Physical Layer Security for Visible Light Communication Systems

Citation for published version:
Arfaoui, MA, Soltani, MD, Tavakkolnia, I, Ghrayeb, A, Safari, M, Assi, CM & Haas, H 2020, 'Physical Layer Security for Visible Light Communication Systems: A Survey', *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, 9070153, pp. 1887-1908. https://doi.org/10.1109/COMST.2020.2988615

Digital Object Identifier (DOI):
10.1109/COMST.2020.2988615

Document Version:
Peer reviewed version

Published In:
IEEE Communications Surveys and Tutorials

Physical Layer Security for Visible Light Communication Systems: A Survey

Mohamed Amine Arfaoui*, Mohammad Dehghani Soltani, Iman Tavakkolnia, Ali Ghrayeb,
Majid Safari, Chadi Assi, and Harald Haas

***Abstract*—Due to the dramatic increase in high data rate services and in order to meet the demands of the fifth-generation (5G) networks, researchers from both academia and industry are exploring advanced transmission techniques, new network architectures and new frequency spectrum such as the visible light and the millimeter wave (mmWave) spectra. Visible light communication (VLC) particularly is an emerging technology that has been introduced as a promising solution for 5G and beyond, owing to the large unexploited spectrum, which translates to significantly high data rates. Although VLC systems are more immune against interference and less susceptible to security vulnerabilities since light does not penetrate through walls, security issues arise naturally in VLC channels due to their open and broadcasting nature, compared to fiber-optic systems. In addition, since VLC is considered to be an enabling technology for 5G, and security is one of the 5G fundamental requirements, security issues should be carefully addressed and resolved in the VLC context. On the other hand, due to the success of physical layer security (PLS) in improving the security of radio-frequency (RF) wireless networks, extending such PLS techniques to VLC systems has been of great interest. Only two survey papers on security in VLC have been published in the literature. However, a comparative and unified survey on PLS for VLC from information theoretic and signal processing point of views is still missing. This paper covers almost all aspects of PLS for VLC, including different channel models, input distributions, network configurations, precoding/signaling strategies, and secrecy capacity and information rates. Furthermore, we propose a number of timely and open research directions for PLS-VLC systems, including the application of measurement-based indoor and outdoor channel models, incorporating user mobility and device orientation into the channel model, and combining VLC and RF systems to realize the potential of such technologies.**

***Index Terms*—5G and beyond, Internet-of-Things, visible light communication, Light-Fidelity, physical layer security, multiple-input multiple-output, eavesdropping, secrecy rates.**

I. INTRODUCTION

A. The Need for VLC Technology

The total data traffic is expected to become about 49 exabytes per month by 2021, while in 2016, it was approximately 7.24 exabytes per month [1]. With this drastic increase, 5G networks must urgently provide high data rates, seamless connectivity, robust security and ultra-low latency communications [2]–[4]. In addition, with the emergence of the Internet-of-Things (IoTs) networks, the number of connected devices to the internet is increasing dramatically [5], [6]. This fact implies not only a significant increase in data traffic, but also the emergence of some IoT services with crucial requirements. Such requirements include higher data rates, higher connection density, ultra reliable low latency communication (URLLC) and improved security. Hence, traditional radio-frequency (RF) networks, which are already crowded, are unable to satisfy these high demands [7]. Network densification [8], [9] has been proposed as a solution to increase the capacity and coverage of 5G networks. However, with the continuous dramatic growth in data traffic, researchers from both industry and academia are trying to explore new network architectures, new transmission techniques and new spectra to meet these demands. One of the new communication technologies that has been proposed as an auspicious solution for 5G and beyond is visible light communication (VLC) [10], which operates in the visible light frequency spectrum and uses light for both illumination and data communication purposes simultaneously.

VLC has gained significant interest due to its high data rates [10]. The motivation behind the interest in VLC is twofold: 1) The advantages that VLC offers when compared to RF, including the large available frequency spectrum [11], high speed and robustness against interference [12], and 2) the availability of low cost light emitting diodes (LEDs) [13]. LEDs exhibit a high electrical-to-optical conversion efficiency, long life span, low cost and high operational speed [14]–[17]. While VLC technologies bring efficient solutions to many real-life problems, they are not intended to replace RF technologies. Rather, VLC can be viewed as a complementary technology to RF. There are applications where VLC is more suitable than RF, whereas there are other applications where the opposite is true. For example, recent advances in wireless communication technologies have shown that millimeter-wave (mmWave) communications, which is an RF technology, is the most efficient for air-to-ground communications [18], [19]. On the other hand, it has been shown through experiments that VLC is efficient in indoor environments, such as airport halls and aircraft cabins [20], [21]. This suggest that neither technology can be considered as a replacement for the other. In fact, in some cases, one may need to combine both technologies to reap the best performance. It all depends on the underlying environment and application. As such, both technologies should be exploited together to meet the expectations of 5G networks and beyond.

Several survey papers have been already published over the past few years in the literature on VLC-related technologies [22]–[34]. However, a comprehensive and comparative study on securing VLC systems, at least from a PLS perspective, is still missing. Specifically, the authors in [22] presented

---

M. A. Arfaoui and C. Assi are with Concordia Institute for Information Systems Engineering (CIISE), Concordia University, Montreal, Canada, e-mail:{m_arfaou@encs, assi@ciise}.concordia.ca. M. D. Soltani, I. Tavakkolnia, M. Safari, and H. Haas are with the LiFi Research and Development Centre, Institute for Digital Communications, School of Engineering, The University of Edinburgh, UK. e-mail: {m.dehghani, i.tavakkolnia, majid.safari, h.haas}@ed.ac.uk. Ali Ghrayeb is with Texas A & M University at Qatar, Doha, Qatar, e-mail: ali.ghrayeb@qatar.tamu.edu. **Corresponding author*: M. A. Arfaoui (m_arfaou@encs.concordia.ca). The statements made herein are solely the responsibility of the authors.

the differences among various categories of optical wireless communications (OWC) technologies such as free space optical (FSO) communications, VLC and light fidelity (LiFi). Over the last few years, [23]–[25] were the first papers that surveyed LED-based VLC systems and their applications. In [26], the authors brought attention to the strongest feature of LEDs, which is their ability to provide smart lighting and data transmission simultaneously. Along the same lines, the authors of [27] highlighted the benefits and challenges of VLC networks, as compared to RF networks.

Going deep into VLC technology, the authors in [28] studied the methods employed for enhancing the performance of VLC, including modulation schemes and dimming control techniques, while in [29], the authors focused on the VLC link level transmission, the medium access techniques and the visible light sensing. On the other hand, the authors in [30] focused on the channel models for VLC, whereas the authors in [31] reviewed the optical noise sources and noise mitigation mechanisms for VLC. A study on interference reduction techniques in VLC was recently presented in [32], where the authors reviewed and compared two different designs for VLC networks, namely, the user-centric network and network-centric designs. Positioning and localization techniques for indoor and outdoor VLC applications were reviewed in [33]. Recently, the authors in [34] surveyed all the optimization techniques, previously reported in the literature, that aim to improve the performance of VLC systems, with emphasis on new technologies such as non-orthogonal multiple-access (NOMA), simultaneous wireless information and power transfer (SWIPT), cooperative transmission and space division multiple access (SDMA).

B. Are VLC Systems Secure?

Some of the noted advantages of VLC systems over RF systems is the higher security that VLC systems provide. This is basically inherited from to the fact that light does not penetrate through walls. However, security issues arise naturally in VLC systems due to their open and broadcast nature [35]. Specifically, VLC systems could be as vulnerable as their RF counterparts when their nodes are deployed in public areas and/or when there are large windows in the coverage areas [36]. Thus, security for VLC systems is as important as it is for RF systems. Hence, since VLC is considered as a promising technology for 5G networks and beyond, and since robust end-to-end security is one of the critical requirements of the next generation networks, security should be deeply investigated in the VLC context.

Security in wireless communication systems, including 5G wireless networks, may be enhanced by introducing physical layer security (PLS) techniques [37], [38]. In fact, PLS techniques have been applied to a wide range of RF applications in an effort to improve the overall system security by complementing existing cryptography-based security techniques [39]. The potential of PLS stems from its ability to leverage features of the surrounding environments via sophisticated encoding techniques at the physical layer [40]. Indeed, PLS schemes can be applied in the same spirit to VLC systems.

C. PLS-RF vs PLS-VLC

PLS for RF systems, several review articles have been reported in the literature [41]–[46], which provided comprehensive overviews and insightful comments to understand the fundamental principles, technology status, and future trends of PLS. In [41], security features, security vulnerabilities, and existing security solutions for long term evolution (LTE) and LTE-advanced were reviewed. In [42], the authors reviewed the secrecy performance from a PLS perspective of broadcast and multi-antenna systems, with an emphasis on the multiple-access channel (MAC), relay channels, physical-layer key generation and secure coding. The authors in [43] reviewed different jamming techniques, employed in the literature, that aim at improving the secrecy performance of RF networks. In [44], the authors provided a comprehensive review on various multiple-antenna techniques in PLS, with an emphasis on transmit beamforming designs for multiple-antenna nodes in point-to-point systems and heterogeneous networks. In [45], the fundamentals and technologies of PLS were reviewed and the technologies, challenges, and solutions were also summarized from different methodological viewpoints that involve wiretap coding, multi-antenna and relay cooperation and physical-layer authentication. In [46], security designs from optimization and signal processing viewpoints were reviewed, where the authors summarized all the PLS techniques pertaining to resource allocation, beamforming/precoding, antenna/node selection and cooperation.

Although several PLS techniques were proposed in the literature for RF systems, as mentioned above, the adoption of techniques developed for RF channels can not be straightforwardly applied to VLC channels. This is mainly due to the fact that there exist many fundamental specificities in the transmission protocols and modulation schemes of VLC systems that make them different from RF systems. In fact, the channels and transmitted optical signals in VLC are real and positive valued. In addition, due to the limited dynamic range of the LEDs [47], VLC systems impose a peak-power constraint, i.e., amplitude constraint, on the channel input, which makes unbounded inputs not admissible. Note that RF signals are equally amplitude-bounded and the peak-to-average power ratio (PAPR) is a problem for RF power amplifiers. However, in VLC systems, high PAPR is used for intensity-modulation direct detection (IM/DD), which is the case for the direct current (DC) biased optical orthogonal frequency division multiplexing (DCO-OFDM) [48]. Due to these differences, PLS techniques developed for RF systems may not extend to VLC systems in a straightforward manner, which necessitates the development of new PLS schemes specific to VLC systems.

Recently, the authors in [34], [49] surveyed a batch of works conducted on PLS for VLC and FSO networks, and proposed several open problems to optimize and enhance the security performance of these systems. However, the coverage of PLS-VLC in these two papers is rather limited in scope and/or depth. For instance, a large number of recently published papers on this topic were not covered; some of the covered aspects, such as information theoretic security, lacked depth and breadth, owing to the relatively wide coverage scope of those papers; and several key system design challenges were not addressed. Such design issues include input signaling schemes (continuous versus discrete), transmission schemes (spatial modulation, spatial multiplexing, etc.), the geometry and parameters of VLC networks, availability of the channel state information (CSI), real-life measurement-based channel models, users mobility, devices orientation and links blockage. In this paper, however, we address all of the above-mentioned challenges where we provide an in-depth coverage of all published papers on PLS-VLC. In addition, we present a comparative study of existing techniques, and propose future research directions that incorporate several realistic system design parameters.

D. Contributions and Outline

Against the above background, this paper provides an in-depth coverage of all published papers on PLS-VLC. In addition, it presents a comparative study of existing techniques, and propose future research directions that incorporate several realistic system design parameters. Specifically, most of the research done on PLS-VLC can be classified as either information theoretic, i.e., secrecy capacity, achievable secrecy rate and capacity-equivocation region; or signal processing-based, i.e., precoding, beamforming, access points (APs) selection and optimization. Motivated by this, unlike [34], [49], the present paper aims at providing a unified overview of all PLS-VLC related studies that have been published so far and addresses several key features of VLC systems. Among the features considered in this study are:

1) The characteristics of the VLC channel.
2) The input distribution: continuous versus discrete.
3) The transceiver design: architectures of the transmitter/receiver.
4) The number of legitimate users and unauthorized receivers.
5) The availability of the channel state information (CSI).
6) The geometry of the communication environment.
7) The type of signaling scheme employed: precoding, artificial noise, spatial modulation, etc.

While combining the above features, four types of VLC systems are studied in this paper, which are single-input-single-output (SISO), multiple-input-single-output (MISO), multiple-input-multiple-output (MIMO) and hybrid RF/VLC. For each type, both cases of single active user (AU) and multiple AUs are considered and the effect of the number and CSI of the eavesdroppers (EDs) on the secrecy performance is also discussed. Furthermore, several open research problems are proposed to further advance the state-of-the-art of VLC technologies.

The rest of the paper is outlined as follows. In Section II, the generalized model of VLC wiretap systems is presented. Specifically, in this section, the paper provide a brief overview about the VLC channel model adopted in the literature and discusses the constraints that must be taken into account in designing the transmission strategies and PLS schemes for VLC. In Section III, all the PLS schemes employed for the MIMO VLC system are reviewed. In Section IV, all the works related to secure MISO VLC systems from a PLS point of view are reviewed. In Section V, all the PLS techniques employed for the SISO VLC system and relay-aided systems are reviewed. In Section VI, the secrecy performance of hybrid wireless systems that combine both RF and VLC transmissions is reviewed. In Section VII, some open research directions on securing VLC systems with their associated challenges are presented. Specifically, in this section, the paper discusses several problems that have not been investigated, and proposes various ideas on how to improve the secrecy performance of real-life and practical VLC systems. In Section VIII, a summary of the paper is provided.

E. Research Methodology

In this paper, we surveyed the literature of PLS for VLC systems following the general guidelines for conducting systematic literature review that is presented in [50]. First, we surveyed the state of the art of PLS concept from information theory and security engineering points of view. Then, we surveyed the state of the art of VLC technology. Finally, we identified the intersections between the the literature of PLS and VLC. Our main objective is to provide an in-depth analysis of the PLS techniques used for securing VLC systems while highlighting their strengths and weaknesses. We also aimed at identifying gaps in current research and suggest areas for further investigations.

We surveyed a number of papers that appeared in top telecommunication venues. We surveyed top venues and looked for papers that were related to PLS and VLC. For each venue, we performed a combination of automatic and manual database search on all papers that were published since 2010, which contained the terms “PLS” and “VLC” in either the Title, Abstract, or Keywords. In addition, we explored top online libraries including IEEE Xplore [51], Elsevier Science Direct [52], Wiley Online Library [53] and ACM Digital Library [54], for papers that contained the terms “PLS” and “VLC” anywhere in their full text. The reviewed papers were selected through a number of iterations. The initial search resulted in more than 100 papers that were manually examined to identify their relevance PLS for VLC systems. After filtering irrelevant papers, we identified PLS techniques that were adopted for securing VLC systems. Those papers were included for further analysis throughout this work. It is worth noting that some of the identified papers were based on previous works that might have not been included in the initial search results (primary studies). These secondary studies were also included in the survey whenever necessary.

F. Abbreviations and Notations

A list of abbreviations used in this paper is presented in Table I. In addition, the following notations are adopted throughout the paper. Upper case bold characters denote matrices and lower case bold characters denote column vectors. $[\![1, N]\!]$ denotes the discrete interval with bounds 1 and N, $\mathbb{N}$ denotes the set of natural numbers, $\mathbb{R}^N$ denotes the set of N-dimensional real-valued vectors and $\mathbb{R}_+^N$ denotes the set of N-dimensional real-valued vectors with positive elements. $\{\cdot\}^T$

TABLE I: Table of Abbreviations

5G	Fifth generation
AN	Artificial noise
AP	Access point
AU	Active user
CDF	Cumulative distribution function
CSI	Channel state information
DD	Direct detection
ED	eavesdropper
IB	Information bearing
IM	Intensity modulation
IoTs	Internet-of-Things
LED	Light emitting diode
LiFi	Light-fidelity
LoS	Line of sight
MIMO	Multiple-input-multiple-output
MISO	Multiple-input-single-output
NOMA	Non orthogonal multiple access
PD	photo diode
PDF	Probability density function
PLS	Physical layer security
PMF	Probability mass function
PPP	Poisson point process
RF	Radio-frequency
SISO	Single-input-single-output
SINR	Signal to interference plus noise ratio
SNR	Signal to noise ratio
SOP	Secrecy outage probability
VLC	Visible light communication

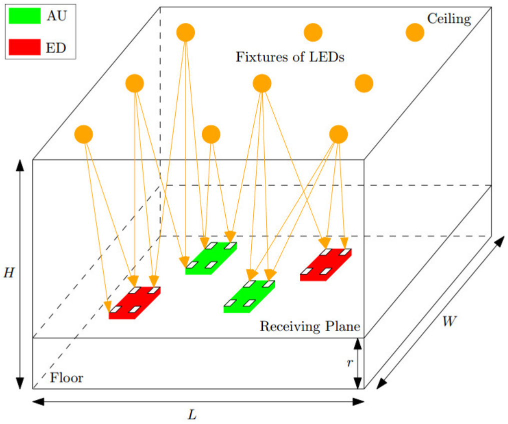


Fig. 1: A MIMO VLC system consisting of a transmitter with $M = 9$ APs, multiple AUs and multiple EDs.

denotes transpose operator, $\{\cdot\}^{-1}$ denotes matrix inversion and $|\cdot|$ denotes the absolute value of the determinant. For $N \in \mathbb{N}$ such that $N \neq 0$, $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. $||\cdot||_\infty$ and $||\cdot||_2$ denote the infinity norm and the Euclidean norm, respectively. $F_{\mathbf{s}}$ and $f_{\mathbf{s}}$ denote the joint cumulative distribution function and the joint probability mass/density function of $\mathbf{s}$, respectively. $\mathbb{E}(\cdot)$ denotes the expected value, $I(\cdot;\cdot)$ denotes the mutual information and $C^+ = \max(C, 0)$. We use $\log[\cdot]$, without a base, to denote natural logarithms and information rates are specified in (nats/s/Hz).

