \qquad (8)$$

To distinguish from the exact secrecy capacity, we define in (8) $R_{\rm s}$ as the achievable secrecy rate. Due to the lack of the complete knowledge of the exact secrecy capacity $C_{\rm s}$, the secrecy rate $R_{\rm s}$ is of interest in this paper. It is shown in (8) that a non-negative secrecy rate can only be achieved when the legitimate user achieves a higher SNR than the strongest eavesdropper. In the case that a eavesdropper receives signals from a less-degraded link than the legitimate user, the achievable secrecy rate drops to zero. It can also be seen from (8) that when the legitimate user and the eavesdropper use different grades of receivers, the achieved secrecy capacity at the legitimate user is offset by a constant, whose value is proportional to the logarithm of $\sigma_{\rm ne}/\sigma_{\rm nb}$. Therefore, without loss of generality, $\sigma_{\rm nb} = \sigma_{\rm ne}$ is assumed in the following analysis.

Theorem 1: When the legitimate user is served by the nearest AP in its vicinity, the cummulative distribution function (CDF) of the secrecy rate $R_{\rm s}$ is given by:

$$F_{R_{\rm s}}(\upsilon) = 1 - \frac{1}{1 + \frac{\lambda_{\rm e}}{\lambda_{\rm a}} 4^{\frac{\upsilon}{m+3}}} \exp\left(-\pi\lambda_{\rm e}\left(4^{\frac{\upsilon}{m+3}} - 1\right)L^2\right), \qquad (9)$$

where $\upsilon \geq 0$.

IEEE Proof

Proof: According to (8), we have $R_s \geq 0$. Therefore, the CDF of the secrecy rate R_s can be calculated by:

$$\begin{aligned} F_{R_s}(\upsilon) &= \mathbb{P}[R_s \leq \upsilon] \\ &= \mathbb{P}\left[\frac{P_{\rm rx}^2(x_0, o)}{P_{\rm rx}^2(x_0, e^*(x_0))} \leq 4^{\upsilon}\right] \\ &= \mathbb{P}\left[\|e^*(x_0) - x_0\| \leq \sqrt{\beta x_0^2 + (\beta - 1)L^2}\right], \quad (10) \end{aligned}$$

where $\beta = 4^{\upsilon/(m+3)}$. Since the legitimate user is served by the nearest AP, the PDF of x_0 is [31]:

$$f_{x_0}(x_0) = 2\pi\lambda_a x_0 \exp\left(-\pi\lambda_a x_0^2\right). \quad (11)$$

When conditioned on distance x_0, (10) is the probability that no eavesdroppers exist within a circle, which is centered at x_0 and has a radius of $\sqrt{\beta x_0^2 + (\beta - 1)L^2}$. Such probability can be calculated using the void probability of PPP [32]. As a result, (10) can be calculated as:

$$\begin{aligned} &F_{R_s}(\upsilon) \\ &= \mathbb{E}_{x_0}\left[\mathbb{P}\left[\|e^*(x_0) - x_0\| \leq \sqrt{\beta x_0^2 + (\beta - 1)L^2}\,\middle|\, x_0\right]\right] \\ &= \int_0^{\infty} \mathbb{P}\left[\|e^*(x_0)-x_0\| \leq \sqrt{\beta x_0^2+(\beta-1)L^2}\,\middle|\, x_0\right] f_{x_0}(x_0)\mathrm{d}x_0 \\ &= \int_0^{\infty} \left(1 - \exp\left(-\pi\lambda_e\left(\beta x_0^2 + (\beta - 1)L^2\right)\right)\right) 2\pi\lambda_a x_0 \\ &\quad \times \exp\left(-\pi\lambda_a x_0^2\right)\mathrm{d}x_0 \\ &= 1 - \frac{1}{1 + \frac{\lambda_e}{\lambda_a}\beta}\exp\left(-\pi\lambda_e(\beta - 1)L^2\right). \quad (12) \end{aligned}$$

After plugging $\beta = 4^{\upsilon/(m+3)}$ into (12), we obtain (9). ■

Corollary 1: When the legitimate user is served by the n-th nearest AP in its vicinity, the CDF of the secrecy rate is:

$$F_{R_s}(\upsilon) = 1-\left(\frac{1}{1 + \frac{\lambda_e}{\lambda_a}4^{\frac{\upsilon}{m+3}}}\right)^n \exp\left(-\pi\lambda_e\left(4^{\frac{\upsilon}{m+3}} - 1\right)L^2\right), \quad (13)$$

where $\upsilon \geq 0$.

Proof: The distance distribution of the legitimate user to the n-th nearest AP is given by [31]:

$$f_{x_n}(x_n) = \frac{2(\pi\lambda_a x_n^2)^n}{x_n\Gamma(n)}\exp\left(-\pi\lambda_a x_n^2\right). \quad (14)$$

By using (14) and following similar steps as in (12), (13) can be obtained. ■

The secrecy outage probability, denoted by $p_{\rm so}$, is defined as the probability that the secrecy rate is below a target secrecy rate $\bar{R}_s$. Mathematically, it is formulated as:

$$p_{\rm so} = \mathbb{P}\left[R_s \leq \bar{R}_s\right] = F_{R_s}(\bar{R}_s), \quad (15)$$

which can be obtained directly from Theorem 1.

Corollary 2: When the legitimate user is served by the nearest AP in its vicinity, the secrecy outage probability is lower bounded by:

$$p_{\rm so}^{\rm LB} = 1 - \exp\left(-\pi\lambda_e\left(4^{\frac{\bar{R}_s}{m+3}} - 1\right)L^2\right), \quad (16)$$

when the density of VLC APs approaches infinity.

Proof: (16) can be obtained from $p_{\rm so}^{\rm LB} = \lim_{\lambda_a\to\infty} p_{\rm so}$. ■

Theorem 1 and Corollary 2 provide an important guideline for the design of VLC networks: installing more VLC APs can help decrease the secrecy outage probability of a typical legitimate user; however, when the density of APs reaches a certain level, further increasing the density of APs is not meaningful since it can no longer enhance the secrecy performance. In other words, it is impossible for a legitimate user in the network to simultaneously achieve a target secrecy rate $\bar{R}_s$ and have an outage probability lower than $p_{\rm so}^{\rm LB}(\bar{R}_s)$. Given a target secrecy rate $\bar{R}_s$ and a target outage probability $\bar{p}_{\rm so} > p_{\rm so}^{\rm LB}(\bar{R}_s)$, this requirement can be achieved by installing more APs in the network so that the density of APs satisfies $\lambda_a \geq \lambda_e(1 - \bar{p}_{\rm so})4^{\bar{R}_s/(m+3)}\big/\left(\bar{p}_{\rm so} - p_{\rm so}^{\rm LB}(\bar{R}_s)\right)$. From (9) and (16), it is shown that reducing the semi-angle of the LED, or equivalently increasing the Lambertian order, can also help improve the secrecy performance of the network. Nevertheless, the actual choice of the semi-angle of the LED should also satisfy the illumination requirement.

Theorem 2: When the legitimate user is served by the nearest AP in its vicinity, the ergodic secrecy rate at the legitimate user is:

$$\begin{aligned} \mathbb{E}[R_s] = \frac{m+3}{\ln(4)}\Big[&\exp\left(\pi(\lambda_e + \lambda_a)L^2\right)\mathrm{Ei}\left(-\pi(\lambda_e + \lambda_a)L^2\right) \\ &- \exp\left(\pi\lambda_e L^2\right)\mathrm{Ei}\left(-\pi\lambda_e L^2\right)\Big], \quad (17) \end{aligned}$$

where $\mathrm{Ei}(a) = -\int_{-a}^{\infty}\exp(-t)/t\mathrm{d}t$ is the exponential integral function [33].

