PHILOSOPHICAL TRANSACTIONS A

rsta.royalsocietypublishing.org

Research

Article submitted to journal

Subject Areas:

xxxxx, xxxxx, xxxx

Keywords:

xxxx, xxxx, xxxx

Author for correspondence:

Harald.Haas

e-mail: Harald.Haas@ed.ac.uk

THE ROYAL SOCIETY
PUBLISHING

Optical Wireless Communications for Cyber Secure Ubiquitous Wireless Networks

Hanaa Abumarshoud, Cheng Chen, Mohamed Sufyan Islim and Harald Haas

School of Engineering, LiFi Research and Development Centre, Institute for Digital Communications, University of Edinburgh, Edinburgh EH9 3JL, UK

Wireless connectivity is no longer limited to facilitating communications between individuals, but is also required to support diverse and heterogeneous applications, services and infrastructures. Internet of things (IoT) systems will dominate future technologies, allowing any and all devices to create, share, and process data. If artificial intelligence resembles the brain of IoT, then high-speed connectivity forms the nervous system that connects the devices. For IoT to safely operate autonomously, it requires highly secure and reliable wireless links. In this article, we shed light on the potential of optical wireless communications (OWC) to provide high-speed secure and reliable ubiquitous access as an enabler for fifth generation (5G) and beyond wireless networks.

1. Introduction

An OWC system using signals from light emitting diodes (LEDs) was first introduced by Pang *et al.* in 1998 [1] for intelligent transport systems (ITSs), where fast switching of an LED-based traffic light between the ON and OFF states was used to transmit an audio signal to a receiver located at a distance of 20 m. Utilizing white LEDs for data transmission started to take shape in the early 2000s, when Tanaka *et al.* from Keio University in Japan developed simulations of LED-based 10 Mbps wireless home links [2]. The term *iLight* was then used in 2002 to refer to the frequent switching of high brightness LED displays to transmit an audio signal, which achieved a transmission speed of 128 kbps [3].

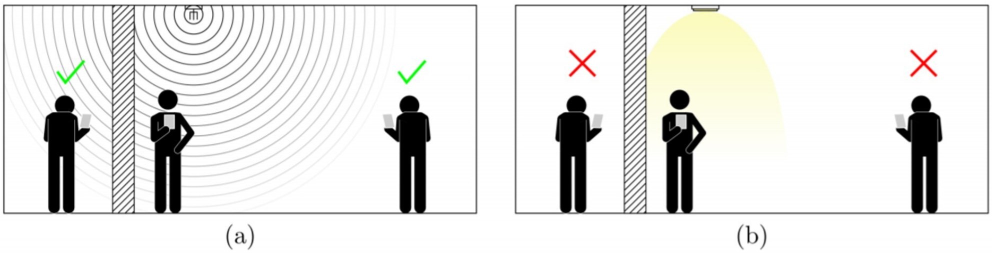

Figure 1. (a) Confidential information can be easily intercepted via RF-based network. (b) OWC transmission provides enhanced security in physical layer.

A proof-of-concept implementation of a high-speed visible light communication (VLC) link was developed by Afgani *et al.* in 2006 [4], where it was proved that orthogonal frequency division multiplexing (OFDM)-based intensity modulation (IM)/direct detection (DD) transmissions are feasible and able to provide significant data rate enhancement for VLC systems. The developed prototype used a single off-the-shelf LED and covered a transmission distance of about one meter with a bit error ratio (BER) of 10^{-3} without the use of channel or source coding techniques. A 10 Gbps link was realised from a single Gallium Nitride (GaN)-based series-biased blue micro-LED array [5] opening the door for realising high speed indoor OWC systems. Following that, several novel modulation schemes were proposed to enhance the spectrum and power efficiency of OWC transmissions. This could be achieved utilising OFDM-based transmissions, color-based modulation, spatial modulation [6] and multiple-input multiple-output (MIMO) techniques [7]. A 11.28 Gbps VLC link was reported in 2016 [8] based on experimental demonstrations of wavelength division multiplexing (WDM) transmissions with rate adaptive OFDM modulation. The highest data rate achieved to date was reported in 2019 [9], where a 15.73 Gbps link was realised over a distance of 1.6 m using OFDM-modulated signals from four single-color LEDs with adaptive bit loading. The rapid recent advancements in the research and implementation of OWC indicate that it will be a key enabler for future ubiquitous connectivity, particularly when the demand for data usage outgrows the available supply from existing wireless technologies [10] [11].

It is highlighted above that during the last decade, significant progress has been achieved in two key areas: i) OWC can achieve link data rates that are comparable with current high performance wireless systems and most importantly ii) OWC technology can be used to build ultra-dense wireless access networks for mobile access; the coverage of a single OWC could be in the region of a few centimeters. Because of the very small cells, these networks are also referred to as optical attocellular networks. These two circumstances now form a solid base to utilise a unique advantage of OWC which is its unique potential to enhance wireless security.

Security in wireless networks is becoming as important as reliability and quality of service because of the growing machine-type communications and the support of autonomous systems. Malicious attacks of wireless networks could turn these autonomous systems into weapons which, of course, has to be avoided. Moreover, it was reported that around 2.1 billion users' confidential data was leaked in March 2019, and it is anticipated that the cost of cyber crime could exceeded 2 trillion dollars globally [12]. These figures highlight the importance of improving the security of communications networks.

Light signals cannot penetrate opaque objects, which offers enhanced physical layer security (PLS) for wireless access. As shown in Figure 1(a), a radio frequency (RF) signal can be easily intercepted by eavesdroppers from behind a wall or from a distant location. In the case of an OWC link, however, this is no longer possible and the leakage of confidential information outside the coverage area can be avoided, as shown in Figure 1(b) [13].

Information security threats could pose serious implications, not only on the profitability and competitiveness of the business, but also on national security and staff safety. OWC can address these security concerns by containing the communication within the secure-vetted area where it should be accessed from. The small-cells concept and the extreme densification of OWC access point (AP)s allow for geolocation-based monitoring of users access and mobility patterns. For example, the OWC APs in a certain establishment can be categorized based on their fixed locations within the building. The user connection policies can be devised based on the attocell APs privilege categories. A user who is authorized for a general communication-access can be assumed to connect through their optical APs or any other common-space AP inside the office. Any abnormal access behaviour can be detected when such a user is connected through an optical attocell AP located in a restricted area of the building. This concept can be developed further to enable the creation of optical geo-fences for users to allow location-based user-centric cyber-security applications.

In the following sections, we discuss why reliable, secure and high-speed wireless connectivity is a vital player in the development of future autonomous services and applications. We also present a concise overview of the design of secure OWC systems and examine the effect of dynamic user association and power allocation on enhancing the confidentiality of such networks.

The rest of the paper is organised as follows. In Section 2, the wiretap channel model for secure OWC is introduced. In addition, the differences between OWC and RF PLS designs, channel uncertainty and performance metrics are discussed. In Section 3, a number of recent advanced techniques that can improve the secrecy performance of OWC systems are reviewed. A number of important results are presented and discussed. Finally, a paper summary and discussions about potential future research directions are presented in Section 4.