II. GENERALIZED MODEL OF INDOOR VLC WIRETAP SYSTEMS

A. System Model

Consider the IM/DD VLC wiretap system shown in Fig. 1, which consists of a room of size $L \times W \times H$, where L, W and H denote the length, width and height of the room, respectively. The room is equipped with M APs that are located at its ceiling, where each AP is equipped with a fixture of LEDs. These APs act as a single transmitter, i.e., they can cooperate together through a centralized controller in order to illuminate the room and to communicate data simultaneously. The transmitter sends simultaneously N sets of confidential messages to N spatially dispersed AUs in the presence of K EDs. For all $i \in [\![1, N]\!]$, the ith AU is equipped with $N_i \in \mathbb{N}$ PDs, whereas for all $k \in [\![1, K]\!]$, the kth ED is equipped with $K_j \in \mathbb{N}$ PDs. At each channel use, and for $i \in [\![1, N]\!]$, the set of confidential messages intended for the ith AU are precoded into an $M \times 1$ precoded signal that is denoted by $\mathbf{s}_i$. After this, the N precoded vectors are encoded into an $M \times 1$ vector $\mathbf{s}$ through superposition coding (SC) and then transmitted through the M APs. Based on this, the transmitted signal $\mathbf{s}$ is expressed as

$$\mathbf{s} = \sum_{i=1}^{N} \mathbf{s}_i, \tag{1}$$

Based on the above, for $i \in [\![1, N]\!]$ and $k \in [\![1, K]\!]$, the received signals at the ith AU and the kth ED are expressed, respectively, as

$$\begin{aligned} \mathbf{y}_i &= \mathbf{H}_i \mathbf{s} + \mathbf{n}_{AU,i} \\ \mathbf{z}_k &= \mathbf{G}_k \mathbf{s} + \mathbf{n}_{ED,k}, \end{aligned} \tag{2}$$

where $\mathbf{H}_i$ and $\mathbf{G}_k$ are the $N_i \times M$ and $K_k \times M$ channel matrices of the ith AU and the kth ED, respectively, and $\mathbf{n}_{AU,i}$ and $\mathbf{n}_{ED,k}$ are multivariate additive white Gaussian noise (AWGN) that are $\mathcal{N}\left(0, \sigma_A^2 \mathbf{I}_{N_i}\right)$ and $\mathcal{N}\left(0, \sigma_E^2 \mathbf{I}_{K_k}\right)$ distributed, respectively. It is important to highlight that, since the legitimate receivers are usually active, the CSI of each AU is available at the transmitter through a limited-feedback mechanism [55]–[57]. However, this is not the case for the EDs. In fact, the CSI of the EDs is not available at the transmitter in general, especially if the EDs are passive or not registered in the network.

The system model presented above refers to the generalized MIMO VLC wiretap system. It is typically the same concept as the multi-input, multi-output, multi-eavesdropper (MIMOME) channel model introduced in [58], which is a well-known concept in PLS for RF systems. In addition, this system model includes a variaty of VLC wiretap systems for arbitrary numbers of APs M, AUs N, EDs K, and PDs at each receiver. When all receivers are equipped with a single PD, the system is reduced to the MISO VLC wiretap system, which has been adopted in a large body of works [59]–[80]. Additionally, when the transmitter is equipped with one AP, i.e., $M = 1$, the system corresponds to the SISO VLC wiretap system, which

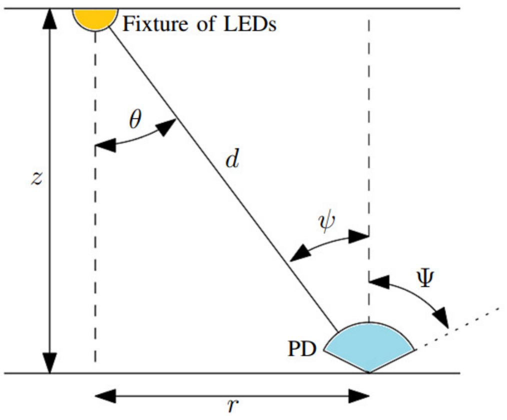


Fig. 2: VLC path gain description.

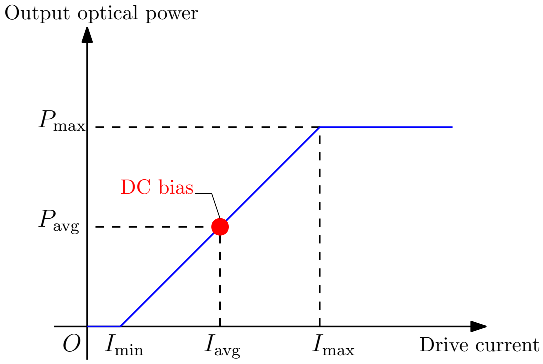
has also been considered in many papers [81]–[89]. The choice of a suitable PLS technique and its corresponding secrecy performance for any VLC wiretap system highly depend on the parameters M, N and K, as well as the number of PDs and the availability of the CSI at each receiver.

B. Channel Model and Operating Constraints

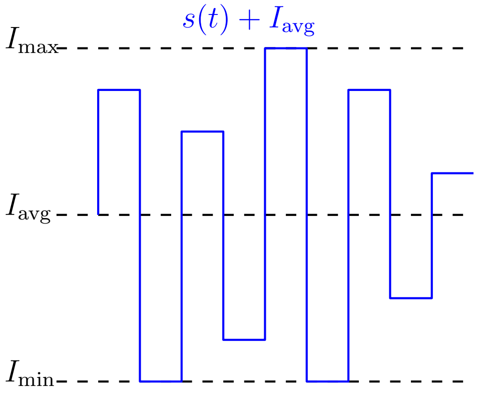
It is important to mention that almost all work on secure VLC systems have only considered the LoS component h_{LoS} presented in (2) in their adopted VLC channel models and ignored the NLoS component h_{NLoS}. This is mainly due to two reasons: 1) no closed-form expression for the NLoS component h_{NLoS} is readily available in the literature, and 2) the optical power received from signals reflected more than once is negligible compared to the LoS component, especially if the receiver is far away from the walls or is located close to the cell center [90]. Thus, unless otherwise stated, only the LoS component is considered in the analysis presented in this paper. In this case, assuming that the considered LEDs have a Lambertian emission pattern, the LoS component h_{LoS} of the channel gain between one fixture of LEDs and one PD is expressed as [91], [92]

$$h_{\text{LoS}} = \eta R_p T \frac{(m+1)}{2\pi} \frac{n_c^2 A_g}{\sin(\Psi)^2} \cos^m(\theta) \frac{\cos(\psi)}{d^2} \text{rect}\left(\frac{\psi}{\Psi}\right), \tag{3}$$

where η denotes the electro-optical conversion factor of the LEDs, R_p denotes the PD responsivity, T denotes the gain of the transimpedance amplifier at the receiver, $m = \frac{-\log(2)}{\log(\cos(\theta_{1/2}))}$ is the order of the Lambertian emission, such that $\theta_{1/2}$ represents the half-power semi-angle of the LED, A_g is the geometric area of the PD, n_c is the refractive index of the receiver's optical concentrator, and as shown in Fig 2, Ψ is the field of view (FoV) of the receiver's PD, $d = \sqrt{r^2 + z^2}$ is the Euclidean distance between the LED and the PD, such that r and z are the horizontal and vertical distances between the LED and the PD, $\theta \in [0, \theta_{1/2}]$ is the radiation angle and $\psi \in [0, \pi]$ is the incidence angle.



(a) Electrical to optical range of a typical LED.



(b) Operating range of the transmitted electrical signal $s + I_{\text{avg}}$.

Fig. 3: Limited linear dynamic range of a typical LED.

Typical LEDs suffer from nonlinear distortion and clipping effects, which imposes additional operating constraints on the emitted optical power. Precisely, the electrical to optical transfer characteristic of LEDs leads to unique optical power constraints imposed on the transmitted signals [93], [94]. In fact, typical LEDs exhibit a limited and non-linear current-power transfer function that can be approximated with a polynomial function with order two [95]. As seen in Fig. 3a, this non-linear input-output characteristic can be linearized with the aid of predistortion over the limited dynamic range of $[I_{\min}, I_{\max}]$, which linearly corresponds to the optical power range $[0, P_{\max}]$ of the LED, where $I_{\min}$ denotes the turn-on current, $I_{\max}$ denotes the maximum tolerable alternating current (AC) and $P_{\max} = \eta I_{\max}$ is the optical power of associated to $I_{\max}$ [96]. Therefore, based on the direct linear relationship between the radiated optical power and drive current, the signal to be electrical signal to be transmitted is $s + I_{\text{avg}}$, where s is a zero-mean information-bearing signal and $I_{\text{avg}} = \frac{1}{2}(I_{\min} + I_{\max})$ is the direct current (DC) bias. Consequently, as seen in Fig. 3b, the constraint imposed on the transmitted signal $s + I_{\text{avg}}$ in the electrical domain may be expressed as $I_{\min} \leq s + I_{\text{avg}} \leq I_{\max}$, i.e., $|s| \leq \frac{1}{2}(I_{\max} - I_{\min})$. The constraint ensures the non-negativity of the signals as well as the normal operation of the LEDs. For the case of multiple fixtures of LEDs, and based on the above, the transmitted signal $\mathbf{s}$ in (1) should satisfy a peak-power constraint, i.e., an amplitude constraint, that is expressed as

$$||\mathbf{s}||_\infty \leq A, \tag{4}$$

where $A = \frac{1}{2}(I_{\max} - I_{\min})$ is the maximum allowed signal amplitude at the input of each fixture of LEDs. The peak-power constraint implies that the information bearing (IB) signal $\mathbf{s}$ is bounded. Consequently, from an information-theoretic perspective, the capacity achieving input distribution can not be Gaussian, since Gaussian inputs are not admissible for such constraints [97]. However, it is shown in [98] that the channel can be modelled in the *electrical* domain as an AWGN channel with an average power constraint, and this falls within the Shannon framework which determines the upper bound on the achievable data rate. This is in fact a matter of electrical systems versus optical system modeling. In other words, the commonly derived Shannon channel capacity formulas obtained under average electrical power constraints cannot be applied in a straightforward manner to VLC systems due to the presence of the peak-power constraint.

In the following sections, we review all the works related to secure VLC systems as well as all the associated PLS techniques reported in the literature. For ease of presentation, we group those techniques according to what system model they have been developed for, e.g., MIMO, MISO and SISO.

III. THE MIMO VLC WIRETAP SYSTEM

A. Single ED

For the special case when $N = 1$ AU and $K = 1$ ED, the secrecy capacity of the MIMO VLC wiretap channel in (2) is given by [99], [100]

$$\begin{aligned} C_s = \max_{F_{\mathbf{s}}} \ & \left[\mathrm{I}\left(\mathbf{s};\mathbf{y}_1\right) - \mathrm{I}\left(\mathbf{s};\mathbf{z}_1\right)\right]^+ \\ \text{s.t} \ & \int_{\mathcal{S}} \mathrm{d}F_{\mathbf{s}}(\mathbf{x}) = 1, \end{aligned} \tag{5}$$

where $\mathcal{S} = [-A, A]^M$. In general, neither the secrecy capacity C_s nor the optimal probability distribution that achieves C_s, i.e., the one that solve the optimization problem in (5), have been determined in closed-form expression or at least characterized in the literature, except some special cases that will be discussed later in the paper. Due to this, based on the system configuration and the type of the input signaling scheme, several upper and lower bounds were derived in the literature in order to characterize the secrecy performance of the MIMO VLC wiretap channel. In this context, it should be noted that conceptually there are two approaches for transmission design of MIMO wiretap channels. One is to perform precoding under fixed input probability distribution and system constraints. The other is to optimize the input distributions that can achieve secrecy rates as close as possible to the secrecy capacity [101].

Although security for VLC systems was extensively studied in the literature, only a few papers investigated the secrecy performance of MIMO VLC systems [102]–[105]. For the case of $N = 1$ AU and $K = 1$ ED, the authors in [102] derived an achievable secrecy rate for the system using continuous log-concave distributions. Afterwards, an iterative algorithm based on the convex-concave procedure (CCP) was proposed to jointly obtain the best covariance matrix and signaling scheme. From the information-theoretic point of view, even if continuous input signaling schemes achieve the secrecy capacity of MIMO system, continuous transmit signals are rarely used in practical communication systems. This is mainly due to the fact that, if the probability density function (PDF) of a transmit signal is continuous, the task of signal detection at the receiver will be significantly complicated. Therefore, in practice, transmit signals are discrete signals drawn from finite discrete constellations, such as pulse amplitude modulation (PAM) in the context of optical wireless communication. Due to this fact, the authors in [103] derived an achievable secrecy rate for the same system using discrete distributions with finite support sets. Precisely, assuming that the probability mass function (PMF) of the transmitted signal $\mathbf{s}$ is given by $f_{\mathbf{s}}(\mathbf{s}) = \sum_{i=1}^{Q} p_i \delta\left(\mathbf{s} - \mathbf{q}_i\right)$, where Q represents the number of mass points of $\mathbf{s}$, $\{\mathbf{q}_i \,|i \in [\![1, Q]\!]\}$ is its set of mass points, $\{p_i \,|i \in [\![1, Q]\!]\}$ is its set of mass probabilities and $\delta\left(\cdot\right)$ denotes the Dirac function, the proposed achievable secrecy rate in [103] is given by $R_{s,1}^{+}$, where

$$\begin{aligned} R_{s,1} = & \frac{1}{2}\log\left[\det\left(\mathbf{B}\right)\right] - \log\left[\sum_{i=1}^{Q}\sum_{j=1}^{Q} p_i p_j \exp\left(\frac{d_{i,j}}{2\sigma_A^2}\right)\right] \\ & - \frac{1}{2}\log\left[\det\left(\mathbf{I}_{K_1} + \frac{\mathbf{G}_1\mathbf{K}_{\mathbf{s}}\mathbf{G}_1^T}{\sigma_E^2}\right)\right], \end{aligned} \tag{6}$$

in which $\mathbf{K}_{\mathbf{s}} = \mathbb{E}\left(\mathbf{s}\mathbf{s}^T\right)$ represents the covariance matrix of the transmitted signal $\mathbf{s}$, $\mathbf{B} = 2\mathbf{I}_{N_1} - \left(\mathbf{I}_{N_1} + \frac{\mathbf{H}_1\mathbf{K}_{\mathbf{s}}\mathbf{H}_1^T}{\sigma_A^2}\right)^{-1}$ and, for all $i, j \in [\![1, Q]\!]$,

$$\begin{aligned} d_{i,j} = & \left(\mathbf{q}_i + \mathbf{q}_j\right)^T \mathbf{H}_1^T \mathbf{B}^{-1} \mathbf{H}_1 \left(\mathbf{q}_i + \mathbf{q}_j\right) \\ & - ||\mathbf{H}_1\mathbf{q}_i||_2^2 - \left|\left|\mathbf{H}_1\mathbf{q}_j\right|\right|_2^2, \end{aligned} \tag{7}$$

The core idea behind the achievable secrecy rate $R_{s,1}^{+}$ is based on the relation embedded on the Kullback–Leibler (KL) divergence, also known as the relative entropy, between continuous and discrete input distributions that have the same covariance matrix [106]. In addition, the achievable secrecy rate $R_{s,1}^{+}$ is valid for all possible configurations of the considered MIMO VLC wiretap channel, i.e., MIMO, MISO and SISO VLC wiretap channels.

Motivated by the result in (6), the authors in [103] investigated the case where the transmitter aims to send a zero-mean vector $\mathbf{u}$ containing L confidential messages, where $1 \leq L \leq M$, to the AU in the presence of an ED. Therefore, the transmitted signal is expressed as $\mathbf{s} = \mathbf{s}_1 = \mathbf{W}\mathbf{u}$, where $\mathbf{W}$ is the associated $M \times L$ precoding matrix. In this case, $\mathbf{u}$ and $\mathbf{W}$ were assumed to satisfy $||\mathbf{u}||_\infty \leq A$ and $||\mathbf{W}||_\infty \leq 1$ in order to fulfill the amplitude constraint in (4). Moreover, the authors in [103] assumed that the confidential messages are independent and identically distributed (i.i.d) according to a generic scalar random variable u that follows a truncated discrete generalized normal (TDGN) distribution within $[-A, A]$. Moreover, the ED was assumed to be randomly located within the coverage area and a precoding scheme based on the generalized singular value decomposition (GSVD) of the channel matrices was proposed in order to enhance the secrecy performance of the system.

