# Statistical Modeling and Analysis on the Confidentiality of Indoor VLC Systems

Jian Chen and Tao Shu

***Abstract*— While visible light communication (VLC) is expected to have a wide range of applications in the near future, the security vulnerabilities of this technology have not been well understood so far. In particular, due to the extremely short wavelength of visible light, the VLC channel presents several unique characteristics than its radio frequency counterparts, which impose new features on the VLC security. Taking a physical-layer security perspective, this paper studies the intrinsic secrecy capacity of VLC as induced by its special channel characteristics. Different from existing models that only consider the specular reflection in the VLC channel, a modified Monte Carlo ray tracing model is proposed to account for both the specular and the diffusive reflections, which is unique to VLC. A deep neural network model is also proposed to describe the spatial VLC channel response based on a limited number of channel response samples calculated from the ray tracing model. Based on these models the upper and the lower bounds of the VLC secrecy capacity are derived, which allow us to evaluate the VLC communication confidentiality against a comprehensive set of factors, including the locations of the transmitter, receiver, and eavesdropper, the VLC channel bandwidth, the ratio between the specular and diffusive reflections, and the reflection coefficient. Our results reveal that due to the different types of reflections, the VLC system becomes more vulnerable at specific locations where strong reflections exist.**

***Index Terms*— Physical layer security, indoor VLC, multipath reflection, secrecy capacity.**

## I. Introduction

VISIBLE light communication (VLC), which integrates communication and illumination, has now become a very active research topic in the area of wireless communication. Compared with its radio frequency (RF) counterparts, VLC enjoys many nice features, such as license free, interference free, reusable spectrum, wider bandwidth, higher transmission rate, higher energy efficiency and so on. Because of these nice features, VLC has been considered to be a promising and urgently-needed solution for offloading the crowded RF traffic in fifth generation (5G) networks.

Manuscript received November 21, 2019; revised February 20, 2020; accepted April 6, 2020. Date of publication April 16, 2020; date of current version July 10, 2020. This work was supported in part by the U.S. National Science Foundation (NSF) under Grant CNS-1837034, Grant CNS-1745254, Grant CNS-1659965, and Grant CNS-1460897. This article was presented at the 21st International Conference on Information and Communications Security (ICICS 2019), Beijing, China, in December 2019. The associate editor coordinating the review of this article and approving it for publication was M. Sheng. *(Corresponding author: Tao Shu.)*

The authors are with the Department of Computer Science and Software Engineering, Samuel Ginn College of Engineering, Auburn University, Auburn, AL 36849 USA (e-mail: jzc0111@auburn.edu; tshu@auburn.edu).

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

Digital Object Identifier 10.1109/TWC.2020.2986964

While VLC is expected to have a wide range of applications in the near future, the security vulnerabilities of this technology have not been well understood so far. In typical VLC systems, data is transmitted by modulating the output intensity of the emitters, and the data signal is captured using photo-diodes as receivers. Contrary to the initial belief that VLC is intrinsically secure because the propagation of visible light is directive and can be confined within a closed space, recent studies have revealed that this is not necessarily true, especially in public areas [1], [2]. Without any sort of wave-guiding transmission media, the light illumination that a VLC link piggybacks on is diffusive in most real-world applications, which makes VLC links inherently susceptible to eavesdropping by an unintended receiver in the same room. For example, the diffusive visible light illumination can be easily picked up and recorded by an eavesdropper using a VLC receiver at many locations in the space, and may be analyzed afterwards to reveal the information embedded in the light. Such a unique "what-you-see-is-what-you-get" feature of visible light [3] makes eavesdropping a highly realistic threat to VLC, as its light can be seen at many locations due to its diffusiveness. This threat applies to most public indoor environments, such as libraries, meeting rooms, shopping centers, or aircrafts. Even worse, eavesdropping from outside of the space is possible when there are windows on the wall [1], [4], [5].

In particular, due to the extremely short wavelength of visible light ($0.38 \sim 0.69$ $\mu$m), the VLC channel presents several unique features than its RF counterparts. For example, a VLC channel is a mix of both specular reflection and diffusive reflection, which allows a VLC signal to be overheard (or seen) at much more locations than a RF signal whose reflection is dominantly specular, even when an eavesdropper is outside the main-lobe of the intended VLC communication. As a result, in contrast to the conventional multi-path RF channel, a VLC channel is no longer a discrete sequence of a small number of signal paths, but rather a continuous combination/clusters of signal paths reflected by the entire environment – a direct consequence of the diffusive reflection of visible light. Such a drastic change on channel characteristics imposes new security features on VLC communication, and requires a different method to investigate than its well-studied RF counterparts.

With that in mind, in this work we attempt to investigate the intrinsic confidentiality of VLC communication as induced by its special channel characteristics. We consider the issue of communication confidentiality, because eavesdropping has been foreseen as the most common threats faced by

VLC communications once they are deployed [2], [4], [6]. In contrast to many existing confidentiality studies that take measures at upper layers of the network protocol stack, such as access control, password protection, and end-to-end encryption, our investigation takes a physical-layer security perspective and targets at the fundamental issue of VLC channel's secrecy capacity, by characterizing how easily a VLC signal would be overheard when it is transmitted over the channel. Note that our study aims at understanding the intrinsic security limits faced by the VLC signal itself, which is independent from any cryptographic measures that could be added on the upper layers. Our work is also distinguishable from other VLC security papers [7]–[10] that aim at exploiting physical layer features to provide encryption in the sense that our focus is on the intrinsic information-theoretic secrecy limits of the channel, while their studies are from the operational/implementation perspectives of VLC systems. In practice, our study may lead to a better design of VLC transceivers that possess certain built-in eavesdropping-proofness, and may be used in orthogonal with upper-layer cryptographic methods to further enhance the security of VLC systems.

So far, the study on the secrecy capacity of VLC in the literature is still quite preliminary. Most of the existing models consider the VLC channel as a wiretap channel under line of sight, and have ignored the different types of signal reflections on the channel. In contrast, our study in this paper aims to exploit the unique characteristics of VLC channel in calculating its secrecy capacity. To the best of our knowledge, except for our preliminary conference paper [11], this is the first work that comprehensively considers the impact of both the specular and the diffusive reflections on secrecy capacity of indoor VLC and also investigates the spatial characteristics/distribution of the secrecy capacity over the indoor communication space. More specifically, the main contributions of our study are as follows:

1) A modified Monte Carlo ray tracing method is proposed to account for both the specular and diffusive reflections in calculating VLC channel impulse response at a given location.
2) A deep neural network (DNN) regression model is proposed to efficiently estimate the VLC channel impulse response as a function of the VLC link location in the communication space based on the training data set of a limited number of channel response samples calculated according to the ray tracing model.
3) Based on these models, the upper bound and the lower bound of the VLC secrecy capacity are calculated considering multiple reflections under specific conditions.
4) Leveraging the secrecy capacity bounds, we depict the spatial characteristics/distribution of the VLC secrecy capacity over given indoor communication space.
5) We also study how the multiple types of reflections affect VLC secrecy capacity against a comprehensive set of factors, including the locations of the VLC transmitter, receiver, and eavesdropper, the VLC channel bandwidth, the ratio between the specular and the diffusive reflections, and the reflection coefficient.

The reminder of this paper is organized as follows. Section II describes the related work. VLC system models are presented in Section III, Section IV, and Section V, respectively. Experimental design are presented in Section VI. Evaluations and Discussions are analyzed in Section VII, followed by Conclusions and future work in Section VIII.

## II. Related Work

While the research on VLC has achieved significant development in many fields, such as channel modelling [12]–[15], modulation [16], channel estimation [17]–[19], and channel capacity analysis [20], [21], the security aspect of VLC has not been well understood so far. Existing research on VLC security is preliminary, as evidenced by the limited number of related works and the narrow scope of problems addressed in the literature. In [2], the authors discussed different scenarios of VLC sniffing, and the results of the experiment suggested that VLC channels should not be considered intrinsically secure. Yin and Haas also confirmed the vulnerabilities of multiuser VLC networks by providing an analytical framework to characterize the secrecy performance [22]. Actually due to the broadcast feature of VLC, an unintended receiver within the same communication room may receive the information without being noticed, and this kind of threat could even apply to a scenario that the unintended receiver from outside of the room could eavesdrop merely through the windows or door gaps. The feasibility of such an attack was verified in [5], where an attacker outside a room was able to accurately figure out the program being played on a TV set in the room just by observing the change of light intensity illuminated by the TV through the window. Eavesdropping outside the direct beam of the light was also verified by testbed in [1].

For most cases of securing VLC system, conventional cryptographic methods can be implemented at specific layers of the protocol stack to provide data confidentiality, integrity, and authenticity for VLC applications. The secret keys required by these cryptographic methods can be generated by taking advantage of the physical layer characteristics of the VLC channels, e.g., [23]–[25]. But it is facing great challenges with the elevated capability of computation. As a promising complement to it, physical layer security, mainly represented by non-cryptographic methods, exploits the noise and the structure of the VLC channel to limit the amount of information that can be overheard by unauthorized eavesdroppers [26]–[28].

From an information-theoretic point of view, the physical-layer security was first introduced by Wyner as a wiretap channel model [29]: an eavesdropper sniffs a degraded signal from the main channel. The secrecy capacity is derived as the difference between the information capacity for the two channels. Different with RF communication, which is typically modeled as a Gaussian broadcast channel with an average power constraint at the transmitter side, the signal in VLC is typically modulated onto the intensity of the emitted light, it must satisfy average, peak as well as non-negative amplitude constraints, imposed by practical illumination requirements [20], [21], [30]. Due to the fundamental differences, results

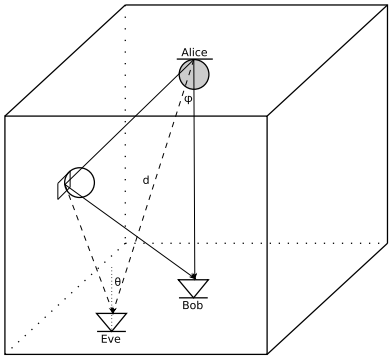



Fig. 1. A typical indoor VLC network system with Alice, Bob and Eve considering reflections.

