IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2021.DOI

6G Networks Physical Layer Security using RGB Visible Light Communications

S. SODERI[12] (Senior Member, IEEE), R. DE NICOLA[12]
[1]IMT School for Advanced Studies, Lucca, Italy (e-mail: simone.soderi@imtlucca.it)
[2]CINI Cybersecurity Laboratory, Roma, Italy

Corresponding author: S. Soderi (e-mail: simone.soderi@imtlucca.it).

This work was partially funded by EU H2020 research project SPARTA (grant agreement n.830892).

ABSTRACT Visible Light Communication (VLC) is a key technology for the sixth-generation (6G) wireless communication thanks to the possibility of using artificial environmental lights as a data transfer channel. Although VLC systems are more resistant against interference and less susceptible to security vulnerabilities like most wireless networks, VLC is even inherently susceptible to eavesdropping attacks. Moreover, since VLC is considered an enabling technology for 6G, specific mechanisms are needed to enforce data security. This paper considers improving the security of the next generation of wireless communications by using the Watermark Blind Physical Layer Security (WBPLSec) in VLCs. The main intuition is that RGB LEDs offer the possibility for Wavelength Division Multiplexing (WDM) as a useful support for the Spread-Spectrum (SS) watermarking. In this paper, we propose an approach that aims at obtaining VLC Physical Layer Security (PLS) by combining watermarking with an RGB LED jamming. We provide a performance analysis of the proposed security architecture based on the secrecy capacity in terms of its existence and outage probability. We prove that WBPLSec can be used to significantly improve confidentiality in the next generation of wireless communications. The results offer the possibility of creating a secure region around the legitimate receiver by leveraging the jamming optical power.

INDEX TERMS 6G, Visible light communication, RGB, Physical layer security (PLS), Jamming, Spread-spectrum, Watermarking.

I. INTRODUCTION

The sixth-generation (6G) mobile communication technology is one of the emerging research areas which will change our society. Its launch is expected around 2030 when our society it is expected to be data-driven and unlimited wireless connectivity [1], [2]. The next-generation communications system aims to achieve high spectral and energy efficiency, low latency, and massive connectivity because of the extensive growth of telecommunications systems. We live in a hyper-connected society where sensors can exchange data even without human intervention. Internet of Things (IoT) systems generate a massive amount of data transmitted via a networking infrastructure connecting plenty of communicating computing devices. In such a scenario, the risk of cyberattacks is very high.

Many contributors outline the 6G vision and illustrate its benefits while providing arguments on how it will accelerate the digitization process in our society [3], [4].

6G wireless networks are expected to achieve data rates up to 10 Tbps with the aid of TeraHertz (THz) and optical frequency bands. This performance will be achieved with multiple technology enablers such as Artificial Intelligence (AI), new physical-layers, semantic communications, quantum computing, intelligent networks, and Visible Light Communication (VLC) [5].

Fig. 1 depicts challenges and opportunities in developing 6G wireless networks in terms of technology enablers, Key Performance Indicators (KPI), and it specifically considers at VLC applications. Thus, Physical Layer Security (PLS), network security, and AI security will be fundamental for the evolution of the security landscape of next-generation telecommunication networks [6].

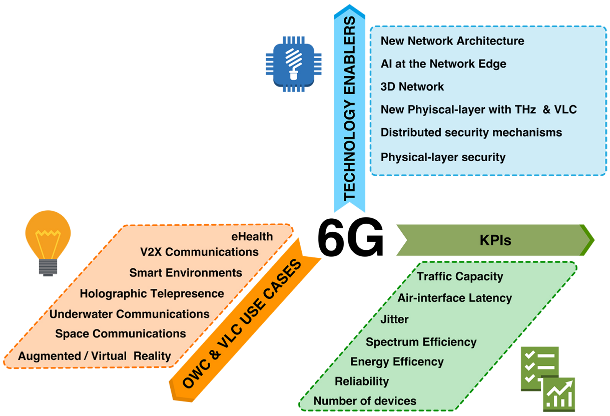

FIGURE 1: 6G challenges and VLCs' contribution.

A. BACKGROUND

Traditional Radio Frequency (RF) solutions cannot meet the traffic capacity growing demand. Still, due to the scarcity of frequencies, there is a need to develop new technologies to support the next generation of wireless communications requirements. While optical spectrum is already a key enabler for the global Internet, Optical Wireless Communication (OWC) is a promising candidate for high-speed wireless communications [7]. The optical spectrum can be used to provide next-generation communication systems that are fast, secure, robust, and efficient. As seen in Fig. 2 and Table 2, the optical bandwidth is several orders of magnitude larger than the spectrum resources available in the RF bands. Due to the opportunity offered by the license-free operation over a significantly wider spectrum, many technological solutions have proliferated in OWCs. OWCs utilize three different regions of the electromagnetic spectrum: Ultraviolet (UV), visible light, and Infrared (IR). As shown in Fig. 2, VLCs are a branch of OWCs that involve electromagnetic waves in the visible spectrum for communications [8]–[10]. IEEE 802.15.7 standard [11] issued in 2011 by the Visible Light Communication Task Group has been a significant step towards the commercialization and widespread VLC networks. VLC links benefit from the license-free light spectrum, the immunity to Radio Frequency (RF) interference, and the use of inexpensive LEDs and Photo-Diodes (PDs) for transmission and reception, respectively. VLCs require Electrical-to-Optical (EO) conversion in transmission through LEDs and Optical-to-Electrical (OE) conversion in reception through PDs. If we consider that many light bulbs already use LEDs, it is easy to see that the implementation of VLCs is not such a remote possibility. Besides, VLCs exploit existing illumination infrastructure for wireless communications. If light changes fast enough, human eyes will not perceive the flickering effect and a LED scan receive data.

However, 6G technology do not guarantee satisfactory *security* and *privacy* [7]. In the coming years, researchers shall face many challenges in building a trustworthy and secure 6G. In this scenario, PLS techniques could represent an efficient solution to secure Wireless Sensor Networks (WSNs) [4]. Indeed, PLS aims at securing communications by exploiting the physical properties of the communication channel. They relay on processing the signal sent over a channel to guarantee some security properties without resorting to protocols or algorithms at layers higher than the physical one. The next generation of low-power sensors networks is where PLS can reduce energy consumption by guarantee faster computations than cryptography, extending the battery life of portable devices.

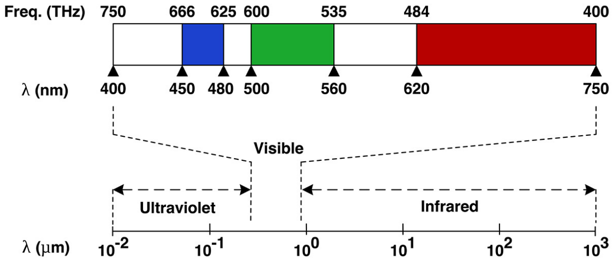

FIGURE 2: Electromagnetic spectrum and wavelength of the visible light.

Since confidentiality is one of the major concerns of wireless communication, researchers proposed many innovative solutions to improve it. Confidentiality through PLS was first considered in 1949 by Shannon, who presented the first application of information-theoretic secrecy [12]. This paper proposes an alternative to cryptography by using watermarking as a *covert-channel* to transfer information between two devices. Such covert-channel is an essential part of the PLS solution that we propose here. The remaining part of the proposed architecture over VLC consists of *jamming* intended as a luminous signal capable of destroying a specific part of the communication between the two devices.

This paper focuses on a particular architecture that uses watermarking and jamming to improve communications security by operating at the physical-layer and then creating a *secure region* around the legitimate receiver.

B. CONTRIBUTION

The Watermarked Blind Physical Layer Security (WBPLSec) protocol utilizes a jamming receiver in conjunction with a Spread-Spectrum (SS) watermarking technique [13]. This technique has received considerable interest in the last few years as it is as a standalone security solution for sensor networks. In a paper presented in 6G Wireless Summit 2020 [14], we provided a first proposal on how to apply a watermark-based physical layer security solution to VLCs. The current paper significantly extends that proposal with a deeper analysis about the existence of the Secrecy Capacity (C_s) and the probability of outage (P_{out}). In particular, the conference paper [14] proposed the intuition of using the two primitives of watermarking and jamming on VLC to improve communication security. That work presented preliminary results that used a channel model for VLCs that only predicted line of sight (LOS), and in numerical simulations, the channel coefficients were deterministic. In this paper, we consider a complete channel model that includes non-line-of-sight (NLOS) reflections due to obstacles or people in the room, which leads us to evaluate the coefficients according to a Rayleigh-type distribution. In the conference paper, the secrecy rate is computed by estimating the differential entropy using assumptions on the transmitted signal distributions, while during the simulations, the deterministic channel coefficients were estimated in numerical form. This work proposes calculating the existence of the secrecy capacity in closed form by evaluating the Signal-to-Interference-plus-Noise Ratio (SINR) as random variables whose probability density functions are derived below. It also calculates the probability of outage the secrecy capacity, which is very useful for understanding where a secure communication can or cannot occur.

The actual contributions fall within the following categories:

- **WBPLSec in 6G networks.** The proposed technique examines in-depth how the combination of watermarking and jamming can be successfully employed on VLC-based 6G networks. A novel RGB VLC transceiver architecture is defined in which the new PLS protocol implements watermark-based communication with an intentionally jamming receiver.
- **Security region.** With the application of WBPLSec we can build a *security region* around the legitimate receiver where 6G communication can take place securely.
- **Evaluation of SINR distribution.** Based on the proposed architecture where the receiver contains a jammer and considering a full reflection channel model, this paper calculates the distribution of SINR at the legitimate receiver and attacker levels. These distributions are an essential step to support the final part of the paper.
- **Analysis and evaluation.** The performance evaluation of a blind PLS protocol for 6G is based on the *secrecy capacity* in terms of its *existence* and *outage probability*.

C. ORGANISATION

The rest of the paper is organized as follows: Section II describes the main motivation and the innovation introduced for 6G secure communications. Section III briefly discusses alternative approaches. Section IV describes the VLC channel, whereas Section V introduces our model for the physical layer security over VLC networks. Section VI thoroughly discusses the secrecy capacity expression of a watermark-based VLC and the probability of outage of the secrecy capacity. Section VII presents the numerical results. Section VIII concludes the paper. A list of important acronyms is given in Table 1.