As an illustration, Fig. 4 presents the average achievable secrecy rate $R_{s,1}^{+}$, obtained through 10^5 independent Monte-Carlo trials on the location of the AU and the ED, versus the square of the amplitude constraint A^2 in [dBm], for the system

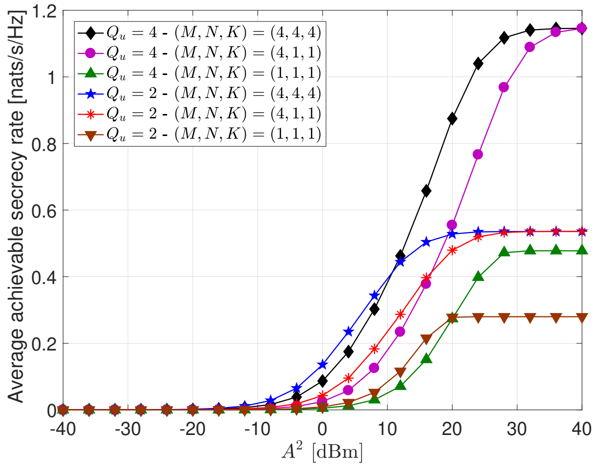


Fig. 4: Average achievable secrecy rate $R_{s,1}^{+}$ versus the square of the amplitude constraint A^2, for the system configurations $(M,N,K) = (4,4,4)$, $(4,1,1)$ and $(1,1,1)$ and for the number of mass points $Q_u = 2$ and $Q_u = 4$.

configurations $(M,N,K) = (4,4,4)$, $(4,1,1)$ and $(1,1,1)$ and for the number of mass points $Q_u = 2$ and $Q_u = 4$ of the random scalar variable u. The number of confidential messages is fixed to $L = 1$ and the precoding matrix $\mathbf{W}$ was optimized using the brute force (BF) search methods. The noise variance at the two receivers is fixed to $\sigma_A^2 = \sigma_E^2 = -68.93$ [dBm]. Fig. 4 shows that increasing the number of light sources of the transmitter and/or increasing the number of PDs at the receivers will increase the achievable secrecy rate $R_{s,1}^{+}$. In other words, it shows that increasing the system diversity will improve the secrecy performance of the system. In addition, Fig. 4 shows that the best number of mass points Q_u is a function of the operating range of the amplitude constraint A.

On the other hand, an upper bound on the secrecy capacity C_s was derived in [102], [103]. The key idea was converting the amplitude constraint into an average power constraint as $||\mathbf{s}||_\infty \leq A \implies \text{Trace}(\mathbf{K_s}) = \mathbb{E}\left(\mathbf{s}^T\mathbf{s}\right) \leq MA^2$, which is the trace constraint on the input covariance. The derived upper bound is given by

$$U_B = \max_{\mathbf{K_s}\geq 0} \frac{1}{2}\log\left[\frac{\det\left(\mathbf{I}_M + \frac{1}{\sigma_A^2}\mathbf{H}_1^T\mathbf{H}_1\mathbf{K_s}\right)}{\det\left(\mathbf{I}_M + \frac{1}{\sigma_E^2}\mathbf{G}_1^T\mathbf{G}_1\mathbf{K_s}\right)}\right] \quad \text{s.t. } \text{Trace}(\mathbf{K_s}) \leq MA^2. \tag{8}$$

It was stated in [107] that the optimal covariance matrix, solution of the optimization problem in (8), is expressed through the active eigenvectors, i.e., the ones associated to positive eigenvalues, of the matrix $\frac{\mathbf{H}_1^T\mathbf{H}_1}{\sigma_A^2} - \frac{\mathbf{G}_1^T\mathbf{G}_1}{\sigma_E^2}$. Based on this, the closed form expression of the upper bound (8) was derived for the special case where the number of PDs at the receivers is one, i.e., the SISO and MISO VLC wiretap systems. However, for the general case, iterative approaches were employed in [102], [103] in order to solve the optimization problem in (8).

B. Multiple EDs

For a MIMO VLC system with $N = 1$ AU and multiple EDs, the authors in [104] established a secure communication mechanism by minimizing the bit error rate (BER) in a protected zone and maximizing it everywhere else. On the other hand, for a MIMO VLC system with multiple AUs and multiple EDs, the authors of [105] improved the secrecy performance by using a continuous signaling scheme and applying angle diversity transmitters that are capable of transmitting data in narrow beams and effectively minimizing the leakage of information. By comparing different types of optical network deployments, they concluded that the hexagonal deployment is the best in terms of secure communications, whereas the Poisson point process (PPP) deployment is the worst.

IV. THE MISO VLC WIRETAP SYSTEM

A. System Model

In this section, each receiver is equipped with a single PD. The transmitter intends to transmit N sets of confidential messages to N spatially dispersed AUs in the presence of K EDs. As such, for all $i \in [\![1,N]\!]$ and $k \in [\![1,K]\!]$, the received signals at the ith AU and the kth ED are expressed, respectively, as

$$\begin{aligned} y_i &= \mathbf{h}_i^T\mathbf{s} + n_{A,i} \\ z_k &= \mathbf{g}_k^T\mathbf{s} + n_{E,k}, \end{aligned} \tag{9}$$

where $\mathbf{h}_i, \mathbf{g}_k \in \mathbb{R}_+^M$ are the $M \times 1$ channel gain vectors of the ith AU and the kth ED, respectively, and $n_{A,i}$ and $n_{E,k}$ are AWGN samples that are $\mathcal{N}\left(0,\sigma_A^2\right)$ and $\mathcal{N}\left(0,\sigma_E^2\right)$ distributed, respectively. In the following subsections, we review all the works reported in the literature on secure MISO VLC systems for the two cases when the transmitter communicates with a single AU or with multiple AUs.

B. Single AU

For a single AU, a large body of work in the literature proposed various PLS techniques that aim to provide secure communications, for both cases of single ED [59]–[75] and multiple EDs [76]–[80]. In the following, both cases of single and multiple EDs will be studied, respectively.

Single ED. In this case, it was shown in [108] that the optimal joint probability distribution $f_\mathbf{s}$ of the transmitted signal $\mathbf{s}$ that achieves the secrecy capacity of the system is unique, symmetric and discrete with a finite support set. However, neither the secrecy capacity nor the optimal input probability distribution were derived in closed-form and, thus, it remains an open problem. Therefore, both continuous [59]–[69] and discrete [70]–[75] signaling schemes were employed, in order to characterize the secrecy capacity of the system. In addition, beamforming and artificial noise (AN) based beamforming are the widely used PLS techniques for securing MISO VLC systems.

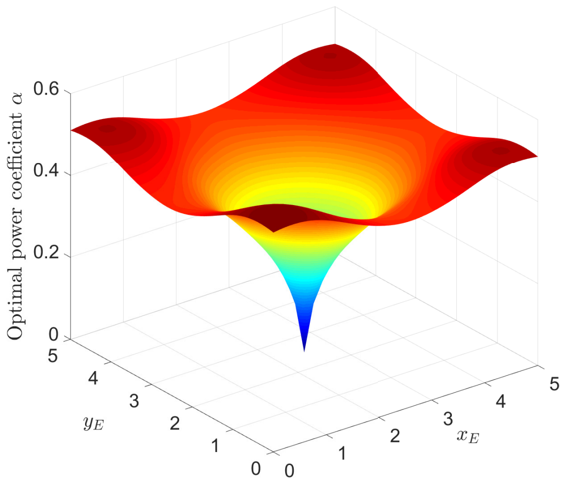
For the case of continuous signaling schemes, beamforming was employed in [59]–[62]. With beamforming, the transmitted signal is expressed as $\mathbf{s} = \mathbf{v}u$, where u denotes the confidential message intended to the AU and $\mathbf{v}$ denotes its associated beamforming vector. In [59], [60], the PDF of u was assumed to be uniform within $[-A, A]$ and the authors investigated the performance of beamforming for both scenarios, namely, when the ED's CSI is available at the transmitter or not. In the former scenario, zero-forcing (ZF) beamforming, also known as null steering, was employed in order to force the ED's reception to zero, i.e., $\mathbf{g}_1^T\mathbf{v} = 0$. However, in the latter case, the ED was assumed to be located within a predefined area known to the transmitter and robust beamforming was employed in order to maximize the worst case achievable secrecy rate. In [61], the authors used the truncated generalized normal (TGN) distribution as a probability distribution for u and derived closed-form expression for the optimal beamformer that maximizes the achievable secrecy rate of the system. In addition, they optimized over the TGN parameters to further enhance the secrecy performance of the system. In [62], a learning-based anti-eavesdropping framework via intelligent beamforming has been proposed to prevent the ED from wiretapping the IB signals, where the optimal beamforming policy was derived using a reinforcement learning (RL) scheme.

AN based beamforming was adopted in [63]–[69]. Specifically, in [63], [64], the proposed schemes consist of transmitting the IB signal from one AP and jamming signals from the remaining APs. Moreover, the IB and jamming signals were assumed to follow uniform distributions in [63] and truncated Gaussian distributions in [64]. In [65], among the M fixture of LEDs, M_t fixtures are used to transmit the IB signal and the remaining $(M - M_t)$ are used to transmit jamming signals. In [66], [67], the authors proposed an AN based beamforming scheme where, based on the available CSI of the AU and the ED, each transmitter's AP can choose to convey data or jamming signals. In [68], [69], the IB signal and the jamming signals were transmitted jointly through all APs. Specifically, the proposed scheme in [68], [69] consists of simultaneously transmitting a scalar information signal u and a scalar jamming signal x through two different beamforming vectors $\mathbf{v}$ and $\mathbf{w}$, respectively. In this case, the transmitted signal is given by $\mathbf{s} = \mathbf{v}u + \mathbf{w}x$, where $|u| \leq \alpha$, $|x| \leq (1 - \alpha)$, $||\mathbf{v}||_\infty \leq 1$ and $||\mathbf{w}||_\infty \leq 1$, such that $\alpha \in]0, 1]$, in order to satisfy the the amplitude constraint $||\mathbf{s}||_\infty \leq 1$. In addition, the effect of the jamming signal was forced to be canceled at the AU, i.e., $\mathbf{h}_1^T\mathbf{w} = 0$ and u and x were assumed to follow a uniform distribution in [68] and a TGN distribution in [69]. Note that in [69], both cases of perfect and imperfect ED's CSI were considered, where the derived achievable secrecy rates were maximized with respect to the corresponding beamforming vectors in the former case, and robust beamforming was employed in the latter case. However, in [68], the CSI of the ED was completely unknown to the transmitter. Therefore, the authors showed that the best transmission strategy to adopt is to send the IB signal u into the direction of the AU, i.e., $\mathbf{v} = \frac{\mathbf{h}_1}{||\mathbf{h}_1||_\infty}$, and the jamming signal into the orthogonal direction of the the AU, i.e., $\mathbf{h}_1^T\mathbf{w} = 0$. This AN scheme is known as the null-space AN, since the jamming signals are transmitted over the null space of the AU's channel gain $textbfh_1$.

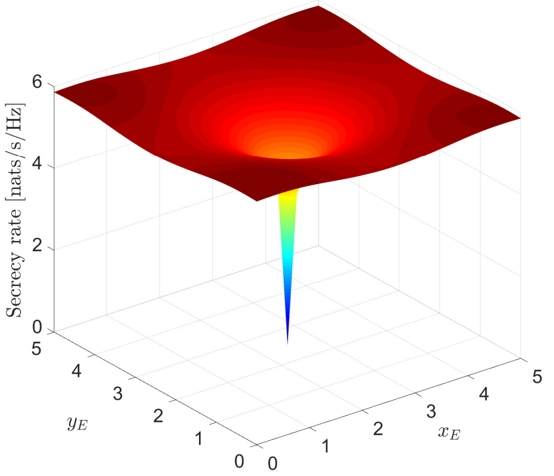
For the case of discrete signaling schemes, beamforming was employed in [70], where the authors tried to solve the secrecy capacity numerically since no closed-form expression of the secrecy capacity has been derived yet. In [71]–[73], AN aided precoding was employed. Specifically, in [71], the adopted secrecy performance measure is the signal to interference plus noise ratio (SINR) and the proposed scheme consists of transmitting a scalar IB signal through beamforming simultaneously with different jamming signals that are linearly precoded into a multi-dimensional jamming vector, i.e., $\mathbf{s} = \mathbf{v}u + \mathbf{W}\mathbf{x}$, where $\mathbf{x}$ is a vector of the jamming signals and $\mathbf{W}$ is its associated precoding matrix. In the same context, the authors in [72] recently employed the same AN based beamforming scheme adopted in [69]. However, differing from [69], both the IB signal u and the jamming signal x were drawn from a TDGN distribution. In addition, the ED was assumed to be randomly located in the coverage area and the authors used a stochastic geometry model to evaluate the statistics of the ED's SINR and the average achievable secrecy rate of the system.

One important aspect that should be investigated in the AN based precoding scheme in general is the optimal power allocation between the AN signals and the IB signals. With the objective of maximizing the achievable secrecy rate of the system, optimal design of the power allocation between the AN and the IB signals should be carried, subject to the amplitude constraint imposed on the transmitted electrical signals. In the literature, different optimization techniques have been developed and/or adopted for this secrecy enhancement problem. The choice of each optimization technique depends on the availability of the ED's CSI and the type of the input signaling scheme. For example, consider a room of size $L \times W \times H$ = 5m × 5m × 3m, where the transmitter is equipped with $M = 16$ APs located on the ceiling of the room. The AU is located at the center of the room and the ED is randomly located within the room. Assuming that the AN based beamforming scheme of [68], [69] was employed as a transmission strategy, Fig. 5 presents the optimal fraction of amplitude α allocated to the IB signal and the resulting achievable secrecy rate, versus the location of the ED where $\frac{A^2}{\sigma_A^2} = \frac{A^2}{\sigma_E^2} = 98.83$ dB. This figure shows that when the ED is close to the AU, the amplitude fraction α and the achievable secrecy rate decrease. Meaning, the transmitter has to allocate more amplitude, and power equivalently, to the jamming signals in order to degrade the reception of the ED.

Additionally, the authors in [72] employed the CCP technique to obtain the optimal beamfomring vectors of the AN and the IB signals that maximize the average achievable secrecy rate of a MISO VLC system with a randomly located ED and a discrete input signaling scheme. To this end, assuming the same indoor setting as in Fig. 5, Fig. 6 presents the average secrecy capacity, obtained numerical following the approach of [108], the average achievable secrecy rate with and without the use of AN, resulting from the adopted technique in [72], versus the square of the amplitude constraint A^2. This figure shows that how the use of well designed AN signals can improve



(a) Optimal fraction of amplitude α versus the ED's location (x_E, y_E).



(b) Secrecy rate versus the ED's location (x_E, y_E).

Fig. 5: Optimal fraction of amplitude α and the resulting secrecy rate versus the location of the ED (x_E, y_E) for an indoor MISO VLC system equipped with $M = 16$ LEDs in an indoor environment with size $L \times W \times H = 5\text{m} \times 5\text{m} \times 3\text{m}$.

the secrecy performance of MISO VLC systems, especially for the case when the transmitter has a coarse estimate of the statistics of the ED.

The potential of spatial modulation (SM) to enhance the secrecy performance of MISO VLC wiretap systems was investigated in [73]–[75]. Specifically, in [73], AN based beamforming was proposed, where SM was used to transmit the IB signal and truncated Gaussian was adopted for the jamming signal. In [75], the authors studied the secrecy performance of the MISO VLC system employing SM, termed as the MISO SM-VLC. The authors obtained a lower bound and an accurate closed-form expression for the approximate achievable secrecy rate of the generalized space shift keying (GSSK) VLC system and also derived closed-form expressions for the pairwise error probability and bit error rate of the system. Similar results were obtained in [74], where the authors proposed a LED pattern selection algorithm in order to enhance the secrecy performance of the GSSK VLC system.

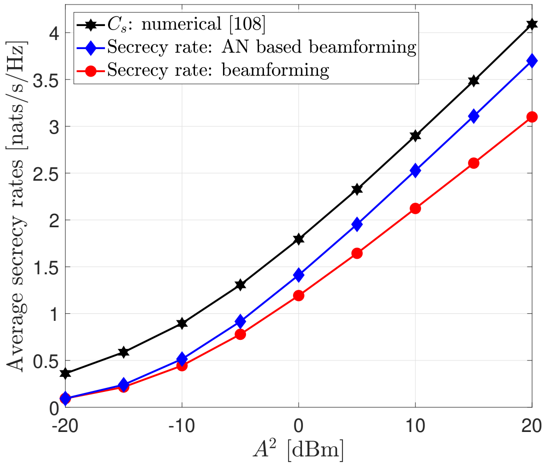


Fig. 6: Average secrecy capacity C_s and average achievable secrecy rate with and without the use of AN signals versus A^2 for an indoor MISO VLC system for an indoor MISO VLC system equipped with $M = 16$ LEDs in an indoor environment with size $L \times W \times H = 5\text{m} \times 5\text{m} \times 3\text{m}$.

