Multi-RIS aided VLC Physical Layer Security for 6G Wireless Networks

Simone Soderi, *Senior Member, IEEE,* Alessandro Brighente, *Member, IEEE,*
Saiqin Xu, *Student Member, IEEE,* and Mauro Conti, *Fellow, IEEE*

Abstract—Recent studies highlighted the advantages of VLC over radio technology for future 6G networks. Thanks to the use of RISs, researchers showed that is possible to guarantee communication secrecy in a VLC network where the adversary location is unknown. However, the problem of authenticating the transmitter with a low-complexity physical layer solution while guaranteeing communication secrecy is still open. This paper proposes a novel multi-RIS architecture to guarantee source authentication, communication secrecy, and integrity in a VLC scenario. We leverage the intuition that a signal transmitted by users located in different positions will undergo a different propagation path to discriminate between the legitimate intended transmitter and an attacker. To increase the channel's variability and reduce the chances that an adversary might be able to replicate it, we leverage the reconfiguration capabilities of RIS. We derive a statistical characterization of the non-line-of-sight VLC channel, representing the light reflected by RIS elements. Via numerical simulations, we show that the channel variability combined with the configurability capabilities of RISs provide sufficient statistics to authenticate the legitimate transmitter at the physical layer.

Index Terms—Security, Jamming, Protocols, Wireless LAN

1 Introduction

The vision for 6G is to tightly couple and enhance interactions between the human, digital, and physical worlds. This cyber-physical continuum aims to improve the quality of our lives by leveraging networks as powerful tools. Both opportunities and challenges mark the journey toward 6G. The potential of 6G technologies is vast, but realizing this potential requires addressing several technical and practical challenges. Countries and standardization organizations worldwide have announced their plans for 6G research, and a series of pioneering projects [1] focusing on next-generation wireless networks have been initiated. These efforts aim to address the limitations of 5G and explore the potential of 6G technologies [2]. Fundamental values such as sustainability, trustworthiness, and digital inclusion are crucial in designing future networks. Trustworthiness in 6G networks includes ensuring data transparency, security, privacy, and network robustness [3], [4]. Thus, the transformation towards 6G networks presents unprecedented opportunities for economic growth and addressing societal challenges [3]. It necessitates a fundamental shift in network design to accommodate growing traffic, devices, energy efficiency, security, privacy, and efficiency in deployment. To this aim, projects such as Hexa-X [5] call for an x-enabler fabric of connected intelligence, networks of networks, sustainability, global service coverage, extreme experience, and trustworthiness designed with security and privacy as key design criteria.

The advent of 5G and the prospective 6G technologies emerged from the rigorous surge in data traffic and the need for innovative technologies to manage this change. Traditional Radio-Frequency (RF) communication, while instrumental in the early stages of wireless communication, is now facing new challenges in handling the current data traffic. In this context, VLC, an emerging technology, has gained considerable attention as a potential enabler for 5G and beyond. VLC, unlike RF, offers higher data rates [6], high speed and robustness against interference [7], a large available frequency spectrum [8], and a low cost implementation thanks to Light Emitting Diodess (LEDs) [9]. Despite its potential, VLC faces challenges in achieving optimal transmissions, such as signal loss, the influence of ambient light conditions, and Non-Line-Of-Sight (NLOS) conditions. Thus, to address these issues, recent works have explored the use of RIS [10]. 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 the induced electrical field [11]. Not only RIS can be used for increased data rate, but also to enhance the security of wireless networks [12], [13]. Integrating VLC and RIS technologies hence presents a promising path for enhancing the Physical Layer Security (PLS) of 6G networks. However, further research is needed to fully realize the potential of these technologies and address the challenges associated with their implementation.

- *Simone Soderi is with Scuola IMT Alti Studi Lucca, Piazza San Francesco 19, 55100 Lucca, Italy and the Department of Mathematics, University of Padua, 35121 Padua, Italy. E-mail:* simone.soderi@imtlucca.it.
- *Mauro Conti, Alessandro Brighente, and Saiqin Xu are with the Department of Mathematics, University of Padua, 35121 Padua, Italy. E-mail:* conti@math.unipd.it;alessandro.brighente@unipd.it;
- *Saiqin Xu is with National Key Laboratory of Radar Signal Processing, Xidian University, Xi'an, 710071, China. E-mail:* xusaiqin@stu.xidian.edu.cn.

Motivation. In the coming years, researchers shall face many challenges in building a trustworthy and secure 6G [1]. VLC utilization within indoor environments has been widely considered an excellent secure alternative to radio technology [14]. This heightened level of security can be attributed to the directional nature of optical signals and their substantial resistance to obstructions, rendering them significantly more challenging to intercept from external sources. Consequently, VLCs exhibits reduced vulnerability to wireless communication threats such as jamming and eavesdropping. Within this framework, PLS aims to safeguard communications by harnessing the inherent physical properties of the communication channel, eschewing the need for higher-level protocols or algorithms. PLS finds particular applicability in low-power 6G sensor networks, as it reduces energy consumption and enables fewer calculations than encryption, which extends the battery life of portable devices. Numerous proposed solutions employ RIS to enhance signal reception performance. In our previous work [12], we showed for the first time in the VLC literature that a RIS employed at the receiver side can strengthen the security of physical-level communications, employing a wiretap channel model to elevate the legitimate channel's quality while simultaneously degrading the attacker's channel [15], [10]. However, this solution cannot provide source authentication, i.e., discriminate between a signal received from the legitimate transmitter or a malicious user. Integrating source authentication with a low-cost physical layer solution would represent a significant benefit for the overall security of the resulting system.

Contribution. Notably, RIS technology in the context of VLCs offers a valuable foundation for generating randomness, thereby facilitating the implementation of device authentication using the non-Line-Of-Sight (LOS) channel representing the reflected components. Although the literature presents a statistical channel model for VLC LOS channels [16], the common model for the non-LOS component is deterministic and geometrical. Although widely accepted, this may not represent a reliable model in real-life scenarios. Therefore, we propose the first non-LOS VLC statistical channel model. Leveraging the combination of our statistical model with the configurability of RISs, we propose the first VLC system using a RIS during transmission to implement a physical layer authentication scheme. The reflections generated by the RIS (in its configurations) in the light of Alice's RGB LED provide such variability that an attacker is unlikely to be able to reproduce. We hence propose a challenge-response-based physical layer authentication scheme, where the receiver compares the estimated channel from the received signal and compares it with a previously built knowledge base of legitimate channels. Our results highlight the positive impact of RIS technology also in transmission, which allows the receiver (i.e., Bob) to authenticate the legitimate transmitter (i.e., Alice). Furthermore, we show that the newly derived model has no negative impact on the secrecy capacity of our previously proposed jamming scheme [12].

We summarize the contribution of our paper as follows.

- We propose a novel statistical channel model to characterize the behaviour of a non-LOS VLC channel under the assumption of uniformly located users.
- We present for the first time in the literature a novel architecture for physical-layer security that uses a RIS in transmission for authentication and a RIS in reception to improve secrecy capacity. Our solution consists of a challenge/response-based physical layer authentication scheme where the receiver compares the estimated channel with a trusted knowledge base.
- We validate our framework through numerical simulations demonstrating the positive impact of RIS in terms of authentication. In particular, we show that the conjunction of spatial separation between transmitters and the use of RIS characterize the channel behaviour sufficiently to distinguish transmitters. We further prove that the receiver RIS guarantees communication secrecy without relying on the assumption of a known Eve's location.

In our proposed architecture, the RIS is placed at the transmitter and receiver rather than directly in the channel to avoid the complexities of coordinating three nodes and to mitigate security risks, such as potential control signal attacks and tampering vulnerabilities. This design choice simplifies system management and enhances security by reducing potential points of failure and attack.

Organization. The remainder of the paper is organized as follows. Section 2 discusses the related works. Section 3 briefly recalls the concepts useful for understanding the paper. Section 4 describes the system and threat model considered. We present our authentication scheme in Section 5. Then, Section 6 introduces our optimization framework, and Section 7 presents the results of the simulations. Section 8 discusses the security properties we achieve with our mechanism.

Finally, Section 9 concludes the paper by discussing our findings and the current proposal's limitations.

2 Related Works

VLC is a subject that has harvested considerable attention within the research community. A diverse collection of studies has been directed towards the deployment of this communication modality across various domains, including but not limited to Vehicle-To-Vehicle (V2V) networks, as evidenced in the experimental investigations by Dahri *et al.* [17], and underwater communication systems, as explored by Akram *et al.* [18]. The pervasive dissemination and application of VLC technology have the cybersecurity community's attention, keen to discern and address the potential susceptibilities inherent in such a transmission medium. Different works investigate the PLS of VLC [19] focusing on different properties. The different proposals to deal with PLS in VLC include beamforming [20], [21], friendly jamming [22], [23], and signal mapping [24], [25]. 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 wireless communication per-

formances [10]. In this paper, we specifically focus on the security of VLC in RIS application from the PLS point of view.

The literature contains several proposals supporting the integration of RIS across multiple domains, such as the augmentation of Unmanned Aerial Vehicless (UAVs) communications, highlighted in the study by Mursia *et al.* (2021) [26]. However, a real gap exists in comprehensive studies on the security attributes of this emergent technology. The integration of RIS with various attributes has been explored in the context of LiFi applications of VLC, as discussed in the work by Abumarshoud et al. (2021) [27]. In this study, the authors examine how RIS can enhance several PLS features, including secrecy capacity, resistance to jamming, and the facilitation of secure beamforming. Despite this, the study does not deeply examine security considerations, nor does it provide an estimation of secrecy capacity. Further, in the research presented by Li *et al.* (2021) [28], a novel mechanism that integrates RIS to strengthen the security of UAV communications is put forward, employing an alternating optimization technique. The study also validates that the introduced algorithm enhances the average secrecy rate compared to other standard benchmark algorithms.