II. MOTIVATION

This section discusses the motivation behind the interest in VLCs as a technology for secure communications in the 6G domain. This motivation is twofold: (*i*) the advantages that VLC offers over traditional wireless communications and (*ii*) the ability to use RGB LEDs to combine watermarking and jamming in order to have communications that are resilient to eavesdropping attacks.

TABLE 1: List of important acronyms.

Acronym	Definition
6GFP	6G Flagship Program
AI	Artificial Intelligence
ASK	Amplitude Shift Keying
AWGN	Additive White Gaussian Noise
DC	Direct-Current
DD	Direct-Detection
DSSS	Direct Sequence Spread Spectrum
EO	Electrical-to-Optical
FOV	Field-Of-View
IDS	Intrusion Detection Systems
IM	Intensity Modulation
IoT	Internet of Things
IR	Infrared
KPI	Key Performance Indicators
LED	Light Emitting Diodes
LiFi	Light-Fidelity
LOS	Line-Of-Sight
NLOS	Non-Line-Of-Sight
OE	Optical-to-Electrical
OWC	Optical Wireless Communication
PD	Photo-Diodes
PLS	Physical Layer Security
RGB	Red-Green-Blue
RF	Radio Frequency
SINR	Signal-to-Interference-plus-Noise Ratio
SNR	Signal-to-Noise Ratio
SS	Spread-Spectrum
UV	Ultraviolet
VLC	Visible Light Communication
WBPLSec	Watermark Blind Physical Layer Security
WDM	Wavelength Division Multiplexing
WSN	Wireless Sensor Network

TABLE 2: Visible light spectrum.

	Wavelength [nm]	Frequency [THz]
Visible Light[1]	400 to 750	400 to 750
Red Light	620 to 750	400 to 484
Green Light	500 to 560	535 to 600
Blue Light	450 to 480	625 to 666

[1] Medium available for VLCs.

A. OPPORTUNITY WITH OPTICAL FREQUENCY BANDS

To realize the performance and application scenarios of 6G, we expect four new paradigm shifts for current wireless communication networks: global coverage, utilization of all spectrums, smart applications with the aid of AI, and network security by design.

For to this paper, it is essential to note that the study of usable frequencies will examine sub-6 GHz, mmWave, THz, and optical frequency bands [15]. VLC is a wireless communication technology that uses visible light for data transmission. It is the most common form of wireless communication technology today and one of the fastest and most efficient. Compared with RF, VLC has an unlicensed and free of charge optical bandwidth. Table 2 shows how the spec-

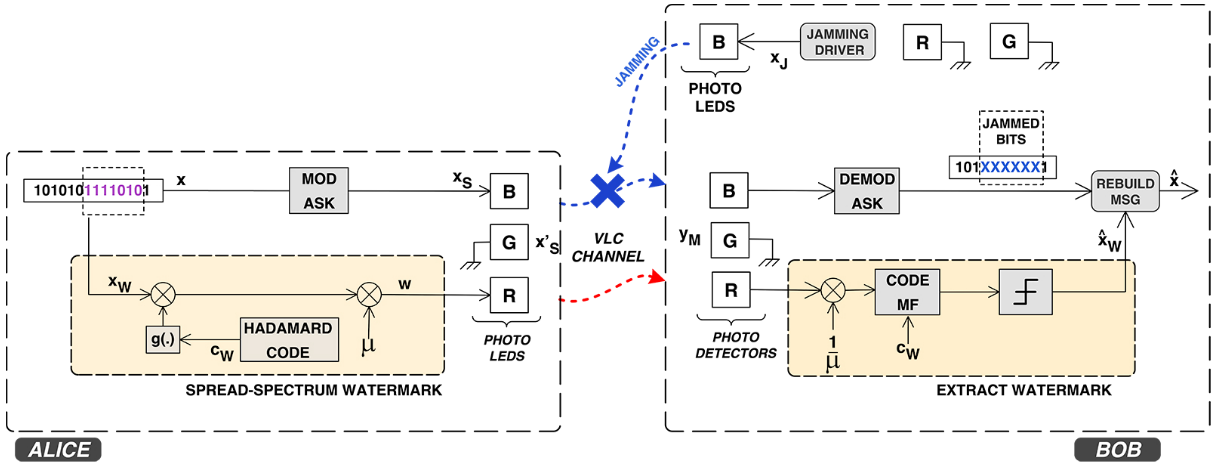

FIGURE 3: WBPLSec system model in a VLC network.

trum of visible light is potentially larger than the available bandwidth of RF. This makes very high data rate communication possible and virtually fulfills the $1-10$ Gb/s/m^3 KPI associated with 6G [16]. Furthermore, since the optical band does not overlap with RF bands, there is no electromagnetic interference [17].

The extremely high demand for data-rate in 6G poses major challenges in terms of security and privacy. Due to the high computational demand, existing security schemes are not appealing [16]. The 6G Flagship Program (6GFP) [18] is advising to consider security at each layer, but the security protection at physical layer is of fundamental importance [19]. To secure 6G wireless networks, we need to provide efficient PLS schemes with existing authentication and cryptographic protocols [1]. For example, low-power sensor networks are where PLS can provide significant advantages over cryptography in computational demand.

B. SECURITY INNOVATION IN 6G

The core characteristics of VLC, such as directional propagation, human visibility, and spatial confinement, guarantee inherent security in specific scenarios. For instance, the VLC signal isolation enhances communication security by preventing eavesdropping of in-room or in-building communications [9]. This paper proposes WBPLSec, an architecture to enhance 6G communications security by combining watermarking with a jamming receiver over VLC networks. This standalone security solution has been already investigated with success for other mediums such as RF and acoustic communications [13], [20].

WBPLSec has been proposed as a way to achieve *confidentiality* in 6G communications.

There are two common approaches to implement VLCs; the first uses white LEDs, the second RGB LEDs. The second solution guarantees a higher bandwidth, since it uses the three different independent channels to increase the data throughput [21], [22]; see Table 2.

Let us consider an example of the architecture of we would like to propose. Considering the case that Alice wants to send a secret message (x) to Bob. Alice transmits the watermarked signal using an RGB LED. Bob receives the message through a single RGB color-tuned PD but while receiving it, he jams Alice's VLC using an RGB LED. Eve, the eavesdropper, may use multiple PDs to violet secrecy. The system model is depicted in Fig. 3.

The scheme proposed exploits three RGB independent channels and uses a Wavelength Division Multiplexing (WDM) to watermark the VLC. It relies on four main actions (see Fig. 3):

- **Spread-Spectrum watermarking**: part of the secret message is first modulated with a spreading sequence and then transmitted by using only the red light;
- **Jamming Receiver**: Bob jams Alice's message using RGB LED;
- **Selective jamming**: Bob jams only part of the on the way message, and knowing the jammed part, he can rebuild the clean message. The jamming has not affect on the Spread-Spectrum (SS) watermark;
- **Communication hiding**: the proposed method transmits information through two independent paths using blue light and red light. The first one is a narrow-band Amplitude Shift Keying (ASK) signal transmitted through the blue light. At the same time, the SS watermark signal uses the red light and create in this way a covert channel.

The actual steps of WBPLSec are described in Algorithm 1.

Application scenario. WBPLSec on the VLC network can be successfully applied in those scenarios where RGB LEDs are used for lighting. In this paper, the discussion is done by considering the case of indoor VLCs; this is because it is necessary to define a channel model to calculate the secrecy capacity of the proposed model. Intuitively, this architecture, which uses watermarking and jamming on RGB VLC, can be also applied on outdoor VLC and underwater communications where optical signals are already successfully used. Each use case will have to use the corresponding channel model.

C. LIMITATIONS OF RELATED WORKS

Although many methods propose PLS solutions on VLC that include jamming, in almost all cases, these algorithms must involve other nodes in the network in order to coordinate and degrade the attacker's channel. Other solutions instead rely on architectures that use OFDM, signal reflections, or RIS, and this requires a more complex receiver in terms of modulation and demodulation. On the contrary, our solution aims at providing a mechanism that by combining for the first time watermarking and jamming is resilient to man-in-the-middle attacks. Our methodology is compatible with traditional VLCs watermarking and is a kind of covert-channel that can be used or ignored if a receiver does not implement our algorithm there will be no jamming. Currently, no work combines jamming at the receiver side with a covert-channel mechanism in VLC networks. Moreover, if we consider communications inside a room we could spread the jamming within the walls of the room so that the created security region coincides with the room. In this way, the communication will always be secure, whether the attacker is in the room and subjected to jamming or outside the room where he will not receive any signal.

III. RELATED WORK

This paper proposes the application of WBPLSec to VLCs. Although some contributions [4], [7], [23] suggest using VLCs as a means to achieve secure communications. our proposal to combine watermarking and jamming in VLCs is new. We use watermarking as a *covert channel* to re-compose the information disrupted by the legitimate receiver, who uses *jamming* as a security tool. In this section we briefly discuss some of the works by other researchers concerned with OWC technology, jamming, and covert channel communications.

A. OWC AND VLC TECHNOLOGIES

Over the years, researchers have published many papers on OWC and VLC, proposing new modulation schemes and comparing the performance with classical RF communications [24]. More recently, there have been contributions selecting VLCs as an enabling technology for next-generation wireless communications. Indeed, VLCs can offer low latency communications and a spectrum of several orders of magnitude greater than traditional communications [25]. The continued study by academia and the wireless device industry have identified new opportunities using optical frequency bands. Following this trend, in recent years, Haas *et al.* have developed Light-Fidelity (LiFi) that extends the concept of VLC to achieve high-speed, secure, two-way wireless communications. LiFi uses frequencies above 10 GHz, which results in more complex network infrastructure with smaller cells [26], [27]. In some situations, the VLC channel consists mainly of only the LOS; in that case, the optical signals will not be subject to fading. Thus, the absence of fading, combined with the fact that in VLC systems the wavelength of the optical signals is much smaller than the receiving PDs allows these systems to provide precise and reliable positioning services with centimeter-level accuracy [28], [29]. The possibility of determining the position of the receiver with a certain accuracy is a feature that makes VLC/OWC very interesting from a cybersecurity point of view and gives an advantage to legitimate receivers over attackers. The high performance provided by VLC may, in some cases, degrade rapidly if the receiver rotates or moves; then there would be a loss of signal. A solution to this problem can be offered by reconfigurable intelligent surfaces (RIS). Surfaces made of metal or liquid crystal could be dynamically configured to direct the transmitted light signal to the moving receiver [30], [31].