Proof: The ergodic secrecy rate can be calculated based on the CDF of R_s:

$$\begin{aligned} \mathbb{E}[R_s] &= \int_0^{\infty}\left(1 - F_{R_s(\upsilon)}\right)\mathrm{d}\upsilon \\ &= \frac{m+3}{\ln(4)}\int_1^{\infty}\frac{1}{\beta\left(1+\frac{\lambda_e}{\lambda_a}\beta\right)}\exp\left(-\pi\lambda_e(\beta-1)L^2\right)\mathrm{d}\beta \\ &= \frac{m+3}{\ln(4)}\Bigg[\int_1^{\infty}\frac{\exp\left(-\pi\lambda_e(\beta - 1)L^2\right)}{\beta}\mathrm{d}\beta \\ &\quad - \int_1^{\infty}\frac{\exp\left(-\pi\lambda_e(\beta - 1)L^2\right)}{\beta + \frac{\lambda_a}{\lambda_e}}\mathrm{d}\beta\Bigg], \quad (18) \end{aligned}$$

where the integration variable has been changed from υ to β. After applying [33, eq. 3.351.5], the first integration in (18) can be calculated as:

$$\int_1^{\infty}\frac{\exp\left(-\pi\lambda_e(\beta-1)L^2\right)}{\beta}\mathrm{d}\beta = -\exp\left(\pi\lambda_e L^2\right)\mathrm{Ei}\left(-\pi\lambda_e L^2\right). \quad (19)$$

After applying [33, eq. 3.352.2], the second integration in (18) can be calculated as:

$$\begin{aligned} &\int_1^{\infty}\frac{\exp\left(-\pi\lambda_e(\beta - 1)L^2\right)}{\beta + \frac{\lambda_a}{\lambda_e}}\mathrm{d}\beta \\ &\quad = -\exp\left(\pi(\lambda_e+\lambda_a)L^2\right)\mathrm{Ei}\left(-\pi(\lambda_e+\lambda_a)L^2\right). \quad (20) \end{aligned}$$

After plugging (19) and (20) into (18), (17) is obtained. ■

IEEE Proof

Corollary 3: When the legitimate user is served by the nearest AP in its vicinity, the ergodic secrecy rate at the legitimate user is upper bounded by:

$$R_{\mathrm{s}}^{\mathrm{UB}} = \frac{m+3}{\ln(4)} \left(-\exp\left(\pi \lambda_{\mathrm{e}} L^2\right) \mathrm{Ei}\left(-\pi \lambda_{\mathrm{e}} L^2\right)\right). \quad (21)$$

Proof: The upper bound on the secrecy rate can be obtained from $R_{\mathrm{s}}^{\mathrm{UB}} = \lim_{\lambda_{\mathrm{a}}\to\infty} \mathbb{E}[R_{\mathrm{s}}]$. Based on the equality

$$\lim_{\lambda_{\mathrm{a}}\to\infty} \exp\left(\pi(\lambda_{\mathrm{e}}+\lambda_{\mathrm{a}})L^2\right) \mathrm{Ei}\left(-\pi(\lambda_{\mathrm{e}}+\lambda_{\mathrm{a}})L^2\right) = 0, \quad (22)$$

we obtain (21). ■

Theorem 2 and Corollary 3 indicate that increasing the density of VLC APs can help enhance the ergodic secrecy rate of a typical legitimate user. However, when the density of APs exceeds a certain level, installing more APs can not enhance the ergodic secrecy rate any further. While satisfying the illumination requirement, using LEDs with a smaller semi-angle can increase the ergodic secrecy rate of a typical user. Specifically, it can be seen from (17) and (21) that a linear relationship exists between the ergodic secrecy rate and the Lambertian order m. Given the choice of LEDs, the maximum ergodic secrecy rate can not exceed the upper bound given in (21). To achieve a target ergodic secrecy rate $\bar{R}_{\mathrm{s}}$, whose value is smaller than $R_{\mathrm{s}}^{\mathrm{UB}}$, the density of APs needs to exceed λ_{a}^*, where λ_{a}^* is the numerical solution for λ_{a} to equation $\exp\left(\pi\ (\lambda_{\mathrm{e}}+\lambda_{\mathrm{a}})L^2\right) \mathrm{Ei}\left(-\pi\ (\lambda_{\mathrm{e}}+\lambda_{\mathrm{a}})L^2\right) = \ln(4)\bar{R}_{\mathrm{s}}/(m+3) + \exp\left(\pi\lambda_{\mathrm{e}}L^2\right) \mathrm{Ei}\left(-\pi\lambda_{\mathrm{e}}L^2\right)$.

B. Optimal AP to Serve the Legitimate User

Due to the randomness of eavesdroppers, it is not always optimal to serve the legitimate user with the nearest AP. For example, if the eavesdropper is close to the nearest AP around the legitimate user but far away from the second nearest AP around the legitimate user, selecting the second nearest AP to serve the legitimate user may yield a higher secrecy rate. Therefore, with the cooperation among APs, the secrecy performance at legitimate users can be further enhanced. However, it should be noted that selecting the optimal AP to serve legitimate users requires the knowledge of the location information of all eavesdroppers at the central controller, which can be achieved with indoor sensing and localization technologies. Despite the additional implementation and computation complexity, this optimal scheme yields an enhanced secrecy rate, which is useful for network designers to quantify the secrecy performance provided by the nearest AP and optimal AP and to decide which scheme is more suitable for practical implementations. When the optimal AP is selected to serve the legitimate user, the secrecy rate is formulated as:

$$R_{\mathrm{s}} = \left[\max_{x\in\Phi_{\mathrm{a}}} \left\{\frac{1}{2}\log_2\left(\frac{P_{\mathrm{rx}}^2(x,o)}{P_{\mathrm{rx}}^2(x,e^*(x))}\right)\right\}\right]^+. \quad (23)$$

Due to the intractability of the secrecy rate expression given in (23), the distribution function of R_{s} is hard to obtain. In the following, we provide two analytical bounds on the CDF of the secrecy rate.

Corollary 4: With the cooperation among VLC APs, the CDF of the secrecy rate at the typical legitimate user is lower bounded by:

$$F_{R_{\mathrm{s}}}(\upsilon) \geq \exp\left(-\frac{\lambda_{\mathrm{a}}}{\lambda_{\mathrm{e}}} 4^{-\frac{\upsilon}{m+3}} \exp\left(-\pi\lambda_{\mathrm{e}}\left(4^{\frac{\upsilon}{m+3}}-1\right)L^2\right)\right), \quad (24)$$

and is upper bounded by:

$$F_{R_{\mathrm{s}}}(\upsilon) \leq 1 - \frac{1}{1+\frac{\lambda_{\mathrm{e}}}{\lambda_{\mathrm{a}}}4^{\frac{\upsilon}{m+3}}} \exp\left(-\pi\lambda_{\mathrm{e}}\left(4^{\frac{\upsilon}{m+3}}-1\right)L^2\right). \quad (25)$$

Proof: With the cooperation of VLC APs, the CDF of the secrecy rate can be calculated with the help of the probability generating functional (PGFL) of the PPP [23]:

$$\begin{aligned}
&F_{R_{\mathrm{s}}}(\upsilon) \\
&= \mathbb{P}\left[\max_{x\in\Phi_{\mathrm{a}}}\left\{\frac{1}{2}\log_2\left(\frac{P_{\mathrm{rx}}^2(x,o)}{P_{\mathrm{rx}}^2(x,e^*(x))}\right)\right\} \leq \upsilon\right] \\
&= \mathbb{P}\left[\frac{1}{2}\log_2\left(\frac{P_{\mathrm{rx}}^2(x,o)}{P_{\mathrm{rx}}^2(x,e^*(x))}\right) \leq \upsilon, \forall x\in\Phi_{\mathrm{a}}\right] \\
&= \mathbb{E}_{\Phi_{\mathrm{e}}}\left[\mathbb{E}_{\Phi_{\mathrm{a}}}\left[\prod_{x\in\Phi_{\mathrm{a}}} \mathbf{1}\left(\|e-x\| \leq \sqrt{\beta l^2+(\beta-1)L^2}\right)\right]\right] \\
&= \mathbb{E}_{\Phi_{\mathrm{e}}}\left[\exp\left[-\lambda_{\mathrm{a}}\int_{\mathbb{R}^2}\mathbf{1}\left[\|e-x\| > \sqrt{\beta l^2+(\beta-1)L^2}\,\middle|\, x\right]\mathrm{d}x\right]\right],
\end{aligned} \quad (26)$$

where $\mathbf{1}(\mathcal{A}) = 1$ with event $\mathcal{A}$ being true, and zero otherwise. Based on Jensen's inequality, the lower bound can be calculated as:

$$F_{R_{\mathrm{s}}}(\upsilon) \geq \exp\left[-2\pi\lambda_{\mathrm{a}}\int_0^\infty \mathbb{P}\left[\|e-x\| > \sqrt{\beta x^2+(\beta-1)L^2}\,\middle|\, x\right] \times x\mathrm{d}x_0\right]. \quad (27)$$