In [29], the authors propose a secure transmission design for an IRS-assisted multi-antenna system. They focus on maximizing the secrecy rate by optimizing the transmit beamforming at the base station and the passive beamforming at the IRS. The proposed algorithm significantly improves the secrecy rate compared to other benchmark schemes. The study [30] presents a secure transmission scheme for multi-RIS-assisted wireless communications. The authors propose a joint active and passive beamforming design to maximize the worst-case secrecy rate. The results show that the proposed scheme can effectively improve the system's secrecy performance. In [31], the authors propose multiple RIS-aided Secure, Precise Wireless Transmission (SPWT) schemes in a three-dimensional wireless communication scenario. The schemes are designed to enhance communication performance and energy efficiency simultaneously. The results show that single-user and multiuser schemes can achieve SPWT, transmitting confidential messages precisely to desired users' locations. The paper [32] investigates robust beamforming design for a RIS-assisted multiuser millimetre wave system with imperfect CSI. The authors propose a weighted sum-rate maximization problem to jointly optimize the transmitter beamforming, RIS placement, and reflect beamforming. The results reveal that the proposed scheme can potentially enhance the performance of existing wireless communication, considering a desirable trade-off among beamforming gain, user priority, and error factor. Finally, [33] discusses the potential of RIS in enhancing the performance of Optical Wireless Communication (OWC) networks. The authors highlight the benefits of multi-RIS systems in creating opportunities for multi-hop transmission of directed power, even in highly crowded spaces.

It is also worth noting that the last few years have introduced solutions that improve PLS using watermarking and jamming primitives with and without any receiving RIS. Recently, Soderi *et al.* in [34] prompted the implementation of Watermark Blind Physical Layer Security (WBPLSec) to improve the PLS of VLC (see Figure 2(a)).An evolution of it was later proposed [12], incorporating RIS in reception, with which the authors showed improved performance from a secrecy capacity point of view, even without knowing the attacker's position (see Figure 2(b)). WBPLSec was already applied on different communication means such as radio frequency [35], acoustic communications [36] showing the improvement of performances from the secrecy capacity of the channel point of view. In a vision of continuous evolution of security at the physical level, our proposal (see Figure 3) extends [34], and [12] integrating a RIS in transmission to further improve the security of communication in terms of authentication at the physical level.

Artificial Noise (AN) is a recognized technique to enhance communication security by degrading eavesdroppers' channel quality, as demonstrated by Xu *et al.* [37]. While we do not directly implement AN in our VLC system model, we acknowledge its potential benefits and consider it a viable security option. Our system shares the spreading code for watermarking, which aids Physical Layer Authentication (PLA) and secure communication, and this code could include parameters for effective AN generation. Accurate Channel State Information (CSI), obtained through channel estimation with pilot signals, is critical for designing orthogonal AN to the legitimate user's channel, thereby minimizing interference to the intended receiver while degrading the eavesdropper's channel. Although we currently do not use AN, integrating it with our security measures, such as spreading codes and channel estimation, could enhance security in future work, leveraging the benefits shown in massive Multiple Input Multiple Output (MIMO) systems and adapting them to VLC systems.

Our architecture integrates multiple RISs at both the transmitter and receiver, exploiting the RIS at the transmitter for physical layer authentication and the RIS at the receiver for enhanced confidentiality. This dual-RIS configuration creates a robust security framework that mitigates eavesdropping and unauthorized access, enhancing security and system performance, especially in high-interference environments. Current studies primarily focus on single RIS setups, as seen in [38], [39], which discuss the security enhancements, cost-effectiveness, and energy efficiency of RISs. However, these studies do not explore multiple RIS deployments; we address this gap with empirical data and theoretical analysis, showcasing the performance gains and security enhancements achievable through a multi-RIS approach and contributing to future research on complex RIS configurations for 6G networks.

3 Background

This section briefly introduces the concepts that are useful for understanding the remainder of the paper. In particular, after a recall about VLC and PLA concepts, in Section 3.3, we summarize the VLC channel model, and in Section 3.4 we detail of the WBPLSec algorithm.

3.1 VLC Signals Model and RIS contribution

Currently, we can use several types of luminescent diodes (LEDs) for VLC. They differ in the semiconductors used,

which emit different wavelengths such as λ_R for red in the range $620 \text{ nm} \leq \lambda \leq 750 \text{ nm}$; λ_G for green in the range $500 \text{ nm} \leq \lambda \leq 560 \text{ nm}$; and λ_B for blue in the range $450 \text{ nm} \leq \lambda \leq 480 \text{ nm}$.

An RGB discrete-time signal can then be written as follows [40].

$$s[n] = \sum_{i=0}^{N_l} \beta_i \cdot g_i[n - \Delta_i], \tag{1}$$

where β_i refers to the power associated with the emission of the $i-th$ RGB color (i.e., with $i \in \{R, G, B\}$), N_l is the number of LEDs used for the VLC, $g_i(t)$ is the unit power waveform emitted by each LED and Δ_i represents the time length of the color $i-th$.

Notice that this model considers the emission of non-simultaneous RGB signals. By taking advantage of Bloch's law [41, Chapter 3] defining light perception, we can configure the duration of the signals to avoid flickering and dimming phenomena.

3.2 Physical-Layer Authentication (PLA) Remarks

Academia has shown great interest in PLA in recent years due to its potential to reduce computational resources required for authentication compared to traditional cryptography-based methods at higher levels [42]. One approach to PLA is through Physical Unclonable Functions (PUFs), which exploits the unique physical microstructures of integrated circuits inherited from manufacturing variations [43]. PUFs operate based on challenge-response pairs (CRPs), where responses to specific challenges are stored in a database and used for authentication [44]. PUFs provides an additional level of security by allowing authentication based on the unique distortion that the transmitter device applies to the transmitted signal. A further example would be the active radio fingerprinting, whereby the transmitter uniquely modifies the radio signal before sending it [45].

Another approach to PLA is using CSI, which extracts features from the channel, location, and signal to fingerprint due to minor hardware imperfections using machine learning techniques [44]. While these techniques offer potential benefits for wireless networks, they also present challenges in implementation, such as the need for accurate channel estimation and the potential for increased computational overhead [46].

Overall, PLA techniques have the potential to play a crucial role in developing next-generation wireless networks. In this paper, we want to propose a new architecture that exploits RIS in transmission to authenticate light signals.

3.3 VLC Channel Model

VLC systems employ Intensity Modulation (IM) techniques in conjunction with Direct-Detection (DD) methods. Optimal illumination levels are sustained at the transmission end by adjusting the Direct-Current (DC) bias of the comprehensive signal injected into the LED. In contrast, the signal is proportional to the optical power received at the photodiode. An intrinsic VLC channel comprises two principal elements: the LOS channel and the diffuse channel. The former element accounts for the fraction of light that impinges directly upon the photodiode without any reflection from surrounding objects. The latter, also referred to as the NLOS component, encapsulates all light rays that are reflected from various obstacles within the environment. This article considers only the NLOS component (see Figure 1).

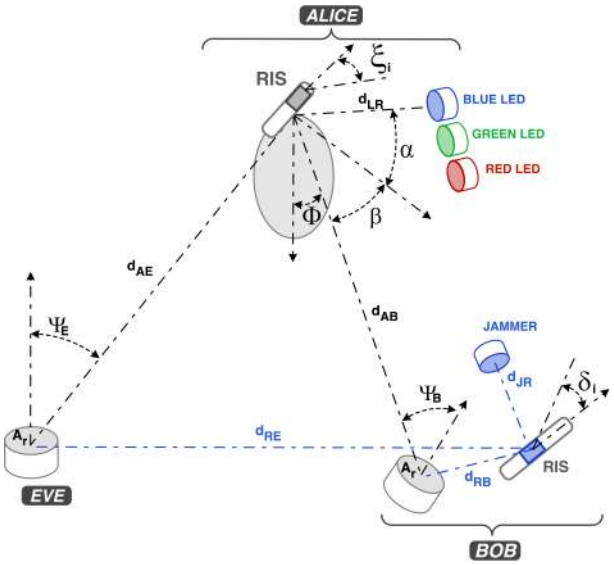


Fig. 1: Contribution of RIS in transmission and reception in the NLOS VLC channel model. d_{LR} and d_{JR} are the distances between the transmitter or the jammer and their RIS, whereas d_{AB} and d_{AE} are the distances between each RIS and one receiver.

Assuming to have Lambertian light source, it is important recall that in terms of reflections on the RIS, we can define the channel DC gain of the first reflection as a NLOS contribution given by

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

where A_r is the receiver collection area, R is the photodiode 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, ψ is the angle of incidence ($\psi \in \{\Psi_E, \Psi_B\}$), and ψ_{FOV} is the receiver's angle Field-Of-View (FOV). And, ρ denotes the reflection coefficient, dA_w represents the emission area of a micro surface for the single RIS element, α expresses the incidence angle of a reflection point and β is the radiation angle of the receiver. For the same two-dimensional RIS surface area, a larger number of RIS elements impose that each of them has a smaller surface dA_w. This impacts the reflection contribution for a single RIS element. Moreover d_{1B} denotes the distance between the transmitter and its RIS (i.e., d_{LR} or d_{JR}), whereas d_{2B} is the distance between the RIS and one receiver (i.e., d_{AB} or d_{AE}). Following our architecture, depicted in Figure 1, we assumed $d_{1B} \ll d_{2B}$.

The total received power for Alice with one RGB LED, for a given transmission power (P_t), is given by the DC channel, i.e. $P_r = P_t \cdot dH_{ref}(0)$. In a VLC system, the Signal-

to-Noise Ratio (SNR), i.e. γ_v, is proportional to the square of the received optical power, i.e., $\gamma_v = {}^{dH^2_{ref}(0)P_t^2}/_{\sigma^2}$ where P_t is the transmitted optical power, $dH_{ref}(0)$ is the channel DC gain and σ^2 is the spectral density of the background noise.

