Abstract—Visible Light Communication (VLC) is one of the most promising enabling technology for future 6G networks to overcome Radio-Frequency (RF)-based communication limitations thanks to a broader bandwidth, higher data rate, and greater efficiency. However, from the security perspective, VLCs suffer from all known wireless communication security threats (e.g., eavesdropping and integrity attacks). For this reason, security researchers are proposing innovative Physical Layer Security (PLS) solutions to protect such communication. Among the different solutions, the novel Reflective Intelligent Surface (RIS) technology coupled with VLCs has been successfully demonstrated in recent work to improve the VLC communication capacity. However, to date, the literature still lacks analysis and solutions to show the PLS capability of RIS-based VLC communication.

In this paper, we combine watermarking and jamming primitives through the Watermark Blind Physical Layer Security (WBPLSec) algorithm to secure VLC communication at the physical layer. Our solution leverages RIS technology to improve the security properties of the communication. By using an optimization framework, we can calculate RIS phases to maximize the WBPLSec jamming interference schema over a predefined area in the room. In particular, compared to a scenario without RIS, our solution improves the performance in terms of secrecy capacity without any assumption about the adversary’s location. We validate through numerical evaluations the positive impact of RIS-aided solution to increase the secrecy capacity of the legitimate jamming receiver in a VLC indoor scenario. Our results show that the introduction of RIS technology extends the area where secure communication occurs and that by increasing the number of RIS elements the outage probability decreases.

Index Terms—RIS, Physical Layer Security, VLC, Jamming, Watermarking, 6G.

I. INTRODUCTION

The amount of traffic data in 2021 is estimated at around 235.7 Exabytes per month, while in 2016 was estimated at around 73.1 Exabytes per month [1]. To manage this great amount of data, the traditional RF communication is inefficient and unable to satisfy the high-demand [2]. For this reason, the scientific community is exploring innovative technology to manage traffic demand. Recent technologies include the most famous 5G and its possible successor, 6G. In this context, VLC is a communication medium that obtained great attention as enabling technology for 5G and beyond. Currently we can find application of VLCs in many different sectors, spacing from smart home devices [3], vehicle-to-vehicle communication [4] and underwater communication [5].

Differently from RF, the potential of VLC is that it offers an higher data rate [6], high speed and robustness against interference [7], a large available frequency spectrum [8], and a low cost implementation thanks to Light Emitting Diodes (LEDs) [9]. Furthermore, VLC operates within the spectrum of visible light and uses light for both illumination and data transmission. However, VLCs present different challenges to achieving an optimal transmission. Signal loss and poor detection are often observed when transferring data at long distances and Non-Line-Of-Sight (NLOS). Moreover, this can also occur when transferring data at short ranges with line-of-sight when the photodetector is not angled toward the incident light. To capture and steer the VLC, generally, receivers are equipped with a convex lens that cannot dynamically steer the incident light beam. This helps the receiver reduce signal loss and improve detection performance. Modern receivers are equipped with a mechanism to dynamically steer the incoming beam, such as stretching a flexible matrix containing dielectric nano-resonators or ultra-fast switching of mie-resonant silicon nanostructure. However, all these methods have a weak effect on the refracted beam, even at high optical intensity [10].

To increase the quality of the received beam, recent works are investigating the implementation of RIS element [11]. RIS is a novel technology that implements electronically configurable physical characteristics, which can be obtained by varying the temperature of a nano-cell or re-orientating Liquid-Crystal alignment based on induced electrical field. The configurable characteristic of such technology allows obtaining great advantages in a wide range of applications. Proposals of RIS application include unmanned aerial vehicles [12] and autonomous vehicles [13].

Motivation. The use of VLCs in an indoor environment is considered safer than radio-based technology [14]. Due to the directivity of the optical signals and their high obstacles’ impermeability, it is harder to intercept them from the outside. Therefore, it is less prone to the typical threats of wireless communication such as jamming or eavesdropping. Furthermore, the RIS permits extremely efficient VLCs signal propagation redirection at very little power consumption since varactor diodes can apply a phase shift or absorb the incoming signal in a real-time reconfigurable manner.

Therefore, the advantages RIS can overcome some of the limitations of VLC. Recent studies proved that RIS can also...
improve the VLC communication performance [15], [11] from different point of view. However, RIS is a novel technology, and its application in VLC has only been proposed in some preliminary works, and it has been only initially explored.