After calculating the integration part in (27), the lower bound result in Corollary 4 is obtained. The upper bound can be obtained straightforwardly from the following inequality:

$$\left[\max_{x\in\Phi_{\mathrm{a}}}\left\{\log_2\left(\frac{P_{\mathrm{rx}}^2(x,o)}{P_{\mathrm{rx}}^2(x,e^*(x))}\right)\right\}\right]^+ \geq \left[\log_2\left(\frac{P_{\mathrm{rx}}^2(x_0,o)}{P_{\mathrm{rx}}^2(x_0,e^*(x_0))}\right)\right]^+. \quad (28)$$

In other words, choosing the nearest AP to serve the legitimate user is sub-optimal, which gives an upper bound on the CDF of the secrecy capacity. Therefore, the upper bound expression shown in (25) can be obtained directly from Theorem 1. ■

Based on the upper bound on the CDF of the secrecy rate, a lower bound on the ergodic secrecy rate can be obtained, as given in (17). An upper bound on the ergodic secrecy rate can be obtained by integrating the complement of the CDF of R_{s}:

$$\begin{aligned}
&\mathbb{E}[R_{\mathrm{s}}] \\
&= \int_0^\infty \left(1-F_{R_{\mathrm{s}}(\upsilon)}\right)\mathrm{d}\upsilon \\
&\leq \frac{m+3}{\ln(4)}\int_1^\infty\left(1-\exp\left(-\frac{\lambda_{\mathrm{a}}}{\lambda_{\mathrm{e}}\beta}\exp\left(-\pi\lambda_{\mathrm{e}}(\beta-1)L^2\right)\right)\right)\frac{1}{\beta}\mathrm{d}\beta.
\end{aligned} \quad (29)$$

IEEE Proof

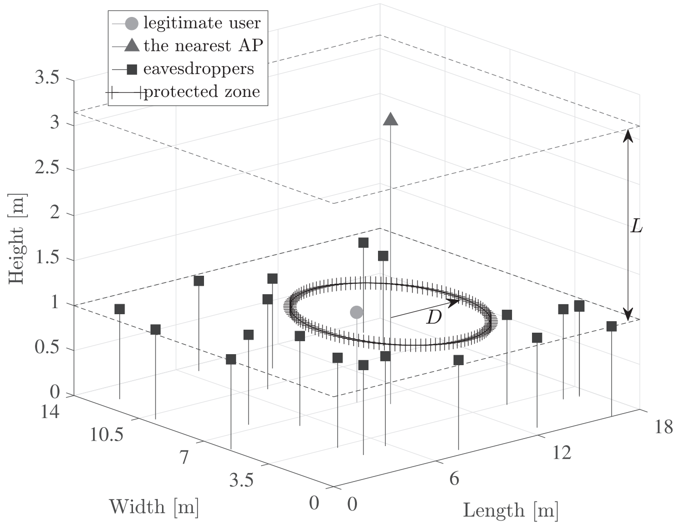

Fig. 2. Random network model with a secrecy protected zone. In this model, each VLC AP has a disk-shaped protected zone, which is centered around the AP and has a radius of D on the user plane. For simplicity, only the protected zone around the nearest AP is drawn.

Because of the nested exponential function in (29), a closed-form expression is not available. However, (29) can be efficiently calculated using numerical methods.

IV. Enhancing Secrecy Rate in VLC Networks With a Protected Zone

In order to further enhance the secrecy performance of legitimate users in VLC networks, a strategy named the "protected zone" [34] can be implemented. As depicted in Fig. 2, a protected zone is an eavesdropper-free area (on the user plane), which allows only legitimate users to enter. If any eavesdropper enters the protected zone, such behavior will be made aware to the AP, and the AP will notify the legitimate user and temporarily stop the communication. A practical implementation of the protected zone in VLC networks can be achieved with motion sensors that are already built in modern energy-efficient lighting devices. We acknowledge that there might be means to break the suggested enforcement of the protected zone. However, a deeper investigation of this aspect is outside the scope of this work. A secrecy protected zone can be completely described by its center, i.e., its associated AP, and a security radius D. The security radius is defined as the smallest horizontal distance between the AP and any eavesdroppers that are undetectable.

Lemma 1: Given that the horizontal distance between the nearest AP to the legitimate user is x_0, the PDF of the horizontal distance between this AP and the nearest eavesdropper, that is outside the protected zone, is:

$$f_{\|e^*(x_0)-x_0\|}(\alpha) = 2\pi\lambda_e\alpha\exp\left(-\pi\lambda_e(\alpha^2 - D^2)\right), \quad (30)$$

for $\alpha \geq D$, and zero otherwise.

Proof: (30) can be obtained using the void probability of PPP [32]. ∎

With Lemma 1, we are ready to obtain the CDF of the secrecy rate enhanced by the protected zone.

Corollary 5: When the legitimate user is served by the nearest AP in its vicinity, which has a protected zone with radius D, the CDF of the enhanced secrecy rate is given by:

$$F_{R_s}(\upsilon) = 1 - \frac{\exp\left(-\pi\lambda_e\left(\left(4^{\frac{\upsilon}{m+3}} - 1\right)L^2 - D^2\right)\right)}{1 + \frac{\lambda_e}{\lambda_a}4^{\frac{\upsilon}{m+3}}}, \quad (31)$$

for $\upsilon \geq \frac{m+3}{2}\log_2\left(D^2/L^2 + 1\right)$, and

$$F_{R_s}(\upsilon) = \frac{\exp\left(-\pi\lambda_a\left(D^2 - \left(4^{\frac{\upsilon}{m+3}} - 1\right)L^2\right)4^{-\frac{\upsilon}{m+3}}\right)}{1 + \frac{\lambda_a}{\lambda_e}4^{-\frac{\upsilon}{m+3}}}, \quad (32)$$

for $0 \leq \upsilon < \frac{m+3}{2}\log_2\left(D^2/L^2 + 1\right)$.

Proof: Since the protected zone has a radius D, the minimum distance between the nearest eavesdropper and the AP is D. Therefore,

$$e^*(x_0) = \arg\min_{e\in\Phi_e, e\notin\mathcal{B}(x_0,D)} \|e - x_0\|, \quad (33)$$

where $\mathcal{B}(x_0, D)$ denotes the disk-shaped area centered at x_0 with radius D. Due to the exclusive region in (33), the derivation of the CDF of the enhanced secrecy rate needs to be separated into two scenarios. First, when $\sqrt{(\beta-1)L^2} \geq D$, i.e., $\upsilon \geq \frac{m+3}{2}\log_2\left(D^2/L^2 + 1\right)$, the CDF of the enhanced secrecy rate can be calculated as:

$$\begin{aligned} F_{R_s}(\upsilon) = &\int_0^\infty \left(1 - \exp\left(-\pi\lambda_e\left(\beta x_0^2 + (\beta-1)L^2 - D^2\right)\right)\right) \\ &\times 2\pi\lambda_a x_0\exp\left(-\pi\lambda_a x_0^2\right)\mathrm{d}x_0, \quad (34) \end{aligned}$$

which gives the result in (31). Second, when $\sqrt{(\beta-1)L^2} < D$, i.e., $0 \leq \upsilon < \frac{m+3}{2}\log_2\left(D^2/L^2 + 1\right)$, the CDF of the enhanced secrecy rate can be calculated as:

