Data Sniffing Over an Open VLC Channel

I. Marin-Garcia
FIEC
ESPOL
Guayaquil, Ecuador
imaringa@espol.edu.ec

A. M. Ramirez-Aguilera
Facultad de Ciencias
UASLP
San Luis de Potosí, Mexico
atziry@fc.uaslp.mx

V. Guerra[1]; J. Rabadan[2];
R. Perez-Jimenez[3]
IDeTIC
ULPGC
Las Palmas de Gran Canaria, Spain
{vguerra[1],jrabadan[2],rperez[3]}@idetic.eu

***Abstract*— The feasibility of using Visible Light Communications (VLC) technology is a reality nowadays. As this technology is being inserted into the mass market, deliberation about the security provided by this technology, which is one of their main selling points, should be taken into consideration. In this paper, different scenarios of VLC sniffing are studied. A physical experiment in laboratory conditions was performed to demonstrate that, without other supported security elements, as cryptography, VLC sniffing is not only a possible but a probable attack. This type of attack could also be exploited in more complex attacks such as Spoofing and Man-in-the-Middle.**

Keywords*— *Visible Light Communication; Sniffing; Network Security.

I. INTRODUCTION

In the last few years, the use of Visible Light Communication (VLC) has become a topic of interest in the data networks area. This increase of interest is based on many reasons among which are the use of unused or unlicensed frequency bands, the marketability of the new technology or the inherent security perceived on the use of VLC. The inception of this security perception is that visible light, the frequency band used in VLC, cannot go through objects, and therefore, indoor communication is inherently protected from external observers.

Among these topics, the aim of this work is to study the security robustness of VLC. Although the current IEEE VLC standard [1] takes into consideration communication security through the optional use of cryptography, due to implementation design, designers may leave security concerns and their solutions to be implemented at the highest layers of the communication stack were access to computing power and memory is greater. This decision may be founded on the belief that VLC is essentially safe at short distances or indoor scenarios since the medium makes inspecting and capturing the VLC frames extremely difficult from away or from outside. Another justification for the lack of security requirements may be that VLC is implemented in a wide range of applications and devices which go from data intensive, and computing power reachable such as computer-to-computer links; to links between simple devices such as inter-vehicular communication or geolocation systems in which, the devices don't have robust computing capabilities.

This paper is focused on the possibility of accomplishing the sniffing of data packages transmitted through a VLC link. To perform the task in a realistic way, we defined the coverage area of a VLC emitter, usually defined using Line-of-Sight (LOS) approaches; even if technical VLC links also consider NLOS components with, mostly, lambertians approximations. Nonetheless, as mentioned by [2], developers commit a common mistake: to not take into account the security issues and functions that may be implemented. Moreover, in the case of the VLC standard, the application of security is not required as stated on Section 7.2 of the IEEE 802.15.7 document. Hence, security is not guaranteed since in practice security properties, such as confidentiality and integrity, would be implemented at the logical layer where the resources and libraries are more conveniently accessible.

The fact that security implemented at the logic/application level has been broken multiple times, in the last several years, as proven with attacks against wireless protocols with similar security schemes, makes us believe that the "optional" security implementation should be a "must". Based on several studies [3]-[6] that have been done along these lines. Furthermore, in recent years works [7]-[9] about exploiting AES-CCM*, also implemented in other platforms and technologies, have been presented, which limit the assurance of security AES-CCM* encryption provides.

On this paper, we study different simulation scenarios, which include NLOS reflections using both Lambertian and Phong [10] scattering pattern, in order to determine the amount of power received through a room with multiple synchronized emitters. An experimental demonstration of a sniffing scenario has been also performed. The results of the experiment suggest that VLC channels should not be considered intrinsically secure anymore.

