IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 13, 2021, accepted August 22, 2021, date of publication August 30, 2021, date of current version September 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3108727

Realistic Secrecy Performance Analysis for LiFi Systems

HANAA ABUMARSHOUD[1], MOHAMMAD DEHGHANI SOLTANI[2], MAJID SAFARI[2], (Senior Member, IEEE), AND HARALD HAAS[1], (Fellow, IEEE)

[1]LiFi Research and Development Centre, Technology and Innovation Centre, Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow G1 1XQ, U.K.

[2]School of Engineering, Institute for Digital Communications, The University of Edinburgh, Edinburgh EH8 9YL, U.K.

Corresponding author: Hanaa Abumarshoud (hanaa.abumarshoud@strath.ac.uk)

This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/P003974/1 [U.K. Programmable Fixed and Mobile Internet Infrastructure (INITIATE)]. The work of Harald Haas was supported by EPSRC through the Established Career Fellowship under Grant EP/R007101/1, in part by The Wolfson Foundation, and in part by The Royal Society.

ABSTRACT This paper studies the secrecy performance of light-fidelity (LiFi) networks under the consideration of random device orientation and partial knowledge of the eavesdroppers' channel state information. Particularly, the secrecy capacity and secrecy outage probability are analysed for the case of a single eavesdropper as well as for the case of multiple eavesdroppers. Moreover, a machine learning based access point (AP) selection algorithm is presented with the objective of maximising the secrecy capacity of legitimate users. Our results show that optimising the AP selection while taking into account the random behaviour of the optical channel results in a significant enhancement in the achievable secrecy performance. In fact, using the derived realistic secrecy expressions as the basis for AP selection results in up to 30% secrecy capacity enhancement compared to the limited assumption of fixed orientation.

INDEX TERMS Light-fidelity (LiFi), physical layer security (PLS), random orientation, secrecy capacity.

I. INTRODUCTION

As a promising 5G enabler, optical wireless communication (OWC) networks allow the use of a huge unregulated spectrum, which includes infrared (IR) and visible light, for the purpose of wireless data communications. Hence, this emerging technology is envisioned to handle a large portion of future mobile traffic [1]. Compared to radio frequency (RF) networks, OWC offers considerable advantages including high energy efficiency and high speed connectivity. OWC inherently provides enhanced security in comparison to RF networks as the light does not penetrate through walls and opaque objects. However, security problems emerge due to the broadcast feature, which makes OWC as vulnerable as other RF wireless systems if eavesdroppers exist within the coverage area of the access point (AP) of interest. It is noted that OWC links differ from RF links in that the optical channel input is strictly non-negative due to the requirements of intensity modulation. Moreover, unlike RF links that are typically modelled as Gaussian inputs with average power constraints, OWC channels are modelled as amplitude constrained inputs. Investigating the secrecy performance of amplitude-constrained wiretap channels is relatively new compared to the massive body of literature available on average power-constrained Gaussian wiretap channels [2]. In order to ensure a robust and secure connection for legitimate users, various physical layer security (PLS) techniques can be employed. However, it is not straightforward to directly develop the PLS solutions used in RF systems for OWC systems. This is due to the natural distinctions in OWC systems which can be summarised as follows: 1) the transmitted signal in OWC is required to be real and positive in order to allow for intensity modulation at the light-emitting diodes (LEDs), 2) the limited dynamic range of the LEDs imposes a peak-power constraint on the channel input, this implies that the information bearing signal is bounded and the capacity achieving input distribution cannot be Gaussian, and 3) the optical channel gain is not subject to fading characteristics such as RF channels but rather dependant on the user behaviour statistics such as the location and orientation of the device [3]. It is, thus, critical to study and evaluate the secrecy performance under these specifications in order to gain better insights on the application of PLS in OWC systems.

A number of surveys have been reported in the literature regarding PLS in OWC systems [4], [5]. In [4], the PLS in OWC, including free-space optical (FSO) systems and visible

The associate editor coordinating the review of this manuscript and approving it for publication was Yan Huo.

light communication (VLC), has been reviewed. A survey has recently been written on PLS of VLC [5]. Various VLC system configurations, including single-input-single-output (SISO) and multiple-input-multiple-output (MIMO), as well as hybrid RF/VLC networks have been considered and the secrecy capacity for each of them has been presented. The work in [6] investigated techniques and solutions to enhance the security and provide a secure communication in VLC. In this regard, PLS techniques can be classified into three main groups: I) friendly jamming, II) precoding, and III) combined friendly jamming and precoding. In [6], a multiple-input-single-output (MISO) wiretap VLC channel is considered. The channel is modeled as deterministic, real-valued, and Gaussian, subject to amplitude constraints. Null-steering and artificial noise strategies are used to achieve positive secrecy rates when the eavesdropper's channel state information (CSI) is perfectly known and entirely unknown to the transmitter, respectively. In both scenarios, the legitimate receiver's CSI is available to the transmitter. In [7], a friendly jamming method is introduced to enhance the PLS in a VLC system. Both cases of known and uncertain CSI of the eavesdropper at the jammer side are considered and robust beamforming schemes are proposed with the aim of maximising the achievable secrecy rate. Both jamming and transmit beamforming techniques are deployed in [8] to enhance the security of PLS in a MISO VLC system with multiple eavesdroppers. The work in [9] studies the secrecy performance of a multi-user MIMO VLC system. The optical channel is modeled as deterministic and real-valued and it is assumed that the AP has perfect knowledge of the channel gain of all users, including eavesdroppers. To achieve better insights on the inherent security capabilities in VLC systems, there is a need to investigate the secrecy performance under more realistic conditions. Towards this direction, the secrecy outage probability of the VLC downlink is characterised in [10] considering the randomness of the locations of the legitimate user and eavesdroppers. Moreover, the impact of imperfect CSI on the secrecy capacity is evaluated in [11], where the legitimate users are assumed to be uniformly distributed in a protected zone around the AP.

Light-fidelity (LiFi), as a subset of OWC, is a high-speed, bidirectional, and fully networked wireless communication technology in which visible light and infrared are used for downlink and uplink transmissions, respectively [12]–[14]. Since LiFi supports user mobility, the optical channels are highly influenced by user behavior induced variations such as random device orientation [15]. As a result, it is essential to assess the impact of user behavior on the secrecy performance of LiFi systems. All PLS studies in LiFi assume that the receiver's device always faces vertically upward and its orientation is constant over time, resulting in a deterministic behaviour for the optical channel, i.e., the channel gain value is fixed for given AP-user locations. However, in practice, this assumption can be only valid for fixed devices such as laptops with LiFi dongles. Mobile users, on the contrary, tend to tilt their smartphones in random ways, resulting in frequent changes in the device orientation. These variations were shown to have a significant effect on the received signal strength at the user terminals [16] and, thus, need to be taken into consideration for proper PLS implementations.

In light of the above discussion, we summarise the paper contributions as follows:

- We derive lower bounds for the secrecy capacity and upper bounds for the secrecy outage probability in LiFi systems with the existence of a single eavesdropper taking into consideration the random behaviour of the optical channel, i.e., random receiver orientation as well as the imperfect knowledge of the eavesdroppers' exact CSI.
- We extend the secrecy capacity and secrecy outage probability analysis for the case of colluding eavesdroppers, where multiple illegitimate users combine their isolated observations to eavesdrop the legitimate user's link.
- We propose a machine learning (ML)-based AP selection algorithm to demonstrate that employing the proposed secrecy measures as the basis for AP selection provides significant enhancement in the secrecy performance of LiFi systems.

The rest of the paper is organised as follows. The system model is presented in Section II, Section III and Section IV provide secrecy capacity and secrecy outage probability analysis for the case of a single eavesdropper and multiple eavesdroppers, respectively, while Section V provides asymptotic secrecy capacity analysis. In Section VI, we discuss the secrecy-based AP selection algorithm and we show the simulation and analytic results in Section VII. Finally, the paper is concluded in Section VIII.

II. SYSTEM MODEL

A. LiFi SYSTEM CONFIGURATION

We consider an indoor LiFi network, where multiple LEDs are installed on the ceiling. It is assumed that the LEDs are point sources that follow Lambertian patterns and work in the linear range of the current-to-power curve. The LEDs are assumed to be facing vertically downward. The LED APs aim to transmit confidential messages to legitimate users in the presence of one or more eavesdroppers existing within the LiFi cells, also known as *attocells* [17]. Fig. 1 shows a general configuration of the indoor LiFi network with both legitimate and eavesdropper users. When an AP transmits a signal to legitimate users, passive eavesdroppers can also receive the signal and decode it. We refer to the AP, legitimate user, and eavesdropper as Alice, Bob, and Eve, respectively. At the receiver side, a photodiode (PD) is mounted on the user equipment (UE) to detect the received signal by means of direct detection. The orientation of UEs is assumed to follow a Laplace distribution as shown in [18] for static users. The received signals at Bob and Eve can be expressed as:

$$y_B = h_B x + z_B, \tag{1}$$

and

$$y_E = h_E x + z_E, \tag{2}$$

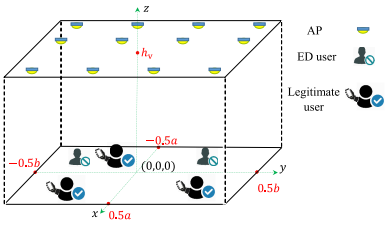

FIGURE 1. System configuration: a LiFi system with multiple APs, legitimate users and eavesdroppers (ED users).

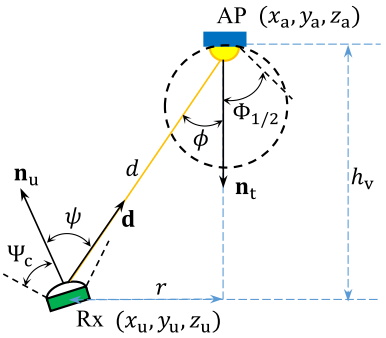

FIGURE 2. LOS propagation model.

respectively, where x is the transmitted signal, h_B and h_E denote the channel gain of Bob and Eve, respectively. Also, $z_B \sim \mathcal{N}(0, \sigma_B^2)$ and $z_E \sim \mathcal{N}(0, \sigma_E^2)$ denote the additive white Gaussian noise at Bob and Eve with variances σ_B^2 and σ_E^2, respectively. Since LiFi systems employ intensity modulation at the transmitter and direct detection at the receiver, the optical signal x follows the following constraint:

$$x \geq 0, \tag{3}$$

which states that the signal must be strictly non-negative. Moreover, for practical considerations, the average signal power is constrained by the nominal optical intensity in order to guarantee that the required illumination level is satisfied, which can be mathematically expressed as:

$$E(x) = \zeta P, \tag{4}$$

where $\zeta \in (0, 1]$ is the power dimming factor and P is the LED nominal optical power.