Multiple EDs. For the case of multiple EDs, both continuous [76]–[79] and discrete [80] signaling schemes were employed. However, only beamforming was employed to secure this class of VLC systems. In [76], [77], the authors proposed a LED selection scheme to improve the secrecy outage probability (SOP) of the system. The SOP represents the probability that the instantaneous secrecy capacity C_s falls below a target secrecy rate R_{th} [109], i.e., $\mathbb{P}\left(C_s \leq R_{th}\right)$. However, due to the amplitude constraint imposed on the transmitted signal, the secrecy capacity is not readily available and a modified SOP was employed as a secrecy performance measure instead. In addition, the authors in [76], [77] assumed that the EDs are not colluding. In this case, only the ED with the strongest SNR is considered as a potential threat. Moreover, the EDs were assumed to be randomly located in the coverage area and thus their CSI is unknown to the transmitter. In such a case, stochastic geometry approaches can be used to characterize the system secrecy performance.

The proposed approaches in [76], [77] are based on proposing stochastic geometric models for the channel gains of the EDs [110], [111]. Stochastic geometry is a powerful tool for dealing with spatial uncertainty [112], [113]. In fact, when the EDs are distributed randomly in the considered area, stochastic geometry can be used to determine the statistics of their individual CSI and, thus, it can provide closed-form expressions for typical secrecy performance measures. In [76], [77], the number of EDs was modeled using the PPP model and the locations of each ED were assumed to be uniform within the coverage area. Based on this, the authors employed a stochastic geometry model to derive a closed-form expression of the SOP and proposed a beamforming scheme that enhances the secrecy performance.

The same problem but with colluding and randomly located EDs was considered in [78]. The authors employed beamforming as a transmission strategy and used stochastic geometry to derive an approximate expression of the average achievable secrecy rate. Then, the resulting problem of optimal beamforming that maximizes the average achievable secrecy rate was solved. In [79], an experimental AN based precoding scheme was proposed. The experimental setup consists of eight arrays of LEDs, where four arrays are used for data transmission and four arrays are used for AN transmission. Experimental and simulation results show that the proposed scheme highly outperforms the scheme that does not inject AN. In [80], the EDs were assumed to be colluding and randomly located similar to [78]. However, differing from [78], only discrete input signaling schemes were employed and the authors derived an average achievable secrecy rate using stochastic geometry and proposed a beamforming solution that maximizes the resulting average achievable secrecy rate.

C. *Multiple AUs*

Several studies in the literature have proposed transmission strategies and precoding designs to secure MU-MISO VLC broadcast channels [114]–[123]. It was assumed in [114]–[118] that there were no EDs, but the AUs were treated as potential EDs when a message was not intended for them, i.e., when the messages were confidential. In [119]–[123], however, external EDs were assumed to coexist with the AUs, while the AUs were continually treated as potential EDs.

Although it was assumed in [114]–[118] that there is no external ED in the vicinity of the AUs, the transmitted messages to the AUs were assumed to be confidential, such that each AU is supposed to receive and decode only its own message, i.e., users remain ignorant about messages that are not intended to them. In other words, the transmitter has to communicate each message to its intended AU while keeping each AU unaware of the other messages. In [114], the secrecy performance of a two-user MISO broadcast channel with confidential messages was considered, where a per-antenna amplitude constraint and a per-antenna power constraint were assumed and the authors investigated the problem of optimal linear precoding schemes. ZF precoding in conjunction with continuous uniform signaling scheme was employed in [115], [116] to cancel information leakage between users. The same problem was investigated in [117], [118], where the transmitter was assumed to communicate with multiple spatially dispersed AUs. Linear precoding schemes were developed to enhance the secrecy performance of the system. In [117] a GSVD-based precoding was proposed, whereas in [118], the optimal linear precoding scheme was obtained through CCP programing. In this context, typical secrecy performance measures, such as the max-min fairness, the harmonic mean, the proportional fairness and the weighted fairness, were investigated. These secrecy performance measures are defined as follows. Let S be the objective function that represents the secrecy performance measure of interest and for all $i \in [\![1, N]\!]$, let R_i be the achievable secrecy rate of the ith AU. Thus, the aforementioned secrecy performance measures are defined as [124]:

i) Max-min fairness: $S = \min\limits_{1 \leq i \leq N} R_{s,i}$.

ii) Harmonic mean: $S = K \left(\sum_{i=1}^{N} R_i^{-1} \right)^{-1}$.

iii) Proportional fairness: $S = \left(\prod_{i=1}^{N} R_i \right)^{\frac{1}{K}}$.

iv) Weighted fairness: $S = \sum_{i=1}^{N} \alpha_i R_i$, where $(\alpha_i)_{1 \leq i \leq N} \in \mathbb{R}^+$,

with an increasing order of achievable secrecy sum-rate and a decreasing order of user fairness [124].

The problem of secure MU-MISO broadcast channels with multiple EDs was investigated in [119]–[123]. For the case when there is only one ED, i.e., $K = 1$, the authors in [119], [120] studied the potential of employing ZF precoding and AN schemes in providing secure VLC communications. In the same case, an AN based precoding scheme was proposed in [121], [122]. The proposed scheme was designed to solve the max-min fairness SINR problem among AUs in two different scenarios: known and unknown ED's CSI at the transmitter. In the former case, the proposed scheme was designed in such a way that it kept the SINR of the ED below a predefined threshold, whereas in the latter case, the traditional null-space AN scheme was employed, which consists of sending jamming signals in all the orthogonal directions of the AUs. For the case when $K > 1$, the authors in [123] proposed a three-dimensional network model, where the VLC APs were modeled by a two-dimensional homogeneous PPP in the ceiling and the locations of of both the AUs and the EDs were modeled by another independent two-dimensional homogeneous PPP. In this case, for VLC networks with and without APs cooperation, the secrecy performance of the system was evaluated using the SOP and the ergodic secrecy rate.

V. THE SISO VLC WIRETAP SYSTEM

A. *System Model*

In this section, we consider the SISO VLC case where the transmitter is equipped with $M = 1$ AP. The transmitter intends to transmit $N \in \mathbb{N}$ confidential messages to N AUs, each equipped with a single PD, in the presence of a set of K spatially dispersed EDs, each equipped with a single PD. Let $\{u_i | i \in [\![1, N]\!]\}$ be the set of confidential messages intended to the AUs, where for all $i \in [\![1, N]\!]$, u_i is the confidential message intended for the ith AU. The confidential messages are encoded via SC into one scalar signal $s = \sum_{i=1}^{N} u_l$, that should satisfy the amplitude constraint in (4), i.e., $|s| \leq A$. Based on this, for all $i \in [\![1, N]\!]$ and $k \in [\![1, K]\!]$, the received signals at the ith AU and the kth ED are expressed, respectively, as

$$\begin{aligned} y_i &= h_i s + n_i \\ z_k &= g_k s + w_k, \end{aligned} \tag{10}$$

where $h_i, g_k \in \mathbb{R}^+$ are the channel gains of the ith AU and the kth ED, and n_i and w_k are AWGN samples that are $\mathcal{N}\left(0, \sigma_A^2\right)$ and $\mathcal{N}\left(0, \sigma_E^2\right)$ distributed, respectively. For all $i \in [\![1, N]\!]$ and $k \in [\![1, K]\!]$, let $\rho_{A,i} \triangleq \frac{h_i^2}{\sigma_A^2}$ and $\rho_{E,k} \triangleq \frac{g_k^2}{\sigma_E^2}$ denote the normalized received SNR at the ith AU and at the kth ED, respectively. Finally, let $\rho_E = \sum_{k=1}^{K} \rho_{E,k}$. In the following, we review all the works and results reported in the literature on secure SISO VLC systems for the single AU and multiple AUs cases.

B. Single AU

In this subsection, we assume that the transmitter communicates with $N = 1$ AU. In this case, note that if $\rho_{A,1} \leq \rho_E$, then the SISO VLC wiretap channel is not degraded and, therefore, the secrecy capacity $C_s = 0$ [125]. However, If $\rho_E < \rho_{A,1}$, then the SISO VLC wiretap channel is strictly degraded and the secrecy capacity is not null [125]. Therefore, we assume to the end of this part that $\rho_E < \rho_{A,1}$. In this case, It was shown in [125] that the secrecy capacity achieving probability distribution is unique, symmetric and discrete with a finite support set. However, neither the secrecy capacity nor the optimal input probability distribution were derived in closed-form and it remains an open problem. Therefore, several upper and lower bounds were derived in the literature in an attempt to characterize the secrecy capacity of the system.

The problem of secure SISO VLC systems with a single AU and single ED with perfect CSI was investigated in [59], [81]–[83]. In [59], an achievable secrecy rate for the system was proposed and it is given by $R^+_{s,2}$, such that

$$R_{s,2} = \frac{1}{2}\log\left(1 + \frac{2A^2}{2\pi e}\rho_{A,1}\right) - \frac{\gamma}{\sqrt{2\pi\sigma_E^2}}\exp\left(\frac{-\gamma^2}{2\sigma_E^2}\right)$$
$$- \left(1 - 2\mathcal{Q}\left(\frac{\gamma}{\sigma_E} + \sqrt{\rho_E}A\right)\right)\log\left(\frac{2\left(\sqrt{\rho_E}A + \gamma\right)}{\sqrt{2\pi}\left(1 - 2\mathcal{Q}\left(\frac{\gamma}{\sigma_E}\right)\right)}\right)$$
$$- \mathcal{Q}\left(\frac{\gamma}{\sigma_E}\right) + \frac{1}{2}, \tag{11}$$

where $0 < \gamma$ is a free parameter and $\mathcal{Q}(\cdot)$ denotes the $\mathcal{Q}$-function. The core idea behind the achievable secrecy rate $R^+_{s,2}$ is based on the capacity results of free space optical intensity channels provided in [97]. In [81], [82], the authors considered the illumination requirement of LEDs and added an average optical power constraint along with the peak-power constraint. Then they derived upper and lower bounds on the secrecy capacity of the system.

Based on the type of the input distribution p_s, i.e., either continuous or discrete over the interval $[-A, A]$, two achievable secrecy rates were proposed in the literature. Specifically, assuming that the transmitted signal s is continuous, an achievable secrecy rate for the system, that was proposed in [83], is given by $R^+_{s,3}$, such that

$$R_{s,3} = \frac{1}{2}\log\left(1 + \frac{\exp\left(2h_{u_1}\right)}{2\pi e}\rho_{A,1}\right) - \frac{1}{2}\log\left(1 + \sigma_{u_1}^2\rho_E\right), \tag{12}$$

where h_{u_1} denotes the differential entropy u and $\sigma_{u_1}^2$ denotes its variance. Several continuous input distributions were proposed in the literature, which aim to maximize the achievable secrecy rate $R_{s,3}$, including the uniform distribution, the truncated Gaussian distribution and the truncated generalized normal (TGN) distribution [83]. Furthermore, by using discrete probability distributions, another achievable secrecy rate was proposed in [83]. This achievable secrecy rate is $R^+_{s,1}$ in (6) for the special case when $(M, N, K) = (1, 1, 1)$.

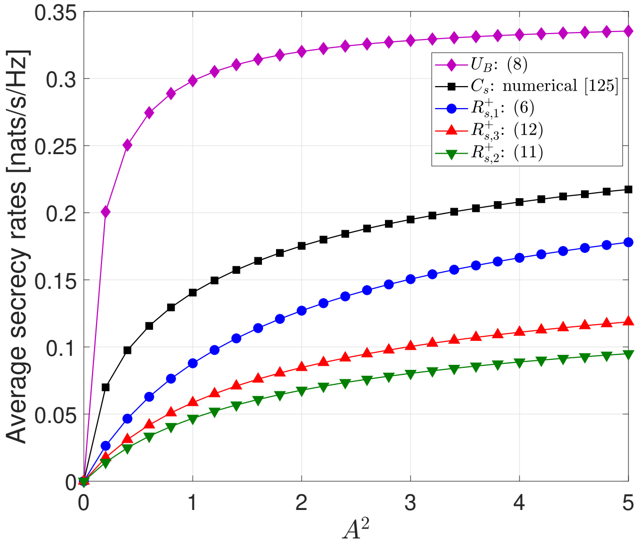


Fig. 7: Upper bound U_B, secrecy capacity C_s and lower bounds $R^+_{s,1}$, $R^+_{s,2}$ and $R^+_{s,3}$ versus A^2. $\sigma_A^2 = \sigma_E^2 = -98.83$ [dBm].

Fig. 7 presents the upper bound U_B in (8), the numerical calculation of the secrecy capacity C_s and the lower bounds $R^+_{s,1}$, $R^+_{s,2}$ and $R^+_{s,3}$, obtained through 10^5 independent Monte-Carlo trials on the location of the AU and the ED, versus A^2. The secrecy capacity is obtained numerically by using the same approach invoked in [125], whereas for the lower bounds $R^+_{s,1}$ and $R^+_{s,3}$, the TGN and the TDGN distributions were adopted, respectively. Specifically, the best parameters of the TGN and the TDGN distributions are obtained through brute force (BF) search methods. As shown in this figure, the lower bound $R^+_{s,1}$, the one that corresponds to the discrete input distributions with finite support sets, is the best lower bound, which is not surprising since it is already known that the optimal input distribution for the degraded SISO VLC wiretap channel is discrete with a finite support set [125].

When the EDs' CSI is not available at the transmitter, it becomes more challenging to characterize the secrecy capacity and quantify the achievable secrecy rate. To overcome this obstacle, researchers have proposed invoking stochastic geometry approaches [83]–[85]. In this context, the locations of the EDs are treated as random variables, and therefore, one may quantify the achievable secrecy rates by averaging over all possible locations. In [83], only one randomly located ED is considered, whereas in [84], [85], multiple randomly located EDs were considered. All receivers, including that of the AU, were assumed to be uniformly distributed within the coverage area and their orientation was assumed to be fixed and facing the transmitter. Specifically, in [83], the statistics of the received SNRs $\rho_{A,1}$ and ρ_E were derived, which lead to evaluating the secrecy performance of the system in terms of the average secrecy rates $\mathbb{E}\left(U_B\right)$, $\mathbb{E}\left(R^+_{s,1}\right)$ and $\mathbb{E}\left(R^+_{s,3}\right)$. In [84], [85], the PPP process was used to model the number of EDs. The main differences between [84], [85] are as follows. The EDs were assumed to be non-colluding in [84] and colluding in [85]. In addition, the authors in [84] studied the impact of multipath reflections on the secrecy performance, whereas only the LoS component of the channel gains was considered in [85]. In both papers, the statistics of the received SNRs were derived, which facilitates evaluating the secrecy performance in terms of the SOP. Finally, the lower bound $R_{s,3}^{+}$ in conjunction with uniform distribution was adopted as an achievable secrecy rate.

C. Multiple AUs

The problem of secure MU-SISO VLC channels was investigated in [88], [89], [126] consists of a transmitter communicating with N AUs in the presence of a set of EDs, where their number is modeled using a PPP model. Specifically, in [88], only the AU at the room center was supposed to be a legitimate user, while all other users were supposed to be EDs. In addition, all the EDs, including the remaining AUs, were assumed to be non-cooperative, i.e., they do not share the eavesdropped information. In this case, only the ED with the highest received SNR $\rho_{E,max}$ was considered as a potential eavesdropper. Based on this, the statistics of $\rho_{E,max}$ were derived, which yielded a closed-form expression of the SOP. However, since the closed-form expression of the secrecy capacity with the input amplitude constraint is not readily available, the amplitude constraint was ignored and Gaussian signaling was adopted instead. In [89], [126], a two-user NOMA-SISO VLC system was considered. The transmitter communicates simultaneously with two uniformly distributed AUs within the coverage area. Assuming that the EDs are not colluding and by considering only the ED with the highest SNR, the authors derived a closed-form expression for the SOP for each AU.

D. Relay-Aided Secure Transmission for VLC

Motivated by their ability to improve the SNR and overall performance of optical wireless communication systems, relaying luminaries have been studied in [127]–[130] under various settings and assumptions, where it was shown that multi-hop diversity gains can be provided at VLC receivers. From a security point of view, consider the indoor VLC system shown in Fig. 8, where a transmitter communicates with multiple AUs in the presence of an ED and a number of cooperative trusted relaying devices assist the links between the transmitter and the AUs. The authors in [86], [87] considered the case where the number of AUs is $N = 2$. In order to enhance the secrecy performance of this broadcast system, the authors investigated two transmission strategies: the direct transmission and the relay-aided transmission. For the direct transmission strategy, superposition coding with uniform signaling was used, whereas in the relay-aided transmission strategy, three secure transmission schemes were studied, which are:

1) Cooperative jamming: the relay acts as a jammer and sends AN signals in order to degrade the ED reception.
2) Decode-and-forward: the transmitter sends the IB signal to the relay, which in turn decodes and then forwards it to the AU.
3) Amplify and forward: the transmitter sends the IB signal to the relay, which in turn amplifies it by infusing more optical power and then forwards it to the AU.