**Contribution.** In this work, we propose a communication framework to increase the secrecy VLC communication at the physical layer. To do this, we implement the WBPLSec algorithm in RIS-aided VLC communication. WBPLSec has been successfully implemented in different type of communication, including VLC [16]. WBPLSec combines watermarking and jamming primitives at the receiver to achieve different security properties, including confidentiality, integrity, and anti-replay. To maximize the jamming interference obtained with RIS phases, we design and present an optimization framework that does not make any assumption on the attacker position. Our results highlight the positive impact of the RIS technology to increase the secrecy capacity.

We summarize the contribution of our paper as follows:

- We present a mechanism that leverages WBPLSec algorithm to secure VLC communication at the physical layer and improve the security properties through RIS.
- We validate our framework through numerical simulations, showing the positive impact of RIS in terms of the secrecy capacity even without any assumption about the adversary’s location.
- We show how our mechanism allows achieving different security properties, including replay attack resistance, high confidentiality, and message integrity, enabling the protection of several threats.

**Organization.** The remainder of the paper is organized as follows. Section II briefly recalls the concepts useful for understanding the paper, while Section III discusses the related works. Section IV describes the system model considered. Then, Section V introduces the our optimization framework and Section VI presents the results of the simulations. Section VII discusses the security properties we achieve with our mechanism. Finally, Section VIII concludes the paper by discussing our findings and the current framework limitations.

## II. BACKGROUND

In this section we briefly introduce the concepts useful to understand the reminder of the paper. In particular in Section II-A we summarize the VLC channel model, in Section II-B we recall the RIS technology, and in Section II-C we detail of the WBPLSec algorithm.

### A. VLC Channel Model

VLCs utilize the Intensity Modulation (IM) scheme along with Direct-Detection (DD). The desired illumination level is maintained on the transmitter side by setting the appropriate Direct-Current (DC) bias of the overall signal fed into the LED. On the other side, the received signal is proportional to the optical power that arrives at the photodiode. An internal VLC channel consists of two main components: the LOS channel and the diffuse channel. The first component considers the contribution of light directly hitting the photodiode without bouncing off other objects. The second component, also known as NLOS, includes all light rays that bounce off obstacles in the room. This article considers only the LOS component (see Figure 1). Assuming to have Lambertian light sources, the LOS component of the channel DC gain, i.e. \( H(0) = \int_{-\infty}^{\infty} h(t) dt \), between one LED and one photodiode is given by [17]

\[
H_d(0) = \begin{cases} 
\frac{Ar(m+1)R}{2\pi d_q^2 \sigma^2} D(\psi) \cos^m(\phi) \cos(\psi), & |\psi| \leq \psi_{FOV} \\
0, & |\psi| > \psi_{FOV}
\end{cases}
\]

where \( A_r \) is the receiver collection area, \( R \) is the photodiode responsivity, \( m = -\ln(2)/\ln(\cos(\phi_{1/2})) \) is the order of the Lambertian emission with half irradiance at \( \phi_{1/2} \), \( \phi \) 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 photodiode, \( \psi \) is the angle of incidence (\( \psi \in \{\psi_E, \psi_B\} \)), and \( \psi_{FOV} \) is the receiver’s angle Field-Of-View (FOV).

The total received power for Alice with one RGB LED, for a given transmission power \( P_t \), is given by the DC channel on the directed path, i.e. \( P_r = P_t \cdot H_d(0) \).

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

\[
\gamma_v = H_z^2(0) P_t / \sigma^2
\]

where \( P_t \) is the transmitted optical power, \( H_d(0) \) is the channel DC gain and \( \sigma^2 \) is the spectral density of the background noise.

In terms of reflections on the RIS, we can define the channel DC gain of the first reflection as follows

\[
dH_{ref}(0) = \begin{cases} 
\frac{Ar(m+1)R}{2\pi d_q^2 \rho d_B} D(\psi) p dA_w \cos^m(\phi) \cdot \cos(\alpha) \cos(\beta) \cos(\psi), & |\psi| \leq \psi_{FOV} \\
0, & |\psi| > \psi_{FOV}
\end{cases}
\]

where \( \rho \) denotes the reflection coefficient, \( dA_w \) represents the emission area of a micro surface, \( \alpha \) expresses the incidence angle of a reflection point and \( \beta \) is the radiation angle of the receiver.
To simplify the mathematical treatment in the remainder of the paper we will denote by $h$ instead of $H_d(0)$, the coefficients of the VLC channel.