B. LIGHT PROPAGATION MODEL

We focus on the downlink transmission of a LiFi network, where the communication is based on a line-of-sight (LOS) link. It is assumed that the attocells are far from the walls so that the diffuse links are negligible [19]. The LOS link geometry is illustrated in Fig. 2. The direct current (DC) gain of the LOS link between the AP and the receiver is given as follows [3]:

$$H_{LOS} = \frac{(m+1)A}{2\pi d^2} \cos^m\phi \; g_f g(\psi) \cos\psi \; \text{rect}\left(\frac{\psi}{\Psi_c}\right), \tag{5}$$

where d is the Euclidean distance between the UE and the AP; A is the physical area of the detector; ϕ and ψ are the angle of radiance with respect to the axis normal to the AP plane, and the angle of incidence with respect to the axis normal to the receiver plane, respectively. Furthermore, $\text{rect}(\frac{\psi}{\Psi_c}) = 1$ for $0 \leq \psi \leq \Psi_c$ and 0 otherwise. The gain of the optical filter is denoted by g_f, and Ψ_c is the receiver field of view (FOV). The optical concentrator, $g(\psi)$, is given as:

$$g(\psi) = \begin{cases} \dfrac{\varsigma^2}{\sin^2\Psi_c}, & 0 \leq \psi \leq \Psi_c \\ 0, & o.w, \end{cases} \tag{6}$$

where ς stands for the refractive index. Also, m is the Lambertian order which is given by:

$$m = -\frac{1}{\log_2(\cos\Phi_{1/2})}, \tag{7}$$

where $\Phi_{1/2}$ is the half-intensity angle [3]. The radiance angle ϕ and the incidence angle ψ of the AP and the receiver can be calculated using the rules from analytical geometry as:

$$\cos\phi = \frac{-d \cdot n_t}{\|d\|}, \tag{8a}$$

$$\cos\psi = \frac{d \cdot n_u}{\|d\|}, \tag{8b}$$

where $n_t = [0, 0, -1]^{\text{T}}$ and n_u are the normal vectors at the AP and the receiver planes, respectively and d denotes the distance vector from the receiver to the AP. The symbols $\cdot$ and $\|\cdot\|$ denote the inner product and the Euclidean norm operators, respectively. Also, $(.)^{\text{T}}$ denotes the transpose operator.

C. RANDOM ORIENTATION

Device orientation is an important factor that can influence the performance of the UEs significantly. Many studies have ignored the impact of device orientation in their analysis. The statistics of device orientation has been derived through a set of experimental measurements for both sitting and walking activities in [18], [20]. The normal vector, n_u, can be expressed in terms of polar angle, θ, and azimuth angle, ω, in the spherical coordinates as shown in Fig 3. Accordingly, we have:

$$n_u = [\sin(\theta)\cos(\omega), \sin(\theta)\sin(\omega), \cos(\theta)]^T. \tag{9}$$

The azimuth angle ω shows the angle between the positive direction of the X axis and the projection of n_u in the XY-plane. Here, we define $\Omega = \omega + \pi$ as the facing direction of the user [18]. For the rest of the paper, we use this angle as it provides a better physical concept.

Substituting (9) in (8a) and (5), it can be inferred that for a fixed UE location and facing direction of the user, the channel gain depends on the polar angle θ. The experimental measurements reported in [18] confirmed that the polar angle, θ, follows a Laplace distribution for sitting activities with the mean and variance of $\mu_\theta = 41°$ and $\sigma_\theta = 7.68°$, respectively. Therefore, the probability density function (PDF) of the polar angle is given as [18]:

$$f(\theta) = \frac{\exp\left(-\frac{|\theta-\mu_\theta|}{b_\theta}\right)}{2b_\theta}. \tag{10}$$

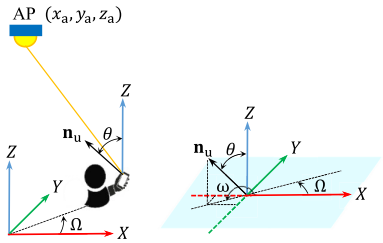

FIGURE 3. Geometry of a randomly-oriented UE and its spherical coordinates.

Based on the Laplace distribution for θ, it is shown that the channel gain follows a truncated Laplace distribution as follows [18]:

$$f_{\mathrm{H}}(h) = \frac{\exp\left(-\frac{|h-\mu_{\mathrm{H}}|}{b_{\mathrm{H}}}\right)}{b_{\mathrm{H}}\left(2-\exp\left(-\frac{h_{\max}-\mu_{\mathrm{H}}}{b_{\mathrm{H}}}\right)\right)} + F_{\theta}\left(\theta_0\right)\delta(h), \quad (11)$$

where $h_{min} \leq h \leq h_{max}$. The mean and scale parameter of the channel gain are given as:

$$\mu_{\mathrm{H}} = \frac{H_0}{d^{m+2}}\left(\lambda_1 \sin\mu_\theta + \lambda_2 \cos\mu_\theta\right), \quad (12a)$$

$$b_{\mathrm{H}} = \frac{H_0}{d^{m+2}} b_\theta \left|\lambda_1 \cos\mu_\theta - \lambda_2 \sin\mu_\theta\right|, \quad (12b)$$

where $H_0 = \frac{(m+1)A g_f \varsigma^2 h_v^m}{2\pi \sin^2 \Psi_c}$. The factors λ_1 and λ_2 depends on the UE location and facing direction of the user, which are given as:

$$\lambda_1 = \frac{r}{d}\cos\left(\Omega - \tan^{-1}\left(\frac{y_{\mathrm{u}}-y_{\mathrm{a}}}{x_{\mathrm{u}}-x_{\mathrm{a}}}\right)\right), \quad (13a)$$

$$\lambda_2 = \frac{h_v}{d}, \quad (13b)$$

where h_v and r are respectively the vertical and horizontal distance between the UE and the AP as shown in Fig. 2. Note that in (11), $F_\theta(\theta_0) = \int_0^{\theta_0} f(\theta)d\theta$, where $\theta \leq \theta_0$ results in $\psi \leq \Psi_c$, and therefore, the channel gain becomes zero. The angle θ_0 is given as [21]:

$$\theta_0 = \cos^{-1}\left(\frac{\cos\Psi_{\mathrm{c}}}{\sqrt{\lambda_1^2+\lambda_2^2}}\right) + \tan^{-1}\left(\frac{\lambda_1}{\lambda_2}\right). \quad (14)$$

Finally, it should be noted that the support range of the channel gain in (11) is $h_{min} \leq h \leq h_{max}$ with

$$h_{\min} = \begin{cases} \frac{H_0}{d^{m+2}}\cos\Psi_{\mathrm{c}}, & \cos\ \psi < \cos\Psi_{\mathrm{c}} \\ \frac{H_0}{d^{m+2}}\min\{\lambda_1,\lambda_2\}, & \text{o.w,} \end{cases} \quad (15a)$$

$$h_{\max} = \begin{cases} \frac{H_0}{d^{m+2}}\lambda_2, & \text{if } \lambda_1 < 0 \\ \frac{H_0}{d^{m+2}}\sqrt{\lambda_1^2+\lambda_2^2}, & \text{if } \lambda_1 \geq 0. \end{cases} \quad (15b)$$

III. SECRECY EVALUATION FOR THE CASE OF A SINGLE EAVESDROPPER

In this section, we provide analytical expressions for the secrecy capacity and secrecy outage probability with the existence of a single eavesdropper. We assume a LiFi system with an average optical power constraint as described in Section II. We refer to the AP, legitimate user, and eavesdropper as Alice, Bob, and Eve, respectively. Moreover, we assume that the AP acquires accurate CSI of the legitimate user's channel gain, h_B, as well as an estimate of the CSI of any potential eavesdroppers. This assumption is adopted because eavesdroppers are usually passive users that do not share their information with the APs. The estimated CSI of the eavesdropper's channel gain can be obtained with the aid of built-in motion sensors deployed in LED fixtures, as assumed in [22]. More specifically, we assume that the AP acquires imperfect CSI estimate of h_E, denoted as $\hat{h}_E$, such that:

$$\hat{h}_E = h_E + \delta_E, \quad (16)$$

where δ_E is a zero-mean Gaussian distributed random variable, i.e., $\delta_E \sim \mathcal{N}(0, \sigma^2)$. Consequently, we can say that the estimated CSI of Eve at Alice follows a Gaussian distribution such that:

$$\hat{h}_E \sim \mathcal{N}(\mu, \sigma^2), \quad (17)$$

where μ is the expected value of the estimated channel gain of Eve. It is noted that this noisy stochastic error model has been adopted as a reasonable model for imperfect CSI in indoor VLC systems in [23]–[25].

In the following, we present the secrecy analysis under the assumption of a deterministic channel gain of Bob. We then move to a more realistic assumption which includes the effect of random receiver orientation. It is noted that we present the expressions of the secrecy capacity and the secrecy outage probability as calculated with the knowledge available at the APs, i.e. the calculations are based on the imperfect CSI of Eve. This is because those expressions are utilised for the PLS decisions at the APs. The goal is to optimise the secrecy capacity of the system based on the available imperfect CSI. Similarly, by assuming random orientation of Bob's device, we can achieve robust PLS design for the worst case scenarios.

A. SECRECY CALCULATIONS WITH IMPERFECT CSI OF EVE

Proposition 1: For the case of a single eavesdropper with a normally distributed CSI error, $\hat{h}_E \sim \mathcal{N}(h_E, \sigma^2)$ the secrecy capacity, which defined as the difference between Bob and Eve's channel capacities, can be lower bounded as:

$$\mathcal{C}_s^{1_E} \geq \frac{1}{4}\ln\left(\frac{e\zeta^2P^2h_B^2 + 2\pi\sigma_B^2}{2\pi\sigma_B^2\sigma_E^{-2}}\right)\Upsilon(\kappa) - \frac{1}{2}\ln\left(\zeta^2P^2(\mu^2+\sigma^2)+\sigma_E^2\right), \quad (18)$$

where κ is the maximum value of the square of Eve's channel gain, and $\Upsilon(\kappa) = erf\left(\frac{\sqrt{\kappa}-\mu}{\sqrt{2\sigma^2}}\right) + erf\left(\frac{\sqrt{\kappa}+\mu}{\sqrt{2\sigma^2}}\right)$ with $erf(w)$

representing the error function evaluated as $\frac{1}{\sqrt{\pi}}\int_{t=-w}^{w} e^{-t^2}dt$. *Also,* σ_B^2 *and* σ_E^2 *denote the variance of receiver noise at Bob and Eve, respectively, and* $\zeta \in (0, 1]$ *is the dimming factor.*

Proof: The proof is provided in Appendix A. □

Corollary 1: The secrecy outage probability, defined as the probability that the secrecy capacity falls below a predetermined threshold Q in the presence of a single eavesdropper, can be upper-bounded by:

$$\mathcal{P}_{out}^{1_E} \leq 1 + \frac{1}{2}erf\left(\frac{\mu - \sqrt{\Xi}}{\sqrt{2\sigma^2}}\right) - \frac{1}{2}erf\left(\frac{\mu + \sqrt{\Xi}}{\sqrt{2\sigma^2}}\right), \quad (19)$$

where $\Xi = \frac{\sigma_E^2}{\zeta^2 P^2}\left(\frac{e^{-2Q}}{2\pi\sigma_B^2}(e\zeta^2 P^2 h_B^2 + 2\pi\sigma_B^2) - 1\right)$ *and* Q *denotes the outage threshold, i.e., outage occurs if* $\mathcal{C}_s^{1_E} < Q$.

Proof: The proof is provided in Appendix B. □

Proposition 1 and Corollary 1 provide the basis for the secrecy performance evaluation at the AP. It is noted that the provided secrecy outage probability expression is valid for any threshold value Q, and that the decision on the suitable threshold depends on the secrecy design of the system, i.e., the sensitivity of the content and the probability of eavesdropping. Moreover, the provided expressions are generic for any locations of Bob and Eve. In the following subsection, we investigate the effect of random receiver orientation on the secrecy capacity and secrecy outage probability calculations.

B. SECRECY CALCULATIONS WITH RANDOM RECEIVER ORIENTATION

Up to this point, we have not considered the random orientation of Bob's device, i.e., Bob's device has been considered to have a deterministic fixed orientation (i.e., vertically upward orientation). In the following, we derive the secrecy performance metrics taking into account the random receiver orientation model in Section II-C.