B. JAMMING AS A SECURITY TOOL

Secrecy capacity is defined as the maximum transmission rate achievable whenever the eavesdropper's channel observations are noisier than the legitimate user's channel [32]. Theoretical results have shown that secrecy can be improved by exploiting channel variations [33]–[35]. Other contributions use jamming to interfere with wireless communications [36], exploit jamming as a tool for improving security in cooperative networks [37], use friendly jamming as a powerful tool to increase secrecy of wireless systems [38]. Since these schemes are mainly applicable in a mobile environment, a channel-independent protocol called iJAM was introduced [39]. With this protocol, the sender transmits two times each symbol, and the receiver randomly jams complimentary samples over the two symbols. This technique has some weaknesses in terms of communication throughput because it cuts the data rate by half. In addition, it has security weaknesses because an adversary that observes two consecutive transmissions could rebuild the message by comparing and removing the jammed bits. WBPLSec overcomes these problems.

C. COVERT CHANNEL COMMUNICATIONS

Cryptographic protocols are the classical means for protecting data from unauthorized access. Unfortunately, there are cases in which encryption is inappropriate; in these cases the use of unconventional communication channels can be of help. In 1973, Lampson defined the covert channel as a communication channel that is not intended for information transfer [40]. We could say that covert channels are alternative tools to guarantee privacy of digital communications through information hiding [41]. We can use them for different legitimate and non-legitimate purposes. In some cases, we can use covert channels to improve network security, while in other cases, to breach it. Government and companies can use these channels to protect their communications, cyber-criminals can exploit this technology in the same way. For instance, Hanspach *et al.* proposed using covert channels to circumvent network security policies by establishing new communication paths [42]. Authors recently considered using covert channel for authentication [43]. The strength of this approach is the *encapsulation* of information in an existing medium, to avoid any modification of standard protocols. Any system that uses TCP/IP can benefit of hidden communications that transmit information through networks without triggering Intrusion Detection Systems (IDS) [44].

D. VLC SECURITY

VLC has gained significant interest due high data-rate, robustness against interference, and low cost of LEDs and PDs. By their nature, indoor VLCs are confined, for example, by the room's walls where the communication is taking place [8]. On the one hand, this can limit communication by making it necessary to install other light sources to propagate communication between different hotspots [45]. On the other hand, it offers a considerable advantage in terms of security and privacy. In practice, VLCs offer better PLS and privacy than RF systems because light waves cannot pass through walls, making it nearly impossible to intrude into sensitive structures by picking up the wireless signal.

Over the past few years, many papers investigated security of VLCs; we refer to [46] for a survey. Many contributions in the literature propose VLC-based PLS solutions to enhance security of wireless communication systems [47]. An example is given by SecLight [48]; there light intensity and reflections are combined with the channel estimation to enhance security of VLC in IoT. An interesting set of contributions investigated solutions using jamming to improve security of VLCs [49], [50]. For instance, Mostafa *et al.* [51] proposed friendly jamming to prevent eavesdropping. Some authors have proposed other jamming schemes to improve the performance of PLS in VLC systems. In such an indoor VLC scheme, they assumed to have many LEDs mounted on the room's ceiling. The LED closest to the legitimate receiver will transmit the information while the others will create a light interference towards the attacker to reduce its SINR [52]. From another perspective, depending on the receiver technology, camera-based VLC uses a camera as a receiver instead of PDs to secure mobile communications [53].

In addition, other contributions show how using VLCs can have a high directional gain that makes interception of information transmission very unlikely, making the links more secure than we would have with traditional RF communications [54]. Among the research contributions in PLS for VLCs, it is also worth mentioning those that use multiple-input multiple-output transceiver-based beamforming techniques to create secure communication zones [55]. Other researchers have posited a physical layer encryption method based on optical OFDM to strengthen the confidentiality of VLC systems. This method performs a complex encryption operation on OFDM signals that make it resistant to statistical and brute force attacks [56]. The use of RIS is considered a new area of research to improve VLC security. These reconfigurable surfaces can be used in at least three ways: dynamic multipath tuning, producing jamming, and beam steering to the legitimate receiver [57].

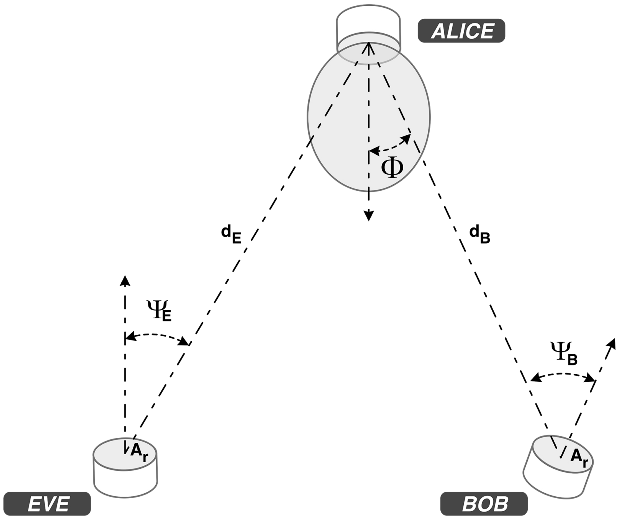

FIGURE 4: LOS in the VLC channel model.

IV. VLC CHANNEL MODEL

In this section we introduce the VLC channel model presented that will be instrumental for evaluating the secrecy capacity of the model we propose.

VLCs, in general, utilize the Intensity Modulation (IM) scheme along with Direct-Detection (DD). In particular, with IM/DD technique, the transmitted signal $x_i(t)$ is the optical power generated when the modulated current signal passes through the LED. However, the dynamic range of the LED is inherently limited. Therefore, the modulating signal must satisfy certain *amplitude constraints* to avoid clipping distortion [58]. On the other side, the received signal $y(t)$ is proportional to the optical power that arrives at the Photo-Diodes (PD) [8]. On the transmitter side, the desired illumination level is maintained by setting the appropriate Direct-Current (DC) bias of the overall signal fed into the LED [9]. The DD technique supports only the modulation variation to transmit the information through light intensity alteration. The phase of the signal can not be considered because the transmitted light is incoherent.

The received signal $y(t)$, after the PD, in a VLC is conventionally modeled as follows

$$y(t) = h(t) * x_i(t) + n(t), \tag{1}$$

where $h \in \mathbb{R}_+$ is the channel gain and $n(t)$ is the background light noise, which is modeled as a signal-independent Additive White Gaussian Noise (AWGN) [8].

An indoor VLC channel consist of two main components: the Line-Of-Sight (LOS) channel and the diffuse channel. The first is composed of the light that directly hits the PD without bouncing on other objects. The second, also known as Non-Line-Of-Sight (NLOS), includes all light rays that bounce the objects in the room. Thus, this paper considers the LOS component (see Fig. 4) and the first reflection as NLOS (see Fig. 5).

Modeling a VLC channel should define the transmitter as the light source and consider the amount of light received by the PD. There are various models of VLC channels that differ in terms of source and reflection surfaces [59]. This paper uses the Lambertian emission law that says that the intensity of light emitted by an ideal diffuse source detected by an observer is directly proportional to the cosine of the angle between the normal to the surface and the observer's direction. In this model, the observer (i.e., receiver) can be considered a new light source with an intensity equal to the previously received power, while the observer will be elsewhere. In our opinion, this model works well in the presence of obstacles such as a room with objects can be. Thus, assuming to have Lambertian light source, the LOS component of the channel DC gain, i.e. $H(0) = \int_{-\infty}^{\infty} h(t)dt$, between one LED and one PD is given by [8]

$$H_d(0) = \begin{cases} \frac{Ar(m+1)R}{2\pi d^2} D(\psi)\cos^m(\phi)\cos(\psi), & |\psi| \le \psi_{FOV}, \\ 0, & |\psi| > \psi_{FOV}, \end{cases} \quad (2)$$

where A_r is the receiver collection area, R is the PD responsivity, $m = {}^{-\ln(2)}/_{\ln(\cos(\phi_{\frac{1}{2}}))}$ is the order of the Lambertian emission with half irradiance at $\phi_{\frac{1}{2}}$, ϕ is the angle of irradiance, $D(\psi) = {}^{n^2}/_{\sin^2(\psi_{FOV})}$ is the gain of the optical concentrator with n refractive index, d is the LOS distance between the LED and the PD, ψ is the angle of incidence, and ψ_{FOV} is the receiver's angle Field-Of-View (FOV).

The channel DC gain of the first reflection is shown as

$$dH_{ref}(0) = \begin{cases} \frac{A_r(m+1)R}{2\pi^2 d_{1B}^2 d_{2B}^2} D(\psi)\rho dA_w \cos^m(\phi) & \\ \cdot\cos(\alpha)\cos(\beta)\cos(\psi), & |\psi| \le \psi_{FOV}, \\ 0, & |\psi| > \psi_{FOV}, \end{cases} \quad (3)$$

where A_r is the receiver collection area, R is the PD responsivity, $m = {}^{-\ln(2)}/_{\ln(\cos(\phi_{\frac{1}{2}}))}$ is the order of the Lambertian emission with half irradiance at $\phi_{\frac{1}{2}}$, ϕ is the angle of irradiance, $D(\psi) = {}^{n^2}/_{\sin^2(\psi_{FOV})}$ is the gain of the optical concentrator with n refractive index, d_{1B} is the distance between the transmitter, i.e. Alice, and a reflection point, d_{2B} is the distance between the reflection point and the receiver, i.e. Bob, ρ denotes the reflection coefficient, dA_w represents the emission area of a micro surface, α expresses the incidence angle of a reflection point and β is the radiation angle of the receiver, ψ is the angle of incidence, R is the PD responsivity, and ψ_{FOV} is the receiver's angle FOV.

Under the assumption that Alice has one RGB LED, for a given transmission power (P_t), the total received power is given by the DC channel on the directed path, i.e. $H_d(0)$, and reflected path diffused path through the walls, i.e. $H_{ref}(0)$ [60].