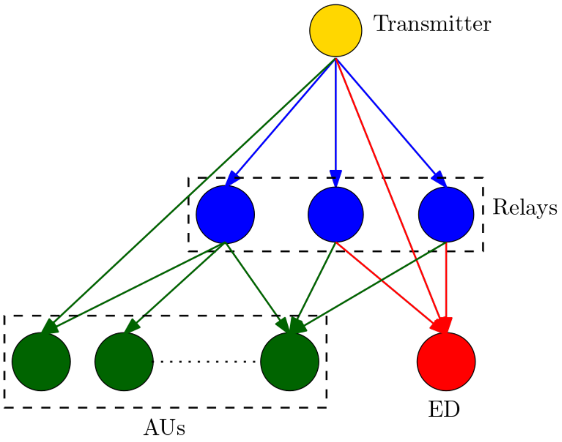


Fig. 8: An indoor VLC system model in which a transmitter communicates with multiple AUs in the presence of an ED. A number of cooperative trusted relaying devices assist the links between the transmitter and the AUs.

For all these transmission schemes, the authors derived the achievable secrecy regions and studied the performance of each scheme with respect to the geometry of the coverage area and the location of the ED.

VI. HYBRID VLC/RF SYSTEMS

In indoor environments, the light diffused from LED sources is naturally confined to a small area. In addition, the light beams are susceptible to indoor blockages, such as the human body, which may cause severe fluctuations in the received SNR. Consequently, the hybrid integration of VLC and RF systems was envisioned to significantly improve the user experience, since VLC systems can support very high data rates in specific areas and RF systems can provide greater coverage area to support mobility [131]–[133]. In addition, one of the challenges of adopting VLC systems in indoor environments is the VLC uplink transmission mechanism, especially if one relies on the existing indoor infrastructure for using LEDs for illumination and as VLC APs. To overcome these limitations, two alternatives were proposed in the literature. The first alternative is the invention of light-fidelity (LiFi) technology. LiFi is a fully networked optical communication system that includes both uplink and downlink transmissions [57]. The uplink operates over the infrared (IR) spectrum while the downlink operates over the visible light spectrum [57]. The second alternative consists of deploying hybrid wireless fidelity (WiFi)/LiFi.

WiFi and LiFi technologies are bidirectional and can jointly provide high coverage and high data rates. Fig. 9 presents an illustration of the hybrid WiFi/LiFi architecture, where the RF AP is a WiFi node and the VLC AP is a LiFi node. When a user is inside the LiFi coverage, it can be served through both APs and, hence, the received data rates and the quality of service (QoS) are higher. This is said assuming that the user has the multi-homing capability, i.e., it can aggregate the information from the WiFi and LiFi transmitters. Moreover, when a user is outside the LiFi coverage, it can still be served through the WiFi AP. Based on this, since hybrid VLC/RF systems encompass VLC components and

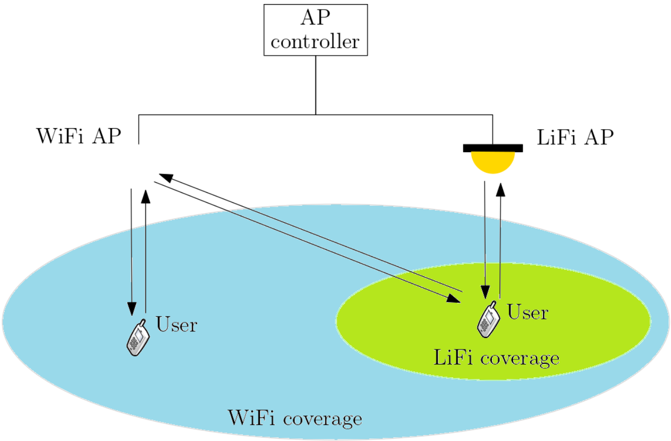


Fig. 9: Illustration of the heterogeneous LiFi-WiFi system.

RF components jointly, security for hybrid VLC/RF systems should be attentively investigated due to the broadcast nature of both communication systems, which is the focus of this section.

Security for hybrid VLC/RF networks was investigated in [134]–[138]. In [134], a downlink hybrid RF/VLC wiretap system was considered, where one RF AP, equipped with multiple antennas, and one VLC transmitter, equipped with multiple LEDs, communicate jointly with one AU in the presence of one ED. The two receivers were assumed to have the multi-homing capability, i.e., they can aggregate the information from the RF and VLC transmitters. The authors employed beamforming as a transmission strategy and then optimized over the beamforming vectors and the transmit powers at both the VLC and RF AP. Then, they formulated the PLS scheme in order to minimize the total consumed power while achieving target RF and VLC information rates at the AU and maintaining zero information rate at the ED. In [135], [136], a bidirectional hybrid RF/VLC wiretap system was considered, where one VLC transmitter, equipped with one AP, transmits confidential messages to a randomly located AU in the presence of one randomly located ED. In addition, it was assumed that the two receivers harvest energy from the light intensity. In addition, the AU communicates with an RF AP and this uplink transmission of the information is performed over an RF link that suffers from Rician fading, while the ED tries to acquire the transmitted information. The authors derived the secrecy outage probability using stochastic geometry and evaluated the secrecy performance of the system with respect to the geometry of the coverage area. In [137], secrecy performance of a relay-assisted hybrid VLC/RF SISO system was investigated, where a relay can extract the DC component and collect energy from the optical transmitted signal in the VLC link and then use this collected energy to retransmit data through the RF link to the AU. Recently, the authors in [138] investigated the secrecy performance of a hybrid VLC/RF system equipped with decode-and-forward relaying, where they developed PLS algorithms based on ZF beamforming techniques that mitigate eavesdropping in both RF and VLC networks.

VII. FUTURE RESEARCH DIRECTIONS

Although many papers have been published on various aspects of VLC systems, we believe there are still many open problems that need to be addressed to bring the potential of VLC-related technologies to their full potential. Since this paper is concerned with security, we dedicate the rest of this section to highlighting a number of open research problems related to security for VLC.

A. *Input Signaling Schemes*

The input signaling schemes present a fundamental feature in designing wireless communication systems. In fact, any transmission scheme and the resulting system performance depend on the type of adopted input signaling scheme. In general, each input signaling scheme consists of two main parts, namely, the input probability distribution and the precoding scheme, also known as the transmission strategy. The input probability distribution defines the probability distribution according to which the signals are transmitted. This can be either continuous or discrete. The precoding scheme defines the form or the shape of the transmitted signal, and it includes the modulation scheme as well. Among the well known precoding schemes for the case of a single AU, one can cite beamforming, AN based beamforming, OFDM and spatial modulation [139], [140], etc. On the other hand, for the case of multiple AUs, one can cite linear precoding, such as GSVD-based precoding and ZF precoding, orthogonal multiple acces (OMA) such as orthogonal frequency division multiple access (OFDMA) [141], NOMA [142], [143] and spatial modulation. As shown in previous sections, the input signaling scheme has a high impact on the secrecy performance of VLC systems. However, the optimal input signaling scheme for secure VLC systems is still an open problem.

Recall that VLC systems impose a peak-power constraint, i.e. amplitude constraint, on the channel input, which is fundamentally different from the average power constraint. In fact, when average power constraints are imposed, it was shown that Gaussian signaling schemes are optimal [58]. However, from an information theoretic point of view, finding the optimal input signaling schemes that achieve the secrecy capacity of a Gaussian wiretap channel under an amplitude constraint is still an open problem. This is attributed to the fact that, when input distributions of unbounded support like Gaussian inputs are not permissible, the optimal input distribution is either unknown or only known to be discrete for the special cases of a degraded SISO wiretap channel [125] and a MISO wiretap channel [108]. However, for both cases, neither the optimal input distribution nor the secrecy capacity were derived in closed-form expressions in the literature. Given that VLC falls into this category since amplitude constraints must be satisfied, the optimal signaling scheme for secure VLC systems is still an open problem.

B. *PLS for Indoor VLC Systems: What is Missing?*

A summary of the input signaling schemes and the PLS techniques employed to secure VLC systems that are reported in the literature are presented in Table II and Table III, respectively. By having a closer look at this two tables, one can note that there is a good number of problems related to secure indoor VLC systems that have not been resolved or even considered. A list of these problems is detailed on the following.

1) For the MU-MISO VLC broadcast channel considered in subsection IV-C, all previous works used only continuous input distributions. However, adopting continuous input signaling is unrealistic since digital data streams should be transmitted. In addition, discrete input signaling has been shown to be optimal for the two-user IM-DD discrete memoryless free space optical broadcast channels with non-negativity, peak and average intensity constraints at the transmitter [144]. Although it is not straightforward to derive optimal precoding schemes for secure communications in MU-MISO VLC broadcast channels with an arbitrary number of AUs using discrete distributions, there is a good chance that the secrecy performance of these systems may be enhanced by adopting this class of input distributions.
2) The secrecy performance of the MU-MIMO VLC broadcast channel adopted in has not been investigated in the literature. In a typical MU-MIMO VLC broadcast channel, the transmitter is equipped with multiple APs and serves multiple AUs, each equipped with multiple PDs, in the presence of a set of colluding EDs with imperfect CSI. This model is not only a generalized model that encompasses all the VLC systems adopted in the literature but also the most realistic one [145], [146]. Therefore, investigating the secrecy performance of this system is also an important contribution to the topic of secure VLC systems.

C. Incorporating Realistic and Measurements Based VLC Channel Models

All of the studies on secure VLC systems reported in the literature employed the VLC channel model presented in section II-A. In this model, it usually assumed that the receiver in an indoor VLC system is either stationary or uniformly distributed within the area of interest and that its orientation is constant (vertically upward and fixed). However, the presence of mobility and device orientation as well as link blockage, which are inherent features of wireless networks, require more realistic and non uniform models. In addition, none of the previous studies on secure VLC systems have considered the actual statistics of the receiver's mobility and orientation. This is attributed to the simplicity of the adopted model and also to the lack of proper channel models for the mobility and orientation of VLC devices in indoor scenarios. Nevertheless, several measurement-based channel models for VLC system were derived recently for various environments, such as indoor VLC systems [147]–[153], VLC-based vehicular communication [154] and underwater VLC systems [155], [156].

TABLE III: Summary of PLS techniques for Secure Indoor VLC Systems.

Environment's State	Recommended Techniques
Perfect CSI	1) Optimal precoding [102], [118] 2) GSVD precoding [103], [117] 3) ZF precoding [60], [68], [116], [120] 4) AP selection [76], [77]
Imperfect CSI	1) Robust precoding [59], [60] 2) AN based beamforming [69], [72] 3) AP arrangement [63]–[67] 3) Stochastic geometry [83]–[85], [88], [89], [126]
No available CSI	1) Null-space artifitial noise [68] 2) Protected zone [104]

In general, a receiver in a VLC system can be mobile and can have a random orientation. From section II-A, the channel gain of an indoor VLC receiver is expressed as

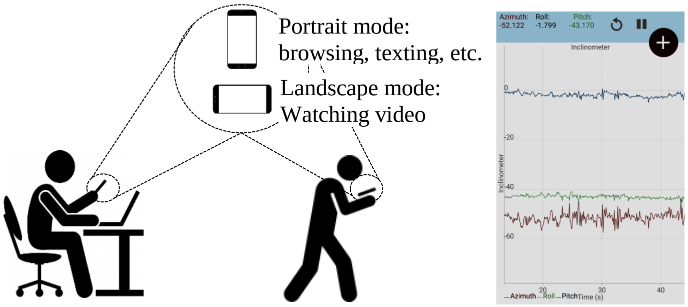
$$h = C\cos(\theta)^m \frac{\cos(\psi)}{d^2}\mathrm{rect}\left(\frac{\psi}{\Psi}\right), \tag{13}$$

where $C = \dfrac{\eta\, R\, T\, (m+1)}{2\,\pi} \frac{n_c^2 A_g}{\sin(\Psi)^2}$. The user's mobility will induce randomness in the distance d, the angle of transmission θ as well as the angle of incidence ψ, whereas the random orientation of the user's device will induce randomness only in the angle of incidence ψ. Recently, the authors in [149]–[152] derived measurement-based VLC channel models for indoor VLC receivers with random orientation, where they showed that the incidence angle ψ follows a truncated Laplace distribution if the receiver is stationary and a truncated Gaussian distribution if the receiver is mobile. The experimental measurements were obtained for both sitting and walking activities, in portrait and landscape modes as shown in Fig. 10. The impact of device orientation on LoS link availability is assessed in [157]. In [158], the authors used the Laplace distribution to derive the PDF of SNR and BER of indoor VLC systems analytically. It was shown that the random orientation of a device can influence the user's performance, which depends on its location.

Considering the receiver's mobility, several mobility models have been proposed in the literature to model the distribution of mobile users in indoor scenarios. The most commonly used mobility model in indoor systems is the random waypoint (RWP) mobility model [159]–[163]. In this stochastic model, each user of the network uniformly chooses a random destination point ("waypoint") in a given deployment area. A user moves to this destination with a velocity v chosen uniformly in the interval $[v_{\min}, v_{\max}]$. When it reaches the destination, it remains static for a random pause time and then starts moving again according to the same rule. Recently, the authors in [164], [165] derived the channel statistics for indoor mobile VLC receivers using the RWP mobility model, where the receiver's orientation is assumed to be fixed in [164] and uniformly distributed in [165]. In addition, motivated by the results of [164], the authors in [166] investigated the secrecy performance of the strongest AU in a SISO NOMA VLC system in the presence of multiple mobile and colluding EDs, where the receivers' orientation was assumed to be fixed

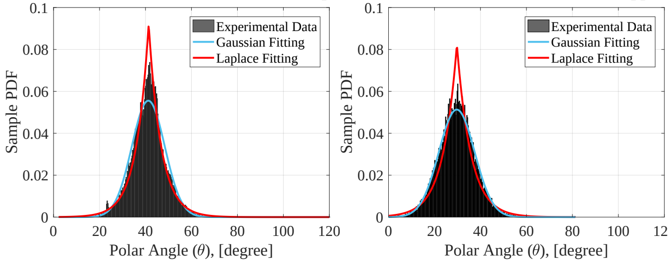
TABLE II: Summary of Input Signaling Schemes for Secure Indoor VL Systems.

			Continuous signaling scheme	Discrete signaling scheme
MIMO	Single AU	Single ED	[102]	[103]
		Multiple EDs	∅	[104]
	Multiple AUs	Single ED	∅	
		Multiple EDs	[105]	∅
MISO	Single AU	Single ED	[59]–[69]	[70]–[75]
		Multiple EDs	[77]–[79]	[80]
	Multiple AUs	Without EDs	[114]–[116], [118]	∅
		Single ED	[119]–[122]	∅
		Multiple EDs	[123]	∅
SISO	Single AU	Single ED	[59], [81]–[83]	[83]
		Multiple EDs	[84], [85]	∅
	Multiple AUs	Single ED	[86], [87]	∅
		Multiple EDs	[88], [89]	∅
Hybrid RF/VLC	Single AU	Single ED	[134]–[136], [138]	∅
		Multiple EDs	∅	
	Multiple AUs	Single ED		
		Multiple EDs		



(a) Measurement setup.

(b) Sensor App.



(c) Sitting activities [151].

(d) Walking activities [151].

Fig. 10: Illustration of experimental setup for both sitting and walking activities.

and their mobility was characterized using the RWP mobility model. Based on this, the channel statistics and the SOP of the strongest AU were derived using stochastic geometry.

Based on the above discussion, re-investigating the secrecy performance of VLC systems by considering the aforementioned measurement-based channel models and mobility models presents an interesting future research direction, since it helps to develop adequate PLS techniques for VLC systems in practical and real-life scenarios. Furthermore, in order to analyze the performance of mobile users more realistically, an orientation-based RWP (ORWP) mobility model was first proposed in [151] and then extended in [152]. The ORWP model provides a more realistic framework for performance evaluation of mobile users in VLC systems by incorporating the orientation of the device and the mobility of the user. Therefore, studying the secrecy performance for mobile users according to the ORWP mobility model can be another future research topic.

The VLC channel is also susceptible to link blockage. Due to the inherent nature of the VLC channel, the link between a pair of receiver and transmitter can be interrupted by obstructions such as a human body or other similar objects. However, it is noted that the main cause of link blockage is the mobile users in the indoor environment. The blockers can be modeled either as cylindrical objects [167] or rectangular prisms [168]. When the communication link is interrupted by blockers, adding extra power cannot compensate for the data loss. Solutions to simplify the effect of link blockage were introduced in [152], [169], [170]. A multi-directional receiver (MDR) for which PDs are located at different sides of a smartphone is introduced in [152], [169] and has been assessed in the presence of link blockage, user mobility as well as device random orientation. It is denoted that the MDR structure outperforms the conventional configuration for which all PDs are placed on one side of a smartphones, for example on the screen side. In [170], the author proposed an omnidirectional receiver in which PDs are embedded on all sides of a smartphone. This configuration is a robust scheme against blockage. Its superior performance is compared to a single-PD and two-PD configurations. Accordingly, the secrecy performance of the VLC system can be evaluated in the presence of blockers with different densities in an indoor environment. Moreover, the MDR configuration and omnidirectional receiver are the other two interesting future perspectives that should be studied from a secrecy performance aspect.