$$\begin{aligned} F_{R_s}(\upsilon) = &\int_{\sqrt{\frac{D^2-(\beta-1)L^2}{\beta}}}^\infty 2\pi\lambda_a x_0\exp\left(-\pi\lambda_a x_0^2\right) \\ &\times\left(1 - \exp\left(-\pi\lambda_e\left(\beta x_0^2 + (\beta-1)L^2 - D^2\right)\right)\right)\mathrm{d}x_0 \\ &+ \int_0^{\sqrt{\frac{D^2-(\beta-1)L^2}{\beta}}} 2\pi\lambda_a x_0\exp\left(-\pi\lambda_a x_0^2\right) \\ &\times\mathbb{P}\left[e^*(x_0)\in\mathcal{B}(x_0,D)\right]\mathrm{d}x_0, \quad (35) \end{aligned}$$

in which the critical point $x_0 = \sqrt{(D^2-(\beta-1)L^2)/\beta}$ is found by solving $\sqrt{\beta x_0^2 + (\beta-1)L^2} = D$. Since $e^*(x_0) \notin \mathcal{B}(x_0, D)$, $\mathbb{P}\left[e^*(x_0)\in\mathcal{B}(x_0,D)\right] = 0$, and the second integration in (35) reduces to zero. After calculating the first integration in (35), we obtain (32). To this end, the proof is completed. ∎

It can be seen from Corollary 5 that the radius of the protected zone has a strong impact on the CDF of the secrecy rate and on the secrecy outage probability. On the one hand, if the radius of the protected zone is small enough so that the target secrecy rate satisfies $\bar{R}_s \geq \frac{m+3}{2}\log_2\left(D^2/L^2 + 1\right)$, given a fixed density of eavesdroppers, the secrecy outage probability is lower bounded by:

$$p_{so}^{LB} = 1 - \exp\left(-\pi\lambda_e\left(\left(4^{\frac{\bar{R}_s}{m+3}} - 1\right)L^2 - D^2\right)\right), \quad (36)$$

IEEE Proof

which is obtained when the density of the APs goes to infinity. On the other hand, if the radius of the protected zone is large enough so that the target secrecy rate satisfies $\bar{R}_\mathrm{s} < \frac{m+3}{2}\log_2\left(D^2/L^2+1\right)$, increasing the density of VLC APs can efficiently reduce the secrecy outage probability, and the worst-case scenario of the secrecy outage probability is upper bounded by:

$$p_\mathrm{so}^\mathrm{UB} = \exp\left(-\pi\lambda_\mathrm{a}\left(D^2-\left(4^{\frac{\bar{R}_\mathrm{s}}{m+3}}-1\right)L^2\right)4^{-\frac{\bar{R}_\mathrm{s}}{m+3}}\right), \quad (37)$$

which is obtained by letting λ_e approach infinity.

Corollary 5 provides an essential guideline to network designers so that they can design a suitable protected zone around each VLC AP in order to provide legitimate users with guaranteed secrecy service. Specifically, for legitimate users to achieve a target secrecy rate $\bar{R}_\mathrm{s}$ with a target secrecy outage probability $\bar{p}_\mathrm{so}$, network designers can set up the protected zone with radius no smaller than D^*, where $D^* = ((4^{\bar{R}_\mathrm{s}/(m+3)}-1)L^2 + (\ln(1-\bar{p}_\mathrm{so}) + \ln(1+4^{\bar{R}_\mathrm{s}/(m+3)}\lambda_\mathrm{e}/\lambda_\mathrm{a}))/\pi\lambda_\mathrm{e})^{1/2}$ for $\bar{p}_\mathrm{so} \geq 1-(1+4^{\bar{R}_\mathrm{s}/(m+3)}\lambda_\mathrm{e}/\lambda_\mathrm{a})^{-1}$, and $D^* = ((4^{\bar{R}_\mathrm{s}/(m+3)}-1)L^2 - (\ln\bar{p}_\mathrm{so} + \ln(1+4^{-\bar{R}_\mathrm{s}/(m+3)}\lambda_\mathrm{a}/\lambda_\mathrm{e}))4^{\bar{R}_\mathrm{s}/(m+3)}/\pi\lambda_\mathrm{a})^{1/2}$ for $\bar{p}_\mathrm{so} < 1-(1+4^{\bar{R}_\mathrm{s}/(m+3)}\lambda_\mathrm{e}/\lambda_\mathrm{a})^{-1}$. Also, it is evident that a more stringent secrecy requirement with a larger $\bar{R}_\mathrm{s}$ and/or a smaller $\bar{p}_\mathrm{so}$ requires the implementation of a larger secrecy protected zone.

Theorem 3: When the legitimate user is served by the nearest AP in its vicinity, which has a protected zone with radius D, the enhanced ergodic secrecy rate at the typical legitimate user is:

$$\begin{aligned}
&\mathbb{E}[R_\mathrm{s}] \\
&= \frac{m+3}{\ln(4)}\Bigg[-\exp\left(\pi\lambda_\mathrm{e}\left(L^2+D^2\right)\right)\mathrm{Ei}\left(-\pi\lambda_\mathrm{e}\left(L^2+D^2\right)\right) \\
&\quad + \ln\left(\frac{D^2}{L^2}+1\right)\Bigg] + \frac{m+3}{\ln(4)}\exp\left(\pi\lambda_\mathrm{a}L^2\right)\Bigg[\mathrm{Ei}\left(-\pi\lambda_\mathrm{a}L^2\right) \\
&\quad + \exp\left(\pi\lambda_\mathrm{e}\left(L^2+D^2\right)\right)\mathrm{Ei}\left(-\pi(\lambda_\mathrm{a}+\lambda_\mathrm{e})\left(L^2+D^2\right)\right) \\
&\quad - \mathrm{Ei}\left(-\pi\lambda_\mathrm{a}\left(L^2+D^2\right)\right)\Bigg]. \qquad (38)
\end{aligned}$$

Proof: Based on Corollary 5, the enhanced ergodic rate can be calculated by integrating the complement of the CDF. Since the CDF has different expressions at different regions, the integration should be separated into two parts:

$$\begin{aligned}
&\mathbb{E}[R_\mathrm{s}] \\
&= \frac{m+3}{\ln(4)}\int_1^{\frac{D^2}{L^2}+1}\left(1-\frac{\exp\left(\frac{-\pi\lambda_\mathrm{a}\left(D^2-(\beta-1)L^2\right)}{\beta}\right)}{1+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}\frac{1}{\beta}}\right)\frac{1}{\beta}\mathrm{d}\beta \\
&\quad + \frac{m+3}{\ln(4)}\int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\lambda_\mathrm{e}\left((\beta-1)L^2-D^2\right)\right)}{\beta+\frac{\lambda_\mathrm{e}}{\lambda_\mathrm{a}}\beta^2}\mathrm{d}\beta, \qquad (39)
\end{aligned}$$

where for simplicity the variable of integration has been changed from υ to β. The first integration in (39) can be simplified to:

$$\begin{aligned}
&\int_1^{\frac{D^2}{L^2}+1}\left(1-\frac{\exp\left(\frac{-\pi\lambda_\mathrm{a}\left(D^2-(\beta-1)L^2\right)}{\beta}\right)}{1+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}\frac{1}{\beta}}\right)\frac{1}{\beta}\mathrm{d}\beta \\
&\qquad = \ln\left(\frac{D^2}{L^2}+1\right)+\exp\left(\pi\lambda_\mathrm{a}L^2\right) \\
&\qquad\quad \times\int_1^{\frac{D^2}{L^2}+1}\frac{\exp\left(-\frac{\pi\lambda_\mathrm{a}\left(L^2+D^2\right)}{\beta}\right)}{\beta+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}}\mathrm{d}\beta, \qquad (40)
\end{aligned}$$

in which the integration part can be obtained as:

$$\begin{aligned}
&\int_1^{\frac{D^2}{L^2}+1}\frac{\exp\left(-\frac{\pi\lambda_\mathrm{a}\left(L^2+D^2\right)}{\beta}\right)}{\beta+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}}\mathrm{d}\beta \\
&= \mathrm{Ei}\left(-\pi\lambda_\mathrm{a}L^2\right)-\mathrm{Ei}\left(-\pi\lambda_\mathrm{a}\left(L^2+D^2\right)\right) \\
&\quad + \exp\left(\pi\lambda_\mathrm{e}\left(L^2+D^2\right)\right)\mathrm{Ei}\left(-\pi(\lambda_\mathrm{a}+\lambda_\mathrm{e})\left(L^2+D^2\right)\right) \\
&\quad - \exp\left(\pi\lambda_\mathrm{e}\left(L^2+D^2\right)\right)\mathrm{Ei}\left(-\pi\lambda_\mathrm{a}L^2-\pi\lambda_\mathrm{e}\left(L^2+D^2\right)\right). \\
&\qquad (41)
\end{aligned}$$