In the indoor VLC channel the LOS and diffuse components are separated from each other in the time domain [61]. Therefore, the channel transfer function is expressed as

$$H(0) = H_d(0) + H_{ref}(0), \quad (4)$$

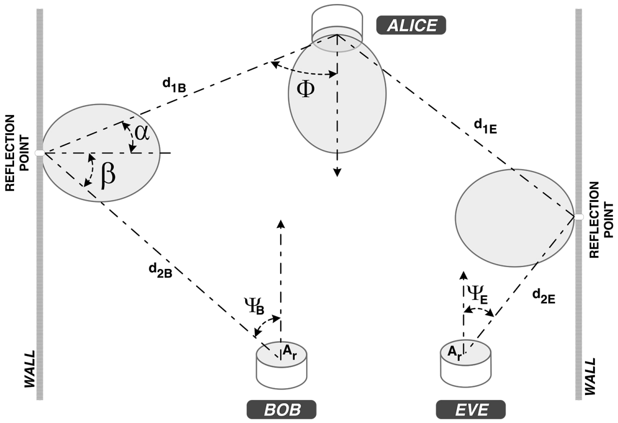

FIGURE 5: NLOS in the VLC channel model.

where H_d represent the LOS link and H_{ref} is the contribution given by the diffuse reflections [61], [62]. To consider people's movement between transmitter and receiver, the fluctuation in channel gain H can be described by Rayleigh distribution

$$f_H(h) = \frac{h}{\sigma_p^2} e^{-\frac{h^2}{2\sigma_p^2}} \qquad h > 0, \quad (5)$$

where σ_p is the scale parameter accounting for people density in the room.

Considering both direct and reflected paths, when $d^2 \gg A_r$, the received optical power (P_r) can be computed by taking into account walls' reflections as follows

$$P_r = P_t \left(H_d(0) + \int_{wall} dH_{ref}(0) \right) \quad (6)$$

where P_t is the transmitted optical power from the RGB LED.

In a VLC system, the Signal-to-Noise Ratio (SNR), i.e. γ_v, is proportional to the square of the received optical power:

$$\gamma_v = \frac{H^2(0)P_t^2}{\sigma^2}, \quad (7)$$

where P_t is the transmitted optical power, $H(0)$ is the channel DC gain and σ^2 is the spectral density of the background noise.

V. WBPLSEC SYSTEM MODEL

In this section we present a modified version of the non-degraded wiretap channel model [63] that takes into account the *jamming channel* utilized to jam the received signal and also the eavesdropper. Fig. 6 shows the model used to analyze the physical layer security in VLC.

The source message $(x_S)^N$ of length N is encoded into code-word $(x'_S)^N$ with the same length. In particular, the encoder embeds the watermark $(x_W)^{N_W}$ of length N_W into the host signal $(x_S)^N$. The legitimate user, Alice, transmits $(x'_S)^N$ to Bob through the *main channel*. Eve receives this

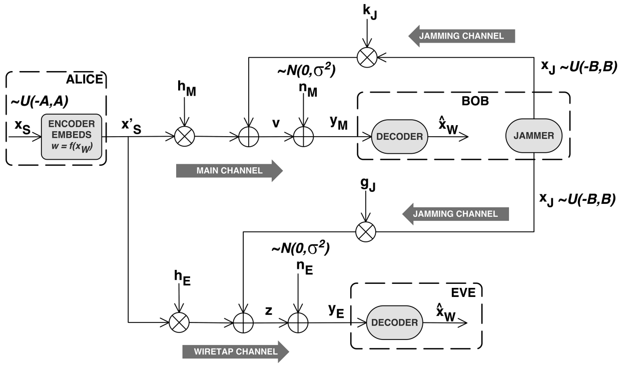

FIGURE 6: Non-degraded wiretap channel model with jamming receiver.

signal through the *wiretap channel*. The *i*-th sample of the signal received by Bob and Eve are respectively:

$$y_M(i) = h_M(i)x'_S(i) + k_J(i)x_J(i) + n_M(i), \tag{8}$$

$$y_E(i) = h_E(i)x'_S(i) + g_J(i)x_J(i) + n_E(i), \tag{9}$$

where h_M, k_J, h_E, g_J are the channel's gains. x'_S is the data signal, x_J is the jamming signal, n_M and n_E are the complex zero-mean Gaussian noise with variance σ^2.

In 1997, Cox *et al.* [64] defined the methodology for the digital watermarking. They introduced three different ways (equations) to watermark a signal. We exploit the first of their equations. It states that the watermarked signal v' can be expressed by

$$v'(i) = v(i) + \mu w(i), \tag{10}$$

where $v(i)$ is the i-th sample of the signal, μ is the scaling parameter and $w(i)$ is the watermark.

In our scenario, equation (10) becomes

$$x'_S(i) = x_S(i) + \mu w(i), \tag{11}$$

where $x_S(i)$ is the i-th sample of the continuous ASK transmitted signal [65], μ is the scaling parameter and $w(i)$ is the SS watermark.

The host ASK modulated signal x_S can be expressed as

$$x_S(i) = \begin{cases} A_a\sqrt{\dfrac{2}{T_{hs}}} \cdot cos(2\pi f_{hs} i), & \text{for } 0 \leq i \leq T_{hs}, \\ 0, & \text{elsewhere,} \end{cases} \tag{12}$$

where A_a is the amplitude, T_{hs} is the symbol time and f_{hs} is the frequency of the modulated signal.

We use the Direct Sequence Spread Spectrum (DSSS) technique for signal watermarking that can be expressed as

$$w(i) = \sum_{k=-\infty}^{+\infty} \sum_{j=0}^{N_c-1} g(i - kT_b - jT_c)(c_W(i))_j(x_W(i))_k, \tag{13}$$

where $(x_W(i))_k$ is the k-th data bit of the watermark signal, $(c_W(i))_j$ represents the j-th chip of the orthogonal pseudo-noise (PN) sequence, $g(i)$ is the pulse waveform, T_c is the chip length, and $T_b = T_{hs} = N_c T_c$ is the bit length.

```
Algorithm 1: WBPLSec for VLC networks.
Input: $x$ (shared secret); $N$; $N_W$
Output: $x$ (rebuilt)
ALICE: begin
    $x_S$ = Mod.ASK($x$);                         ▷ Modulation ASK
    $w$ = Mod.DSSS($x_W$);                        ▷ Embed watermark
    Tx.Light.BLUE($x_S$);                          ▷ Transmission
    Tx.Light.RED($w$);                             ▷ Transmission
end
BOB: begin
    $M$ := Random(1, $N_W$);                       ▷ Bits jammed
    $jam_s$ := $(N - M)$;                          ▷ Start of jamming
    $c$ := 0; $b_{rx}$ := 0;
    $h_B$;                                         ▷ Pass-band blue light filter
    $h_R$;                                         ▷ Pass-band red light filter
    $x_J$ = Jamming($N_W$);                        ▷ Algorithm 2
    $\hat{x}$ = Demod.ASK($h_B * y_M$);            ▷ Demodulation ASK
    $\hat{x}_W$ = Demod.DSSS($h_R * y_M$);         ▷ Extract watermark
    Function ReBuild.Signal($M$, $jam_s$):
        while $c < M$ do
            if $b_{rx} \leq jam_s$ then
                $b_{rx} = b_{rx} + 1$;             ▷ No Replacement
            else
                $\hat{x}(b_{rx})$ = $\hat{x}_W(c)$;  ▷ Replace bit
                $b_{rx} = b_{rx} + 1$;
                $c = c + 1$;
            end
        end
        return $\hat{x}_S$
end
```

Signal watermarking is performed relying on the traditional spread spectrum [66]. The secret x that Alice and Bob want to exchange is ASK modulated to create the host signal while a part of x, x_W, is used to create the SS watermark. The main idea behind the watermark embedding phase is that the transmitter marks, utilizing SS, the host signal x_S selecting the last N_W of x. Then x_W is given by

$$x_W(i) = \begin{cases} x_S(i), & \text{for } N - N_W \leq i \leq N, \\ 0, & \text{elsewhere.} \end{cases} \tag{14}$$

Let us now consider the VLC application of the WBPLSec. The model is shown in Fig. 6, in which the jamming receiver, together with the watermarking, provides secrecy. Please notice that Bob rebuilds the original message by using the information contained in the watermark. Indeed, he replaces the destroyed bits with those in the watermark [13], [20]. To simplify the derivation of the secrecy capacity expression, we assumes that x_S, x_J and w are uniformly distributed over the interval $[-A, A]$.

A. JAMMING STRATEGY

A key feature of WBPLSec architecture is the jamming receiver. As shown in Fig. 3, we assumed to transmit the ASK signal through the blue light and the SS watermark through the red light. The VLC channel composes the signal consistently. Bob jams to interfere with the ASK received signal. With this technique, Bob destroys a specific part of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3139456, IEEE Access

TABLE 3: Main parameters for jamming.

Parameter	Description
N	Number of bits
M	Number of jammed bits
N_W	Number of bits to create the watermark
T_b	Bit time

Algorithm 2: Jamming receiver (Bob)

```
Input: $N$; $N_W$
Output: Deletion of $N_W$ bits.
$M$ := Random(1, $N_W$);                ▷ Bits jammed
$jam_s$ := $(N - M)$;                   ▷ Start of jamming
$c$ := 0; $b_{rx}$ := 0;
while $c < M$ do
    if $b_{rx} \leq jam_s$ then
        $b_{rx} = b_{rx} + 1$;          ▷ No Jamming
    else
        Jamming(ON);                    ▷ Blue light ON
        Wait($T_b$);                    ▷ Jamming 1 bit
        Jamming(OFF);                   ▷ Blue light OFF
        $b_{rx} = b_{rx} + 1$;
        $c = c + 1$;
    end
end
```

the information received by suppressing up to M bits of the payload transmitted by Alice.

Clearly, jamming effectiveness depends on Alice and Eve's distance from Bob, and this determines the region where we can have a secure communication. Later on in this paper, we will define it a *secure region*. Jamming is obtained by increasing blue light intensity and altering the dynamic of the PD while weakening part of Alice's signal. Table 3 contains the description of the main parameters used for jamming. The legitimate receiver, Bob, can efficiently implement the jamming strategy through the procedure sketched in Algorithm 2. It is worth noticing that, Algorithm 2 assumed to jam the last N_W bits of the message x because we used the last N_W bits to build the watermark. However, it is not mandatory to use the latest N_W; everything would continue to work if we use N_W bits chosen at random in the x message.

