A study on the VLC security at the physical layer for two indoor scenarios

Simona Riurean[1*],

[1]University of Petrosani, Department ACIEE, 20 University Str., 332006, Romania

Abstract. The visible light communication (VLC) systems are generally considered secure since the light cannot penetrate through solid objects. However, both in the line of sight (LoS) scenarios as well as in non LoS scenarios with wide and strong optical signal, information security must be considered. The conventional information security technologies used for wireless communications based on radio frequency are not suitable to be applied straight for VLCs because of the limited hardware resources, especially for the optical receivers (oRx). In this paper, a study on the VLC security at the physical layer approach based on optical beamforming to achieve secure transmissions for indoor and underground scenarios is presented.

1. A short view on the VLC technology

The academic community agrees that the VLC technology development started with the demonstration of a reliable indoor wireless transmission system, in Japan, in 2001 [1]. There was also a VLC kit offered for sale that raised an unexpected interest and the development team found that they were out of stock in a surprisingly short time after launching the product. The kit was developed with white LEDs and some off-the-shelf components reaching an impressing performance for that time: a data rate of 400 Mbps [2].

Following the Nobel Prize awarded in 2014 to the researchers who discovered the white LED [3], the research regarding the VLC deployments have raised with the same speed as the electronic parts with low costs were improved and became available for research teams and to design and develop systems ready to be applied in a number of areas.

Despite the major drawbacks that the currently LEDs have, for fast transmission and a long-range optical link communication in VLC systems, the limited bandwidth (up to about 20MHz) and non-linearity, since 2001 to date, there are more and more systems and new coined wireless communication technologies based on the visible light.

For example, professor Hass coined Li-Fi technology in 2011 and the last decade brought an unexpected number of researches works in this direction [4]. Li-Fi is designed to be a multiple-input-multiple-output (MIMO) and full-duplex transmission that allow mobility, a fully networked communication system, due to the specially designed access points embedded into the lighting fixtures.

* Corresponding author: sriurean@yahoo.com

The Optical Camera Communication (OCC) technology, although the receiver has a slower response than a VLC system because the image sensor cannot recognize high-frequency signals, it has important benefits of high mobility and low cost since mobile smart devices as smartphones, are widely spread [5,6].

The Free Space Optics (FSO) technology is applied in outdoor environments and recently is intensively researched and developed for the vehicle to vehicle (V2V) communication [7,8] and underwater transmission [9,10], as well.

2. The general configuration of a VLC system

The main components of a VLC system with a line of sight (LoS) topology are (i) the optical transmitter (oTx) with the VLC signal generation (SG) part and the optical module (the artificial light emission device LED and Lens), (ii) the optical wireless channel (OWC) under the Additive White Gaussian Noise (AWGN) influence, and (iii) the optical receiver (oRx) (with optical filter (OF), optical concentrator (OC), and photodetector (PD), with the signal recovery (SR) module as shown in figure 1.

Fig. 1. General configuration of a VLC system with LoS topology

The LED device is driven by DC bias current with alternating current (AC) to represent signals. The oTx electric current energy is turned into optical power, is transmitted wirelessly, and then is detected by the PD, being converted into current again which is processed by oRx hardware circuit to replicate the transmitted signals. All the key features are related to the hardware circuit current energy and optical power [11].

In order to build a robust VLC setup, many significant characteristics of the proper artificial light emission device have to be considered. Reliable candidates for artificial light sources can be a red-blue-green-yellow light-emitting diode (RBGY LED), red-blue-green LED (RGB LED) white LEDs (WLEDs), array or stripe of SMD LEDs, µLEDs, organic LEDs (OLEDs), laser diodes (LDs). Their light intensity, the wavelength of light, the light scattering, the modulation speed, the cut-off frequency, and the power requirements, must all be considered [12].

The blue LED with yellow phosphor (aka WLED) is the most commonly used in VLC systems [13].