To simplify the mathematical treatment in the remainder of the paper, we will denote by h instead of $dH_d(0)$, the coefficients of the VLC channel.

3.4 WBPLSec Security Solution

In this section, we present transceivers architectures that use RIS and WBPLSec.

By using a jamming receiver in combination with a Spread-Spectrum (SS) watermarking procedure [47], the WBPLSec algorithm serves as a potent security protocol. As an independent security algorithm designed for sensor networks, it has significantly raised researchers' curiosity in recent years. Its successful implementations extend across various communication ecosystems, notably in wireless [35], acoustic domains [36], and CAN bus networks [48]. This sophisticated technique enables an authenticated receiver to construct a security perimeter around itself by harnessing jamming, thereby establishing a conduit for confidential communication under predetermined conditions.

VLC Application with and without RIS. The WBPLSec protocol has been recently proposed to achieve confidentiality in VLC [34], [12]. The first paper combines watermarking and jamming in WBPLSec to provide an autonomous security solution in 6G networks. As depicted in Figure 2(a), the receiver uses a RIS to improve jamming performance in the second contribution. The RIS can degrade the attacker's channel even without knowing the attacker's location. Both of the previous solutions do not involve the use of any RIS in transmission, which is instead one of the contributions of this article to implement PLA.

First, it should be said that there are several ways to implement VLC. The one that uses RGB LEDs provides the greatest bandwidth since it also uses three independent channels but also provides greater freedom to combine these three signals in a way that, as we shall see, establishes secure communication.

WBPLSec without RIS. Let us consider an RGB LEDs architecture to implement WBPLSec over VLC as depicted in Figure 2(a). That is an architecture without any RIS [34].

We now recall how the WBPLSec algorithm works in the case without RIS [35], [34]. Let's consider that Alice wants to send a secret message of N bits $(x_S)^N$ to Bob. Alice transmits the watermarked signal $(x'_S)^N$ using an RGB LED. Bob receives the message through a single RGB color-tuned photodiode, but he jams M bits (with $M < N$) of Alice's message using an RGB LED while receiving it. We write the jamming signal as $(x_J)^M$. Eve, the attacker, may use multiple Photo-Diodes (PDs) to breach the secrecy. The scheme proposed [34] (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*: A segment of the confidential communication, precisely N_W of N bits, is initially modulated utilizing a spreading sequence to generate the watermark signal $(w)^{N_W}$. Subsequently, this signal is transmitted exclusively via the red spectrum of the LED light.;

(ii) *jamming receiver*: Bob jams Alice's message using RGB LED;

(iii) *selective jamming*: Bob selectively interferes with a portion of the incoming message, a process that does not impact the SS watermark. Due to his knowledge of the specific segments he has jammed, Bob can reconstruct the original, clean message. This targeted jamming ensures the integrity of the SS watermark signal remains intact [49].

(iv) *communication hiding*: Our method transmits data through dual distinct pathways by harnessing both blue and red lights. The primary path is a narrowband Amplitude Shift Keying (ASK) signal transmitted via blue light, denoted as $(x_S)^N$. Concurrently, the SS watermark signal $(w)^{N_W}$ is transmitted using red light, thereby establishing a covert communication channel.

The choice of colours associated with the signals is an arbitrary choice that does not limit the discussion in this article. Even if the attacker knew this scheme, if it filters blue light only when jamming with the WBPLSec algorithm is applied, Eve would receive an unusable signal because the jamming would partly wipe it.

WBPLSec with one RIS in reception. Let us consider now a VLC that always uses RGB LEDs, but with a receiving RIS, then the model changes as shown in Figure 2(b).

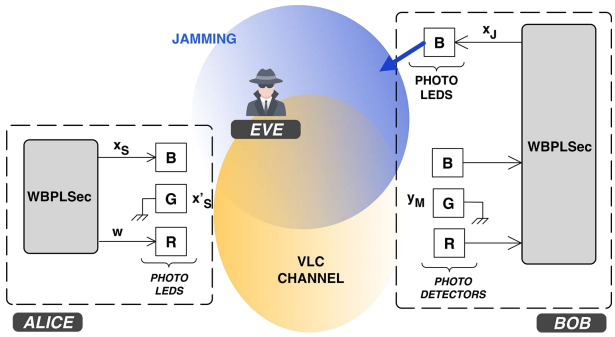
In [12] we assumed that the jammer transmits a signal $(x_J)^M$ and exploits a receiving RIS to select the direction of the jamming signal to degrade the attacker's channel in an area of the room without necessarily knowing where he/she is. We denoted as $\boldsymbol{h}_{JR}$ the channel between the jammer and the RIS and as $\boldsymbol{h}_{RB}(\boldsymbol{\delta})$ the channel between RIS and Bob where $\boldsymbol{\delta}$ are the yaw angles of the each RIS element. We can say the same, and with similar notation, for the adversary's channel. The reflected signal affects both the signal received by Bob and Eve. The use of RIS as written in [12] allowed us to degrade the channel of the attacker even without knowing his exact position.

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.

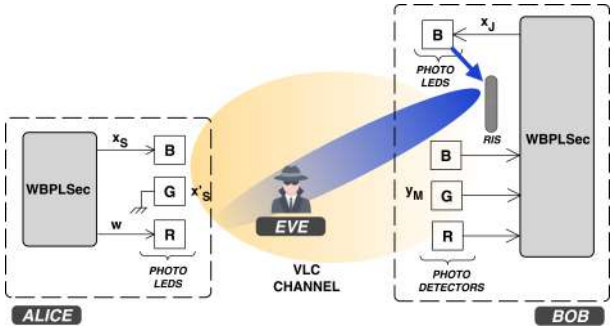
4 Multi-RIS architecture System Model

We propose a new architecture for VLC that embeds RIS in the transmitter and in the receiver. In particular, we leverage the RIS in transmission to implement a PLA scheme. Whereas the receiving RIS is used to implement the algorithm WBPLSec as proposed in [12]. Thus, this new model depicted in Figure 3 ensures the wireless communication's authenticity, confidentiality, and integrity.

It is important to note that the transmitter proposed in Figure 3 uses the three RGB channels for authentication. In contrast, only two LEDs, Blue and Red, are necessary to implement the WBPLSec algorithm. Similar to other architectures already known in the literature [50], we can also utilize the third LED (i.e., Green) to balance the white light



(a) System model without any RIS [34].



(b) System model with one RIS at the receiver [12].

Fig. 2: Different system models with and without RIS.

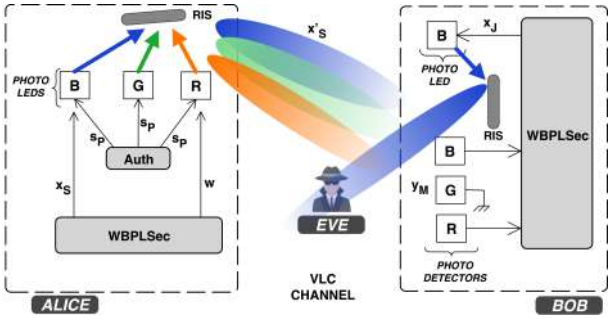


Fig. 3: System model using WBPLSec for VLC in the cases with and without RIS.

emitted by the transmitter, thereby preventing discomfort to the users' eyes. The order in which the LED colours were chosen to transmit the host signal and the watermark is purely arbitrary and does not limit the discussion of this article. Whatever the choice, it is essential to use the third LED to keep the white light properly balanced.

RIS Technology. Based on a comparative analysis of RIS technologies [51], [52], we chose micro mirror-array RIS for our proposed system due to their efficiency, more straightforward implementation, and superior signal control, especially in scenarios requiring precise phase adjustment. While liquid crystal-based RIS offers advantages in beam steering and amplification, they are more complex and require specific environmental conditions; mirror-array RIS, in contrast, enhances communication security, is easier to integrate, and provides sufficient phase control without the added complexity and power requirements, making them more cost-effective and power-efficient for practical implementation.

4.1 Signal Model

In this section, we provide a mathematical formulation for the wiretap channel presented in Figure 4.

At Bob's side, we assume that the jammer transmits a signal $(x_J)^M$ and leverages a RIS with $K_r = K_{r,x} \times K_{r,y}$ elements to suitably select the jamming signal direction, where $K_{r,\cdot}$ denotes the number of elements along one of the two dimensions of a two-dimensional RIS. We denote as $h_{JB}(\boldsymbol{\delta})$ the channel between the jammer Bob, accounting for the whole jammer-to-RIS and RIS-to-Bob channel contributions. We express it as a function of the RIS rotations to account for the effect of the RIS configuration. Similarly, we define $h_{JE}(\boldsymbol{\delta})$ as the channel from the jammer to Eve, accounting for both the jammer-to-RIS and RIS-to-Eve channel contributions. As discussed in Section 3.3, we model the RIS reflected channel as the NLOS VLC channel (2) [12]. Therefore the jamming signal at Bob can be computed as

$$y_{JB}(\boldsymbol{\delta}) = h_{JB}(\boldsymbol{\delta}) x_J, \tag{3}$$

whereas the received jamming signal at Eve as

$$y_{JE}(\boldsymbol{\delta}) = h_{JE}(\boldsymbol{\delta}) x_J, \tag{4}$$

where $\boldsymbol{\delta} = [\delta_1, \ldots, \delta_{K_r}]$ denotes the yaw angle of each RIS element, as described in [53].