The choice of assigning the SS watermark signal to the red light and the ASK signal to the blue light was dictated by the desire to guarantee a greater bandwidth to the SS watermark. Intuitively, we can say that the proposed architecture would be effective also if the role of blue and red light is reverse.

VI. SECRECY CAPACITY OF THE WBPLSEC IN VLC

In this section, we address the general problem of physical layer security by investigating the secrecy capacity of a Rayleigh VLC channel. We assumed that IM/DD channels are modeled with amplitude constraints [58].

First, we need to introduce some preliminaries. Since WBPLSec algorithm relies on an intentional interference it is necessary to take into account the Signal-to-Interference-plus-Noise Ratio (SINR).

The SINR at the legitimate receiver, γ_M, is given by

$$\gamma_M = \frac{H_M^2(0)P_t^2}{\sigma^2 + K^2 P_j^2}, \tag{15}$$

where P_t is the transmitted optical power, $H_M(0)$ is the channel DC gain between Alice and Bob, P_j is the jamming optical power, and σ^2 is the background noise spectral density. It is assumed that Alice and Bob experience the same background noise. The jammer is installed close to the receiver's photo-detector and generates an artificial selective interference that destroys part of the information received. Please notice that with this architecture, the jamming channel k_J cannot be described using equation (4) that is valid only in the far-field condition, i.e., when $d^2 \gg A_r$. This is not the case for Bob's jammer. We imposed $K(0) = K$ without loss in generality, considering that the P_j undergoes an average attenuation in the near-field region at the legitimate receiver. Channels are power limited, and it is assumed that $P_t = E'_S/N$) is the average transmitted power, $P_j = M \cdot P_t$ is the average jamming power when Bob jams M samples over N with $M < N$.

The SINR at the eavesdropper, γ_E, is given by

$$\gamma_E = \frac{H_E^2(0)P_t^2}{\sigma^2 + G_J^2(0)P_j^2}, \tag{16}$$

where $H_E(0)$ is the channel DC gain between Alice and Eve, $G_J(0)$ is the channel DC gain between Bob and Eve, and σ^2 is the background noise spectral density. It is assumed that Bob and Eve experience the same σ^2.

As in Fig. 3, it is also assumed that the channel fluctuations are described by a Rayleigh probability density function, which means that $H_M(0)$, $H_E(0)$ and $G_J(0)$ are Rayleigh distributed. Hence, the distribution of the SINR at the legitimate receiver can be written as follows

$$p(\gamma_M) = \begin{cases} \dfrac{e^{-\frac{\gamma_M\left(K^2P_j^2+\sigma^2\right)}{2\sigma_p^2P_t^2}}\left(K^2P_j^2+\sigma^2\right)}{2\sigma_p^2P_t^2}, & \gamma_M \geq 0, \\ 0, & \text{elsewhere}, \end{cases} \tag{17}$$

where γ_M is the SINR at Bob's receiver, P_j is the jamming optical power and σ^2 is the background noise spectral density, P_t is the transmitted optical power and σ_p is the scale parameter based on the people density in the room.

Similarly, the distribution of γ_E is given by

$$p(\gamma_E) = \begin{cases} \dfrac{e^{-\frac{\gamma_E\sigma^2}{2\sigma_p^2P_t^2}}\left(\sigma_p^2P_t^2\left(2\sigma_f^2P_j^2+\sigma^2\right)+\sigma_f^2\gamma_EP_j^2\sigma^2\right)}{2\left(\sigma_p^2P_t^2+\sigma_f^2\gamma_EP_j^2\right)^2}, \gamma_E \geq 0, \\ 0, \qquad \text{elsewhere}, \end{cases} \tag{18}$$

where γ_E is the SINR at Eve's receiver, and σ^2 is the background noise spectral density, σ_p and σ_f are the scale parameters based on the people density in the room for the main and jamming channel (see Fig. 6), respectively.

When Bob has a better channel realization than Eve, i.e. $\gamma_M > \gamma_E$, the secrecy capacity (C_s) of the legitimate link is defined for the non-degraded Gaussian wiretap channel [63], [67] as follows

$$\begin{aligned} C_s &= \max_{p(x'_S)} (\mathbb{I}(X'_S;Y_M) - \mathbb{I}(X'_S;Y_E)) = \\ &= \max\{C_M - C_E, 0\} = \\ &= \begin{cases} \frac{1}{2}\log_2 \frac{1+\gamma_M}{1+\gamma_E}, & \text{if } \gamma_M > \gamma_E, \\ 0, & \text{if } \gamma_M \leq \gamma_E. \end{cases} \end{aligned} \tag{19}$$

where $p(f_{x'_S})$ is the statistical distribution of the input signal x'_S and $\mathbb{I}(.;.)$ stands for the mutual information over the main and wiretap channels, C_M is the channel capacity from Alice to Bob, i.e. the main channel, and C_E is the channel capacity from Alice to Eve, i.e. the wiretap channel exploited by the eavesdropper.

A. EXISTENCE OF SECRECY CAPACITY

The existence of non-zero secrecy capacity is an important metric because it indicates the feasibility of secure communication. As shown in Fig. 3, the main channel and the eavesdropper's channel are independent. In addition, by knowing the probability density function of SINRs given by (17) and (18), the probability of existence of a strictly positive C_s is

$$\begin{aligned} &P[C_s > 0] = P[\gamma_M > \gamma_E] = \\ &= \int_0^\infty \int_0^{\gamma_M} p(\gamma_M) \cdot p(\gamma_E) d_{\gamma_E} d_{\gamma_M} = \\ &=1 + \frac{\left(P_j^2 K^2 + \sigma^2\right) e^{\frac{\frac{2\sigma^2}{P_j^2} + K^2}{2\sigma_{fp}^2}}}{2\sigma_{fp}^2 P_j^2} \cdot \\ &\left(\text{Ci}\left(\frac{\frac{2\sigma^2}{P_j^2} + K^2}{2\sigma_{fp}^2} \right) - \text{Si}\left(\frac{\frac{2\sigma^2}{P_j^2} + K^2}{2\sigma_{fp}^2} \right) \right), \end{aligned} \tag{20}$$

where $\text{Ci}(z) = \int_0^z \left({}^{\cosh(t)}/_t \right) dt$ is the hyperbolic cosine integral function, $\text{Si}(z) = \int_0^z \left({}^{\sinh(t)}/_t \right) dt$ is the hyperbolic sine integral function. We assumed that any VLC receiver experiences the same people density in the room, i.e., $\sigma_{fp} = \sigma_f = \sigma_p$.

Remark 1. It is interesting to observe that the probability of existence is independent of Alice's transmitted power. Moreover, it is useful to evaluate (20) by varying the jamming intensity, i.e., P_j. From (20) it follows that when $P_j \to \infty$ we have that

$$\begin{aligned} &\lim_{P_j \to \infty} P[C_s > 0] = \\ &=1 + \frac{K^2 e^{\frac{K^2}{2\sigma_{fp}^2}} \left(\text{Ci}\left(\frac{K^2}{2\sigma fp^2} \right) - \text{Si}\left(\frac{K^2}{2\sigma fp^2} \right) \right)}{2\sigma_{fp}^2}, \end{aligned} \tag{21}$$

and when $P_j \to 0$ we have that

$$\lim_{P_j \to 0} P[C_s > 0] = \frac{1}{2}. \tag{22}$$

B. OUTAGE PROBABILITY OF SECRECY CAPACITY

We can also characterize the secrecy capacity of a VLC channel in terms of outage probability, P_{out}, i.e., the probability that the instantaneous secrecy capacity is less than a target secrecy rate $R_s > 0$. In this section, we derive a closed-form of the P_{out}, but first, we must understand its significance. P_{out} provides a security metric when Alice and Bob do not have information about the eavesdropper's channel. In this case, Alice can only set the secrecy rate to a target R_s and knowing that $C_s = C_M - C_E$, Alice can assume that the Eve's capacity is $C'_E = C_M - R_s$. If $R_s < C_s$, Eve's channel will be worst than Alice's one, i.e., $C'_E < C_E$, ensuring perfect secrecy. Otherwise, if $R_s > C_s$, then $C'_E > C_E$ and the communication security is compromised.

For computing P_{out} it is useful to consider the probability density function of γ_M and γ_E (equations (17) and (18)). It can be shown that the P_{out} is given by

Proposition 1.

$$\begin{aligned} &P_{out}(R_s) = P[C_s < R_s] = \\ &= 1 - e^{-\frac{\left(4^{R_s}-1\right)\left(P_j^2 K^2 + \sigma^2\right)}{2\sigma_{fp}^2 P^2}} + 2^{(2R_s - 1)} \cdot \\ &\cdot \frac{\left(P_j^2 K^2 + \sigma^2\right) e^{\frac{-\frac{\left(4^{R_s}-1\right)\left(P_j^2 K^2 + \sigma^2\right)}{P^2} + 4_s^R \left(\frac{\sigma^2}{P_j^2} + K^2 \right) + \frac{\sigma^2}{P_j^2}}{2\sigma_{fp}^2}}}{\sigma_{fp}^2 P_j^2} \cdot \\ &\cdot \left(\text{Si}\left(\frac{\sigma^2 + 4_s^R \left(P_j^2 K^2 + \sigma^2\right)}{2\sigma_{fp}^2 P_j^2} \right) \right. \\ &\left. -\text{Ci}\left(\frac{\sigma^2 + 4_s^R \left(P_j^2 K^2 + \sigma^2\right)}{2\sigma_{fp}^2 P_j^2} \right) \right). \end{aligned} \tag{23}$$

Proof.

$$\begin{aligned} P_{out}(R_s) &= P[C_s < R_s] = \\ &= P[C_s < R_s | \gamma_M > \gamma_E] \cdot P[\gamma_M > \gamma_E] + \\ &+ P[C_s < R_s | \gamma_M \leq \gamma_E] \cdot P[\gamma_M \leq \gamma_E]. \end{aligned} \tag{24}$$

Now we have that

$$P[C_s < R_s | \gamma_M \leq \gamma_E] = 1. \tag{25}$$

And,

$$P[\gamma_M \leq \gamma_E] = 1 - P[\gamma_M > \gamma_E] \tag{26}$$

where $P[\gamma_M > \gamma_E]$ is expressed by (20).

