INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2016, VOL. 62, NO. 1, PP. 7-13
Manuscript received November 10, 2015; revised March, 2016. DOI: 10.1515/eletel-2016-0001

Practical Aspects of Physical and MAC Layer Security in Visible Light Communication Systems

Grzegorz J. Blinowski

***Abstract*—Visible light communication (VLC) has been recently proposed as an alternative standard to radio-based wireless networks. Originally developed as a physical media for PANs (Personal area Networks) it evolved into universal WLAN technology with a capability to transport internet suite of network and application level protocols. Because of its physical characteristics, and in line with the slogan "what you see is what you send", VLC is considered a secure communication method. In this work we focus on security aspects of VLC communication, starting from basic physical characteristics of the communication channel. We analyze the risks of signal jamming, data snooping and data modification. We also discuss MAC-level security mechanisms as defined in the IEEE 802.15.7 standard. This paper is an extension of work originally reported in Proceedings of the 13th IFAC and IEEE Conference on Programmable Devices and Embedded Systems — PDES 2015.**

***Keywords*—Wireless networks, visible light communication, wireless network security, industrial wireless standards, IEEE 802.15.7**

I. INTRODUCTION

VISIBLE light communication (VLC) is a wireless optical communication technology through which baseband signals are modulated on the light emitted by an LED: [1] – [5]. The decreasing cost and hence rapid adaptation of LED-based light make VLC a promising communication technique and a significant alternative to radio-based wireless communication. Wi-Fi, Bluetooth, etc. - the "traditional" radio based communication systems suffer from limited channel capacity and transmission rate due to the limited radio spectrum available. At the same time the user request for data transmission throughput and availability continues to increase. VLC data transmission networks provide an attractive alternative to traditional wireless techniques.

Notable differences making VLC systems more attractive than radio-based networks are:

- VLC systems are interface-orthogonal to cellular, Wi-Fi, Bluetooth and other radio-frequency based networks,
- light does not penetrate solid objects,
- light can be easily directed through optics,
- most indoor, and a significant percentage of outdoor, environments are illuminated.

VLC was proposed both for in-door and out-door applications – see [6] and [3]. In-door applications include a range of communication facilities provided today by Wi-Fi networks, Bluetooth and Personal Area Networks (PAN). Indoor VLC applications range from: office communication – [7], multimedia conferencing – [8], peer-to-peer data exchange, data broadcasting – especially multimedia such as home-audio and video streams, see: [9] – [12], to positioning: [13] – [14]. Currently available commercial VLC systems focus mainly on data broadcasting, and include solutions for museums, shopping centers, exhibition centers, airports and train stations as well as accessibility for disabled persons. VLC based positioning systems, for example "smart carts" that guide the customers to the shelves according to their list of products are already available. VLC systems also provide a safe alternative to electromagnetic interference from radio frequency communications in hazardous environments, such as mines and petrochemical plants, and in applications where traditional WLAN communication may interfere with specialized equipment, for example in hospitals and in aircraft passenger cabins' in-flight entertainment systems (where the additional benefit is the reduced weight of cabling and the potential for integration with passengers' own mobile devices) [15].

The most promising outdoor applications of VLC technology are advertising (via LED signboards), pedestrian steering (via indicator boards), and road safety and traffic management, see [6]. VLC-based positioning and navigation provide a viable alternative to GPS in environments where the GPS signal is weak or non-existent. As LED headlights and taillights in commercially available cars are being introduced, street lamps, signage and traffic signals are also moving to LED technology, and VLC based vehicle-to-vehicle ("VANETs" – Vehicle Area Networks) and vehicle-to-roadside communications have become a reality – [16]. VLC also provides a viable solution for short-range communications underwater where, due to strong signal absorption, RF use is impractical – [17]. In this work we will focus only on in-door applications.

Recently VLC is starting to be considered as a way of augmenting or event replacing RF networks, for example hOME Gigabit Access project (OMEGA) [18], sponsored by European Union developed a wide range of techniques aimed at VLC based multimedia networks. The usage of smartphone cameras and light sensors brings VLC to the field of mobile computing and sensing. In this way VLC has a potential to evolve into a general WLAN standard – in [19] with the OpenVLC platform the authors have demonstrated that with current Software Defined Radio (SDR) toolkits it is relatively easy to bring TCP/IP suite to the VLC medium.

One of the features in which VLC techniques are considered superior to traditional radio-based communication is security. The directivity, and high obstacle impermeability of optical signals are considered to provide a secure way to

This work was supported by the Statutory Grant of the Polish Ministry of Science and Higher Education to the Institute of Computer Science, Warsaw University of Technology.