The paper is organized as follows: Section II briefly states VLC security specifications and the security domain properties used in the paper; Section III describes the attack scenarios tested for the paper and the relevance they have in the VLC security estimations. Section IV reports the simulations. Section V describes the simulation results. Section VI presents the experiment done to support the paper claims and its results. Finally the conclusions are provided.

This work was founded in part by the Spanish Research Administration, MINECO Project ARIES Ref. TEC2013-47682-C2-1.

978-1-5090-2526-8/16/$31.00 ©2016 IEEE

II. VLC Security

The security suite specifications on section 7 of the IEEE 802.15.7 standard state that "the MAC sublayer is responsible for providing security services on specified incoming and outgoing frames when requested to do so by the higher layers". The method used to provide this security in the standard is the use of AES-CCM* cryptography which, based on the procedures indicated on the standard, provides the security services of: Data Confidentiality, Data Authenticity and Replay Protection. Nevertheless, the security services, or properties, of Data Integrity, Non-repudiation and Availability [11] are not considered in the IEEE 802.15.7 standard in its current (2011) version.

As it is shown above, the use of techniques and security protocols is pragmatically non-existent and the standard leaves these security issues to the upper layers on the end-devices. Since the security is optional, as mentioned by section 7 of the IEEE 802.15.7 standard, and can be abstained from the implementations by developers, some basic attacks such as sniffing, Denial of Service (DoS) and Man in the Middle (MiM) are neither prevented nor mitigated. The justification for the lack of security requirements may be that VLC is used in very different types of environments with heterogeneous hardware that may or may not have the computing power [12]-[14] and memory [15] required to encrypt and decrypt the communication between the VLC devices.

Furthermore, if security were implemented following the standard, the cryptographic mechanism would be based on symmetric key cryptography, which requires that all devices involved on the communication know in advance shared knowledge. This means that, for example, an attacker that is already part of the network can easily sniff out the data since it already has the key. This key is provided by the higher layers which would open further attacks that are not considered in this paper.

In addition, the standard requires that if one of the devices in the communication is unable to (or chooses not to) use the security suite, by default, the other devices should move to an unencrypted mode of communication. Therefore, it minimizes the importance or need of enforcing the security suite in all applications.

Finally, for the present work the channel secrecy capacity (Cs), as defined by [16]-[17], is the maximum data rate at which the attacker is unable to decode information, and can be expressed in terms of the SNR (γ_{Bob} and γ_{Eve}) of the receiver and the potential eavesdropper using (1). Therefore, the outage probability of Cs > 0, as expressed in (2), depends inversely on the distance ratio (d_{Bob}/d_{Eve}) and the pathloss exponent (α= 4 in the case of VLC scenarios).

$$Cs=\begin{cases}\log(1+\gamma_{Bob})-\log(1+\gamma_{Eve}) & \gamma_{Bob}>\gamma_{Eve}\\ 0 & \gamma_{Bob}\leqslant\gamma_{Eve}\end{cases} \quad (1)$$

$$P(Cs>0)=P(\gamma_{Bob}>\gamma_{Eve})=\frac{1}{1+(d_{Bob}/d_{Eve})^{\alpha}} \quad (2)$$

When the distance from the light source to the attacker is greater than the distance to the receiver, the outage probability of Cs>0 is better for a VLC LOS system than for a RF system; for example, if $d_{Eve}=2*d_{Bob}$ the probability is 94.12% for VLC LOS systems and 80.00% for RF. But, when the distance from the light source to the attacker is smaller than the distance to the receiver, the probability of Cs>0 is better for a RF system; for example, if $d_{Eve}=0.5*d_{Bob}$ the probability is 5.88% for VLC and 20.00% for RF systems.

III. Attack Scenarios

For the sniffer attacks, the objective of the passive attacker (Eve) is to get the information sent from an emitter (Alice) to a static receiver (Bob). Further retransmissions of the information can be done through other channels, such as RF, but it is outside the scope of the present analysis. Since this is a passive attack, Eve just needs to be able to receive the signal. In this case we considered three different scenarios as shown in Fig. 1.