D. Security for Outdoor VLC systems

Outdoor VLC applications are less explored when compared to their indoor counterparts. This is mainly due to two facts: 1) the dual use of LEDs is not always practical in an outdoor VLC environment, and 2) the level of interference and noise is considerably higher in outdoor environments. Nevertheless, several outdoor VLC applications have been identified in the literature. The adoption of VLC in outdoor applications was reviewed in [171], where the authors revealed the issues that arise in the outdoor usage of VLC, identified emerging challenges and proposed future research directions. In this context, VLC outdoor applications include, but are not limited to, [172],

1) Vehicle-to-everything (V2X) communication.
2) Pedestrian-to-infrastructure (P2I) communication.
3) Building-to-building (B2B) communication.

V2X communications is a new concept that uses the latest generation of information and communication technology that connect vehicles to everything. In its turn, and as shown in Fig. 11, V2X communication includes [173]

1) Vehicle-to-infrastructure (V2I) communication, also known as road to vehicle (R2V) communication.
2) Vehicle-to-vehicle (V2V) communication.

The V2X technology links the various elements of transportation, such as pedestrians, vehicles, roads, and cloud environments. This leads to the building of an intelligent transport system and promoting the development of new modes and new forms of automobiles and transportation services by gathering more information and promote the innovation and application of automated driving technology [176]. In addition, V2X communication is of great significance for improving traffic efficiency, saving resources, reducing accidents, and improving traffic management [176], [177]. Additionally, in outdoor environment, the VLC technologie can be incorporated in the building of smart city to provide green and ubiquitous wireless connection [178]. Specifically, in a large scale outdoor domain, the LED street luminaries can be modified and networked to provide various and low-cost services (video broadcasting, stream media, real time voice, high precision positioning and so on) to the pedestrians and the grounding vehicles in moving or static status [179], [180]. On the other hand, B2B communications define all the communications technologies that enable connection between buildings. Both RF and OWC (including the visible light and the IR spectra) are used for this type of mission [181]. Therefore, VLC may be used to connect buildings situated within a reasonable distance from each other, such as campuses, bank buildings, and headquarters to provide access to information, data and media. In a duplex configuration, as shown in Fig 12, the information goes from building A to B and vice-versa. The return path, if needed, may use a different technology. Return path solutions are the Ethernet cable, power wires, RF or infra-red technologies. Nevertheless, it is worth emphasising that in this outdoor VLC application, laser diodes (LDs) adapt better than LEDs, owing to their high transmission range. In this case, the return path is just a different laser light emitted from the receiver side since they have very narrow beams [172].

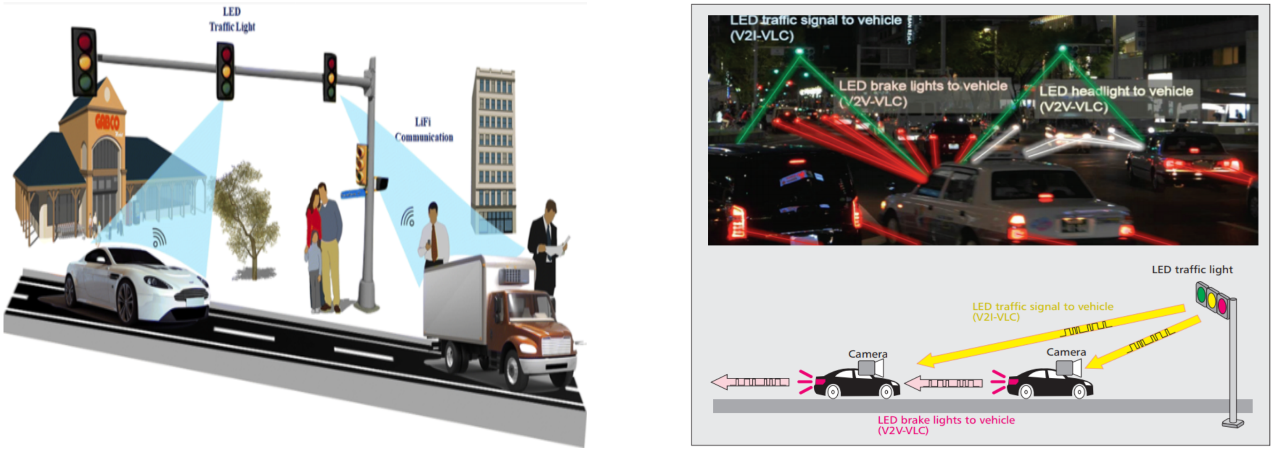
For outdoor applications of VLC, security issues arise naturally for VLC-based V2X communication, VLC-based P2I communication and VLC-based B2B communication. Specifically, for the case of V2X and P2I communications, vehicles and pedestrians commonly use RF, FSO or VLC wireless communication techniques for both communications. Manufacturers, regulators and the public are understandably concerned about large-scale systems failure or malicious attacks via these wireless networks. In the context of V2X communication, only a few papers have recently investigated the security problems in V2X communications. In [182], common V2X threats as well as security issues and security requirements of V2X in cellular network were reviewed, where the authors discussed existing V2X authentication solutions proposed in the literature. In [183], the authors presented an implementation and evaluation of the use of ultrasonic audio and image camera visual light side-channels for secure V2V communications. The constraints imposed by these side-channels necessitates the development of new schemes for small throughput, secure and attributable exchange of session key information between vehicles. Therefore, the authors used Blockchain as a V2V message transport, since it provides a secure, verifiable, shared, open and distributed ledger. In [184], the authors studied the secrecy performance of vehicular heterogeneous networks from a PLS point of view. In fact, the considered network model contains an ED, and the security problem was formulated using stochastic geometry. Finally, a secure cooperative communication scheme was proposed to enhance the secrecy performance of the system. Except [184], none of the works reported in the literature has studied the potential of PLS in providing secure V2X communications, for both RF and VLC wireless networks.

Based on the above, improving the security of VLC-based V2X communications, VLC-based P2I communications and VLC-based B2B communications from a PLS point of view can be considered as a potential future work. However, some fundamental features should be clearly defined and deeply investigated before performing security analysis. These features include:

- The framework and the network configuration, such as distances, dimensions, transmit light sources, optical receivers, etc.
- Realistic and measurement-based channel models should be derived. These channel models should encompass the effect of interference as there are fewer physical barriers in outdoor environments (unlike the indoor environment).
- The effect of sunlight during the day, outdoor illumination during the night, and weather conditions should be studied. It has been shown that solar irradiance does not prevent high speed VLC communication [185]. However, careful considerations and system design are required to minimize the effect of those sources of impairment on the performance of VLC systems.

VIII. CONCLUDING REMARKS AND LESSONS LEARNED

We provided in this paper a comprehensive and comparative review of all PLS techniques reported in the literature that aim


LED Traffic Light
LiFi Communication
LED traffic signal to vehicle (V2I-VLC)
LED brake lights to vehicle (V2V-VLC)
LED headlight to vehicle (V2V-VLC)
LED traffic light
LED traffic signal to vehicle (V2I-VLC)
Camera
Camera
LED brake lights to vehicle (V2V-VLC)

(a) VLC-based V2I and P2I communications [174].

(b) VLC-based V2I and V2V communications [175].

Fig. 11: VLC-based V2V, V2I and P2I communications for practical design of smart cities and intelligent transportation systems.

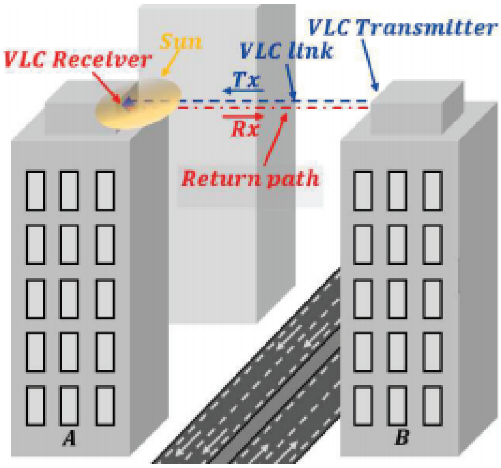


Fig. 12: VLC-based B2B communications. Building A exchanges data with building B [172].

to enhance the security of VLC systems. The reported techniques cover both information theoretic and signal processing aspects of VLC systems. Different types of VLC systems were considered, including SISO, MISO and MIMO VLC systems, as well as hybrid RF/VLC systems. In addition, we considered the impact of various VLC features on the secrecy performance, including the input signaling schemes, the geometry and parameters of the network, the number of legitimate receivers and eavesdroppers, and the CSI availability at the transmitting nodes. We have shown the potential of several PLS techniques in enhancing the secrecy performance of VLC systems. Such techniques may include the use of discrete input signaling, the use of artificial noise when the CSI of the EDs is not available as well as the use of relay and hybrid VLC/RF systems. We also listed a number of open research problems that have great potential for advancing the state-of-the-art of security for VLC systems.

Literally speaking, VLC is a technology that will boost the emergence of next generation wireless networks. However, this technology has some shortcomings that should be carefully investigated. Security is one of these shortcomings, which is due to the broadcast nature of VLC systems. We have shown in this survey that, using some metrics such as the secrecy rates, the secrecy performance of VLC system can be significantly improved in various and distinct scenarios through well designed PLS techniques. What has been accomplished so far in the totality of the research works on security for VLC systems, albeit being fundamental and original, it serves as a starting point for developing realistic PLS techniques tailored to real-world settings in an effort to bring the deployment of VLC-based systems (such as LiFi) closer than ever.

ACKNOWLEDGMENT

M. A. Arfaoui and C. Assi acknowledge the financial support from Concordia University and FQRNT. M. D. Soltani acknowledges the School of Engineering for providing financial support. A. Ghrayeb is supported in part by Qatar National Research Fund under NPRP Grant NPRP8-052-2-029 and in part by FQRNT. H. Haas acknowledges the financial support from the Wolfson Foundation and Royal Society. He also gratefully acknowledges financial support by the Engineering and Physical Sciences Research Council (EPSRC) under the Established Career Fellowship grants EP/R007101/1 and EP/S016570/1 ‘Terabit Bidirectional Multi-User Optical Wireless System (TOWS) for 6G LiFi’.

REFERENCES

[1] C. V. Networking, “Cisco global cloud index: Forecast and methodology, 2016–2021,” White Paper, Cisco, San Jose, CA, USA Nov. 2019.
[2] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, “What will 5G be?” *IEEE J. on selected areas in commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.
[3] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, “5G: A tutorial overview of standards, trials, challenges, deployment, and practice,” *IEEE J. on selected areas in commun.*, vol. 35, no. 6, pp. 1201–1221, Apr. 2017.
[4] P. Pirinen, “A brief overview of 5G research activities,” in *Proc. IEEE 5GU*, Akaslompolo, Finland, Nov. 2014.
[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, Jun. 2015.

[6] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE J. on selected areas in commun.*, vol. 34, no. 3, pp. 510–527, Feb. 2016.

[7] D. Tsonev, S. Videv, and H. Haas, "Towards a 100 Gb/s visible light wireless access network," *Optics express*, vol. 23, no. 2, pp. 1627–1637, Jan. 2015.

[8] N. Bhushan, J. Li, D. Malladi, R. Gilmore, D. Brenner, A. Damnjanovic, R. Sukhavasi, C. Patel, and S. Geirhofer, "Network densification: the dominant theme for wireless evolution into 5G," *IEEE Commun. Magazine*, vol. 52, no. 2, pp. 82–89, Feb. 2014.

[9] X. Ge, S. Tu, G. Mao, C.-X. Wang, and T. Han, "5G ultra-dense cellular networks," *IEEE Wireless Commun.*, vol. 23, no. 1, pp. 72–79, Mar. 2016.

[10] A. R. Ndjiongue, H. C. Ferreira, and T. Ngatched, "Visible light communications (VLC) technology," *Wiley Encyclopedia of Electrical and Electronics Engineering*, Jun. 2015.

[11] S. Rajagopal, R. D. Roberts, and S.-K. Lim, "IEEE 802.15. 7 visible light communication: modulation schemes and dimming support," *IEEE Commun Mag.*, vol. 50, no. 3, pp. 72–82, Mar. 2012.

[12] A. Jovicic, J. Li, and T. Richardson, "Visible light communication: Opportunities, challenges and the path to market," *IEEE Commun. Magazine*, vol. 51, no. 12, pp. 26–32, Dec. 2013.

[13] Y. Tanaka, S. Haruyama, and M. Nakagawa, "Wireless optical transmissions with white colored LED for wireless home links," in *Proc. IEEE PIMRC*, vol. 2, London, UK, Sep. 2000.

[14] T. Kishi, H. Tanaka, Y. Umeda, and O. Takyu, "A high-speed LED driver that sweeps out the remaining carriers for visible light communications," *J. of Lightwave Technology*, vol. 32, no. 2, pp. 239–249, Jan. 2014.

[15] A. B. Siddique and M. Tahir, "Joint rate-brightness control using variable rate MPPM for LED based visible light communication systems," *IEEE Trans. on Wireless Commun.*, vol. 12, no. 9, pp. 4604–4611, Aug. 2013.

[16] L. Zeng, D. C. O'Brien, H. Le Minh, G. E. Faulkner, K. Lee, D. Jung, Y. Oh, and E. T. Won, "High data rate multiple input multiple output (MIMO) optical wireless communications using white LED lighting," *IEEE J. Select. Areas in Commun.*, vol. 27, no. 9, pp. 1654 – 1662, Dec. 2009.

[17] T.-C. Lin, Y.-T. Chen, Y.-F. Yin, Z.-X. You, H.-Y. Kao, C.-Y. Huang, Y.-H. Lin, C.-T. Tsai, G.-R. Lin, and J.-J. Huang, "Large-signal modulation performance of light-emitting diodes with photonic crystals for visible light communication," *IEEE Trans. on Electron Devices*, no. 99, pp. 1–6, Aug. 2018.

[18] X. Huang, J. A. Zhang, R. P. Liu, Y. J. Guo, and L. Hanzo, "Airplane-Aided Integrated Networking for 6G Wireless: Will It Work?" *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 84–91, Jul. 2019.

[19] S. K. Rao, "Advanced antenna technologies for satellite communications payloads," *IEEE Trans. on Antennas and Propagation*, vol. 63, no. 4, pp. 1205–1217, Apr. 2015.

[20] R. Perez-Jimenez, J. Rufo, C. Quintana, J. Rabadan, and F. Lopez-Hernandez, "Visible light communication systems for passenger in-flight data networking," in *Proc. IEEE ICCE*, Las Vegas, NV, USA, Jan. 2011.

[21] M. Sui, Z. Xia, W. Zhu, J. Shen, and J. Chen, "A visible light communication based aircraft cabin wireless network demo system," in *Proc. Asia Communications and Photonics Conference*. Hong Kong: Optical Society of America, Nov. 2015.

[22] M. Z. Chowdhury, M. T. Hossan, A. Islam, and Y. M. Jang, "A comparative survey of optical wireless technologies: architectures and applications," *IEEE Access*, vol. 6, pp. 9819–9840, Jan. 2018.

[23] H. Elgala, R. Mesleh, and H. Haas, "Indoor optical wireless communication: potential and state-of-the-art," *IEEE Commun. Mag.*, vol. 49, no. 9, pp. 56–62, Sep. 2011.

[24] H. Elgala, R. Mesleh, and H. Haas, "Indoor broadcasting via white LEDs and OFDM," *IEEE Trans. on consumer electronics*, vol. 55, no. 3, pp. 1127–1134, Oct. 2009.

[25] N. Kumar and N. R. Lourenco, "Led-based visible light communication system: a brief survey and investigation," *J. Eng. Appl. Sci*, vol. 5, no. 4, pp. 296–307, 2010.

[26] A. Sevincer, A. Bhattarai, M. Bilgi, M. Yuksel, and N. Pala, "Lightnets: Smart lighting and mobile optical wireless networks—a survey," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 4, pp. 1620–1641, Apr. 2013.

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

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

[29] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, "Visible light communication, networking, and sensing: A survey, potential and challenges," *IEEE Commun. Surveys & tutorials*, vol. 17, no. 4, pp. 2047–2077, Sep. 2015.

[30] Y. Qiu, H.-H. Chen, and W.-X. Meng, "Channel modeling for visible light communications—a survey," *Wireless Communications and Mobile Computing*, vol. 16, no. 14, pp. 2016–2034, Feb. 2016.

[31] K. Sindhubala and B. Vijayalakshmi, "Survey on noise sources and restrain techniques in visible-light communication." *Light & Engineering*, vol. 24, no. 2, Apr. 2016.

[32] X. Li, R. Zhang, and L. Hanzo, "Optimization of visible-light optical wireless systems: Network-centric versus user-centric designs," *IEEE Commun. Surveys & Tutorials*, Mar. 2018.

[33] Y. Zhuang, L. Hua, L. Qi, J. Yang, P. Cao, Y. Cao, Y. Wu, J. Thompson, and H. Haas, "A survey of positioning systems using visible LED lights," *IEEE Commun. Surveys & Tutorials*, vol. 20, no. 3, pp. 1963–1988, Feb. 2018.

[34] M. Obeed, A. M. Salhab, M.-S. Alouini, and S. A. Zummo, "On optimizing VLC networks for downlink multi-user transmission: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2947 – 2976, Mar. 2019.

[35] Y. Liang, H. V. Poor *et al.*, "Physical layer security in broadcast networks," *Security and Commun. Net.*, vol. 2, no. 3, pp. 227–238, May 2009.