Similarly, the second integration in (39) can be simplified to:

$$\begin{aligned}
&\int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\lambda_\mathrm{e}\left((\beta-1)L^2-D^2\right)\right)}{\beta+\frac{\lambda_\mathrm{e}}{\lambda_\mathrm{a}}\beta^2}\mathrm{d}\beta \\
&\quad = \exp\left(\pi\lambda_\mathrm{e}\left(L^2+D^2\right)\right)\Bigg[\int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\lambda_\mathrm{e}\beta L^2\right)}{\beta}\mathrm{d}\beta \\
&\qquad - \int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\lambda_\mathrm{e}\beta L^2\right)}{\beta+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}}\mathrm{d}\beta\Bigg]. \qquad (42)
\end{aligned}$$

Applying [33, eq. 3.352.2], the two integrations in (42) can be calculated as:

$$\int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\lambda_\mathrm{e}\beta L^2\right)}{\beta}\mathrm{d}\beta = -\mathrm{Ei}\left(-\pi\lambda_\mathrm{e}\left(L^2+D^2\right)\right), \quad (43)$$

and

$$\begin{aligned}
&\int_{\frac{D^2}{L^2}+1}^{\infty}\frac{\exp\left(-\pi\lambda_\mathrm{e}\beta L^2\right)}{\beta+\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}}\mathrm{d}\beta \\
&\quad = -\exp\left(\pi\lambda_\mathrm{a}L^2\right)\mathrm{Ei}\left(-\pi\lambda_\mathrm{e}L^2\left(\frac{\lambda_\mathrm{a}}{\lambda_\mathrm{e}}+\frac{D^2}{L^2}+1\right)\right). \qquad (44)
\end{aligned}$$

Combining (40) – (44) gives the result shown in (38), which completes the proof. ■

Note that the expression for the ergodic secrecy rate in Theorem 3 can be simplified to the one given in Theorem 2 when $D = 0$. Also, it is shown in Theorem 3 that the ergodic secrecy rate scales linearly with the Lambertian order m, regardless of the size of the protected zone. Given the choice of LEDs, the density of APs and the density of eavesdroppers, a target ergodic secrecy capacity $\bar{R}_\mathrm{s}$ can be achieved through the implementation of a protected zone with radius D^*, where

IEEE Proof

TABLE I

SIMULATION PARAMETERS

Parameter	value
Room dimensions	$18 \times 14 \times 3.5$ m^3
Height of VLC APs	3.15 m
Height of mobile users	1 m
Semi-angle of VLC APs, $\Phi_{1/2}$	30°
Transmit optical power of VLC APs, P_{tx}	1 W
Receiver detection area, A	1 cm^2
Receiver responsivity, η	0.4 A/W
Reflective index of the optical concentrator, n	1.5
Optical filter gain, T	1
Receiver FOV, Ψ_{fov}	90°
Receiver noise power, $\sigma_{\text{nb}}^2 = \sigma_{\text{ne}}^2$	−103.98 dBm

D^* is the numerical solution for D by letting (38) equal $\bar{R}_{\text{s}}$. Since the expression in (38) monotonically increases with respect to D, the numerical solution for D^* is unique.

V. SIMULATION RESULTS AND DISCUSSIONS

A. Results Based on the PPP Model

In this section, we use a MATLAB implementation to validate the derived results. Simulation results are obtained by averaging 20, 000 realizations of Monte Carlo simulations. A typical office of size $18 \times 14 \times 3.5$ m^3 is considered, as illustrated in Figs. 1 and 2. If not otherwise specified, the network parameters used for the simulation setup are described in Table I.

First, we consider the scenario where the legitimate user is served by the nearest AP in its vicinity, without the implementation of the secrecy protected zone. Therefore, malicious eavesdroppers can be horizontally as close as possible to the AP that serves the legitimate user. By fixing the density of eavesdroppers ($\lambda_{\text{e}} = 0.2$), the secrecy outage probability at the typical legitimate user is evaluated at different values of the AP density, as shown in Fig. 3. It can be seen that, when λ_{a} is small, increasing the density of VLC APs can efficiently reduce the secrecy outage probability at the legitimate user. However, when λ_{a} is large, further increasing the density of VLC APs only slightly reduces the secrecy outage probability. For example, given that the target secrecy rate is $\bar{R}_{\text{s}} = 1$ bit/s/Hz, increasing λ_{a} from 0.1 to 1 can cause the secrecy outage probability to drop by 0.3. In comparison, when λ_{a} is increased from 1 to 10, the secrecy outage probability only drops by 0.1. Also, it is shown that a lower bound on the secrecy outage probability exists even if the density of VLC APs approaches infinity. This result is in agreement with Corollary 2. In Fig. 4, the ergodic secrecy rate is plotted against the density of APs. It is shown that the ergodic secrecy rate at the legitimate user drops when the density of eavesdroppers increases. Given a fixed density of eavesdroppers, increasing the density of VLC APs can efficiently enhance the ergodic secrecy rate when λ_{a} is small. However, the ergodic secrecy rate of the legitimate user tends to saturate at high AP densities. As a result, increasing the density of VLC APs when λ_{a} is large does not bring a significant incrementation to the ergodic secrecy rate. Instead, increasing the density of APs when λ_{a} is small is more meaningful.

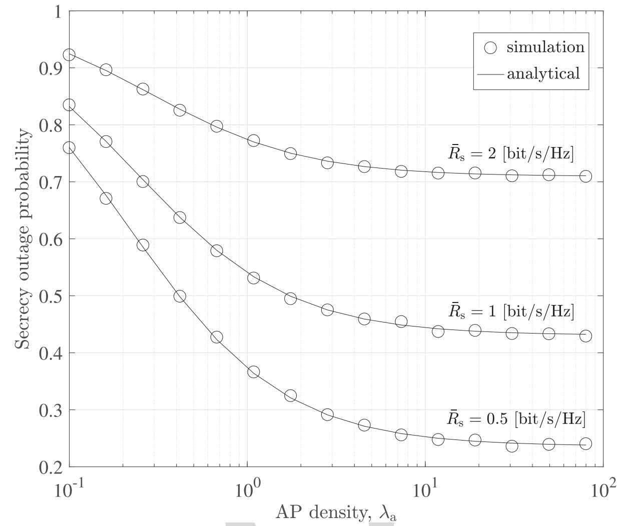

Fig. 3. Secrecy outage probability versus VLC AP density. The legitimate user is served by the nearest AP in its vicinity. $\lambda_{\text{e}} = 0.2$.

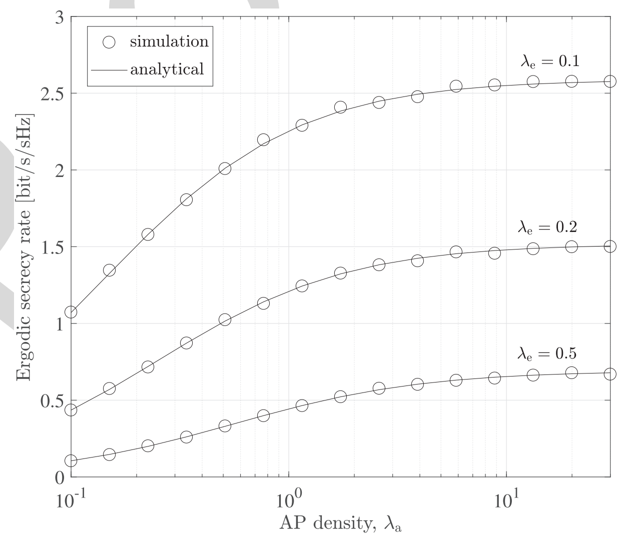

Fig. 4. Ergodic secrecy rate versus VLC AP density. The legitimate user is served by the nearest AP in its vicinity.