On the other hand, we have also

$$
\begin{aligned}
&P[C_s < R_s | \gamma_M > \gamma_E] = \\
&= P\left[\frac{1}{2}\left(\frac{1+\gamma_M}{1+\gamma_E}\right) < R_s \middle| \gamma_M > \gamma_E\right] = \\
&= P\left[\gamma_M < 4^{R_s}(1+\gamma_E) - 1 \middle| \gamma_M > \gamma_E\right] = \\
&= \int_0^\infty \int_{\gamma_E}^{4^{R_s}(1+\gamma_E)-1} p(\gamma_M, \gamma_E | \gamma_M > \gamma_E) d_{\gamma_E} d_{\gamma_M} = \\
&= \int_0^\infty \int_{\gamma_E}^{4^{R_s}(1+\gamma_E)-1} \frac{p(\gamma_M)\cdot p(\gamma_E)}{P[\gamma_M > \gamma_E]} d_{\gamma_E} d_{\gamma_M} \qquad (27)
\end{aligned}
$$

Combining the previous equations, i.e., (25), (26), (20), and (27), and after some algebraic calculations, we get (23). □

VII. NUMERICAL RESULTS

We now present the numerical results confirming the existence and the outage probability of the secrecy capacity, modeled in the previous section. The performance of the WBPLSec method to secure VLCs are investigated by considering the scenario depicted in Fig. 7 with VLCs inside a standard room size of 5 m × 5 m × 4 m. The reference coordinate system origins being positioned in the center of the room for the simulations.

Currently, there are no devices that allow the implementation of the proposed model efficiently. Indeed in the coming years, RGB and PD LEDs will arrive to support this type of VLC. Therefore, since we could not perform actual experiments, in this section we provide some numerical evaluations. In particular, we focus on the parametric analysis of the developed model and then show the trend of the secrecy capacity and the existence of the secure communication region around Bob.

Table 4 lists all the parameters used for the parametric analysis, including the transmitted power, the jamming intensity, and the orientations of the transmitter and receivers. Alice, Bob, and Eve utilize LEDs with the same characteristics. During simulations, we assumed that Alice was installed on the room's roof, whereas Bob and Eve could freely move inside the room. Without loss in generality, we considered the first reflection from each room's wall. Instead, higher-order reflections were neglected.

The room contains some obstacles such as furnitures and other people that randomly obstruct the line of sight between Alice and any VLC receiver. The channel variations induced by these obstacles were modeled with a Rayleigh distribution. The author assumed to have the same people density on both the main and the eavesdropper channels; this results in having the same parameter for both channels, i.e., $\sigma_p = \sigma_f = \sigma_{fp}$.

Fig. 8 presents the normalized received optical power with LOS and NLOS contributions with Alice had coordinates $(0, 0, 2)\ m$. As shown in Fig. 3, Alice consists of one RGB LED that radiates 10 mW optical power. The WBPLSec architecture includes a second transmitter, i.e., the jammer; thus, Fig. 9 presents the normalized jamming power emitted by Bob when he is placed in the corner of the room (Bob's coordinates are $(-1, -1, -1)\ m$). It is essential to understand the jamming power pattern around the legitimate receiver to understand its effectiveness.

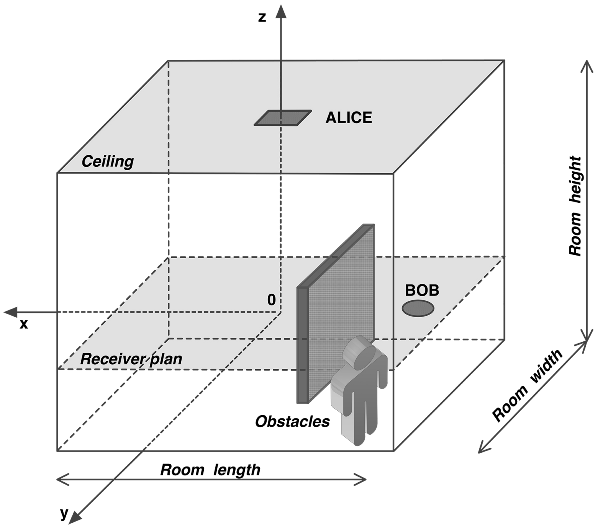

FIGURE 7: Example of the VLC in a room with obstacles such as walls, furniture's and persons. The reference coordinate system origin is positioned in the center of the room.

TABLE 4: Simulation parameters.

Parameter	Value
P_t	$10\ mW$
σ	10^{-10}
σ_f, σ_p	(0.98, 1.33, 1.57, 1.77) $^{people}/_{m^2}$
A_r	$1\ cm^2$
ψ_{FOV}	120°
$\phi_{\frac{1}{2}}$	30°, 70°
ρ	0.8
n	1.5
R	1 $^{A}/_{W}$
K	10^{-5}
N	$16384\ bits$
M	$(8 \div 8192)\ bits$
R_s	(0.5, 2) $^{bits}/_{s/Hz}$
Room (length, width, height)	$5 \times 5 \times 4\ m$
Alice coordinates (x,y,z)	(0,0,2) m

Fig. 10 shows the *secure region* that Bob can create around him by using a jammer. The problem is to tune the optimal jamming intensity to have $\gamma_M > \gamma_E$, meaning that Bob can significantly degrade Eve's reception. This condition guarantees existence of the secrecy capacity or, in short, a confidential VLC between Alice and Bob when Eve is inside such region.

The Fig. 11 shows what happens when the attacker moves close to the transmitter. In fact, with Alice positioned on the roof and Bob on the floor when Eve moves on the plane (X, Y, 1), i.e., at about 1 meter from the ceiling, Bob's

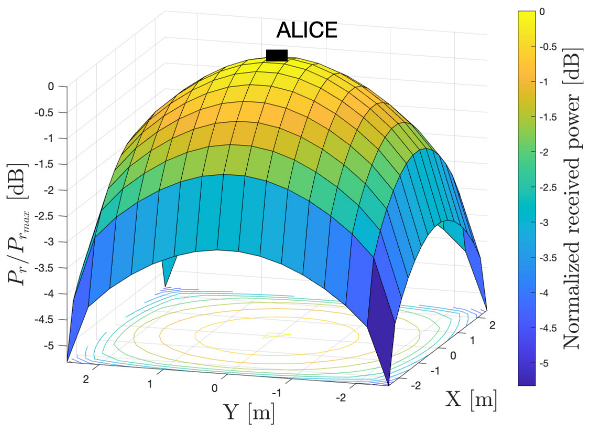

FIGURE 8: Bob normalized received power. (Alice's coordinates $(1, 1, 1.5)\ m$, $P_t = 10\ mW$).

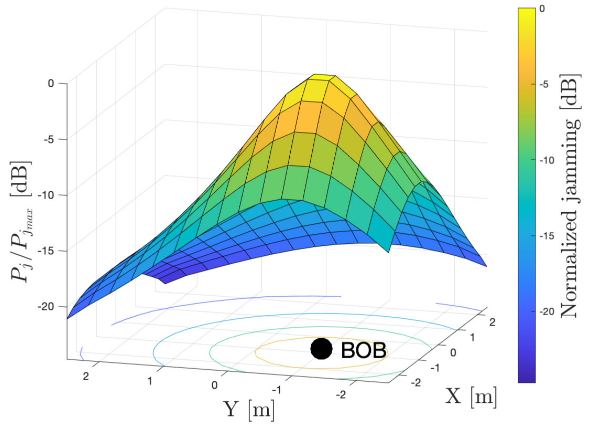

FIGURE 9: Normalized jamming power (P_j) around Bob (Bob's coordinates are $(-1, -1, -1)\ m$).

jamming is less effective, and γ_E is always greater than γ_M, and therefore we have no secure region. In this situation, Alice may decide not to transmit at all. Fig. 10 and Fig. 11 considered a jamming intensity of 2048 bits out of 16384 total and $\phi_{\frac{1}{2}} = 70°$.

The parametric analysis also evaluated the impact of varying the half power angle ($\phi_{\frac{1}{2}}$), as shown in Fig. 12. It was observed that an angle of 30°, that therefore concentrates the light more highly, makes jamming more effective and increases the size of the safe communication region compared to the region obtained with $\phi_{\frac{1}{2}} = 70°$. It is important to note that the choice of $\phi_{\frac{1}{2}}$ will still need to be weighted so that people do not see a bright spot on the floor due to a narrow-angle.

Fig. 13 presents the existence of the C_s as a function of the jamming optical power emitted by the legitimate receiver. It can be seen that the probability of the existence of the secrecy capability increases rapidly as the intensity of jamming increases.

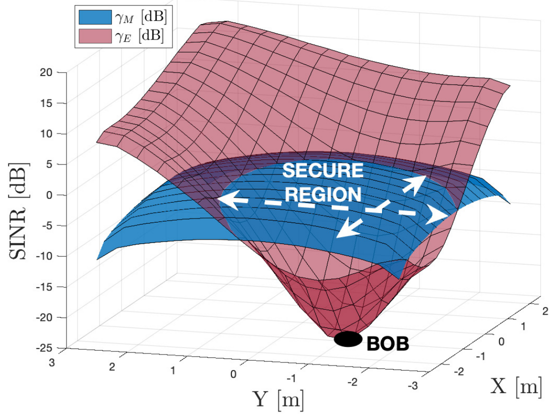

FIGURE 10: Secure region around Bob (i.e., the region where $\gamma_M > \gamma_E$) when Alice is close to the ceiling (i.e., her coordinates are $(0, 0, 2)\ m$) and Bob is close to the floor (i.e., his coordinates are$(-1, -1, -1)\ m$). Bob jams $M = 2048$ bits.