B. Reflective Intelligent Surfaces

A RIS provides a re-configurable reflection channel that can be exploited, among the others, to suitably direct signals in predefined directions. We adopt the RIS model in [18], where each element of the RIS acts as a mirror reflecting light in a suitably selected direction. As VLC highly depend on the existence of a LOS channel, thanks to RIS it is possible to relax this condition. Furthermore, RIS can serve the same function a beamformer serves in classical RF communications, hence creating suitably combined signals [18]. The main advantage of RIS is that it is passive, hence minimizing the overall system power requirements. In this paper, we model the signal reflected by the RIS via the NLOS VLC channel (2).

C. WBPLSec Standalone Security Solution

WBPLSec algorithm utilizes a jamming receiver in conjunction with a Spread-Spectrum (SS) watermarking technique. As a standalone security solution for sensor networks, this technology has received considerable attention in recent years. WBPLSec has been successfully applied in different context, including wireless communication [19] and acoustic communication [20]. With this technique, the legitimate receiver creates a security region around itself by leveraging jamming, enabling communication with a high degree of confidentiality under certain conditions. More precisely, to make jamming effective, the communication channel must allow for intentionally interfering with data transmission. Communication channels with possible transmission collision are most likely to fit this condition, e.g., wireless networks. Secondly, network receiver nodes must be equipped with at least one transmitter and one receiver, which can be used simultaneously.

VLC Application Domain. The WBPLSec protocol has been recently proposed to achieve confidentiality in VLC [16]. In that case, watermarking and jamming are combined in WBPLSec to provide a standalone security solution in 6G networks. That solution does not include the use of any RIS, which is the subject of this paper. There are several ways to implement VLC. The one that uses RGB LEDs provides the most bandwidth since it also uses three independent channels. Suppose an architecture that uses RGB LEDs to implement WBPLSec on VLC depicted in Figure 2(a).

Let’s consider the case that Alice wants to send a secret message of $N$ bits $(x_S)^N$ to Bob. Alice transmits the watermarked signal $(x_S^w)^N$ using an RGB LED. Bob receives the message through a single RGB color-tuned photodiode, but he jams $M$ ($M < N$) bits of the Alice’s VLC $(x_J)^M$ using an RGB LED while receiving it. Eve, the eavesdropper, may use multiple PDs to violet secrecy. The scheme proposed [16] (see Figure 2(a)) exploits three RGB independent channels and uses a Wavelength Division Multiplexing (WDM) to watermark the VLC. It relies on four main actions: (i) SS watermarking: part of the secret the message, i.e., $N_W$ of $N$ bits, are first modulated with a spreading sequence to create the watermark signal $(w)^{NW}$ and then transmitted by using only the red light; (ii) jamming receiver: Bob jams Alice’s message using RGB LED; (iii) selective jamming: Bob jams only part of the on-the-way message, and he can rebuild the clean message by knowing the jammed part. The jamming does not affect the SS watermark [21]; (iv) communication hiding: the proposed method transmits information through two independent paths using blue and red lights. The first is the narrow-band Amplitude Shift Keying (ASK) signal transmitted through the blue light, i.e., $(x_B)^N$. At the same time, the SS watermark signal uses the red light $(w)^{NW}$ and creates, in this way, a covert channel.

It is worth noting that compared to applying WBPLSec in RF wireless communications, in the case of RGB LED-based VLcs, SS watermarking and jamming primitives can be implemented without requiring additional transceivers.

III. RELATED WORKS

VLC is a widely studied topic in literature. Different studies aim at implementing this type of communication in different fields, such as Vehicle-To-Vehicle networks [4] or underwater communication [22]. The wide diffusion and application of VLC have raised the attention of the security community to investigate the vulnerabilities of such a medium. Different works investigate the physical layer security of VLC [23] focusing on different properties. The different proposals to deal with PLS in VLC include beamforming [24], [25], friendly jamming [26], [27], and signal mapping [28], [29].
However, these works focus on the traditional implementation of VLC communication.

Among the different enabling technologies used in the VLC context, RIS represents a very recent and promising technology to improve the wireless communication performances [11]. In this paper we specifically focus on the security of VLC in RIS application from the PLS point of view.