The two most representative values of LEDs are their optical power (P_{oTx}) as a function of wavelength (λ) or as a function of the LED's supply current/forward current (I_{oTx}). The unit of P_{oTx} (λ) is Watts/nm. For these two characteristics P_{oTx} (λ) and P_{oTx} (I_{oTx}), the manufacturers usually provide graphs with the normalized values.

The value of the optical power P_{oTx} changes with the intensity of the driving current I_{oTx} multiplied by its maximum value. The oTx driving circuit has to be designed as to match the LED's communication frequency, the cut-off frequency, as well as its non-linear behaviour.

One important characteristic of LED when the security is considered at the physical layer, is the Lambertian emission.

Usually, the ideal VLC systems consider the Lambertian emission order (m) as being equal to 1, that results from the relation:

$$m = (-\ln 20) / [\ln (\cos (\Phi 1/2))] \quad (1)$$

The Lambertian emission order depends on the semi-angle at half radiation luminous intensity $\Phi_{1/2}$. If $\Phi_{1/2} = 60^{\circ}$, then m = 1.

The oTx Lambertian radiant intensity is:

$$R(\varphi) = (m + 1) / 2\pi \cos^{m}(\varphi) \quad (2)$$

The R(φ) measurement unit is 1/sr.

In order to increase the optical communication link, the proper lens in front of the LED is used. The LED's low light flux brought by the large viewing angle must be reallocated to increase luminescence and the transmission range in communication applications. For this reason, the appropriate lens in front of the optical emitter must drive to achieve a long data transmission range while dramatically reducing the overall system size for use in thin electronic products. The proper beam of the visible light has to be obtained according to the specific application of VLC system and properly designed (and aligned) to hit the active area of the PD.

As for the photodetector, the regular p-type/intrinsic/n-type (PIN) PDs, avalanche photodiodes (APDs), and single-photon avalanche diodes (SPADs) are the most suitable candidates. APDs are in fact, PIN PDs operating at high reverse-bias voltages. APD and PIN PDs are the most widely used as PDs in VLC systems due to their fast response time and low noise. However, APD although more stable for high/low temperatures, needs much higher reverse voltage than PIN PD, which is an important issue. Therefore, PIN PDs are considered for a number of commercial embedded circuit implementations [14].

To avoid interference from various data streams collected from undesirable parts of the spectrum onto the active area of the PD, as well as the negative effects of AWGN, the optical filter (OF) is placed in front of PD. Its gain is defined as $T_s(\theta)$.

In order to improve the PD's sensitivity and therefore its goodput value, lens that acts like optical concentrator (OC), with gain $g(\theta)$, aim to collect and concentrate the spectrum intensity onto the PD's active area.

In case that the $|\theta| \leq \Omega_{FoV}$, the $g(\theta)$ is expressed as:

$$g(\theta) = (n^2) / (\sin^2(\Omega_{FoV})) \quad (3)$$

The notation θ represents the incidence angle of the light ray and *n* is the internal refraction order. The field of view (FoV) is the solid angle through which the PD is sensitive to the electromagnetic radiation in the visible light spectrum.

Any losses due to optical concentrator interface reflections or the filter's imperfections are counted into the $T_s(\theta)$.

The Ω_{FoV} is determined by the type of the PD. In case of a semisphere PD, the Ω_{FoV} is usually expressed as:

$$\Omega_{FoV} \leq \pi/2 \quad (4)$$

The g(θ) increases with the reduced FoV.

If PD archives $\Omega_{FoV} \approx \pi/2$, then $g(\theta) \approx n^2$ for the entire FoV.

On the other side, when the incidence angle of the light ray (θ) is larger than the Ω_{FoV}, the active area of the PD does not detect any ray of light.