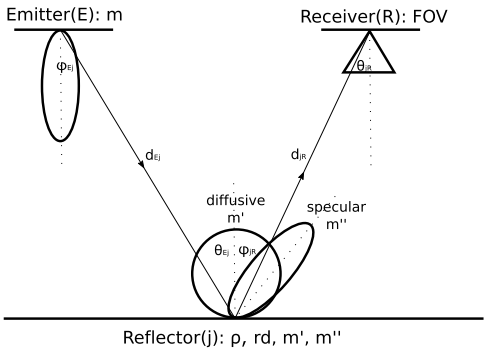



Fig. 2. Reflection pattern is described by Phong's model.

on the secrecy capacity obtained for RF networks can not be directly applied to VLC networks.

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 [31]–[33], with the use of the derived capacity lower and upper bounds in [34]. Mostafa, *et al.* analyzed the achievable secrecy rate for single-input single-output (SISO) and multiple-input single-output (MISO) scenarios, and proposed various beamforming and jamming schemes to enhance the confidentiality of VLC links [27]. In addition, Arfaoui, *et al.* derived in closed-form the achievable secrecy rate as a function of the discrete input distribution for wiretap channel under the amplitude constraints of the input signal [35], [36]. To address the issue of priori knowledge of locations or channel state information of eavesdropper, in [37], [38], Cho, *et al.* investigated the secrecy connectivity in VLC in the presence of randomly located eavesdroppers, and they also study how the multipath reflections affect the secrecy outage probability. However, when considering the multipath reflections, they only deal with the impact of main channel without considering of the inter-symbol interference from multipath reflections.

## III. VLC Channel Modelling

In a typical indoor VLC system (Figure 1), data signal is transmitted by modulating the output intensity of the emitter (Alice), and then it is captured using simple photo-diodes as receivers (Bob or Eve). As the indoor optical wireless channel is significantly different from the RF channel, statistical propagation models developed for the RF, which characterize the multipath fading, can't be directly applied to VLC. Accounting for the multiple types of reflections in the indoor VLC system requires a distinct channel modeling that is able to capture the unique characteristics of a VLC channel. In particular, a VLC channel response could be decomposed into the line of sight (LOS) path component and the non-line of sight (NLOS) path component, which are described respectively as follows.

According to [15], the emitter source is modeled as a generalized Lambertian radiation pattern

$$P(m,\phi) = \frac{m+1}{2\pi}\cos^m(\phi) \tag{1}$$

where $m$ is the Lambertian order defining the radiation lobe, which specifies the directivity of the source, $\phi$ is the angle between the initial direction of ray and the direction of maximum power, which specifies the emitting angle. The coefficient $(m+1)/2\pi$ ensures that integrating radiation intensity pattern over the surface of a hemisphere can obtain the source power. $m = 1$ corresponds to a traditional Lambertian source.

So, the LOS path gain can be calculated as

$$h_{LOS} = P(m,\phi)A_D\cos(\theta)\frac{1}{d^2}\delta(t-\frac{d}{c}) \tag{2}$$

where $A_D$ is the detecting surface area of the receiver, $\theta$ is the incident angle between incident light and the receiver normal direction, product of both gives the effective collection area of the receiver. $d$ is the LOS distance between the emitter and receiver, which depicts the geometric attenuation. $c$ is the speed of light and Dirac delta function gives the time delay.

Multipath channel gain due to the reflections by the walls was studied in [12]. The proposed deterministic model calculated the reflection channel gain by partitioning a wall into many elementary reflectors and summing up the impulse response contributions from different reflectors as secondary sources until reaching the time limit. However, there is a problem with this model, in that they only take into account diffusive reflection and can't simulate specular reflection when light reaches a wall. In reality, for grazing incidence there is strong specular reflection with quite different behavior. If there are polished surface, such as windows or mirrors, the specular reflection is dominant over diffusive reflection. In order to consider the high specular reflection of smooth surfaces, here we use the Phong's model to approximate the reflection patterns (Figure 2), considered as the sum of the diffusive component and the specular component [18], [39]. In this model, the surface characteristics are defined by two parameters: the percentage of incident signal that is reflected diffusely $r_d$ and the directivity of the specular component of the reflection $m''$. Due to the high attenuation, in this paper, we consider only the first reflection since the channel gain of the higher order reflections is small enough to be neglected [18].

So, the NLOS path gain can be described as

$$\begin{aligned} h_{NLOS} = \sum_{j=1}^{n} & P(m,\phi_{Ej})\Delta A\cos(\theta_{Ej})\frac{1}{d_{Ej}^2}\rho_j\Big[r_{dj}P(m',\phi_{jR}) \\ & +(1-r_{dj})P(m'',\phi_{jR}-\theta_{Ej})\Big]A_D\cos(\theta_{jR}) \\ & \times\frac{1}{d_{jR}^2}\delta\left(t-\frac{d_{Ej}+d_{jR}}{c}\right) \end{aligned} \tag{3}$$

TABLE I
MAIN NOTATIONS

| Notation | Explanation | Notation | Explanation |
|---|---|---|---|
| $m, m', m''$ | Lambertian directivity order | $I_{LOS}$ | LOS intensity |
| $\phi$ | Emitter radiation angle | $I_{NLOS}$ | NLOS intensity |
| $\theta$ | Receiver incident angle | $\Delta t$ | Time delay between NLOS and LOS |
| $d$ | Transmission distance | $\alpha, \beta$ | Gamma fitting parameters |
| $\rho$ | Reflection coefficient | $H_B, H_E$ | Channel gain |
| $r_d$ | Diffusive percentage | $\sigma_B^2, \sigma_E^2$ | Variance of noise |
| $\Delta A$ | Reflector effective area | $I(X;Y)$ | Mutual information between X and Y |
| $A_D$ | Receiver effective area | $\xi$ | Dimming target |
| $c$ | Speed of light | $A$ | Maximum optical intensity |

where the wall is divided into n grid reflectors, each of which has an area of $\Delta A$, $\rho$ is the surface reflection coefficient, $m'$ gives the directivity of the diffusive reflection component and $m''$ gives the directivity of the specular reflection component, $\phi$ and $\theta$ represent emitting angle and incident angle, respectively. Such a model is general enough to accommodate various reflection settings of the wall. For example, for a wall of homogeneous material, $\rho_j$ and $r_{dj}$ are identical for all the grids, so the subscript j can be dropped in the notation, resulting in a common setting of $\rho$ and $r_d$ in the channel model. For a wall of heterogeneous materials, e.g., a glass window embedded in the wall, different $\rho_j$ and $r_{dj}$ should be used for different areas of the wall, reflecting the heterogeneous reflection behavior of the different parts of the wall.

Therefore, the channel gain considering both the LOS and NLOS can be described as

$$H = h_{LOS} + h_{NLOS}. \tag{4}$$

We use a modified Monte Carlo ray-tracing statistical approach to numerically calculate the channel impulse response, as explained later in the experimental section. In case that the consideration of higher order reflections is desirable, it can be recursively calculated by a nested ray tracing model. For example, the second-order reflection can be considered by treating the first-order reflected light at each grid as a secondary light illumination source. For each secondary light source, the proposed Monte Carlo ray tracing model (Equations (2) and (3)) can be applied to compute its contribution to the second-order reflection. The actual second-order reflection is just the summation of the contribution from all secondary light sources.

To improve the readability of our paper, we summarized the main notation in Table I.

## IV. CHANNEL IMPULSE RESPONSE FITTING AND SYNTHESIZING

Although the channel impulse response with multiple reflections could be numerically calculated using different approaches, there is lacking an analytical expression for it in current literature. The main drawback of the numerical methods is their excessive computational time complexity. Due to the additional NLOS reflections, numerical computation of the impulse response of a single VLC channel turns out to be very time consuming, and it becomes even more prohibitive when one needs to calculate the channel response as a function of the VLC link location over the entire communication space, e.g., to characterize the spatial distribution of the VLC channel secrecy capacity. Therefore, for the very first time, we propose a fast analytical approach to synthesize channel impulse response using gamma probability distribution function fitting and Deep Neural Network regression.

### A. Channel Impulse Response Fitting as a Gamma Probability Distribution

When analyzing the numerically calculated channel impulse response (Figure 3(a)), we notice that it could be divided into two distinct components, LOS and NLOS. The LOS component is a scalar channel gain related to the propagation attenuation of the VLC signal over the distance between the transmitter and the receiver, and can be easily calculated according to the channel model and system geometry. On the other hand, however, the NLOS component is much more complicated, as it presents some time-series structure, as shown in Figure 3(b), where the NLOS impulse response has been normalized by the total NLOS light intensity. Based on the fact that the integral of the normalized NLOS time series equals to one, we hypothesize that this time series can be fitted analytically by some probabilistic distribution function. Physically, this hypothesis reflects the insight that the NLOS channel response is actually the distribution of the reflected light power over different time delays [40]. To verify our hypothesis, we have tested a number of probabilistic distribution functions, among which the gamma distribution turns out to be the most promising one for the fitting.