[36] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The spy next door: Eavesdropping on high throughput visible light communications," in *Proc. ACM*, Paris, France, Sep. 2015.

[37] A. Yener and S. Ulukus, "Wireless physical-layer security: lessons learned from information theory," *Proc. of the IEEE*, vol. 103, no. 10, pp. 1814–1825, Sep. 2015.

[38] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Magazine*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[39] T. Bilski, "New threats and innovative protection methods in wireless transmission systems," *J. of Telecommun. and Inform. Technology*, vol. 3, pp. 26–33, Mar. 2014.

[40] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[41] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 1, pp. 283–302, Apr. 2014.

[42] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, Feb. 2014.

[43] M. Atallah, G. Kaddoum, and L. Kong, "A survey on cooperative jamming applied to physical layer security," in *Proc. IEEE ICUWB*, Montreal, QC, Canada, Oct. 2015.

[44] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, Nov. 2016.

[45] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, Aug. 2016.

[46] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, Nov. 2018.

[47] H. Elgala, R. Mesleh, and H. Haas, "An LED model for intensity-modulated optical communication systems," *IEEE Photonics Tech. Letters*, vol. 22, no. 11, pp. 835–837, Apr. 2010.

[48] S. D. Dissanayake and J. Armstrong, "Comparison of ACO-OFDM, DCO-OFDM and ADO-OFDM in IM/DD systems," *J. of lightwave techn.*, vol. 31, no. 7, pp. 1063–1072, Apr. 2013.

[49] M. Obeed, A. M. Salhab, M.-S. Alouini, and S. A. Zummo, "Survey on physical layer security in optical wireless communication systems," in *Proc. IEEE ComNet*, Hammamet, Tunisia, Nov. 2018.

[50] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," *Softw. Eng. Group, School Comput. Sci. Math., Keele Univ., Keele, U.K., and Dept. Comput. Sci., Univ. Durham, Durham, U.K*, Jul. 2007.

[51] IEEE Xplore Digital Library, [Online]. Available: http://ieeexplore.ieee.org/, Accessed: Jan. 2019.

[52] Elsevier Science Direct, [Online]. Available: https://www.sciencedirect.com/, Accessed: Jan. 2019.

[53] Wiley Online Library, [Online]. Available: https://onlinelibrary.wiley.com/, Accessed: Jan. 2019.

[54] ACM Digital Library, [Online]. Available: http://dl.acm.org/, Accessed: Jan. 2019.

[55] M. D. Soltani, X. Wu, M. Safari, and H. Haas, "On limited feedback resource allocation for visible light communication networks," in *Proc. Mobicom*, Paris, France, Sep. 2015.

[56] M. D. Soltani, M. Safari, and H. Haas, "On throughput maximization based on optimal update interval in Li-Fi networks," in *Proc. IEEE PIMRC*, Montréal, QC, Canada, Oct. 2017.

[57] M. D. Soltani, X. Wu, M. Safari, and H. Haas, "Bidirectional user throughput maximization based on feedback reduction in LiFi networks," *IEEE Trans. on Commun.*, vol. 66, no. 7, pp. 3172–3186, Feb. 2018.

[58] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5515 – 5532, Oct. 2010.

[59] A. Mostafa and L. Lampe, "Physical-layer security for MISO visible light communication channels," *IEEE J. on Selected Areas in Commun.*, vol. 33, no. 9, pp. 1806–1818, May 2015.

[60] A. Mostafa and L. Lampe, "Optimal and robust beamforming for secure transmission in MISO visible-light communication links," *IEEE Trans. Signal Process.*, vol. 64, no. 24, pp. 6501–6516, Aug. 2016.

[61] M.-A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the input distribution and optimal beamforming for the MISO VLC wiretap channel," in *Proc. IEEE GlobalSIP*, Washington DC, USA, Dec. 2016.

[62] L. Xiao, G. Sheng, S. Liu, H. Dai, M. Peng, and J. Song, "Deep reinforcement learning enabled secure visible light communication against eavesdropping," *IEEE Transactions on Communications*, 2019.

[63] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," in *Proc. IEEE Globecom*, Austin, TX, USA, Dec. 2014.

[64] H. Zaid, Z. Rezki, A. Chaaban, and M. S. Alouini, "Improved achievable secrecy rate of visible light communication with cooperative jamming," in *Proc. IEEE GlobalSIP*, Orlando, FL, USA, Dec. 2015.

[65] D. Tian, W. Zhang, J. Sun, and C.-X. Wang, "Physical-layer security of visible light communications with jamming," in *Proc. IEEE ICCC*, Changchun, China,, Aug. 2019.

[66] S. Cho, G. Chen, and J. P. Coon, "Securing visible light communications with spatial jamming," in *Proc. IEEE ICC*, Shanghai, China, May. 2019.

[67] S. Cho, G. Chen, and J. P. Coon, "Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems," *IEEE Trans. on Information Forensics and Security*, vol. 14, no. 10, pp. 2633 – 2648, Mar. 2019.

[68] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Proc. IEEE ICC*, Sydney, Australia, Jun. 2014.

[69] M.-A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the secrecy capacity of MISO visible light communication channels," in *Proc. IEEE Globecom*, Washington DC, USA, Dec. 2016.

[70] M.-A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "Discrete input signaling for MISO visible light communication channels," in *Proc. IEEE WCNC*, San Francisco, CA, USA, Mar. 2017.

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

[72] M. A. Arfaoui, H. Zaid, Z. Rezki, A. Ghrayeb, A. Chaaban, and M.-S. Alouini, "Artificial Noise-Based Beamforming for the MISO VLC Wiretap Channel," *IEEE Trans. on Commun.*, vol. 67, no. 4, pp. 2866–2879, Dec. 2018.

[73] F. Wang, C. Liu, Q. Wang, J. Zhang, R. Zhang, L.-L. Yang, and L. Hanzo, "Optical jamming enhances the secrecy performance of the generalized space shift keying aided visible light downlink," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 4087–4102, Apr. 2018.

[74] F. Wang, C. Liu, Q. Wang, J. Zhang, R. Zhang, L. L. Yang, and L. Hanzo, "Secrecy analysis of generalized space-shift keying aided visible light communication," *IEEE Access*, vol. 6, p. 18, Jan. 2018.

[75] H. Li, F. Wang, J. Zhang, and C. Liu, "Secrecy performance analysis of miso visible light communication systems with spatial modulation," *Digital Signal Processing*, vol. 81, pp. 116–128, 2018.

[76] S. Cho, G. Chen, and J. P. Coon, "Secrecy analysis in visible light communication systems with randomly located eavesdroppers," in *Proc. IEEE ICC*, Paris, France, May. 2017.

[77] S. Cho, G. Chen, and J. P. Coon, "Securing visible light communication systems by beamforming in the presence of randomly distributed eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 2918–2931, Feb. 2018.

[78] M.-A. Arfaoui, A. Ghrayeb, and C. Assi, "Enhancing the secrecy performance of Gaussian MISO VLC wiretap channels with randomly located eavesdroppers," in *Proc. IEEE ICC*, Kansas City, MO, USA, May. 2018.

[79] C.-W. Chow, Y. Liu, C.-H. Yeh, C.-Y. Chen, C.-N. Lin, and D.-Z. Hsu, "Secure communication zone for white-light LED visible light communication," *Optics Communications*, vol. 344, pp. 81–85, Jun. 2015.

[80] M.-A. Arfaoui, A. Ghrayeb, and C. Assi, "Discrete input signaling for secure MISO VLC systems with randomly located eavesdroppers," in *Proc. IEEE PIMRC*, Bologna, Italy, Sep. 2018.

[81] J.-Y. Wang, C. Liu, J.-B. Wanga, Y. Wu, M. Lin, and J. Cheng, "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," *IEEE Trans. on Commun.*, vol. 66, no. 12, pp. 6423–6436, Jul. 2018.

[82] 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 ICC*, Kansas City, MO, USA, May. 2018.

[83] 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. Letters*, vol. 22, no. 7, pp. 1382 – 1385, Apr. 2018.

[84] 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 WCNC*, Barcelona, Spain, Apr. 2018.

[85] S. Cho, G. Chen, and J. P. Coon, "Physical layer security in visible light communication systems with randomly located colluding eavesdroppers," *IEEE Wireless Commun. Letters*, vol. 7, no. 5, pp. 768 – 771, Oct. 2018.

[86] A. Arafa, E. Panayirci, and H. V. Poor, "Relay-Aided Secure Broadcasting for VLC," in *Proc. IEEE GlobalSIP*, Anaheim, CA, USA, Nov. 2018.

[87] A. Arafa, E. Panayirci, and H. V. Poor, "Relay-aided secure broadcasting for visible light communications," *IEEE Trans. on Commun.*, vol. 67, no. 6, pp. 4227 – 4239, Feb. 2019.

[88] G. Pan, J. Ye, and Z. Ding, "On secure VLC systems with spatially random terminals," *IEEE Commun. Letters*, vol. 21, no. 3, pp. 492–495, Dec. 2017.

[89] X. Zhao, H. Chen, and J. Sun, "On physical-layer security in multiuser visible light communication systems with non-orthogonal multiple access," *IEEE Access*, vol. 6, pp. 34 004–34 017, Jun. 2018.

[90] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights," *IEEE trans. on Consumer Elect.*, vol. 50, no. 1, pp. 100–107, Jun. 2004.

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

[92] F. R. Gfeller and U. Bapst, "Wireless in-house data communication via diffuse infrared radiation," *Proc. of the IEEE*, vol. 67, no. 11, pp. 1474–1486, Nov. 1979.

[93] R. Mesleh, H. Elgala, and H. Haas, "LED nonlinearity mitigation techniques in optical wireless OFDM communication systems," *J. of Optical Commun. and Networking*, vol. 4, no. 11, pp. 865–875, Nov. 2012.

[94] H. Elgala, R. Mesleh, and H. Haas, "A study of LED non linearity effects on optical wireless transmission using OFDM," in *Proc. IEEE IFIP*, Cairo, Egypt, May. 2009.

[95] I. Neokosmidis, T. Kamalakis, J. W. Walewski, B. Inan, and T. Sphicopoulos, "Impact of nonlinear LED transfer function on discrete multitone modulation: Analytical approach," *J. of Lightwave tech.*, vol. 27, no. 22, pp. 4970–4978, Jul. 2009.

[96] B. Li, J. Wang, R. Zhang, H. Shen, C. Zhao, and L. Hanzo, "Multiuser MISO transceiver design for indoor downlink visible light communication under per-LED optical power constraints," *IEEE Photonics Journal*, vol. 7, no. 4, pp. 1–15, Jun. 2015.

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

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

[99] S. R. Aghdam, A. Nooraiepour, and T. M. Duman, “An overview of physical layer security with finite-alphabet signaling,” *IEEE Communications Surveys & Tutorials*, Early Access 2018.

[100] A. Dytso, M. Goldenbaum, H. V. Poor *et al.*, “Amplitude Constrained MIMO Channels: Properties of Optimal Input Distributions and Bounds on the Capacity,” *Entropy*, vol. 21, no. 2, p. 200, Feb. 2019.

[101] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, “A survey on MIMO transmission with finite input signals: Technical challenges, advances, and future trends,” *Proc. of the IEEE*, no. 99, pp. 1–55, Jul. 2018.

[102] M.-A. Arfaoui, A. Ghrayeb, and C. Assi, “On the Achievable Secrecy Rate of the MIMO VLC Gaussian Wiretap Channel,” in *Proc. IEEE PIMRC*, Montreal, Qc, Canada, Oct. 2016.

[103] M. A. Arfaoui, A. Ghrayeb, and C. M. Assi, “Secrecy Performance of the MIMO VLC Wiretap Channel with Randomly Located Eavesdropper,” *IEEE Trans. on Wireless Commun.*, vol. 19, no. 1, pp. 265–278, Jan. 2020.

[104] H. Le Minh, A. T. Pham, Z. Ghassemlooy, and A. Burton, “Secured communications-zone multiple input multiple output visible light communications,” in *Proc. IEEE Globecom*, Austin, TX, USA, Dec. 2018.

[105] Z. Chen and H. Haas, “Physical layer security for optical attocell networks,” in *Proc. IEEE ICC*, Paris, France, May. 2017.

[106] T. M. Cover and J. A. Thomas, *Elements of Information Theory 2nd Edition*. Wiley-Interscience, 2006.

[107] S. Loyka and C. D. Charalambous, “Optimal signaling for secure communications over Gaussian MIMO wiretap channels,” *IEEE Trans. on Inform. Theory*, vol. 62, no. 12, pp. 7207–7215, Oct. 2016.

[108] Z. Rezki and M.-S. Alouini, “Secret-key agreement with public discussion over multi-antenna aransmitters with amplitude constraints,” in *Proc. IEEE ISIT*, Aachen, Germany, Aug. 2017.

[109] P. C. Pinto, J. Barros, and M. Z. Win, “Wireless physical-layer security: The case of colluding eavesdroppers,” in *Proc. IEEE ISIT*, Seoul, South Korea, Jul. 2009.

[110] M. Haenggi, “The secrecy graph and some of its properties,” in *Proc. IEEE ISIT*, Toronto, ON, Canada, Aug. 2008.

[111] P. C. Pinto, J. Barros, and M. Z. Win, “Physical-layer security in stochastic wireless networks,” in *Proc. IEEE ISIT*, Guangzhou, China, Nov. 2008.

[112] F. Baccelli, B. Błaszczyszyn *et al.*, “Stochastic geometry and wireless networks: Volume II Applications,” *Foundations and Trends® in Networking*, vol. 4, no. 1–2, pp. 1–312, Jan. 2010.

[113] M. Haenggi, *Stochastic geometry for wireless networks*. Cambridge University Press, Nov. 2012.

[114] A. Mostafa and L. Lampe, “On linear precoding for the two-user MISO broadcast channel with confidential messages and per-antenna constraints,” *IEEE Trans. Signal Process.*, vol. 65, no. 22, pp. 6053–6068, Aug. 2017.

[115] T. V. Pham and A. T. Pham, “Max-min fairness and sum-rate maximization of mu-vlc local networks,” in *Proc. IEEE Globecom*, San Diego, CA, USA, Dec. 2015.

[116] T. Pham, H. Le Minh, and A. Pham, “Multi-user visible light communication broadcast channels with zero-forcing precoding,” *IEEE Trans. Commun.*, vol. 65, no. 6, pp. 2509 – 2521, Apr. 2017.

[117] M.-A. Arfaoui, A. Ghrayeb, and C. Assi, “Achievable secrecy sum-rate of the MISO VLC broadcast channel with confidential messages,” in *Proc. IEEE Globecom*, Singapore, Dec. 2016.

[118] M. A. Arfaoui, A. Ghrayeb, and C. M. Assi, “Secrecy Performance of Multi-User MISO VLC Broadcast Channels With Confidential Messages,” *IEEE Trans. on Wireless Commun.*, vol. 17, no. 11, pp. 7789–7800, Sep. 2018.

[119] T. V. Pham and A. T. Pham, “On the secrecy sum-rate of MU-VLC broadcast systems with confidential messages,” in *Proc. IEEE CSNDSP 2016*, Prague, Czech Republic, Jul. 2016.

[120] T. V. Pham and A. T. Pham, “Secrecy sum-rate of multi-user MISO visible light communication systems with confidential messages,” *Optik-International J. for Light and Electron Optics*, vol. 151, pp. 65–76, Dec. 2017.

[121] T. V. Pham, T. Hayashi, and A. T. Pham, “Artificial-noise-aided precoding design for multi-user visible light communication channels,” in *Proc. IEEE ICC*, Kansas City, MO, USA, May. 2018.

[122] T. V. Pham, T. Hayashi, and A. T. Pham, “Artificial-noise-aided precoding design for multi-user visible light communication channels,” *IEEE Access*, vol. 7, pp. 3767–3777, Dec. 2018.

[123] L. Yin and H. Haas, “Physical-layer security in multiuser visible light communication networks,” *IEEE J. on Selected Areas in Commun.*, vol. 36, no. 1, pp. 162–174, Jan. 2018.

[124] Z.-Q. Luo and S. Zhang, “Dynamic spectrum management: Complexity and duality,” *IEEE J. of Selected Topics in Signal Process.*, vol. 2, no. 1, pp. 57–73, Feb. 2008.

[125] O. Ozel, E. Ekrem, and S. Ulukus, “Gaussian wiretap channel with amplitude and variance constraints,” *IEEE Trans. Inform. Theory*, vol. 61, no. 10, pp. 5553 – 5563, Jul. 2015.

[126] X. Zhao and J. Sun, “On Secrecy Performance of the Strong User in MISO-NOMA Visible Light Communication System,” *Electronics*, vol. 8, no. 4, p. 462, Apr. 2019.

[127] M. Safari and M. Uysal, “Relay-assisted free-space optical communication,” *IEEE Trans. on Wireless Commun.*, vol. 7, no. 12, pp. 5441–5449, Dec. 2008.

[128] F. E. Alsaadi, M. Nikkar, and J. M. Elmirghani, “Adaptive mobile optical wireless systems employing a beam clustering method, diversity detection, and relay nodes,” *IEEE Trans. on Commun.*, vol. 58, no. 3, pp. 869–879, Mar. 2010.