The first scenario, Fig.1.a, is the simplest one in which we have an emitter (Alice) sending data to a receiver (Bob). The area in which any receiver sees the communication is defined assuming that the emitter has a generalized Lambertian pattern and only the Line-of-Sight components are considered. As any other receiver located under Alice area of illumination Eve receives the signal and therefore may sniff away the messages. This is possible since, even if the security mechanisms of [1] were implement, the key would be known by all members of the network.

The second scenario Fig. 1.b considers that Alice is located at an indoor environment where the surfaces present lambertian-based scattering, objects in the area of illumination may display reflectance characteristics. Therefore the area of illumination would be different from the expected one and an attacker (Eve) that should be outside the area of communication can still sniff the information away.

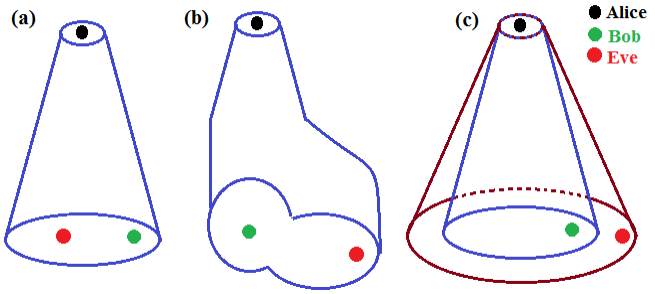

Fig. 1. Standard attack scenario: (a) the attacker (Eve) is located in the same area covered by the emitter. (b) An area of coverage that, due to reflections and other channel significant variations, is different from the expected area of coverage. (c) The attacker in located outside the calculated (expected) area of coverage but it is able to get enough signal.

The third scenario, Fig 1.c, expands the first and second ones. In this case Eve is outside the theoretical area covered by Alice's emissions, such as in a room corner or outside the room with direct view of Alice. In this case, using the

appropriate optical system, Eve may receive enough signal to sniff away the information.

In all the previous scenarios, Eve is a passive device who only receives the VLC transmission and does not interact with the VLC network. Promiscuous devices that not only sniff but also interact with the VLC network as identified devices may be possible and would not invalidate the premises of the attacks above described.

IV. Environment Simulations

In order to validate the expected lack of security, simulations of three cases were studied: The first case was done considering only the Line-of-Sight (LOS) of each emitter with Lambertian radiation pattern. The second case also considered in the received Non-Line-of-Sight (NLOS) components using a Lambertian pattern for the reflections. Finally, the third case considers the whole optical components in the transmission, not only the LOS components but also NLOS components, modeled as Lambertian or even non Lambertian when semi-specular surfaces are present, applying a Phong reflection model. These simulations were based in the propagation channel model of [18], where the impulse response of the indoor VLC channel, in terms of the wavelength, is described as the summatory of the two components, LOS (3) and NLOS (4). The NLOS reflection model assumes that the percentage of incident signal reflected diffusely from the surfaces is 43% and the directivity of the specular reflection is 250 at all the wavelengths, comprising the whole visible spectrum.

$$h_0^l(t)=\frac{1}{(d_{E_l,R})^2}F_E(\theta,n,\lambda)A_{eff}(\Psi)\delta\left(t-\frac{d_{E_l,R}}{c}\right) \quad (3)$$

$$\sum_{k=1}^{\infty}h_0^l(t)=\sum_{i=1}^{N}\sum_{u=1}^{U}\frac{1}{(d_{u,R})^2}F_l(\theta_{u,R},\theta',\lambda)A_{eff}(\Psi_{u,R})\delta(x)$$
$$\forall\, x=t-\left(\sum_{j=1}^{u}\frac{d_{j-1,j}}{c}\right)-\frac{d_{u,R}}{c} \quad (4)$$

In the three simulated scenarios, the simulated room was 5.00 meter wide by 5.00 meters depth and 3.00 meters height. There were 8 synchronized light (emitters) sources and the measurements were done at a z-offset of 0.80 meters, with an average luminance level of 546 lux, as shown in Fig. 2.