When $|\theta| \leq \Omega_{FoV}$, the effective light collection area of PD with lens and filter is:

$$A_{eff\_oRx}(\theta) = A_{oRx}(\theta)\, Ts(\theta)\, g(\theta) \cos(\theta) \quad (5)$$

On the other hand, the effective light collection area of PD with lens and filter ($A_{eff\_oRx}(\theta)$) is null when $|\theta| > \Omega_{FoV}$, $g(\theta)$.

In the PD's spreadsheets the manufacturers always present the relationship diagrams between the wavelength λ and generated current/power, in unit of A/W [11].

The value of received optical power is the $P_{oRx}(\lambda,t)$ that depends of spectrum wavelength (λ) and time (t). The $P_{oRx}(\lambda,t)$ affects the Rx circuit current responses. The intensity modulation and direct detection (IM/DD) technique for wireless visible light transmission is used here to model both the oTx and oRx behaviours.

3. The physical layer security in VLC setups

The researchers refer to the VL wireless communication systems as secure since the light rays cannot penetrate through the solid objects, unlike the radio-frequency (RF) waves (see figure 2). The Physical Layer Security (PLS) although is not intensively considered in the research of VLC systems, can play an important role in reducing both the complexity and latency of novel security standards.

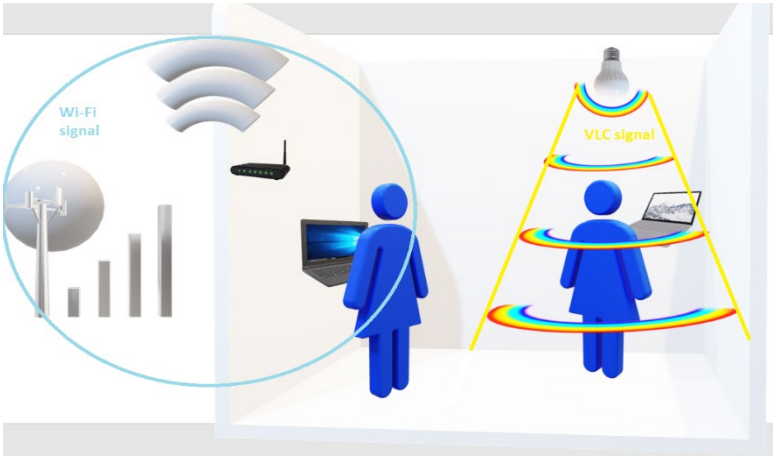


Fig. 2. Wi-Fi signal configuration versus a VLC signal in a LoS scenario

Unlike the RF signals that have a uniform distribution with a relatively long range and penetrates through the solid objects, the visible light signals cannot pass through objects and have a cone-shape distribution. In the case of a LoS scenario, as in figure 2 can be seen, at the physical layer, security is not supposed to be an issue.

However, in the case of non LoS scenarios, with mobility and MIMO communication, especially when Intelligent Reflective Surface (IRS) is used, an extensive investigation of the PLS becomes necessary. The IRSs consist of an array of dedicated IRS units that can be designed to change the phase, amplitude, or frequency of incident radio or optical signals. Typically, signals transmitted from different signal sources (antennas in case of RF and LEDs in case of the optical signal) are sent towards IRSs, which reflects a beamformed signal towards the legitimate users. In a VLC system with MIMO and IRSs, the information is possible to be focused on the legitimate users, while noise-only to eavesdroppers.

Thus, in a plausible scenario, the IRS creates an alternative transmission path when the LoS is blocked between the oTx and oRx or the IRS is placed in a position it can reflect the beam of rays to different legitimate users. The IRS scheme can be important for high-

frequency communications where the optical path loss, caused by shadowing or obstacles on the LoS optical path, becomes significant.

Most of the traditional massive MIMO systems in RF communication, use special techniques like beamforming and jamming with additional, artificial noise insertion to enable a secure physical layer transmission.

However, the achievable secrecy rate is limited even with these techniques when the links of the legitimate user (the oRx) and the eavesdropper are highly correlated (as seen in figure 3). IRS can be used in such a scenario to constructively add the beamformed signal towards the user and destructively add towards the eavesdropper.

