Enhancing Security in 6G Visible Light Communications

Simone Soderi*‡, *Senior Member, IEEE*
*IMT School for Advanced Studies, Lucca, Italy
‡CINI Cybersecurity Laboratory, Roma, Italy
email:simone.soderi@imtlucca.it

***Abstract*—This paper, considers improving the confidentiality of the next generation of wireless communications by using the watermark-based blind physical layer security (WBPLSec) in Visible Light Communications (VLCs). Since the growth of wireless applications and service, the demand of a secure and fast data transfer connection requires new technology solutions capable to ensure the best countermeasure against security attacks. VLC is one of the most promising new wireless communication technology, due to the possibility of using environmental artificial lights as data transfer channel in free-space. On the other hand, VLC are even inherently susceptible to eavesdropping attacks. This work proposes an innovative scheme in which red, green, blue (RGB) light-emitting-diodes (LEDs) and three color-tuned photo-diodes (PDs) are used to secure a VLC by using a jamming receiver in conjunction with the spread spectrum watermarking technique. To the best of the author's knowledge, this is the first work that deals physical layer security on VLC by using RGB LEDs.**

***Index Terms*—6G; VLC; Physical Layer Security; Spread Spectrum Watermarking; Jamming.**

I. Introduction

The ever-increasing demand of wireless applications is obvious contrast with spectrum scarcity. The annual global traffic request is expected to reach 1.6 zetta-bytes per month by 2021 [1]. Conventional radio frequency (RF) solutions are not able to cope with this increasing demand. There is the need to develop new technologies that support this incredible request. In literature there are many contributions that show how the optical wireless communication (OWC) is a promising candidate to high speed wireless communications. Due to the advantage of the license-free operation over a significantly wider spectrum, many technological advances have proliferated in OWCs. OWCs utilize three different regions of the electromagnetic spectrum: ultraviolet (UV), visible light, and infrared (IR). As shown in Figure 1, visible light communications (VLCs) are a branch of OWCs that involve electromagnetic waves in the visible spectrum to communicate [2]–[4].

In 2011 the Visible Light Communication Task Group issued the IEEE 802.15.7 standard [5]. It was a major step towards the commercialization and widespread deployment of VLC networks. VLC links benefit from the license-free light spectrum, immunity to radio frequency (RF) interference, and the use of inexpensive light-emitting diodes (LEDs) and photodiodes (PDs) for the transmission and the reception, respectively. Besides, VLCs support their *dual use* of the existing illumination infrastructure for wireless communication purposes. Actually, if the light changes fast enough the human eyes can not perceive the flickering effect and LEDs can transmit data.

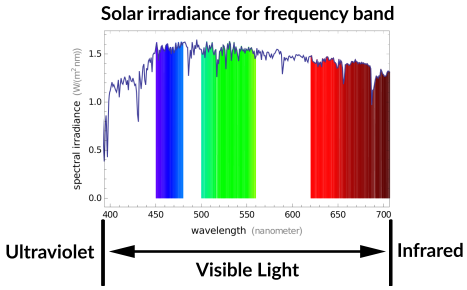

Fig. 1. Solar irradiance for frequency band.

The wireless industry proposes to move communications above 10 GHz. In accordance to this trend, in recent years Haas *et al.* developed the light-fidelity (Li-Fi). It extends the concept of VLC to achieve high speed, secure, bi-directional and fully networked wireless communications. On the other hand, the usage of high frequencies leads to a more complex supporting infrastructure with smaller cells [6], [7].

The rest of this paper is organized as follows: Section II describes the motivation behind this research and the innovation introduced for 6G secure communications. Section III continues with the proposed system model for the physical layer security over VLC networks. Section V introduces the secrecy capacity expression of a watermark-based VLC. Finally, the paper is concluded in Section VI.