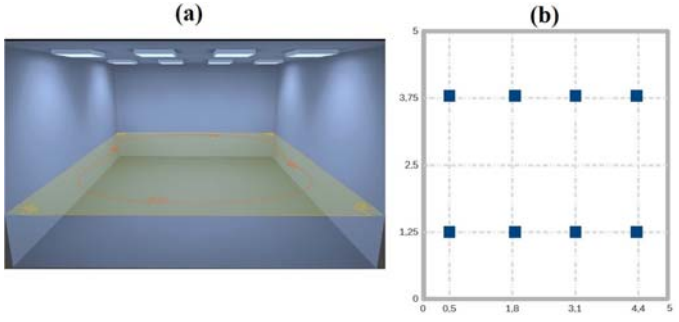

Fig. 2. Illumination scenario. (a) Shows the 3D render using the design software DIALux[19]. (b) Shows the emitters positioning inside the room.

The position of the different emitters and receivers, and the general simulation specifications are shown in TABLE I. As it can be observed the characterization of, both, the emitters and the receivers, follows a real case according to the illumination standards of an office [20]. The reflection coefficients used for the room surfaces are based on [21].

TABLE I. Simulation Parameters

Parameter	Value
Transmitter Positions (x,y) z = 3.00 m	L_1=(0.50,1.25) L_2=(1.85,1.25) L_3=(3.10,1.25) L_4=(4.36,1.25) L_5=(0.50,3.79) L_6=(1.85,3.79) L_7=(3.10,3.79) L_8=(4.36,3.79)
Transmitter Orientation	Elevation:-90°; Azimuth: 0°
Transmitter Dimensions	0.60 x 0.60 m^2
Emitted Optical Power	41 W
Receiver Positions	r_{xy}=(x,y,0.80) x=[0.00:0.10:5.00] y=[0.00:0.10:5.00]
Receiver Orientation	Elevation: 90°; Azimuth: 0°
Receiver Effective Area	1.00 cm^2
Receiver FOV	85°
Number of rays	10,000
Maximum number of reflections	3
Resolution (Δt)	0.20ns
Simulation time	40.00ns

A. *Case 1: LOS Components only*

The first simulation considers only the components obtained from LOS configuration. Therefore, no reflected light was considered for the calculation of the power arriving at a particular point. The results were obtained using a 0.10 by 0.10 meters grid located at 0.80 meters elevation. This simulation provided us with a baseline to study the power that reached different points in the room.

B. *Case 2: LOS + NLOS (Lambertian Reflection pattern)*

In the second case, a lambertian reflection pattern was used in the simulation and added to the power provided by the baseline. The simulation is based on 10.000 rays per emitter and a 0.10 by 0.10 meters grid is used to determine the power reached at a 0.80 meters height plane. In this case, it was expected than the real power reached at any point was greater than on the Case 1 and proved possible the second and third proposed attack scenario.

C. *Case 3: LOS + NLOS (Phong Reflection Pattern)*

In the third case, a Phong reflection model was used for the NLOS components, which were, latter on, added to the LOS values. As in the previous case, 10.000 rays were initially emitted from the emitters and a 0.10 by 0.10 meters

grid at 0.80 meters height was used to collect and map the power density that reached the receivers. As in the previous case, the result of this simulation may prove the viability of the second and third proposed attack scenarios.

V. Simulations Results

As can be observed in Fig.3, as expected, the higher power received is directly under the emitters and decreases with the distance from them. This "basic" simulation provides an approximation to the power levels at a location inside the studied room. However, even if this kind of simulation is used in some lighting studies, that may be used to define the areas of coverage of building lighting infrastructure usable for VLC, it lacks of complexity and completely, providing false expectations regarding the area covered by the lighting fixtures and their security implications.