On Alice's side, we assume that NLOS components are transmitted via a RIS with $K_t = K_{t,x} \times K_{t,y}$ elements. Following the WBPLSec applied to VLCs [34] and its evolution with one RIS [12], we can now write the signals received by Bob and Eve respectively for a multi-RIS architecture:

$$y_M = [h_{AB}(\boldsymbol{\xi})] x'_S + y_{JB}(\boldsymbol{\delta}) + n_M, \tag{5}$$
$$y_E = [h_{AE}(\boldsymbol{\xi})] x'_S + y_{JE}(\boldsymbol{\delta}) + n_E, \tag{6}$$

where $h_{AB}(\boldsymbol{\xi})$ and $h_{AE}(\boldsymbol{\xi})$ are the channel's gains between Alice-Bob and Alice-Eve, respectively, as a function of $\boldsymbol{\xi} = [\xi_1, \ldots, \xi_{K_t}]$ denoting the yaw angle of the each Alice's RIS element. Since we apply WBPLSec [35], [34], x'_S is the transmitted watermarked signal given by $x'_S = x_S + \mu w$. n_M and n_E are the complex zero-mean Gaussian noise with variance σ_E^2 and σ_B^2, respectively. Note that we neglected the noise terms in (3) and (4) to only consider it once in the overall received signals in (5) and (6). Also, we assume that each node can efficiently estimate channels e.g., via [54].

Given the received signals, and assuming $\mathbb{E}[|x_S|^2] = 1$, we can define the Signal-to-Interference Plus Noise Ratio (SINR) at Bob's side as

$$\gamma_M = \frac{|h_{AB}(\boldsymbol{\xi})|^2 P_t^2}{\sigma_M^2 + |h_{JB}(\boldsymbol{\delta})|^2 P_j^2}. \tag{7}$$

The SINR at Eve's side is given by

$$\gamma_E = \frac{|h_{AE}(\boldsymbol{\xi})|^2 P_t^2}{\sigma_E^2 + |h_{JE}(\boldsymbol{\delta})|^2 P_j^2}. \tag{8}$$

In both cases we assumed that the red and blue LEDs transmit the same power P_t.

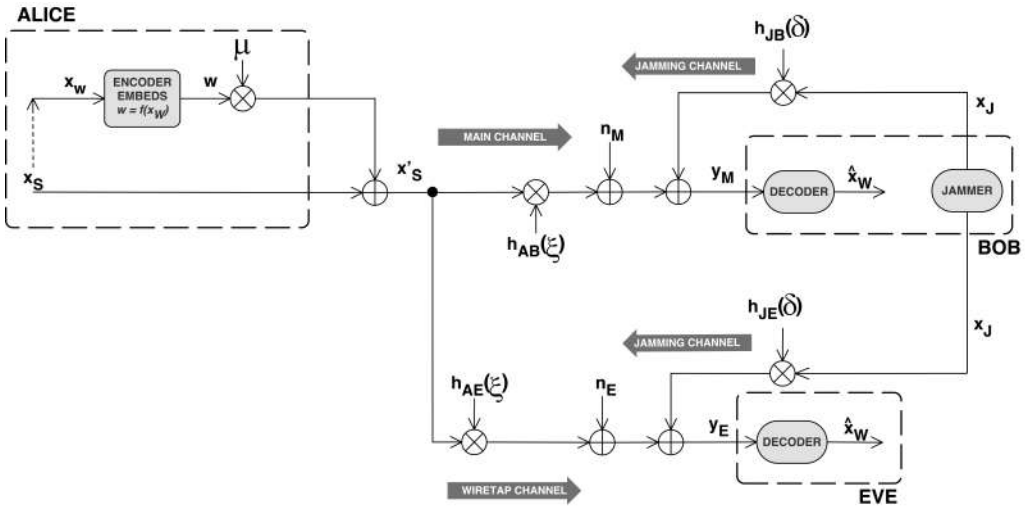


Fig. 4: Modified non-degraded wiretap channel model with a multi-RIS architecture. By applying an NLOS model, the channel coefficients depend on the yaw angles of the RISs.

4.2 Threat Model

To evaluate the resilience of our proposed architecture, we incorporate a threat model that sets the potential for adversarial interference with the communicating parties, herein referred to as Alice and Bob, at any given moment. Expressly, we have foreseen a scenario wherein an adversary gains access to the communication channel amidst transmission, thereby acquiring the capability to intercept and inject data (as per the MitM attack paradigm). Within this context, an adversary might engage in passive surveillance or actively manipulate the communicative exchange.

The plethora of attacks to which a VLC system may be susceptible is multifaceted. The prototypical offensive schemes that an adversary could execute in VLC communication are as follows.

- **Impersonation Attack**: To attack the authentication system, Eve tries to impersonate Alice. To this aim, she must find a suitable RIS configuration such that her channel to Bob mimics the channel between Alice and Bob. We assume a strong attacker, knowing the legitimate channel between Alice and Bob and Alice's RIS configuration.
- **Message Injection Attack**: Under this type of attack, an unauthorized entity transmits a crafted, malicious message to Bob, potentially containing a harmful command.
- **Replay Attack**: Herein, an adversary captures a legitimate message from prior communication and retransmits it, thereby mimicking an authentic exchange to deceive the receiver or gain unauthorized benefits.
- **Message Modification**: In this scenario, the adversary actively tampers with the content of the communication as it occurs, altering the message mid-transit, which is a divergent approach from the aforementioned Message Injection Assault where the attack does not necessitate real-time communication interference.
- **Eavesdropping**: In this passive attack, the intruders stealthily intercept and record communications. They can later analyze this data to understand the system's workings, potentially compromising future communications and extracting sensitive information.
- **Adversarial Jamming**: This approach involves the attacker creating disruptive interference to hinder communication, essentially rendering the network unavailable, a form of Denial of Service (DOS) attack. It usually involves overwhelming the network with traffic or disrupting its regular operation.

4.3 RIS-Reflected Signal Channel Distribution

This section derives the channel distribution for the RIS-reflected signals. Due to the deterministic nature of the VLC channel, the authors in [16] derive the distribution functions of the channel gain for uniformly distributed users, offering valuable statistical insights into the channel characteristics. Motivated by this, we explore the distribution for the RIS-reflected signals given in a simple and closed form. The vertical distance from the RIS to the receiving plane is denoted by L, and r is the horizontal distance from the received Bob to RIS. Additionally, we denote the maximum cell radius as r_e. By substituting $d_{2B} = \sqrt{r^2 + L^2}$, $\cos(\beta) = L/\sqrt{r^2 + L^2}$ and $\cos(\psi) = L/\sqrt{r^2 + L^2}$ in (2), the NLOS channel gain can be expressed as

$$dH_{ref}(0) = \frac{C(m+1)L^2}{(r^2 + L^2)^2}; \tag{9}$$

where C is given by:

$$C = \frac{A_r R}{2\pi^2 d_{1B}^2} D(\psi)\rho dA_w \cos^m(\phi)\cos(\alpha). \tag{10}$$

Define function $h = u(r) = C(m+1)L^2(r^2 + L^2)^{-2}$. It is evident that h is a monotonic decreasing function with respect to r. Therefore, the probability density function

(PDF) of the unordered channel gain can be calculated using the "change of variable" method as follows:

$$\begin{aligned} f_h(h) &= |\frac{\partial}{\partial h} u^{-1}(h)| \cdot f_r(u^{-1}(h)) \\ &= \frac{1}{2r_e^2} \left(C(m+1)L^2\right)^{\frac{1}{2}} h^{-\frac{3}{2}}, \end{aligned} \tag{11}$$

where u^{-1} denotes the inverse function of u, and $f_r(r) = 2r/r_e^2$ is the PDF of variable r following the uniform distribution. The cumulative distribution function (CDF) of the unordered variable h can therefore be obtained as

$$F_h(h) = -\frac{1}{r_e^2}(C(m+1)L^2)^{\frac{1}{2}} h^{-\frac{1}{2}} + \frac{L^2}{r_e^2} + 1. \tag{12}$$

for $h \in [h_{min}, h_{max}]$, where h_{min} and h_{max} are given as $h_{min} = C(m+1)L^2/(r_e^2+L^2)^2$ and $h_{max} = C(m+1)L^2/L^4$. Therefore, the inverse function of CDF can be obtained as

$$\hat{h} = \left(-F_h(h) + \frac{L^2}{r_e^2} + 1\right)^{-2} \left(\frac{1}{r_e^2}(C(m+1)L^2)^{\frac{1}{2}}\right)^2. \tag{13}$$

Hence, the receiver Bob with RGB LED has three components defined as $\boldsymbol{x} = [r, g, b]$, which are the random number from 0 to 1. Then, the channel reflected by one unit RIS can be rewritten as

$$dH_{ref}(0) = \left(-\boldsymbol{x}_i + \frac{L^2}{r_e^2} + 1\right)^{-2} \left(\frac{1}{r_e^2}(C(m+1)L^2)^{\frac{1}{2}}\right)^2. \tag{14}$$

where the $\boldsymbol{x}_i$ denoted random numbers for the ith element of RIS.

We use a geometric channel model and associated parameters to derive the NLOS path channel coefficients, similar to the model by Sun *et al.* in [55], but with key technical differences. While Sun *et al.* focus on optimizing RIS configuration and transceiver matrices to minimize MSE in a MIMO VLC system using an alternating optimization algorithm under perfect CSI, our model extends this approach by considering the statistical interactions between multiple RISs, accounting for the combined effects on the NLOS path. Our proposal leads to a more comprehensive channel model that captures the increased complexity and potential interference in a multi-RIS environment, providing a refined understanding of channel dynamics for improved system performance and security.

5 Challenge-Response-based PLA Scheme with a RIS-aided Transmitter

In this paper, we propose a challenge-response-based PLA authentication scheme. Our PLA scheme involves an enrollment phase at instant k_1 in which the legitimate receiver builds the necessary knowledge of the wireless channel connecting it to the transmitter. Then, during the second phase (that happens at the time instant $k_2 > k_1$), the CSI estimated by the receiver will be used for authentication so that Bob can verify the sender's identity. We divide our scheme into the following phases [44], [56]: knowledge base creation, challenge generation, identity verification.