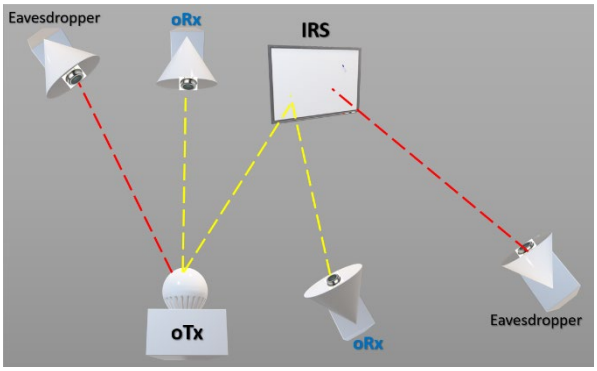


Fig. 3. A VLC system in a LoS scenario with IRS

As the signal travels in a nonLoS path, it is difficult for the eavesdropper to detect the incident angle of the signal. However, when the environment is built to make the system secure with IRS, the system needs to detect and locate the eavesdropper.

The IRS controller, which controls the phase of IRS, can be compromised by an active attacker to focus the beam towards unintended users. If the location of the IRS is exposed, a passive attacker can also locate itself near the IRS to exploit a correlated channel for eavesdropping [15].

3.1. The security issue in VLC standard

A significant event for wider implementation of VLC systems was the advent of the IEEE 802.15.7 standard in 2011. The standard outlines three physical layers (PHY) (from PHY I to PHY III) and the Media Access Control (MAC) layer. The PHY I layer is designed for outdoor setups, and the PHY II with PHY III layers are considered for the indoor applications. The physical network topologies supported by the Media Access Control (MAC) layer are peer-to-peer, star and broadcast. In peer-to-peer topology, the role of the controller is performed by one of the two nodes involved in the communication between them. The star topology allows all nodes to communicate with each other through a single centralized controller.

The broadcast topology permits a real-time, synchronized communication between all hosts. This has features that refers to colour function and visibility, avoid flicker, dimming, support for mobility, support for pairing and disassociation in the VLC Personal Area Network (VPAN) generation of network beacons if the device is a coordinator, and reliability of the connection between MAC entities [16].

In the IEEE 802.15.7-2011 standard, 3 classes of devices are considered: mobile, vehicles and infrastructure. The MAC 802.15.7 layer is very close to the IEEE 802.15.4 MAC Wireless Personal Area Network (WPAN). Though, many scenarios of VLC setups

technology are not considered in this standard, therefore, the IEEE Task Group 7m, is expected to revise it [16].

This standard does not provide any specific security mechanism. However, in case of the use of VLC in safety-oriented applications (such as body area networks or V2V communication), a strong security infrastructure is mandatory to assure the veracity of the data. Therefore, security mechanisms that will not greatly diminish the Quality-of-Service (QoS) of the overall network must be considered [17].

3.2. Study on the PLS for two different scenarios

Depending on the indoor scenario, the VLC architecture, its area of application, and the signal's power, there are different probabilities of data interception, therefore sensitive data must be transmitted wireless in a secure manner. The risks of data snooping, signal jamming, and modification in a number of VLC architecture, are analysed in [18,19].

The PLS is here investigated and compared in two different environments, (i) the medical facilities (a hospital room) and (ii) the underground spaces dedicated to mining activities.

We must extend the investigation of the PLS for medical facilities due to the advances registered in body area network (BAN) smart devices dedicated to both health and wellbeing that are today world widespread.

Into the indoor environments, the beams of lights suffer from normal transmission (photons do not interact with any material), light refraction (during transmission, photons' velocity is changed), light absorption (when photons give energy to the materials they hit) and/or reflection (when photons of identical energy are immediately emitted by the material). Depending on the light's behaviour when hitting the objects and environment, materials indoor are translucent (light is transmitted diffusely), transparent (low amount of light is absorbed and reflected) or opaque (materials absorb all the energy from the light photons).