Author is with Institute of Computer Science, Warsaw University of Technology, Nowowiejska 15/19, 00-665 Warszawa; Poland (e-mail: g.blinowski@ii.pw.edu.pl).

transmit data within an indoor environment, making the data difficult to intercept from outside. The common slogan summarizing VLC security features is: "What You See Is What You Send" (WYSIWYS) [20].

As recent history teaches us, a common mistake in the development of novel communications techniques was to neglect or downplay the security issues. Such was the case with the internet protocol suite - both on the network and, application layer), various encryption and authentication algorithms and protocols, fiber-optics based networks, and more recently – radio-based wireless networks. Currently the VLC industry seems to be on the same path again: the indubitable "pro-security" physical characteristics of visual light communication have steered the developers' focus away from the security track.

In this paper we address security of VLC communications, both from the channel (i.e. information theory) and higher level (MAC) perspective. As far as VLC standards are concerned, we will refer to the IEEE Standard 802.15.7 [21]; however, our discussion should also be relevant to other proposed VLC techniques not covered by the current IEEE norm.

The structure of this paper is as follows: in section II we will describe the basis of VLC technology – the mechanisms of VLC physical layer. In section III we will discuss how security issues could be approached in this communication media; we will also analyze which aspects of VLC should be put into the focus of security research. In sections IV and V we will discuss (respectively) the security of the physical and MAC levels of VLC networks. Section VI summarizes the paper and outlines the areas of future research.

II. The VLC Date Link– an Overview

A VLC physical layer consists of: the transmitter, the propagation channel and the receiver. Their properties are as follows:

Transmitter – Two types of white-light LEDs are used in solid-state lightning: 1) red-green-blue (RGB) emitters; 2) blue-LED on yellow-light emitting phosphorus layer ("single-chip"). The VLC transmitter may use both types, but the second type is more widespread in illumination due to its energy efficiency and lower complexity. Different types and form factors of LED are employed in various environments: high power LEDs or LED arrays are the choice for typical in-door illumination purposes, while low-power devices are used in smart-phones and other mobile appliances. The slow response of yellow phosphorus to blue light modulation limits its spectral component bandwidth to 2MHz, hence the yellow component is filtered- out at the receiver and only the blue component is detected, bandwidth of 8 MHz may be attained with this simple filtering technique [22]. With simple analogue pre-equalization at the transmitter side 40 Mb/s throughput may be attained without the use of a blue filter [23]. By combining a simple pre- and post-equalization, 75 Mb/s can be achieved [24]. Data throughput of up to 100-230 Mb/s has been demonstrated in a single-emitter–single-receiver scenario and On-Off Keying (OOK) – [25]. Higher data rates of about 1 Gb/s are also attainable with more advanced modulation techniques such as DMT and OFDM. Similar data rates were also attained with arrays of separately driven light sources [26].

The receiver collects and concentrates the incoming light on a photo-detecting element. Both imaging and non-imaging receivers are used. Photocurrent generated in the detector is amplified and fed to the D/A circuitry. Currently in devices such as smartphones, tablets, etc., low cost photodiodes or typical optical sensors are used as photodetectors for the VLC channel. With current technology achieving sufficient photo-detector sensitivity, the required bandwidth is not a problem (the transmitter and channel loss and dispersion are the major bandwidth limiting factors). It should be noted that as photodetectors work in an Intensity Modulation/Direct Detection (IM/DD) regime, they produce a signal proportional to the intensity (not the amplitude) of the incident wave: the detector works as a squarer.

