LIBERO: LIght Bias as effective countermeasure against EavesdROpper attacks

Valeria Loscri, Mauro Biagi

LIBERO: LIght Bias as effective countermeasure against EavesdROpper attacks

Valeria Loscri, *Senior Member, IEEE* and Mauro Biagi, *Senior Member, IEEE*

***Abstract*—Visible Light Communication (VLC) is expected to enable a wide range of applications in the next generation wireless networks. These applications are recognized as sensitive and prone to dangerous threats. So far, VLC research activities have been more focused on developing high data rate solutions and more robust systems for both indoor and outdoor applications, with a reduced focus on the security aspects. This is mostly due to the fact that VLC systems are based on short range and occurs in line of sight and it is then considered inherently secure by design. The specific characteristics of VLC systems make the traditional countermeasures adopted in radio-frequency-based systems not applicable, with a concrete need to conceive ad hoc solutions. Basing on these premises, in this work we consider a physical layer perspective by analyzing the intrinsic properties of visible light signals so as to develop a secure by design VLC system to be used in downlink. By exploiting the light bias, we guarantee an improved security level in respect of eavesdropper attack by granting also a good illumination level. A key aspect of this work is that the proposed solution does not rely on external devices or extra hardware.**

***Index Terms*—Light Bias, Eavesdropper, Countermeasures, Optical Wireless, Visible light communications**

I. Introduction

VISIBLE light communication (VLC) has become a hot research topic, and it is still attracting huge interest form industry as well as from academia. It is considered among the key communication technology for the next generation wireless communication systems. This is also demonstrated by the huge investment of tech companies like Nokia and Huawei on VLC-based systems [1], [2]. Most of the work at this extent, has been devoted to improve data rate, "chasing" very high data rate to enable new applications [3], [4], [5]. There are several advantages that have been associated to VLC, making it more secure by design in respect of the traditional wireless communication based on radio frequency (RF). One of the most recognised characteristics of VLC is related to the RF immunity to RF signals, based on the fact that VLC occurs at higher frequency (400-790 THz). Another feature of visible signal is not penetrability through walls. Moreover, eavesdropping attacks have been longer considered difficult to implement in a VLC system, due to the fact that a potential eavesdropper has to be on the same line of the transmitter-receiver communication to intercept data. Based on these premises, the research on VLC has been focused on the performance, robustness and resilience of the communication systems, much more than on security aspects.

Recently, it has been demonstrated that VLC systems are prone and vulnerable to certain types of attacks. Just as an example, in [6], the authors have demonstrated that the RF immunity of VLC is not available, and RF transmissions can interfere with VLC transmissions [6]. Based on the principle "what-you-see-is-what-you-get" that is specific for VLC, eavesdroppers can quite easily retrieve light signals at different locations, due to the diffusiveness of the light. This specific threat can apply both indoor and also from outdoor, when windows on the walls permit the creation of gaps to make the light signals to exit, creating potentially dangerous data leakage [7]. In [8], the authors have theoretically proved the effectiveness of an eavesdropper attack, through existing door gaps. VLC channels are characterized with very specific features, being a mix of specular and diffusive reflection. This makes this type of channel quite different than RF counterpart, where the dominant behaviors is dictated by the multipath, with several signal paths that can be added or subtracted to each other. In VLC systems, and above all in indoor VLC applications, there is a quite complex combination of paths reflected by the whole environment. This specificity makes in sort that traditional approaches developed for RF-based systems, cannot be applied to the VLC context and different schemes have to be conceived explicitly accounting of the characteristics of visible signals.

Even though there are some recent solutions developed for RF-based wireless systems related to advanced smart jamming attacks [9], [10], [11], these approaches are not suitable for VLC systems. For VLC systems, several security approaches in literature are developed at higher layers of the protocol stack, i.e., application layer, through access network policy, reinforced password, etc. In contrast with these approaches, we aim to consider a physical layer perspective and leverage on the specific features of a VLC system to implement an eavesdropper resilient system. Our work aims at proposing a security solution that is implemented on the transmitter and receiver nodes, without requiring any supplementary devices or equipment.

In this work, we implement an amplitude-hopping (bias-hopping from now on) that recall the time-hopping of Ultra Wide Band systems as well as frequency hopping of Bluetooth technology even though in the case of amplitude bias, subtraction is needed. In fact, the idea is to leverage the combination of light bias to enable a secret communication between a transmitter (Alice) and a receiver (Bob) nodes. Our system

Valeria Loscri is with FUN Team of Inria Lille, France (e-mail: valeria.loscri@inria.fr).

Mauro Biagi is with the Department of Information, Electrical, and Telecommunication (DIET) engineering, "Sapienza" University of Rome, Via Eudossiana 18, 00184 Rome, Italy (e-mail: mauro.biagi@uniroma1.it).

hinders the correct decoding for an eavesdropper (Eve) node, also when it is in its best and more favourable conditions and can acquire as much as information as possible.

To the best of our knowledge, this is the first work investigating the possibility to exploit light bias to implement a security VLC system. The main contributions of our study can be summarized as follows:

- we formulate a security scheme robust against eavesdropper attacks, based on the exploitation of light bias as unique *discrete* signature, between a pair transmitter-receiver;
- we consider different combination of light bias levels and we provide a detailed evaluation of the impact of this parameter on the security of the system also by detailing the receiver mechanism utilized by Bob and Eve;
- we evaluate the impact of the scheme also on illumination level in terms of flickering and dimming;
- we evaluate the impact of the frequency of changing the light bias levels, in terms of security effectiveness;
- we validate the security robustness in respect of different levels of knowledge of Eve on the systems and prove that the system is robust also in the case of high level of knowledge from Eve side.

REMARK: It is worth to notice that we do not need to rely on knowledge of the channel, location of the eavesdropper or the presence of the eavesdropper itself. Indeed, the implementation of our solution is completely independent on all these features, making the solution suitable also in presence of multiple eavesdroppers. However, in order to grant secrecy the Alice-Bob link performance in terms of reliability is a bit worse with respect to the case in which no possible countermeasures against passive attacks are considered. Besides, we consider Line-of-Sight (LoS) position for the eavesdropper, putting it in the most favourable condition to "steal" data from the victims. Last, we detail the detection mechanism for Bob and Eve in order to evaluate both reliability and secrecy of the link directly by measuring the error rate.

The reminder of this paper is organized as follows. Section II revise the literature contributions regarding cyber attacks, and in particular eavesdropper attacks in VLC systems and the main countermeasures adopted right now. In Section III, we present the specific threat model and characterize the system in terms of illumination. Section IV describes the detection approach implemented at the receiver stage (Bob) and at eavesdropper stage (Eve). In Section V, we provide evaluation and discussion of our system. Finally, we conclude the paper and provide future perspective in Section VI.