A gamma distribution can be parameterized in terms of a shape parameter $\alpha$ and a rate parameter $\beta$. The corresponding probability density function (PDF) in the shape-rate parametrization is

$$f(x;\alpha,\beta) = \frac{\beta^\alpha x^{\alpha-1} e^{-\beta x}}{\Gamma(\alpha)}; \quad x > 0; \alpha, \beta > 0 \tag{5}$$

where $\Gamma(\alpha)$ is the gamma function. Given a numerically computed NLOS channel response, its fitted gamma distribution expression (i.e., the fitted parameters $(\alpha, \beta)$) can be obtained by nonlinear regression. For instance, Figure 3(c) plots the fitted gamma distribution function for the numerically calculated and normalized NLOS channel impulse response in Figure 3(b). The fitting in this case turns out to be

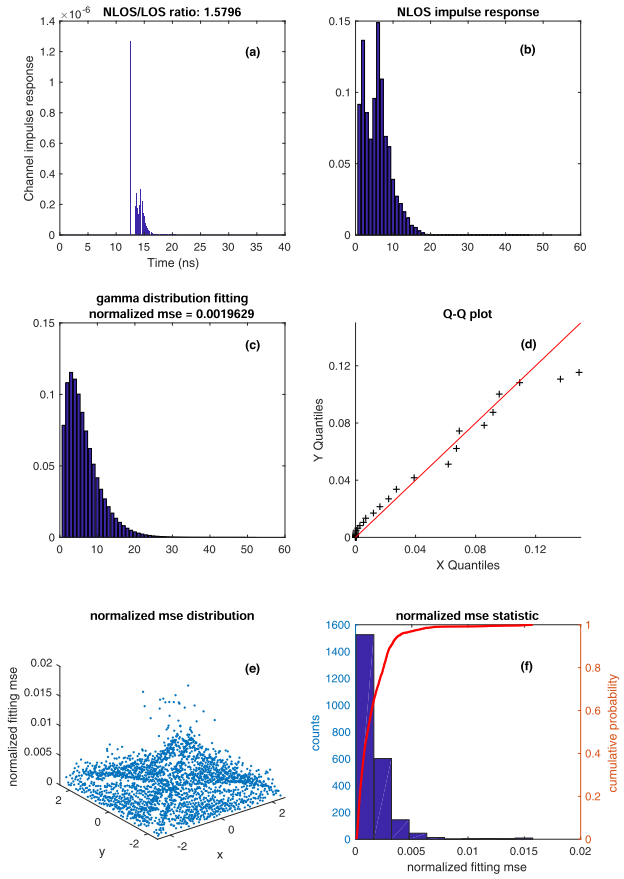



Fig. 3. A typical example of channel impulse response fitting. (a) a numerically calculated channel impulse response with LOS and NLOS; (b) the NLOS impulse response normalized with total NLOS intensity; (c) the fitted NLOS impulse response; (d) Q-Q plot to evaluate the fitting result; (e) normalized fitting mse spatial distribution over the experimental area; (f) normalized fitting mse statistic from e.

very accurate according to the normalized mean square error (normalized $mse < 0.002$). To graphically assess how well the numerical calculation matches with the fitted gamma distribution, a scatter quantile-quantile (Q-Q) plot is shown in Figure 3(d), where the calculated set (X) and fitted set (Y) of quantiles are plotted against each other. The cross points (+) are referred to as percentiles, below which a certain proportion of the data fall. Ideally, if X and Y quantiles come from the same distribution, then all + marks should be aligned along the diagonal line (the red line in the figure). Indeed, it can be observed in Figure 3(d) that most of the + marks are aligned well with the diagonal line, except a couple exceptions, which are just a little off the diagonal line. This observation confirms that the fitted gamma distribution matches reasonably well with the numerical calculations.

In order to statistically verify the accuracy of gamma fitting for more general cases, we compared the calculated NLOS channel response against their gamma fitting outcomes in Figures 3(e) and 3(f) for 2401 VLC channels, which are taken over a 49-by-49-grid area with a distance interval of 0.1 m per grid, in an indoor VLC communication environment. According to the spatial distribution of the normalized mse in Figure 3(e) and the normalized mse histogram and cumulative

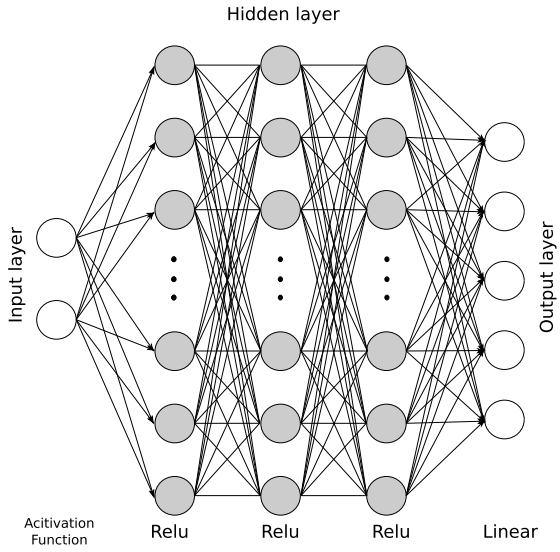



Fig. 4. Framework of the DNN regression model. Input layer includes the x and y coordinates of receiver, output layer includes the fitted parameters for synthesizing impulse response, each of the three hidden layers includes 64 neurons. The DNN is fully connected between each adjacent layers. The activation function for each layer is listed at the bottom.

density function (CDF) in Figure 3(f), it can be observed that more than 2200 (i.e., over 90% of the tested VLC channels) channel impulse responses fitting achieve normalized mse less than 0.005. This exemplifies the accuracy and reliability of the proposed gamma distribution fitting in general cases.

### *B. Channel Impulse Response Synthesizing With Deep Neural Network Regression*

Now we can analytically express the channel impulse response as a LOS scalar plus a NLOS gamma distribution, for which the key parameters include LOS intensity $I_{LOS}$, NLOS intensity $I_{NLOS}$, the time delay $\Delta t$ between NLOS and LOS, $\alpha$, and $\beta$. Although we can get those key parameters for some sample locations using numeric calculations, it becomes prohibitive when calculating the channel impulse response at an arbitrary location. Being aware of those key parameters are following nonlinear distribution over locations from the numeric samples, we develop a Deep Neural Network (DNN) regressor to model the key parameters of channel impulse response at an arbitrary location. In order to keep the DNN regressor as simple but effective as possible and avoid over-fitting, we defined a 4-layer deep neural network model with 3 hidden layers of 64 neurons through empirical experiments as shown in Figure 4. To simplify our analysis, but without loss of generality, we assume that the location of the VLC transmitter is fixed in the middle of the ceiling, and are interested in obtaining the channel impulse response as a function of the receiver's location. Accordingly, the proposed DNN has two inputs, the $x$ and $y$ coordinates of the receiver's location, and five outputs, $I_{LOS}$, $I_{NLOS}$, $\Delta t$, $\alpha$, and $\beta$. Each of the three hidden layers includes 64 neurons with their own sets of parameters. The DNN model is set as a sequential model with loss function specified as mean square error and optimizer specified as Adam, and each layer inside this model

is fully connected between its adjacent layers. As the DNN model is used as a nonlinear regression model, the activation function of the last layer is specified as linear function and the activation function for three hidden layers is set as rectified linear unit (ReLU), which is nonlinear.

The DNN regression model needs to be trained and tested before it can be used for channel response prediction at an arbitrary receiver location. The detailed procedure for DNN training and testing is presented in Section VI. Based on the predicted channel response parameters, the channel impulse response at a given receiver location can be represented analytically as

$$H = I_{LOS}\delta(t - \frac{d}{c}) + I_{NLOS}f(t - \frac{d}{c} - \Delta t; \alpha, \beta) \quad (6)$$

where $\frac{d}{c}$ is the light propagation delay between the transmitter and the receiver by following the LOS path, and $f$ is the Gamma distribution function. The proposed DNN regression allows us to efficiently obtain the channel impulse response at an arbitrary location based on an analytic function, rather than time-consuming numerical calculations.

## V. Secrecy Capacity Analysis

Consider an indoor VLC system consisting of a transmitter Alice, an intended receiver Bob, and an eavesdropper Eve, as shown in Figure 1. Due to the diffusive and specular reflections of light, the signal transmitted from Alice to Bob may also be overheard by Eve. The received signals at Bob and Even can be represented respectively by

$$\begin{cases} Y_B = H_B X + Z_B, Z_B \sim N(0, \sigma_B^2) \\ Y_E = H_E X + Z_E, Z_E \sim N(0, \sigma_E^2) \end{cases} \quad (7)$$

where $X$ denotes the transmitted light intensity from Alice, $H_B$ and $H_E$ denote the main channel gain, defined between Alice and Bob, and the wiretap channel gain, defined between Alice and Eve, respectively. $Z_B$ and $Z_E$ are zero-mean additive white Gaussian noise (AWGN) at Bob and Eve, respectively, which are assumed to be independent from each other. The variance of noise $\sigma_k^2 (k = B, E)$ is given by [41]

$$\begin{cases} \sigma_k^2 = \sigma^2 + W_{ISI} \\ \sigma^2 = \sigma_{thermal}^2 + \sigma_{shot}^2 \end{cases} \quad (8)$$

where $\sigma_{thermal}^2$ and $\sigma_{shot}^2$ denote variances of the thermal noise in the receiver electronic circuits and the shot noise caused by ambient illumination from other light sources, respectively. These two noises are well modeled by an additive white Gaussian process. $W_{ISI}$ denotes the inter-symbol interference (ISI) caused by the multiple reflections in a VLC channel, which may become significant under high symbol transmission rate. This is illustrated in Figure 5, where the ISI for symbol 4 (S4) accounts for the accumulated power from all previous symbols (S1, S2, S3) over S4's reception window $[4t, 5t]$, where $t = 1/B$ is the reception time duration of a symbol at the receiver and $B$ is simply the symbol rate of the VLC channel (binary intensity modulation is assumed). From this figure, it is clear that the received signal power and the ISI of a symbol (light pulse) can be calculated by partitioning

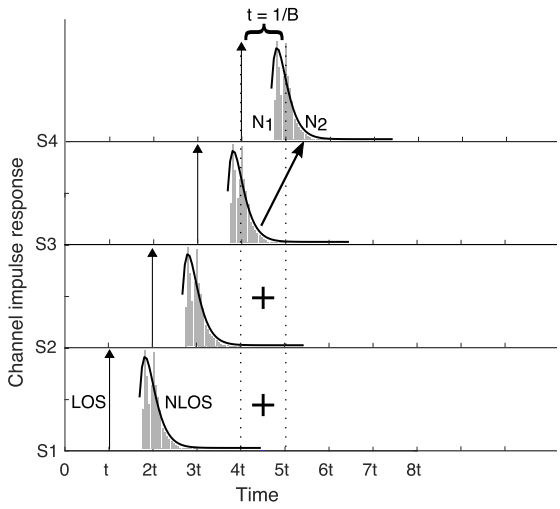



Fig. 5. Impact of ISI on system model caused by reflection. S stands for Symbol, t stands for inter symbol time interval.

the channel impulse response into two parts according to the symbol's reception window: The first part, denoted by $N_1$ in the figure, accounts for the first $t$ seconds of the channel response inside the reception window, as measured beginning from the LOS component. The integral of $N_1$ contributes to the received signal power of the symbol. On the other hand, the second part, denoted by $N_2$ in the figure, includes all the remainder outside the reception window, whose integral amounts to the ISI ($W_{ISI}$) to the received symbol. So, $H_k$ and $\sigma_k^2$ can be represented by

$$\begin{cases} H_k = N_1^{(k)} \\ \sigma_k^2 = \sigma^2 + N_2^{(k)} \end{cases} \quad k = B, E. \quad (9)$$

where $N_1^{(k)}$ and $N_2^{(k)}$ are the integral of $N_1$ and $N_2$ defined w.r.t. the channel response at receiver $k$, respectively.