Although different works propose the integration on RIS in different fields (e.g., Unmanned Aerial Vehicles (UAV) [12]), there is a lack of study on the security properties of this new technology. The integration of RIS with attributes was studied in [30], which particularly focus on the LiFi application of VLC. Here the authors discussed how RIS can improve different PLS properties such as Secrecy capacity, jamming protection, and secure beamforming. However, the paper does not inspect the security topic deeply and does not provide secrecy capacity estimation. In [31] the authors propose a mechanism which implement RIS to improve the UAVs communication security through alternating optimization technique. The paper also demonstrates that the proposed algorithm improves the average secrecy rate compared with other benchmark algorithms.

Differently from previous work we aim at implementing RIS and WBPLSec protocol [19] to improve the PLS of VLC communication (see Figure 2(b)). This technique was already applied on different communication means such as radio frequency [19], acoustic communications [20] showing the improvement of performances from the secrecy capacity of the channel point of view. We show that the integration of RIS in VLC communication allows WBPLSec to achieve even better performance than is a non RIS-aided VLC communication [16]. We then discuss the benefits of introducing WBPLSec in the communication and the security properties that it introduces in the communication.

IV. SYSTEM MODEL

Let us consider the scenario depicted in Figure 3. The legitimate user, Alice, transmits \( (x_j)^N \) to the legitimate receiver, \( Bob \), through the main channel. A malicious eavesdropper, Eve, receives this signal through the wiretap channel. In our model, Bob is equipped with a jammer that generates a jamming signal to degrade the quality of the main channel by applying WBPLSec. Bob hence simultaneously receives Alice’s signal and controls the jamming signal. We assume that the jammer transmits a signal \( (x_j)^M \) and exploits a RIS to suitably select the jamming signal direction. We denote as \( h_{JR} \in \mathbb{R}^{K \times 1} \) the channel between the jammer and the RIS. The reflected signal impacts both on the signal received by Bob and Eve. Let us denote as \( h_{RB} \in \mathbb{R}^{1 \times K} \) and \( h_{RE} \in \mathbb{R}^{1 \times K} \) the channel from the RIS to Bob and from the RIS to Eve, respectively. The reflected channel is given by the NLOS channel (2).

Therefore the jamming signal at Bob can be computed as

\[
y_{JB}(\delta) = h_{RB}(\delta)h_{JR}x_j, \quad (3)
\]

whereas the received jamming signal at Eve as

\[
y_{JE}(\delta) = h_{RE}(\delta)h_{JR}x_j, \quad (4)
\]

where \( \delta = [\delta_1, \ldots, \delta_K] \) denotes the yaw angle of the each RIS element, as described in [18].

In accordance with the WBPLSec applied to VLCs [16], considering both the useful signal and the jamming signal, the signal received by Bob and Eve are respectively:

\[
y_M = h_B x_S + y_{JB}(\delta) + n_M, \quad (5)
\]

\[
y_E = h_E x_S + y_{JE}(\delta) + n_E, \quad (6)
\]

where \( h_B \) and \( h_E \) are the channel’s gains between Alice with Bob and Eve respectively, \( x_S \) is Alice’s watermarked data signal, and \( n_M \) and \( n_E \) are the complex zero-mean Gaussian noise with variance \( \sigma_M^2 \) and \( \sigma_E^2 \), respectively. Notice that we neglected the noise terms in (3) and (4) to only consider it once in the overall received signals in (5) and (6).

Given the received signals, we can define the Signal-to-Interference Plus Noise Ratio (SINR) at Bob’s side as

\[
\gamma_M = \frac{|h_B|^2P_i^2}{\sigma_M^2 + |y_{JB}|^2P_j^2}. \quad (7)
\]

The SINR at Eve’s side is given by

\[
\gamma_E = \frac{|h_E|^2P_i^2}{\sigma_E^2 + |y_{JE}|^2P_j^2}. \quad (8)
\]

We assume that \( \mathbb{E}[|x_S|^2] = 1 \). Furthermore, assuming that \( \mathbb{E}[|x_j|^2] = 1 \), the interference component is given by

\[
\mathbb{E}[|y_{JB}|^2] = \mathbb{E}[|h_{RE}\Theta h_{BR}|^2]. \quad (9)
\]

Secrecy Capacity.