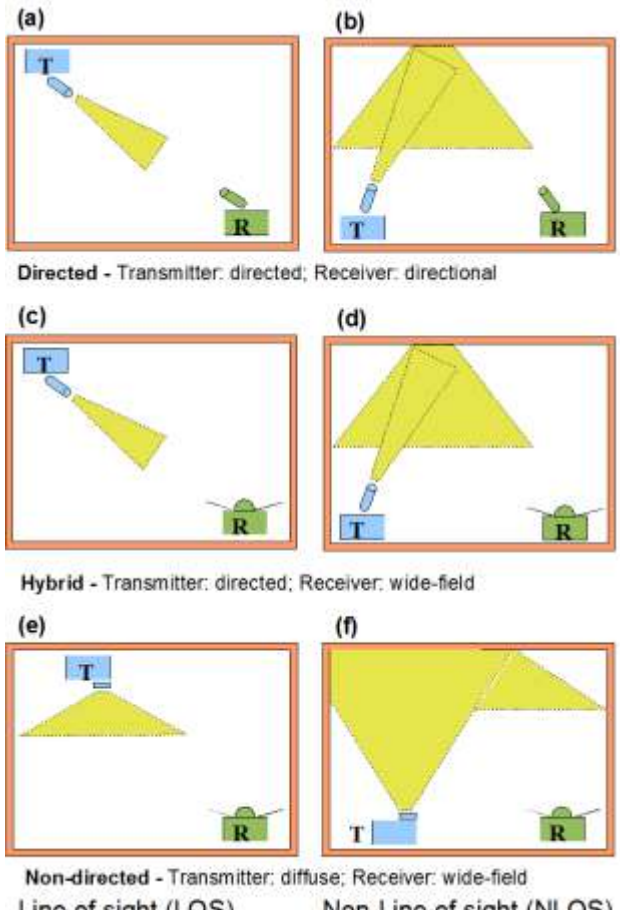

Fig. 1. Classification of links according to LOS/NLOS (line-of-sight) and directionality of transmitter and receiver.

The propagation channel in the case of indoor environments communication may be characterized by six different link configurations, as originally defined in [27] for IR links. *The propagation* channel requires a direct or indirect line-of-sight (LOS) between the transmitter and the receiver. The degree of directionality is a second factor determining the channel type which is dependent on the source beam-angle and detector field of view (FOV). All possible channel configurations are show in figure 1. The most common link types used by VLC are:

- (a) directed-LOS – mainly for short range (<1m) mobile-mobile and fixed-mobile communication and also for infrastructure uplink communications

- (e) non-directed LOS – mainly for infrastructure downlink
- (f) non-directed NLOS (dispersed) – mainly for infrastructure downlink

In general, in all of the above cases, the propagation channel is formed by a number of line-of-sight paths from the transmitter to the receiver, and a diffuse channel is formed by light from the source reflecting off multiple surfaces. The combination of the directed and the diffuse channel determine the overall power received; hence the Signal to Noise Ratio (SNR)) and, in consequence, the bandwidth of the channel.

In outdoor environments, directed or dispersed LOS is used; in this case light from other sources, both artificial and natural, must be taken into account.

III. Security in Various Aspects of VLC Communication

Security of VLC communication up-to date has been mainly tackled with respect to the physical layer. The idea of physical-layer security was introduced by Wyner in his paper on the degraded discrete memoryless wiretap channel [28]. Secrecy capacity was defined as the maximum rate of reliable sender-receiver transmission while the communication is completely obscure to the eavesdropper. A single-letter characterization of the secrecy capacity of non-degraded, wiretap channel was formulated in [29], while the secrecy capacity of the Gaussian multiple-input, single-output (MISO) and multiple-input, multiple-output (MIMO) wiretap channel was resolved in [30] and [31], respectively. It was shown that in case of a Gaussian MISO wiretap channel using zero-forcing via beamforming the eavesdropper's reception is optimal at asymptotic high Signal to Noise Ratio (SNR). When the channel state information for the eavesdropper is not available artificial noise (a jamming signal) added to the transmitted data signal results in an increase of achievable secrecy rates - [32] and [33]. In [34] a MIMO approach to establishing a secure communication zone has been described – the authors proposed to use MIMO technique and beam-forming (similar to RF Wi-Fi networks) to establish a secure channel between the transmitter the receiver located in a particular physical location. BER (Bit Error Rate) is minimized at the receiver's location, while it remains unacceptable high in the rest of the area. In this way a potential eavesdropper physically located some distance from the legitimate receiver is unable to properly decode the data. This is attained without significant influence on the lighting characteristics and is therefore unobservable to the users. Similar approach was proposed in [35] using MISO (Multiple Input Single Output) technique, together with null-steering and artificial noise - an achievable secrecy rate was calculated numerically. Similar approach was also proposed and in part verified in the real environment in [36]. We will return to channel-level security issues with respect to the possibility of signal jamming in section IV.

For the purpose of this work we will consider three classes of VLC devices: infrastructure, fixed and mobile. Their characteristics are summarized in Table 1. As defined in IEEE 802.15.7 - three basic MAC topologies are supported by VLC: peer-to-peer, star and broadcast. The first is typically used between two handheld devices such as smart phones; star topology is used as a replacement for Wi-Fi networks; and broadcast is used in multimedia applications, advertising applications and vehicular networks. Indoor VLC modes are summarized on figure 2.