Second, we consider the scenario where the legitimate user is served by the optimal AP when APs are cooperated in the network. For the typical legitimate user, the optimal AP is not necessarily the nearest one, depending on the locations of potential eavesdroppers. With the cooperation among VLC APs, the optimal AP that brings the highest secrecy rate to the legitimate user is selected. For Monte Carlo simulations, the optimal AP is found out through the exhaustive search method. In Fig. 5, the secrecy outage probability is plotted against different eavesdropper densities, and it can be seen that the simulation results are well bounded by the derived analytical results. On the one hand, by assuming that the optimal AP is the nearest one, we underestimate the secrecy rate at the legitimate user. As a result, this assumption leads to an upper bound on the secrecy outage probability. On the other hand, the lower bound on the secrecy outage probability is

IEEE Proof

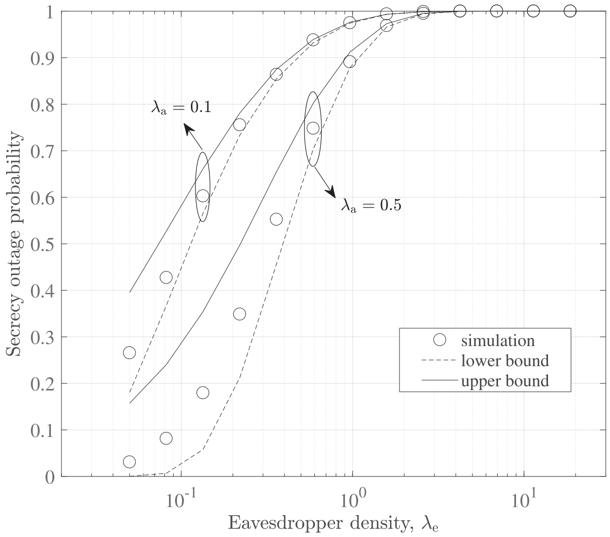

Fig. 5. Secrecy outage probability versus eavesdropper density. The legitimate user is served by the optimal AP. $\bar{R}_s = 0.5$ bit/s/Hz.

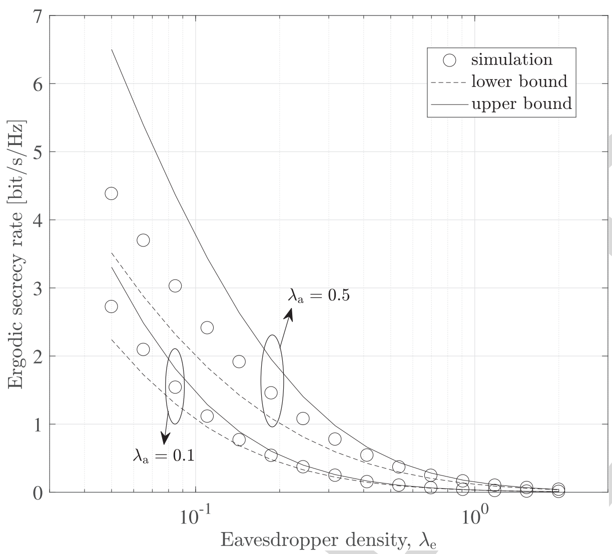

Fig. 6. Ergodic secrecy rate versus eavesdropper density. The legitimate user is served by the optimal AP.

obtained from Jensen's inequality, as described in Corollary 4. Comparing the lower bound with the upper bound, it can be seen that the lower bound is closer to the simulation results. It is also shown in Fig. 5 that both theoretical bounds on the secrecy outage probability are reasonably tight when the eavesdropper density is large. In Fig. 6, the ergodic secrecy rate at the legitimate user is computed for different values of the eavesdropper density. It should be noted that assuming the optimal AP is the nearest one gives the lower bound on the ergodic secrecy rate in Fig. 6, which corresponds to the upper bound on the secrecy outage probability in Fig. 5. Again, both analytical bounds become tighter as the eavesdropper density increases. Based on the results shown in Fig. 5 and Fig. 6, we can conclude that the optimal AP that maximizes the secrecy performance at the legitimate user is not necessarily the nearest one. To investigate deeper, we show in Fig. 7

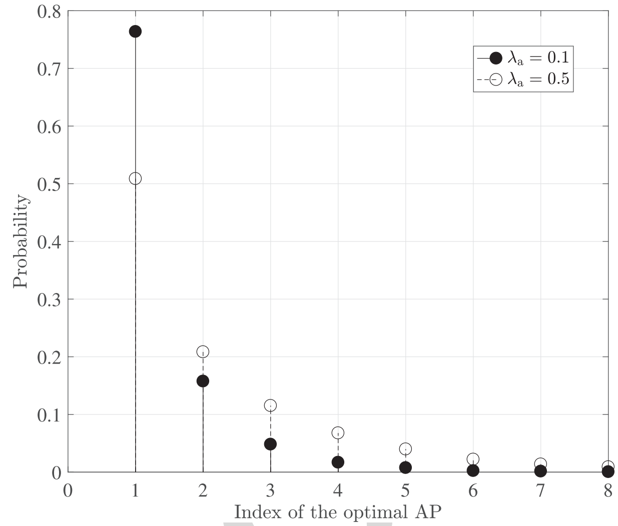

Fig. 7. Probability mass function (PMF) of the index of the optimal AP. $\lambda_e = 0.2$.

the probability mass function (PMF) of the index of the optimal AP that maximizes the secrecy rate at the legitimate user. Index i relates to the i-th nearest neighboring AP to the legitimate user. For example, index 1 corresponds to the nearest AP, index 2 corresponds to the second nearest AP, and so on. It is shown in Fig. 7 that, compared to other neighboring APs, the nearest AP is most likely the optimal one. However, it is also possible that the optimal AP is the second nearest, third nearest, etc. Fig. 7 also shows that with a smaller value of λ_a, it is more likely that the nearest AP is the optimal one, which therefore explains why the analytical bounds are tighter for smaller values of λ_a, as observed in Fig. 5 and Fig. 6.

Third, we consider the scenario where the legitimate user is served by the nearest AP in its vicinity, with the implementation of a secrecy protected zone. It is assumed that any malicious eavesdroppers that are inside the protected zone can be detected by the AP so that these eavesdroppers do not cause any secrecy information loss at the legitimate user. As a result, the secrecy information loss at the legitimate user is caused by the eavesdroppers that are outside the protected zone only. In Fig. 8, the secrecy outage probability is plotted against the density of VLC APs. It is shown that, for a given target secrecy rate, the secrecy outage probability decreases as the AP density increases. However, when λ_a is large, further increasing the density of VLC APs only slightly reduces the secrecy outage probability. Also, it is shown that there exists a lower bound on the secrecy outage probability when λ_a approaches infinity. After implementing a secrecy protected zone with radius D, the secrecy outage probability is reduced significantly. More specifically, when $\lambda_a = 1$, $\lambda_e = 0.2$ and the target secrecy rate is $\bar{R}_s = 2$ bit/s/Hz, implementing a secrecy protected zone with radius $D = 1$ m reduces the secrecy outage probability by 0.2. If the secrecy protected zone has a radius of $D = 2$ m, the secrecy outage probability can be reduced to nearly zero. It is also shown in Fig. 8 that, with a sufficiently large protected area, the secrecy outage probability is no longer bounded at the lower end, i.e., increasing the density of VLC

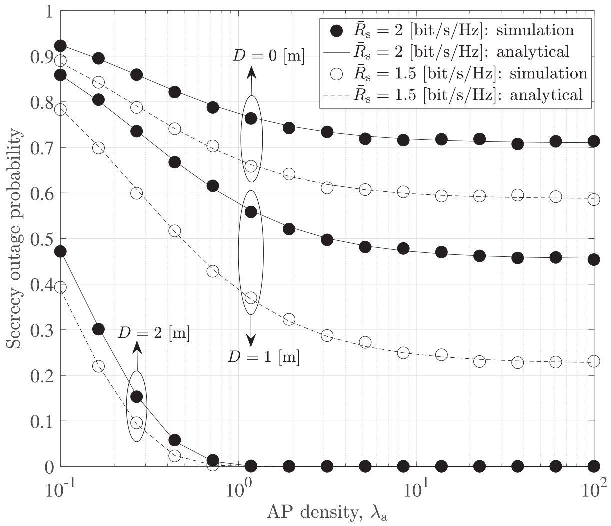

Fig. 8. Secrecy outage probability versus VLC AP density. The legitimate user is served by the nearest AP in its vicinity, and eavesdroppers are outside the protected zone with radius D. $\lambda_e = 0.2$.