II. Motivation and Security Innovation in 6G

Compared with RF, VLC has an unlicensed and free of charge optical bandwidth. Table I shows how the visible light spectrum is potentially lager than the RF's available bandwidth. This makes very high data rate communication possible and virtually fulfills the $1 - 10$ Gb/s/m^3 key-performance-indicator (KPI) associated to 6G [8]. Furthermore, since the optical band does not overlap with existing RF bands, there is no electromagnetic interference with those systems [9].

The extreme high demand of data-rate in 6G networks delineated so far, clearly poses major challenges in terms of security and privacy. Due to the high computation complexity,

TABLE I
VISIBLE LIGHT SPECTRUM

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

[1] Medium available for VLCs.

existing security schemes are not attractive [8]. The 6G Flagship Program (6GFP) [10] has recently established as security has to be considered at each individual layer but the *strongest security protection* may be achieved in the physical layer [11]. VLC is foreseen as a key enabler technology to achieve fast wireless communications. Efficient schemes should integrate physical-layer security into existing authentication and cryptography mechanisms for further securing wireless networks [12]. The next generation of low-power sensors networks is an area where physical layer security can provide awesome advantages in terms of number of computations than cryptography. This study shows that the proposed architecture can enhance device's cybersecurity by implementing a physical layer standalone security solution on VLC networks.

In VLC, the signal isolation property can also be used to enhance communication security by preventing eavesdropping on in-room or in-building communications [3]. In this paper, the author addresses the problem of the *physical layer security* presented in [13], [14], in which secure communications are obtained by combining watermarking with a jamming receiver over VLC networks. The idea proposed with the watermarked blind physical layer security (WBPLSec) protocol addresses countermeasures against the *confidentiality attacks*.

So far, there are two common approaches to implement VLCs. The first uses white LEDs, whereas the alternative one uses red, green, blue (RGB) LEDs. The second solution is preferable, since each color component has a higher bandwidth, as shown in Table I, and the three different independent channels can be used for increasing the data throughput [15], [16]. As shown in Figure 2, author assumed

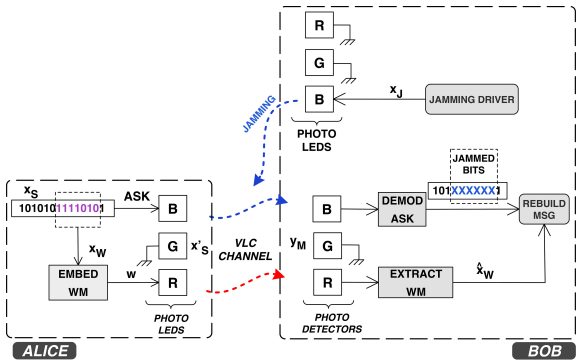

Fig. 2. WBPLSec system model in a VLC network.

that Alice transmits by using an RGB LED and Bob has a single RGB color-tuned PD and one RGB LED to jams the Alice's VLC. The eavesdropper, Eve, is also equipped with a single PD. To the best of the author's knowledge, this is the first work that deals physical layer security on VLC by using RGB LEDs.

The truly innovative process for deploying a physical layer security on 6G VLC networks consists of

1) *RGB LEDs*: The scheme proposed here exploit the three independent channels to secure the communication;
2) *Spread-Spectrum watermarking*: the message to be transmitted is first modulated with a spreading sequence and then transmitted by using only the red light;
3) *Jamming Receiver*: as shown in Figure 2, the jammer is implemented inside the receiver by using an RGB LED, and then utilized to jam the Alice's transmission;
4) *Selective jamming*: Bob jams only part of the received signal and knowing which samples are jammed, the receiver is able to rebuild a clean symbol. Instead, the jamming does not have any effect on the spread-spectrum (SS) signal;
5) *Two independent paths*: the proposed method transmits the information through two independent paths by using the blue light and red light. The information is sent via a narrow-band amplitude shift keying (ASK) signal through the blue light. Whereas, the SS signal uses the red light because it has a wider bandwidth than the blue one. The SS signal implements the watermark. The narrow-band signal is partially jammed by Bob's blue light. Finally, the watermark in the SS signal is utilized to re-compose the entire symbol.