TABLE I
CLASSES OF VLC DEVICES AND THEIR CHARACTERISTICS

Class / attribute	**Infra-structure**	**fixed**	**mobile**
Device example	Data- streaming Integrated with room light	PC, laptops, other desktop appliances - e.g.: projectors, printers	Smartphone
Fixed coordinator	Yes	Both P2P and coordinator based	Both P2P and coordinator based
Power available	Ample	Limited	Moderate
Form factor	Unconstrained	Constrained	Critically-constrained
Light source	Intense	Weak – moderate	Weak
Mobility	No	No	Yes
Source dispersion	High (ambient)	moderate	moderate
Range	3 m	1 – 3 m	0.1 -3 m
MAC topology applicable	Star, broadcast	P2P, broadcast and star (as client)	P2P, broadcast (as client)

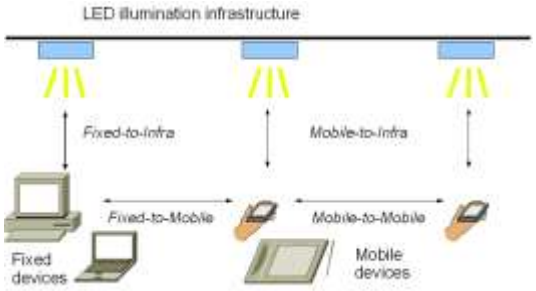

Fig. 2. Indoor VLC modes

We will consider four basic aspects of VLC communication security, namely: availability, confidentiality, authenticity, and integrity with respect to infrastructure, fixed and mobile classes of VLC devices. The threats that we consider are the possibilities of: jamming, snooping and data modification. Each threat should be considered separately for all communication schemes, i.e. mobile-to-mobile, infrastructure-to-mobile, mobile-to-infrastructure, etc. Intuitively we know that, for example it is easier to eavesdrop on infrastructure-to-mobile communication than on mobile-to-mobile, but some sort of risk assessment associated with each communication scheme should provide us with an answer about the areas of highest threat level.

We will use qualitative threat characteristics: "low", "medium" and "high" based on the communication scheme's

physical characteristics. Figure 3 shows qualitative estimations of: range, power and radiation angle for each communication scheme. In regard to range, mobile-to-mobile range is considered "low" (~ 10 cm), "medium" (up to 1 m) applies to fixed-to-fixed and fixed-to-mobile, and all communications with infrastructure are considered to have "high" range (up to 3 m). Power is "low" for mobile devices, "medium" for fixed, and "high" when infrastructure is the sender. The radiation semi angle is typically 20 to 45 degrees for mobile and fixed devices; when infrastructure ambient lighting is used we consider the angle to be "high" (typically 60 degrees or more). Narrow radiation angles which may be achieved with laser or highly focused transmitter optics are not currently popular and will not be considered.

I	3	3	-
F	2	2	3
M	1	2	3
R/S	**M**	**F**	**I**

Range (R)

I	1	2	-
F	1	2	3
M	1	2	3
R/S	**M**	**F**	**I**

Power (P)

I	2	2	-
F	2	2	3
M	2	2	3
R/S	**M**	**F**	**I**

Radiation semi-angle (A)

Fig. 3. Qualitative classification of (R) data transmission range, (P) Power and (A) Radiation Angle for communication between: mobile, fixed and infrastructure devices. Senders are grouped by columns, receivers by rows.

We define the risks of jamming, snooping and data modification as follows:

Jamming: $J = R / P$ (1)

Snooping: $S = P * A$ (2)

Data modification: $M = J * S = R * A$ (3)

Jamming (1) is directly proportional to range – the longer the range, the easier to introduce a concealed transmitting device, this feature being inversely proportional to the transmission power. Snooping (2) is directly proportional to transmission power and the radiation angle – the wider and more powerful the transmission beam, the easier to oversee the communication. Data modification risk (3) is estimated as a product of the risks of jamming and snooping. The calculated risks are shown in figure 4.

IV. PHYSICAL LAYER SECURITY

The risk estimation results are consistent with intuition: the greatest risk of violating VLC security arises when communication with infrastructure is concerned. In the following sections of this paper we will focus on indoor infrastructure downlink communication security. We should therefore focus mainly on this aspect of communication.

Transmission snooping

The IEEE 802.15.7 standard states that "Because of directionality and visibility, if an unauthorized receiver is in the path of the communication signal, it can be recognized." However, this is not always true: when communication with the infrastructure is concerned both in the case of the NLOS channel and LOS, an unauthorized receiver may be easily introduced into the environment without being recognized.