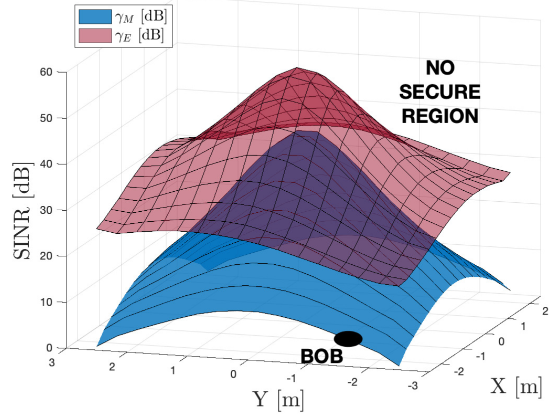

FIGURE 11: There is no secure region around Bob when Eve moves close to Alice. Eve is on the $(X, Y, 1)\ m$ plane, while Bob is on the floor and has coordinates $(-1, -1, -2)\ m$. Bob jams $M = 2048$ bits.

In Fig. 14 we plot the probability of outage (P_{out}) of the secrecy capacity for different Rayleigh channels conditions and secrecy rate (R_s) values. In all scenarios, we have that P_{out} rapidly decreases when jamming optical power increases.

VIII. CONCLUDING REMARKS

VLC is considered a key enabler technology for fast wireless communications. Such a kind of communication exploits the paradigm transmitting while illuminating. The availability of this free spectrum creates an opportunity for low-cost broadband communication that could alleviate spectrum congestion. This study shows that WBPLSec, a watermark-based VLC with a jamming receiver, can enhance devices'

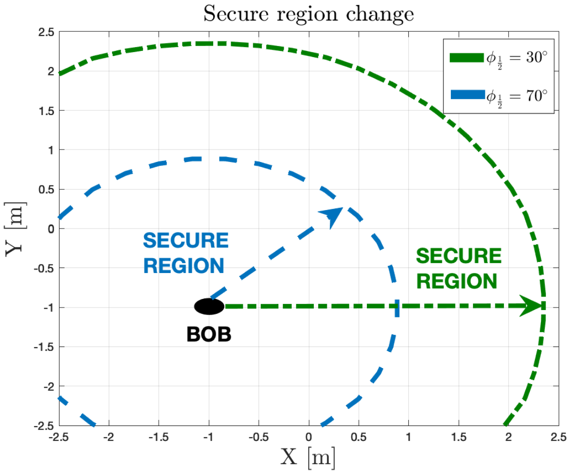

FIGURE 12: Variation of the secure region as $\phi_{\frac{1}{2}}$ changes.

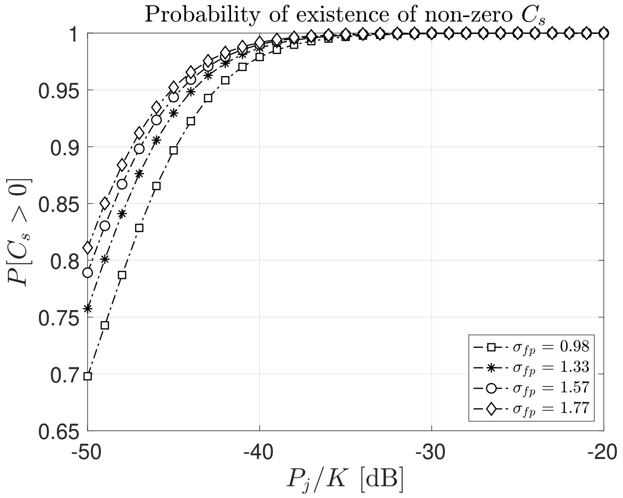

FIGURE 13: Existence of the secrecy capacity (C_s) as a function of the jamming power.

cybersecurity by implementing a physical layer standalone security solution. We computed closed-form expressions for the existence of the secrecy capacity and of its outage probability for a modified wiretap channel. Our approach offers legitimate receivers the possibility to create a *secure region* that guarantees confidential communication between them and the transmitters. Thus, exploiting this blind full-rate protocol, a legitimate receiver can, for example, exchange a secret shared key with a neighboring device in the same room by exploiting VLCs. Moreover, if the attacker was outside the security region created by Bob, the communication could be eavesdropped; in this case, Alice could still figure out if she is in a jamming coverage area and decide not to transmit at all.

We evaluated the robustness of our approach by considering attackers with continuous access to wireless networks and with the possibility of moving freely within rooms. We also considered that attackers' capabilities might change depending on their position relatively to the security region of interest.

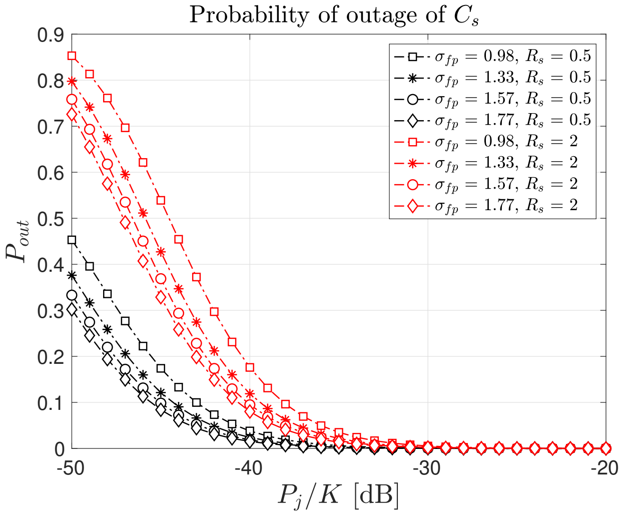

FIGURE 14: Outage probability of the secrecy capacity (P_{out}) versus the jamming power.

In such a scenario, we expect attacks like the followings:

- **Eavesdropping**: This attack aims at passively sniffing the communication to analyze it in a second moment to compromise future communication.
- **Message Injection Attack**: The goal of this attack is to send a customized and malicious message to Bob to compromise the communication between Alice and Bob.
- **Replay Attack**: This attack aims to reuse a previously transmitted and sniffed message in successive communication to replicate the legitimate transmission.
- **Message Modification**: In this case, the goal is to modify the message during transmission.

WBPLSec can indeed mitigate these attacks.

Confidentiality of messages is obtained thanks to the jamming phase, which allows only Bob to know the jamming points and consequently to reconstruct the message. This property allows preventing *eavesdropping*.

Replay protection is assured because Bob has randomly chosen and destroyed a part of the message, and with each subsequent communication, it will have different information and the distorted bits will also be different. This property will prevent any attempt by Eve to reuse an old message and thus avoid *message injection* and *replay attacks*.

Integrity of sent messages is guaranteed because a unique watermark for each transmission is added and in case the attacker tries to modify the watermarked message, Bob would notice an abnormal increase in the number of errors during the extraction of the watermark itself. This property prevents *message modification attacks*.

Finally, it is essential to note that the proposed algorithm is backward compatible with the technology used by VLCs. Alice can insert the watermark used only by a receiver that implements WBPLSec; otherwise, if the receiver does not implement this algorithm, the watermark will not be used, and the jamming will not be transmitted. Bob, for his part, does not assume to know Eve's position, and so when Bob jams, this interference is radiated identically in different directions creating precisely a secure region where Bob can communicate with Alice when Eve is within this area. Possible developments of this work may involve methods of targeting the light beam such that jamming is concentrated in areas of the room where the attacker is most likely to be located.

ACKNOWLEDGMENTS

The authors would like to thank Maurizio Angelo Bonuccelli for insightful comments that helped us to significantly improve the paper.

REFERENCES

[1] M. Katz, M. Matinmikko-Blue, and M. Latva-Aho, "6Genesis Flagship Program: Building the Bridges Towards 6G-Enabled Wireless Smart Society and Ecosystem," in 2018 IEEE 10th Latin-American Conference on Communications (LATINCOM), Nov 2018, pp. 1–9.

[2] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6g wireless communications: Vision and potential techniques," IEEE Network, vol. 33, no. 4, pp. 70–75, 2019.

[3] S. Amakawa, Z. Aslam, J. Buckwater, S. Caputo, A. Chaoub, Y. Chen, Y. Corre, M. Fujishima, Y. Ganghua, S. Gao, J. Grzyb, C. Han, G. JUe, J. Kokkoniemi, Z. Lai, Y. Li, M. Millhaem, I. Moerman, L. Mucchi, S. Myllymäki, R. Nichols, I. Ocket, M. Robertson, and M. Rodwell, "White paper on rf enabling 6g – opportunities and challenges from technology to spectrum," 6G Flagship, University of Oulu, no. 13, 2021.

[4] M. Ylianttila, R. Kantola, A. V. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T. H. Nguyen, F. Liu, T. M. Hewa, M. Liyanage, I. Ahmad, J. Partala, R. Abbas, A. Hecker, S. Jayousi, A. Martinelli, S. Caputo, J. Bechtold, I. Morales, R. Stoica, G. Abreu, S. Shahabuddin, E. Panayirci, H. Haas, T. Kumar, B. O. Ozparlak, and J. Röning, "6g white paper: Research challenges for trust, security and privacy," CoRR, vol. abs/2004.11665, 2020. [Online]. Available: https://arxiv.org/abs/2004.11665

[5] C. D. Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang, and M. Liyanage, "Survey on 6g frontiers: Trends, applications, requirements, technologies and future research," IEEE Open Journal of the Communications Society, vol. 2, pp. 836–886, 2021.

[6] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening New Horizons for Integration of Comfort, Security, and Intelligence," IEEE Wireless Communications, vol. 27, no. 5, pp. 126–132, 2020.

[7] P. Porambage, G. Gür, D. P. Moya Osorio, M. Livanage, and M. Ylianttila, "6g security challenges and potential solutions," in 2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit), 2021, pp. 622–627.

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

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

[10] A. Al-Kinani, C. Wang, L. Zhou, and W. Zhang, "Optical wireless communication channel measurements and models," IEEE Communications Surveys Tutorials, vol. 20, no. 3, pp. 1939–1962, thirdquarter 2018.

[11] "IEEE Standard for Local and metropolitan area networks–Part 15.7: Short-Range Optical Wireless Communications," IEEE Std 802.15.7-2018 (Revision of IEEE Std 802.15.7-2011), pp. 1–407, April 2019.

[12] C. Shannon, "Communication theory of secrecy systems," The Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, Oct 1949. [Online]. Available: https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[13] S. Soderi, L. Mucchi, M. Hämäläinen, A. Piva, and J. H. Iinatti, "Physical layer security based on spread-spectrum watermarking and jamming receiver." Trans. Emerging Telecommunications Technologies, vol. 28, no. 7, 2017. [Online]. Available: http://dblp.uni-trier.de/db/journals/ett/ett28.html#SoderiMHPI17

[14] S. Soderi, "Enhancing security in 6g visible light communications," in 2020 2nd 6G Wireless Summit (6G SUMMIT), 2020, pp. 1–5.