Proposition 2: Considering random receiver orientation, the secrecy capacity, which is defined as the difference between Bob and Eve's channel capacities with the existence of a single eavesdropper, can be lower-bounded as:

$$\begin{aligned}
&\tilde{\mathcal{C}}_s^{1_E} \\
&\geq \frac{1}{4}\Upsilon(\kappa) b_H \iota_1 e^{-\frac{\mu_H}{b_H}}\left(e^{\frac{\mu_H}{b_H}}\log\left(\frac{e\mu_H^2 P^2\zeta^2}{2\pi\sigma_B^2}\right) - 2Ei\left(\frac{\mu_H}{b_H}\right)\right) \\
&\quad + \frac{1}{4}\Upsilon(\kappa) b_H \iota_1 e^{\frac{\mu_H-\kappa_H}{b_H}} \\
&\quad \times \left(2e^{\frac{\kappa_H}{b_H}}Ei\left(-\frac{\kappa_H}{b_H}\right) - \log\left(\frac{e\kappa_H^2 P^2\zeta^2}{2\pi\sigma_B^2}\right)\right) \\
&\quad - \frac{1}{4}\Upsilon(\kappa) b_H \iota_1 \left(2e^{\frac{m\mu_H}{b_H}}Ei\left(-\frac{\mu_H}{b_H}\right) - \log\left(\frac{e\mu_H^2 P^2\zeta^2}{2\pi\sigma_B^2}\right)\right) \\
&\quad + b_H \iota_1 \left(-e^{\frac{\mu_H-\kappa_H}{b_H}} - e^{-\frac{\mu_H}{b_H}} + 2\right) \\
&\quad \times \left(\frac{1}{4}\Upsilon(\kappa)\log\left(\sigma_E^2\right) - \frac{1}{2}\log\left(P^2\zeta^2\left(\mu^2 + s^2\right) + \sigma_E^2\right)\right),
\end{aligned} \quad (20)$$

where $\iota_1 = \frac{1}{b_H\left(2-\exp\left(-\frac{h_{\max}-\mu_H}{b_H}\right)\right)}$ *and* κ_H *is the maximum value of* h_B.

Proof: The proof is provided in Appendix C. □

Corollary 2: For a high signal-to-noise-ration (SNR) scenario and when considering random orientation of Bob, the secrecy outage probability, defined as the probability that the secrecy capacity falls below a predetermined threshold Q in the presence of a single eavesdropper, can be approximated as:

$$\begin{aligned}
&\tilde{\mathcal{P}}_{out}^{1_E} \\
&\approx \iota_3 b_H \iota_1 e^{\frac{\frac{s^2}{2\iota_2^2} + b_H\kappa_H}{b_H^2}} \\
&\quad \times \left(-\left(\mathcal{L}_4 e^{\frac{\mu}{\iota_2 b_H}} + \mathcal{L}_5 e^{\frac{3\mu}{\iota_2 b_H}}\right) + e^{\frac{2\mu_H}{b_H}}\left(\mathcal{L}_6 e^{\frac{1\mu}{\iota_2 b_H}} + \mathcal{L}_7 e^{\frac{3\mu}{\iota_2 b_H}}\right)\right) \\
&\quad + \iota_3 b_H \iota_1 e^{\frac{2\mu}{\iota_2 b_H}}\left(e^{\frac{\kappa_H}{b_H}}\left(\mathcal{L}_2 e^{\frac{\mu_H}{b_H}} + \mathcal{L}_3 e^{\frac{1.\mu_H}{b_H}} - 1\right) + \mathcal{L}_1 e^{\frac{2\mu_H}{b_H}}\right),
\end{aligned} \quad (21)$$

where

$$\begin{aligned}
\iota_2 &= \sqrt{\frac{\sigma_E^2 e^{-2Q+1}}{2\pi\sigma_B^2}} \\
\iota_3 &= \frac{\iota_2\kappa_H - \iota_2\mu_H - 2\mu}{\iota_2 b_H}, \\
\mathcal{L}_1 &= -\frac{1}{2}erf\left(\frac{\mu - \iota_2\kappa_H}{\sqrt{2}\sqrt{\sigma^2}}\right) + \frac{1}{2}erf\left(\frac{\iota_2\kappa_H + \mu}{\sqrt{2}\sqrt{\sigma^2}}\right) - 1, \\
\mathcal{L}_2 &= \frac{1}{2}erf\left(\frac{\mu - \iota_2\mu_H}{\sqrt{2\sigma^2}}\right) + \frac{1}{2}erf\left(\frac{\iota_2\mu_H + \mu}{\sqrt{2\sigma^2}}\right) + 1, \\
\mathcal{L}_3 &= \frac{1}{2}erf\left(\frac{\mu - \iota_2\mu_H}{\sqrt{2s^2}}\right) - \frac{1}{2}erf\left(\frac{\iota_2\mu_H + \mu}{\sqrt{2s^2}}\right) + 1, \\
\mathcal{L}_4 &= \frac{1}{2}erf\left(\frac{\iota_2 b_H(-\iota_2\mu_H - \mu) + \sqrt{2}s^2}{\iota_2 b_H\sqrt{2s^2}}\right) \\
&\quad - \frac{1}{2}erf\left(\frac{\sigma^2 - \iota_2 b_H\mu}{\iota_2 b_H\sqrt{2s^2}}\right), \\
\mathcal{L}_5 &= \frac{1}{2}erf\left(\frac{\iota_2 b_H(\mu - \iota_2\mu_H) + \sigma^2}{\iota_2 b_H\sqrt{2\sigma^2}}\right) \\
&\quad - \frac{1}{2}erf\left(\frac{\iota_2 b_H\mu + \sigma^2}{\iota_2 b_H\sqrt{2\sigma^2}}\right), \\
\mathcal{L}_6 &= \frac{1}{2}erf\left(\frac{\iota_2 b_H(\iota_2\mu_H - \mu) + \sigma^2}{\sqrt{2}\iota_2 b_H\sqrt{\sigma^2}}\right) \\
&\quad - \frac{1}{2}erf\left(\frac{\iota_2 b_H(\iota_2\kappa_H - \mu) + \sigma^2}{\sqrt{2}\iota_2 b_H\sqrt{\sigma^2}}\right), \\
\mathcal{L}_7 &= \frac{1}{2}erf\left(\frac{\iota_2 b_H(\iota_2\mu_H + \mu) + \sigma^2}{\sqrt{2}\iota_2 b_H\sqrt{\sigma^2}}\right) \\
&\quad - \frac{1}{2}erf\left(\frac{\iota_2 b_H(\iota_2\kappa_H + \mu) + \sigma^2}{\sqrt{2}\iota_2 b_H\sqrt{\sigma^2}}\right).
\end{aligned}$$

Proof: The proof is provided in Appendix D. □

IV. SECRECY EVALUATION FOR THE CASE OF MULTIPLE COLLUDING EAVESDROPPERS

In this section, we focus on the derivation of the secrecy performance metrics with the assumption of multiple colluding eavesdroppers. To this end, we assume the existence of N_E eavesdroppers that combine their isolated observations to reconstruct the confidential message as in [26]. Using maximum ratio combining (MRC), the combined SNR of all eavesdroppers is utilised to detect Bob's message. To evaluate the secrecy performance in this scenario, we assume that the AP can obtain an estimate of the location of the colluding eavesdroppers. We start with the case where the AP has a knowledge of the exact value of Bob's channel. Then, we add random device orientation to the analytical derivations.

A. SECRECY CALCULATIONS WITH IMPERFECT CSI OF EAVESDROPPERS

Proposition 3: The secrecy capacity with the existence of N_E colluding eavesdroppers is defined as the difference between Bob's capacity and the capacity obtained by the combined SNR of the colluding eavesdroppers, and can be lower-bounded as:

$$\begin{aligned}\mathcal{C}_s^{N_E} \geq\ & \frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\left(e\zeta^2P^2h_B^2+2\pi\sigma_B^2\right)\right)\\ &\times\left(1-\mathcal{Q}_{N_E/2}\left(\sqrt{\lambda},\sqrt{\frac{\kappa N_E}{\sigma^2}}\right)\right)\\ &-\frac{1}{2}\ln\left(\zeta^2P^2\sigma^2(N_E+\lambda)+\sigma_E^2\right),\end{aligned}\tag{22}$$

where $\mathcal{Q}_M(a,b)$ is the Marcum-Q-function.

Proof: The proof is provided in Appendix E. □

Corollary 3: The secrecy outage probability, defined as the probability that the secrecy capacity of Bob falls below a predetermined threshold Q in the presence of N_E colluding eavesdroppers, can be upper-bounded as:

$$\begin{aligned}&\mathcal{P}_{out}^{N_E}\\ &\leq \mathcal{Q}_{k/2}\left(\sqrt{\lambda},\sqrt{\frac{\sigma_E^2}{\sigma^2\zeta^2P^2}\left(\frac{e^{-2Q}}{2\pi\sigma_B^2}(e\zeta^2P^2h_B^2+2\pi\sigma_B^2)-1\right)}\right),\end{aligned}\tag{23}$$

where Q is the outage threshold such that outage occurs if $\mathcal{C}_s^{N_E}<Q$.

Proof: The proof is provided in Appendix F. □

B. EFFECT OF RANDOM RECEIVER ORIENTATION

Proposition 4: Considering random receiver orientation, the secrecy capacity is defined as the difference between Bob's capacity and the capacity obtained by the combined SNR of N_E colluding eavesdroppers, and can be lower-bounded as:

$$\begin{aligned}&\tilde{\mathcal{C}}_s^{N_E}\\ &\geq -b_H\iota_1\tilde{\Upsilon}(\kappa)e^{\frac{\mu_H-\kappa_H}{b_H}}\left(e^{\frac{\kappa_H}{b_H}}Ei\left(-\frac{\kappa_H}{b_H}\right)-\frac{1}{3}\log\left(\frac{e\kappa_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right)\\ &+b_H\iota_1e^{-\frac{\mu_H}{b_H}}\tilde{\Upsilon}(\kappa)\left(Ei\left(\frac{\mu_H}{b_H}\right)-\frac{1}{2}e^{\frac{\mu_H}{b_H}}\log\left(\frac{e\mu_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right)\\ &+b_H\iota_1\tilde{\Upsilon}(\kappa)\left(e^{\frac{\mu_H}{b_H}}Ei\left(-\frac{\mu_H}{b_H}\right)-\frac{1}{2}\log\left(\frac{e\mu_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right)\\ &+b_H\iota_1\left(-e^{\frac{\mu_H-\kappa_H}{b_H}}-e^{-\frac{\mu_H}{b_H}}+2\right)\\ &\times\left(\tilde{\Upsilon}(\kappa)\log\left(\sigma_E^2\right)-\frac{1}{2}\log\left(P^2\zeta^2\left(\mu^2+s^2\right)+\sigma_E^2\right)\right),\end{aligned}\tag{24}$$

where $\tilde{\Upsilon}(\kappa)=\frac{e^{-\lambda/2}\left(1-\mathcal{Q}_{N_E/2}\left(\sqrt{\lambda},\sqrt{\frac{\kappa N_E}{\sigma^2}}\right)\right)}{2^{N_E/2+1}\,\sigma^{N_E}\,\Gamma(N_E/2)}$,

Proof: The proof is provided in Appendix G. □

Corollary 4: The secrecy outage probability, which is defined as the probability that the secrecy capacity falls under a predetermined threshold Q for the case of N_E colluding eavesdroppers and random orientation of Bob, can be calculated as:

$$\begin{aligned}&\tilde{\mathcal{P}}_{out}^{N_E}\\ &=\int_{\tilde{h}=0}^{\kappa_H}\mathcal{P}_{out}^{N_E}f_H(\tilde{h})d\tilde{h}\\ &=\int_{\tilde{h}=0}^{\kappa_H}f_H(\tilde{h})\mathcal{Q}_{k/2}\\ &\quad\times\left(\sqrt{\lambda},\sqrt{\frac{\sigma_E^2}{\sigma^2\zeta^2P^2}\left(\frac{e^{-2Q}}{2\pi\sigma_B^2}(e\zeta^2P^2\tilde{h}_B^2+2\pi\sigma_B^2)-1\right)}\right)d\tilde{h}.\end{aligned}\tag{25}$$

It is noted that there is no closed-form solution for the integral in (25) and it can be solved numerically.