II. Related Work

In this Section, we present the different contributions existing in literature showing the potential impact of eavesdropping attacks in Optical Wireless Communication (OWC) and the proposed countermeasures for eavesdropper attacks.

Eavesdropper attacks in OWC

OWC and more specifically VLC based networks, are considered to be resilient to eavesdropping attacks, by design. This is based on the consideration that light signals cannot penetrate walls or objects. Just recently, there have been an increasing interest to prove the resilience of OWC/VLC in respect of different cyber security attacks, such as jamming and eavesdropping. One of the first contributions in this sense is given in [8]. The authors provide an experimental validation of an eavesdropping model exploiting degraded signal-to-noise ratio (SNR), based on the exploitation of secondary or reflected paths. This seminal work is important, since it demonstrates the vulnerability of VLC networks. A further demonstration of the feasibility to eavesdrop a VLC system is provided in [12], where the authors provide a quite accurate characterisation of the eavesdropping channel in different scenarios, both via simulation and through experiments. They conclude that an eavesdropper can perform a successful attacks also outside the expected coverage area of the VLC infrastructure. In [13], the authors derive the achievable secrecy rate of the multiple-input multiple-output (MIMO) VLC Gaussian wiretap channel. They consider both the cases of known and unknown position of the eavesdropper. In [14], authors further confirm that network security in VLC systems is an important challenge and focus on signal reflections and their impact on secrecy performance in a system under eavesdropper attack. Wang et. al consider a generalized space-shift keying (GSSK) Visible Light Communication (GSSK-VLC) and provide a detailed secrecy analysis of the system. they also provide the pairwise error probability and bit error rate of GSSK-VLC. They derive some closed-form expressions for the error and propose an optimal LED pattern selection algorithm. An advanced approach combining VLC side channel and demonstrating the data leakage in VLC systems is proposed in [15], where the authors demonstrate experimentally that visible light signals are affected by RF signal leakage that can be sniffed by an eavesdropper even in presence of obstacles, such as walls. In [16], the authors demonstrate the impact of eavesdropping attacks, by considering both diffusive and mirrored reflections. They derive the confidentiality of a VLC communication system, by considering the impact of several parameters, such as the locations of the different devices in the communication system, namely the transmitter, the receiver and the eavesdropper, the reflection characteristics, the bandwidth, etc. the secrecy outage probability (SOP) of an hybrid visible light and Rf system is derived in [17].

Eavesdropper countermeasures in OWC

Most of the existing works in literature implementing security solutions against eavesdropping attacks, are based on friendly jammer approaches, requiring complex decoding schemes at the receivers, that are not suitable in an IoT application perspective. Moreover, the approaches based on friendly jamming [18] work from a theoretical point of view since they are able to grant a good level of secrecy. Just for example the contribution in [18] refers to the distribution of a disturbing signal that is Gaussian truncated related to a light bias level. However, introducing a continuous distributed noise is not of practical use in symbol-by-symbol detection since the receiver must know the artificial noise value that belongs to a

continuous time interval, hence in principle, infinite values are possible. Moreover, the modulation used is continuous and Eve channel is required. In fact, in [18] no performance measured in terms of error rate have been reported. In [19], the authors conceive a friendly jammer solution, having no access to the transmitted data. The objective of the friendly jammer is to degrade the the signals received by the eavesdropper, while the quality of the legitimate receiver should be not impacted. The authors provide an evaluation of the secrecy capacity under the assumption that the jammer perfectly knows the channel characteristics of the eavesdropper. An enhanced approach is proposed by the same authors in [20], where a multiple-input, single-output (MISO) wiretap channel in VLC is considered. In this paper, the authors consider both, the case of perfectly known and unknown channel state information (CSI) at the transmitter. In [21], the authors reformulate the problem to derive optimal secrecy in a VLC MISO context, by taking into consideration amplitude constraint that occur in real-world applications. An assumption done by the authors is related to the position of the eavesdropper, that is expected to be located in a certain area. In particular, they derive a closed-form lower bound of the capacity, based on beamforming leveraging. Their main objective is to derive a robust beamforming approach by characterizing all the channel realization of a potential eavesdropper expected in a certain area. In [22], the author proposes an RGB (Red-Green-Blue) LED (Light Emitting Diode) friendly jammer, combined with a spread spectrum watermarking scheme. In particular, the authors consider the modulation of the message with a spreading spectrum sequence and then the message/payload is transmitted through the red link. The main drawback of this approach is that it does require extra hardware and relies on the combination of RGB LEDs, that in the optic of exploiting the same infrastructure for illumination and communication is not a doable solution if not properly optimized so as to provide the right color rendering which is not the case of [22]. Recently in [23] a mechanism including beamforming and artificial noise has been considered by requiring the presence of multiple LEDs. Moreover, the presence and position (and so channel) of the eavesdropper is required so leading to an analysis that represents the best case since, in real system, in general such information is not available. Besides, very recently, in [24] and [25] the problem of visible light communication links with secrecy problem have been tackled. In detail in [24] the analysis has been carried out under perfect Eve CSI or unknown CSI but with a focus on SINR, thus meaning, the impact of interference only in terms of power for what concerns the role played by the artificial noise. Analogously in [25] a constraint optimisation so as to take the signal below clipping, is considered still granting secrecy. The main issue is that secrecy is always reported in terms of secrecy capacity that, at last, depends on the SINR both at the main receiver and eavesdropper. Most of the contributions on countermeasures against eavesdropping attacks existing literature, focus on how to improve the secrecy capacity of systems under attacks. No detection mechanism have been reported especially by evaluating the number of errors the eavesdropper suffers from. In fact, it is possible that the SINR of Alice-Bob is high while the one of Alice-Eve is lower. However *lower* does not necessarily guarantee very poor performance for Eve, especially in modulation formats with few constellation symbols.

The first part of this section demonstrates the vulnerability of VLC systems in respect of eavesdropping attacks. The contributions in literature span from 2014 to 2022, demonstrating how this is a timely and urgent open challenge. In the second part, we provide a description of the most prominent literature for eavesdropping countermeasures, that is where we contribute to with our proposed approach LIght Bias as effective countermeasure against EavesdROpper attacks - LIBERO.

REMARK: Our solution is characterized with some interesting features as follows:

- Most of the previous contributions are based on two main approaches, Artificial Noise (AN) and friendly jamming. AN can be considered the closer approach to our solution, but it is worth to note that our bias-hopping approach, but in respect of AN, LIBERO does not rely on knowledge of Eve channel and is easily implementable since it is not based on the injection of a continuous distributed noise as the current AN-based contributions existing in literature. Moreover, very often, AN approaches are used jointly with precoding so requiring also CSI at the transmitter. Concerning friendly jamming approaches, most of them need extra hardware to implement the jamming attack, and generally, they are based on the assumption to know the eavesdropper position.