The second case results, Fig. 4, showed no large variations from the LOS components of Fig. 3 and the LOS+NLOS (lambertian reflection pattern) values. However the power received at the perimeter is higher and could be considered for attacks such as in the proposed third attack scenario with little significance for the proposed second attack scenario.

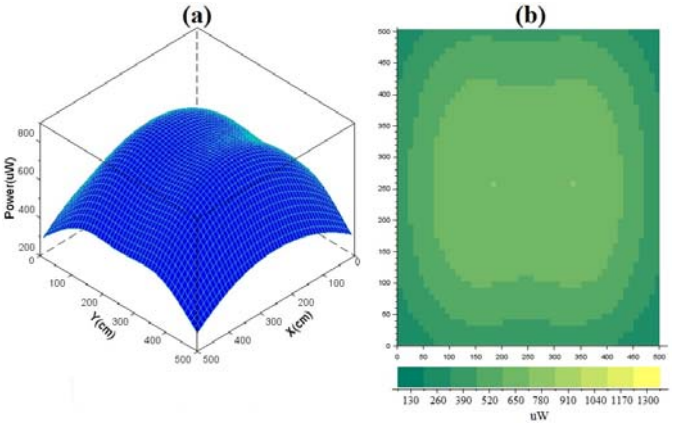

Fig. 3. Simulation considering only LOS components. (a) Power distribution, (b) Power output set in ranges.

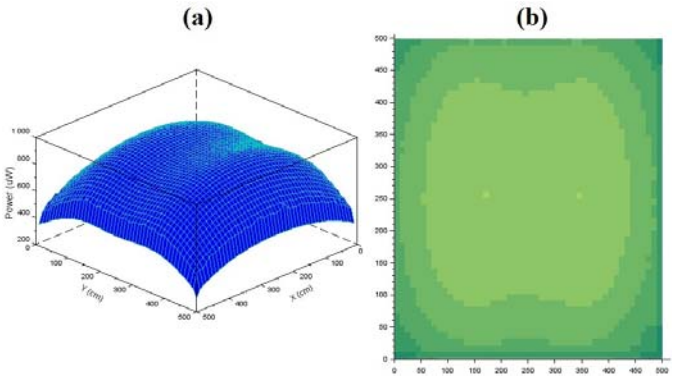

Fig. 4. Lambertian reflection pattern simulation results. (a) Power distribution of LOS+NLOS, (b) Power output of LOS+NLOS set in ranges

If we aggregate the LOS components to the Phong reflection model components, Fig 5.a and Fig. 5.b even if the center of the room, in general, receives more power, there are points in the perimeter with similar or even higher power receptions (Fig. 6 (b) at y≈320 and x≈490) noted by the lighter color. This results seem to validate the second proposed attack scenario and could be used to validate also the third proposed attack scenario.

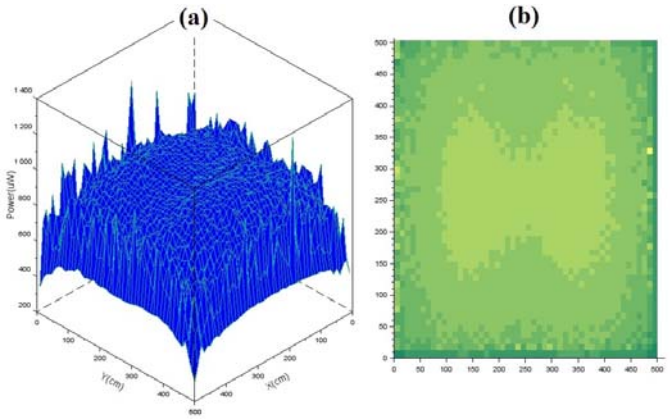

Fig. 5. Phong reflections pattern simulation results. (a) represent the aggregation of the LOS and Phong components and (b) maps in 2D the power received after adding the LOS power and the NLOS using Phong simulation components

VI. Experimental Results

In order to demonstrate the feasibility of an attack as the one presented on the third scenario, Eve being outside the expected area of Alice's coverage, an experimental setup was performed. Fig. 6.b depicts the geometry of the experiment whilst the actual mount is shown in Fig. 6.a.