V. ASYMPTOTIC SECRECY CAPACITY ANALYSIS

In order to get more insights on the secrecy performance, we analyse the secrecy capacity performance in the high transmit SNR regime which implies that $\gamma\to\infty$.

A. SINGLE EAVESDROPPER

For the VLC channel with average optical power constraints, the secrecy capacity with the existence of a single eavesdropper is lower-bounded by [27]:

$$\mathcal{C}_s\geq\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\times\frac{e\zeta^2P^2h_B^2+2\pi\sigma_B^2}{\zeta^2P^2\hat{h}_E^2+\sigma_E^2}\right).\tag{26}$$

Let $\gamma_B=\frac{P^2}{\sigma_B^2}$ and $\gamma_E=\frac{P^2}{\sigma_E^2}$ be the transmit SNR for Bob and Eve, respectively. For a high SNR regime, i.e., $\gamma_B\to\infty$ and $\gamma_B\to\infty$, and after some manipulations we have:

$$\tilde{\mathcal{C}}_s^{1_E}\overset{\gamma\to\infty}{\approx}\frac{1}{2}\ln\left(\frac{eh_B^2}{2\pi\hat{h}_E^2}\right),\tag{27}$$

using the PDF of $y = \hat{h}_E^2$ in (36) and applying Jensen's inequality, we get:

$$\hat{\mathcal{C}}_s^{1_E} \overset{\gamma\to\infty}{\approx} \int_{y=0}^{\kappa} \frac{1}{2}\ln\left(\frac{eh_B^2}{2\pi y}\right) f_Y(y)dy \approx \frac{1}{2}\ln\left(\frac{eh_B^2}{2\pi(\mu^2+\sigma^2)}\right). \quad (28)$$

Considering random orientation and following similar steps as in Appendix C, we get:

$$\begin{aligned}\hat{\mathcal{C}}_s^{1_E} &\overset{\gamma\to\infty}{\approx} \int_{\tilde{h}=0}^{\kappa_H} \ln\left(c_1\tilde{h}\right) f_H(\tilde{h})\, d\tilde{h} \\ &\approx b_H\iota_1\Big[2\log(c_1\mu_H) - e^{\frac{\mu_H-\kappa_H}{b_H}}\log(c_1\kappa_H) \\ &\quad + e^{\frac{\mu_H-\kappa_H}{b_H}} e^{\frac{\kappa_H}{b_H}}\left(\mathrm{Ei}\left(\frac{\mu_H}{b_H}\right) - \mathrm{Ei}\left(\frac{\kappa_H}{b_H}\right)\right) \\ &\quad + e^{\frac{-\mu_H}{b_H}}\mathrm{Ei}\left(\frac{-\mu_H}{b_H}\right) - \log(c_1 b_H) + \mathcal{E}\Big], \end{aligned} \quad (29)$$

where $c_1 = \left(\frac{2\pi}{e}(\mu^2+\sigma^2)\right)^{-1}$ and $\mathcal{E}$ is Euler's constant.

B. COLLUDING EAVESDROPPERS

The asymptotic secrecy capacity in the case of colluding eavesdroppers can be written as:

$$\tilde{\mathcal{C}}_s^{N_E} \overset{\gamma\to\infty}{\approx} \int_{y=0}^{\kappa} \frac{1}{2}\ln\left(\frac{eh_B^2}{2\pi\sum_{i=1}^{N_E} y_i}\right) f_Y(y)dy. \quad (30)$$

Let $x = \sum_{i=1}^{N_E} y_i$, it follows that x is distributed according to generalized non-central chi-squared-square distribution, and the PDF of x can be expressed as (61) as shown in Appendix D. As a result, and following similar steps as in Appendix D, the secrecy asymptotic secrecy capacity can be evaluated as:

$$\begin{aligned}\tilde{\mathcal{C}}_s^{N_E} &\overset{\gamma\to\infty}{\approx} \frac{1}{2}\ln\left(\frac{eh_B^2}{2\pi}\right)\left(1 - \mathcal{Q}_{N_E/2}\left(\sqrt{\lambda}, \sqrt{\frac{\kappa N_E}{\sigma^2}}\right)\right) \\ &\quad - \frac{1}{2}\ln\left(\sigma^2(N_E+\lambda)\right). \end{aligned} \quad (31)$$

Considering random orientation, we have:

$$\begin{aligned}\tilde{\mathcal{C}}_s^{N_E} &\overset{\gamma\to\infty}{\approx} b_H\iota_1\left(1 - \mathcal{Q}_{N_E/2}\left(\sqrt{\lambda}, \sqrt{\frac{\kappa N_E}{\sigma^2}}\right)\right) \\ &\quad \times\Big[2\log(c_2\mu_H) - e^{\frac{\mu_H-\kappa_H}{b_H}}\log(c_2\kappa_H) \\ &\quad + e^{\frac{\mu_H-\kappa_H}{b_H}} e^{\frac{\kappa_H}{b_H}}\left(\mathrm{Ei}\left(\frac{\mu_H}{b_H}\right) - \mathrm{Ei}\left(\frac{\kappa_H}{b_H}\right)\right) \\ &\quad + e^{\frac{-\mu_H}{b_H}}\mathrm{Ei}\left(\frac{-\mu_H}{b_H}\right) - \log(c_2 b_H) + \mathcal{E}\Big] \\ &\quad - \frac{1}{2}b_H\iota_1\ln\left(\sigma^2(N_E+\lambda)\right) \\ &\quad \times\left(-e^{\frac{\mu_H-\kappa_H}{b_H}} - e^{-\frac{\mu_H}{b_H}} + 2\right) \end{aligned} \quad (32)$$

where $c_2 = \sqrt{\frac{2\pi}{e}}$.

VI. DATA-DRIVEN SECURE AP SELECTION

In this section, we describe a data-driven AP selection mechanism that aims to maximise the secrecy performance of a LiFi system based on the secrecy metrics derived in Sections III and IV. For the learning system, we consider supervised ML in order to select the optimal serving AP for each legitimate user. Specifically, we apply a multi-class classifier, namely multi-class k-nearest neighbors (k-NN). With a sufficient number of training data samples, we can obtain a classification model that predicts the optimal AP index for each network user, where the APs' indices represent the classes. We assume that the learning system runs at a central control unit (CCU) that acquires information about available APs and network users. To this end, the CCU is assumed to acquire perfect CSI of all legitimate users. Since the eavesdroppers are likely to be passive users that do not share their information with the AP, we assume that the CCU only acquires an estimate of the CSI of potential eavesdroppers. This can be achieved with the aid of built-in motion sensors deployed in LED fixtures, as assumed in [22]. We assume that multiple users can share the resources of a single AP by means of time division multiple access (TDMA).

In the following, we explain the procedure performed to build and evaluate the AP selection learning system:

1) KPI Design: The objective of the proposed AP selection is to maximise the sum secrecy rate of all the legitimate network users under the proportional fairness constraints. It was shown in [28] that proportional fairness can be achieved by maximising the sum of the logarithm of the users' utility function. Based on this, we formulate our objective function as:

$$\begin{aligned}&\text{maximize} \sum_{i=1}^{N_B}\log\sum_{j=1}^{N_{AP}}\frac{\alpha_{ij}\,\tilde{\mathcal{C}}_{s_{ij}}}{\sum_{i=1}^{N_B}\alpha_{ij}}, \\ &\text{subject to} \sum_{j=1}^{N_{AP}}\alpha_{ij} = 1 \quad \forall i,\ldots,N_B, \\ &\qquad \alpha_{ij}\in\{0,1\} \quad \forall i = 1,\ldots,N_B, \end{aligned} \quad (33)$$

where N_{AP} represents the number of APs, N_B represents the number of legitimate users, and α_{ij} is a binary variable that indicate user association such that $_{ij} = 1$ if user i is associated with AP i and $\alpha_{ij} = 0$ otherwise. Furthermore, $\tilde{\mathcal{C}}_{s_{ij}}$ denotes the secrecy capacity of user i when connected to AP j, here $\tilde{\mathcal{C}}_{s_{ij}}$ is calculated from (20) or (24) depending on the number of eavesdroppers detected in the coverage area of AP j.

2) Training set generation: We use Matlab simulations to generate the training samples for the learning system. The training samples are stored in the matrix $\mathbf{T} = [\mathbf{u}, \mathbf{v}, \mathbf{s}] \in \mathbb{R}^{M\times(5N_B+2N_E+1)}$ which is used as the input of the learning system. The predictor vectors $\mathbf{u}$, $\mathbf{v}$, $\mathbf{s}$ represent the legitimate users' information, the eavesdroppers' information, and the optimal AP selection for

TABLE 1. Simulation parameters.

Description	Notation	Value
Transmitter semi-angle	φ_k	60 deg
FOV of the PDs	ϕ_{c_k}	90 deg
Physical area of PD	A_k	1.0 cm^2
Refractive index of PD lens	n	1.5
Gain of optical filter	$T_s(\phi_k)$	1.0
Alice location	L_A	(0.0, 0.0, 2.5) m
Bob location 1	L_B^1	(1.0, 1.0, 0.6) m
Bob location 2	L_B^2	(1.2, 1.3, 1.4) m

each legitimate user, respectively. The process of generating the training samples is described in Algorithm VI.

3) Building the learning system: We use the training matrix $\mathbf{T}$ to train an $|\mathcal{L}|$-class KNN classifier, where $|\mathcal{L}|$ is the number of AP labels. The input attributes of the classifier are $\mathbf{u}$ and $\mathbf{v}$, and the output is the AP selection label $\mathbf{s}$. After being trained with M training samples, the KNN classifier finds the k nearest training samples from a new observation and declares its class, i.e., AP label. The nearest neighbours are determined based on the Euclidean distance. It is noted that the neighbor search time complexity of the kNN algorithm is $O(MN)$, where M is the number of training examples and $N = 5N_B + 2N_E + 1$ is the number of dimensions in the training set. For simplicity, we can say that the complexity of the KNN algorithm is $O(M)$ since $M \gg N$.

VII. RESULTS

In this section, we present analytic results and Monte Calro simulations to evaluate the secrecy performance under realistic channel assumptions for different scenarios. Solid lines in the figures represent analytic results whereas markers and/or dashed lines indicate results from simulations. For our simulations, we calculate the secrecy capacity using the lower bound in (34) [27] and capture the effect of Eve's imperfect CSI and Bob's random device orientation by generating 10^6 random instances and calculating the average secrecy capacity for each scenario. Moreover, the presented secrecy outage probability results indicate the upper bound on the outage probability, i.e. outage occurs when the secrecy capacity, calculated by means of the lower bound, falls below a certain threshold value. Unless otherwise specified, system parameters for the generated results are set according to Table 1.