- The solution proposed in this work has the intrinsic advantage to be developed in the transmitter and receiver, without relying on extra hardware and can work also with a single LED and photodiode;

- It considers the detection and does not focus on capacity that does not give a practical evaluation of secrecy;

- It does not require complex decoding techniques at the receiver to decode the received messages and it does not require any knowledge about the possible presence or not of the eavesdropper as well as there is no need of the position knowledge for the eavesdropper.

III. System Model

In this section we explain the threat model considered in this work and the different aspects of the system model.

A. Threat Model

The threat model considered in this work is based on the spoofing, Tampering, Repudiation, Information disclosure, denial of services and Elevation of privilege, STRIDE threat models [26]. In particular, we consider the case of an eavesdropper trying to intercept data exchanged between two legitimate nodes. The specific category fitting our threat model is Information Disclosure. Our system is characterized by three main components as represented in Figure 1:

- Attacker: the attacker is a node equipped with the same components of a potential receiver in the system, i.e. a photodiode and decoding capability. In the scenario considered, the attacker is in proximity of the transmitter-receiver system and different conditions from the most

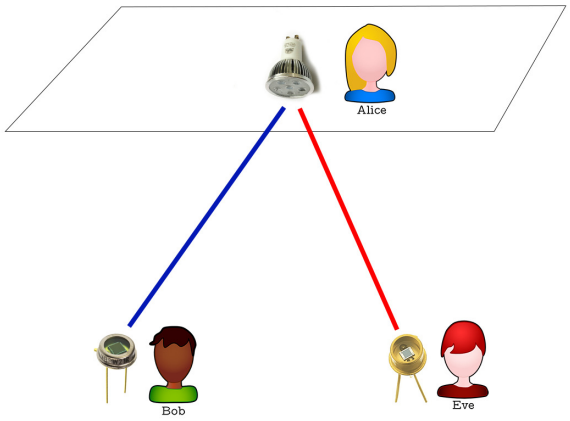

Fig. 1. Eavesdropping scenario. Eve is directly intercepting a VLC-based communication between Alice and Bob. She has similar channel conditions as Bob.

favourable to the worst case for the attacker will be considered. The most favourable condition is represented by the attacker being in line of sight (LoS) within the transmitter, and having the best channel conditions to intercept as much data as possible.

- Victim: the victims of our system are common users, using VLC system to exchange data, that are intercepted to steal their data. These common devices can be part of an Internet of Things system, an indoor wireless network, etc.
- Success of the Attack: the success of the attack is based on the capability of the attacker to intercept and successfully decode the stolen data. In this work, we rely on Bit Error Rate (BER) to quantify the attacks' success. In particular, when the BER approaches value that are not acceptable for the communication service, we consider the attack as failed.

B. Signal model

The Alice-Bob link is characterized by a M-ary pulse amplitude modulation (PAM) modulation and N possible light bias levels. Hence the signal describing the general symbol emitted is

$$s(t;n) = A_m^{(n)} x(t) + I_n \tag{1}$$

where $A_m^{(n)}$ is the m-symbol amplitude that can be positive or negative with respect to the light bias I_n and $x(t)$ is the pulse shape. About I_n, it is worth to highlight that it can change, in principle, symbol by symbol or, on the opposite, it can remain static for several symbols. As it will appear clearer in the following, let the light bias remain static is not a good strategy from the secrecy point of view since it allows Eve to *learn* about the modulation format and symbols. Moreover, the way in which the light bias can change symbol by symbol is linked to an initial seed shared between Alice and Bob (as in example it happens for Bluetooth frequency hopping [27] when with a mechanism of public and secret key the see is exchanged) and that allows the two actors of the communication to operated simultaneously with the right light bias. It has to be remarked that if the seed is generated by Bob and sent to Alice, due to the nature of uplink transmission, it is very difficult for Eve to capture this information. In fact, despite of what happens in the RF context where the emission by Bob can be heard by Eve, in VLC this is not true since the propagation is from floor to ceiling. Furthermore, it is important to note that differently from conventional PAM modulation format, here the amplitude range is referred to the minimum or maximum level. The minimum is zero while the maximum is P_{max}. In other words, if the light bias is above the half maximum value, the highest amplitude will coincide with maximum intensity allowed by the LED, and as a consequence the distance among symbols reduces with respect to the best case, that is, the above mentioned bias set to half-maximum. On the other hand, if the light bias is below the half maximum, then the lowest symbol will coincide with zero light emission. Also in this case the distance among symbols reduces. By observing the histogram

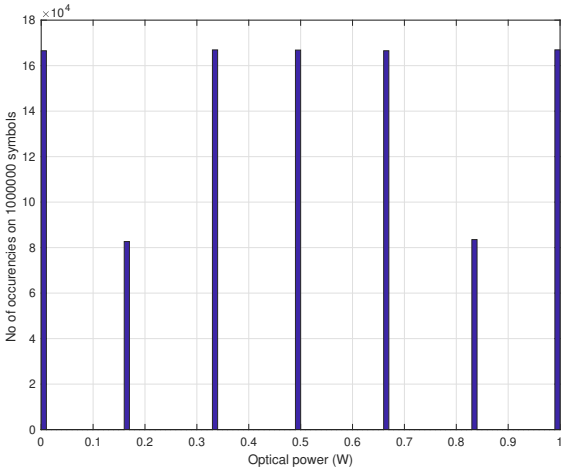

Fig. 2. Histogram of transmitting power levels for N=3 and M=4.

evaluated on 10^6 symbols reported in Fig.2 related to light intensity normalized to 1 Watt, it is possible to appreciate that for N=3 and M=4 we should expect to see 12 different amplitude levels. However what it is possible to infer from Fig.2 is that the distinct levels are 7 since 5 of them correspond to two different light bias levels and different symbols giving rise to the same emitted intensity. This can be justified by observing that the number of occurrences for 5 of 7 levels is twice the lowest (in the histogram) levels. How it becomes more evident later, while Bob has information about the rule allowing I_n to change in time due to the knowledge of the seed generating the pseudo-random sequence, Eve has not so the decoding procedure leads to mis-detection and so a less reliable Alice-Eve channel and consequently a more secure Alice-Bob link.