Fig. 4. Ray of lights with multiple reflections and bounces in a hospital room

Most of the metallic materials, for example, are opaque but layers thinner than 0.1μm can transmit the light. In metals, the refractive index is 0.90–0.95, for glass it is close to 0.05. Around the wavelength of 400nm, the reflectivity of plastic is 1.52, plaster is 1.60 and white paint is 2,1 [20]. As wavelength increases, the reflectance of plaster (walls, floor, and ceiling) slowly increases [21].

The walls, ceiling, floor and furniture in the medical facilities (as seen in figure 4) have predominant reflective characteristics, hence specular reflections and time-dispersion have to be considered due to multiple bounces of light ray into these environments. Root Mean Square (RMS) Delay Spread (DS) and optical path loss are two characteristics that have to be determined for the specific VLC architectures.

Because of the multiple diffused reflections with a multipath channel, a loss of initial signal energy will result. Multipath signals introduced by diffused reflections are superimposed on the LoS signal, thus inter-symbol interference (ISI) caused by multipath cannot be ignored. Moreover, the multipath reflections with Doppler effects jointly must be evaluated in a mobile scenario with multiple users. Therefore, due to the sensible data to be transmitted wireless in these environments, the mobility of these devices and the interaction of photons with multiple objects, security must be considered [22].

On the opposite, the underground environments seem to be more friendly for a robust VLC system, resulting in fewer concerns regarding data security at the physical level (figure 5). The vast majority of the light rays are absorbed underground, some reflections are diffused and these can be well modelled by a lambert model. Unless IRSs are used, in the underground spaces, the security issues are limited in the illuminated area as the environment in an underground mine is predominantly dark grey and black, reflections and multiple bounces are at a minimum level, therefore here is a high grade of security at physical layer because of the interception difficulty of reflected or delayed signals.

The visibility into underground spaces is an important parameter to be considered while modelling the visible-light wireless communication and its PLS. Therefore, since the gallery of a coal mine is composed of coal dust particles, they can dramatically affect the friendly environment for optical transmission and induces a strong reduction of visibility, therefore an important path loss [23].

Fig. 5. Ray of lights with high absorption in underground mine

According to equations from 1 to 5 and the channel impulse response mathematical model presented in [4] and the specific characteristics described in table 1, result simulations presented in figures 6 and 7.

Table 1. Characteristics considered for simulations

No.	Characteristics	Values considered for simulations in	
		hospital room	underground mine
1	Semi-angle of half power [0]	45	45
3	Transmitted optical power by LED [W]	3	0.336
4	Active area of PD (APD) [mm2]	10	7.02
5	Reflectivity used for environment	1.5 and 1.6	0.2
5	Refractive index of the lens in front of PD	1.55	1.515
6	FoV of the PD	45	45
7	Dimensions of space L x W x H [m]	4 x 5 x 2.5	3 x 2.5 3.5
8	Distance between oTx and oRx [m]	1.5	1.5
9	Ambiental light [lx]	400	200

The results of simulation conducted in Octave app are presented in figure 6 for a hospital room and in figure 7 for an underground mine environment.

