Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X
Vol.2 Issue 3 (2016) 38-47. Submitted 12/08/2016. Published 25/08/2016

Physical and MAC Layer Security Realistic Aspects in Perceptible Light Communication Systems

R.Venkadesh, M.Poovitha, W.Mesiya Stalin
Departement of Electronics and Communication Engineering
Dhanalakshmi Srinivasan Institute of Technology, Samayapuram, Tamil Nadu, India

Abstract—Visible light communication (VLC) has been recently proposed as an alternative standard to radio-based wireless networks. Originally developed as a bodily media for PANs (Personal location Networks) it developed into popular WLAN science with a capability to transport internet suite of community and software level protocols. Because of its bodily characteristics, and in line with the slogan "what you see is what you send", VLC is regarded a tightly closed communication method. In this work we focal point on safety components of VLC communication, beginning from primary bodily traits of the conversation channel. We analyze the dangers of signal jamming, statistics snooping and records modification. We also discuss MAC-level protection mechanisms as defined in the IEEE 802.15.7 standard. This paper is an extension of work at first mentioned in Proceedings of the thirteenth IFAC and IEEE Conference on Programmable Devices and Embedded Systems — PDES 2015.

Keywords—Wireless networks, visible mild communication, wireless community security, industrial wireless standards, IEEE 802.15.7

I. INTRODUCTION

Visible light communication (VLC) is a Wi-Fi optical verbal exchange technological know-how via which baseband indicators are modulated on the mild emitted by an LED: [1] – [5]. The lowering fee and for this reason speedy adaptation of LED based mild make VLC a promising communication method and a considerable alternative to radio-based wireless communication. Wi-Fi, Bluetooth, etc. - the “traditional” radio based totally communication systems go through from constrained channel capability and transmission charge due to the restricted radio spectrum available. At the identical time the consumer request for records transmission throughput and availability continues to increase. VLC statistics transmission networks provide an pleasing choice to standard wireless techniques. Notable differences making VLC systems extra captivating than radio-based networks are:

VLC systems are interface-orthogonal to cellular, Wi-Fi, Bluetooth and different radio-frequency primarily based networks,

- light does not penetrate strong objects,
- light can be without difficulty directed via optics,
- Most indoor, and a full-size share of outdoor, environments are illuminated.

VLC was once proposed each for in-door and out-door functions – see [6] and [3]. In-door applications consist of a This work was once supported by means of the Statutory Grant of the Polish Ministry of Science and Higher Education to the Institute of Computer Science, Warsaw University of Technology. Indoor VLC purposes range from: workplace conversation – [7], multimedia conferencing – [8], peer-to-peer records exchange, facts broadcasting – in particular multimedia such as home-audio and video streams, see: [9] – [12], to positioning: [13] – [14]. Currently handy business VLC systems focal point broadly speaking on facts broadcasting, and encompass options for museums, buying centers, exhibition centers, airports and teach stations as properly as accessibility for disabled persons. VLC based positioning systems, for instance "smart carts" that guide the clients to the cabinets according to their list of products are already available. VLC systems additionally supply a secure alternative to electromagnetic interference from radio frequency communications in hazardous environments, such as mines and petrochemical plants, and in functions where common WLAN conversation can also intrude with specialized equipment, for instance in hospitals and in plane passenger cabins' in-flight entertainment systems (where the extra advantage is the reduced weight of cabling and the doable for integration with passengers' very own mobile devices) [15].

The most promising outside purposes of VLC technological know-how are advertising (via LED signboards), pedestrian guidance (via indicator boards), and avenue security and site visitors management, see [6]. VLC-based positioning and navigation grant a attainable alternative to GPS in environments where the GPS sign is vulnerable or non-existent. As LED headlights and rear lights in commercially handy motors are being introduced, avenue lamps, signage and traffic signals are also shifting to LED technology, and VLC primarily based vehicle-to-vehicle ("VANETs" – Vehicle Area Networks) and vehicle-to roadside communications have end up a actuality – [16]. VLC additionally gives a possible solution for short-range communications underwater where, due to robust sign absorption, RF use is impractical – [17]. In this work we will center of attention only on in-door applications.