The WBPLSec on VLC network can be successfully applied in those scenarios where RGB LEDs are used for illumination purposes. The physical layer security mechanism implemented by the WBPLSec [13] consists of steps shown in Algorithm 1, when it used on VLC networks.

III. VLC CHANNEL MODEL

VLCs in general, utilize the intensity modulation (IM) scheme along with the direct-detection (DD). In particular, with IM/DD technique the transmitted signal $x(t)$ is the optical power generated when the modulated current signal passes through the LED. However, the dynamic range of the LED is inherently limited. Therefore, the modulating signal must satisfy certain *amplitude constraints* to avoid clipping distortion [17]. On the other side, the received signal $y(t)$ is proportional to the optical power that arrive at the PD [2]. At the transmitter, the desired illumination level is maintained by setting the appropriate direct-current (DC) bias of the overall signal that fed into the LED [3].

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

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

Algorithm 1 WBPLSec protocol in VLC networks.

1: **procedure** PHYSICAL LAYER SECURITY
2: $SS\ Watermarking\ (ALICE)$: A message x_S is transmitted through the blue light by employing the ASK modulation. A part of the original message, i.e. x_W, is modulated with direct-sequence-spread-spectrum (DSSS) and then transmitted by using the red light. Author assumed to use the wavelength division multiplexing (WDM) available in RGB LEDs to watermark the VLC.
3: $Jamming\ Receiver\ (BOB)$: The receiver jams N_W samples for each symbol transmitted by Alice. The jamming signal x_J consists of the a blue light. Actually, Bob has his own RGB LED. The received y_M signal stimulates the RGB PD into the corresponding color band. The received signal is then processed by the ASK demodulator to recover the data transmitted. Due to the jamming, a portion of the signal is now corrupted and unusable.
4: $Watermark\ Extraction\ (BOB)$: The receiver extracts the watermark using a code matched filter.
5: $Symbol\ Rebuild\ (BOB)$: Knowing which samples are jammed the receiver, i.e. Bob, is able to rebuild a clean symbol using information contained in the watermark.
6: **end procedure**

where $h \in \mathbb{R}_+$ is the channel gain and $n(t)$ is the is the background light noise, which is modeled as a signal-independent additive white Gaussian noise (AWGN) [2].

An indoor VLC channel consist of two main components: the line-of-sight (LOS) channel and the diffuse channel. The first is composed by the light that directly hit the PD without bouncing on the other objects. The second, also known as non-line-of-sight (NLOS), includes all light rays that bounce the objects in the room. Thus, this paper consider only the LOS component as shown in Figure 3. Assuming to have Lambertian light source, the LOS component of the channel DC gain, i.e. $H(0) = \int_{-\infty}^{\infty} h(t)dt$, between one LED and one PD is given by [2]

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

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

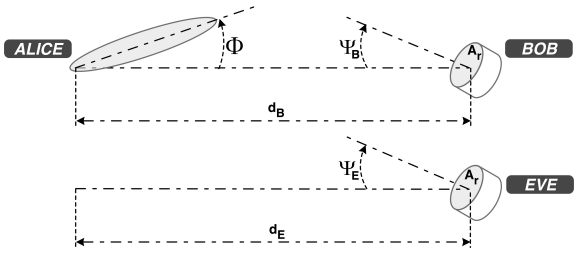

Fig. 3. LOS in the VLC channel model.

In VLC system the signal-to-noise (SNR), i.e. γ_{VLC}, ratio is proportional to the square of the received optical power as follows

$$\gamma_{VLC} = \frac{H^2(0)P_t^2}{\sigma^2}, \quad (3)$$

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

IV. WBPLSEC SYSTEM MODEL

A modified version of the non-degraded wiretap channel model [18] is used and it includes the so-called *jamming channel* utilized to jam the received signal and also the eavesdropper. Figure 4 shows the model used to analyze the physical layer security in VLC.