The secrecy capacity of a channel is a notion in the information-theoretic security and it represents the maximum transmission rate at which the eavesdropper is unable to decode any information while the intended receiver is able to receive all information error-free. It has been shown that under the additive white Gaussian noise (AWGN) main channel and wiretap channel model, the secrecy capacity amounts to the difference between the main channel capacity and the wiretap channel capacity. Based on (7), if $H_B \leq H_E$, which means the main channel is stochastically degraded by the wiretap channel, the secrecy capacity $C$ is essentially zero. Alternatively, if $H_B > H_E$, the secrecy capacity $C$ in the same VLC network can be mathematically expressed as [31], [32], [34]

$$C = \max_{f_X(x)} [I(X; Y_B) - I(X; Y_E)] \quad s.t. \begin{cases} \int_0^A f_X(x)dx = 1; & 0 \leq X \leq A \\ E(X) = \int_0^A x f_X(x)dx = \xi A; & \xi \in (0, 1] \end{cases} \quad (10)$$

where $f_X(x)$ denotes the PDF of X, $I(X;Y)$ denotes the mutual information between two variables X and Y. $A$ denotes

the maximum peak optical intensity of the transmitter, $\xi$ is the dimming target. For a practical system, the maximum optical intensity will be constrained by $A$ and the dimmable average optical intensity will be constrained by $\xi$ to satisfy the consistent illumination requirements.

Since the secrecy capacity is related to the information capacity of the communication channel, 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 our knowledge, the exact information capacity of the VLC channel with such constraints still remains unknown, even for the simplest SISO case, except that some lower and upper bounds have been derived [20], [31], [34]. In this paper, as we aim to study the impact of multiple reflections on secrecy capacity, our analysis will be based on the lower and upper bounds of the secrecy capacity. In particular, accounting for the new structure of the received signal and ISI (9) as induced by the multiple types of reflections in the VLC channel, and by following a similar derivation process in [31], [32], [34], we obtain a new set of lower bound and upper bound on the VLC channel secrecy capacity when the diffusive reflection and the specular reflection in the channel are considered.

*Proposition 1:* a lower bound for (10) is given by

$$C \geq \frac{1}{2} ln \left[ \frac{3(\sigma^2 + N_2^{(E)})(N_1^{(B)2} A^2 + 2\pi e N_2^{(B)} + 2\pi e \sigma^2)}{2\pi e(\sigma^2 + N_2^{(B)})(N_1^{(E)2} \xi^2 A^2 + 3N_2^{(E)} + 3\sigma^2)} \right]. \tag{11}$$

*Proof:* The proposition can be proved by following the framework in [31], [32], [34]. For simplicity, we choose the average-to-peak optical intensity ratio $\xi = 0.5$ and rewrite the objective function in (10) in entropy as

$$C = \max_{f_X(x)} [\mathcal{H}(Y_B) - \mathcal{H}(Y_E)] - \mathcal{H}(Y_B|X) + \mathcal{H}(Y_E|X) \tag{12}$$

then using the entropy power inequality in [42] and given $\mathcal{H}(Y_B|X) = \frac{1}{2} ln(2\pi e(\sigma^2 + N_2^{(B)}))$, $\mathcal{H}(Y_E|X) = \frac{1}{2} ln(2\pi e(\sigma^2 + N_2^{(E)}))$,

$$C \geq \max_{f_X(x)} \left[ \frac{1}{2} ln(e^{2\mathcal{H}(N_1^{(B)} X)} + e^{2\mathcal{H}(Z_B)}) - \frac{1}{2} ln(2\pi e \mathbf{var}(Y_E)) \right] + \frac{1}{2} ln(\frac{\sigma^2 + N_2^{(E)}}{\sigma^2 + N_2^{(B)}}) \tag{13}$$

moreover, we have $\mathcal{H}(N_1^{(B)} X) = \mathcal{H}(X) + ln(N_1^{(B)})$ and $\mathcal{H}(Z_B) = ln(\sqrt{2\pi e(\sigma^2 + N_2^{(B)})})$, so

$$C \geq \max_{f_X(x)} \left[ \frac{1}{2} ln(e^{2(\mathcal{H}(X) + ln(N_1^{(B)}))} + 2\pi e \sigma^2 + 2\pi e N_2^{(B)}) - \frac{1}{2} ln(2\pi e \mathbf{var}(Y_E)) \right] + \frac{1}{2} ln(\frac{\sigma^2 + N_2^{(E)}}{\sigma^2 + N_2^{(B)}}) \tag{14}$$

by choosing an arbitrary input PDF $f_X(x)$ under the given constraints in (10), we can solve the functional optimization problem using the variational method, then $\mathcal{H}(X)$ and $\mathbf{var}(Y_E)$ can be written as

$$\mathcal{H}(X) = ln(A); \mathbf{var}(Y_E) = N_1^{(E)2} \frac{\xi^2 A^2}{3} + \sigma^2 + N_2^{(E)} \tag{15}$$

therefore, substituting (15) into (14), the lower bound on secrecy capacity for $\xi = 0.5$ can be derived.

*Proposition 2:* an upper bound for (10) is given by

$$\begin{aligned} C \leq \frac{1}{2} ln \Bigg\{ & \left[ \left( (1 + \frac{N_1^{(E)2}}{N_1^{(B)2}}) \sigma^2 + \frac{N_1^{(E)2}}{N_1^{(B)2}} N_2^{(B)} + N_2^{(E)} \right) \right. \\ & \left. \times \left( N_1^{(B)2} A^2 \xi + N_2^{(B)} + \sigma^2 \right) \right] \Big/ \left[ \left( \sigma^2 + N_2^{(B)} \right) \right. \\ & \times \left( N_1^{(E)2} A^2 \xi + 2 \frac{N_1^{(E)2}}{N_1^{(B)2}} N_2^{(B)} + N_2^{(E)} \right. \\ & \left. + (1 + 2 \frac{N_1^{(E)2}}{N_1^{(B)2}}) \sigma^2 \right) \\ & \left. \times \left( 1 + \frac{N_1^{(E)2} (\sigma^2 + N_2^{(B)})}{N_1^{(B)2} (\sigma^2 + N_2^{(E)})} \right) \right] \Bigg\}. \end{aligned} \tag{16}$$

*Proof:* The proposition can be proved by following the framework in [31], [32], [34]. The dual expression of the secrecy capacity is employed when deriving the upper bound as in [34]. Given an arbitrary conditional PDF $g_{Y_B|Y_E}(y_B|y_E)$, we have the relative entropy equation

$$\begin{aligned} & I(X; Y_B|Y_E) + E_{XY_E} \{ D(f_{Y_B|Y_E}(y_B|Y_E) || g_{Y_B|Y_E}(y_B|Y_E)) \} \\ & = E_{XY_E} \{ D(f_{Y_B|XY_E}(y_B|X, Y_E) || g_{Y_B|Y_E}(y_B|Y_E)) \} \end{aligned} \tag{17}$$

according to the non-negative property of the relative entropy, we have

$$\begin{aligned} & I(X; Y_B|Y_E) \\ & \leq E_{XY_E} \{ D(f_{Y_B|XY_E}(y_B|X, Y_E) || g_{Y_B|Y_E}(y_B|Y_E)) \} \end{aligned} \tag{18}$$

considering the constrains in (10), we can find an unique PDF $f_{X'}(x)$ that maximizes $I(X; Y_B|Y_E)$, which will lead to the secrecy capacity

$$\begin{aligned} C & \leq E_{X'Y_E} \{ D(f_{Y_B|XY_E}(y_B|X, Y_E) || g_{Y_B|Y_E}(y_B|Y_E)) \} \\ & = E_{X'} \left\{ \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f_{Y_B Y_E|X}(y_B, y_E|X) \right. \\ & \qquad \left. \times ln \left[ \frac{f_{Y_B|XY_E}(y_B|X, y_E)}{g_{Y_B|Y_E}(y_B|y_E)} \right] dy_B dy_E \right\} \\ & = E_{X'} \left\{ \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f_{Y_B Y_E|X}(y_B, y_E|X) \right. \\ & \qquad \left. \times ln[f_{Y_B|XY_E}(y_B|X, y_E)] dy_B dy_E \right\} \\ & \quad - E_{X'} \left\{ \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f_{Y_B Y_E|X}(y_B, y_E|X) \right. \\ & \qquad \left. \times ln[g_{Y_B|Y_E}(y_B|y_E)] dy_B dy_E \right\} \end{aligned} \tag{19}$$