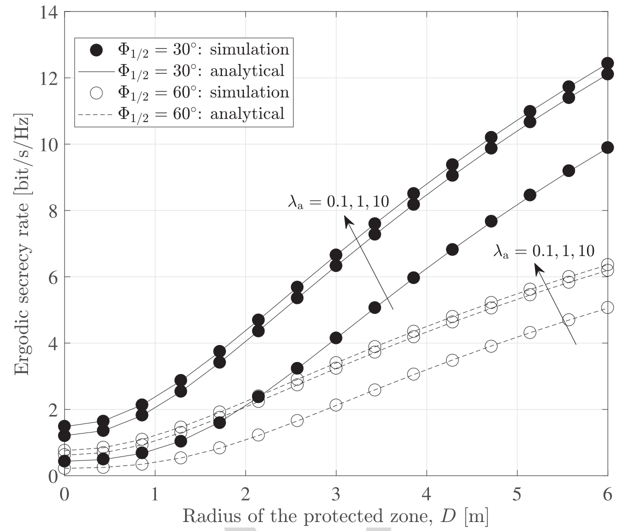

Fig. 10. Ergodic secrecy rate versus the radius of the protected zone. The legitimate user is served by the nearest AP in its vicinity. $\lambda_e = 0.2$.

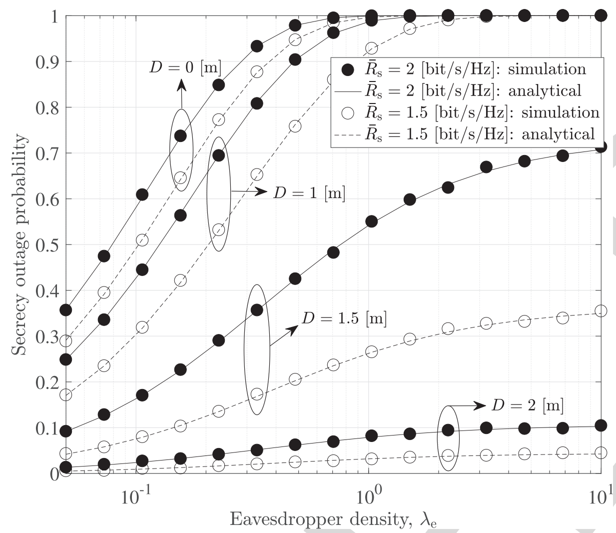

Fig. 9. Secrecy outage probability versus eavesdropper density. The legitimate user is served by the nearest AP in its vicinity, and eavesdroppers are outside the protected zone with radius D. $\lambda_a = 0.5$.

APs can efficiently reduce the secrecy outage probability to zero. In Fig. 9, we fix $\lambda_a = 0.5$ and evaluate the impact of the eavesdropper density on the secrecy outage probability. It can be seen that, without the protected zone, the secrecy outage probability can be as large as one if the eavesdropper density is sufficiently high. However, with the implementation of a protected zone, the worst-case scenario of the secrecy outage probability can be limited below a certain level. For example, when the target secrecy rate is $\bar{R}_s = 2$ bit/s/Hz and the protected zone has a radius of $D = 2$ m, the worst-case secrecy outage probability at the legitimate user does not exceed 0.12, regardless of the eavesdropper density. To further investigate the impact of the protected zone, we show in Fig. 10 the ergodic secrecy rate against the radius of the protected zone while fixing the eavesdropper density to $\lambda_e = 0.2$. The slope of the curve shows that a very small protected area brings only marginal improvement on the secrecy performance. However, by increasing the size of the protected zone further, the secrecy performance at the legitimate user can be enhanced significantly. Specifically, when $\lambda_a = 1$ and $\Phi_{1/2} = 30°$, increasing the radius of the protected zone from 0 to 1 m increases the ergodic secrecy rate by 0.6 bit/s/Hz. In contrast, increasing the radius of the protected zone from 1 to 2 m can increase the ergodic secrecy rate by 1.9 bit/s/Hz. In Fig. 10, it is also shown that using more directional LEDs, i.e., LEDs with a smaller semi-angle, enhances the secrecy performance at the legitimate user. However, the actual choice of LEDs should also take practical illumination requirements into consideration.

B. PPP Model vs. Grid Model

In the following, we compare the secrecy performance between the stochastic PPP model and the deterministic grid model. For the grid model, it implicitly assumes that the number of APs, as well as their locations in the network, are fixed and known. As shown in Fig. 11 and Fig. 12, we use a hexagonal-shaped grid to model the locations of APs within the same indoor space. A total number of 31 APs (represented by red triangles) are considered, and without loss of generality the secrecy performance is studied by focusing on the central hexagonal cell. A legitimate user (represented by the green circle) is randomly distributed within the central cell and is served by the central AP. The eavesdroppers (represented by blue squares) are assumed to follow a Poisson distribution with intensity λ_e. To allow for a fair comparison between the PPP model and the grid model, the density of APs in the PPP model is set to 0.12 so that the expected number of APs in the PPP model equals the total number of APs in the grid model. It can be seen from Fig. 11 that the PPP model and the grid model yield similar results for the secrecy outage probability. Both curves have similar shapes and trends, especially for higher target secrecy rates and with larger eavesdropper densities. In general, the grid model

IEEE Proof

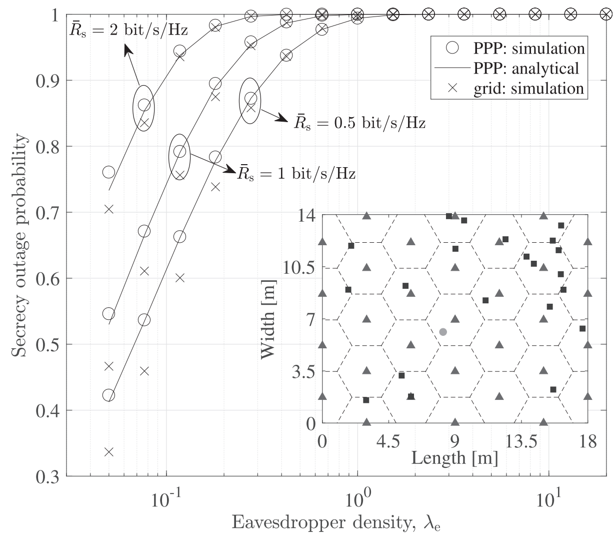

Fig. 11. Secrecy outage probability comparison between the PPP model and the grid model. $\lambda_a = 0.12$.