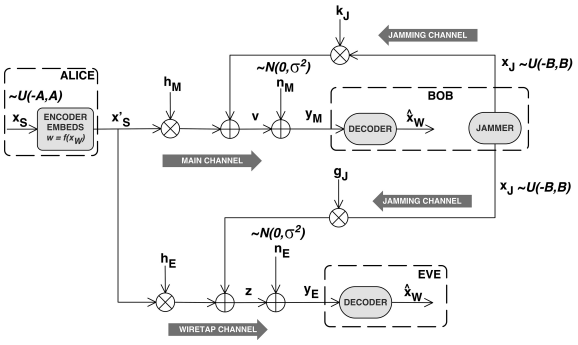

Fig. 4. Non-degraded wiretap channel model with jamming receiver.

The source message $(x_S)^N$ of length N is encoded into code-word $(x'_S)^N$ of length N. In particular, the encoder embeds the watermark $(x_W)^{N_W}$ of length N_W into the host signal $(x_S)^N$. The legitimate user, i.e. Alice, transmits $(x'_S)^N$ to Bob through the *main channel*. Whereas Eve receives this signal through the *wiretap channel*. The *i*-th sample of the signal received by Bob and Eve are, respectively, given by

$$y_M(i) = h_M(i)x'_S(i) + k_J(i)x_J(i) + n_M(i), \quad (4)$$
$$y_E(i) = h_E(i)x'_S(i) + g_J(i)x_J(i) + n_E(i), \quad (5)$$

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

In accordance with the first rule of the framework presented by Cox *et al.* [19] (See Appendix A in [14]), a transmitter combines the original modulated signal with an SS watermark and an embedding rule defined as

$$x'_S(i) = x_S(i) + \mu w(i), \quad (6)$$

where $x_S(i)$ is the i-th sample of the continuous ASK transmitted signal [20], μ is the scaling parameter and $w(i)$ is the SS watermark.

The signal watermarking is done by using the traditional spread spectrum based approach [21]. The main idea implemented in the watermark embedding phase is that the

transmitter marks, utilizing SS, the host signal x_S utilizing its first N_W over N samples. Then x_W is given by

$$x_W(i) = \begin{cases} x_S(i), & \text{for } 1 \leq i \leq N_W, \\ 0, & \text{elsewhere.} \end{cases} \tag{7}$$

The direct sequence spread spectrum (DSSS) technique is selected for the signal watermarking.

In this paper author proposes the application of the WPLSec in a VLC network. The WBPLSec system model is shown in Figure 4, in which the jamming receiver, together with the watermarking, provides secrecy. Actually, Bob rebuilds the original message by using the information contained into the watermark. Indeed, he replaces the destroyed bits with the ones carried by the watermark [13], [14]. Finally, to simplify deriving the secrecy capacity expression, author assumes that x_S, x_J and w are uniformly distributed over the interval $[-A, A]$.

V. Secrecy Capacity of the WBPLSec in VLC

Previous section describes the the VLC channel and the behavior of the WPLSec protocol. This paper takes into account only the LOS component in VLC. Moreover, IM/DD channels are typically modeled with amplitude constraints [17].

The secrecy capacity (C_s) of legitimate link is defined, similarly to the standard capacity, for the non-degraded Gaussian wiretap channel [18], [22] as follows

$$C_s = \max_{f_{x'_S}} (\mathbb{I}(X'_S; Y_M) - \mathbb{I}(X'_S; Y_E)), \tag{8}$$

where $f_{x'_S}$ is the statistical distribution of the input signal x'_S and $\mathbb{I}(.;.)$ states for the mutual information over the main and wiretap channels. Furthermore, the C_s of the wiretap channel described by (4) and (5), can be lower bound as follows