C. A brief discussion about illumination

When a light bias is not used in visible light communications a quite common assumption is to have uniformly distributed symbols since this is able to grant, for example of PAM or On-Off Keying modulation formats a reasonable level of illumination and no flickering. This assumption fails in case of long zero sequences since the LED remains off for several milliseconds. The use of a constant light bias grants the average desired illumination level. However this approach does not guarantee confidentiality to the communication process. On the other hand, having a light bias changing during the transmission, not only grants confidentiality but also allows the achievement of a good average illumination intensity and limited dimming. Flickering is absent also in the case of very long zero sequences transmitted due to the assumption of uniformly distributed light bias changes. However we must also consider that for high bandwidth signals, in order to achieve a sensible dimming, we need to transmit megabits of consecutive zeros that is more than uncommon.

IV. Detection Method

In this section we explain the detection approach adopted by the receiver stage (i.e., Bob) and the eavesdropper (i.e., Eve).

A. Detection operated by Bob

One of the key aspect of detection is the channel knowledge and, more, the light bias changing during time. In this regard once assumed the light bias level as known (since both Alice and Bob share the seed of pseudo-noise light bias generation) the detection follows the Maximum Likelihood criterion that, due to the Gaussianity of the thermal noise, can be reinterpreted as Euclidean distance detector. First of all let us focus on the received signal that, under the Lambertian Channel assumption [28] is as follows:

$$y(t) = \rho h x(t) + w(t) \tag{2}$$

where h is the above mentioned channel, ρ is the responsivity of the PD (measured in Ampere/Watt) and $w(t)$ is the thermal noise. Once assumed the electrical signal sampled at symbol period T_s we have for the k-symbol the following metric

$$d_m^2[k] = \left(y[k] - \rho\tilde{h}(A_m^{(n)} + I_n)\right)^2, m = 0, ..., M-1 \tag{3}$$

where the use of $\tilde{h}$ considers the possibility of basing the detection on an estimated version of the channel. Regarding the estimation procedure, it can be performed according to minimum mean square error mechanism [29], in example, during the key exchange for the seed transmission of light bias sequence. Hence, the decided symbol at k-th symbol time $\hat{m}[k]$ is given by

$$\hat{m}[k] = \underset{m=0,...,M-1}{\arg\min}\ d_m^2[k] \tag{4}$$

by selecting the minimum distance among the possible M ones, once I_n is known and consequently the M amplitudes $A_m^{(n)}$.

B. Detection operated by Eve

The case of detection operated by Eve is slightly different from Bob's one. In fact, in order to properly consider the performance achieved by Eve in eavesdropping the Alice-Bob link, we must focus on the a priori information Eve has on the communication scheme. Although the detection mechanism may be the same, the digital demodulation operated by Bob starts from the assumption of having information on M, N, channel and more, the law used by Alice for changing its light bias levels. Hence, we assume in the following three different detection approaches: 1) **Blind**, in the first detection mechanism named *blind*, at the beginning Eve is not aware of any parameter with the exception of channel between Alice and Eve, 2) **Semi-blind**, in the second mechanism, named as *semi-blind*, Eve is aware of the presence of N light biases and M different amplitudes for the modulation format even though it ignores the values, 3) **Clear**, in the third approach, the most favorable for Eve, named *clear*, Eve is aware of the M number of symbols as well as the number of light bias levels N and their intensity values. However, Eve ignores the law used by Alice, and share with Bob, for changing the I_n values.

- Blind Detection Regarding the blind detection mechanism, the problem is that Eve measures at first how many *amplitudes* are present and, also in the favorable assumption of low noise, the number of measured symbols is in general different from M and it is higher since Eve is not aware of the presence of N. In this way, the receiver operates on the basis of the number of symbols Eve hypothesizes Alice is transmitting (we indicate this number as μ) and the detection is operated on the basis of the received signal

$$y_e(t) = \rho_E h_e x(t) + w_e(t) \tag{5}$$

where ρ_E is the responsivity of the PD of Eve, h_e is the channel between Alice and Eve and $w_e(t)$ is the noise level at Eve. Then Eve computes

$$d_m^2[k] = \left(y[k] - \rho\tilde{h}_e(A_m^{(n)})\right)^2, m = 0, ..., \mu - 1 \tag{6}$$

and detect the symbol according to

$$\hat{m}[k] = \underset{m=0,...,\mu-1}{\arg\min}\ d_m^2[k] \tag{7}$$

It is important to notice that in (6) Eve does not subtract the light bias and, more, the minimum in (7) is checked among μ and not M.

- Semi-blind Detection Regarding the second mechanism, that is semi-blind, Eve tries to estimate the values of I_n on the basis of the observation of some symbols and by operating an histogram. In this case the detector works as follows. It evaluates

$$d_{m,n}^2[k] = \\ = \left(y[k] - \rho\tilde{h}_e(A_m^{(n)} + \tilde{I}_n)\right)^2, m = 0, ..., M-1, n = 1, ..., N \tag{8}$$

and detect the symbol according to

$$\hat{m}[k] = \underset{\substack{m=0,...,M-1,\\ n=1,...,N}}{\arg\min}\ d_{m,n}^2[k] \tag{9}$$

where we emphasize that in (8) the value of the light bias is I_n is only estimated. **- Clear Detection** Last in the clear detection we have that Eve does not use the estimated version of light bias but the real values utilized by Alice. However, we must emphasize that Eve is not aware about the light bias used currently since there is no information about the sequence utilized by the transmitter to switch between a light bias level and the next one in a temporal evolution. For this reason the minimum is not checked on M symbols but on NM possible combinations of light bias levels and modulation amplitudes hence the detection is operated as

$$d^2_{m,n}[k] = \\ = \left(y[k] - \rho\tilde{h}_e(A^{(n)}_m + I_n)\right)^2, m = 0, ..., M-1, n = 1, ..., N \tag{10}$$

and detect the symbol according to

$$\hat{m}[k] = \underset{\substack{m=0,...,M-1,\\ n=1,...,N}}{\arg\min} \; d^2_{m,n}[k] \tag{11}$$

It it important to highlight that (10) consider I_n in place of $\tilde{I}_n$ in (8).

C. Theoretical Performance

Let us analyze now the performance in terms of error probability. For what concerns Alice-Bob link, the error probability can be evaluated as

$$P^{(AB)}_E = \sum_{i=0}^{M-1} \sum_{\substack{j=0,\\ j\neq i}}^{M-1} P(\hat{m} = j, m = i) = \\ = \frac{1}{MN} \sum_{n=1}^{N} \sum_{i=0}^{M-1} \sum_{\substack{j=0,\\ j\neq i}}^{M-1} Q\left(\frac{h\rho|\Delta^{(n)}_{i,j}|}{\mathcal{N}_0 B}\right) \tag{12}$$

where $Q(.)$ is the so called Q-function, $\Delta^{(n)}_{i,j} = A^{(n)}_i - A^{(n)}_j$ is the distance among amplitudes related to the light bias I_n, while $\mathcal{N}_0 B$ measures the noise power. As expected, the higher is the distance, the better are the performance, moreover by high values of N the distance among symbols reduces so increasing the error probability.