The emitter side comprised an arbitrary function generator configured to output a TTL signal of 8KHz with the fixed frame 0x5A. Real data would have been used, but to transmit actual information was not in the scope of the problem. To drive the YB-WLED lamp, a basic MOSFET switch using IRF840 was implemented. For the ON periods, the measured driving current was 180 mA, whilst the measured optical power was 5mW.

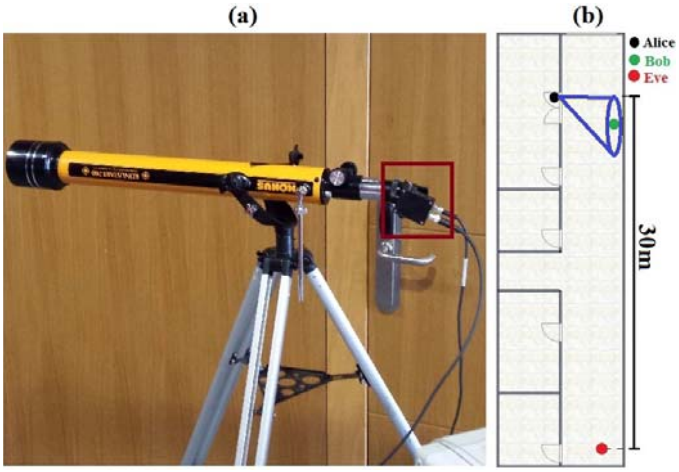

Fig. 6. Experimental setup: (a) Experiment assembly with the PDA36-A amplified PIN photodiode framed in red. (b) Geometry of the experiment showing Aline in black, Bob on green and Eve on red.

Regarding the receiver, a PDA36-A amplified PIN photodiode [22] mounted to a Konustar-700 refractor telescope [23] was used. The arrangement was performed without the eyepiece, as there was no need of image formation. Finally, the output signal was captured using a DSO1052B oscilloscope [24]. The main characteristics of the experimental setup are shown in Table II.

TABLE II. PARAMETERS OF THE EXPERIMENTAL SETUP

Parameter	Value
Distance	30 m
Emitted Power	5 mW
Lens Focal Length	700 mm
Transimpedance Gain	70 dB
Oscilloscope's Sample Rate	500 Kbps

Although the used bandwidth does not comply with the current VLC standard, if a higher bandwidth were required, avalanche photodiodes and/or second amplification stages could be used to achieve the required bandwidth and reception gain.

Using the aforementioned experimental setup, the sniffing over an unencrypted VLC channel was performed. Fig. 7 shows the received signal. After processing the signal, the estimated SNR was approximately 45 dB. In addition, considering the eavesdropping and the propagation in a telescope-based link, Eve´s bandwidth would be presumably much higher that Bob´s, only limiting the attack by power constrains