[15] X. You et al., "Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts," Science China Information Sciences, vol. 64, no. 1, p. 110301, 2020. [Online]. Available: https://doi.org/10.1007/s11432-020-2955-6

[16] E. Calvanese Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Ktenas, N. Cassiau, L. Maret, and C. Dehos, "6G: The Next Frontier: From Holographic Messaging to Artificial Intelligence Using Subterahertz and Visible Light Communication," IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 42–50, Sep. 2019.

[17] L. Cheng, W. Viriyasitavat, M. Boban, and H. Tsai, "Comparison of Radio Frequency and Visible Light Propagation Channels for Vehicular Communications," IEEE Access, vol. 6, pp. 2634–2644, 2018.

[18] 6G Flagship Program. [Online]. Available: https://www.oulu.fi/6gflagship/

[19] B. Aazhang, P. Ahokangas, H. Alves, M.-S. Alouini, J. Beek, H. Benn, M. Bennis, J. Belfiore, E. Strinati, F. Chen, K. Chang, F. Clazzer, S. Dizit, K. DongSeung, M. Giordiani, W. Haselmayr, J. Haapola, E. Hardouin, E. Harjula, and P. Zhu, "Key drivers and research challenges for 6g ubiquitous wireless intelligence (white paper)," 09 2019.

[20] S. Soderi, "Acoustic-based security: A key enabling technology for wireless sensor networks," International Journal of Wireless Information Networks, 2019. [Online]. Available: https://doi.org/10.1007/s10776-019-00473-4

[21] G. Cossu, A. Khalid, P. Choudhury, R. Corsini, and E. Ciaramella, "3.4 Gbit/s visible optical wireless transmission based on RGB LED," Optics express, vol. 20, pp. B501–6, 12 2012.

[22] S. Pergoloni, A. Petroni, T.-C. Bui, G. Scarano, R. Cusani, and M. Biagi, "ASK-based spatial multiplexing RGB scheme using symbol-dependent self-interference for detection," Opt. Express, vol. 25, no. 13, pp. 15 028–15 042, Jun 2017. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-25-13-15028

[23] S. Rehman, S. Ullah, P. Chong, S. Yongchareon, and D. Komosny, "Visible Light Communication: A System Perspective—Overview and Challenges," Sensors, vol. 19, p. 1153, 03 2019.

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

[25] A. Kaul and J. Gupta, "Revolutionary 6g: Technologies, architecture, coverage, and performance," in 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2021, pp. 1–6.

[26] H. Haas, L. Yin, Y. Wang, and C. Chen, "What is lifi?" Journal of Lightwave Technology, vol. 34, no. 6, pp. 1533–1544, March 2016.

[27] S. Dimitrov and H. Haas, Principles of LED Light Communications: Towards Networked Li-Fi. Cambridge University Press, March 2015. [Online]. Available: https://elib.dlr.de/95588/

[28] B. Zhu, J. Cheng, Y. Wang, J. Yan, and J. Wang, "Three-dimensional vlc positioning based on angle difference of arrival with arbitrary tilting angle of receiver," IEEE Journal on Selected Areas in Communications, vol. 36, no. 1, pp. 8–22, 2018.

[29] B. Zhu, Z. Zhu, Y. Wang, and J. Cheng, "Optimal optical omnidirectional angle-of-arrival estimator with complementary photodiodes," Journal of Lightwave Technology, vol. 37, no. 13, pp. 2932–2945, 2019.

[30] A. R. Ndjiongue, T. M. N. Ngatched, O. A. Dobre, and H. Haas, "Toward the use of re-configurable intelligent surfaces in vlc systems: Beam steering," IEEE Wireless Communications, vol. 28, no. 3, pp. 156–162, 2021.

[31] ——, "Re-configurable intelligent surface-based vlc receivers using tunable liquid-crystals: The concept," J. Lightwave Technol., vol. 39, no. 10, pp. 3193–3200, May 2021. [Online]. Available: http://www.osapublishing.org/jlt/abstract.cfm?URI=jlt-39-10-3193

[32] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press, 2011.

[33] S. Mathur, M. Narayan, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in In MobiCom '08, 2008, pp. 128–139.

[34] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments," in Proceedings of the 15th Annual International Conference on Mobile Computing and Networking, ser. MobiCom '09. New York, NY, USA: ACM, 2009, pp. 321–332. [Online]. Available: http://doi.acm.org/10.1145/1614320.1614356

[35] H. Jeon, N. Kim, M. Kim, H. Lee, and J. Ha, "Secrecy capacity over correlated ergodic fading channel," in IEEE Military Communications Conference, 2008. MILCOM 2008., Nov 2008, pp. 1–7.

[36] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. Schmitt, "Detection of Reactive Jamming in DSSS-based Wireless Communications," IEEE Transactions on Wireless Communications,, vol. 13, no. 3, pp. 1593–1603, March 2014.

[37] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," IEEE Transactions on Wireless Communications,, vol. 8, no. 10, pp. 5003–5011, October 2009.

[38] J. Vilela, M. Bloch, J. Barros, and S. McLaughlin, "Wireless Secrecy Regions With Friendly Jamming," IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 256–266, June 2011.

[39] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in 2011 Proceedings IEEE INFOCOM,, April 2011, pp. 1125–1133.

[40] B. W. Lampson, "A Note on the Confinement Problem," Commun. ACM, vol. 16, no. 10, pp. 613–615, Oct. 1973. [Online]. Available: http://doi.acm.org/10.1145/362375.362389

[41] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," Proceedings of the IEEE, vol. 87, no. 7, pp. 1062–1078, 1999.

[42] M. Hanspach and M. Goetz, "On Covert Acoustical Mesh Networks in Air," CoRR, vol. abs/1406.1213, 2014. [Online]. Available: http://arxiv.org/abs/1406.1213

[43] G. Bernieri, S. Cecconello, M. Conti, and G. Lain, "Tambus: A novel authentication method through covert channels for securing industrial networks," Computer Networks, vol. 183, p. 107583, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128620312214

[44] S. Wendzel and J. Keller, "Design and implementation of an active warden addressing protocol switching covert channels," in Proc. 7th International Conference on Internet Monitoring and Protection (ICIMP 2012). IARIA, 2012, pp. 1–6.

[45] X. Wu and H. Haas, "Handover skipping for lifi," IEEE Access, vol. 7, pp. 38 369–38 378, 2019.

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

[47] A. Mostafa and L. Lampe, "Enhancing the security of vlc links: Physical-layer approaches," in 2015 IEEE Summer Topicals Meeting Series (SUM), 2015, pp. 39–40.

[48] X. Liu, X. Wei, L. Guo, and Y. Liu, "SecLight: A New and Practical VLC Eavesdropping-Resilient Framework for IoT Devices," IEEE Access, vol. 7, pp. 19 109–19 124, 2019.

[49] S. Cho, G. Chen, and J. P. Coon, "Securing visible light communications with spatial jamming," in ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–6.

[50] 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 Transactions on Communications, vol. 66, no. 9, pp. 4087–4102, 2018.

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

[52] T. V. Pham and A. T. Pham, "Energy-efficient friendly jamming for physical layer security in visible light communication," in 2021 IEEE International Conference on Communications Workshops (ICC Workshops), 2021, pp. 1–6.

[53] W.-Y. Chu, T.-G. Yu, Y.-K. Lin, S.-C. Lee, and H.-C. Hsiao, "On using camera-based visible light communication for security protocols," in 2020 IEEE Security and Privacy Workshops (SPW), 2020, pp. 110–117.

[54] E. Panayirci, A. Yesilkaya, T. Cogalan, H. V. Poor, and H. Haas, "Physical-layer security with optical generalized space shift keying," IEEE Transactions on Communications, vol. 68, no. 5, pp. 3042–3056, 2020.

[55] H. Le Minh, A. T. Pham, Z. Ghassemlooy, and A. Burton, "Secured communications-zone multiple input multiple output visible light communications," in 2014 IEEE Globecom Workshops (GC Wkshps), 2014, pp. 505–511.

[56] Y. M. Al-Moliki, M. T. Alresheedi, Y. Al-Harthi, and A. H. Alqahtani, "Robust lightweight channel-independent ofdm-based encryption method for vlc-iot networks," IEEE Internet of Things Journal, pp. 1–1, 2021.

[57] H. Abumarshoud, L. Mohjazi, O. A. Dobre, M. Di Renzo, M. A. Imran, and H. Haas, "Lifi through reconfigurable intelligent surfaces: A new frontier for 6g?" IEEE Vehicular Technology Magazine, pp. 2–11, 2021.

[58] A. Mostafa and L. Lampe, "Physical-layer security for miso visible light communication channels," IEEE Journal on Selected Areas in Communications, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.

[59] A. Ramirez-Aguilera, J. Luna-Rivera, V. Guerra, J. Rabadan, R. Perez-Jimenez, and F. Lopez-Hernandez, "A review of indoor channel modeling techniques for visible light communications," in 2018 IEEE 10th Latin-American Conference on Communications (LATINCOM), 2018, pp. 1–6.

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

[61] V. Jungnickel, V. Pohl, S. Nonnig, and C. von Helmolt, "A physical model of the wireless infrared communication channel," IEEE Journal on Selected Areas in Communications, vol. 20, no. 3, pp. 631–640, 2002.

[62] A. R. Ndjiongue, T. M. N. Ngatched, and H. C. Ferreira, "Access Telecommunication Systems Using VLC Technology: Cascaded LD-LED Channel Analysis," in 2018 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 1–6.

[63] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[64] I. J. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673–1687, Dec 1997. [Online]. Available: https://doi.org/10.1109/83.650120

[65] J. G. Proakis, Digital communications, 4th ed. Boston: McGraw-Hill, 2000. [Online]. Available: http://www.loc.gov/catdir/description/mh021/00025305.html

[66] H. Malvar and D. Florencio, "Improved spread spectrum: a new modulation technique for robust watermarking," IEEE Transactions on Signal Processing, vol. 51, no. 4, pp. 898–905, Apr 2003.

[67] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," in 2006 IEEE International Symposium on Information Theory, July 2006, pp. 356–360.

• • •