Snooping on VLC transmission is of course limited by physical factors, and is more difficult than Wi-Fi snooping, but there is no obvious reason why it should not be possible. In [37]

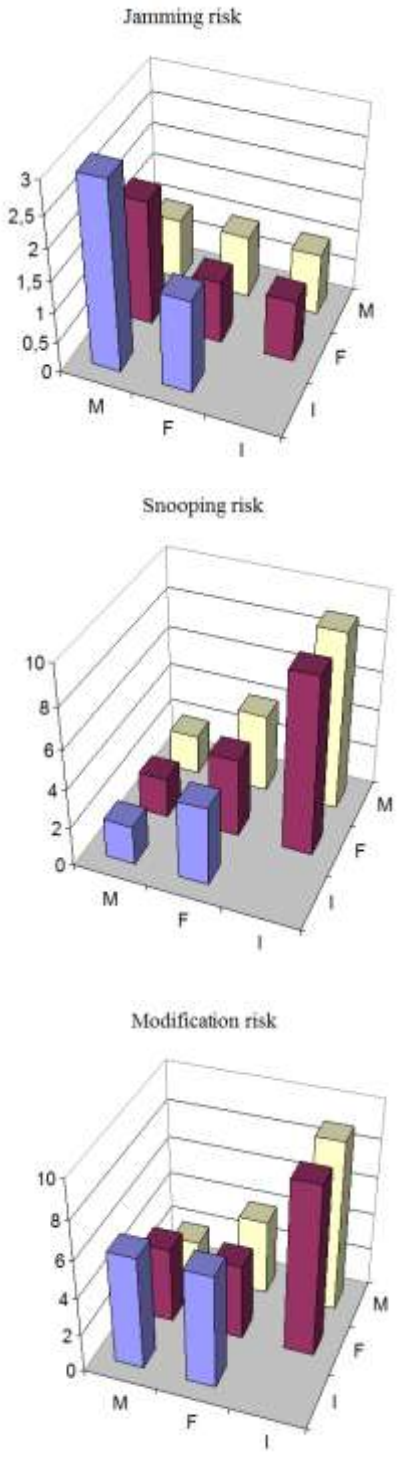

Fig. 4. Qualitative estimation of risk of: jamming, snooping and data modification of communication between: mobile (M), fixed (F) and infrastructure (I) devices. Sender are grouped by columns, receivers by rows.

it was shown experimentally that eavesdropping on VLC transmission is indeed possible. The equipment used based on a standard low-cost SDR design was able to achieve acceptable BER rates in a range of different scenarios. The authors evaluated different room configurations and were able to decode high-order modulated 64-QAM VLC signals outside of the room – via door-gaps, key holes and windows protected by special "privacy" coatings.

Transmission jamming and data modification

What are the possible schemes for introducing a signal jamming or data-modifying device into the VLC infrastructure channel? The attacker may choose to use both directed and non-directed light sources in the LOS or NLOS models, but due to power considerations a LOS model will be preferred. In general, the attacker's aim is to achieve a higher illumination at the receiver than that provided by the transmitter. One possible way of achieving this goal may be to use optical beamforming.

The major practical factor from the attacker's point of view is to ensure that the illumination provided by the rogue transmitter remains undetected by users. Hence, the attacker may use a highly directed transmitter. VLC infrastructure networks may consist of numerous independent transmitters to provide adequate coverage and capacity. Multi-transmitter "femtocell" VLC networks are also studied as an extension to traditional Wi-Fi and cellular networks – see [38]. In such environments the installation of a rogue transmitter may easily pass undetected. A second possibility is hijacking a part of the legitimate VLC infrastructure via wired or wireless channel; in a large installation such malicious intervention may also pass undetected.

Data modification in VLC networks may be attained by reactive jamming techniques. As was demonstrated in [39], real time reactive jamming is easily in reach of attackers with the use of SDR technology. In the above mentioned work, ZigBee (IEEE 802.15.4) protocol devices were used – it is worth noting the MAC-level similarities of ZigBee and the VLC 802.15.7 standard.

What are the possible schemes for introducing a signal jamming into the VLC infrastructure channel? The attacker may choose to use LOS or NLOS models, but due to power considerations a LOS model will be preferred. In general, the attacker's aim is to achieve a higher illumination at the receiver than that provided by the transmitter.

Let us consider this possibility in more detail. An optical communication link is modelled as a Poisson channel. The input to the Poisson channel is a non-negative waveform $\lambda(t)$. The output of the channel is an inhomogeneous Poisson process with intensity $\lambda(t) + \lambda_0$. The second term represents the additive Poisson noise of intensity λ_0.