The idea we develop in this paper is to exploit the RIS configuration properties to improve the system performance given by WBPLSec in terms of information confidentiality. The secrecy capacity of the legitimate link for non-degraded Gaussian wiretap channels [32], [33] is a widely accepted
metric for confidentiality at the physical layer. It can be defined as
\[
C_s = \max \{C_M - C_E, 0\} = \begin{cases} 
\frac{1}{2} \log_2 \frac{1+\gamma_M}{1+\gamma_E}, & \text{if } \gamma_M > \gamma_E, \\
0, & \text{if } \gamma_M \leq \gamma_E.
\end{cases}
\tag{10}
\]
where \(C_M = \log_2 (1+\gamma_M)\) is the channel capacity from Alice to Bob, i.e. the main channel, and \(C_E = \log_2 (1+\gamma_E)\) is the channel capacity from Alice to Eve, i.e. the wiretap channel exploited by the eavesdropper.

**Area Secrecy Capacity.**

Although secrecy capacity provides a measure of confidentiality, in some scenarios, it relies on the limiting assumption that the location of Eve is known. To remove this assumption, we propose the use of area secrecy capacity [34], which defines the average secrecy capacity over a predefined area. We denote as \(A \in \mathbb{R}^3\) the area of interest, and as \(C_E(a), \gamma_E(a)\) as the channel capacity and the SINR for an eavesdropper at location \(a \in A\). By denoting as \(|A|\) the area value of \(A\), we define the area secrecy capacity as
\[
C_s(A) = \frac{1}{|A|} \int_A \{\max\{C_M - C_E(a), 0\}\} da = \begin{cases} 
\frac{1}{2|A|} \int_A \log_2 \frac{1+\gamma_M}{1+\gamma_E(a)}, & \text{if } \gamma_M > \gamma_E(a), \\
0, & \text{if } \gamma_M \leq \gamma_E(a).
\end{cases}
\tag{11}
\]
The area secrecy capacity provides a sub-optimal metric as, compared to the secrecy capacity in (10), it does not consider the actual Eve’s channel. Instead, it exploits an average estimation of the punctual secrecy capacities obtained over hypothetical Eve’s locations over an area of interest. However, by removing the assumption on Eve’s location, this metric provides high generalization and applicability to those scenarios where the estimation of Eve’s location is challenging.

**V. RIS-ADDED JAMMING OPTIMIZATION**

In this section, we define the optimization problem to obtain the RIS phases configurations that maximizes the communication secrecy. To show the advantages obtained using the area secrecy capacity to avoid assuming a known eavesdropper location, we provide the solution of two different problems: i) optimization with known Eve location (Section V-A), and ii) optimization with unknown Eve location (Section V-B).

**A. Known Eve Location**

Assuming a known Eve location, we achieve the best communication secrecy by maximizing the secrecy capacity (10), through the adjustment of RIS phases. Therefore, we define the following problem
\[
\max_{\Theta} C_s, \tag{12a}
\]
\[\text{s.t. } \theta_k \in [0, 2\pi], \forall k = 1, \ldots, K. \tag{12b}\]
Notice that we only optimize the phases of the RIS as we are dealing with a single-receiver scenario. Therefore the optimal value of \(C_s\) is achieved via maximal power transmission.

Regarding the jamming power \(P_j\), the best results would be achieved by choosing the maximum available power. However, we investigate via numerical evaluation the impact of \(P_j\).

Problem (12) is non-convex [35], and finding the optimal solutions is a complicated task. However, we noticed that, thanks to the application of WBPLSec, we can remove the interference component of (7) similarly to what is commonly done in the literature in successive interference cancellation [36]. We can hence write the SNR at Bob’s side as
\[
\hat{\gamma}_M = \frac{|h_{BE}|^2 P_j^2}{\sigma_B^2}, \tag{13}\]
and modify the secrecy capacity in (10) as
\[
\hat{C}_s = \begin{cases} 
\frac{1}{2} \log_2 \frac{1+\hat{\gamma}_M}{1+\gamma_E}, & \text{if } \gamma_M > \gamma_E, \\
0, & \text{if } \gamma_M \leq \gamma_E.
\end{cases} \tag{14}
\]

Thanks to the interference removal capacity of WBPLSec, Bob’s spectral efficiency is now independent from the RIS phases, and can hence be removed from the optimization problem (12), which can hence be rewritten as
\[
\max_{\Theta} \frac{1}{2} \log_2 (1 + \gamma_E), \tag{15a}
\]
\[\text{s.t. } \theta_k \in [0, 2\pi], \forall k = 1, \ldots, K; \tag{15b}\]
where we can rewrite the objective function (15a) as
\[
\min_{\Theta} \log_2 (1 + \gamma_E), \tag{16}\]
where we neglected the term 1/2 as it is constant.