each parts in (19) can be rewritten as

$$\begin{aligned} &E_{X'}\Big\{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_{Y_B Y_E|X}(y_B,y_E|X) \\ &\qquad \times ln[f_{Y_B|XY_E}(y_B|X,y_E)]dy_B dy_E\Big\} \\ &= -[\mathcal{H}(Y_B|X') + \mathcal{H}(Y_E|X',Y_B) - \mathcal{H}(Y_E|X')] \\ &= -\frac{1}{2} ln\left[2\pi e(\sigma^2 + N_2^{(B)})(1 + \frac{N_1^{(E)2}(\sigma^2 + N_2^{(B)})}{N_1^{(B)2}(\sigma^2 + N_2^{(E)})})\right] \end{aligned} \tag{20}$$

and

$$\begin{aligned} &E_{X'}\Big\{\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_{Y_B Y_E|X}(y_B,y_E|X) \\ &\qquad \times ln[g_{Y_B|Y_E}(y_B|y_E)]dy_B dy_E\Big\} \\ &= -\frac{1}{2} ln(2\pi s^2) \\ &\quad - E_{X'}\Big\{\Big[(1-\mu\frac{N_1^{(E)}}{N_1^{(B)}})^2(N_1^{(B)2}X^2 + \sigma^2 + N_2^{(B)}) \\ &\quad +\mu^2((1+\frac{N_1^{(E)2}}{N_1^{(B)2}})\sigma^2 + \frac{N_1^{(E)2}}{N_1^{(B)2}}N_2^{(B)} + N_2^{(E)})\Big]\Big/2s^2\Big\} \\ &\geq -\frac{1}{2} ln\Big[2\pi e\Big((1+\frac{N_1^{(E)2}}{N_1^{(B)2}})\sigma^2 + \frac{N_1^{(E)2}}{N_1^{(B)2}}N_2^{(B)} + N_2^{(E)}\Big) \\ &\quad \Big(N_1^{(B)2}A^2\xi + N_2^{(B)} + \sigma^2\Big)\Big/\Big(N_1^{(E)2}A^2\xi + 2\frac{N_1^{(E)2}}{N_1^{(B)2}}N_2^{(B)} \\ &\quad +N_2^{(E)} + (1+2\frac{N_1^{(E)2}}{N_1^{(B)2}})\sigma^2\Big)\Big] \end{aligned} \tag{21}$$

therefore, substituting (20) and (21) into (19), the upper bound on secrecy capacity can be derived.

## VI. Experimental Design

Without loss of generality, we design an indoor VLC environment with 5 m in length, 5 m in width, and 3 m in height. Similar to Figure 1, the emitter is fixed at the center of ceiling and the receiver is placed on the receiver plane with a height of 0.85 m that is close to the height of a regular desk. We partition the receiver plane into small grid area with length of 0.1 m, resulting in 49-by-49-grid points taken as potential receiver location. Additional parameters assumed in the calculation are listed in table II. The default parameter value will be taken from the table hereafter if not specified.

We use a modified Monte Carlo ray tracing model from [18] and [43] for numerical calculation of the channel impulse response. Our calculation is implemented using Matlab R2017a. Firstly, a large number of rays are randomly generated according to the radiation pattern from the emitter. When a ray impinges on a wall, the reflection point is converted into a new optical source, so a new ray is generated with a similar distribution as the reflection pattern of that wall. In order to consider both the specular and diffusive reflections, when a ray arrives at the wall, a random number in the range (0, 1) is generated. If the generated number is smaller than the diffusive percentage $r_d$, the reflection for this ray is determined to be purely diffusive; otherwise, it becomes a specular reflection. This treatment ensures that among all the rays reflected by any small contiguous area of the wall, we can expect that $r_d$ fraction of them represent the diffusive reflection and $(1 - r_d)$ fraction of them represent specular reflection, which is consistent with our model in (3). After each reflection the power of the ray is reduced by the reflection coefficient of the wall. Since this model implements both diffusive and specular reflections, so it can represent real world scenarios more plausibly.

TABLE II
Numerical Calculation Parameters

| | Parameter | Value |
|---|---|---|
| Room | Room size | $5 \times 5 \times 3\,m^2$ |
| | Reflection Coefficient ($\rho$) | 0.8 |
| | Diffusive Percentage ($r_d$) | 75% |
| Emitter | Emitter height | 3 m |
| | Emitted Optical Power | 1 W |
| | Number of Rays | 68000 |
| | Modulation Bandwidth | 500 MHz |
| | Lambertian Order ($m, m', m''$) | (1, 1, 250) |
| Receiver | Receiver height except $B_1', E_2', E_3'$ | 0.85 m |
| | Receiver height for $B_1', E_2', E_3'$ | 1.45, 0.25, 0.25 m |
| | Receiver Effective Area | $10^{-4}\,m^2$ |
| | Receiver FOV | $60^\circ$ |
| | Resolution ($\Delta t$) | 0.2 ns |

Then for each of the calculated 2401 channel impulse responses from 49-by-49-grid receivers, we use the nonlinear regression model in Matlab to fit the NLOS part of channel impulse response as gamma probability distribution. So far, we can get the seven key parameter sets, including receiver location coordinates, LOS intensity, NLOS intensity, the time delay $\Delta t$ between NLOS and LOS, $\alpha$, and $\beta$, which will be used as training dataset for the DNN regression model. Before feeding the training dataset into the DNN regression model, it has been preprocessed. Min-Max normalization is applied to the training dataset to guarantee stable convergence. For the sake of enabling fast and easy experimentation, the DNN regression model is implemented on Keras [44], which is a high-level neural networks Python library for deep learning and running on top of TensorFlow. The training dataset are split into two parts, of which 90% are used to fit the model and the left 10% are used to evaluate the fitting result. The two evaluation metrics mean square error and mean absolute value are shown in Figure 6. The overlapped curves of training and testing show the comparable error level, which indicates the DNN regression model is neither over-fitted nor under-fitted. Since mean square error gives a relatively high weight to large errors, mean absolute error is used to show average deviation of fitted parameters. Both of the two metrics rapidly converge to a relative low error level, which confirms the efficacy and veracity of the training process. To give a more intuitive evaluation of the trained DNN regression model, we predicate the key parameters at the same locations of calculated training dataset. Comparison between the calculated and fitted parameters is shown in Figure 7. The calculated and

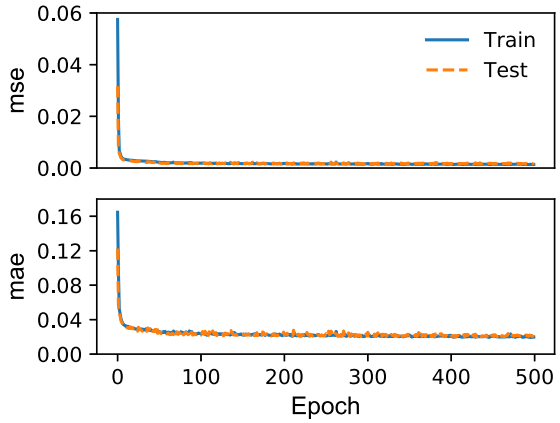



Fig. 6. Loss function plot that shows the fitting residuals, MSE - mean square error and MAE - mean absolute error. An epoch refers to a training iteration with a random portion of training dataset.

fitted parameters for $\Delta t$, $I_{LOS}$, and $I_{NLOS}$, match well with each other. For $\alpha$ and $\beta$, we can also observe a reasonably good match on most of the grids except for a few mismatch over the diagonal line. In terms of the relative low fitting error level, the overall accuracy should be taken as valid.

Once the DNN regression model finishes training and testing, it can be used to predict the key parameters for synthesizing channel impulse response at any possible location inside the indoor VLC system. Finally, the synthesized channel impulse response could be substituted into equations (11) and (16) to calculate the corresponding secrecy capacity lower and upper bound. In order to quantitatively present the secrecy capacity bounds, we set the dimming target $\xi$ as 0.5 during calculation.

## VII. Evaluations and Discussions

In order to test the key factors that impact the secrecy capacity, we create different scenarios by changing the locations of Bob and Eve, shown as in Figure 8. It shows the planimetric position of Alice (yellow illuminant), Bob (black triangle), and Eve (empty triangle), with Alice locates on the ceiling, Bob and Eve locates on the receiver plane. As shown in Figure 9, when fixing Alice at $A_1$, Bob at $B_1$, the secrecy capacity changes with the optimal peak intensity $A$ when Eve locates at $E_2$ and $E_3$, respectively. It is worth noting that our derivations of the upper and lower bounds are valid only when $A \geq 0$ dB, otherwise the secrecy capacity would be 0 (for $A < 0$ dB). As the increase of $A$, the secrecy capacity also increases accordingly until it saturates, which is consistent with previous study [31]. Moreover, if we move Eve from $E_2$ to $E_3$, the secrecy capacity increases as a result of degradation of communication channel, which indicates that the system security performance depends on the relative strength of the main channel compared to the wiretap channel. As we discussed before, for a practical VLC system, the maximum optical intensity will be constrained by $A$ to satisfy the consistent illumination requirements. Considering maximizing the secrecy capacity and energy efficiency, we can refer to Figure 9 to find the minimum $A$ that saturates the secrecy

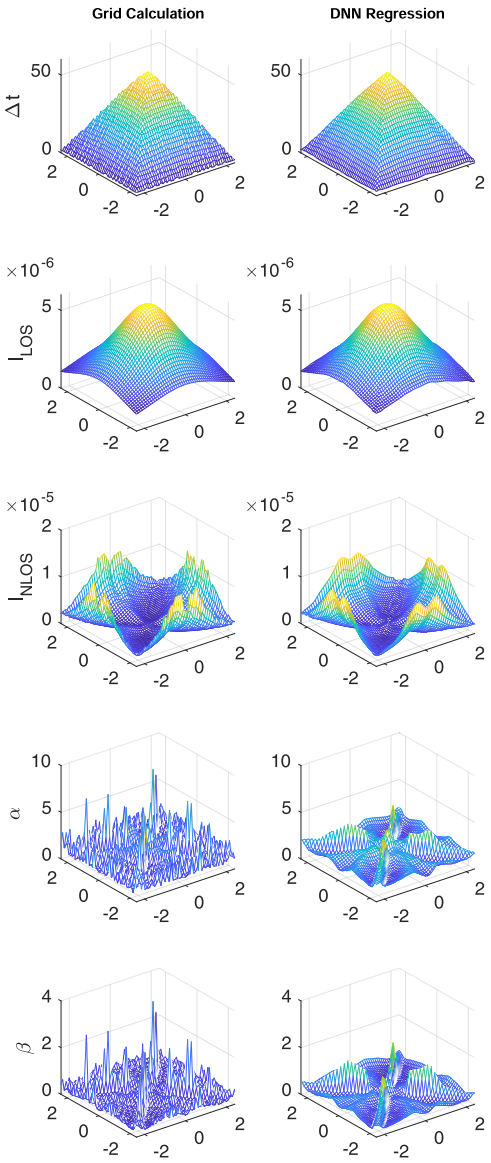



Fig. 7. Calculated and fitted parameters comparison for $\Delta t$, LOS intensity, NLOS intensity, $\alpha$, $\beta$. Left and right columns refer to the calculated and fitted results, respectively.