Knowledge-base creation. During this step, the legitimate transmitter Alice leverages the RIS controlled channel to send multiple pilot signals to Bob, each transmitted using a different RIS configuration. The controllability provided by the RIS allows Alice to generate multiple different measurements using a single pilot signal. Bob estimates the transmission channel for each received pilot signal and stores the result in its knowledge base. We assume that this step is trusted as common in the literature [44], such that Bob can build a knowledge base solely composed of legitimate measurements.

The signal received by Bob at location ℓ using configuration s can be represented similarly to (5) as

$$y_\ell = [h_{AB}(\boldsymbol{\xi}^{(s)})]_\ell s_P + n_M^{(s)}, \tag{15}$$

where s_P is the pilot signal, and $\boldsymbol{\xi}^{(s)}$ is the s-th RIS configuration, $s = 1, \cdots, S$. In the case of a mobile Bob, this step is repeated for multiple Bob's locations to build a location-independent knowledge base[1]. We notice that the knowledge base creation phase is performed offline, and is not constrained to be executed in a strict time interval. This ensures avoiding imposing stressful computational burdens on the RIS and its configuration. Such an offline phase assumption is common in similar works on physical layer authentication [44] and supervised machine learning applied to wireless communications [57], [58], [59]. The knowledge creation base should be resistant to possible exploitation by the attacker. Indeed, selecting RIS configurations with a predefined policy (e.g., maximizing the SNR at the receiver) would provide an attacker with information that can be exploited to predict channels and create a knowledge base of its own to impersonate the legitimate user. Thus, to avoid attacks, we resort to random configurations of the RIS elements.

Challenge generation. After building the knowledge base, Bob knows the communication channel that Alice is likely to use. To authenticate Alice, Bob sends her a challenge message. Alice responds to the challenge by using a random RIS configuration. Bob estimates the channel from the response and uses it to authenticate Alice.

At the transmitter, we assume that the SS watermark (i.e., w) is sent using the red-light of the RGB LED, whereas the host signal (i.e., x_S) is first reflected by the RIS and only the NLOS component is broadcast.

Identity verification. At this stage, we are in normal operation, considering the possible presence of an attacker in the network. We assume that the attacker *Eve* has access to the challenge with a Man-in-the-Middle (MitM) model and receives the signal through the *wiretap channel*. To increase the unpredictability or the response, Alice leverages a random configuration of its RIS rotations to create a response to Bob's challenge. Thus, we do not optimize the rotations for higher spectral efficiency, but we mainly leverage them to introduce randomness. After receiving a response to his challenge, Bob estimates the transmission channel and compares such an estimate with its knowledge base. The PLA scheme is based on the fact that Eve's channel is significantly different from Alice's one. Therefore, if Bob estimates the channel from a response generated by Eve, he should not

1. To reduce the number of points for which Bob needs to create a knowledge base, we assume that we can use interpolation. However, we leave this analysis for future works

find a reasonable match in its dictionary. Therefore, if the channel *belongs* to the knowledge base, then Bob deems the transmission as authenticated. Otherwise, Bob discards the subsequent messages.

Bob uses a correlator to evaluate whether the estimated channel belongs to the dictionary. We choose this function due to its simplicity and efficient implementations, as done in standard systems [60]. Let us denote as $\boldsymbol{\mathcal{H}}_\ell = \{\boldsymbol{h}_1^\ell, \boldsymbol{h}_2^\ell, \cdots, \boldsymbol{h}_{\mathrm{L}}^\ell\}$ the set of channel measurements obtained in the knowledge base creation phase for Bob at location ℓ. Let us denote as $\tilde{\boldsymbol{h}}^\ell$ the channel estimate obtained by Bob for the current challenge. When using the correlator, Bob computes the following value:

$$c_\ell = \frac{1}{\mathrm{L}} \left| \sum_{i=1}^{\mathrm{L}} \frac{\mathbb{E}\left[(\boldsymbol{h}^\ell - \mu_{h^\ell})(\boldsymbol{h}_i^\ell - \mu_{h_i^\ell})\right]}{\sigma_{h^\ell}\sigma_{h_i^\ell}} \right|, \tag{16}$$

where L is the number of the phase values for RIS, μ_{h^ℓ} and $\mu_{h_i^\ell}$ are the mean of $\boldsymbol{h}^\ell$ and $\boldsymbol{h}_i^\ell$, and σ_{h^ℓ} and $\sigma_{h_i^\ell}$ are the corresponding standard deviation respectively. And the legitimacy of the estimated channel increases with the larger value of the Pearson coefficient c_ℓ. We assume that the receiver knows a threshold value T_c to decide the legitimacy of the channel. In particular, Bob at location ℓ considers the received signal legitimate only if $c_\ell \geq T_c$.

6 RIS-Aided Jamming Optimization

This section defines the optimization problem to obtain the RIS phase configurations that maximize communication secrecy. We describe important metrics in Section 6.1. To show the advantages of our proposal in real-life scenarios, we consider optimization over unknown Eve location (Section 6.2).

6.1 RIS-aided Receiver

Secrecy Capacity. We leverage the RIS configurability 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 [61], [62] is a widely accepted metric for confidentiality at the physical layer. It can be defined as

$$C_s = \max\{C_M - C_E, 0\} = \begin{cases} \frac{1}{2}\log_2 \frac{1+\gamma_M}{1+\gamma_E}, & \text{if } \gamma_M > \gamma_E, \\ 0, & \text{if } \gamma_M \leq \gamma_E. \end{cases} \tag{17}$$

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 MitM.

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 use the *area secrecy capacity* [12], which defines the average secrecy capacity over a predefined area. We denote as $\mathcal{A} \in \mathbb{R}^3$ the area of interest (e.g., a portion of the room), and as $C_E(a), \gamma_E(a)$ as the channel capacity and the SINR for an attacker at location $a \in \mathcal{A}$. By denoting as $|\mathcal{A}|$ the area value of $\mathcal{A}$, we define the area secrecy capacity as

$$\begin{aligned} C_s(\mathcal{A}) =& \frac{1}{|\mathcal{A}|}\int_{\mathcal{A}} (\max\{C_M - C_E(a), 0\})da = \\ =& \begin{cases} \frac{1}{2|\mathcal{A}|}\int_{\mathcal{A}} \log_2 \frac{1+\gamma_M}{1+\gamma_E(a)}\, da, & \text{if } \gamma_M > \gamma_E(a), \\ 0, & \text{if } \gamma_M \leq \gamma_E(a). \end{cases} \end{aligned} \tag{18}$$

The concept of area secrecy capacity offers a less-than-ideal measure since, in contrast to the secrecy capacity delineated in Eq. 17, it fails to account for the specific characteristics of Eve's channel. Instead, it relies on an aggregate approximation of discrete secrecy capacities computed across a range of Eve's presumed positions within a designated area of interest.

However, by issuing with the presupposition regarding the exact positioning of Eve, this metric extends enhanced generalizability and practical relevance to contexts wherein specifying Eve's locale presents considerable difficulties.

6.2 Unknown Eve Location

In realistic situations, the precise whereabouts of the adversarial eavesdropper, Eve, might elude the jammer. Consequently, it becomes infeasible to fine-tune the RIS to direct the jamming signal accurately towards Eve. To navigate this limitation, we eschew the optimization of secrecy capacity predicated on a singular, known location of Eve. Instead, we establish a matrix of potential Eve positions systematically dispersed over a pre-established *area of interest* ($\mathcal{A}$). In this case, the objective function of our optimization problem is given by the area secrecy capacity in (18), and we can write the optimization problem as

$$\max_{\boldsymbol{\delta} C_s(\mathcal{A})} \tag{19a}$$

$$\text{s.t. } \delta_k \in [0, 2\pi],\ \forall k = 1, \cdots, K. \tag{19b}$$

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 evaluating the possible Eve's locations over $\mathcal{A}$.

We notice that the contribution of the RIS at the transmitter's side does not play any role in the optimization of the RIS used for jamming. Therefore, our problem is the one in [12], and we solve it using the same approach.

7 Simulations Results

In this section, we evaluate the performance of the multi-RIS architecture using numerical simulations.

Table 1 presents the parameters selected for the parametric analysis, encompassing the transmitted power, the intensity of the jamming signal, and the orientation of the transmitter and the receiver. We assumed that the LEDs employed by Alice, Bob, and Eve are homogeneous regarding their specifications. The configuration presupposes Alice's installation on the ceiling and the unrestricted mobility of Bob and Eve within the confines of the room.

To validate our proposed approach, we designed a MATLAB-based simulator to investigate VLC authentication mechanism, where we considered the indoor scenario

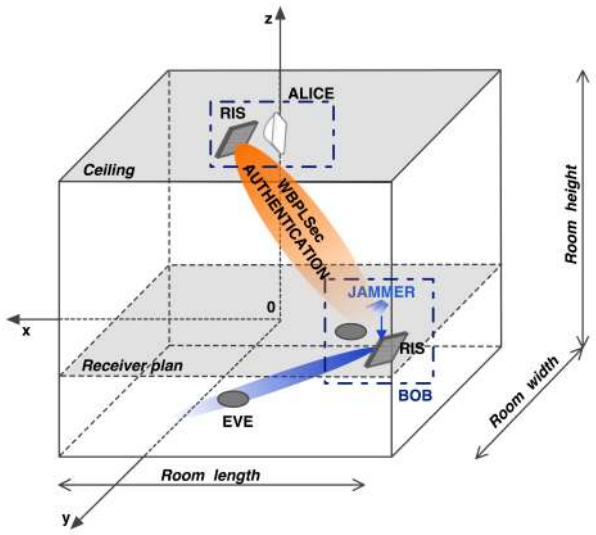


Fig. 5: Multi-RIS architecture applied to indoor VLC. In the simulations, Bob moves around a grid of points.