From (16) we see that our goal is now the minimization of the SNR at Eve’s side. Considering that the variables of (15) are the components of matrix \(\Theta\) uniquely present at the denominator of (8), we can rewrite problem (15) as
\[
\max_{\delta} |h_{jc}^{\delta_\delta}(\delta)|^2, \tag{17a}
\]
\[\text{s.t. } \delta_k \in [0, 2\pi], \forall k = 1, \ldots, K. \tag{17b}\]

Problem (17) is non-convex, therefore it is difficult to find an optimal solution. We propose the use of Particle Swarm Optimization (PSO), a population-based optimization technique, to find the best solution [37]. Due to space constraint we do not provide a technical description of PSO. The interested reader can refer to [37], [38] for more details and examples.

**B. Unknown Eve Location**

In real-life scenarios, the location of Eve can be unknown to the jammer. Therefore, it is not possible to optimally configure the RIS to convey the jamming signal towards Eve. To circumvent this problem, instead of optimizing the secrecy capacity over a single known Eve location, we define a grid of possible Eve locations distributed over a predefined area of interest \((A)\). In this case, the objective function of our optimization problem is given by the area secrecy capacity in (11), and problem (12) can be rewritten as
\[
\max_{\Theta} C_s(A). \tag{18a}\]
s.t. \( \theta_k \in [0, 2\pi], \forall k = 1, \ldots, K. \) \hspace{1cm} (18b)

In this case, the objective of the optimization problem is to find a configuration of the RIS that provides the best trade-off among the secrecy capacities obtained, considering the possible Eve’s locations over \( \mathcal{A} \). As in problem (12), we set as variable matrix \( \Theta \) and do not consider power optimization due to the same previously discussed motivations.

Without loss of generality, to simplify problem (18) from a computational perspective, we replace the continuous area among the secrecy capacities obtained evaluating the possible Eve’s locations over \( \mathcal{A} \). As in problem (12), we set as variable matrix \( \Theta \) and do not consider power optimization due to the same previously discussed motivations.

Applying the same considerations on the effect of WBPLSec on Bob’s SINR and on the dependencies of variables we outlined in Section V-A, we can rewrite problem (18) as

\[
C_s(\mathcal{A}) = \frac{1}{|\mathcal{A}|} \sum_{a \in \mathcal{A}} \max\{C_M - C_E(a), 0\} =
\begin{cases}
\frac{1}{|\mathcal{A}|} \sum_{a \in \mathcal{A}} \log_2 \frac{1 + \gamma_M}{1 + \gamma_E(a)}, & \text{if } \gamma_M > \gamma_E(a), \\
0, & \text{if } \gamma_M \leq \gamma_E(a).
\end{cases}
\]

\hspace{1cm} (19)

Applying the same considerations on the effect of WBPLSec on Bob’s SINR and on the dependencies of variables we outlined in Section V-A, we can rewrite problem (18) as

\[
\min_{\Theta} \sum_{a \in \mathcal{A}} \log_2(1 + \gamma_E(a)) \hspace{1cm} (20a)
\]

s.t. \( \theta_k \in [0, 2\pi], \forall k = 1, \ldots, K. \) \hspace{1cm} (20b)

The resulting problem (20) is non-convex, and it is hence difficult to find an optimal solution. Also in this case, we resort to PSO to efficiently find the best solution [37].

VI. Simulations Results

Table I reports the parameters used for the parametric analysis, including the transmitted power, the jamming intensity, and the orientation of the transmitter and receiver. The LEDs used by Alice, Bob, and Eve are identical in their characteristics.

For simulations, we assumed Alice was installed on the roof, while Bob and Eve could freely move within the room.

To validate our proposed approach, we designed a MATLAB-based simulator to solve problems (17) and (20), where we considered the indoor scenario with parameters reported in Table I. With the architecture proposed (see Figure 4), Bob’s jammer is installed close to the RIS and the jamming channel cannot be described using (1) that is valid only in the far-field region. For this reason, we assume that \( P_j \) undergoes a deterministic path-loss attenuation in the near-field region at the RIS. For both known and unknown Eve’s location cases, we fix the location of Alice, Bob, the jammer, and the RIS, while we consider a grid \( \mathcal{N} \) of Eve’s locations.