In the MAC model introduced in [40] there are K independent inputs and one output. The channel output is a superposition of the outputs of K independent single-user Poisson channels. Hence, for inputs $\lambda_1(t); \lambda_2(t); \ldots \lambda_K(t)$ the output of the channel is an inhomogeneous Poisson process $\nu(t)$, with intensity:

$$\lambda(t) = \sum_{i=1}^{K} \lambda_i(t) \qquad (5)$$

In the general case of K transmitters, it was shown in [40] that the maximum total throughput of the Poisson MAC monotonically increases with the number of transmitters and is bounded from above (this is in contrast to the Gaussian MAC, where the maximum total throughput grows unbounded as the log of the number of transmitters). The Poisson MAC has a capacity achieving output which is a Poisson process with an intensity L equal to the sum of its K binary inputs. A Poisson process of intensity λ has the entropy rate $\lambda(1-\log(\lambda))$ bits/sec. – it does not monotonically increase with the input, and is concave with a peak at input intensity 1/e. Therefore, adding more inputs to a Poisson MAC eventually saturates the entropy rate (and hence the information content) of the output.

The consequences of the above, as far as signal jamming is concerned, are as follows: given the channel capacity limitation, a signal source with sufficient transmitting power will be able to saturate the channel obscuring the data source; the same result may also be obtained by a larger number of rogue low-power transmitters.

The major practical factor from the attacker's point of view is to ensure that the illumination provided by the rogue transmitter remains undetected by users. Hence, the attacker may use a highly directed transmitter. VLC infrastructure networks typically consist of numerous independent transmitters to provide adequate coverage and capacity. Multi-transmitter "femtocell" VLC networks are also studied as an extension to traditional Wi-Fi and cellular networks – see [38] In such environments the installation of a rogue transmitter may easily pass undetected. Another possible way of effective jamming may be to use optical beamforming. Similar to beamforming in WLAN optical beamforming may be attained by focusing light emitted from multiple LEDs. Optical beamforming in VLC was also demonstrated in practice with a solid-state spatial light modulator [41]. Limited amount of research was done towards optical beamforming, however it was demonstrated [42] that significant SNR improvements can be achieved by this means – hence it is also a viable jamming technique. A third possibility is hijacking a part of the legitimate VLC infrastructure via wired or wireless channel; in a large installation such malicious intervention may also pass undetected.

V. MAC Layer Security

What is the current state of security of the standardized VLC protocol? IEEE standard 802.15.7 defines the security mechanisms to be carried out by the MAC sublayer when requested by the higher protocol levels. The major assumption of the current IEEE standard is that data confidentiality and integrity should be provided by cryptographical means, but the implementation of these services should not be unnecessarily complicated and should not consume too many computational resources. This assumption aligns with the PAN (personal area networks) and BAN (body area networks) paradigm within which the computing resources may have significantly limited capabilities in terms of computing power, available storage, and power drain. However, VLC networks are also considered as a LAN technology (or at least as an LAN augmentation); hence the currently proposed security mechanisms may prove to be too weak.

The cryptographic mechanism of the IEEE 802.15.7 standard is based on symmetric-key cryptography and uses keys that are provided by higher layer processes. Cryptographic frame protection uses a key shared between two peer devices (link key)

or a key shared among a group of devices (group key), thus allowing some flexibility and application-specific trade-off between key storage and key maintenance costs versus the cryptographic protection provided. The standard defines 8 security levels:

- "None" (no encryption and no integrity),
- integrity-only provided by the MIC-32, MIC-64 and MIC-128 algorithms (three levels),
- encryption-only, and:
- encryption plus MIC (the three aforementioned variants).

Encryption uses the CCM* algorithm based on 128 bit AES in CBC-MAC mode. The optional key frame counter mechanism forces key initialization and prevents replay attacks. Frame encryption is provided for data, beacon payload and command payload. The standard itself does not define higher-level aspects of key generation, retrieval and management– these are explicitly identified as outside the standard's scope. This approach carries the following risks:

- As security services provided by integrity and encryption are optional, there is a large risk that in practical applications security will be turned off by default or not implemented at all,
- some of the MAC header fields are not encrypted, which may lead to attacks already known and described for Wi-Fi (802.11) networks,
- the standard does not define protection of the keying material or the distribution of keys (as, for example, 802.15.4 does)
- If a group key is used for peer-to-peer communication, protection is provided only against outsider devices and not against potential malicious devices in the key-sharing group.

VI. SUMMARY

VLC is one of the promising wireless communication technologies of the future, therefore improving its transmission security is highly desirable. Today, most of the research in VLC has focused on physical and MAC layer performance enhancements, while security remains in large yet to be addressed. In this paper, we have conducted a risk assessment of VLC communication with respect to the communicating parties of three basic classes: mobile, fixed and infrastructure. We have shown that particularly in case of infrastructure downlink communication security with respect to data snooping, communication jamming and data modification must be emphasized. Analyzing basic physical characteristics of the VLC communication channel we can came to the conclusion that signal jamming and modification is possible in real world VLC applications; while the MAC layer, as currently defined in IEEE 802.15.7 does not provide adequate protection against those risks. In future research we plan to examine such issues as: multi-user and multiple-eavesdropper scenarios, security with respect to user mobility and anti-jamming techniques.