capacity as the maximum optical intensity. It can also be observed from Figure 9 that, while our upper and lower bounds are reasonably tight in the high secrecy capacity regime (i.e., for the cases of $(A_1, B_1', E_2')$ and $(A_1, B_1', E_3')$), they are relatively loose in the low secrecy capacity regime (the cases of $(A_1, B_1, E_2)$ and $(A_1, B_1, E_3)$). In particular, let the tightness of the bounds be defined as the ratio of the gap between the upper bound and the lower bound to the value of the lower bound. It can be observed from this figure that, when $A \geq 20$ dB, the tightness of the bounds is smaller than 8% for the case of $(A_1, B_1', E_3')$, and is smaller than 10% for the case of $(A_1, B_1', E_2')$. Such a tightness should be reasonably sufficient from an engineering's point of view. How to improve the bounds in the low secrecy capacity regime is out of the scope of this paper, and will be pursued in our future study.

In the following subsections, some additional numerical results are provided to show the security performance of the indoor VLC system with multiple reflections considered.

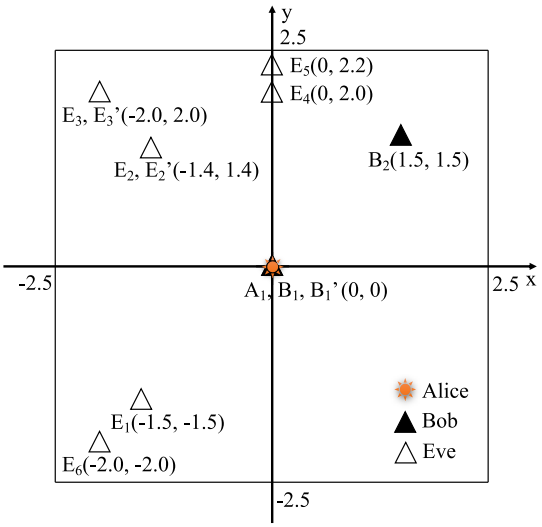



Fig. 8. Planimetric locations of Alice, Bob, and Eve for different experimental scenarios. $A_x$ refers to Alice, $B_x$ refers to Bob, and $E_x, E_x'$ refers to Eve at different height.

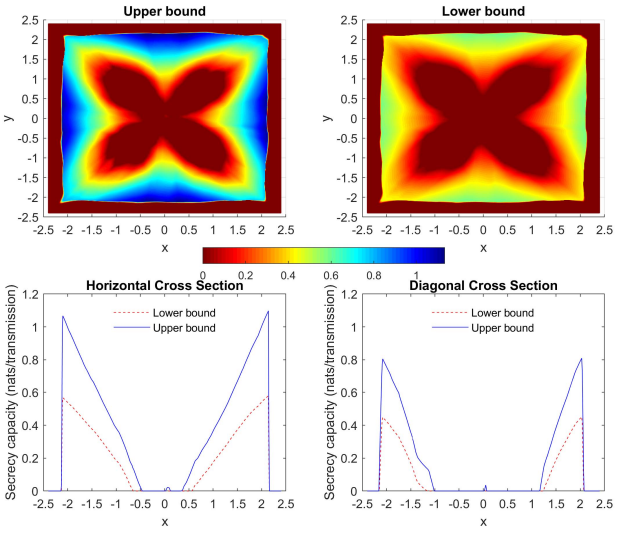



Fig. 10. Spatial characteristics of secrecy capacity bounds when Alice locates at $A_1$, Bob locates at $B_1$, and Eve locates at any place.

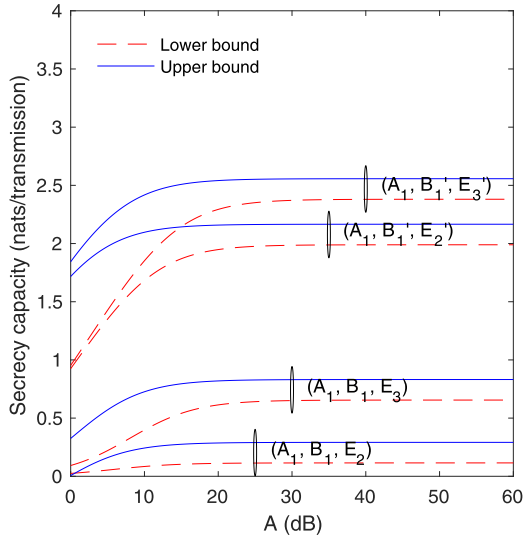



Fig. 9. Secrecy capacity bounds versus the optimal peak intensity A when Alice locates at $A_1$, Bob locates at $B_1$ and $B_1'$, Eve locates at $E_2$, $E_3$, $E_2'$, and $E_3'$.

We start from the spatial characteristics of the secrecy capacity, and then discuss the other factors that impact secrecy capacity at a specific location.

### A. Spatial Characteristics of Secrecy Capacity

Since the channel impulse response could be synthesized at any possible location in the indoor VLC system, the spatial character of secrecy capacity can be calculated accordingly. Figure 10 shows the spatial characteristics of secrecy capacity bounds calculated for Eve locating at each grid point with an spatial interval of 0.01 m, when Alice locates at $A_1$ and Bob locates at $B_1$. The upper two panels depict the spatial pattern of the upper bound and lower bound, both of which present similar spatial characteristics. Those red regions show the vulnerable area of the VLC system, where the secrecy capacity approaches zero. They are mostly either following the diagonal line of the experimental plane or nearby the walls. The strong reflections from two adjacent walls might account for this quincunx pattern of the vulnerable zone. When receiver is approaching the walls, the intensity of NLOS part increases significantly, and it could become as strong as, or even stronger than, the intensity of LOS part. It would partially explain those vulnerable areas nearby the walls. The bottom two panels show the horizontal and diagonal cross section of the spatial secrecy capacity bounds. The relative quantity of secrecy capacity bounds is increasing from center to edge as Eve is getting far away from Bob. It's worthwhile to point out that there is a secrecy capacity cutoff on both sides, and it turns out to be result of the fixed modulation bandwidth as approaching the walls, which will be discussed in the next subsection. We can conclude that areas with secrecy capacity approaching zero fall into three cases: 1. when Eve is located nearby Bob; 2. when Eve is located around the diagonal line; 3. when Eve is located nearby the walls.

If Bob is moved from $B_1$ to $B_2$, the corresponding spatial characteristics are shown in Figure 11. A similar vulnerability pattern can be observed from the upper two panels, but there is more vulnerable area inside the indoor VLC system. Since moving Bob from $B_1$ to $B_2$ will degrade the main communication channel, there is an increase of vulnerable area towards outside. Compared with Figure 10, we also notice a decrease of the relative quantity of secrecy capacity bounds, which is consistent with the degradation of the main communication channel. In real world application, it's also consistent with our real life experience as we always want the intended receiver placed at location with the best communication channel. When we have the main communication channel set up, the spatial characteristics would be used to identify the possible vulnerable area where eavesdropping likely takes place, which could be exploited to counter data sniffing. Based

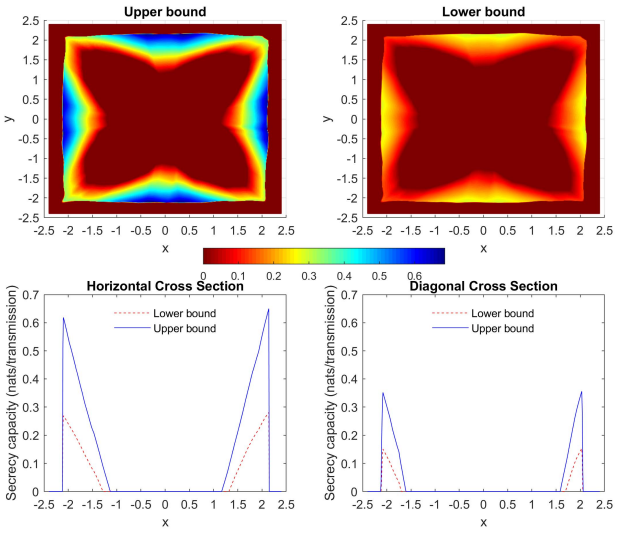



Fig. 11. Spatial characteristics of secrecy capacity bounds when Alice locates at $A_1$, Bob locates at $B_2$, and Eve locates at any place.

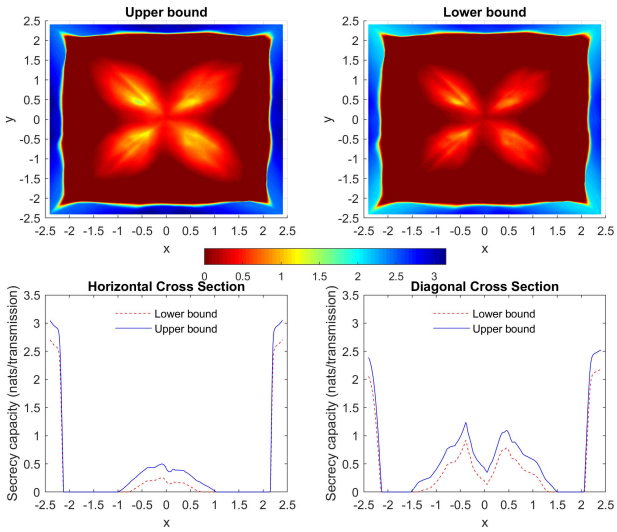



Fig. 12. Spatial characteristics of secrecy capacity bounds when Alice locates at $A_1$, Eve locates at $E_1$, and Bob locates at any place.

on the limited vulnerable area, additional detection mechanism could be instrumented to tell when an eavesdropping attack is under way.