2. PLS for OWC systems

As previously discussed, one of the advantages of OWC links is that they are inherently secure in confined areas because light signals do not penetrate walls. Hence, users located outside the room in which the APs are configured cannot listen to the communication. Nevertheless, OWC links are susceptible to eavesdropping by malicious users existing under the coverage area of the same AP. As a result, securing optical transmissions is particularity crucial for OWC links deployed in open public spaces such as shopping malls, museums, libraries and airports. In this section, we discuss some common PLS techniques that have been recently applied to secure OWC transmissions.

(a) PLS preliminaries

In this article, we adopt the widely used notion of “Alice,” “Bob,” and “Eve” referring to the OWC AP, legitimate user and eavesdropper in a wiretap channel model [14], respectively, as shown in Figure 2. In this regard, Alice transmits a confidential signal to Bob, that is ideally kept entirely hidden from Eve, without using secret-key encryption. It is commonly assumed that Alice obtains accurate information about Bob’s channel by receiving channel state information (CSI) feedback from legitimate users. Furthermore, Eve is typically assumed as a malicious passive user (i.e. not communicating with Alice, just listening), and thus Eve’s CSI does not exist precisely because there is no uplink channel. Simply speaking, the goal of secrecy design in OWC systems is to enable Alice to convey confidential messages to Bob, while minimizing the chances of Eve decoding these messages.

(b) PLS design in OWC vs RF

OWC links differ from RF links in that the optical channel input is strictly non-negative due to the requirements of IM/DD. Moreover, unlike RF links, conventionally modelled as Gaussian inputs with average power constraints, the modulating signal in VLC must satisfy particular amplitude constraints due to the illumination requirement and the limited dynamic range of the

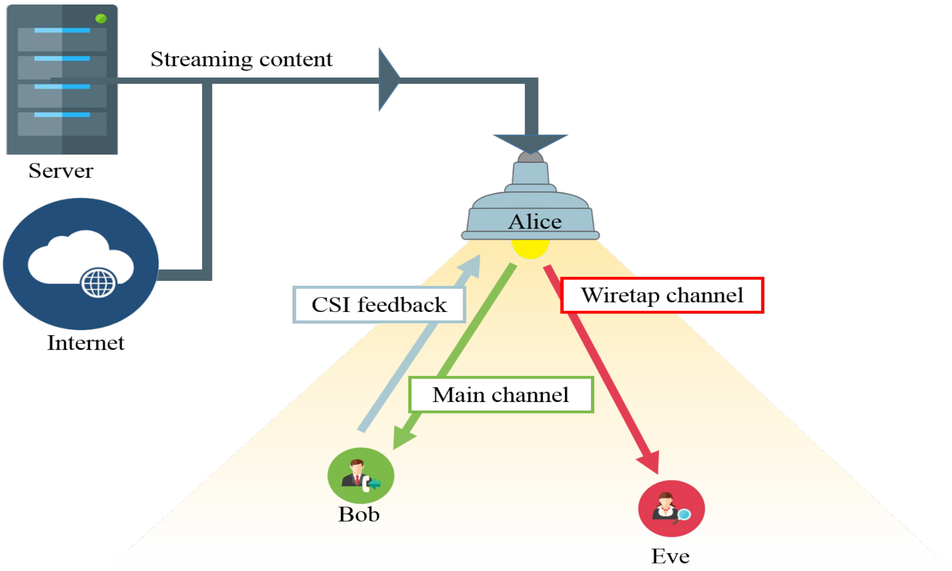

Figure 2. Generic system model of PLS related to eavesdropping problem in VLC

.

LEDs [15]. As a result, IM/DD channels are typically modelled as amplitude constrained inputs. Despite the massive body of literature investigating average power-constrained Gaussian wiretap channels, the subject of securing amplitude-constrained wiretap channels is relatively new, with few interesting results. Another difference between PLS design in RF and OWC systems is that RF security is based on the assumption that Eve and Bob's channels are independent of each other. This can be justified by the spatial decorrelation and multi-path fading properties of RF links [16]. In OWC, however, the channels of Eve and Bob can have very similar, or even equal, gains if both are located in close or symmetric locations with respect to the AP. This means that it is highly possible for Eve to know the exact characteristics of Bob's channel from this spatial correlation characteristics. It also means that it is more challenging to design a PLS technique that degrades Eve's link without affecting Bob.

(c) What does Alice know about Eve?

The design of a secure transmission link requires that Alice obtains some knowledge of the CSI of Eve. It is very likely, however, for Eve to be a malicious user that does not share any information with the network and only listens [17]. Under this assumption, secrecy performance can be alleviated by adopting design schemes that explicitly take Eve's channel uncertainty into consideration, which are referred to as robust transmission schemes. Yet, it is noted that robust transmission design is effective only when the actual realizations of Eve's channel do not considerably deviate from their nominal estimates. Therefore, it is of paramount importance to devise reasonable uncertainty models of Eve's channel and perform secrecy design based on worst-case scenarios.

The first attempts in this direction presented the location of Eve via a two-dimensional uncertainty model [13]. In this model, Eve has a fixed vertical separation from the AP and its location in the xy-plane is bounded by a square area with respect to a reference point, e.g., the room centre. Based on this, the CSI of Eve can be estimated with bounded error. Consequently, there exists a worst-case scenario regarding Eve's location that minimizes the achievable secrecy rate. Then, the design problem of maximizing the worst-case secrecy rate yields a robust solution for the given assumption. It is worth noting that the reliability of such an approach highly depends on the chosen reference point. Using Bob's location as a reference point might sound like the most valid assumption; since Alice may try to place herself in the proximity of Bob to be able to listen to his messages. However, given the small coverage area of a typical OWC cell, as well as the high symmetry of the optical channel, Eve may instead locate herself in a symmetrical position with respect to the cell centre.

To investigate the impact of unknown eavesdroppers' locations on secrecy performance, stochastic geometry techniques have been proposed to model malicious users' locations based on certain distributions. An interesting scenario was implemented in [18], where eavesdroppers were assumed to be outside the room trying to listen to the legitimate users' signals through the windows. The randomness of eavesdroppers' locations outside the windows was modeled by a homogeneous Poisson point process (PPP) with uniform density, while the number of potential eavesdroppers was assumed to follow a Poisson distribution. Since windows in a wall have a fixed vertical separation from the AP, the distance between Alice and Eve can be bounded by minimum and maximum possible values. An ellipsoidal model was adopted to quantify the CSI of the Alice-Eve link which lead to obtaining upper bounds for the CSI error to facilitate the design of robust PLS techniques.