We validate our approach based on two different metrics: the secrecy capacity (14) achieved at each Eve’s location and the outage probability defined as

\[
P_{\text{out}} = \frac{\sum_{n \in \mathcal{N}} \mathbb{I}(\hat{C}_s(n) - T_h \cdot \hat{C}_s|_{\text{max}}) \leq 0}{|\mathcal{N}|},
\]

where \( \hat{C}_s|_{\text{max}} = \max_{n \in \mathcal{N}} \hat{C}_s(n) \), \( |\mathcal{N}| \) denotes the cardinality of \( \mathcal{N} \), \( T_h \in [0, 1] \) is a variable we select to define the secrecy capacity threshold, and \( \mathbb{I} \) is the indicator function

\[
\mathbb{I}(x) = \begin{cases} 1, & \text{if } x \geq 0; \\
0, & \text{otherwise}. \end{cases}
\]

In other words, the outage probability (21) provides, given a selected \( T_h \), the fraction of points over Eve’s grid of location where we achieve a secrecy capacity higher or equal than the \( T_h \) percent of the highest achievable secrecy capacity \( C_{\text{max}} \).

Notice that we use the secrecy capacity (14) for both known and unknown Eve’s location cases. When Eve’s location is known, this metric choice is trivial. When we solve the optimization problem without knowing Eve’s location, the RIS phases direct the jamming to an area where we assume the adversary is. However, this might include the case where the area of interest does not include Eve’s actual location.

This represents a worst-case scenario, as the hypothesis over the possible Eve’s locations is wrong. Keeping the value of the phases fixed, we used the punctual secrecy capacity to

\begin{table}[h]
\centering
\caption{Simulation parameters.}
\begin{tabular}{|l|l|}
\hline
Parameter & Value \\
\hline
RIS size \((K)\) & 4, 8, 16, 20, 32 \\
\hline
\(P_t\) & 1 W \\
\hline
\(P_j = P_j(M/N)\) & (0.1, 0.5) W \\
\hline
\(\sigma\) & \(10^{-10}\) \\
\hline
\(A_r\) & 1 cm\(^2\) \\
\hline
\(\psi_{\text{FOV}}\) & 120\(^\circ\) \\
\hline
\(\phi_\frac{1}{2}\) & 70\(^\circ\) \\
\hline
\(\rho\) & 0.8 \\
\hline
\(n\) & 1.5 \\
\hline
\(R\) & \(1/A/W\) \\
\hline
Room (length, width, height) & \(5 \times 5 \times 4 \) m \\
\hline
Alice coordinates \((x,y,z)\) & \((0,0,2)\) m \\
\hline
Bob coordinates \((x,y,z)\) & \((-1.1,0,5)\) m \\
\hline
\end{tabular}
\end{table}
calculate the system’s performance also when the RIS does not direct the jamming directly to Eve’s location.

Figure 5 shows the scenario configuration with a view from the above. The RIS is in the upper left corner and is irradiated by the signal coming from Bob’s jammer. We also include the points of Eve’s possible locations in the area of interest \( A \), i.e., all the points considered in the area secrecy rate computation.

Figure 6 shows the secrecy rate obtained for different Eve locations around the room when increasing the number \( K \) of RIS elements and considering known Eve locations. We notice that such an increase provides better performance in terms of secrecy rate over the entire area and except around Alice location, the weak spot of WBPLSec [19].

Figure 7 shows the secrecy rate obtained for different Eve locations around the room when increasing the number \( K \) of RIS elements and considering unknown Eve locations. As for Figure 6, we notice that increasing the RIS size provides performance improvement especially around Bob location. Comparing these results with those in Figure 6, we notice that, thanks to our formulation, removing the hypothesis on known Eve locations does not worsen the system secrecy.

Figure 9 shows the outage probability (21) vs. the threshold \( T_h \) obtained without RIS and for increasing number of RIS elements. In particular, Figure 9(a) shows the results obtained with known Eve location, and Figure 9(b) those obtained with unknown Eve location. In both figures we can see the advantage brought by the introduction of the RIS. Furthermore, we notice that the outage probability tends to zero when increasing the RIS size in both known and unknown Eve location cases.

VII. SECURITY ANALYSIS

In this section we analyze the security properties of our schema. In Section VII-A we discuss the possible threat model and attacker capabilities. Then, in Section VII-B we analyze the security properties which our methodology ensures.

A. Threat Model

To assess the robustness of our design, we use a threat model in which an attacker could interfere with Alice and Bob at...
any moment. In particular, we consider the scenario where an attacker can obtain access to the communication channel during transmission and is therefore capable of both receiving and transmitting. An attacker in this setting could passively eavesdrop or modify the communication. The most common attacks that an attacker can perform on VLC communication can be summarized as follows.