Recently VLC is starting to be regarded as a way of augmenting or event changing RF networks, for instance home Gigabit Access challenge (OMEGA) [18], backed through European Union developed a broad vary of methods aimed at VLC based totally multimedia networks. The usage of Smartphone cameras and mild sensors brings VLC to the field of cellular computing and sensing. In this way VLC has a manageable to evolve into a usual WLAN fashionable – in [19] with the Open VLC platform the authors have tested that with present day Software Defined Radio (SDR) toolkits it is distinctly easy to convey TCP/IP suite to the VLC medium. One of the aspects in which VLC methods are regarded most fulfilling to typical radio-based conversation is security. The directivity, and high obstacle impermeability of optical alerts are regarded to supply a secure way to transmit information inside an indoor environment, making the records challenging to intercept from outside. The common slogan summarizing VLC security features is: "What You See Is What You Send" (WYSIWYS) [20].

As recent records teach us, a frequent mistake in the improvement of novel communications strategies was once to neglect or downplay the protection issues. Such was once the case with the net protocol suite - both on the network and, software layer), a number of encryption and authentication algorithms and protocols, fiber-optics based networks, and more these days – radio-based wireless networks. Currently the VLC industry looks to be on the equal path again:

the indubitable "pro-security" bodily characteristics of visual mild conversation have recommended the developers' focal point away from the safety track.

In this paper we tackle security of VLC communications, both from the channel (i.e. records theory) and higher degree (MAC) perspective. As a ways as VLC requirements are concerned, we will refer to the IEEE Standard 802.15.7 [21]; however, our dialogue must additionally be applicable to other proposed VLC methods not covered by means of the present day IEEE norm.

The shape of this paper is as follows: in section II we will describe the groundwork of VLC technological know-how – the mechanisms of VLC bodily layer. In section III we will discuss how safety issues should be approached in this verbal exchange media; we will also analyze which factors of VLC have to be put into the focus of safety research. In sections IV and V we will talk about (respectively) the security of the bodily and MAC degrees of VLC networks. Section VI summarizes the paper and outlines the areas of future research.

II. THE VLC DATE LINK– AN OVERVIEW

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

Transmitter – Two sorts 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 ("singlechip"). The VLC transmitter can also use both types, however the 2d kind is greater giant in illumination due to its power affectivity and lower complexity. Different sorts and form elements of LED are employed in a number of environments: high energy LEDs or LED arrays are the choice for ordinary indoor illumination purposes, whilst low-power units are used in smart-phones and other mobile appliances. The slow response of yellow phosphorus to blue mild modulation limits its spectral component bandwidth to 2MHz, consequently the yellow issue is filtered- out at the receiver and solely the blue aspect is detected, bandwidth of 8 MHz might also be attained with this simple filtering approach [22]. With easy analogue pre-equalization at the transmitter side forty Mb/s throughputs may be attained except the use of a blue filter [23]. By combining a easy pre- and post-equalization, 75 Mb/s can be accomplished [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 statistics quotes of about 1 Gb/s are additionally plausible with more superior modulation methods such as DMT and OFDM. Similar records costs were also attained with arrays of one at a time pushed 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 units such as smart phones, tablets, etc., low fee photodiodes or usual optical sensors are used as photograph detectors for the VLC channel. With cutting-edge science achieving adequate photo detector sensitivity, the required bandwidth is now not a trouble (the transmitter and channel loss and dispersion are the essential bandwidth limiting factors). It ought to be cited that as picture detectors work in an Intensity Modulation/Direct Detection (IM/DD) regime, they produce a sign proportional to the intensity (not the amplitude) of the incident wave: the detector works as a squarer.