Apart from the uncertainty regarding the availability of Eve's CSI, there are a number of other uncertainties that exist in a secure VLC transmission system. In some situation, Bob and Eve may have positions in a symmetric manner with respect to Alice's position. However, this is the case when all optical detector are facing upwards towards the ceiling. In practice, this may not be the case when mobile users tilt their mobile devices with a random orientation. The statistics of the user device orientation have been evaluated experimentally in several publications [19]. By taking this phenomenon into account, the channel spatial correlation issue can be weakened, thereby potentially improving the secrecy of the link. In some cases, random human bodies in Alice's coverage area may cause blockage to either Eve's or Bob's link. It has been found that the blockage probability is higher when a user is further away from the AP [20], which may have a considerable impact on the transmission secrecy performance. When a user is close to the walls and other opaque objects, the effects of non-line-of-sight (NLOS) channels due to reflections may start to dominate the optical wireless channel [21], which adds another factor to consider when securing the transmissions.

(d) Secrecy Performance Metrics

In order to quantify the secrecy of a wireless communication link, two performance metrics, secrecy capacity and secrecy outage probability, have been widely used in PLS studies [14]. In addition, many researchers have developed theoretical results for these two metrics in a number of secure VLC studies. In the following, we will briefly introduce and discuss the two metrics.

(i) Secrecy Capacity

In a typical wiretap channel, assuming 'Alice' send a desired message x, 'Bob' received signal y and 'Eve' received the signal z, the secrecy capacity is defined as [16]:

$$C_\mathrm{s} = \max_{\mathcal{P}(x)} \left[I(x;y) - I(x;z) \right] \tag{2.1}$$

where $I(x;y)$ denotes the mutual information between x and y and $\mathcal{P}(x)$ refers to the distribution of the transmitted signal x. The definition (2.1) can be interpreted as the maximum information rate at which the legitimate user can reliably decode its signal without being susceptible to eavesdropping. In other words, secrecy capacity is the difference between Bob and Eve's channel capacities, which indicates the maximum rate at which the confidential message is recovered reliably at 'Bob' while keeping it useless at 'Eve'. The amplitude constraint on the OWC channel input makes it difficult to explicitly solve for a closed-from solution for the secrecy capacity. As a result, many researchers work on performance bounds on the secrecy capacity [14]. In addition, stochastic geometry-based distributions are widely employed in the mathematical analysis to model malicious users' locations and to increase the tractability. In the single-input single-output (SISO) scenario, an expression for the average secrecy rate has been derived in a single cell case [22]. Lower bounds for secrecy capacities in the SISO and multiple-input single-output (MISO) cases are concluded in [13]. A number of theoretical results in MIMO scenario have been presented in [23].

(ii) Secrecy Outage Probability

The secrecy outage probability is defined as the probability that the secrecy capacity of a communications link is below a predetermined threshold [22]:

$$\mathcal{P}_{\mathrm{so}} = \mathbb{P}[C_{\mathrm{s}} < C_{\mathrm{th}}], \tag{2.2}$$

where C_{th} refers to the outage threshold. The value of C_{th} is selected to ensure the transmission from Alice to Bob is sufficiently reliable and secure. Secrecy capacity reflects the transmission speed of a specified secure transmission, while the secrecy outage probability reflects the probability that the considered secure transmission system fails. Analytical results for the secrecy outage probability in a SISO scenario have been presented in a number publications. In the MISO scenario, the secrecy outage probability with an LED selection scheme is considered in [24]. A comprehensive secrecy capacity and secrecy outage probability analysis has also been considered in a multicell multi-user scenario in [25], where the location of APs are modelled by a two-dimensional homogeneous PPP. The authors of [26] have provided an analysis of a system with colluding eavesdroppers, where multiple eavesdroppers collaborate to obtain a better signal. Despite the usefulness of this metric in characterizing the expected differences between the Alice-Bob and Alice-Eve link capacities, it does not provide accurate insights on Eve's capability to successfully decode Bob's messages. For example, a secrecy outage probability of 0.1 indicates that the instantaneous secrecy capacity is below a certain threshold 10% of the time, but it does not evaluate the amount of information leakage to the eavesdroppers when outage occurs. Moreover, the secrecy capacity could be higher than the predetermined threshold, and yet Eve might be able to decode part of the confidential signal. Thus, the decision on an acceptable secure threshold is very important, particularly in OWC systems where the channels of Bob and Eve can be highly correlated.

3. Securing OWC transmissions

Various PLS techniques have been proposed in literature to enhance the secrecy performance of OWC systems. Some of these are borrowed from RF communications, such as jamming and beamforming, and others are specifically designed for OWC. In the following, we discuss recent applications of PLS techniques in OWC systems.

(a) Optimal LED Selection

Based on the existence of random malicious users, connecting Bob to the nearest AP does not necessarily yield the best secrecy rate. This is particularly crucial if Eve is closer to the AP than Bob, as shown in Figure 3. Motivated by this, the work in [25] proposed an APs' cooperation scheme that enhances the secrecy rate by selecting the optimal serving AP for each legitimate user. It was shown that such an optimal AP selection scheme can contribute to achieving better security in VLC systems, at the cost of additional implementation and computational complexity.

An optimal LED selection scheme for secrecy enhancement of generalized space-shift keying (GSSK) based VLC systems was proposed in [27]. Due to the symmetrical gain of the VLC channel, the mutual information rate between Alice and Bob can significantly degrade if Bob is located in a position that observes similar channel gains from different LEDs, leading to a low achievable secrecy rate. Thus, the decision on the LEDs selection must be optimised to guarantee the security of the system under the assumption that the location of Eve is unknown. Results demonstrated