Moving now to evaluate the performance of the Alice-Eve link we define I_s and I_z as two different light bias levels and their distance as $\delta_{sz} = I_s - I_z$. Since the detector operates the MN comparisons (differences) we have that in this case the error probability can be detailed as

$$P^{(AE)}_E = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{\substack{j=0,\\ j\neq i}}^{M-1} \sum_{s=1}^{N} \sum_{z=1}^{N} Q\left(\frac{h_e\rho_e|\Delta^{(s,z)}_{i,j} + \delta_{sz}|}{\mathcal{N}_0 B}\right) \tag{13}$$

For this latter expression the same considerations made for (12) hold with the difference that $\Delta^{(s,z)}_{i,j} = A^{(s)}_i - A^{(z)}_j$. Additionally the most important aspect is given by the term $\Delta_{i,j} + \delta_{sz}$ since when two light intensity levels coincide, thus meaning that we consider different i, j, s, z combinations giving rise to the same intensity level, the sum is zero thus meaning that this term brings a contribution to the error probability equal to 1/MN that is a not negligible contribution so justifying why this approach is powerful in granting unreliability on Alice-Eve link.

Remark on the presence of multiple LEDs

If from one hand is highly reasonable that more than one LED is present in a room, from the point of view of Eve opportunities to (passive) attack Alice-Bob, this is not necessarily a strength point. In fact, since Eve is interested in detecting the signals sent toward Bob, Eve must share the same Bob's attocell. In fact, if we assume that Eve is served by another access point it has no possibility of detecting signals sent by Alice. The only one possibility to capture the signal intended to Bob is to assume that each access point is simultaneously transmitting the data intended to Bob so leading to a huge network inefficiency since increasing the number of LEDs does not lead to increase access opportunities. However, also in this case the detection mechanism works exactly in the same way of assuming a single LED. The only one exception is referred to the case in which one is able to receive signals coming from different LEDs. In that case the (2) becomes

$$y(t) = \sum_{\ell} \rho h_\ell x(t) + w(t) \tag{14}$$

where h_ℓ is the channel coefficient from the ℓ-th access point to the reference receiver. It is possible to infer from this that the detection mechanisms consist in subtracting the sum of the channel coefficients $\sum_\ell h_\ell$ in place of the single one as in (3)

V. Numerical Evaluation

Let us start by detailing the assumption we made in setting up the system. We consider a room whose dimensions are 4 meters × 5 meters while the height is 3 meters even though the receiver is assumed to be 1 meter distant from the floor. We consider a single LED access point (Alice) posed in the position (2,2.5,3) thus meaning the center of the room on the ceiling.

We report in Table I the parameters we consider for simulations that are, for what concerns the receiver, identical for Bob and Eve. It is important to point out that, for propagation scenarios as that considered in this work and about the bandwidth we consider (10Mhz), such a bandwidth does not lead to intersymbol interference (ISI) since the pulse

TABLE I
Simulation parameters

Transmitting LEDs	
Transmit power ($P^{\text{LED}}_{\text{max}}$)	5W
Half-power angle ($\Phi_{1/2}$)	60°
Bandwidth (B_{LED})	10 MHz
Receiving PDs	
Field of view angle (Ψ)	60°
Area (A_{pd})	10 mm^2
Responsivity (ρ)	0.3 A/W
Bandwidth (B_{PD})	10 MHz

length is 100ns. Higher values till to 100Mhz work in the same way [30]. In case of bandwidth exceeding the above mentioned values, we encounter ISI effect that increases the error rate of both Alice-Bob and Alice-Eve links. Anyway, proper channel equalization mechanisms can help in lowering the error rate. However, the performance that each link can achieve cannot be better than those achievable with a no-ISI channel, thus meaning, that equalization does not impact on the security aspects of the link. Regarding the illumination level we can observe the fluctuations offered in the illumination service by the single LED when M=4 and N=9. In fact, in Fig.3 we report the lighting level by sampling it every 25ms that is the sampling rate of the human eye [31, Chapt.2]. We must remember that since the pulse length is 100ns (corresponding to a bandwidth of 10Mhz as from Table I) the average intensity takes into account the emission related to 250000 pulses. The continuous blue curve shows the average intensity in 5 seconds of transmission that is equivalent to 50 million symbols. Despite of the startup phase in the first few milliseconds, the average intensity is around 300 lumen and the fluctuation is around 1 lumen thus meaning 0.3% that is imperceptible by human eye. As a comparison

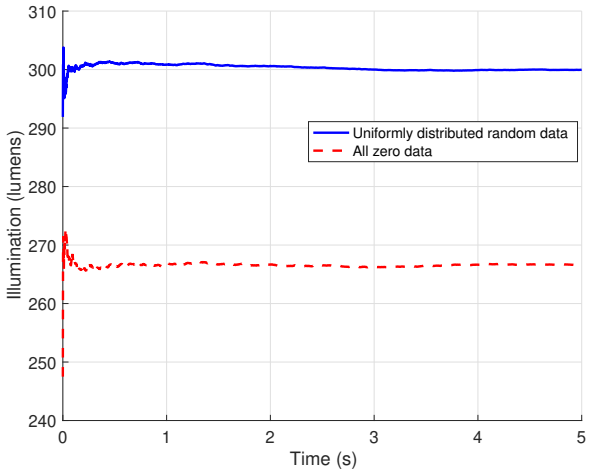

Fig. 3. Illumination levels expressed in lumen by considering different random symbols and all 0 symbols

we report still in Fig.3 the average intensity of a situation in which Alice sends a sequence characterized by all zeros. Usually, when a light bias is utilized and maximum intensity dynamic is taken into account, transmitting long sequences of 0 leads to have (for example in an on off keying modulation) LED turned off for several seconds. As it is possible to appreciate even in this particular case of all zero transmission (that is not so realistic because we are talking about very long zero sequence) we are in presence of a dimming with respect to the previous case since the illumination level is lower by 10%. However no fluctuations (flickering) is present. This is due to the different light bias that leads to have, especially when it is higher than the half-maximum, to transmit a certain level of light for representing the logical zero sequence.