- **Message Injection Attack**: This attack involves sending a malicious and customized message to Bob, for instance, with a malicious command.
- **Replay Attack**: An attacker reuses a previously transmitted and sniffed message in subsequent communications to replicate the legitimate transmission.
- **Message Modification**: Here, the attacker attempts to modify the message during transmission. Unlike the Message Injection Attack, the attacker modifies the message in real-time during a transmission.
- **Eavesdropping**: Attackers use passive sniffing to intercept and collect communication so they can analyze it a second time to compromise future communication.
- **Adversarial Jamming**: Here, the attacker leverages disturbing interference to disrupt the communication and make it no anymore available (Denial of Service).

### B. Security Properties

In the following, we discuss the security features of our approach and we state which of the attacks described in the previous section can be prevented by each security property. Note that these properties are achieved at the physical layer level, allowing subsequent protection to all the above layers.

**Replay attack Resistance.** Generally, this feature requires synchronization and nonce exchange between the parties. In our schema, replay attack protection is guaranteed because Bob randomly chose and destroyed a set of bits. Only he knows this information, and the next time a new secret is shared, the jammed bits will be different. In this way, Eve cannot reuse the old messages. This property allows protecting from Replay and Message Injection Attacks.

**Confidentiality.** The message’s confidentiality is ensured by the jamming phase. Indeed, only Bob know the jamming points and therefore reconstruct the message. Since Bob jams a maximum of $M$ bits out of the total $N$ bits transmitted by Alice, to force the message, the attacker should calculate $2^M$. This property allows the protection from Eavesdropping.

**Integrity.** There are two possibilities for an attacker to modify the message: in real-time or in a secondary moment. While the first approach is unfeasible due to the anti-replay property, the second would compromise the watermark, raising errors during the demodulation and watermarking verification. This property prevents Message Injection and Message Modification attacks. Furthermore, if the attacker performs jamming to perturbate the information, the integrity verification property identifies an unexpected message alteration.

**Jamming Resistance.** Thanks to the watermark, our mechanism can partially mitigate Adversarial Jamming attacks. In fact, in the most favorable case, if the adversary would destroy the frames $N_W$ frames dedicated to transmitting the watermark, Bob can still reconstruct the original message using the WBPLSec algorithm. Instead, if Eve jams other frames, our mechanism will still suffer from this type of attack.

### VIII. Conclusion

VLC is considered a key technology for future wireless communications and the introduction of RIS technology can improve the quality of the received beam. To the best of our knowledge, we propose for the first time in literature that using RIS on VLC improves the effectiveness of jamming in WBPLSec without any assumptions about the attacker’s location. We evaluated the robustness of our approach in an indoor wireless communications scenario, where the VLC transmitter on the ceiling can move unconstrained further down. We considered a VLC channel model with only the LOS component for numerical simulations.

Our results show that the introduction of RIS technology extends the area where secure communication occurs and that by increasing the number of RIS elements the outage probability decreases.

Unfortunately our proposal suffers from some limitations. First, the channel is simulated based on a widely accepted geometrical model, which can be limited compared to a real device implementation. However, currently no works are using real RIS hardware for VLC system. Second, since the problem is non-convex, PSO may not identify the optimal solution. For this reason we will investigate other approaches in future works.

### REFERENCES

[1] Cisco. (2021) “VNI Complete Forecast Highlights”. [Online]. Available: https://www.cisco.com/c/dam/m/en_us/solutions/service-provendvni-forecast-highlights/pdf/Global_2021_Forecast_Highlights.pdf

[2] D. Tsonev, S. Videv, and H. Haas, “Towards a 100 gb/s visible light wireless access network,” *Optics express*, pp. 1627–1637, 2015.

[3] S. V. Tiwari, A. Sewaiwar, and Y.-H. Chung, “Smart home technologies using visible light communication,” in *2015 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2015, pp. 379–380.

[4] F. A. Dahri, H. B. Mangrio, A. Baqai, and F. A. Umran, “Experimental evaluation of intelligent transport system with vlc vehicle-to-vehicle communication,” *Wireless Personal Communications*, pp. 1885–1896, 2019.

[5] Y. Acar, M. Backes, S. Fahl, S. Garfinkel, D. Kim, M. L. Mazurek, and C. Rkaskey, “Comparing the usability of cryptographic apis,” in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 154–171.