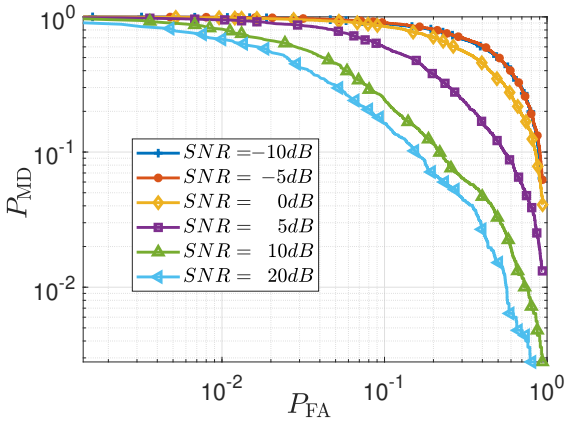


Fig. 6: Misdetection probability (P_{MD}) and False-alarm probability (P_{FA}) vs SNR

TABLE 1: Simulation parameters.

Parameter	Value
Alice's RIS size (K_t)	$0, 1, 2 \times (1, 2, 3, 4)$
Bob's RIS size (K_r)	$0, 1, 2 \times (1, 2, 3, 4)$
P_t	$1\ W$
$P_j = P_t(M/N)$	$(0.1, 0.5)\ W$
σ	10^{-7}
A_r	$1\ cm^2$
ψ_{FOV}	$120°$
$\phi_{\frac{1}{2}}$	$70°$
ρ	1
n	1.5
R	$1\ A/W$
Room (length, width, height)	$5 \times 5 \times 4\ m$
Alice coordinates (x,y,z)	$(0,0,2.5)\ m$
Bob coordinates (x,y,z)	$(\ :,\ :,0.1)\ m$
Eve coordinates (x,y,z)	$(0.5 \sim 1.5, 0.7 \sim 1.7, 2.6)\ m$
Grid dimension	11×11
Maximum number of phases for Bob's RIS	256

with parameters reported in Table 1. We consider a VLC network with an RIS having elements with unitary gain and fully controllable phases organized at equally spaced

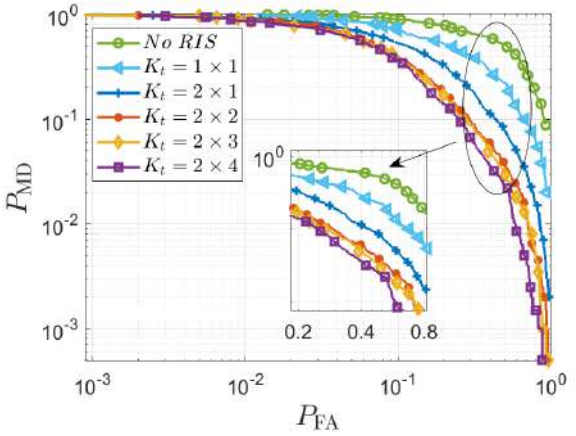


Fig. 7: Misdetection probability (P_{MD}) and False-alarm probability (P_{FA}) vs the size of RIS.

positions along two lines. For challenge-response authentication, the phases (in radians) of the RIS elements are randomly set in an angular interval (modulus 2π) around the configuration, independently for each element. We resort to the correlation coefficient test for authentication, with a threshold achieving a target probability of false alarm P_{FA} (i.e., the probability of wrongly authenticating a message coming from Eve) and probability of misdetection P_{MD} (i.e., the probability of wrongly discarding a message from Alice).

To verify the performance of the proposed method, we investigate the MD probability and FA probability accuracy vs. SNR. Eve is a dynamic trajectory where moving from $(0.5, 0.7, 2.6)$ m to $(1.5, 1.7, 2.7)$ m on XOY plane with 20 trajectories. We take the average channel results over the entire trajectory, and we conduct 5000 Monte-Carlo experiments. The SNR is set as $\{-10, -5, 0, 5, 10, 20\}$ dB, and the size of RIS is 2×4, i.e, 2 rows and 4 columns. From Figure 6, we see that higher SNR generally provides stronger security to a certain extent in the PLA authentication, and the proposed method can exhibit a stable authentication performance even in the presence of Eve's dynamic locations.

Figure 7 shows the MD probability and the FA probability by comparing the size of the RIS element and VLC channel without RIS in [16]. We collect the 2000 samples for the Alice-Bob communication link, another 2000 samples for the Eve-Bob communication link, and the SNR is set as 10 dB. Four sizes of RIS are considered: 1×1, 2×1, 2×2, 2×3, and 2×4 are considered. We notice that a large size significantly reduces the MD and FA probability, especially compared to the implementation without RIS.

We also investigate the case wherein Eve has perfect knowledge of the CSIs of channels between the RIS and Alice/Bob and channels without RIS. With RIS, Eve can continuously adjust her RIS phase to match as much as possible the channel between Alice and Bob, and hence impersonate Alice. However, in the case of VLC channel without RIS, Eve can easily mimic the behavior of the legitimate channel due to the reduced diversity. Here, Eve is located at $(0.5, 0.7, 2.6)$, which is different from Alice. Similarly, the position of the RIS is also different from

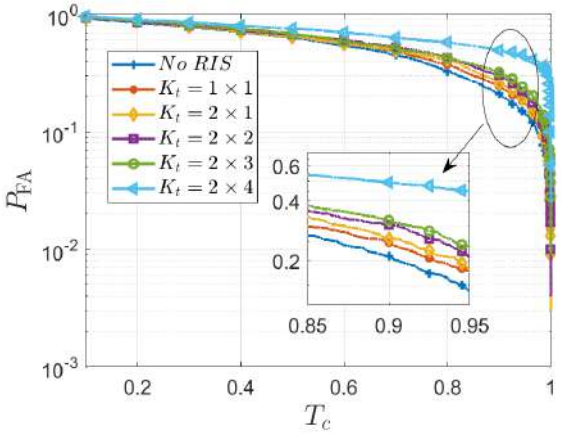


Fig. 8: False-alarm probability (P_{FA}) vs the threshold T_c of the correlation coefficient.

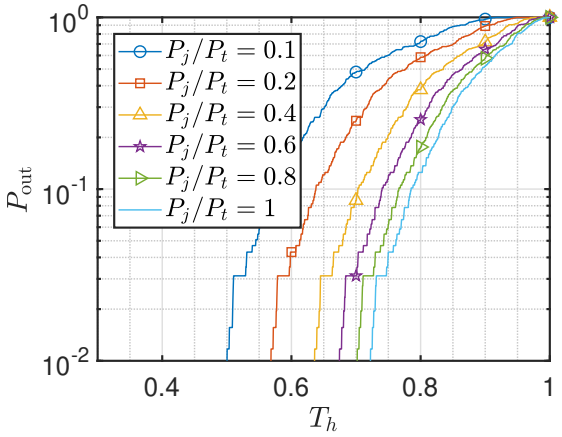


Fig. 9: Outage probability (P_{out}) with different jamming power values. RISs size $K_r = K_t = 2 \times 4$ and SNR= 15 dB.

Alice's RIS position. In addition, we consider the different sizes of RIS: $1 \times 1, 2 \times 1, 2 \times 2, 2 \times 3, 2 \times 4$, and set the SNR as 0 dB. Figure 8 shows the FA probability vs the threshold used at the receiver. Our aim is to show how good Eve is at impersonating Alice and hence cause a false alarm for varying threshold values at the receiver. We observe that the size of RIS increases the authentication FA probability obtained by varying the size of Eve's RIS for the random phase of each IRS element around the optimal configuration. However, Eve is not able to attack the system with probability 1.

Secrecy Analysis With the architecture proposed (see Figure 5), Bob's jammer is installed close to the RIS, and the jamming channel cannot be described using the far-field assumption. For this reason, we assume that P_J undergoes a deterministic path-loss attenuation in the near-field region at the RIS. We fix the location of Alice, Bob, the jammer, and the RIS while considering a grid $\mathcal{N}$ of Eve's locations. We validate our approach based on the outage probability defined as

$$P_{\text{out}} = \frac{\sum\limits_{n \in \mathcal{N}} \mathbb{1}\left(\hat{C}_s(n) - T_h \cdot \hat{C}_s|_{\max}\right)}{|\mathcal{N}|}, \tag{20}$$

where $\hat{C}_s|_{\max} = \max\limits_{n \in \mathcal{N}} \hat{C}_s(n)$, $|\mathcal{N}|$ denotes the cardinality of $\mathcal{N}$, $T_h \in [0, 1]$ is a variable we select to define the secrecy capacity threshold, and $\mathbb{1}$ is the indicator function, i.e., $\mathbb{1}(x) = 1$ if $x \geq 0$ and 0 otherwise. In other words, the outage probability (20) 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 $C_{\max}$. Notice that, when computing P_{out}, we use the secrecy capacity (17) to represent the worst-case scenario [12]. In the following, we consider a scenario with SNR of 15 dB. We notice that, while the receiver RIS rotation should be optimized to maximize the area secrecy capacity, the transmitter RIS configuration should be randomized at each challenge response. This ensures the non-predictability of the response and hence reduces the chances for the attacker to be able to eventually mimic a legitimate response.

Figure 9 shows the outage probability versus the threshold value T_{h} for different ratios between the transmit power P_t and the jamming power P_j. In the simulations, we considered both transmitting and receiving RISs to have size 2×4. We notice that when the ratio P_j/P_t increases, the outage probability decreases. However, we also notice that ratio values higher than 0.6 do not provide a significant performance increase, meaning that it is sufficient to limit the jamming power signal to approximately half of the transmit power. We also notice that the outage probability for $T_h \leq 0.5$ is very low, thus meaning that the worst-case secrecy capacity is always higher than half of the best-recorded value.