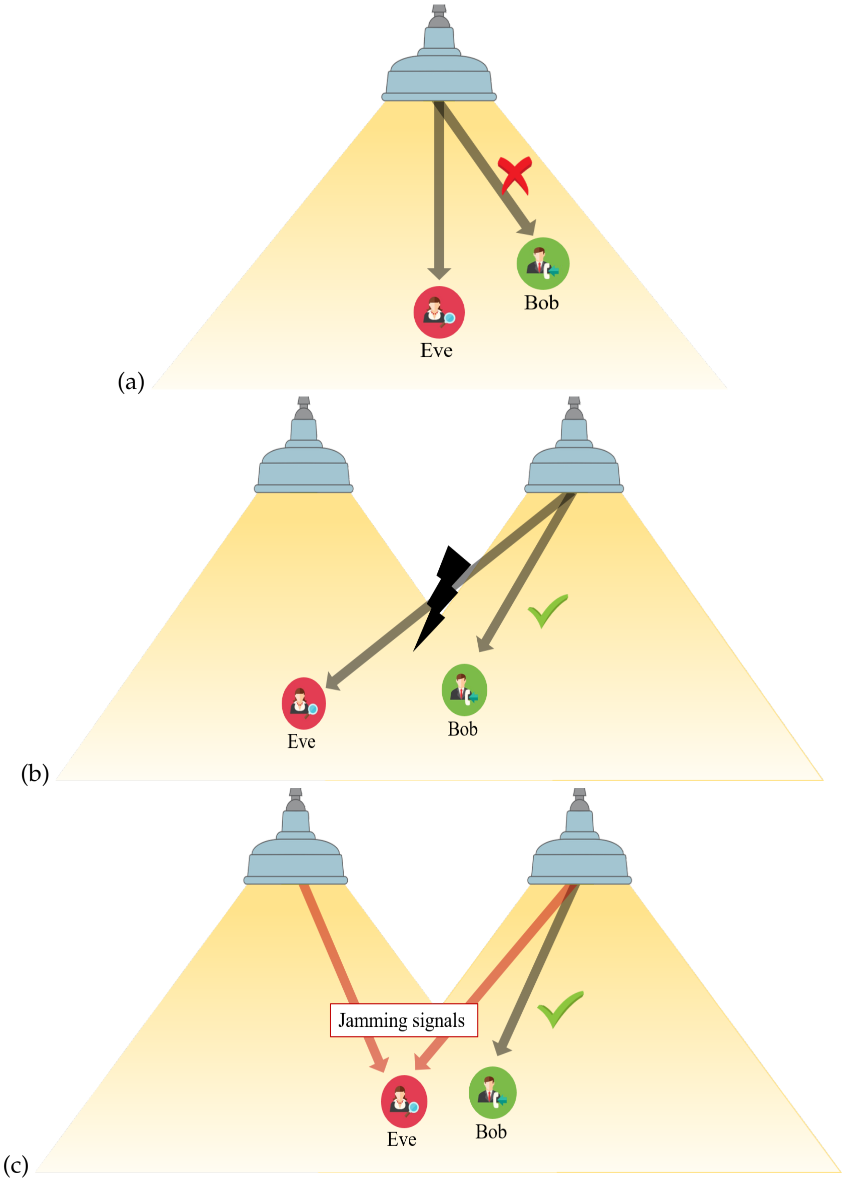

Figure 3. (a) Degraded wiretap channel, Eve's rate is higher than Bob's., (b) Bob's channel is secured by LED selection, and (c) Bob's channel is secured by jamming: jamming signals are transmitted in the null space of Bob.

that the proposed optimal LEDs selection is capable of enhancing the achievable secrecy rate of Bob, particularly in the medium SNR region. A simple LED selection scheme was proposed in [24], where only the nearest LED to Bob is selected to transmit the information bearing signal so as to maximise the information rate between Alice and Bob. It was shown that such a selection scheme is not optimal and cannot outperform beamforming in terms of secrecy capacity. It does, however, provide a simple cost-effective solution when the legitimate user is relatively close to one of the transmitting LEDs.

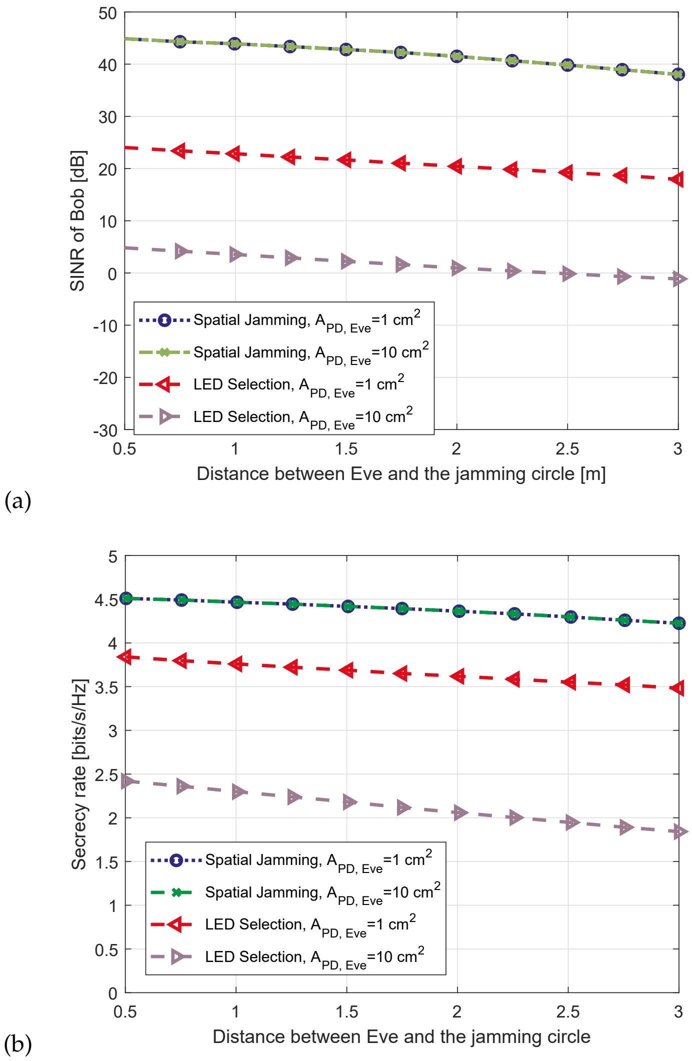

Figure 4. The achieved secrecy performance in terms of (a) the optimised SINR of Bob and (b) the secrecy rate, for different locations of Eve [29].

(b) Friendly jamming

It is not possible to secure Alice-Bob connection without jamming in scenarios with a degraded wiretap channel, i.e. the received signal-to-noise-ratio (SNR) at Eve is equal to or better than the received SNR at Bob as shown in Figure 3(a). Jamming refers to the intentional insertion of well-designed interfering signals that severely degrade the eavesdropper's ability to decode the confidential signal. The idea is to transmit an interference signal in the null-space of the eavesdropper as illustrated in figure 3(c). Consequently, the legitimate user does not receive the interference, while the eavesdropper's received signal suffers high interference [28]. It is noted that designing null-space dependent interference is not always feasible since the eavesdroppers' location could be very close to the legitimate user, and given the non-fading characteristics of the OWC channel, it is highly probable that the legitimate user would also receive some interference as well from the jamming signal. Also, in the scenario where it is possible to produce such a null-space dependent artificial interference, the secrecy performance is not necessarily optimal.

In some scenarios, allowing low levels of interference at Bob usually means that we can transmit higher interference signals to Eve and, thus, we can achieve a higher secrecy rate.