[129] H. Yang and A. Pandharipande, “Full-duplex relay VLC in LED lighting triangular system topology,” in *Proc. IEEE ISCCSP*. Athens, Greece: IEEE, 2014.

[130] A. T. Hussein and J. M. Elmirghani, “10 Gbps mobile visible light communication system employing angle diversity, imaging receivers, and relay nodes,” *J. of Optical Commun. and Networking*, vol. 7, no. 8, pp. 718–735, Aug. 2015.

[131] M. B. Rahaim, A. M. Vegni, and T. D. Little, “A hybrid radio frequency and broadcast visible light communication system,” in *Proc. IEEE Globecom*, Houston, TX, USA, Dec. 2011.

[132] F. Wang, Z. Wang, C. Qian, L. Dai, and Z. Yang, “Efficient vertical handover scheme for heterogeneous VLC-RF systems,” *J. of Optical Commun. and Networking*, vol. 7, no. 12, pp. 1172–1180, Dec. 2015.

[133] A. A. Purwita, M. D. Soltani, M. Safari, and H. Haas, “Handover Probability of Hybrid LiFi/RF-Based Networks with Randomly-Oriented Devices,” in *Proc. IEEE VTC*, Porto, Portugal, July. 2018.

[134] M. F. Marzban, M. Kashef, M. Abdallah, and M. Khairy, “Beamforming and power allocation for physical-layer security in hybrid RF/VLC wireless networks,” in *Proc. IEEE IWCMC*, Valencia, Spain, Jun. 2017.

[135] G. Pan, J. Ye, and Z. Ding, “Secure hybrid VLC-RF systems with light energy harvesting,” *IEEE Trans. on Commun.*, vol. 65, no. 10, pp. 4348–4359, May. 2017.

[136] G. Pan, J. Ye, and Z. Ding, “Secrecy outage analysis of hybrid VLC-RF systems with light energy harvesting,” in *Proc. IEEE SPAWC*, Sapporo, Japan, Jul. 2017.

[137] Z. Liao, L. Yang, J. Chen, H.-C. Yang, and M.-S. Alouini, “Physical Layer Security For Dual-Hop VLC/RF Communication Systems,” *IEEE Commun. Letters*, vol. 22, no. 12, pp. 2603–2606, Oct. 2018.

[138] J. Al-Khori, G. Nauryzbayev, M. M. Abdallah, and M. Hamdi, “Secrecy Performance of Decode-and-Forward Based Hybrid RF/VLC Relaying Systems,” *IEEE Access*, vol. 7, pp. 10 844–10 856, Jan. 2019.

[139] M. D. Renzo, H. Haas, A. Ghrayeb, S. Sugiura, and L. Hanzo, “Spatial modulation for generalized MIMO: challenges, opportunities and implementation,” *Proc. of the IEEE*, vol. 102, no. 1, pp. 56–103, Jan. 2014.

[140] M. Di Renzo, H. Haas, and P. Grant, “Spatial modulation for multiple-antenna wireless systems: A survey,” *IEEE Commun. Magazine*, vol. 49, no. 12, pp. 182–191, Jan. 2012.

[141] N. I. Miridakis and D. D. Vergados, “A survey on the successive interference cancellation performance for single-antenna and multiple-antenna OFDM systems,” *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 1, pp. 312–335, Apr. 2012.

[142] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, “A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends,” *IEEE J. on Selected Areas in Commun.*, vol. 35, no. 10, pp. 2181–2195, Jul. 2017.

[143] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, “A survey of non-orthogonal multiple access for 5G,” *IEEE Commun. Surveys & Tutorials*, vol. 20, no. 3, pp. 2294–2323, May. 2018.

[144] M. Soltani and Z. Rezki, “The capacity of the optical broadcast channel with peak and average intensity constraints,” in *Proc. IEEE ISIT*, Vail, CO, USA, Jun. 2018.

[145] J. Yang, I.-M. Kim, and D. I. Kim, “Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers,” *IEEE Trans. on Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, Apr. 2013.

[146] A. Mukherjee and A. L. Swindlehurst, “User selection in multiuser MIMO systems with secrecy considerations,” in *Proc. IEEE Asolimar*, Pacific Grove, CA, USA, Nov. 2009.

[147] F. Miramirkhani, O. Narmanlioglu, M. Uysal, and E. Panayirci, “A mobile channel model for VLC and application to adaptive system

design," *IEEE Commun. Letters*, vol. 21, no. 5, pp. 1035–1038, Jan. 2017.

[148] F. Miramirkhani and M. Uysal, "Channel modeling and characterization for visible light communications," *IEEE Photonics J.*, vol. 7, no. 6, pp. 1–16, Nov. 2015.

[149] A. A. Purwita, M. D. Soltani, M. Safari, and H. Haas, "Impact of terminal orientation on performance in LiFi systems," in *Proc. IEEE WCNC*, Barcelona, Spain, Apr. 2018.

[150] Z. Zeng, M. D. Soltani, H. Haas, and M. Safari, "Orientation Model of Mobile Device for Indoor VLC and Millimetre Wave Systems," in *Proc. IEEE VTC*, Chicago, USA, Aug. 2018.

[151] 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, 2019.

[152] M. D. Soltani, M. A. Arfaoui, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. M. Assi, M. O. Hasna, and H. Haas, "Bidirectional Optical Spatial Modulation for Mobile Users: Toward a Practical Design for LiFi Systems," *IEEE J. on Selected Areas in Commun.*, vol. 37, no. 9, pp. 2069–2086, Aug. 2019.

[153] A. A. Purwita, M. D. Soltani, M. Safari, and H. Haas, "Terminal orientation in OFDM-based LiFi systems," *IEEE Trans. on Wireless Commun.*, vol. 18, no. 8, pp. 4003–4016, Jun. 2019.

[154] M. Elamassie, M. Karbalayghareh, F. Miramirkhani, R. C. Kizilirmak, and M. Uysal, "Effect of fog and rain on the performance of vehicular visible light communications," in *Proc. IEEE VTC*, Porto, Portugal, Jul. 2018.

[155] M. Elamassie, F. Miramirkhani, and M. Uysal, "Performance characterization of underwater visible light communication," *IEEE Trans. on Commun.*, vol. 67, no. 1, pp. 543–552, Aug. 2018.

[156] F. Miramirkhani and M. Uysal, "Visible light communication channel modeling for underwater environments with blocking and shadowing," *IEEE Access*, vol. 6, pp. 1082–1090, Nov. 2017.

[157] M. D. Soltani, Z. Zeng, I. Tavakkolnia, H. Haas, and M. Safari, "Random Receiver Orientation Effect on Channel Gain in LiFi Systems," in *Proc. IEEE WCNC*, Marrakech, Morocco, Apr. 2019.

[158] 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. 41 690–41 701, 2019.

[159] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Trans. on mobile computing*, no. 3, pp. 257–269, Sep. 2003.

[160] E. Hyytiä and J. Virtamo, "Random waypoint model in n-dimensional space," *Operations Research Letters*, vol. 33, no. 6, pp. 567–571, Nov. 2005.

[161] E. Hyytia, P. Lassila, and J. Virtamo, "Spatial node distribution of the random waypoint mobility model with applications," *IEEE Trans. on mobile computing*, vol. 5, no. 6, pp. 680–694, Apr. 2006.

[162] T. Ali and M. Saquib, "Performance evaluation of WLAN/cellular media access for mobile voice users under random mobility models," *IEEE Trans. on Wireless Commun.*, vol. 10, no. 10, pp. 3241–3255, Aug. 2011.

[163] M. D. Soltani, H. Kazemi, M. Safari, and H. Haas, "Handover Modeling for Indoor Li-Fi Cellular Networks: The Effects of Receiver Mobility and Rotation," in *Proc. IEEE WCNC*, San Fransisco, USA, Mar. 2017.

[164] A. Gupta and P. Garg, "Statistics of SNR for an indoor VLC system and its applications in system performance," *IEEE Commun. Letters*, vol. 22, no. 9, pp. 1898 – 1901, Jul. 2018.

[165] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, C. Assi, H. Haas, M. Hasna, and M. Safari, "SNR Statistics for Indoor VLC Mobile Users with Random Orientation," in *Proc. IEEE ICC*, Shanghai, China, May. 2019.

[166] M. A. Arfaoui, A. Ghrayeb, and C. Assi, "Effect of Mobility on the Secrecy Performance of NOMA SISO-VLC Wiretap Systems," in *Proc. IEEE ISIT*, Paris, France, Jul. 2019.

[167] K. Dong, X. Liao, and S. Zhu, "Link blockage analysis for indoor 60ghz radio systems," *Electronics Letters*, vol. 48, no. 23, pp. 1506–1508, November 2012.

[168] T. B. Hoang, S. Kandukuri, S. Sahuguede, and A. Julien-Vergonjanne, "Infrared mobile transmissions for smart indoor applications," in *Proc. IEEE CSNDSP*, Budapest, Hungary, Jul. 2018.

[169] I. Tavakkolnia, M. D. Soltani, M. A. Arfaoui, , A. Ghrayeb, C. Assi, M. Safari, and H. Haas, "MIMO System with Multi-directional Receiver in Optical Wireless Communications," in *Proc. IEEE ICC*, Shanghai, China, May. 2019.

[170] C. Chen, M. D. Soltani, M. Safari, A. A. Purwita, X. Wu, and H. Haas, "An Omnidirectional User Equipment Configuration to Support Mobility in LiFi Networks," in *Proc. IEEE ICC*, Shanghai, China, May. 2019.

[171] A.-M. Căilean and M. Dimian, "Current challenges for visible light communications usage in vehicle applications: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 4, pp. 2681–2703, May. 2017.

[172] A. Ndjiongue and H. C. Ferreira, "An overview of outdoor visible light communications," *Trans. on Emerging Telecommunications Technologies*, vol. 29, no. 7, pp. 1–15, Jul. 2018.

[173] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A Survey of Vehicle to Everything (V2X) Testing," *Sensors*, vol. 19, no. 2, p. 334, Jan. 2019.

[174] P. K. Sharma, J. H. Ryu, K. Y. Park, J. H. Park, and J. H. Park, "Li-Fi based on security cloud framework for future IT environment," *Human-centric Computing and Information Sciences*, vol. 8, no. 1, p. 23, Aug. 2018.

[175] T. Yamazato, I. Takai, H. Okada, T. Fujii, T. Yendo, S. Arai, M. Andoh, T. Harada, K. Yasutomi, K. Kagawa *et al.*, "Image-sensor-based visible light communication for automotive applications," *IEEE Commun. Magazine*, vol. 52, no. 7, pp. 88–97, Jul. 2014.

[176] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, and L. Zhao, "Vehicle-to-everything (v2x) services supported by LTE-based systems and 5G," *IEEE Commun. Standards Magazine*, vol. 1, no. 2, pp. 70–76, Jul. 2017.

[177] 5GAA, "An assessment of LTE-V2X (PC5) and 802.11p direct communications technologies for improved road safety in the EU," [Online]. Available: http://5gaa.org/wp-content/uploads/2017/12/5GAA-Road-safety-FINAL2017-12-05.pdf, Dec. 2017.

[178] I. Yaqoob, I. A. T. Hashem, Y. Mehmood, A. Gani, S. Mokhtar, and S. Guizani, "Enabling communication technologies for smart cities," *IEEE Commun. Magazine*, vol. 55, no. 1, pp. 112–120, Jan. 2017.

[179] T. H. Do and M. Yoo, "Visible light communication based vehicle positioning using LED street light and rolling shutter CMOS sensors," *Optics Commun.*, vol. 407, pp. 112–126, Jan. 2018.

[180] N. Zhu, Z. Xu, Y. Wang, H. Zhuge, and J. Li, "Handover method in visible light communication between the moving vehicle and multiple LED streetlights," *Inter. J. for Light and Electron Optics*, vol. 125, no. 14, pp. 3540–3544, Jul. 2014.

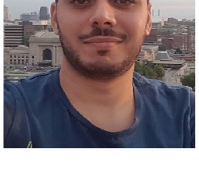
[181] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Commun. Surveys & tutorials*, vol. 16, no. 4, pp. 2231–2258, Jun. 2014.

[182] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Vehicular Communications*, Apr. 2018.

[183] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. M. Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," [Online]. Available: https://arxiv.org/abs/1704.02553, Apr. 2017.

[184] L. Wang and X. Liu, "Secure cooperative communication scheme for vehicular heterogeneous networks," *Vehicular Communications*, vol. 11, pp. 46–56, Jan. 2018.

[185] M. S. Islim, S. Videv, M. Safari, E. Xie, J. J. McKendry, E. Gu, M. D. Dawson, and H. Haas, "The impact of solar irradiance on visible light communications," *J. of Lightwave Technology*, vol. 36, no. 12, pp. 2376–2386, Jun. 2018.



Mohamed Amine Arfaoui (S'16) received the B.E. degree in electrical and computer engineering from the École Polytechnique de Tunisie, Tunisia, in 2015, and the M.Sc. degree in information systems engineering from Concordia University, Montreal, QC, Canada, in 2017. He is currently pursuing the Ph.D. degree in information systems engineering with Concordia University, Montreal. His research interests include communication theory, optical communications and physical layer security.

Mohammad Dehghani Soltani (S'15) 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, UK, in 2019. During his MSc, 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 PhD was funded by the British Engineering and Physical Sciences Research Council (EPSRC) Project TOUCAN. During his PhD, 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 at the University of Edinburgh, funded by EPSRC 'Terabit Bidirectional Multi-User Optical Wireless System (TOWS) for 6G LiFi'.

Iman Tavakkolnia (S'15, M'19) received the B.Sc. degree in telecommunication engineering from the University of Tehran, Tehran, Iran, in 2006, the M.Sc. degree in communication systems from the Sharif University of Technology, Tehran, in 2011, and the Ph.D. degree in electrical engineering from The University of Edinburgh, Edinburgh, U.K., in 2018,where he is currently a Research Associate with the LiFi Research and Development Centre. His research interests include communication theory, optical fiber communication, and visible light communication.

Ali Ghrayeb received the Ph.D. degree in electrical engineering from The University of Arizona, Tucson, AZ, USA, in 2000. He is currently a Professor with the Department of Electrical and Computer Engineering, Texas A&M University at Qatar. Prior to his current position, he was a professor with the Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada. He has coauthored two books and published over 200 journal and conference papers. His research interests include wireless and mobile communications, physical layer security, massive MIMO, and visible light communications. He served as an instructor or co-instructor in technical tutorials at several major IEEE conferences. He served as the Executive Chair for the 2016 IEEE WCNC conference. He has served on the editorial board of several IEEE and non-IEEE journals. He is a Fellow of the IEEE.

Chadi M. Assi received the Ph.D. degree from the City University of New York (CUNY) in 2003. He is currently a Full Professor at Concordia University. He was a recipient of the Prestigious Mina Rees Dissertation Award from CUNY in 2002 for his research on wavelength-division multiplexing optical networks. He is on the Editorial Board of IEEE Communications Surveys and Tutorials, the IEEE Transactions on Communications, and the IEEE Transactions on Vehicular Technologies. His current research interests are in the areas of network design and optimization, network modelling, and network reliability.

Majid Safari (S'08- M'11) received his Ph.D. degree in Electrical and Computer Engineering from the University of Waterloo, Canada in 2011. He also received his B.Sc. degree in Electrical and Computer Engineering from the University of Tehran, Iran, in 2003, M.Sc. degree in Electrical Engineering from Sharif University of Technology, Iran, in 2005. He is currently a senior lecturer (Associate Professor) in the Institute for Digital Communications at the University of Edinburgh. Before joining Edinburgh in 2013, He held postdoctoral fellowship at McMaster University, Canada. Dr. Safari 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. His main research interest is 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.

Harald Haas (S'98-A'00-M'03-SM'16-F'17) received the Ph.D. degree from The University of Edinburgh in 2001. He is currently the Chair of Mobile Communications at The University of Edinburgh, and he is the Initiator, Co-Founder, and Chief Scientific Officer of pureLiFi Ltd., and the Director of the LiFi Research and Development Centre, The University of Edinburgh. He has authored 500 conference and journal papers. His main research interests are in optical wireless communications, hybrid optical wireless and RF communications, spatial modulation, and interference coordination in wireless networks. He is an Associate Editor of the IEEE Journal of Lightwave Technologies. He gave two TED Global talks "Wireless Data From Every light Bulb" and "Forget Wi-Fi: Meet the New Li-Fi Internet" which together have been downloaded more than 5.5 million times. In 2012 and 2017, he was a recipient of the prestigious Established Career Fellowship from the Engineering and Physical Sciences Research Council (EPSRC) in the U.K. In 2014, he was selected by EPSRC as one of ten Recognizing Inspirational Scientists and Engineers Leaders in the U.K. He was a co-recipient of the EURASIP Best Paper Award for the Journal on Wireless Communications and Networking in 2015 and the Jack Neubauer Memorial Award of the IEEE Vehicular Technology Society. In 2016, he received the Outstanding Achievement Award from the International Solid State Lighting Alliance. He was a co-recipient of recent best paper awards at VTC-Fall, 2013, VTC-Spring 2015, ICC 2016, ICC 2017 and ICC 2018. In 2019 he received the James Evans Avant Garde Award of the IEEE Vehicular Technology Society. Haas is a Fellow of the Royal Academy of Engineering.