REFERENCES

[1] M. Nakagawa, "Visible Light Communications," In Proc. Conference on Lasers and Electro-Optics/Quantum Electronics and Laser Science Conference and Photonic Applications Systems Technologies, Baltimore, 2007, DOI: 10.1109/CCNC.2012.6181092

[2] R, Kraemer and M. D. Katz, "Short-range wireless communications – Emerging technologies and applications," Wireless World Research Forum, John Wiley & Sons, 2009

[3] H. Elgala, R. Mesleh and H. Haas, "Indoor Optical Wireless Communication: Potential and State-of-the-Art," IEEE Communications Magazine, Volume: 49, Issue: 9, 2011, pp. 56-62.

[4] S. Hranilovic, L. Lampe and S. Hosur, "Visible light communications: the road to standardization and commercialization," In IEEE Communications Magazine, vol. 51, Iss. 12, ISSN: 0163-6804, 2013, pp. 24-54.

[5] A. Tsiatmas, C.P. A. Baggen, F.M. Willems, J.P. Linnartz and J.W. Bergmans, "An illumination perspective on visible light communications," In Communications Magazine, IEEE, 52.7, 2014, pp. 64-71.

[6] Samsung Electronics, ETRI, VLCC, University of Oxford, "Visible Light Communication: Tutorial," 2008, http://www.ieee802.org/802_tutorials/2008-03/15-08-0114-02-0000-VLC_Tutorial_MCO_Samsung-VLCC-Oxford_2008-03-17.pdf

[7] M. B. Rahaim, A.M. Vegni and T. D. Little, "A hybrid radio frequency and broadcast visible light communication system," in Proc. IEEE Global Communications Conference (GLOBECOM) Workshops, 2011, pp. 792–796.

[8] L.B. Chen, et al. "Development of a dual-mode visible light communications wireless digital conference system," In Consumer Electronics (ISCE 2014), The 18th IEEE International Symposium on, 2014, pp. 1-2.

[9] J. P. Javaudin, M. Bellec, D. Varoutas and V. Suraci, "OMEGA ICT Project: Towards Convergent Gigabit Home Networks," in Proc. International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Cannes, France, 2008

[10] K.D. Langer, et al., "Optical Wireless Communications for Broadband Access in Home Area Networks," In Proc. International Conference on Transparent Optical Networks, ICTON, 2008, pp. 149 - 154, DOI: 10.1109/ICTON.2008.4598756

[11] D.C. O'Brien, et al, "Home access networks using optical wireless transmission," In Proc. Personal, Indoor and Mobile Radio Communications, 2008, IEEE 19th International Symposium on, pp. 1-5, 2008

[12] D.C. O'Brien, et al, "Gigabit Optical Wireless for a Home Access Network," in Proc. IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, 2009, pp. 1-5.

[13] M. Yoshino, S. Haruyama and M. Nakagawa, "High-accuracy positioning system using visible LED lights and image sensor," Radio and Wireless Symposium, IEEE, vol., no., 2008, pp.439-442, 22-24.

[14] Z. X. Ren, H. M. Zhang, L. Wei and Y. Guan, "A High Precision Indoor Positioning System Based on VLC and Smart Handheld," in Applied Mechanics and Materials, Vol. 571, 2014, pp. 183-186.

[15] GBI Research, "Visible Light Communication (VLC) - A Potential Solution to the Global Wireless Spectrum Shortage," Tech. Rep. GBI Research, 2011,

[16] A. Cailean, et al. "Visible light communications: Application to cooperation between vehicles and road infrastructures," In Intelligent Vehicles Symposium (IV), IEEE 2012, pp. 1055-1059.

[17] N. Farr, A. Bowen and J. Ware, C. Pontbriand, M. Tivey, "An integrated, underwater optical/acoustic communications system," In Proc. OCEANS 2010, IEEE-Sydney, pp. 1-6.

[18] Home Gigabit Access (OMEGA) Project. [Online]. Available: http://www.ict-omega.eu/

[19] Q. Wang, D. Giustiniano and D. Puccinelli, D., "OpenVLC: Software-defined visible light embedded networks," In Proceedings of the 1st ACM MobiCom workshop on Visible light communication systems, September 2014, pp. 15-20

[20] J.P. Conti, "What you see is what you send," Engineering & Technology, 2008, pp. 66-67.