The term 'spatial jamming' is used when multiple transmitting LEDs decide whether to transmit an information signal or, alternatively, a jamming signal based on the spatial locations of users. Such an approach can be implemented if the APs are able to know the exact locations of legitimates users and potential eavesdroppers by means of channel estimation methods. In [29], two optimisation problems were formulated in order to decide on the jamming signals. The first problem formulation aims to maximise the legitimate user signal-to-interference-and-noise-ratio (SINR) subject to a constraint on the eavesdropper's SINR, while the second problem formulation aims to maximise the secrecy rate under the spatial jamming strategy. Both optimisation problems were carried out for the case of a known eavesdropper, i.e., when the AP has perfect knowledge of Eve's location, as well as a random eavesdropper, i.e., the AP only acquires an estimate of the location of Eve. The proposed optimisation problems were numerically solved by means of Sequential Quadratic Programming (SQP) using MATLAB. Figure 4 shows the optimised SINR and the optimised secrecy rate of a legitimate user under spatial jamming compared to LED selection. The x-axis in the figure represents the horizontal distance between the eavesdropper and the the center of the jamming circle. The jamming circle denotes the location of the LED that is transmitting the jamming signals. Results are shown for two different assumptions regarding Eve's photo-detector (PD) physical area. It is shown that spatial jamming outperforms LED selection in terms of Bob's SINR and secrecy capacity. Moreover, it is noted that the performance gap is more significant when Eve has a larger PD area. The reason behind this is that a larger PD area enhances the eavesdropper's reception capability, and thus the decision on the LED selection is affected. As shwon in Figure 3(b), Bob might be connected to a further AP to ensure that Eve is not receiving the data signal. For this reason, we see that Bob's SINR and secrecy rate under the LED selection method degrades when Eve's PD area is increased from 1 cm^2 to 10 cm^2. We can also see from the figure that increasing the PD area of Eve under spatial jamming does not affect the secrecy rate of Bob. This is because a larger PD area implies that Eve receives more of the jamming signals along with the information signals.

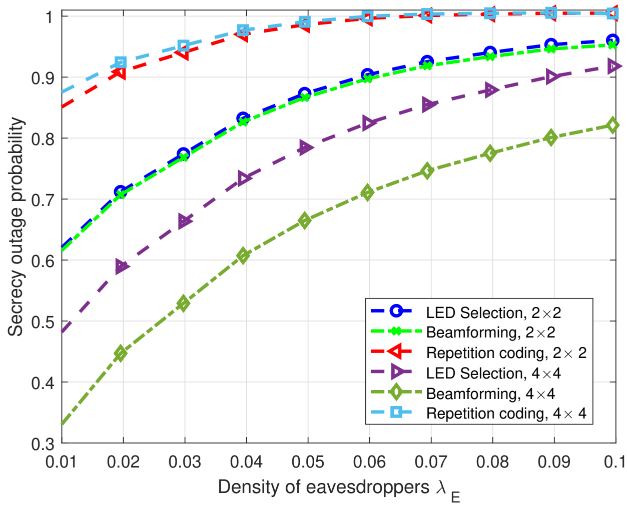

Figure 5. Secrecy outage probability for different MIMO configurations under LED selection, beamforming and repetition coding [29].

(c) Secure beamforming

Typical indoor OWC systems usually consist of multiple LEDs installed on the ceiling of a room and multiple connected users. Hence, it is natural to exploit the spatial transceiver sources to provide secrecy via adaptation in the space domain. To this end, different beamforming techniques have been exploited to enhance the received signal strength at legitimate users, while significantly reducing it at any potential eavesdroppers. This can be achieved by decomposing the legitimate and illegitimate channels into parallel independently encoded subchannels. Under the idealised assumption that the AP will acquire perfect CSI for all users (including eavesdroppers), optimal beamformer design can be obtained to maximize the secrecy capacity under certain system requirements. It is noted, however, that the optimal performance is not always possible since malicious eavesdroppers usually tend to hide themselves from the AP. For a more realistic assumption of imperfect CSI, a robust beamformer can be designed to maximise the secrecy capacity based on the worst-case scenario of Eve's location.

In [30], optimal and robust transmit beamformer designs were proposed to maximize the achievable secrecy rate in a VLC multiple-input-single-output (MISO) wiretap channel subject to amplitude constraints. While the optimal beamformer relied on the acquisition of perfect CSI for Eve and Bob links, the robust beamformer was based on combined uncertainties corresponding to variations in location, orientation, half-angle, and multi-path reflections. Under the premise of perfect CSI, the proposed optimal design outperformed generalized eigenvector and zero-forcing precoding at the cost of increased complexity. For the case of imperfect CSI, the robust beamformer was shown to outperform the optimal beamformer and the performance gain was more evident for higher degrees of CSI errors. The same problem was tackled in [18] with the objective of minimising the total LED power consumption while satisfying a minimum required secrecy rate. Optimal and robust beamformer designs were proposed for different degrees of CSI uncertainty. Results showed that the proposed beamformer design improves the achievable secrecy capacity under low-to-moderate transmit power constraints, compared to beamformer designs that do not consider power minimization. Also, it was shown that the achievable secrecy capacity of the proposed beamformer increases for higher transmit power values.

Various performance measures were considered in [31] to design secure linear precoding schemes for multi-user VLC systems. Specifically, max-min fairness, harmonic mean, proportional fairness and weighted fairness measures were used as objectives for the optimisation problems, which were solved using iterative algorithms. The presented results demonstrated that the proposed precoding schemes can offer around a 20% enhancement in average secrecy rates compared to their conventional zero-forcing counterparts. This enhancement, however, comes at the expense of increased computational complexity, which is proportional to the square root of the number of active network users. Moreover, it was shown that the weighted fairness based beamformer provided the highest average secrecy rate, while the max-min fairness beamformer provided the lowest performance.

Figure. 5 shows a comparison of the secrecy outage probability achieved by means of LED selection and beamforming for 2×2 and 4×4 MIMO systems. The results are also compared to the secrecy outage probability under repetition coding in which all transmitting LEDs emit the legitimate user signal with equal power regardless of the location of Eve. Multiple eavesdroppers are assumed to be randomly distributed according to a PPP with intensity λ_{E}. It can be seen from the figure that increasing the number of transmitters reduces the secrecy outage probability in the case of LED selection and beamforming. This is because of the added degrees of freedom created by having more transmitting LEDs. In the case of repetition coding, however, increasing the number of LEDs has an adverse effect on the secrecy performance. This is because the eavesdropper is also receiving multiple copies of the legitimate use's signal which increases the possibility that Eve can decode Bob's messages. It is also seen from 5 that for the case of 2×2 MIMO configuration, the gap in the secrecy outage probability between beamforming and LED selection is small. However, for the 4×4 case, beamforming can achieve better performance due to the availability of extra spatial degrees of freedom to steer the signal towards the legitimate user while suppressing it everywhere else.

(d) LED protected zone

A "protected zone" approach was proposed in [25] as a way to enhance the secrecy rate of indoor OWC systems. A protected zone is defined to be an eavesdroppers-free disk area centered at the cell centre with a predetermined radius. A practical implementation of this idea can be realised by the aid of LEDs with built-in motion sensors. In the case of a malicious user entering this zone, the AP is expected to detect its presence, notify the legitimate user and stop the transmission of the confidential message. Simulation results showed that increasing the radius of the protected zone from 1 m to 2 m reduced the secrecy outage probability from 0.2 to nearly zero. A related discussion in [32] investigated the concept of an "insecure region"; the region in which Eve would have better channel conditions compared to Bob. It was shown that when Bob is located directly under the AP, the entire coverage area is secure as Bob has the highest possible channel gain. However, when Bob moves away from the room centre, the insecure area appears and expands as the distance between Bob and the Alice increases. It is noted, however, that such definitions of secure and insecure regions highly depend on the implemented secrecy measures. This is because Eve might have lower channel gain compared to Bob and still be able to successfully receive and decode the information signal. It is clear that the network design of a suitable protected zone, i.e. when eavesdroppers are not allowed to exist in an insecure region, has a high impact on system performance. A small radius, on the one hand, would lead to higher secrecy but it might result in frequent interruptions of the LED transmission, leading to lower rate performance. On the other hand, a large radius may significantly reduce the secrecy rate and render the confidential message susceptible to eavesdropping.