Figure 10 shows the outage probability versus the threshold value T_h for varying RIS sizes. We assume that both the transmitter and receiver RIS size coherently change (thus, $K_r = K_t$). We notice that an increasing RIS size provides lower outage probabilities for a given threshold value. In particular, we notice that, for the maximum considered size, less than 10% of possible Eve locations achieve a secrecy capacity lower than 0.8 times the maximum recorded value.

Results in both Figure 9 and Figure 10 confirm that our proposed optimization problem can guarantee high secrecy levels despite the randomness of our proposed non-LOS channel model (14).

8 Security Analysis

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.

Authentication Attack Resistance. Sender authentication refers to validating the sender's identity of a specific communication. This property is guaranteed by leveraging the channel's variability given by both the statistical channel

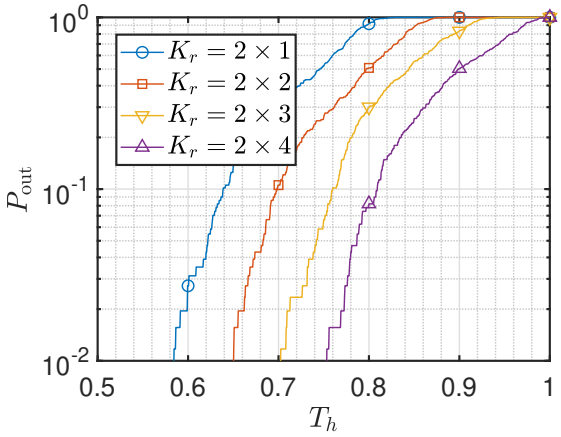


Fig. 10: Outage probability (P_{out}) versus threshold (T_c) with different transmitter and receiver RIS size (K_r) values and SNR $= 15$ dB.

model and the transmitter RIS configurability. Via numerical simulations, we proved that the physical space separation between Alice and Eve and the consequent channel realization difference cannot be compensated by a proper Eve's RIS configuration. Thus, our solution is effective against impersonation attacks.

Confidentiality. The confidentiality of the message is ensured by the jamming phase. Indeed, only Bob knows the jamming points and, therefore, can reconstruct the message. Since Bob jams a maximum of M bits out of the total N bits transmitted by Alice, an attacker must calculate 2^M combinations to force the message. This property protects from *Eavesdropping*.

Integrity. Two potential strategies exist for an adversary to modify the message: instantaneously during transmission or subsequently. The former is unfeasible due to the anti-replay characteristic. At the same time, the latter is likely to corrupt the embedded watermark, resulting in discrepancies during demodulation and watermark authentication. Our proposal guarantees integrity, preventing *Message Injection* and *Message Modification* attacks. Moreover, the integrity verification feature can detect anomalous message alterations should the attacker engage in jamming to disrupt the transmission.

Jamming Resistance. Leveraging the watermark, our protocol exhibits a fortified defense against *Adversarial Jamming* attacks. In an optimal scenario, the adversary would jam up to N_W frames selected for the watermark's transmission; Bob can still reconstruct the authentic message using the WBPLSec algorithm.

Replay attack Resistance. Typically, protecting against replay attacks requires synchronization and a nonce exchange between communicating entities. In our framework, resistance to replay attacks is inherently built-in, as Bob will randomly jam a selection of bits. This information remains exclusively known to him, ensuring that each subsequent message exchange involves a unique set of jammed bits, thereby rendering the reuse of previous messages by Eve futile. Consequently, this mechanism affords protection against both *Replay* and *Message Injection Attacks*.

If Eve chooses to jam alternative frames that are not protected by the same knowledge that Bob possesses, our mechanism may be susceptible to the adverse effects of such interference. In other words, while the system is designed to resist jamming to some degree, it is only partially immune to some forms of jamming attacks, particularly those not anticipated in the protection strategy.

9 Conclusion

VLCs represents an enabling technology for future wireless communications and comes with peculiar security needs. In this paper, we proposed the first multi-RIS-based physical layer solution to guarantee authenticity, confidentiality, and integrity. Our study thoroughly examined the security features of our approach, emphasizing its resilience to various threats. Indeed, using sender authentication, our methodology defends against impersonation attacks and leverages the statistical channel model and transmitter RIS reconfigurability. We ensure message confidentiality through jamming and inhibiting eavesdropping. Our approach maintains message integrity, preventing injection and modification attacks. Even amid adversarial jamming, our system can reconstruct the original message. We also protect against replay attacks with unique jamming patterns per message. However, potential vulnerabilities exist, especially to specific jamming attacks on other frames.

We developed a novel model for the statistical characterization of the non-LOS VLC channel modelling light reflected by the RIS. Through a probabilistic analysis using the P_{MD} and P_{FA} metrics, we showed that the physical separation between transmitters implies the generation of channels that are different enough to be used for authenticating the transmitter. Whereas the secrecy analysis showed that we can guarantee the confidentiality of the communication despite the randomness of the non-LOS channel model. Our work represents a first step towards more secure VLC communications and will open up a thread of subsequent studies aiming at the validation on a real-world testbed and further explorations of the security needs and implications of multi-RIS architectures in VLC.

References

[1] 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.

[2] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas, J. S. Thompson, E. G. Larsson, M. D. Renzo, W. Tong, P. Zhu, X. Shen, H. V. Poor, and L. Hanzo, "On the road to 6g: Visions, requirements, key technologies, and testbeds," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 905–974, 2023.

[3] M. A. Uusitalo *et al.*, "6G Vision, Value, Use Cases and Technologies From European 6G Flagship Project Hexa-X," *IEEE Access*, vol. 9, pp. 160 004–160 020, 2021.

[4] F. Naeem, M. Ali, G. Kaddoum, C. Huang, and C. Yuen, "Security and privacy for reconfigurable intelligent surface in 6g: A review of prospective applications and challenges," *IEEE Open Journal of the Communications Society*, 2023.

[5] "Hexa-X," https://hexa-x.eu/.

[6] A. R. Ndjiongue, H. C. Ferreira, and T. M. Ngatched, "Visible light communications (vlc) technology," *Wiley Encyclopedia of Electrical and Electronics Engineering*, pp. 1–15, 1999.

[7] 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, 2013.

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

[9] Y. Tanaka, S. Haruyama, and M. Nakagawa, "Wireless optical transmissions with white colored led for wireless home links," in *11th IEEE International Symposium on Personal Indoor and Mobile Radio Communications. PIMRC 2000. Proceedings (Cat. No. 00TH8525)*, vol. 2. IEEE, 2000, pp. 1325–1329.

[10] 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*, pp. 156–162, 2021.

[11] A. R. Ndjiongue, T. M. Ngatched, and O. A. Dobre, "Impact of the refractive index on the achievable rate of liquid crystal-based digital-ris indoor vlc systems," *IEEE Photonics Journal*, vol. 15, no. 1, pp. 1–6, 2022.

[12] S. Soderi, A. Brighente, F. Turrin, and M. Conti, "VLC Physical Layer Security through RIS-aided Jamming Receiver for 6G Wireless Networks," in *2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, 2022, pp. 370–378.

[13] R. Kaur, B. Bansal, S. Majhi, S. Jain, C. Huang, and C. Yuen, "A survey on reconfigurable intelligent surface for physical layer security of next-generation wireless communications," *IEEE Open Journal of Vehicular Technology*, 2024.

[14] G. Blinowski, "Security of visible light communication systems—a survey," *Physical Communication*, vol. 34, pp. 246–260, 2019.

[15] A. R. Ndjiongue, T. M. N. Ngatched, O. A. Dobre, and H. Haas, "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.

[16] L. Yin, W. O. Popoola, X. Wu, and H. Haas, "Performance evaluation of non-orthogonal multiple access in visible light communication," *IEEE Transactions on Communications*, vol. 64, no. 12, pp. 5162–5175, 2016.

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

[18] M. Akram, L. Aravinda, M. Munaweera, G. Godaliyadda, and M. Ekanayake, "Camera based visible light communication system for underwater applications," in *2017 IEEE International Conference on Industrial and Information Systems (ICIIS)*. IEEE, 2017, pp. 1–6.

[19] 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.

[20] M. A. Arfaoui, A. Ghrayeb, and C. M. Assi, "Secrecy performance of multi-user miso vlc broadcast channels with confidential messages," *IEEE Transactions on Wireless Communications*, vol. 17, no. 11, pp. 7789–7800, 2018.

[21] Z. Chen and H. Haas, "Physical layer security for optical attocell networks," in *2017 IEEE International Conference on Communications (ICC)*. IEEE, 2017, pp. 1–6.

[22] F. Wang, R. Li, J. Zhang, S. Shi, and C. Liu, "Enhancing the secrecy performance of the spatial modulation aided vlc systems with optical jamming," *Signal Processing*, vol. 157, pp. 288–302, 2019.

[23] 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*, pp. 3042–3056, 2020.

[24] Y. Yang and M. Guizani, "Mapping-varied spatial modulation for physical layer security: Transmission strategy and secrecy rate," *IEEE Journal on Selected Areas in Communications*, pp. 877–889, 2018.

[25] X.-Q. Jiang, M. Wen, H. Hai, J. Li, and S. Kim, "Secrecy-enhancing scheme for spatial modulation," *IEEE Communications Letters*, vol. 22, no. 3, pp. 550–553, 2017.

[26] P. Mursia, F. Devoti, V. Sciancalepore, and X. Costa-Pérez, "Rise of flight: Ris-empowered uav communications for robust and reliable air-to-ground networks," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1616–1629, 2021.

[27] 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*, vol. 17, no. 1, pp. 37–46, 2021.