[21] IEEE, "IEEE standard for local and metropolitan area networks–part 15.7: Short-range wireless optical communication using visible light", IEEE Std 802.15.7-2011, https://standards.ieee.org/findstds/standard/802.15.7-2011.html

[22] D.C. O'Brien, L. Zeng, H. Le-Minh, G. Faulkner, J.W. Walewski and S. Randel, "Visible Light Communications: challenges and possibilities," in proc. International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE PIMRC), Cannes, France, 2008

[23] H. L. Minh, D. C. O Brien, G. Faulkner, L. Zeng, K. Lee, D. Jung, and Y. Oh, "High-speed visible light communications using multiple-resonantequalization," IEEE Photon. Technol. Lett., vol. 20, no. 4, pp. 1243–1245, Jul. 2008

[24] L. Zeng, H. L. Minh, D. C. O Brien, G. Faulkner, K. Lee, D. Jung, and Y. Oh, “Equalisation for high-speed visible light communications using white-leds,” in Proc. 6th Int. Symp. Commun. Syst., Netw. Digit. Signal Process., 2008, pp. 170–173.

[25] K. D. Langer, J. Vucic, C. Kottke, L. Fernandez, K. Habel, A. Paraskevopoulos, M. Wendl, and V. Markov, “Exploring the potentials of optical-wireless communication using white LEDs,” in Proc. 13th Int. Conf. Transp. Opt. Netw., Jun. 2011, pp. 1–5.

[26] A.H. Azhar, T. Tran and D. O'Brien, "A Gigabit/s Indoor Wireless Transmission Using MIMO-OFDM Visible-Light Communications", In IEEE Photonics Technology Letters, vol. 25, No. 2, 2013

[27] J. Kahn J. and J. Barry, "Wireless infrared communications," Proceedings of the IEEE, vol. 85, no. 2, 1997, pp. 265–298, DOI: 10.1109/5.554222

[28] A. D. Wyner, "The wire-tap channel," The Bell System Technical Journal, vol. 54, pp. 1355–1387, 1975.

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

[30] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," IEEE Transactions on Information Theory, vol. 56, no. 7, pp. 3088–3104, 2010.

[31] ——, "Secure transmission with multiple antennas—part II: The MIMOME wiretap channel," IEEE Transactions on Information Theory, vol. 56, no. 11, pp. 5515–5532, 2010.

[32] R. Negi and S. Goel, "Secret communication using artificial noise," in 2005 IEEE 62nd Vehicular Technology Conference, VTC-2005-Fall., vol. 3, 2005, pp. 1906–1910.

[33] A. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), April 2009, pp. 2437–2440.

[34] H. Le Minh, A. T. Pham, Z. Ghassemlooy and A. Burton, "Secured Communications-Zone Multiple Input Multiple Output Visible Light Communications," In Proc. Globecom Workshop - Optical Wireless Communications, 2014

[35] A. Mostafa and L. Lampe, "Physical-Layer Security for Indoor Visible Light Communications," In Proc. IEEE ICC 2014 - Optical Networks and Systems

[36] C.-W. Chow, "Secure communication zone for white-light LED visible light communication,", in Optics Communications 344, pp. 81–85; 2015

[37] J. Classen, J. Chen, J., D. Steinmetzer, M. Hollick, and E. Knightly, "The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications'" In *Proceedings of the 2nd ACM MobiCom Workshop on Visible Light Communication Systems, ser. VLCS* (Vol. 15), 2015

[38] K. Cui, J. Quan and Z. Xu, "Performance of indoor optical femtocell by visible light communication," Optics Communications, 2013, pp. 59-66.

[39] M. Wilhelm, I. Martinovic, J. B. Schmitt and V. Lenders, "Reactive jamming in wireless networks: how realistic is the threat?", In Proc. of the fourth ACM conference on Wireless network security, pp. 47-52, ACM, 2011

[40] A. Lapidoth and S. Shamai, "The Poisson multiple-access channel," Information Theory, IEEE Transactions on, 44(2), 1998, pp. 488-501.

[41] S.M. Kim and S. M. Kim, "Wireless visible light communication technology using optical beamformingm," in Optical Engineering, 52(10), 2013, pp. 106101-106101, DOI:10.1117/1.OE.52.10.106101

[42] L. Wu, Z. Zhang, and H. Liu, “Transmit Beamforming for MIMO Optical Wireless Communication Systems,” Wireless Personal Communications, vol. 78, no. 1, pp. 615–628, 2014. [Online]. Available: http://dx.doi.org/10.1007/s11277-014-1774-3