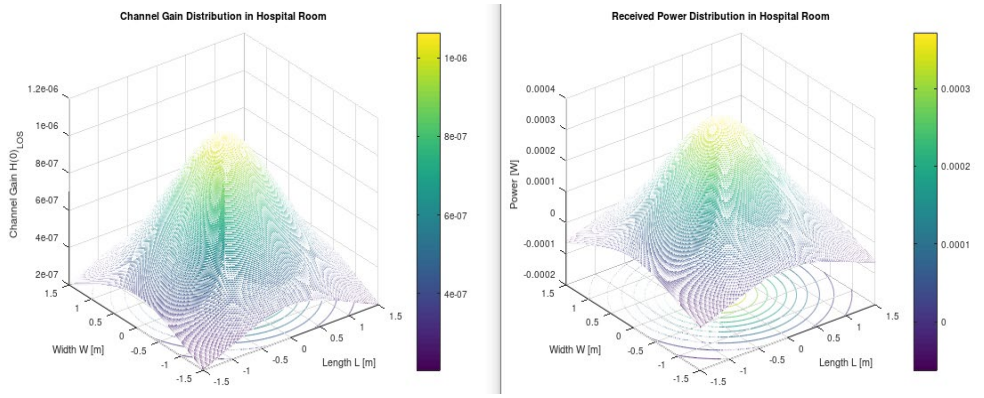
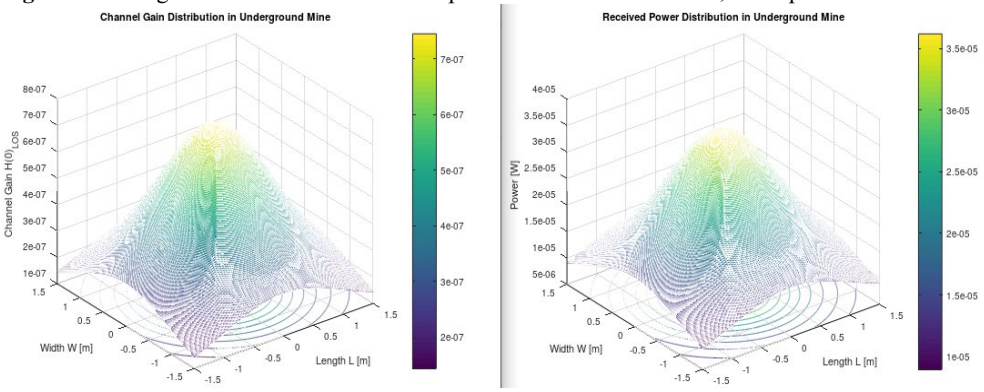


Fig. 6. Channel gain distribution and received power distribution with lens, in underground mine

Fig. 7. Channel gain distribution and received power distribution with lens, in hospital room



The channel gain *H(0)* distribution results and received power *P* distribution with lens in front of oRx are important for PLS and data secrecy during transmission.

Table 2. Results of simulations

	Results of simulations in	
	hospital room	underground mine
H (0)	$7\ 10^{-7}$	$5\ 10^{-7}$

P [W]	$2\ 10^{-4}$	$2.5\ 10^{-5}$

The light distribution in the hospital room is higher due to the high LED power (that may be used here) and the reflective properties of the objects indoor. The light in the underground mine has a narrower distribution and a lower power because of the low LED power (because of the energy source limitation imposed by the security rules) and high rate of light absorption.

The PLS into the medical facilities must be considered, on one hand, because of sensitive data transmitted and because the environment (as shown in simulations above in the hospital room) make possible the eavesdropping.

The more advanced solutions to increase the security communication in VLC systems is a hybrid approach, involving both the physical and application layers. Thus, a general solution to increase the VLC security, no matter the scenario, (LoS, non LoS), application area (indoor, outdoor or underground) or architecture, is to design efficient algorithms, and generic environments capable to be applied in a number of situations, including MIMO and mobile transmission.

In particular, the artificial jamming signal generation property of some advanced modulation techniques is the most important advantage in providing PLS compared to the traditional approaches. The theoretical methods, to develop the maximum achievable secrecy capacity and secrecy rate of the physical layer security algorithms will be much different than the approaches adopted by the traditional systems because of the different system architectures employed.

Also, incorporating user mobility and device orientation into the VLC channel models and combining VLC and RF systems pose new challenges in PLS research and development.

Conclusions

Research challenges in PLS refer to the most suitable physical layer features to be exploited for the definition of security algorithms for heterogeneous environments that pose a number of challenges and characterized by high network scalability and different forms of active malicious attacks. Artificial intelligence can be also exploited to dynamically tune the PLS layer security algorithms.