Before considering performance results in terms of bit error rates on real channel, at first we show the error probability for Additive White Gaussian Noise channel related both to (12) and (13) when M=4 and two different values for N have been considered, namely N=3 and N=9 in Fig.4. Clear detection is used at Eve side. It is possible to appreciate that the behavior of the Alice-Eve link, reported in red dashed curves, is flat since by increasing the SNR value there is not a sensible reduction. This is due to the ambiguity in interpreting the intensity levels since, as specified, there are some light intensities that correspond to multiple light bias levels and symbol combinations. On the other hand the performance in

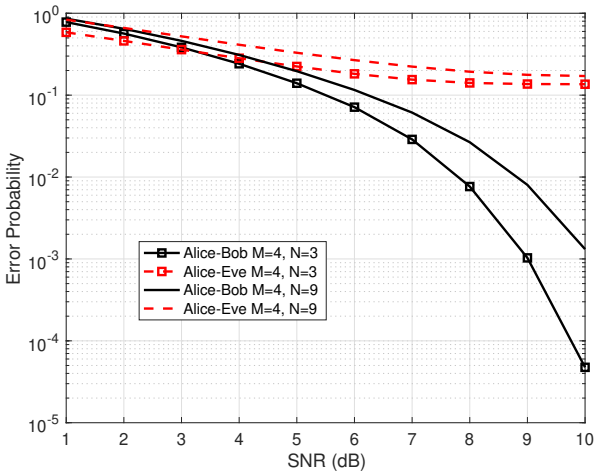

Fig. 4. Error Probability for Alice-Bob and Alice-Eve links for N=3 and N=9 and SNR ranging from 1dB to 10 dB.

terms of error probability for the Alice-Bob link shows that increasing the SNR lowers the number of errors so increasing the reliability. Moreover, by considering N=9 leads to have worse performance. This is due the fact that increasing the number of light bias levels lowers the relative distances among symbols. However, even though the performance of Alice-Eve in that case lowers (error probability increases) this is the price to paid to improve the secrecy of the link. In fact, it is possible to infer from Fig.4 that increasing N leads to a more secure connection since Alice-Eve link lowers its reliability.

Moving now to consider real channel realizations, we consider Eve in three different positions in the room namely (2,2.5,1), that is center of the room, (1,3,1) and (3,4.5,1) when N=7 and M=4 and we consider also a performance comparison with the scheme in [32] in Table II. Regarding the comparison with [32], we remove, with respect to the original contribution, the assumption of fading (since it is not suitable for indoor application) and the noise is considered as real Gaussian distribute (and not complex) since the comparison must be fair and in the same conditions. It is important to note that the first mechanism, that is blind detection, presents a file mismatch. In fact, while the original file sent is characterized by b bits, thus meaning that the number of symbol emitted is b/$\log_2$M=b/2, the blind detection mechanism perceives a higher number of constellation symbols (i.e., no of constellation symbol

measured is in this particular case 16 due to histogram) thus the number of bits of the file received by Eve is twice the length b/2 $\log_2 16$=2b. Hence, not only a comparison in terms of error rate is not possible since the two files have different length but more the file Eve has is not usable. Moving to the

TABLE II
ERROR RATE OF ALICE-EVE LINK FOR EVE AT THREE DIFFERENT ROOM COORDINATES IN THE ROOM, WITH N=7 AND M=4 AND FOR THE APPROACH IN [32]

Coordinates	blind	semi-blind	clear	Work in [32]
(2,2.5,1)	file mismatch	0.42	0.11	0.023
(1,3,1)	file mismatch	0.56	0.27	0.072
(3,4.5,1)	file mismatch	0.66	0.62	0.18

semi-blind approach for which we consider the detector to be aware about the number of light bias and symbols (but not the amplitudes of light bias), the error rate achieved is a value ranging for the considered positions from to 0.66 while for the clear detector where we assume to be aware of N, M and the levels for light bias, we achieve an error rate of that goes from 0.11 to 0.62. Dealing with the last column, we report the error rate that is a value ranging from 0.023 to 0.18 that is lower with respect to the clear detection so showing that for the approach in [32] the error rate is lower, hence the Alice-Bob link results to be less secure. Since the clear detection appears to the best performing approach (for Eve) among the three we mentioned, that is the worst from the Alice-Bob secrecy point of view, from now on we consider the worst case for the security of Alice-Bob link that is Eve aware of N, M and light bias, that is the clear detection we mentioned earlier.

Regarding secrecy, in place of reporting the secrecy capacity [32] that essentially evaluates how much the Alice-Bob is better (or worse) with respect to the Alice-Eve one, we resort to a different, and more practical, key performance indicator. In fact, the secrecy capacity is mainly based on the signal to noise ratio of the two different links. However, in the case when the Alice-Bob link is 3dBs better Alice-Eve one, it is very difficult to understand how much information Eve can capture. Instead, we focus on the error rate of both links, in order to understand if Bob can receive data reliably and Eve unreliably. Hence, in Fig.5 we start to evaluate the impact on the Alice-Bob and Alice-Eve links in terms of reliability by considering different values of N and M when both the receiving nodes are at coordinates (4,1,1).

As expected and known from digital modulation theory, the higher the number of symbols M, the higher the bit error rate since the distance among symbols, for an assigned transmitted power, is lower. This is true both for the Alice-Bob link indicated by the black continuous curves and the Alice-Eve ones characterized by the dashed red curves, see Figure 5. It is important to appreciate that having a low value of N is good in terms of error rate. This is true both for the Alice-Bob link and the Alice-Eve one. Regarding this latter, it is possible to appreciate that having a small number of light bias does not introduce *confusion* in the Eve detection hence, it is able to *understand* the light bias levels and, due to small intensity overlapping as shown in Fig.2, the error rate is low, thus

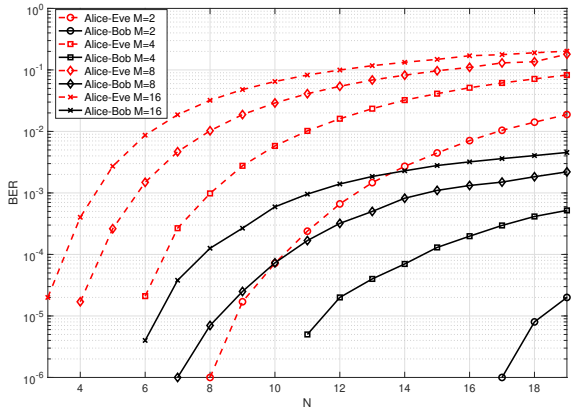

Fig. 5. Bit error rate of Alice and Bob in the center of the room for N ranging from 1 to 19 and M=2,4,8,16.

meaning that the link is not so secure since the data received is corrupted by very few errors. Increasing the number of light bias levels leads to reduce the distance among symbols. This is not true for each light bias utilized, however some of those reduce the distance. In fact, when a high number of light bias is considered, it means that some levels will be close to zero and P_{max} so limiting the amplitude range and so the distance. The main point to be considered is the vertical comparison for the same N value. In fact, if we consider N=14 we have for M=2 Bob with a BER lower that 10^{-6} while Eve is bigger than 10^{-3}. If we consider M=4 Bob is lower than 10^{-3} while Eve close to 2.7×10^{-2}. Hence, while Alice-Bob link is reliable, that Alice-Eve link is largely unreliable. Just in case one aims at improving Alice-Bob performance, it simply requires to have higher LED power. This lowers also Alice-Eve BER, however the reliability of this latter is still poor.