On the contrary, if we fix Alice and Eve at $A_1$ and $E_1$ respectively, we can get the spatial characteristics of secrecy capacity bounds when moving Bob around, which is shown in Figure 12. The upper two panels show the spatial pattern of the upper bound and lower bound, both of which present similar spatial characteristics, which could be used to identify the best location for Bob. Those yellow regions show the possible locations for Bob, where the VLC system secrecy capacity achieves a high value in excess of zero. The bottom two panels show the horizontal and diagonal cross section of the spatial secrecy capacity bounds. Similar with the secrecy capacity cutoff in previous scenario, there is also a secrecy capacity uplifting nearby the walls due to the strong reflections

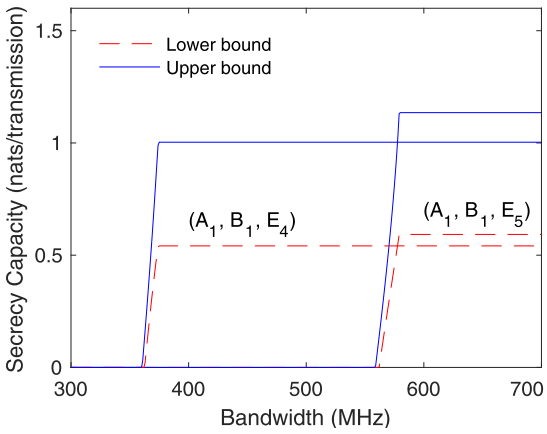



Fig. 13. Secrecy capacity bounds changes with modulation bandwidth when Alice locates at $A_1$, Bob locates at $B_1$, and Eve locates at $E_4$ and $E_5$.

and fixed modulation bandwidth. In such a scenario, when the location of eavesdropper is known, we need to figure out the location for the intended receiver to achieve the secrecy capacity as high as possible. In reality, although an eavesdropper will always hide from the main communication channel in an unconscious place, in a typical indoor VLC system we can still assume the possible locations of eavesdropper (e.g., close to the door, around the corner), then the spatial characteristics could be used to identify the best location for the intended receiver.

### *B. Secrecy Capacity Vs. Modulation Bandwidth*

When considering the impact of multiple reflections on secrecy capacity, inter-symbol time interval (i.e., reception time duration of a symbol) is another significant factor for calculating ISI on secrecy capacity. It is determined by the reciprocal of symbol rate, as stated in section V. For simplicity, the binary intensity modulation is assumed during calculation, so the symbol rate is equivalent to modulation bandwidth if neglecting roll off factor. As long as the modulation bandwidth is determined, the inter-symbol time interval for each receiver at different location will be fixed as the same. However, the time delay from LOS to NLOS for channel impulse response of each receiver at different location will be different because of the different reflection path. So, given a location of receiver, if we change the modulation bandwidth, the impact on secrecy capacity will be identified once the inter-symbol time interval becomes comparable to the time delay from LOS to NLOS for channel impulse response. Figure 13 shows the change of secrecy capacity bounds with the bandwidth when Alice locates at $A_1$, Bob locates at $B_1$, and Eve locates at $E_4$ and $E_5$, respectively.

As we move Eve from $E_4$ to $E_5$, the wiretap channel is degraded, so there is an increase of secrecy capacity as expected. From both scenarios, we see a step function shaped change of secrecy capacity when increasing the modulation bandwidth. This is because for a given location of Eve, the time delay from LOS to NLOS for channel impulse response is determined, there is an increase of secrecy capacity as increase of bandwidth when the inter-symbol time interval

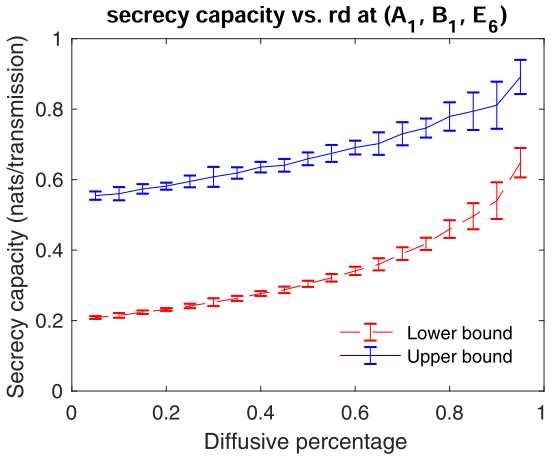



Fig. 14. Secrecy capacity bounds change with the percentage of diffusive reflection when Alice locates at $A_1$, Bob locates at $B_1$, and Eve locates at $E_6$. Error bar represent 95% confidence interval.

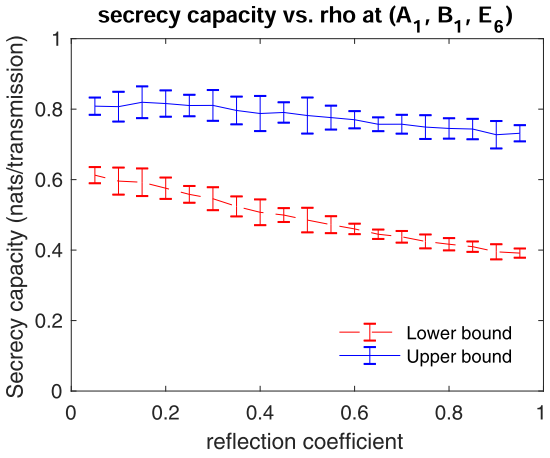



Fig. 15. Secrecy capacity bounds change with the reflection coefficient when Alice locates at $A_1$, Bob locates at $B_1$, and Eve locates at $E_6$. Error bar represent 95% confidence interval.

is approaching the time delay. Once the inter-symbol time interval gets less than the time delay, the secrecy capacity will get saturated. It acts like a cutoff frequency of secrecy capacity due to the impact of reflections. This cutoff frequency varies for each location of Eve, and it increases as Eve getting far away from the center. It could partially explain the drastic drop or rise of secrecy capacity nearby the walls as we discussed in previous subsection (Figure 10, 11, and 12), because we used 500 MHz fixed modulation bandwidth for those scenarios. So, when we deploy a VLC system, we will have to consider not only the quality of the communication channel, but also the modulation bandwidth, as a higher modulation bandwidth would eliminate the feasibility of eavesdropping nearby the reflector, even though it could be far away from the main communication channel.

### C. Secrecy Capacity Vs. Diffusive Percentage

As discussed before, each reflection is supposed to be comprised of specular and diffusive reflections depending on the roughness of the wall. Intuitively, the more rough the wall is, the more diffusive part the reflection will contain. As the increase of the diffusive percentage, we would expect to see the corresponding increase of secrecy capacity, which is verified in Figure 14 when Alice locates at $A_1$, Bob locates at $B_1$, and Eve locates at $E_6$. Since the numerically calculated channel impulse response using statistic approach for a given location varies from time to time, We calculate secrecy capacity bounds ten times for each diffusive percentage, and get the 95% confidence interval. There is a distinct increasing trend with larger uncertainty as the increase of diffusive percentage. Obviously, it would be difficult for eavesdropper to sniff effective data when most of the emitted energy are diffusely reflected. As a testbed exemplification in [1], different flooring materials (e.g., acrylic glass, vinyl plank, glazed tile, carpet, and laminate flooring) result in variable decoding bit error rate for eavesdropper, which imposes potential eavesdropping vulnerability. Thus, for indoor VLC system implementation, the construction material and design should be taken into consideration in case of security vulnerability.

### D. Secrecy Capacity Vs. Reflection Coefficient

On the other hand, when considering the property of the wall, the reflection coefficient is another significant factor that could impact the intensity of reflection. As for each reflection, the total emitted energy would be reduced by the reflection coefficient. Figure 15 shows the change of secrecy capacity with the reflection coefficient when Alice locates at $A_1$, Bob locates at $B_1$, and Eve locates at $E_6$. We can see a decreasing trend of the secrecy capacity with the increase of reflection coefficient, which is consistent with our intuition that high reflection coefficient would generate strong reflection and result in secrecy vulnerability. Considering the feasibility of vulnerability due to the high reflection coefficient, it would suggest to choose materials with low reflection coefficient to reduce the impact of reflections on secrecy capacity when designing an indoor VLC system. But in the real world application, according to [39], since the VLC uses a wide spectrum in 380 $\sim$ 750 nm, spectral reflectance of indoor reflector (e.g., ceiling, floor, plaster wall, plastic wall) varies a lot, which will make the design of indoor VLC system more complicated by inducing spectrum information.

## VIII. Conclusion and Future Work

In this paper, the impact of multiple reflections on secrecy capacity of indoor VLC system is investigated. Base on the established indoor VLC system model with three entities, the system security performance is evaluated against a comprehensive set of factors, including the locations of the transmitter, receiver, and eavesdropper, the VLC channel bandwidth, the ratio between the specular and diffusive reflections, and the reflection coefficient, according to the calculated lower and upper secrecy capacity bounds. Both the specular reflection and diffusive reflection are considered in the system model, as the increase of the specular reflection

part, the VLC system becomes more vulnerable. The spatial characteristics of secrecy capacity are also discussed, which could be used to identify possible vulnerable areas. Due to the addition of LOS and NLOS components, we have found areas with strong reflections, which makes feasible that if an eavesdropper located on those areas, he could sniff data at least partially due to reflection. The possible sniffing attack could also be used as an exploit on insidious attacks such as blocking and spoofing in future complex systems. Our work is also subject to some limitations. In particular, while the upper and lower bounds derived in this paper are reasonably tight in the high secrecy capacity regime, they are relatively loose in the low secrecy capacity regime. We will study how to improve these bounds in the low secrecy capacity regime in our future work.