(e) Securing NOMA transmissions

The term non-orthogonal multiple access (NOMA) refers to a class of multiple access schemes that allow different network users to share the full frequency and time resources. This is achieved by multiplexing users' signals in the power domain based on superposition coding. To recover their respective signals, each user needs to successfully decode and subtract the signals of other network users with a lower decoding order. This process is known as successive interference cancellation (SIC). As a result, NOMA involves the risk of legitimate network users maliciously exploiting the signals of other users during SIC. Hence, the design objective of NOMA-based OWC networks must consider securing the system against active, as well as passive, eavesdroppers. For the external eavesdroppers case, the design problem is to optimise the power allocation, rate allocation and legitimate users' decoding order in a way that ensures the maximum possible secrecy rate. For the case of active eavesdroppers, however, the design problem is much more complicated and the application of PLS techniques might not be sufficient. To this end, encryption-based approaches might be needed to prevent passive eavesdroppers from exploiting the confidential information of other network users. The PLS of NOMA-based VLC systems was investigated in [33]. In this work, the secrecy outage probability expressions for a pair of legitimate users were derived for the case of single and multiple external eavesdroppers. Simulation results showed that system secrecy performance can be enhanced by enlarging the differences between the channel gains of multiplexed users. This is in line with the pairing strategy of NOMA, which favours pairing users with large channel differences in order to allow successful power-domain multiplexing and demultiplexing.

For a user to successfully extract its data signal from the power-domain multiplexed signals in NOMA, it needs to acquire perfect knowledge of the adopted power allocation strategy to facilitate SIC. This implies that Eve cannot obtain useful information if the power allocation coefficients are not known. In the following, we demonstrate the potential of NOMA to inherently secure data transmissions. To this end, we provide simulation results for the outage probability of

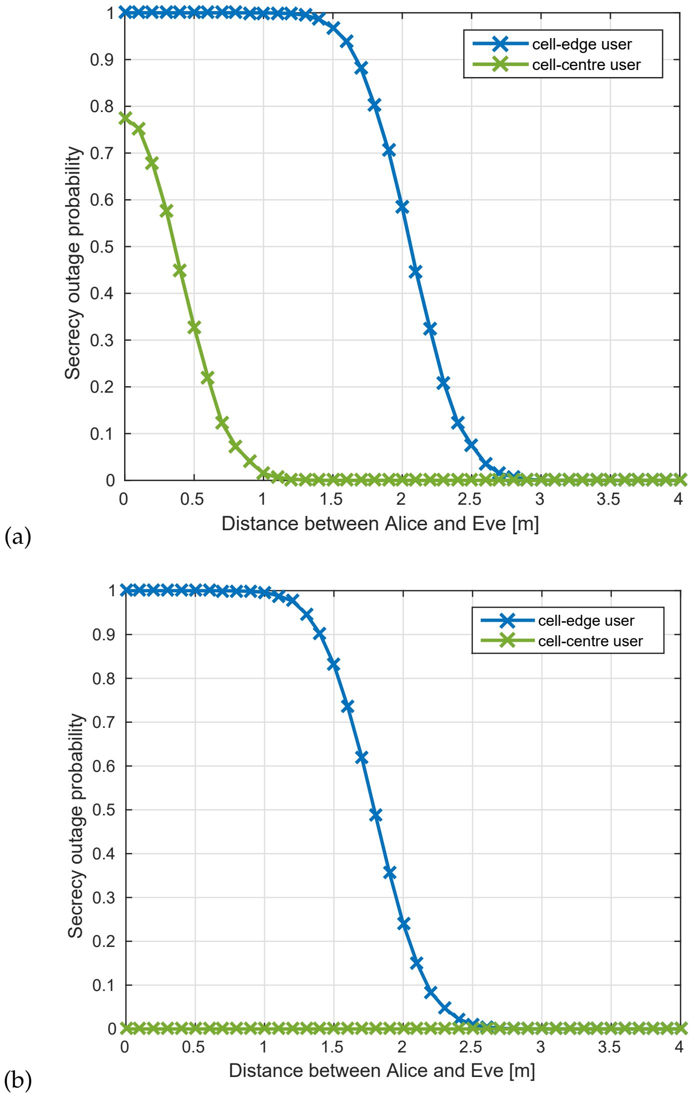

Figure 6. Secrecy outage probability when (a) Eve knows the exact power allocation strategy adopted by Alice, and (b) Eve does not know the exact power allocation strategy.

a NOMA-based VLC system with two legitimate users and a single eavesdropper. he legitimate user which is closer to Alice is referred to as the cell-centre user while the other user is referred to as the cell-edge user. According to the NOMA principle, the cell-centre user is allocated lower power and thus needs to perform SIC to extract its signal, while the cell-edge user directly decodes its received signals assuming the interference as noise. The secrecy outage probability is evaluated with regard to the horizontal distance between Alice and Eve. Secrecy outage occurs if the rate of Eve is higher than the rate of Bob, i.e. the outage threshold is zero. In Figure 6(a), we assume that Eve knows the exact power allocation strategy as well as the users' decoding order, which presents the worst-case scenario. It can be seen that the user existing at the room centre exhibits an acceptable secrecy performance, i.e. less than 0.2 outage probability, when Eve is more than 0.5 m away from the room centre. The other user, however, needs Eve to be more than 2.2 m away from the centre to achieve acceptable secrecy performance. Figure 6(b) shows the secrecy outage probability for the same setup assuming that Eve does not acquire an exact knowledge, but rather an estimate, of the adopted power allocation strategy. This would affect Eve's ability to decode the confidential messages, particularly the signal of the cell-centre user (because it involves SIC). Thus the secrecy outage probability for the cell-centre user reaches zero regardless of Eve's location as shown in Figure 6(b). Hence, we can conclude that the security of NOMA OWC systems can be drastically enhanced by only keeping the power allocation information hidden from Eve.

(f) PLS with realistic channel assumptions

The high density and mobility of users, as well as the short range of OWC APs, imply that changes in users channel conditions and link secrecy can occur with high rate. As a result, future OWC systems will require a degree of autonomy in order to be able to calculate, evaluate and adapt the resource allocation in order to offer the best possible performance [34]. In contrast to conventional radio frequency systems, the channel gain in LiFi is highly dependant on the random orientation of mobile devices. Moreover, blockage of line-of-sight (LOS) links between the transmitter and legitimate user can highly affect the received signal strength and, thus, the achievable secrecy capacity. Hence, it is important to consider these undeterministic factors in the analysis of LiFi systems to provide more realistic insights.