We show the performance in an arbitrary point since it is the only way of showing the impact of M and N simultaneously. However, in order to give evidence of the different reliability levels of the two links in the room, we report the map of BER for the Alice-Bob link in Fig.6 and for the Alice-Eve link in Fig.7. Looking at the color map in Fig.6, ranging from blue (BER=10^{-4}) to red (BER=0.7), we have for the Alice-Bob link presents for N=17 and M=4 a very low level of BER that is around 10^{-4} since the largest part of the room area is blue. We report the number of tile of the floor on the axis with the tile dimensions given by 25cm × 25 cm. Moving towards the room corners the value achieved for BER increases and this is due to a couple of factors. The first one is that the attenuation is higher with respect to other positions due to higher distance. The second one is tilting of the detector. We do not assume to have a direct pointing between Alice and Bob when Bob moves in the room since we consider the PD facing the ceiling in each point. Hence at the corners the yellow areas are just below 10^{-2}. Dealing now with the map related to the Alice-Eve link the behavior is totally different with respect to Alice-Bob one as evident from Fig.7. The range for the color map is the same in order to provide a quick and easy graphical comparison. The map is essentially

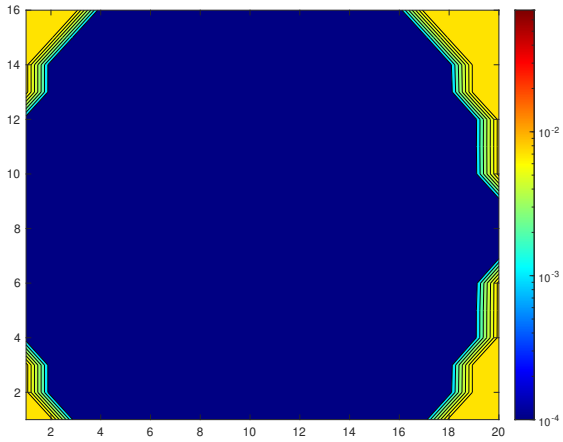

Fig. 6. Bit error rate for N=17, M=4 with the LED in the center of the room and Bob position spanning all the room.

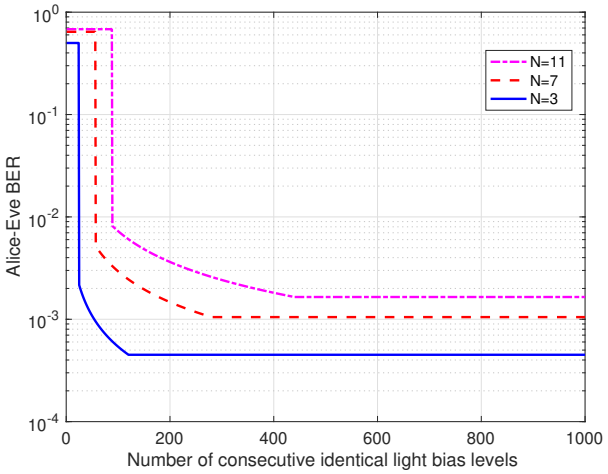

Fig. 8. Bit error rate for Alice-Eve link when light bias presents different duration (in terms of number of symbols) and for different N values (N=7, 11, 13) and M=4.

red with some differences in some areas. In particular, also

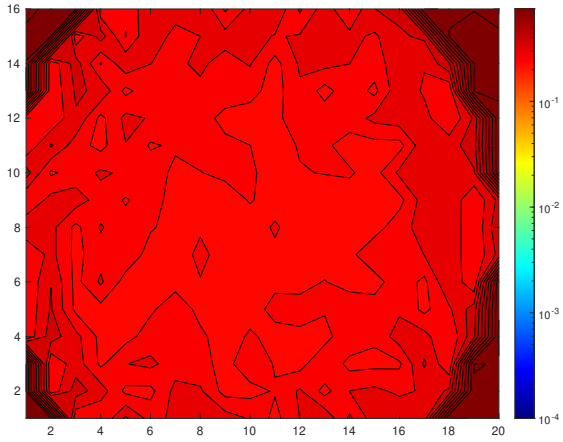

Fig. 7. Bit error rate for N=17, M=4 with the LED in the center of the room and Eve position spanning all the room.

in this case, the room corners present the worst performance while in the center of the room where the attenuation is the minimum one, the Alice-Eve BER is the lowest among the room. The point is that, despite of slightly different coloring, the error rate ranges from 3×10^{-2} to 0.7 so leading to have a really unreliable channel for what concerns Alice-Eve. An unreliable communication channel for the eavesdropper means highly secure Alice-Bob link. In fact, if we assume that we are transmitting a file having performance around 10% of error bits leads to have an useless file since it is heavily corrupted. This is also true for a possible call service since, still, 10% of errors is not acceptable for voice quality service that usually requires, among communication services, the lowest demanding performance. The last performance we detail is the impact of light bias persistence. In other words, we are interested in showing the error rate exhibited by Alice-Eve link when the light bias changes at each symbol or if it is maintained constant for a number of symbols. For this reason in Fig.8 we reported the error rate of the Alice-Eve link when we consider how much frequent (in terms of symbols) we change the light bias level with Eve assumed to be in the center of the room. It is possible to appreciate that the behavior of the three curves related to N=3, N=7 and N=11 present is quite similar. In particular, the higher N, the longer the time needed by Eve to track the symbols amplitudes. In fact, while for light bias changing within few symbols (or at each symbol) the performance are poor, maintaining a certain persistence of the same light bias rapidly lowers the error rate till to achieve the performance of an equivalent Alice-Bob since it allows Eve to perform detection without intensity ambiguities. The only one point to be highlight in this direction is that when the light bias changes, Eve needs time (and so symbols) to understand the light bias variations. Moreover, the higher N the higher the error rate since the distance among symbols decreases and so link reliability as for Alice-Bob link.

VI. Conclusion

In this work, we focused on security issues in VLC, by considering passive attacks performed by an eavesdropper node, Eve, trying to ex-filtrate data from a private VLC transmission between Alice and Bob. In particular, we proposed a new countermeasure approach, LIBERO, based on the exploitation of light bias as unique signature/fingerprinting to secures the communication between Alice and Bob without any knowledge about Eve presence/positions/channel. Through an extensive evaluation of the performance, with different settings in terms of number of modulation index and light bias, and in different scenarios, we demonstrated the effectiveness and robustness of LIBERO against eavesdropper attacks, in the most favourable conditions for the eavesdropper, namely when it is in the LoS intercepting the data. LIBERO is with some very interesting features, since in respect of previous

proposed solutions it does not rely on extra-hardware, it does not make assumptions on the Eve presence, position, etc. We are confident that LIBERO represents a strong initial solution for improving security in VLC systems, and we are planning to test it with different modulation schemes and scenarios. Last, the proposed scheme provides a good illumination quality since flickering is absent and dimming is really limited also in some particular (with very low probability) events.