First, we start with the case of a single eavesdropper. We assume the existence of a single AP and plot the secrecy capacity and secrecy outage probability of Bob versus the horizontal separation between Eve's location and the cell centre. We assume two different locations of Bob according to Table 1, where L_B^1 represents a sitting position and L_B^2 represents a standing position. We assume that the calculation of secrecy capacity and secrecy outage probability is based on the existence of an estimate of the CSI of Eve, rather than the exact value. Thus, as discussed earlier, $\hat{h}_E$ follows a normal distribution with a mean that is equal to the actual value of h_E and σ^2 represents the CSI error. Here, we assume $\sigma^2 = h_E^2$.

Algorithm 1 Generate Training Data Samples

Result: Training data matrix $\mathbf{T}$
Initialise $\mathbf{T} \in \mathbb{R}^{M\times(5N_B+2N_E+1)}$;
for $m = 1{:}M$ **do**
  Generate random legitimate users vector $\mathbf{u} = [\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{N_B}]$ where $\mathbf{u}_i = [x_i, y_i, z_i, \mu_{\theta_i}, \sigma_{\theta_i}]$;
  Generate random eavesdroppers vector $\mathbf{v} = [\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{N_E}]$ where $\mathbf{v}_k = [\mu_k, \sigma_k]$;
  Initialise AP selection vector $\mathbf{s} \in \mathbb{R}^{N_B\times 1}$;
  Generate AP permutation matrix containing all possible AP selection options for all legitimate users $\mathbf{W} \in \mathbb{R}^{P\times N_B}$ where $P = {N_{AP}}^{N_B}$;
  Initialise KPI vector $\mathbf{k} \in \mathbb{R}^{P\times 1}$;
  for $p = 1 : P$ **do**
    Evaluate KPI for permutation p
    for $j = 1 : N_{AP}$ **do**
      $\beta = 0$; $k1 = 0$; $c1 = 0$;
      for $i = 1 : N_B$ **do**
        if $\mathbf{W}(p, i) == j$ **then**
          Calculate secrecy capacity C_s of user i connected to AP j using (24);
          $\beta = \beta + 1$;
        else
          $C_s = 0$;
        end
        $c1 = c1 + C_s$;
      end
      $k1 = k1 + \log(c1/\beta)$;
    end
    $\mathbf{k}(p) = k1$;
  end
  for $p = 1{:}P$ **do**
    if $\mathbf{k}(p) == \max k$ **then**
      $\mathbf{s}(m) = \mathbf{W}(p, :)$;
    end
  end
  Populate the training set matrix
  $\mathbf{T}(m, :) = [\mathbf{u}, \mathbf{v}, \mathbf{s}]$;
end

We also investigate the effect of random receiver orientation when Bob's device is assumed to follow the random orientation model presented in Section II-C. We note that Eve's device is assumed to be fixed and directed to face the AP, which constitutes a worst case scenario for the secrecy performance. It can be seen in Fig. 4 that assuming random receiver orientation for Bob leads to a severe degradation in the secrecy performance compared to a fixed orientation, where Bob's device is assumed to be directed vertically upwards. For example, for the case of the user location L_B^1, random receiver orientation results in almost 25% degradation in the secrecy capacity compared to the case without consideration of the random orientation. Also, we can see from Fig. 4 that the analytic results presented in Proposition 1 and 2 as well as Corollary 1 and 2 are in agreement with the simulation results.

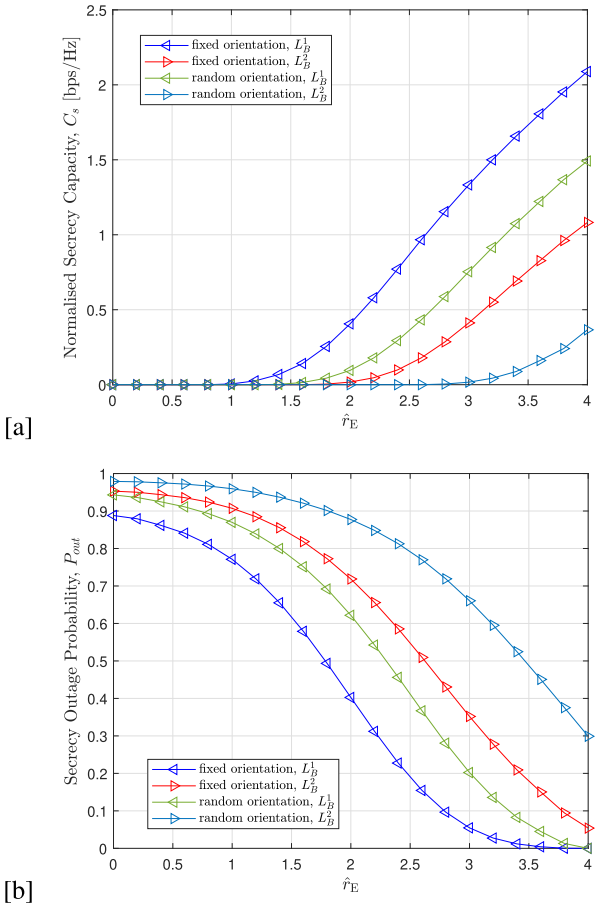

FIGURE 4. Effect of random receiver orientation on (a) secrecy capacity and (b) secrecy outage probability, single eavesdropper, $\mu = \sigma^2$.

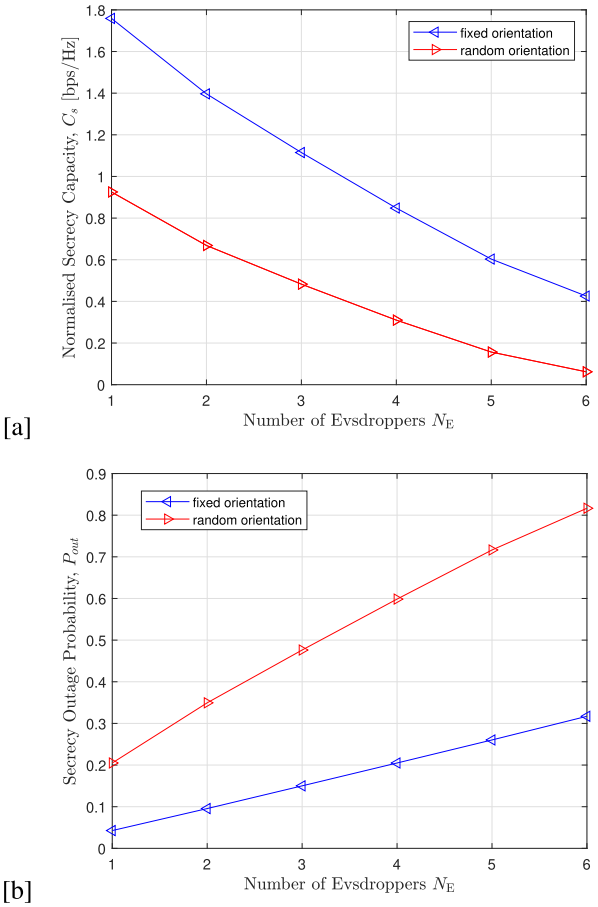

FIGURE 5. Effect of colluding eavesdroppers on (a) secrecy capacity and (b) secrecy outage probability, $\mu = \sigma^2$.

Next, we investigate the effect of having multiple colluding eavesdroppers who utilise their combined SNRs to reconstruct Bob's confidential signal. Fig. 5 shows simulation and analytic results for the secrecy capacity and secrecy outage probability for $N_E = 1, \ldots, 6$. For these results we assume that there exists an estimate of the CSI of each eavesdropper and that $\sigma_i^2 = \mu_i$ for $i = 1, \ldots, N_E$. Moreover, the locations of the eavesdroppers are randomly generated within the coverage area according to uniform distribution. In Fig. 5, fixed orientation scenario assumes that the users' devices are fixed to be oriented vertically upward, which corresponds to the expressions presented in Proposition 3 and Corollary 3. The random orientation scenario corresponds to the assumption of random receivers' orientation considered in Proposition 4 and Corollary 4. We can see that random receiver orientation has a significant impact on reducing the secrecy capacity. For example, the effect of random orientation results in almost 50% drop in the achievable secrecy capacity for the case of two colluding eavesdroppers as shown in Fig. 5 [a]. Fig. 6 shows the secrecy capacity versus transmit SNR compared to the asymptotic secrecy capacity derived in Section V for the case of single and multiple eavesdroppers. It is evident that the secrecy capacity gradually approaches the asymptotic capacity bound.

Next, we investigate the performance of the proposed ML-based secure AP selection. For the purpose of comparison, we present the achievable average secrecy capacity for the following AP selection criteria: 1) 'realistic-secrecy AP selection': which is realised by ML-based classifier that is based on the derived secrecy capacity expressions in 2 and 4, 2) 'limited-secrecy AP selection': which is realised by ML-based classifier that is based on the assumption of fixed device orientation and perfect CSI of Eve, and 3) 'signal-strength AP selection': which assigns each user to its closet AP.

It can be seen from Fig. 7 that performing AP selection based on secrecy calculations enhances the secrecy capacity compared to signal-strength AP selection. This is due to the fact that legitimate users are not always connected to the AP offering the highest signal strength, but rather to the AP offering the highest possible secrecy capacity. Moreover, we can see that the realistic-secrecy AP selection results in higher secrecy capacity compared to limited-secrecy AP selection. This is because the latter decides on the best serving AP taking into account the randomness in the link conditions. Specifically, using the derived realistic metrics results in about $20\% - 30\%$ enhancement in the secrecy capacity compared to limited assumptions, and more than 100% enhancement compared to signal-strength AP selection.

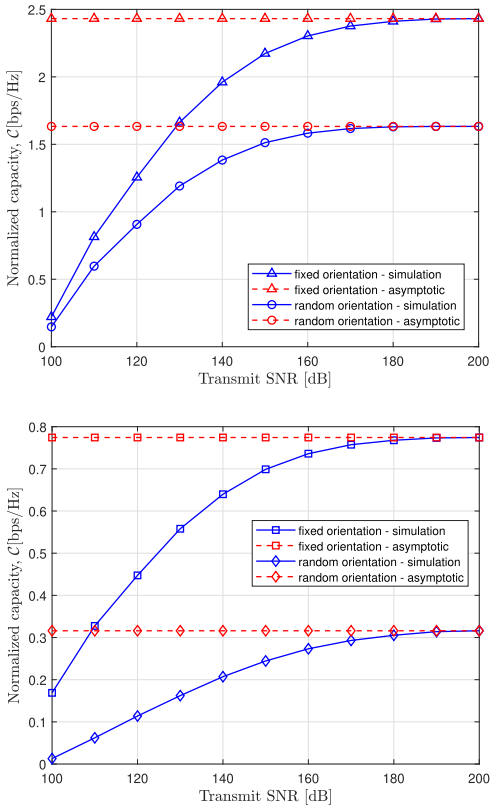

FIGURE 6. Normalised secrecy capacity in the existence of (a) single eavesdropper and (b) five colluding eavesdroppers. Bob is assumed to be located at L_B^1, eavesdroppers are randomly located, and $\mu = \sigma^2$.

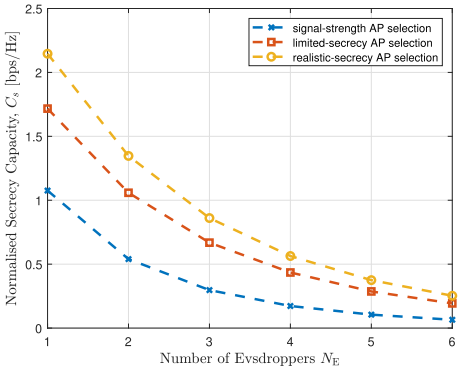

FIGURE 7. Average achievable secrecy capacity for different AP selection criteria.