[28] S. Li, B. Duo, M. Di Renzo, M. Tao, and X. Yuan, "Robust secure uav communications with the aid of reconfigurable intelligent surfaces," *IEEE Transactions on Wireless Communications*, 2021.

[29] K. Xu, S. Gong, M. Cui, G. Zhang, and S. Ma, "Statistically robust transceiver design for multi-ris assisted multi-user mimo systems," *IEEE Communications Letters*, vol. 26, no. 6, pp. 1428–1432, 2022.

[30] B. C. Nguyen, Q.-N. Van, L. T. Dung, T. M. Hoang, N. V. Vinh, and G. T. Luu, "Secrecy performance of multi-ris-assisted wireless systems," *Mobile Networks and Applications*, pp. 1–14, 2023.

[31] T. Shen, W. Cai, Y. Lin, S. Zhang, J. Lin, F. Shu, and J. Wang, "Multi-ris aided 3d secure precise wireless transmission," *Journal of Communications and Networks*, vol. 24, no. 5, pp. 541–554, 2022.

[32] Z. Chen, J. Tang, X. Y. Zhang, Q. Wu, G. Chen, and K.-K. Wong, "Robust hybrid beamforming design for multi-ris assisted mimo system with imperfect csi," *IEEE Transactions on Wireless Communications*, vol. 22, no. 6, pp. 3913–3926, 2023.

[33] A. M. Abdelhady, O. Amin, M.-S. Alouini, and B. Shihada, "Revolutionizing optical wireless communications via smart optics," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 654–669, 2022.

[34] S. Soderi and R. De Nicola, "6G Networks Physical Layer Security Using RGB Visible Light Communications," *IEEE Access*, vol. 10, pp. 5482–5496, 2022.

[35] 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.

[36] S. Soderi, "Acoustic-Based Security: A Key Enabling Technology for Wireless Sensor Network," *International Journal of Wireless Information Networks*, vol. 27, no. 1, pp. 45–59, nov 2019.

[37] J. Xu, W. Xu, J. Zhu, D. W. K. Ng, and A. Lee Swindlehurst, "Secure massive mimo communication with low-resolution dacs," *IEEE Transactions on Communications*, vol. 67, no. 5, pp. 3265–3278, 2019.

[38] R. Kaur, B. Bansal, S. Majhi, S. Jain, C. Huang, and C. Yuen, "A survey on reconfigurable intelligent surface for physical layer security of next-generation wireless communications," *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 172–199, 2024.

[39] F. Naeem, M. Ali, G. Kaddoum, C. Huang, and C. Yuen, "Security and privacy for reconfigurable intelligent surface in 6g: A review of prospective applications and challenges," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 1196–1217, 2023.

[40] S. Pergoloni, Z. Mohamadi, A. M. Vegni, Z. Ghassemlooy, and M. Biagi, "Visible light indoor positioning through colored leds," in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2017, pp. 150–155.

[41] A. K. Jain, *Fundamentals of digital image processing*. Prentice-Hall, Inc., 1989.

[42] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2021.

[43] M. Shakiba-Herfeh, A. Chorti, and H. Vincent Poor, *Physical Layer Security: Authentication, Integrity, and Confidentiality*. Cham: Springer International Publishing, 2021, pp. 129–150.

[44] S. Tomasin, H. Zhang, A. Chorti, and H. V. Poor, "Challenge-response physical layer authentication over partially controllable channels," *IEEE Communications Magazine*, vol. 60, no. 12, pp. 138–144, 2022.

[45] S. Soderi, G. Dainelli, J. Iinatti, and M. Hämäläinen, "Signal fingerprinting in cognitive wireless networks," in *2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, 2014, pp. 266–270.

[46] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *Journal of Communications and Information Networks*, vol. 5, no. 3, pp. 237–264, 2020.

[47] 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.

[48] S. Soderi, R. Colelli, F. Turrin, F. Pascucci, and M. Conti, "Senecan: Secure key distribution over can through watermarking and jamming," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 3, pp. 2274–2288, 2023.

[49] J. G. Proakis, *Digital communications*. Boston: McGraw-Hill, 2000.

[50] L. Jia, J.-Y. Wang, N. Huang, Z. Yang, and M. Chen, "On the mutual information of vlc systems employing color-shift keying," *IEEE Photonics Technology Letters*, vol. 29, no. 17, pp. 1427–1430, 2017.

[51] A. R. Ndjiongue, T. M. N. Ngatched, O. A. Dobre, and H. Haas, "Re-configurable intelligent surface-based vlc receivers using tunable liquid-crystals: The concept," *Journal of Lightwave Technology*, vol. 39, no. 10, pp. 3193–3200, 2021.
[52] J. Xu, C. Yuen, C. Huang, N. Ul Hassan, G. C. Alexandropoulos, M. Di Renzo, and M. Debbah, "Reconfiguring wireless environments via intelligent surfaces for 6g: reflection, modulation, and security," *Science China Information Sciences*, vol. 66, no. 3, p. 130304, 2023.
[53] S. Aboagye, T. M. Ngatched, O. A. Dobre, and A. R. Ndjiongue, "Intelligent reflecting surface-aided indoor visible light communication systems," *IEEE Communications Letters*, 2021.
[54] Z. Wang, L. Liu, and S. Cui, "Channel estimation for intelligent reflecting surface assisted multiuser communications: Framework, algorithms, and analysis," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, pp. 6607–6620, 2020.
[55] S. Sun, F. Yang, J. Song, and R. Zhang, "Intelligent reflecting surface for mimo vlc: Joint design of surface configuration and transceiver signal processing," *IEEE Transactions on Wireless Communications*, vol. 22, no. 9, pp. 5785–5799, 2023.
[56] M. M. Selim and S. Tomasin, "Physical layer authentication with simultaneous reflecting and sensing ris," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*. IEEE, 2023, pp. 1–5.
[57] A. Brighente, F. Formaggio, M. Centenaro, G. M. Di Nunzio, and S. Tomasin, "Location-verification and network planning via machine learning approaches," in *2019 International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOPT)*. IEEE, 2019, pp. 1–7.
[58] F. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R.-F. Liao, and J. Chen, "Threshold-free physical layer authentication based on machine learning for industrial wireless cps," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6481–6491, 2019.
[59] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5g and beyond wireless networks," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 55–61, 2019.
[60] ETSI TR 138 213 V15.3.0, "Physical layer procedures for control (release 15)." 3GPP, Tech. Rep., Oct. 2018.
[61] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[62] 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.

Simone Soderi (SMIEEE) received his M.Sc. degree in 2002 from the University of Florence, and his Dr.Sc. degree in 2016 from the University of Oulu, Finland. His expertise ranges from cybersecurity and wireless communications to embedded systems. He is currently an Assistant Professor at the IMT School for Advanced Studies Lucca, Italy, and an Adjunct Professor at the University of Padua, Italy, where he teaches in the master's degree program in cybersecurity. His research topics include cybersecurity for critical infrastructure systems, 6G, covert channels, network security, physical layer security, electromagnetic emission security, VLC, and UWB. He is an Associate Editor for IEEE Transactions on Information Forensics and Security, and he has been a TPC member of several conferences and a reviewer of many IEEE Transactions. He is the scientific leader of an industrial project investigating network security. Dr. Soderi has published journal and conference papers and book chapters. He holds five patents on wireless communications and vehicle positioning.

Alessandro Brighente is an Assistant Professor at the University of Padova, Italy. He obtained his Ph.D. in Information Engineering from the University of Padova in 2021. He was visiting researcher at Nokia Bell Labs, Stuttgart in 2019, the University of Washington, Seattle, in 2022 and 2023, and TU Delft, The Netherlands, in 2023. He served as TPC for several international conferences, including ESORICS, and WWW. He is the program chair for DevSecOpsRO, in conjunction with EuroS&P 2023, and CPSIoTSec, in conjunction with CNS 2023. He has been a guest editor for IEEE Transactions in Industrial Informatics and for Elsevier's Computers and Security. He is part of several industrial and research projects, including EU-funded ones. His current research interests include security and privacy in cyber-physical systems, wireless communications, the Internet of Things, and Blockchain.

Saiqin Xu is currently working toward the Ph.D. degree with National Laboratory of Radar Signal Processing, Xidian University, Xi'an, China. Since October 2022, she has been a Visiting Student with SPRITZ Security and Privacy Research Group, Department of Mathematics, University of Padova, Italy, with the support of China Scholarship Council. Her research interests include signal processing, parameter estimation, radar systems engineering, artificial neural networks and security for wireless communications.

Mauro Conti is a Full Professor at the University of Padua, Italy. He is also affiliated with TU Delft and University of Washington, Seattle. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Post-Doc Researcher at Vrije Universiteit Amsterdam, The Netherlands. In 2011 he joined as Assistant Professor at the University of Padua, where he became Associate Professor in 2015, and Full Professor in 2018. He has been Visiting Researcher at GMU, UCLA, UCI, TU Darmstadt, UF, and FIU. He has been awarded a Marie Curie Fellowship (2012) by the European Commission, and a Fellowship by the German DAAD (2013). His research is also funded by companies, including Cisco, Intel, and Huawei. His main research interest is in the area of Security and Privacy. In this area, he published more than 450 papers in the topmost international peer-reviewed journals and conferences. He is Editor-in-Chief for IEEE Transactions on Information Forensics and Security, Area Editor-in-Chief for IEEE Communications Surveys & Tutorials, and has been Associate Editor for several journals, including IEEE Communications Surveys & Tutorials, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, and IEEE Transactions on Network and Service Management. He was Program Chair for TRUST 2015, ICISS 2016, WiSec 2017, ACNS 2020, CANS 2021, and General Chair for SecureComm 2012, SACMAT 2013, NSS 2021, and ACNS 2022. He is a Fellow of the IEEE, Senior Member of the ACM, and Fellow of the Young Academy of Europe.