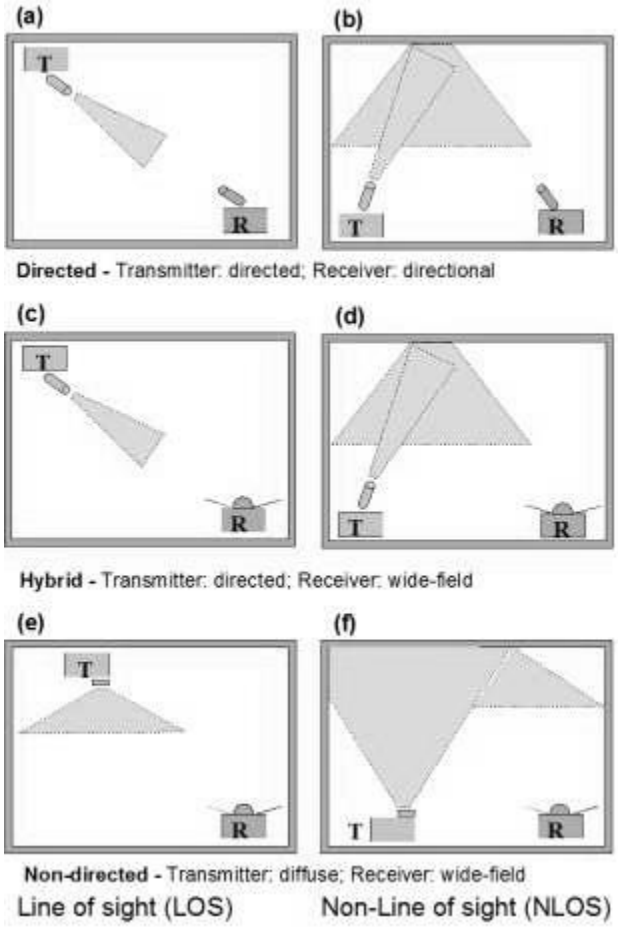

Fig. 1. Classification of links according to LOS/NLOS (line-of-sight) and directionality of transmitter and receiver.

III. SECURITY IN VARIOUS ASPECTS OF VLC COMMUNICATION

Security of VLC dialog up to date has been principally tackled with appreciates to the bodily layer. The questioning of physical-layer safety used to be introduced via Wyner in his paper on the degraded discrete memory much less wiretap channel [28]. Secrecy functionality was once described as the most price of dependable sender-receiver transmission while the communication is without a doubt challenging to recognize to the eavesdropper. A single-letter characterization of the secrecy plausible of non-degraded, wiretap channel used to be formulated in [29], while the secrecy functionality of the Gaussian multiple-input, single-output (MISO) and multiple-input, multiple-output (MIMO) wiretap channel was once resolved in [30] and [31], respectively. It used to be shown that in case of a Gaussian MISO wiretap channel the utilization of zero-forcing by means of the use of beam forming the eavesdropper's reception is most reliable at asymptotic immoderate Signal to Noise Ratio (SNR). When the channel kingdom data for the eavesdropper is no longer handy synthetic noise (a jamming signal) delivered to the transmitted records sign consequences in an make greater of achievable secrecy prices - [32] and [33]. In [34] a MIMO method to placing up a tightly closed conversation sector has been described – the authors proposed to use MIMO method and beam forming (similar to RF Wi-Fi networks) to set

up a tightly closed channel between the transmitter the receiver positioned in a special bodily location. BER (Bit Error Rate) is minimized at the receiver's location, at the same time as it remains unacceptably excessive in the relaxation of the area. In this way, a feasible eavesdropper bodily positioned some distance from the reputable receiver is unable to suited decode the data. This is attained without vast influence on the lighting fixtures traits and is therefore unobservable to the users. A similar approach was proposed in [35] the usage of MISO (Multiple Input Single Output) techniques, together with null-steering and synthetic noise - an conceivable secrecy fee was once calculated numerically. A similar method was once additionally proposed and in area validated in the real surroundings in [36]. We will return to channel-level protection troubles with respect to the opportunity of sign jamming in part IV. For the cause of this work, we will assume about three training of VLC devices: infrastructure, steady and mobile. Their characteristics are summarized in Table 1. As described in IEEE 802.15.7 - three major MAC topologies are supported by means of way of VLC: peer-to-peer, superstar and broadcast. The first is frequently used between two handheld devices such as smart phones; superstar topology is used as a choice for Wi-Fi networks; and broadcast is used in multimedia applications, advertising and marketing applications, and vehicular networks. Indoor VLC modes are summarized in discern 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)