$$\begin{aligned} C_s &= \max_{f_{x'_S}} (\mathbb{I}(X'_S; Y_M) - \mathbb{I}(X'_S; Y_E)) \qquad (9) \\ &\overset{(a)}{\geq} \mathbb{I}(X'_S; Y_M) - \mathbb{I}(X'_S; Y_E) \\ &\overset{(b)}{=} \mathbb{h}(Y_M) - \mathbb{h}(Y_M|X'_S) - \mathbb{h}(Y_E) + \mathbb{h}(Y_E|X'_S) \\ &= \mathbb{h}(Y_M) - \mathbb{h}(k_J \cdot x_J + n_M) \\ &\quad - \mathbb{h}(Y_E) + \mathbb{h}(g_J \cdot x_J + n_E), \qquad (10) \end{aligned}$$

where (a) follows by dropping the maximization, (b) follows the mutual information definition and the $\mathbb{h}(.)$ is the *differential entropy* that is defined for the random variable u as $\mathbb{h}(u) = \int_{-\infty}^{\infty} p(u) log(p(u)) du$ [20].

First, author recalls the assumptions that x_S and w are uniformly distributed over the interval $[-A, A]$. Whereas, x_J is $\sim \mathcal{U}(-B, B)$. Thus, by assuming x_S and w independent random variables, the probability density function (PDF) of x'_S given by (6), i.e. $f_{X'_S}(x'_S) = f(x_S) * f(\mu \cdot w)$, is trapezoidal and it is given by

$$f(x'_S(i)) = \begin{cases} \frac{1}{2A} & A\mu - A < x < -A\mu + A \\ \frac{A\mu + A - x}{4A^2\mu} & A - A\mu < x \leq A + A\mu \\ \frac{A\mu + A + x}{4A^2\mu} & -A - A\mu < x \leq -A + A\mu \\ 0 & \text{otherwise,} \end{cases} \tag{11}$$

where μ is the scaling parameter for the watermark and A is the amplitude of the VLC signal and of the jamming signal as well. Figure 5 shows the effect of variation of the watermark scaling factor, i.e. μ, on the trapezoidal probability density function when $A = 1$.

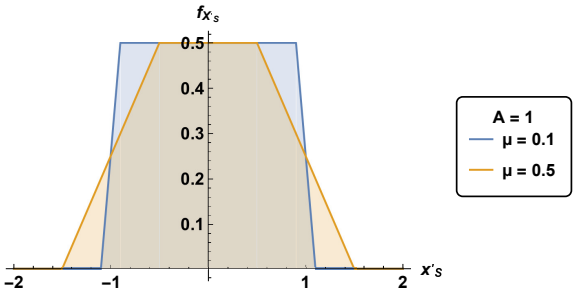

Fig. 5. Effect of varying the watermark scaling parameter (μ) into the trapezoidal probability density function (pdf).

Thus, by assuming $A > 0$ and $0 < \mu < 1$, the differential entropy of x'_S over main and wiretap channel are given by

$$\mathbb{h}(h_M \cdot x'_S) = \frac{\mu}{2} + \log(2A \cdot h_M) \tag{12}$$

$$\mathbb{h}(h_E \cdot x'_S) = \frac{\mu}{2} + \log(2A \cdot h_E) \tag{13}$$

where μ is the watermark scaling parameter.

In addition, by recalling that x_J is $\sim \mathcal{U}(-B, B)$, n_M and $n_E \sim \mathcal{N}(0, \sigma^2)$ we have

$$\mathbb{h}(k_J \cdot x_J) = \log(2B \cdot k_J) \tag{14}$$

$$\mathbb{h}(g_J \cdot x_J) = \log(2B \cdot g_J) \tag{15}$$

$$\mathbb{h}(n_M) = \mathbb{h}(n_E) = \frac{1}{2}\log(2\pi e\sigma^2). \tag{16}$$