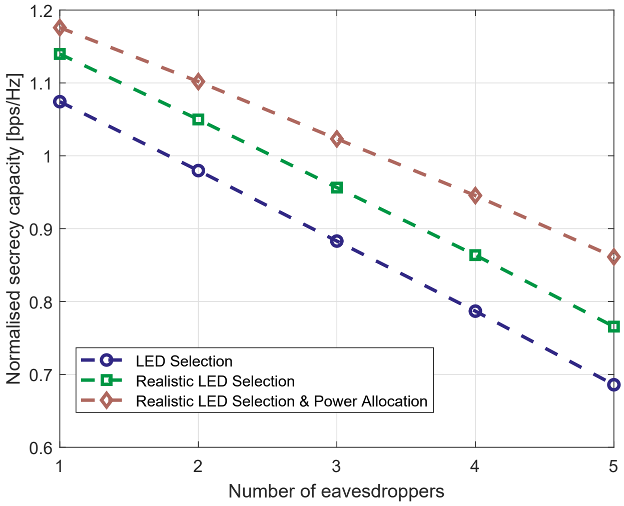

Figure 7. Effect of realistic LED selection and power allocation and PA on the achievable secrecy capacity.

In the following, we investigate the effect of taking the realistic assumptions of the optical channel when designing PLS mechanisms on the secrecy performance. To this end, we compare the simple LED selection strategy to realistic LED selection, i.e., the decision on the serving AP for the legitimate user is not based only on its distance from the AP but also on the estimated secrecy capacity under realistic assumptions. The realistic assumptions are set to be 1) the user device follows a random orientation model as in [19], and 2) the LOS between Alice and Bob is susceptible to blockage as in [20]. Moreover, we show the performance when the transmit power of the APs is also configured so as to maximise the secrecy capacity. The objective of the proposed configurable LED selection and power allocation scheme is to maximize the sum secrecy capacity of all the network legitimate users, which is a key performance metric of the wiretap channel and is defined as the maximum information rate at which the legitimate user can reliably decode its signal without being susceptible to eavesdropping.

This LED selection and power allocation problem represent a Mixed-Integer Non-Linear Programming (MINLP) problem, which makes it difficult to obtain a closed form solution to it. However, since the AP selection involves choosing between a small number of LEDs, typically up to four, we obtain the results for this optimisation by means of the exhaustive search. The main goal is to evaluate the effect of considering realistic secrecy measures when performing LED selection and power allocation on system performance. Figure 7 shows the secrecy capacity versus the number of eavesdroppers for different LED selection strategies. It can be seen from Figure 7 that performing LED selection based on secrecy calculations enhances the achievable secrecy capacity compared to idealistic LED selection. Furthermore, we can see that the best secrecy performance can be achieved by combining LED selection with power allocation based on realistic secrecy measures, which provides a 20% secrecy capacity enhancement compared to idealistic AP selection for the case of 5 colluding eavesdroppers.

4. Summary and Future Directions

OWC hold great potential for enabling high-speed reliable wireless access for future 5G and beyond networks. For such heterogeneous and autonomous networks with extremely high user density, it is particularly critical to secure the communications links against any potential eavesdroppers. The fact that optical signals do not penetrate through walls and have a short communication range implies that OWC transmissions exhibit high inherit security and are unlikely to be decodable by illegitimate users outside the coverage area of the transmitting APs. Nonetheless, optical signals are still susceptible to eavesdroppers existing inside the coverage area since they can observe the optical signals. This article showed that meaningful opportunities exist for the integration of PLS in the context of OWC, while there are some restrictions imposed by the distinct characteristics of the optical channel. We believe that the design of dynamic, hybrid and smart PLS mechanisms can contribute to meeting the security demands expected in future OWC networks. In this context, hybrid security techniques that combine PLS with key-based approaches has the potential to enhance the security of OWC links, particularly with the existence of non-degraded wiretap channels. An adaptive mechanism can be used to switch between PLS and key-based techniques or a combination of both, depending on the density of eavesdroppers and the required degree of security for various applications. Moreover, smart configuration of the transmission patterns in the LEDs can enhance the secrecy performance by adjusting to the changing system parameters. Since light does not penetrate through walls, the APs are only required to secure the transmission from eavesdroppers within the boundaries of the coverage area. Advanced eavesdroppers detection mechanisms are needed to give the AP a better idea of the dynamics of non-registered users. In this case, the AP can decide on the required level of security and accordingly implement specific PLS or key-based techniques.

Ethics. Insert ethics statement here if applicable.

Data Accessibility. Insert details of how to access any supporting data here.

Authors' Contributions. For manuscripts with two or more authors, insert details of the authors' contributions here. This should take the form: 'AB caried out the experiments. CD performed the data analysis. EF conceived of and designed the study, and drafted the manuscript All auhtors read and approved the manuscript'.

Competing Interests. Insert any competing interests here. If you have no competing interests please state 'The author(s) declare that they have no competing interests'.

Funding. Insert funding text here.

Acknowledgements. Insert acknowledgment text here.

Disclaimer. Insert disclaimer text here if applicable.