While maintaining QoS in essential environments, as the medical facilities and mining spaces are, is important to determine how to best develop lightweight key distribution and authorization techniques that positively influence the PHY-layer secrecy features.

The security mechanisms to be used between the oTx and oRx with the IRS panel can be considered to ensure the security of the IRS controller.

New algorithms for PLS in multi-user and broadband VLC systems must be searched to develop improved modulation schemes such as spatial modulations techniques that are derived from it such as index modulation, space shift keying (SSK), OFDM-index modulation techniques (OFDM-IM), or different techniques such as optical MIMO with non-orthogonal multiple excesses (NOMA) systems.

References

1. Y. Tanaka, T. Komine, S. Haruyama and M. Nakagawa, *12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. PIMRC 2001. Proceedings (Cat. No.01TH8598)*, San Diego, CA, USA, (2001).
2. http://www.naka-lab.jp› kit_e
3. [online] www.nobelprize.org/prizes/physics/2014/press-release/, last accessed on 1st of April, 2021
4. S.M. Riurean, et.al. *Application of Visible Light Wireless Communication in Underground Mine* (Springer, Switzerland, 2021).
5. A. E. Marcu, R. A. Dobre and M. Vlădescu, *2020 43rd International Conference on Telecommunications and Signal Processing (TSP)*, Milan, Italy, 2020, pp. 166-169, (2020).
6. S. Riurean, R.A. Dobre, A.E. Marcu, *Proceedings Volume 11718, Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies* **X***;* 117182B (2020).
7. A.M. Căilean, M. Dimian, V. Popa, *Sensors*, 20(**13**), 3764 (2020).
8. Shaaban Rana, Faruque Saleh, *Physical Communication*, **40**, 101094, (2020).
9. Tannaz Sirous, Ghobadi Changiz, Nourinia Javad, et al., *Wireless Personal Communications*, **113** (1), 17-32, (2020).
10. N. Anous, M. Abdallah, M. Uysal, et al., IEEE Access, 6, 22408-22420, (2020).
11. L. Zhou, C. Wang, A. Al-Kinani and W. Zhang, *IEEE Transactions on Communications*, vol. 66, no. 9, pp. 4059-4073, (2018).
12. S. Riurean, In: Antipova T. (eds) Comprehensible Science. ICCS 2020. Lecture Notes in Networks and Systems, vol 186. Springer, Cham (2021).
13. C. H. Yeh, C. W. Chow, H. Y. Chen, Y. L. Liu, and D. Z. Hsu, *J. Optics*, **18**, no. 6, pp. 1–9, (2016).
14. T. Cevik, and S. Yilmaz, Int. J. Comput. Netw. & Commun., vol. **7**, no. 6, pp. 139–150, (2015)
15. M. Ylianttila, White paper, arXiv (2020).
16. Standard IEEE 802.15.7 https://www.ieee802.org
17. H. Kurunathan, R. Severino and E. Tovar, J. Sens. Actuator Netw., **10**, 23, (2021)
18. G. Blinowski, IFACPapersOnLine **48** (4) 234–239, (2015)
19. S. Riurean, R.A. Dobre, A.E. Marcu, Proceedings Volume **11718**, Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X; 117182B (2020)
20. S. Riurean, T. Antipova, Á. Rocha, M. Leba & A. Ionica, J Med Syst **43**:1-10, (2019).
21. Y. Qiu, H.-H. Chen, W.-X. Meng, *Wirel. Commun. Mob. Comput*. **16** (14), 2016-2034, (2016)
22. Z. Ghassemlooy, S. Zvanovec, M.A. Khalighi, L.N. Alves, *Visible Light Communications: Theory and Applications*, (CRC Press; 1st edition, 2017).
23. F. Javaid, A. Wang, M. U. Sana, A. Husain and I. Ashraf, Electronics, **10**(8), 883, (2021).