Therefore, author can lower bound the differential entropy equations $\mathbb{h}(.)$ as follows

$$\mathbb{h}(Y_M) \overset{(c)}{\geq} \frac{1}{2}\log[e^{2\mathbb{h}(h_M x'_S)}) + e^{2\mathbb{h}(k_J x_J)}) + e^{2\mathbb{h}(n_M)})] \tag{17}$$

$$\mathbb{h}(Y_E) \overset{(c)}{\geq} \frac{1}{2}\log[e^{2\mathbb{h}(h_E x'_S)}) + e^{2\mathbb{h}(g_J x_J)}) + e^{2\mathbb{h}(n_E)})] \tag{18}$$

$$\mathbb{h}(k_J \cdot x_J + n_M) \overset{(c)}{\geq} \frac{1}{2}\log[e^{2\mathbb{h}(k_J \cdot x_J) + 2\mathbb{h}(n_M)}] \tag{19}$$

$$\mathbb{h}(g_J \cdot x_J + n_E) \overset{(c)}{\geq} \frac{1}{2}\log[e^{2\mathbb{h}(g_J \cdot x_J) + 2\mathbb{h}(n_E)}] \tag{20}$$

where (c) uses the entropy power inequality [23].

Plugging eqs. (12) to (20) into (10) we achieve the secrecy rate, i.e. R_s, of a watermarked-based communication with jamming receiver in VLC as follows

$$\begin{aligned} R_s = &\frac{1}{2}\log\left(\frac{2A^2 e^{\mu} h_M^2 + 2B^2 k_J^2 + e\pi\sigma^2}{4B^2 k_J^2 + 2e\pi\sigma^2}\right) + \\ &+ \frac{1}{2}\log\left(\frac{4A^2 e^{\mu} h_E^2 + 4B^2 g_J^2 + 2e\pi\sigma^2}{8B^2 g_J^2 + 4e\pi\sigma^2}\right). \end{aligned} \tag{21}$$

Figure 6 shows the secrecy rate R_s as a function of g_J for different locations of Eve but also by varying the watermark intensity with μ. Notice that when the eavesdropper

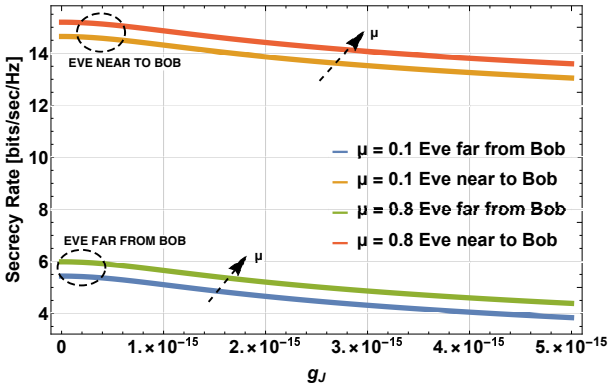

Fig. 6. Secrecy rate of the WBPLSec in VLC network($A = 1$, $B = 2$, $h_M = 10^{-4}$,$k_J = 10^{-4}$).

is close to the legitimate receiver the R_s increases due to the Bob's jamming. This mechanism clearly *enhance the security* between Alice and Bob by creating by creating a *secure region* around the legitimate receiver. In addition, Figure 6 depicts also the effect of varying the watermark scaling parameter. Indeed, the stronger is the watermark, i.e. by increasing μ, the higher is the secrecy rate.

VI. Conclusions

VLC is foreseen as key enabler technology to achieve fast wireless communications. Such a kind of communications exploit the paradigm transmitting while illuminating. The availability of this free spectrum creates an opportunity for low-cost broadband communication that could alleviate the spectrum congestion. This study shows that the watermark-based VLC with a jamming receiver, i.e. WBPLSec, can enhance device's cybersecurity by implementing a physical layer standalone security solution on VLC networks. With this blind full-rate protocol, the legitimate receiver can exchange a secret shared key with a neighboring device in the same room by exploiting VLCs.

References

[1] (2018, November) Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html

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

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

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

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

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

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

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

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

[10] 6G Flagship Program. [Online]. Available: https://www.oulu.fi/6gflagship/

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

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

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

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

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

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

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

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

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

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

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

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

[23] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. USA: Wiley-Interscience, 2006.