VIII. CONCLUSION

This paper investigates the secrecy performance of LiFi systems by deriving analytic expressions for the secrecy capacity and secrecy outage probability under realistic link assumptions, i.e., imperfect knowledge of the CSI of the eavesdroppers and random receiver orientation. It is demonstrated that taking such realistic secrecy measures into account when performing AP selection can lead to significant enhancement in the secrecy capacity without the need for employing specific PLS mechanisms. Our results indicate that the secrecy capacity can be enhanced by up to 30% when the AP selection is performed with the aim of maximising the secrecy capacity based on the proposed realistic expressions, compared to AP selection based on limited assumptions. We believe that considering the distinct characteristics of the optical channel can lead to a better understanding of the secrecy performance of LiFi systems and, thus, leads to implementing more robust PLS mechanisms.

APPENDIX A
PROOF OF PROPOSITION 1

For the VLC channel with average optical power constraints, the secrecy capacity with the existence of a single eavesdropper is lower-bounded by [27]:

$$\mathcal{C}_s \geq \frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\times\frac{e\zeta^2P^2h_B^2+2\pi\sigma_B^2}{\zeta^2P^2\hat{h}_E^2+\sigma_E^2}\right), \tag{34}$$

since the CSI of Eve is modelled to follow a normal distribution [23]–[25], i.e., $\hat{h}_E \sim \mathcal{N}(\mu,\sigma^2)$, we denote the square of the channel gain of Eve as y and obtain its PDF as follows:

$$\begin{aligned} F_Y(y) &= \mathbb{P}[Y\leq y] = \mathbb{P}[h_E^2\leq y] = \mathbb{P}[|\hat{h}_E|\leq\sqrt{y}] \\ &= \mathbb{P}[-\sqrt{y}<\hat{h}_E<\sqrt{y}] = \Phi(\sqrt{y})-\Phi(-\sqrt{y}), \end{aligned} \tag{35}$$

where $\Phi(.)$ denotes the CDF of normal distribution. Differentiating with respect to y we get,

$$\begin{aligned} f_Y(y) &= F_Y'(y) = \frac{1}{2\sqrt{y}}\phi(\sqrt{y})+\frac{1}{2\sqrt{y}}\phi(-\sqrt{y}) \\ &= \frac{1}{2\sqrt{2\pi\sigma^2y}}e^{-\frac{(\sqrt{y}-\mu)^2}{2\sigma^2}}+\frac{1}{2\sqrt{2\pi\sigma^2y}}e^{-\frac{(-\sqrt{y}-\mu)^2}{2\sigma^2}}. \end{aligned} \tag{36}$$

Accordingly, the secrecy capacity with imperfect CSI of Eve can be lower-bounded as:

$$\mathcal{C}_s^{1_E} \geq \int_{y=0}^{\kappa}\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\times\frac{e\zeta^2P^2h_B^2+2\pi\sigma_B^2}{\zeta^2P^2y+\sigma_E^2}\right)f_Y(y)dy. \tag{37}$$

Using the properties of the natural logarithmic function, we can write the integral as:

$$\begin{aligned} \mathcal{C}_s^{1_E} &\geq \int_{y=0}^{\kappa}\left[\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\right)+\frac{1}{2}\ln\left(e\zeta^2P^2y+2\pi\sigma_B^2\right)\right. \\ &\quad \left.-\frac{1}{2}\ln\left(\zeta^2P^2y+\sigma_E^2\right)\right]\times f_Y(y)dy \\ &\geq \int_{y=0}^{\kappa}\left[\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\right)+\frac{1}{2}\ln\left(e\zeta^2P^2y+2\pi\sigma_B^2\right)\right] \\ &\quad \times f_Y(y)dy-\int_{y=0}^{\kappa}\frac{1}{2}\ln\left(\zeta^2P^2y+\sigma_E^2\right)f_Y(y)dy \end{aligned} \tag{38}$$

where κ denotes maximum value of y, which can be calculated for the scenario where Eve is located directly under the AP and with fixed orientation so as to maximise its received channel gain. Based on this, the first integral can be re-written as:

$$\int_{y=0}^{\kappa}\left[\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\right)+\frac{1}{2}\ln\left(e\zeta^2P^2h_B^2+2\pi\sigma_B^2\right)\right]f_Y(y)dy$$

$$= \left[\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\right) + \frac{1}{2}\ln\left(e\zeta^2P^2h_B^2 + 2\pi\sigma_B^2\right)\right] \times \int_{y=0}^{\kappa}\left(\frac{1}{2\sqrt{2\pi\sigma^2 y}}e^{-\frac{(\sqrt{y}-\mu)^2}{2\sigma^2}} + \frac{1}{2\sqrt{2\pi\sigma^2 y}}e^{-\frac{(-\sqrt{y}-\mu)^2}{2\sigma^2}}\right)dy$$
$$= \left[\frac{1}{4}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\right) + \frac{1}{4}\ln\left(e\zeta^2P^2h_B^2 + 2\pi\sigma_B^2\right)\right] \times \left(erf\left(\frac{\sqrt{\kappa}-\mu}{\sqrt{2\sigma^2}}\right) + erf\left(\frac{\sqrt{\kappa}+\mu}{\sqrt{2\sigma^2}}\right)\right). \quad (39)$$

To evaluate the second integral, we use Jensen's inequality which states that $\mathbb{E}[\phi(y)] \leq \phi(\mathbb{E}[y])$ for random variable y and a convex function ϕ. Hence we can write:

$$\int_{y=0}^{\kappa}\frac{1}{2}\ln\left(\zeta^2P^2y + \sigma_E^2\right)f_Y(y)dy \leq \frac{1}{2}\ln\left(\zeta^2P^2\mathbb{E}[y] + \sigma_E^2\right) \leq \frac{1}{2}\ln\left(\zeta^2P^2(\mu^2+\sigma^2)) + \sigma_E^2\right), \quad (40)$$

by combining (40) and (39), we obtain the lower bound for the secrecy capacity in (18), which completes the proof.

APPENDIX B
PROOF OF COROLLARY 1

The outage probability is expressed as:

$$\mathcal{P}_{out}^{1_E} = \mathbb{P}\left[\mathcal{C}_s^{1_E} < Q\right] \quad (41)$$

using the lower-bound of $\mathcal{C}_s^{1_E}$, an upper-bound on the secrecy outage probability can be calculated as:

$$\mathcal{P}_{out}^{1_E} \leq \mathbb{P}\left[\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2} \times \frac{e\zeta^2P^2h_B^2 + 2\pi\sigma_B^2}{\zeta^2P^2y + \sigma_E^2}\right) < Q\right] \leq \mathbb{P}\left[y > \frac{\sigma_E^2}{\zeta^2P^2}\left(\frac{e^{-2Q}}{2\pi\sigma_B^2}(e\zeta^2P^2h_B^2 + 2\pi\sigma_B^2) - 1\right)\right], \quad (42)$$

using the PDF of the square of the channel gain $y = h_E^2$ in (36), we get:

$$\mathcal{P}_{out}^{1_E} \leq 1 - \int_0^{\Xi} f_Y(y)dy = 1 - \int_0^{\Xi}\left(\frac{1}{2\sqrt{2\pi\sigma^2 y}}e^{-\frac{(\sqrt{y}-\mu)^2}{2\sigma^2}} + \frac{1}{2\sqrt{2\pi\sigma^2 y}}e^{-\frac{(-\sqrt{y}-\mu)^2}{2\sigma^2}}\right)dy, \quad (43)$$

where $\Xi = \frac{\sigma_E^2}{\zeta^2P^2}\left(\frac{e^{-2Q}}{2\pi\sigma_B^2}(e\zeta^2P^2h_B^2 + 2\pi\sigma_B^2) - 1\right)$, which gives the expression in (19).

APPENDIX C
PROOF OF PROPOSITION 2

Considering random orientation, the secrecy capacity can be lower-bounded as:

$$\tilde{\mathcal{C}}_s^{1_E} \geq \int_{\tilde{h}=0}^{\kappa_H} f_H(\tilde{h}) \times \mathcal{C}_s^{1_E}(\tilde{h})\, d\tilde{h}, \quad (44)$$

substituting $f_H(\tilde{h})$ from (11) and $\mathcal{C}_s^{1_E}(\tilde{h})$ from (18) we get:

$$\tilde{\mathcal{C}}_s^{1_E} \geq \int_{\tilde{h}=0}^{\kappa_H} f_H(\tilde{h}) \times \left[\frac{1}{4}\Upsilon(\kappa)\ln\left(\frac{eP^2\zeta^2\tilde{h}^2 + 2\pi\sigma_B^2}{2\pi\sigma_B^2\sigma_E^{-2}}\right) - \frac{1}{2}\ln(P^2\zeta^2(\mu^2+\sigma^2) + \sigma_E^2)\right]d\tilde{h}, \quad (45)$$

which can be written as

$$\tilde{\mathcal{C}}_s^{1_E} \geq \int_{\tilde{h}=0}^{\kappa_H}\frac{1}{4}f_H(\tilde{h})\Upsilon(\kappa)\ln\left(\frac{eP^2\zeta^2\tilde{h}^2 + 2\pi\sigma_B^2}{2\pi\sigma_B^2}\right)d\tilde{h} + \int_{\tilde{h}=0}^{\kappa_H}\left(-\frac{1}{2}\ln\left((P^2\zeta^2(\mu^2+\sigma^2)+\sigma_E^2\right) + \frac{1}{4}\Upsilon(\kappa)\ln(\sigma_E^2)\right) \times f_H(\tilde{h})d\tilde{h}, \quad (46)$$

the first integral evaluates to:

$$\frac{1}{4}\Upsilon(\kappa)\int_{\tilde{h}=0}^{\mu_H}\left(\iota_1\exp\left(\frac{-|\tilde{h}-\mu_{\rm H}|}{b_{\rm H}}\right) + F_\theta(\theta)\delta(\tilde{h})\right) \times \ln\left(\frac{eP^2\zeta^2\tilde{h}^2 + 2\pi\sigma_B^2}{2\pi\sigma_B^2}\right)d\tilde{h} + \Upsilon(\kappa)\int_{\tilde{h}=\mu_H}^{\kappa_H}\frac{1}{4}\left(\iota_1\exp\left(\frac{-|\tilde{h}-\mu_{\rm H}|}{b_{\rm H}}\right) + F_\theta(\theta)\delta(\tilde{h})\right) \times \ln\left(\frac{eP^2\zeta^2\tilde{h}^2 + 2\pi\sigma_B^2}{2\pi\sigma_B^2}\right)d\tilde{h}, \quad (47)$$

where $\iota_1 = \frac{1}{b_{\rm H}\left(2-\exp\left(-\frac{h_{\max}-\mu_{\rm H}}{b_{\rm H}}\right)\right)}$, thus we can write the first integral as:

$$\frac{1}{4}\Upsilon(\kappa)\mathcal{F}_1(\tilde{h})|_{\tilde{h}=0}^{\mu_H} + \frac{1}{4}\Upsilon(\kappa)\mathcal{F}_2(\tilde{h})|_{\tilde{h}=\mu_H}^{\kappa_H} = \frac{1}{4}\Upsilon(\kappa)\left(\mathcal{F}_1(\mu_H) - \mathcal{F}_1(0)\right) + \frac{1}{4}\Upsilon(\kappa)\left(\mathcal{F}_2(\kappa_H) - \mathcal{F}_2(\mu_H)\right) = \frac{1}{4}\Upsilon(\kappa)\left(\mathcal{F}_1(\mu_H) + \mathcal{F}_2(\kappa_H) - \mathcal{F}_2(\mu_H)\right) \quad (48)$$

where

$$\mathcal{F}_1 = \int\left(\iota_1\exp\left(\frac{\tilde{h}-\mu_{\rm H}}{b_{\rm H}}\right) + F_\theta(\theta)\delta(\tilde{h})\right) \times \ln\left(\frac{eP^2\zeta^2\tilde{h}^2 + 2\pi\sigma_B^2}{2\pi\sigma_B^2}\right)d\tilde{h} \quad (49)$$

and

$$\mathcal{F}_2 = \int\left(\iota_1\exp\left(\frac{-\tilde{h}+\mu_{\rm H}}{b_{\rm H}}\right) + F_\theta(\theta)\delta(\tilde{h})\right) \times \ln\left(\frac{eP^2\zeta^2\tilde{h}^2 + 2\pi\sigma_B^2}{2\pi\sigma_B^2}\right)d\tilde{h}. \quad (50)$$