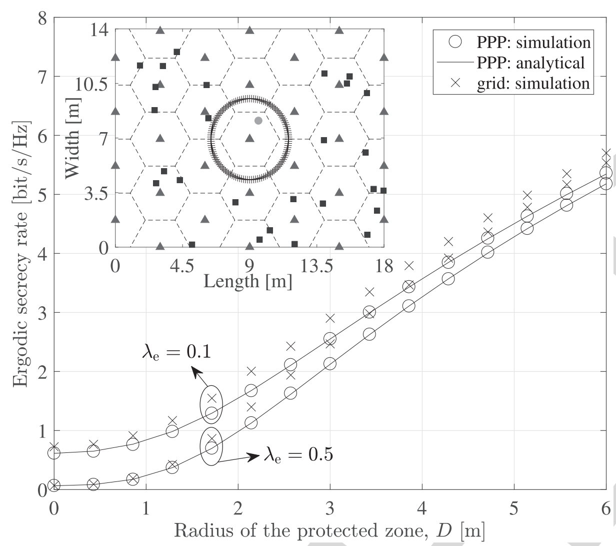

Fig. 12. Ergodic secrecy rate comparison between the PPP model and the grid model. $\lambda_a = 0.12$.

provides slightly superior coverage performance than the PPP model because of its more regularized cell shapes. With the implementation of a secrecy protected zone, we compare in Fig. 12 the achieved ergodic secrecy rate between the PPP model and the grid model. The configuration of the grid model in Fig. 12 is the same as that in Fig. 11, except that the eavesdroppers are prohibited in the circular protected zone centered around the central AP. Results show that both models yield close ergodic secrecy rates, especially for networks with more populated eavesdroppers.

VI. Conclusion

In this work, we studied the performance of physical-layer secrecy in a three-dimensional multiuser VLC network. With the use of mathematical tools from stochastic geometry, analytical expressions for the secrecy outage probability, the ergodic secrecy rate, as well as their lower and upper bounds, are derived in tractable forms and verified through Monte Carlo simulations. Impacts of AP cooperation and the implementation of a secrecy protected zone on the secrecy performance have also been investigated. Results show that cooperating neighboring APs can enhance the secrecy performance of VLC networks, but only to a limited extent. We also show that building a secrecy protected zone around the AP significantly improves the network secrecy performance.

Justifying the application of the PPP model to the performance analysis of VLC networks is an important research direction. Also, improved stochastic models may be developed in the future to more accurately capture the spatial distribution of APs in a real network deployment.

References

[1] 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.

[2] S. Dimitrov and H. Haas, *Principles of LED Light Communications: Towards Networked Li-Fi*. Cambridge, U.K.: Cambridge Univ. Press, 2015.

[3] H. Haas, L. Yin, Y. Wang, and C. Chen, "What is LiFi?" *J. Lightw. Technol.*, vol. 34, no. 6, pp. 1533–1544, Mar. 15, 2016.

[4] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.7: Short-Range Wireless Optical Communication Using Visible Light*, IEEE Computer Society, IEEE Standard 802.15.7-2011, 2011.

[5] X. Li, F. Jin, R. Zhang, J. Wang, Z. Xu, and L. Hanzo, "Users first: User-centric cluster formation for interference-mitigation in visible-light networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 39–53, Jan. 2016.

[6] H. Ma, L. Lampe, and S. Hranilovic, "Coordinated broadcasting for multiuser indoor visible light communication systems," *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3313–3324, Sep. 2015.

[7] L. Yin, W. O. Popoola, X. Wu, and H. Haas, "Performance evaluation of non-orthogonal multiple access in visible light communication," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5162–5175, Dec. 2016.

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

[9] I. Csiszär and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[10] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 539–543.

[11] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[12] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.

[13] O. O. Koyluoglu, C. E. Koksal, and H. El Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.

[14] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[15] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, Jun. 2013.

[16] A. Lapidoth, S. M. Moser, and M. A. Wigger, "On the capacity of free-space optical intensity channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4449–4461, Oct. 2009.

[17] J.-B. Wang, Q.-S. Hu, J. Wang, M. Chen, and J.-Y. Wang, "Tight bounds on channel capacity for dimmable visible light communications," *J. Lightw. Technol.*, vol. 31, no. 23, pp. 3771–3779, Dec. 1, 2013.

[18] A. Chaaban, J. M. Morvan, and M. S. Alouini, "Free-space optical communications: Capacity bounds, approximations, and a new sphere-packing perspective," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1176–1191, Mar. 2016.

IEEE Proof

[19] S. Dimitrov and H. Haas, “Information rate of OFDM-based optical wireless communication systems with nonlinear distortion,” *J. Lightw. Technol.*, vol. 31, no. 6, pp. 918–929, Mar. 15, 2013.

[20] 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.

[21] 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.

[22] G. Pan, J. Ye, and Z. Ding, “On secure VLC systems with spatially random terminals,” *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 492–495, Mar. 2016.

[23] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and its Applications*, 2nd ed. Hoboken, NJ, USA: Wiley, 1996.

[24] L. Zeng *et al.*, “High data rate multiple input multiple output (MIMO) optical wireless communications using white LED lighting,” *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1654–1662, Dec. 2009.

[25] J. Grubor, S. Randel, K. D. Langer, and J. W. Walewski, “Broadband information broadcasting using LED-based interior lighting,” *J. Lightw. Technol.*, vol. 26, no. 24, pp. 3883–3892, Dec. 15, 2008.

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

[27] L. Hanzo, H. Haas, S. Imre, D. O’Brien, M. Rupp, and L. Gyongyosi, “Wireless myths, realities, and futures: From 3G/4G to optical and quantum wireless,” *Proc. IEEE*, vol. 100, pp. 1853–1888, May 2012.

[28] C. Chen, S. Videv, D. Tsonev, and H. Haas, “Fractional frequency reuse in DCO-OFDM-based optical attocell networks,” *J. Lightw. Technol.*, vol. 33, no. 19, pp. 3986–4000, Oct. 1, 2015.

[29] S. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

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

[31] M. Haenggi, “On distances in uniformly random networks,” *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3584–3586, Oct. 2005.

[32] S. Srinivasa and M. Haenggi, “Distance distributions in finite uniformly random networks: Theory and applications,” *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 940–949, Feb. 2010.

[33] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

[34] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, “PHY layer security based on protected zone and artificial noise,” *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2013.

Liang Yin received the B.Eng. degree (Hons.) in electronics and electrical engineering from the University of Edinburgh, Edinburgh, U.K., in 2014, where he is currently pursuing the Ph.D. degree in electrical engineering. His research interests are in visible light communication and positioning, multi-user networking, and wireless network performance analysis. He received the Class Medal Award and IET Prize Award from the University of Edinburgh.

Harald Haas (S’98–AM’00–M’03–SM’17) received the Ph.D. degree from the University of Edinburgh in 2001. He currently holds the Chair of mobile communications with the University of Edinburgh, and is the Initiator, Co-Founder, and the Chief Scientific Officer of pureLiFi Ltd and the Director of the LiFi Research and Development Center, University of Edinburgh. He has authored 400 conference and journal papers including a paper in Science and co-authored a book entitled *Principles of LED Light Communications Towards Networked Li-Fi* (Cambridge University Press, 2015). His main research interests are in optical wireless communications, hybrid optical wireless and RF communications, spatial modulation, and interference coordination in wireless networks. He first introduced and coined spatial modulation and LiFi. LiFi was listed among the 50 best inventions in TIME Magazine 2011. He was an invited speaker with TED Global 2011, and his talk on Wireless Data from Every Light Bulb has been watched online over 2.4 million times. He gave a second TED Global lecture in 2015 on the use of solar cells as LiFi data detectors and energy harvesters. This has been viewed online over 1.8 million times. He was elected as a Fellow of the Royal Society of Edinburgh in 2017. In 2012 and 2017, he was the recipient of the prestigious Established Career Fellowship from the Engineering and Physical Sciences Research Council (EPSRC) within Information and Communications Technology in the U.K. In 2014, he was selected by EPSRC as one of ten Recognising Inspirational Scientists and Engineers Leaders in the U.K. He was the co-recipient of the EURASIP Best Paper Award for the *Journal on Wireless Communications and Networking* in 2015, and co-recipient of the Jack Neubauer Memorial Award of the IEEE VEHICULAR TECHNOLOGY SOCIETY. In 2016, he was a recipient of the outstanding achievement award from the International Solid State Lighting Alliance. He was the co-recipient of recent Best Paper Awards at VTC, 2013, VTC 2015, ICC 2016, and ICC 2017. He is currently an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE JOURNAL OF LIGHTWAVE TECHNOLOGIES.

IEEE Proof