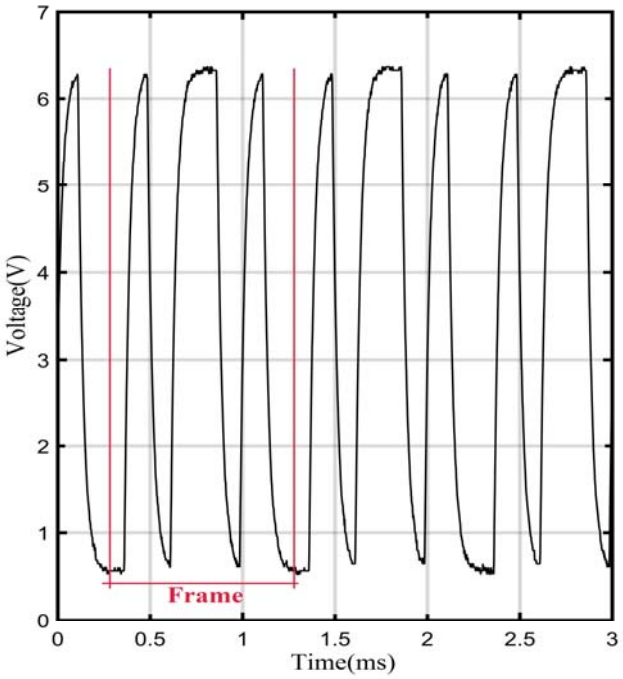

Fig. 7. Captured image of the received signal of the experiment. As can be observed, a 0x5A (01011010) frame is received.

CONCLUSIONS

After finishing the analysis, simulating several scenarios and an experiment testing an attack setup, we come to several conclusions:

Even if the IEEE VLC standard provides a security suite, its implementation is not mandatory and needs to be adopted by all the devices communicating through the channel while it may be also too computing intensive for some of them.

Based on the simulation results, data sniffing over an open VLC channel is a viable attack even when the attacker is located where initially was thought that a passive attack could not be located due to power gaining techniques.

On the results of the third case simulation, the closest to the real world, we find areas with higher received power, due to the addition of LOS and NLOS components, than the ones directly under the emitters. This makes possible that if an attacker was located on those areas, he could sniff data, at least partially due to decrease of bandwidth, from outside the theoretical covered area.

The performed experiment demonstrated the feasibility of sniffing data in a VLC scenario. A SNR of 45dB was obtained using a common telescope and a PIN photodiode followed by a transimpedance amplifier at a distance of 30 meters. The use of cost-affordable devices in this work suggests that sniffing techniques could be an actual threat.

If communication security wants to be achieved when using VLC technologies, a calculation of the emitter's area of coverage using complex models such as Phong should be made. Furthermore, on implementations special attention should be paid to areas that initially were discarded due to low power received since attackers may be located on them.

As presented on this paper, the possible sniffing attack could also be used as an exploit on the down-link in further complex and insidious attacks such as Spoofing and Man-in-the-Middle.

ACKNOWLEDGMENT

We thanks Dr, Jose Martin Luna Rivera of the Universidad Autonoma de San Luis Potosi, Mexico, for his help, patience and support while we did the paper..

REFERENCES

[1] IEEE Standard for Local and Metropolitan Area Networks-Part 15.7: Short-Range Wireless Optical Communication Using Visible Light, IEEE Standard 802.15.7, 2011.

[2] Grzegorz Blinowski, "Security issues in visible light communication systems," *IFAC-PapersOnLine*, Volume 48, Issue 4, 2015, Pages 234-239.

[3] Prasad, R.; Mihovska, A.; Cianca, E.; Mukherjee, S., "Comparative overview of UWB and VLC for data-intensive and security-sensitive applications," in *Ultra-Wideband (ICUWB), 2012 IEEE* International Conference on, vol., no., pp.41-45, 17-20 Sept. 2012

[4] Jiska Classen, Joe Chen, Daniel Steinmetzer, Matthias Hollick, and Edward Knightly. 2015. "The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications," *Proceedings of the 2nd International Workshop on Visible Light Communications Systems (VLCS '15)*. ACM, New York, NY, USA, 9-14.

[5] Mostafa, A.; Lampe, L., "Enhancing the security of VLC links: Physical-layer approaches," *Summer Topicals Meeting Series* (SUM), 2015 , vol., no., pp.39-40, 13-15 Jul. 2015.

[6] Mostafa, A.; Lampe, L., "Physical-layer security for indoor visible light communications," *2014 IEEE International Conference on Communications (ICC)*, vol., no., pp.3342-3347, 10-14 June 2014.