## ACKNOWLEDGMENT

Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of NSF.

## REFERENCES

[1] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The spy next door: Eavesdropping on high throughput visible light communications," in *Proc. 2nd Int. Workshop Visible Light Commun. Syst. (VLCS)*, New York, NY, USA, 2015, pp. 9–14. [Online]. Available: http://doi.acm.org/10.1145/2801073.2801075

[2] I. Marin-Garcia, A. M. Ramirez-Aguilera, V. Guerra, J. Rabadan, and R. Perez-Jimenez, "Data sniffing over an open VLC channel," in *Proc. 10th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Jul. 2016, pp. 1–6.

[3] S. Wu, H. Wang, and C.-H. Youn, "Visible light communications for 5G wireless networking systems: From fixed to mobile communications," *IEEE Netw.*, vol. 28, no. 6, pp. 41–45, Nov. 2014.

[4] G. J. Blinowski, "The feasibility of launching rogue transmitter attacks in indoor visible light communication networks," *Wireless Pers. Commun.*, vol. 97, no. 4, pp. 5325–5343, Dec. 2017. [Online]. Available: https://link.springer.com/article/10.1007/s11277-017-4781-3

[5] Y. Xu, J.-M. Frahm, and F. Monrose, "Watching the watchers: Automatically inferring TV content from outdoor light effusions," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, New York, NY, USA, 2014, pp. 418–428. [Online]. Available: http://doi.acm.org/10.1145/2660267.2660358

[6] J. Classen, D. Steinmetzer, and M. Hollick, "Opportunities and pitfalls in securing visible light communication on the physical layer," in *Proc. 3rd Workshop Visible Light Commun. Syst. (VLCS)*, New York, NY, USA, 2016, pp. 19–24. [Online]. Available: http://doi.acm.org/10.1145/2981548.2981551

[7] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Physical-layer security against known/chosen plaintext attacks for OFDM-based VLC system," *IEEE Commun. Lett.*, vol. 21, no. 12, pp. 2606–2609, Dec. 2017.

[8] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Randomness evaluation of key generation based on optical OFDM system in visible light communication networks," *Electron. Lett.*, vol. 53, no. 24, pp. 1594–1596, Nov. 2017.

[9] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Chaos-based physical-layer encryption for OFDM-based VLC schemes with robustness against known/chosen plaintext attacks," *IET Optoelectron.*, vol. 13, no. 3, pp. 124–133, Jun. 2019.

[10] R. Melki, H. N. Noura, and A. Chehab, "Efficient & secure physical layer cipher scheme for VLC systems," in *Proc. IEEE 90th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2019, pp. 1–6.

[11] J. Chen and T. Shu, "Impact of multiple reflections on secrecy capacity of indoor VLC system," in *Information and Communications Security*, J. Zhou, X. Luo, Q. Shen, and Z. Xu, Eds. Cham, Switzerland: Springer, 2020, pp. 105–123.

[12] J. R. Barry, J. M. Kahn, W. J. Krause, E. A. Lee, and D. G. Messerschmitt, "Simulation of multipath impulse response for indoor wireless optical channels," *IEEE J. Sel. Areas Commun.*, vol. 11, no. 3, pp. 367–379, Apr. 1993.

[13] J. B. Carruthers and S. M. Carroll, "Statistical impulse response models for indoor optical wireless channels," *Int. J. Commun. Syst.*, vol. 18, no. 3, pp. 267–284, Apr. 2005. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/dac.703/abstract

[14] M. I. S. Chowdhury, W. Zhang, and M. Kavehrad, "Combined deterministic and modified Monte Carlo method for calculating impulse responses of indoor optical wireless channels," *J. Lightw. Technol.*, vol. 32, no. 18, pp. 3132–3148, Sep. 15, 2014.

[15] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, *Optical Wireless Communications: System and Channel Modelling With MATLAB*. Boca Raton, FL, USA: CRC Press, Aug. 2012.

[16] D. Zhang and S. Hranilovic, "Bandlimited optical intensity modulation under average and peak power constraints," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3820–3830, Sep. 2016.

[17] X. Chen and M. Jiang, "Adaptive statistical Bayesian MMSE channel estimation for visible light communication," *IEEE Trans. Signal Process.*, vol. 65, no. 5, pp. 1287–1299, Mar. 2017.

[18] S. R. Pérez, R. P. Jiménez, F. J. L. Hernández, O. B. G. Hernández, and A. J. A. Alfonso, "Reflection model for calculation of the impulse response on IR-wireless indoor channels using ray-tracing algorithm," *Microw. Opt. Technol. Lett.*, vol. 32, no. 4, pp. 296–300, Feb. 2002. [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1002/mop.10159/abstract

[19] D. Wu, Z. Ghassemlooy, H. Le-Minh, S. Rajbhandari, and L. Chao, "Channel characteristics analysis of diffuse indoor cellular optical wireless communication systems," in *Proc. Asia Commun. Photon. Conf. Exhib. (ACP)*, Nov. 2011, pp. 1–6.

[20] 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.

[21] 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.

[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] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Robust key generation from optical OFDM signal in indoor VLC networks," *IEEE Photon. Technol. Lett.*, vol. 28, no. 22, pp. 2629–2632, Nov. 15, 2016.

[24] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Secret key generation protocol for optical OFDM systems in indoor VLC networks," *IEEE Photon. J.*, vol. 9, no. 2, pp. 1–15, Apr. 2017.

[25] A. Mukherjee, "Secret-key agreement for security in multi-emitter visible light communication systems," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1361–1364, Jul. 2016.

[26] X. Liu, X. Wei, L. Guo, Y. Liu, and Y. Zhou, "A new eavesdropping-resilient framework for indoor visible light communication," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

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

[28] H. Zaid, Z. Rezki, A. Chaaban, and M. S. Alouini, "Improved achievable secrecy rate of visible light communication with cooperative jamming," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Dec. 2015, pp. 1165–1169.

[29] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/j.1538-7305.1975.tb02040.x

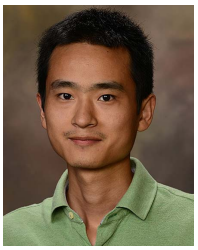
[30] O. Ozel, E. Ekrem, and S. Ulukus, "Gaussian wiretap channel with amplitude and variance constraints," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5553–5563, Oct. 2015.

[31] J.-Y. Wang, S.-H. Lin, C. Liu, J.-B. Wang, B. Zhu, and Y. Jiang, "Secrecy capacity of indoor visible light communication channels," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2018, pp. 1–6.

[32] 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.

[33] J.-Y. Wang, S.-H. Lin, Y. Qiu, N. Huang, and J.-B. Wang, "Tradeoff between secrecy capacity and harvested energy for secure visible light communications with SWIPT," *IEEE Access*, vol. 7, pp. 29543–29552, 2019.

[34] 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.
[35] M. A. Arfaoui, A. Ghrayeb, and C. Assi, "On the achievable secrecy rate of the MIMO VLC Gaussian wiretap channel," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5.
[36] M. A. Arfaoui, A. Ghrayeb, and C. Assi, "Secrecy rate closed-form expressions for the SISO VLC wiretap channel with discrete input signaling," *IEEE Commun. Lett.*, vol. 22, no. 7, pp. 1382–1385, Jul. 2018.
[37] S. Cho, G. Chen, and J. P. Coon, "Secrecy analysis in visible light communication systems with randomly located eavesdroppers," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2017, pp. 475–480.
[38] S. Cho, G. Chen, H. Chun, J. P. Coon, and D. O'Brien, "Impact of multipath reflections on secrecy in VLC systems with randomly located eavesdroppers," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.
[39] K. Lee, H. Park, and J. R. Barry, "Indoor channel characteristics for visible light communications," *IEEE Commun. Lett.*, vol. 15, no. 2, pp. 217–219, Feb. 2011.
[40] R. Pérez-Jiménez, J. Berges, and M. J. Betancor, "Statistical model for the impulse response on infrared indoor diffuse channels," *Electron. Lett.*, vol. 33, no. 15, pp. 1298–1300, Jul. 1997.
[41] 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.
[42] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2012.
[43] F. Lopez-Hernandez, R. Perez-Jimenez, and A. Santamaria, "Ray-tracing algorithms for fast calculation of the channel impulse response on diffuse IR wireless indoor channels," *Opt. Eng.*, vol. 39, no. 10, pp. 2775–2780, 2000.
[44] F. Chollet *et al.* (2015). *Keras*. [Online]. Available: https://keras.io



**Jian Chen** received the B.S. degree in geophysics from the China University of Mining and Technology, Xuzhou, in 2010, the M.S. degree in geophysics from the University of Chinese Academy of Sciences, Beijing, in 2013, and the M.S. degree in geology from Auburn University, Alabama, in 2017, where he is currently pursuing the Ph.D. degree in computer science. His research interests focus on addressing the security, privacy, and performance issues in visible light networking systems.

**Tao Shu** received the B.S. and M.S. degrees in electronic engineering from the South China University of Technology, Guangzhou, China, in 1996 and 1999, respectively, the Ph.D. degree in communication and information systems from Tsinghua University, Beijing, China, in 2003, and the Ph.D. degree in electrical and computer engineering from The University of Arizona in December 2010. He has worked as an Assistant Professor for five years at the Computer Science and Engineering Department, Oakland University, Rochester, Michigan. Prior to Oakland, he was a Senior Engineer with Qualcomm Atheros Inc. from December 2010 to August 2011. He is currently an Assistant Professor with the Department of Computer Science and Software Engineering, Auburn University. His research aims at addressing security and performance issues in wireless networking systems, with strong emphasis on system architecture, protocol design, and performance modeling and optimization.