References

1. G. Pang, C. Chan, H. Liu, and Hugh T. Kwan. 1998 Dual use of LEDs: Signalling and communicationsin ITS. In *proc. 5th World Congr. Intelligent Transport Syst.*
2. Y. Tanaka, S. Haruyama, and M. Nakagawa, Wireless optical transmissions with white colored LED for wireless home links. In *proc. 11th IEEE International Symposium on Personal Indoor and Mobile Radio Communications, PIMRC 2000*. Proceedings (Cat. No.00TH8525), London, UK, 2000, pp. 1325-1329 vol.2. (doi: 10.1109/PIMRC.2000.881634)
3. G. Pang, T. Kwan, H. Liu and Chi-Ho Chan. 2002 LED wireless. *IEEE Industry Applications Magazine*, vol. 8, no. 1, pp. 21-28. (doi: 10.1109/2943.974354)
4. M. Z. Afgani, H. Haas, H. Elgala, and D. Knipp. 2006 Visible light communication using OFDM. In *proc. 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, TRIDENTCOM 2006* pp. 6–134.
5. E. Xie, R. Bian, X. He, M. S. Islim, C. Chen, J. J. D. McKendry, E. Gu, H. Haas, and M. D. Dawson, “Over 10 gbps vlc for long-distance applications using a gan-based series-biased micro-led array,” *IEEE Photonics Technology Letters*, vol. 32, no. 9, pp. 499–502, 2020.
6. Cogalan T, Haas H, Panayirci E. 2020 Optical spatial modulation design. *Phil. Trans. R. Soc.* A 378, 20190195. (doi:10.1098/rsta.2019.0195)
7. Wang Z, Chen J. 2020 Networked multiple-input-multiple-output for optical wireless communication systems. *Phil. Trans. R. Soc.* A 378, 20190189. (doi:10.1098/rsta.2019.0189)
8. H. Chun, S. Rajbhandari, G. Faulkner, D. Tsonev, E. Xie, J. J. D. McKendry, E. Gu, M. D. Dawson,D. C. O’Brien, and H. Haas. 2016 LED based wavelength division multiplexed 10 Gb/s visible light communications. *Journal of Lightwave Technology*, vol. 34, no. 13, pp. 3047–3052.
9. R. Bian, I. Tavakkolnia, and H. Haas. 2019 15.73 Gb/s visible light communication with off-the-shelf LEDs. *Journal of Lightwave Technology*, vol. 37, no. 10, pp. 2418–2424.
10. Manousiadis PP, Yoshida K, Turnbull GA, Samuel IDW. 2020 Organic semiconductors for visible light communications. *Phil. Trans. R. Soc.* A 378, 20190186. (doi:10.1098/rsta.2019.0186)
11. Griffiths AD, Herrnsdorf J, McKendry JJD, Strain MJ, Dawson MD. 2020 Gallium nitride micro-light-emitting diode structured light sources for multi-modal optical wireless communications systems. *Phil. Trans. R. Soc.* A 378, 20190185. (doi:10.1098/rsta.2019.0185)
12. List of data breaches and cyber attacks in January 2019 – 1,769,185,063 records leaked.
13. A. Mostafa and L. Lampe. 2015 Physical-layer security for MISO visible light communication channels. *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1806-1818. (doi: 10.1109/JSAC.2015.2432513)
14. M. A. Arfaoui et al., Physical Layer Security for Visible Light Communication Systems: A Survey. *IEEE Communications Surveys Tutorials*. (doi: 10.1109/COMST.2020.2988615)
15. M. Obeed, A. M. Salhab, M. Alouini and S. A. Zummo, Survey on Physical Layer Security in Optical Wireless Communication Systems. *2018 Seventh International Conference on Communications and Networking (ComNet)*, Hammamet, Tunisia, 2018, pp. 1-5. (doi: 10.1109/COMNET.2018.8622294)
16. A. Yener and S. Ulukus, Wireless Physical-Layer Security: Lessons Learned From Information Theory. *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814-1825, Oct. 2015. (doi:10.1109/JPROC.2015.2459592)
17. A. Mostafa and L. Lampe, Physical-layer security for indoor visible light communications. *2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, 2014, pp. 3342-3347. (doi: 10.1109/ICC.2014.6883837)
18. S. Ma, Z. Dong, H. Li, Z. Lu and S. Li. 2016 Optimal and robust secure beamformer for indoor MISO visible light communication. *Journal of Lightwave Technology*, vol. 34, no. 21, pp. 4988-4998. (doi: 10.1109/JLT.2016.2605000)
19. M. D. Soltani, A. A. Purwita, Z. Zeng, H. Haas and M. Safari, Modeling the Random Orientation of Mobile Devices: Measurement, Analysis and LiFi Use Case. *IEEE Transactions on Communications* vol. 67, no. 3, pp. 2157-2172, March 2019. (doi: 10.1109/TCOMM.2018.2882213)
20. K. Dong, X. Liao and S. Zhu, Link blockage analysis for indoor 60ghz radio systems. *Electronics Letters*, vol. 48, no. 23, pp. 1506-1508, 8 November 2012. (doi: 10.1049/el.2012.2994)
21. C. Chen, D. Basnayaka and H. Haas, Non-line-of-sight channel impulse response characterisation in visible light communications. *2016 IEEE International Conference on Communications (ICC)*, Kuala Lumpur, 2016, pp. 1-6. (doi: 10.1109/ICC.2016.7511382)
22. G. Pan, J. Ye and Z. Ding, On Secure VLC Systems With Spatially Random

Terminals. *IEEE Communications Letters*, vol. 21, no. 3, pp. 492-495, March 2017, (doi: 10.1109/LCOMM.2016.2643632)

23. M. A. Arfaoui, A. Ghrayeb and C. Assi, On the achievable secrecy rate of the MIMO VLC Gaussian wiretap channel. *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Montreal, QC, 2017, pp. 1-5. (doi: 10.1109/PIMRC.2017.8292592)
24. S. Cho, G. Chen and J. P. Coon, Securing Visible Light Communication Systems by Beamforming in the Presence of Randomly Distributed Eavesdroppers. *IEEE Transactions on Wireless Communications*, vol. 17, no. 5, pp. 2918-2931, May 2018, doi: 10.1109/TWC.2018.2804390.
25. L. Yin and H. Haas. 2018 Physical-layer security in multiuser visible light communication networks. *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 1, pp. 162-174. (doi: 10.1109/JSAC.2017.2774429)
26. S. Cho, G. Chen and J. P. Coon, Physical Layer Security in Visible Light Communication Systems With Randomly Located Colluding Eavesdroppers. *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 768-771, Oct. 2018. (doi: 10.1109/LWC.2018.2820709)
27. F. Wang et al., Secrecy Analysis of Generalized Space-Shift Keying Aided Visible Light Communication. *IEEE Access*, vol. 6, pp. 18310-18324, 2018, doi: 10.1109/ACCESS.2018.2799658.
28. F. Wang et al. 2018 Optical jamming enhances the secrecy performance of the generalized space-shift-keying-aided visible-light downlink. *IEEE Transactions on Communications*, vol. 66, no. 9, pp. 4087-4102. (doi: 10.1109/TCOMM.2018.2831687)
29. S. Cho, G. Chen and J. P. Coon, 2019 Securing Visible Light Communications with Spatial Jamming. *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, pp. 1-6, doi: 10.1109/ICC.2019.8761165.
30. A. Mostafa and L. Lampe. 2016 Optimal and robust beamforming for secure transmission in MISO visible-light communication links. *IEEE Transactions on Signal Processing*, vol. 64, no. 24, pp. 6501-6516. (doi: 10.1109/TSP.2016.2603964)
31. 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, Nov. 2018, doi: 10.1109/TWC.2018.2871055.
32. J. Wang, C. Liu, J. Wang, Y. Wu, M. Lin and J. Cheng. 2018 Physical-layer security for indoor visible light communications: secrecy capacity analysis. *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6423-6436. (doi: 10.1109/TCOMM.2018.2859943)
33. X. Zhao, H. Chen and J. Sun, On Physical-Layer Security in Multiuser Visible Light Communication Systems With Non-Orthogonal Multiple Access. *IEEE Access*, vol. 6, pp. 34004-34017, 2018, doi: 10.1109/ACCESS.2018.2847744.
34. H. Abumarshoud, H. Alshaer and H. Haas. 2019 Dynamic multiple access configuration in intelligent Lifi attocellular access points. *IEEE Access*, vol. 7, pp. 62126-62141. (doi: 10.1109/ACCESS.2019.2916344)