Noting the property of delta function, we can see that

$$\int F_\theta(\theta)\delta(\tilde{h})\ln\left(\frac{eP^2\zeta^2\tilde{h}^2+2\pi\sigma_B^2}{2\pi\sigma_B^2}\right)d\tilde{h} = F_\theta(\theta)\int\delta(\tilde{h})\ln(1)d\tilde{h}=0. \quad (51)$$

Furthermore, we note that that $\mathcal{F}_1(0)=0$. Using a high SNR approximation and integration by parts, we get:

$$\mathcal{F}_1(\tilde{h}) = b_H\iota_1 e^{-\frac{\mu_H}{b_H}}\left(e^{\frac{\tilde{h}}{b_H}}\log\left(\frac{e\tilde{h}^2P^2\zeta^2}{2\pi\sigma_B^2}\right)-2\mathrm{Ei}\left(\frac{\tilde{h}}{b_H}\right)\right) \quad (52)$$

and

$$\mathcal{F}_2(\tilde{h}) = b_H\iota_1 e^{\frac{\mu_H-\tilde{h}}{b_H}}\left(2e^{\frac{\tilde{h}}{b_H}}\mathrm{Ei}\left(-\frac{\tilde{h}}{b_H}\right)-\log\left(\frac{e\tilde{h}^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right). \quad (53)$$

Thus, the first integral in (46) reduces to:

$$\begin{aligned}&\frac{1}{4}\Upsilon(\kappa)b_H\iota_1 e^{-\frac{\mu_H}{b_H}}\left(e^{\frac{\mu_H}{b_H}}\log\left(\frac{e\mu_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)-2\mathrm{Ei}\left(\frac{\mu_H}{b_H}\right)\right)\\&+\frac{1}{4}\Upsilon(\kappa)b_H\iota_1 e^{\frac{\mu_H-\kappa_H}{b_H}}\\&\times\left(2e^{\frac{\kappa_H}{b_H}}\mathrm{Ei}\left(-\frac{\kappa_H}{b_H}\right)-\log\left(\frac{e\kappa_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right)\\&-\frac{1}{4}\Upsilon(\kappa)b_H\iota_1\left(2e^{\frac{mu_H}{b_H}}\mathrm{Ei}\left(-\frac{\mu_H}{b_H}\right)-\log\left(\frac{e\mu_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right),\end{aligned} \quad (54)$$

and the secrecy capacity can be lower-bounded as:

$$\begin{aligned}&\tilde{\mathcal{C}}_s^{1_E}\\&\geq\frac{1}{4}\Upsilon(\kappa)b_H\iota_1 e^{-\frac{\mu_H}{b_H}}\left(e^{\frac{\mu_H}{b_H}}\log\left(\frac{e\mu_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)-2\mathrm{Ei}\left(\frac{\mu_H}{b_H}\right)\right)\\&+\frac{1}{4}\Upsilon(\kappa)b_H\iota_1 e^{\frac{\mu_H-\kappa_H}{b_H}}\left(2e^{\frac{\kappa_H}{b_H}}\mathrm{Ei}\left(-\frac{\kappa_H}{b_H}\right)-\log\left(\frac{e\kappa_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right)\\&-\frac{1}{4}\Upsilon(\kappa)b_H\iota_1\left(2e^{\frac{mu_H}{b_H}}\mathrm{Ei}\left(-\frac{\mu_H}{b_H}\right)-\log\left(\frac{e\mu_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right)\\&+b_H\iota_1\left(-e^{\frac{\mu_H-\kappa_H}{b_H}}-e^{-\frac{\mu_H}{b_H}}+2\right)\\&\times\left(\frac{1}{4}\Upsilon(\kappa)\log\left(\sigma_E^2\right)-\frac{1}{2}\log\left(P^2\zeta^2\left(\mu^2+s^2\right)+\sigma_E^2\right)\right),\end{aligned} \quad (55)$$

we get the expression in (20), which completes the proof.

APPENDIX D
PROOF OF COROLLARY 2

The secrecy outage probability can be upper-bounded as:

$$\mathcal{P}_{out}^{1_E}\leq 1+\frac{1}{2}\mathrm{erf}\left(\frac{\mu-\sqrt{\Xi}}{\sqrt{2\sigma^2}}\right)-\frac{1}{2}\mathrm{erf}\left(\frac{\mu+\sqrt{\Xi}}{\sqrt{2\sigma^2}}\right), \quad (56)$$

where $\Xi=\frac{\sigma_E^2}{\zeta^2P^2}\left(\frac{e^{-2Q}}{2\pi\sigma_B^2}(e\zeta^2P^2\tilde{h}^2+2\pi\sigma_B^2)-1\right)$, using high SNR approximation, we could write $\Xi\approx\frac{\sigma_E^2e^{-2Q+1}}{2\pi\sigma_B^2}\tilde{h}^2$. Hence, the outage probability with random orientation can be approximated as:

$$\mathcal{P}_{out}^{1_E}\approx\int_{\tilde{h}=0}^{\kappa_H}f_H(\tilde{h})\left(1+\frac{1}{2}\mathrm{erf}\left(\frac{\mu-\iota_2\tilde{h}}{\sqrt{2\sigma^2}}\right)-\frac{1}{2}\mathrm{erf}\left(\frac{\mu+\iota_2\tilde{h}}{\sqrt{2\sigma^2}}\right)\right)d\tilde{h}. \quad (57)$$

where $\iota_2=\sqrt{\frac{\sigma_E^2e^{-2Q+1}}{2\pi\sigma_B^2}}$, which can be calculated as:

$$\tilde{\mathcal{P}}_{out}^{1_E}\approx\int_{\tilde{h}=0}^{\mu_H}\iota_1\exp\left(\frac{\tilde{h}-\mu_H}{b_H}\right)\mathcal{P}_{out}^{1_E}d\tilde{h}+\int_{\tilde{h}=\mu_H}^{\kappa_H}\iota_1\exp\left(\frac{-\tilde{h}+\mu_H}{b_H}\right)\mathcal{P}_{out}^{1_E}d\tilde{h} \quad (58)$$

which results in (21).

APPENDIX E
PROOF OF PROPOSITION 3

Assuming that colluding eavesdroppers utilise MRC to detect Bob's message, the secrecy capacity at Bob can be calculated as:

$$\mathcal{C}_s^{N_E}\geq\int_{y=0}^{\kappa}\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\left(e\zeta^2P^2h_B^2+2\pi\sigma_B^2\right)\right)f_Y(y)dy-\int_{y=0}^{\kappa}\frac{1}{2}\ln\left(\zeta^2P^2\sum_{i=1}^{N_E}y_i+\sigma_E^2\right)f_Y(y)dy \quad (59)$$

where $y_i=h_{E_i}^2$ and h_{E_i} follows normal distribution, i.e., $h_{E_i}\sim\mathcal{N}(\mu_i,\sigma_i^2)$. Also, κ is the maximum possible value of y. Let $x=\sum_{i=1}^{N_E}y_i$, it follows that x is distributed according to generalized non-central chi-squared-square distribution. For the sake of simplicity we assume that $\sigma_i^2=\sigma^2$ for $i=1,2,\ldots,N_E$. Then the PDF of x can be written as:

$$f_X(x;N_E,\lambda)=\frac{1}{\sigma^2}\sum_{i=0}^{\infty}\frac{e^{\lambda/2}(\lambda/2)^i}{i!}f_{Z_{N_E+2i}}(\frac{z}{\sigma^2}), \quad (60)$$

where N_E specifies the number of degrees of freedom (here this is equal to the number of eavesdroppers) and λ denotes the non-centrality parameter, calculated as: $\lambda=\sum_{i=1}^{N_E}\mu_i^2/\sigma^2$. Also, Z_{N_E+2i} is distributed with the chi-squared probability with N_E+2i degrees of freedom. From (60), the distribution of x is a Poisson-weighted mixture of central chi-squared distributions, which could alternatively be expressed as:

$$f_X(x;N_E,\lambda)=\frac{1}{2^{N_E/2}\,\sigma^{N_E}\,\Gamma(N_E/2)}e^{-\lambda/2}\times{}_0F_1(;\frac{N_E}{2};\frac{\lambda x}{4\sigma^2})e^{-\frac{x}{2\sigma^2}}\,x^{N_E/2-1}, \quad (61)$$

where $\Gamma(n)=(n-1)!$, and ${}_0F_1(;c;w)$ is the confluent hypergeometric function. Thus, the first integral in (59) can

be evaluated as:

$$\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\left(e\zeta^2P^2h_B^2+2\pi\sigma_B^2\right)\right)\times\left(1-\mathcal{Q}_{N_E/2}\left(\sqrt{\lambda},\sqrt{\frac{\kappa N_E}{\sigma^2}}\right)\right) \quad (62)$$

while the second integral can be upper-bounded using Jensen's inequality as:

$$\mathbb{E}\left[\frac{1}{2}\ln\left(\zeta^2P^2x+\sigma_E^2\right)\right]\leq\frac{1}{2}\ln\left(\zeta^2P^2\mathbb{E}[x]+\sigma_E^2\right)\leq\frac{1}{2}\ln\left(\zeta^2P^2\sigma^2(N_E+\lambda)+\sigma_E^2\right), \quad (63)$$

where $\mathbb{E}[x]=\sigma^2(N_E+\lambda)$ is the expectation of random variable x following the PDF in (61). Combining (62) and (63) yields the expression in (22), which completes the proof.

APPENDIX F
PROOF OF COROLLARY 3

Assuming that N_E colluding eavesdroppers combine their SNRs, the outage probability is evaluated as:

$$\begin{aligned}\mathcal{P}_{out}^{N_E}&=\mathbb{P}[\mathcal{C}_s^{N_E}<Q]\\&=\mathbb{P}\Bigg[\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\left(e\zeta^2P^2h_B^2+2\pi\sigma_B^2\right)\right)\\&\quad-\frac{1}{2}\ln\left(\zeta^2P^2\sum_{i=1}^{N_E}y_i+\sigma_E^2\right)<Q\Bigg],\end{aligned} \quad (64)$$

using the PDF of $x=\sum_{i=1}^{N_E}y_i$ in (61), the outage probability can be calculated as:

$$\begin{aligned}\mathcal{P}_{out}^{N_E}&=\mathbb{P}\Bigg[\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\left(e\zeta^2P^2h_B^2+2\pi\sigma_B^2\right)\right)\\&\quad-\frac{1}{2}\ln\left(\zeta^2P^2x+\sigma_E^2\right)<Q\Bigg]\\&=\mathbb{P}\left[x>\frac{\sigma_E^2}{\zeta^2P^2}\left(\frac{e^{-2Q}}{2\pi\sigma_B^2}(e\zeta^2P^2h_B^2+2\pi\sigma_B^2)-1\right)\right]\\&=1-\int_{x=0}^{\Xi}\frac{1}{2^{k/2}\,\sigma^k\,\Gamma(k/2)}e^{-\lambda/2}\,{}_0\\&\quad\times F_1(;\frac{k}{2};\frac{\lambda x}{4\sigma^2})e^{-x/2}\,x^{k/2-1}dx,\end{aligned} \quad (65)$$

where $\Xi=\frac{\sigma_E^2}{\zeta^2P^2}\left(\frac{e^{-2Q}}{2\pi\sigma_B^2}(e\zeta^2P^2h_B^2+2\pi\sigma_B^2)-1\right)$, which yields the expression in (23).