[7] Vidgren, Niko; Haataja, Keijo; Patino-Andres, Jose Luis; Ramirez-Sanchis, Juan Jose; Toivanen, Pekka, "Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned," in *System Sciences (HICSS), 2013 46th Hawaii International Conference on* , vol., no., pp.5132-5138, 7-10 Jan. 2013

[8] Evesti, A.; Suomalainen, J.; Savola, R., "Security risks in the short-range communication of ubiquitous application," in *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for* , vol., no., pp.612-617, 9-12 Dec. 2013

[9] Olawumi, O.; Haataja, K.; Asikainen, M.; Vidgren, N.; Toivanen, P., "Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned," in *Hybrid Intelligent Systems (HIS), 2014 14th International Conference on* , vol., no., pp.199-206, 14-16 Dec. 2014

[10] Bui Tuong Phong, "Illumination for computer generated pictures," *Communications of the ACM*, Vol 18, Issue 6, Pages 311-317, June 1975

[11] Information technology — Security techniques — Code of practice for information security management, ISO Standard 27002, 2013.

[12] Jianxin Zhu; Leina Gao; Xinfang Zhang, "Implementation and Time Performance Analysis of Security Suite in LR-WPAN 802.15.4," in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on* , vol., no., pp.1-5, 12-14 Oct.. 2008.

[13] Algredo-Badillo, I.; Feregrino-Uribe, C.; Cumplido, R.; Morales-Sandoval, M., "FPGA Implementation and Performance Evaluation of AES-CCM Cores for Wireless Networks," in *Reconfigurable Computing and FPGAs, 2008. ReConFig '08. International Conference on* , vol., no., pp.421-426, 3-5 Dec. 2008.

[14] Ignacio Algredo-Badillo, Claudia Feregrino-Uribe, René Cumplido, and Miguel Morales-Sandoval. 2010. Efficient hardware architecture for the AES-CCM protocol of the IEEE 802.11i standard. *Comput. Electr. Eng.* 36, 3 (May 2010), 565-577.

[15] Saberi, I.; Shojaie, B.; Salleh, M.; Niknafskermani, M., "Enhanced AES-CCMP key structure in IEEE 802.11i," in *Computer Science and Network Technology (ICCSNT), 2011 International Conference on* , vol.1, no., pp.625-629, 24-26 Dec. 2011.

[16] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," 2006 IEEE International Symposium on Information Theory, Seattle, WA, 2006, pp. 356-360.

[17] J. Zhu, O. Takahashi, X. Jiang, Y. Nakamura, and Y. Shiraishi, "Outage secrecy capacity over correlated fading channels at high SNR," in Proc. 2012 International Conference on Mobile Computing and Ubiquitous Networking, pp. 92–97.

[18] Lopez-Hernandez FJ, Perez-Jimenez R, Santamarıa A; "Ray-tracing algorithms for fast calculation of the channel impulse response on diffuse IR wireless indoor channels". *Optical. Engineering*. Vol. 39, no 10, Oct. 2000, pp. 2775-2780.

[19] DIALux. Lüdenscheid: DIAL GmbH, 2015.

[20] Dilaura, A. Houser, K. Mistrick, R. "The lighting handbook: Reference and applications," IEANA Lighting Handbook 2011.

[21] Kwonhyung Lee; Hyuncheol Park; Barry, J.R., "Indoor Channel Characteristics for Visible Light Communications" in *Communications Letters, IEEE*, vol.15, no.2, pp.217-219, Feb. 2011.

[22] ThorLabs Technical Staff, *PDA36-A Operating Manual*, ThorLabs, August 17th 2011

[23] Konus Optical and Support Systems, "Konustart-700 refractor telescope", KONUS-1736 Catalogue, 2015

[24] Keysight Technologies, "Oscilloscope, 50MHz, 2 Analog Channels", DSO1052B Datasheet, August 2nd 2014.