ACKNOWLEDGMENT

This publication has been based upon work from COST Action CA19111 NEWFOCUS, supported by COST (European Cooperation in Science and Technology).

REFERENCES

[1] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6g," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 118–125, 2020.

[2] Z. Qadir, K. N. Le, N. Saeed, and H. S. Munawar, "Towards 6g internet of things: Recent advances, use cases, and open challenges," *ICT Express*, vol. 9, no. 3, pp. 296–312, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959522000959

[3] H. Chun, A. Gomez, C. Quintana, W. Zhang, G. Faulkner, and D. O'Brien, "A wide-area coverage 35 gb/s visible light communications link for indoor wireless applications," *Scientific Reports*, vol. 9, no. 1, p. 4952, 2019. [Online]. Available: https://doi.org/10.1038/s41598-019-41397-6

[4] P. Wang, L. Feng, G. Chen, C. Xu, Y. Wu, K. Xu, G. Shen, K. Du, G. Huang, and X. Liu, "Renovating road signs for infrastructure-to-vehicle networking: A visible light backscatter communication and networking approach," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3372224.3380883

[5] C. Zhang and X. Zhang, "Litell: Robust indoor localization using unmodified light fixtures," in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 230–242. [Online]. Available: https://doi.org/10.1145/2973750.2973767

[6] A. Costanzo, V. Loscrì, V. Deniau, and J. Rioult, "On the Interference Immunity of Visible Light Communication (VLC)," in *GLOBECOM 2020 - IEEE Global Communications Conference*, Tapei, Taiwan, Dec. 2020. [Online]. Available: https://hal.science/hal-02935606

[7] G. J. Blinowski, "The feasibility of launching rogue transmitter attacks in indoor visible light communication networks," *Wireless Personal Communications*, vol. 97, no. 4, pp. 5325–5343, 2017. [Online]. Available: https://doi.org/10.1007/s11277-017-4781-3

[8] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The spy next door: Eavesdropping on high throughput visible light communications," in *Proceedings of the 2nd International Workshop on Visible Light Communications Systems*, ser. VLCS '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 9–14. [Online]. Available: https://doi.org/10.1145/2801073.2801075

[9] V. B. A. C. M. L. V. Bout, Emilie Bout, "Evaluation of Channel Hopping Strategies Against Smart Jamming Attacks," in *ICC 2023 - IEEE International Conference on Communications*, Rome, Italy, May 2023. [Online]. Available: https://hal.laas.fr/INRIA/hal-03950904v1

[10] E. Bout, A. Brighente, M. Conti, and V. Loscri, "Folpetti: A novel multi-armed bandit smart attack for wireless networks," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–10.

[11] E. Bout, V. Loscri, and A. Gallais, "How machine learning changes the nature of cyberattacks on iot networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 24, no. 1, pp. 248–279, 2022.

[12] P.-J. R. Marin-Garcia I, Guerra V, "Study and validation of eavesdropping scenarios over a visible light communication channel," *MDPI Sensors (Basel)*, vol. 17, no. 11, 2017.

[13] M. A. Arfaoui, A. Ghrayeb, and C. Assi, "On the achievable secrecy rate of the mimo vlc gaussian wiretap channel," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017, pp. 1–5.

[14] S. Cho, G. Chen, H. Chun, J. P. Coon, and D. O'Brien, "Impact of multipath reflections on secrecy in vlc systems with randomly located eavesdroppers," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 2018, pp. 1–6.

[15] M. Cui, Y. Feng, Q. Wang, and J. Xiong, "Sniffing visible light communication through walls," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3372224.3419187

[16] J. Chen and T. Shu, "Statistical modeling and analysis on the confidentiality of indoor vlc systems," *IEEE Transactions on Wireless Communications*, vol. 19, no. 7, pp. 4744–4757, 2020.

[17] J. Liu, J. Wang, and Q. Wang, "Secrecy performance for hybrid rf/vlc df relaying systems," in *International Conference on Frontiers of Electronics, Information and Computation Technologies*, ser. ICFEICT 2021. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3474198.3478226

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

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

[20] ——, "Physical-layer security for indoor visible light communications," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 3342–3347.

[21] ——, "Physical-layer security for miso visible light communication channels," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1806–1818, 2015.

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

[23] S. Cho, G. Chen, and J. P. Coon, "Cooperative beamforming and jamming for secure vlc system in the presence of active and passive eavesdroppers," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 4, pp. 1988–1998, 2021.

[24] T. V. Pham and A. T. Pham, "Energy efficient artificial noise-aided precoding designs for secured visible light communication systems," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 653–666, 2021.

[25] T. V. Pham, S. Hranilovic, and S. Ishihara, "Design of artificial noise for physical layer security in visible light systems with clipping," in *2023 IEEE 20th Consumer Communications Networking Conference (CCNC)*, 2023, pp. 1054–1059.

[26] L. Kohnfelder and P. Garg, "The threats to our products," *Microsoft Interface*, 1999.

[27] Bluetooth, *Bluetooth Specifications*, 2023. [Online]. Available: https://www.bluetooth.com/specifications/specs/

[28] A. Petroni, G. Scarano, R. Cusani, and M. Biagi, "Modulation precoding for MISO visible light communications," *Journal of Lightwave Technology*, vol. 39, no. 17, pp. 5439–5448, 2021.

[29] A. Petroni and M. Biagi, "On the convenience of perfect channel knowledge for spatial equalization of correlated mimo-vlc links: Is it really worth it?" *J. Lightwave Technol.*, vol. 40, no. 18, pp. 6101–6115, Sep 2022. [Online]. Available: https://opg.optica.org/jlt/abstract.cfm?URI=jlt-40-18-6101

[30] M. Uysal, F. Miramirkhani, O. Narmanlioglu, T. Baykas, and E. Panayirci, "Ieee 802.15.7r1 reference channel models for visible light communications," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 212–217, 2017.

[31] G. Wyzecki and W. Stiles, *Color Science*. Wiley, 1967.

[32] W. Xie, B. Li, Y. Peng, H. Zhu, F. AL-Hazemi, and M. M. Mirza, "Secrecy enhancement for ssk-based visible light communication systems," *Electronics*, vol. 11, no. 7, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/7/1150