APPENDIX G
PROOF OF PROPOSITION 4

The secrecy capacity can be calculated as:

$$\begin{aligned}\tilde{\mathcal{C}}_s^{N_E}&=\int_{\tilde{h}=0}^{\kappa_H}f_H(\tilde{h})\times\ddot{\mathcal{C}}_s^{1_E}(\tilde{h})\,d\tilde{h}\\&\geq\int_{\tilde{h}=0}^{\kappa_H}f_H\times\frac{1}{2}\ln\left(\frac{\sigma_E^2}{2\pi\sigma_B^2}\left(e\zeta^2P^2\tilde{h}^2+2\pi\sigma_B^2\right)\right)\\&\quad\times\left(1-\mathcal{Q}_{N_E/2}\left(\sqrt{\lambda},\sqrt{\frac{\kappa N_E}{\sigma^2}}\right)\right)d\tilde{h}\\&\quad-\int_{\tilde{h}=0}^{\kappa_H}f_H(\tilde{h})\times\frac{1}{2}\ln\left(\zeta^2P^2\sigma^2(N_E+\lambda)+\sigma_E^2\right)\,d\tilde{h},\end{aligned} \quad (66)$$

following similar steps to the proof of Proposition 2, this evaluates to:

$$\begin{aligned}&\tilde{\mathcal{C}}_s^{N_E}\\&\geq\frac{1}{2}\tilde{\Upsilon}(\kappa)b_H\iota_1e^{-\frac{\mu_H}{b_H}}\left(e^{\frac{\mu_H}{b_H}}\log\left(\frac{e\mu_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)-2\mathrm{Ei}\left(\frac{\mu_H}{b_H}\right)\right)\\&\quad+\frac{1}{2}\tilde{\Upsilon}(\kappa)b_H\iota_1e^{\frac{\mu_H-\kappa_H}{b_H}}\\&\quad\times\left(2e^{\frac{\kappa_H}{b_H}}\mathrm{Ei}\left(-\frac{\kappa_H}{b_H}\right)-\log\left(\frac{e\kappa_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right)\\&\quad-\frac{1}{2}\tilde{\Upsilon}(\kappa)b_H\iota_1\left(2e^{\frac{muH}{b_H}}\mathrm{Ei}\left(-\frac{\mu_H}{b_H}\right)-\log\left(\frac{e\mu_H^2P^2\zeta^2}{2\pi\sigma_B^2}\right)\right)\\&\quad+b_H\iota_1\left(-e^{\frac{\mu_H-\kappa_H}{b_H}}-e^{-\frac{\mu_H}{b_H}}+2\right)\\&\quad\times\left(\frac{1}{2}\tilde{\Upsilon}(\kappa)\log\left(\sigma_E^2\right)-\frac{1}{2}\log\left(P^2\zeta^2\sigma^2(N_E+\lambda)+\sigma_E^2\right)\right),\end{aligned} \quad (67)$$

where $\tilde{\Upsilon}(\kappa)=\left(1-\mathcal{Q}_{N_E/2}\left(\sqrt{\lambda},\sqrt{\frac{\kappa N_E}{\sigma^2}}\right)\right)$, which completes the proof.

REFERENCES

[1] H. Haas, E. Sarbazi, H. Marshoud, and J. Fakidis, "Chapter 11—Visible-light communications and light fidelity," in *Optical Fiber Telecommunications VII*, A. E. Willner, Ed. New York, NY, USA: Academic, 2020, pp. 443–493. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128165027000130

[2] H. Abumarshoud, C. Chen, M. S. Islim, and H. Haas, "Optical wireless communications for cyber-secure ubiquitous wireless networks," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 476, no. 2242, Oct. 2020, Art. no. 20200162.

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

[4] M. Obeed, A. M. Salhab, M.-S. Alouini, and S. A. Zummo, "Survey on physical layer security in optical wireless communication systems," in *Proc. 7th Int. Conf. Commun. Netw. (ComNet)*, Nov. 2018, pp. 1–5.

[5] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. M. Assi, and H. Haas, "Physical layer security for visible light communication systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1887–1908, 3rd Quart., 2020.

[6] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 3342–3347.

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

[8] H. Shen, Y. Deng, W. Xu, and C. Zhao, "Secrecy-oriented transmitter optimization for visible light communication systems," *IEEE Photo. J.*, vol. 8, no. 5, pp. 1–14, Oct. 2016.

[9] M. A. Arfaoui, A. Ghrayeb, and C. M. Assi, "Secrecy performance of multi-user MISO VLC broadcast channels with confidential messages," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7789–7800, Nov. 2018.

[10] 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. 2017.

[11] J.-Y. Wang, Y. Qiu, S.-H. Lin, J.-B. Wang, M. Lin, and C. Liu, "On the secrecy performance of random VLC networks with imperfect CSI and protected zone," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4176–4187, Sep. 2020.
[12] 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.
[13] M. D. Soltani, X. Wu, M. Safari, and H. Haas, "Bidirectional user throughput maximization based on feedback reduction in LiFi networks," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3172–3186, Jul. 2018.
[14] H. Abumarshoud, H. Alshaer, and H. Haas, "Dynamic multiple access configuration in intelligent Lifi attocellular access points," *IEEE Access*, vol. 7, pp. 62126–62141, 2019.
[15] M. D. Soltani, "Analysis of random orientation and user mobility in LiFi networks," Univ. Edinburgh, Edinburgh, Scotland, Tech. Rep., 2019. [Online]. Available: http://hdl.handle.net/1842/35965
[16] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, C. M. Assi, M. Safari, and H. Haas, "Measurements-based channel models for indoor LiFi systems," *IEEE Trans. Wireless Commun.*, vol. 20, no. 2, pp. 827–842, Feb. 2021.
[17] S. Dimitrov and H. Haas, *Principles of LED Light Communications: Towards Networked Li-Fi*. Cambridge, U.K.: Cambridge Univ. Press, 2015.
[18] M. D. Soltani, A. A. Purwita, Z. Zeng, H. Haas, and M. Safari, "Modeling the random orientation of mobile devices: Measurement, analysis and LiFi use case," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2157–2172, Mar. 2019.
[19] C. Chen, D. A. Basnayaka, and H. Haas, "Downlink performance of optical attocell networks," *J. Lightw. Technol.*, vol. 34, no. 1, pp. 137–156, Jan. 1, 2016.
[20] A. A. Purwita, M. D. Soltani, M. Safari, and H. Haas, "Impact of terminal orientation on performance in LiFi systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Barcelona, Spain, Apr. 2018, pp. 1–6.
[21] M. D. Soltani, A. A. Purwita, I. Tavakkolnia, H. Haas, and M. Safari, "Impact of device orientation on error performance of LiFi systems," *IEEE Access*, vol. 7, pp. 41690–41701, 2019.
[22] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no.1, pp. 162–174, Jan. 2018.
[23] 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.
[24] K. Ying, H. Qian, R. J. Baxley, and S. Yao, "Joint optimization of precoder and equalizer in MIMO VLC systems," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1949–1958, Sep. 2015.
[25] H. Marshoud, P. C. Sofotasios, S. Muhaidat, G. K. Karagiannidis, and B. S. Sharif, "On the performance of visible light communication systems with non-orthogonal multiple access," *IEEE Trans. Wireless Commun.*, vol. 16, no. 10, pp. 6350–6364, Oct. 2017.
[26] S. Cho, G. Chen, and J. P. Coon, "Physical layer security in visible light communication systems with randomly located colluding eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 768–771, Oct. 2018.
[27] J.-Y. Wang, C. Liu, J.-B. Wang, Y. Wu, M. Lin, and J. Cheng, "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6423–6436, Dec. 2018.
[28] L. Tan, *Resource Allocation and Performance Optimization in Communication Networks and the Internet*. Boca Raton, FL, USA: CRC Press, 2018.

HANAA ABUMARSHOUD received the M.Sc. and Ph.D. degrees in electrical and computer engineering from Khalifa University, United Arab Emirates, in 2013 and 2017, respectively. She is currently a Research Associate with the LiFi Research and Development Centre, University of Strathclyde, U.K. Her main expertise is the application of information theory and signal processing techniques in visible light communications and LiFi systems with particular focus on intelligent communications, resource allocation, multi-user access, and physical layer security.

MOHAMMAD DEHGHANI SOLTANI received the M.Sc. degree from the Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran, in 2012, and the Ph.D. degree in electrical engineering from The University of Edinburgh, Edinburgh, U.K., in 2019. During his M.Sc., he was studying wireless communications, MIMO coding, and low complexity design of MIMO-OFDM systems. He worked for two years in the telecommunication industry in Iran. His Ph.D. was funded by the British Engineering and Physical Sciences Research Council (EPSRC) Project TOUCAN. During his Ph.D., he was studying visible light communication, mobility and handover management in wireless cellular networks, resource allocation, and user behavior modeling. He is currently a Research Associate with the LiFi Research and Development Centre, The University of Edinburgh, funded by EPSRC "Terabit bidirectional multi-user optical wireless system (TOWS) for 6G LiFi."

MAJID SAFARI (Senior Member, IEEE) received the B.Sc. degree in electrical and computer engineering from the University of Tehran, Iran, in 2003, the M.Sc. degree in electrical engineering from the Sharif University of Technology, Iran, in 2005, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Canada, in 2011. He is currently a Reader with the Institute for Digital Communications, The University of Edinburgh. Before joining Edinburgh in 2013, he held a Postdoctoral Fellowship at McMaster University, Canada. His main research interests include the application of information theory and signal processing in optical communications, including fiber-optic communication, free-space optical communication, visible light communication, and quantum communication. He is currently an Associate Editor of IEEE TRANSACTIONS ON COMMUNICATIONS and was the TPC Co-Chair of the 4th International Workshop on Optical Wireless Communication, in 2015.

HARALD HAAS (Fellow, IEEE) received the Ph.D. degree from The University of Edinburgh, in 2001. He is currently the Director of the LiFi Research and Development Centre, University of Strathclyde. He is also an Initiator, a Co-Founder, and the Chief Scientific Officer of pureLiFi Ltd. He has authored 500 conference papers and journal articles, including papers in *Science* and *Nature Communications*. His main research interests include optical wireless communications, hybrid optical wireless and RF communications, spatial modulation, and interference coordination in wireless networks. His team invented spatial modulation. He introduced LiFi to the public at an invited TED Global talk, in 2011. The talk on Wireless Data from Every Light Bulb has been watched online over 2.72 million times. LiFi was listed among the 50 best inventions in *TIME Magazine*, in 2011. 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 2.75 million times. In 2016, he received the Outstanding Achievement Award from the International Solid State Lighting Alliance. In 2019, he was a recipient of the IEEE Vehicular Society James Evans Avant Garde Award. He was elected as a fellow of the Royal Society of Edinburgh (RSE), in 2017. He received the Royal Society Wolfson Research Merit Award, in 2017, and was elevated to an IEEE Fellow. In 2018, he received a three-year EPSRC Established Career Fellowship extension and was elected as a fellow of the IET and the Royal Academy of Engineering (FREng), in 2019.