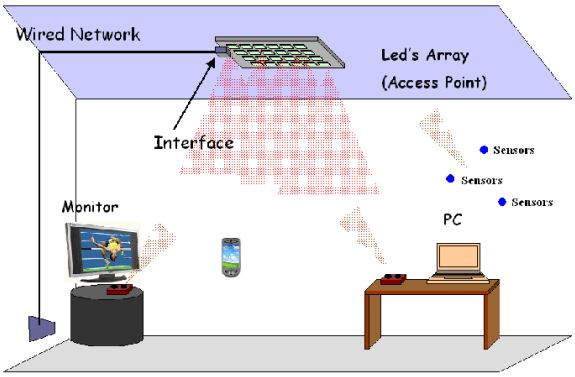

Fig. 2. Indoor VLC modes

We will consider four important elements of VLC conversation security, namely: availability, confidentiality, authenticity, and integrity with understand to infrastructure, constant and mobile classes of VLC devices. The threats that we assume about are the probabilities of jamming, snooping and documents modification. Each threat has to be regarded one by one for all conversation schemes, i.e. mobile-to-mobile, infrastructure to- mobile, mobile-to-infrastructure, etc. Intuitively we be conscious of that for example, it is much less intricate to eavesdrop on infrastructure-automobile conversation than on mobile-to-mobile, however some sort of hazard assessment associated with each conversation scheme have to grant us with an answer about the areas of absolute quality hazard level. We will use qualitative hazard characteristics: “low”, “medium” and “high” particularly primarily based on the communication scheme’s bodily characteristics. Figure three suggests the qualitative estimations of range, power, and radiation angle for every communication scheme. In regard to range, the mobile-to-mobile range is seen "low" (~ 10 cm), "medium" (up to 1 m) applies to fixed-to-fixed and fixed-to-mobile, and all communications with infrastructure are viewed to have "high" differ (up to three m). Power is "low" for cell devices, "medium" for constant and "high" when infrastructure is the sender. The radiation semi-angle is typically 20 to forty five stages for cell and fixed devices; when infrastructure ambient lighting fixtures is used we replicate on consideration on the viewpoint to be "high" (typically 60 levels or more). Narrow radiation angles which may also be performed with laser or distinctly centered transmitter optics are now not nowadays well-known 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 outline the risks of jamming, snooping and records change as follows:

Jamming: J = R / P (1)

Snooping: S = P * A (2)

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

Jamming (1) is at as soon as proportional to fluctuate – the longer the range, the less tough to introduce a hid transmitting device, this characteristic being inversely proportional to the transmission power. Snooping (2) is except extend proportional to transmission strength and the radiation standpoint – the wider and higher powerful the transmission beam, the less complicated to oversee the communication. Data change danger (3) is estimated as a product of the risks of jamming and snooping. The calculated risks are proven in figure 4.

IV. PHYSICAL LAYER SECURITY

The risk estimation results are ordinary with intuition: the biggest risk of violating VLC security arises when verbal exchange with infrastructure is concerned. In the following sections of this paper, we will focal factor on indoor infrastructure downlink communication security. We should, therefore, focal factor generally on this thing of communication.

Transmission snooping

The IEEE 802.15.7 sizable states that "Because of directionality and visibility, if an unauthorized receiver is in the course of the verbal trade signal, it can be recognized." However, this is no longer normally true: when verbal change with the infrastructure is worried every in the case of the NLOS channel and LOS, an unauthorized receiver can additionally be without problems brought into the environment except being recognized. Snooping on VLC transmission is, of course, restrained by means of bodily factors, and is greater challenging than Wi-Fi snooping, on the other hand there is no apparent reason why it ought to now not be possible. In [37] it used to be once shown experimentally that eavesdropping on VLC transmission is surely possible. The equipment used specifically based on a well-known low-priced SDR graph was once successful to reap perfect BER costs in a vary of one of a kind scenarios. The authors evaluated special room configurations and had been in a position to decode high-order modulated 64-QAM VLC indicators backyard of the room – with the useful resource of door-gaps, key holes and windows covered thru distinct “privacy” coatings.

VI. SUMMARY

VLC is one of the promising wireless verbal change technologies of the future, as a result enhancing its transmission protection is especially desirable. Today, most of the lookup in VLC has focused on physical and MAC layer performance enhancements, even as security stays in large however to be addressed. In this paper, we have carried out a threat evaluation of VLC verbal exchange with admire to the speaking occasions of three critical classes: mobile, constant and infrastructure. We have validated that specifically in the case of infrastructure downlink

conversation security with admire to data snooping, dialog jamming and statistics change should be emphasized. Analyzing predominant bodily characteristics of the VLC conversation channel we can come to the conclusion that sign jamming and exchange is viable in actual world VLC applications; even as the MAC layer, as currently described in IEEE 802.15.7 does no longer furnish enough protection closer to those risks. In future research, we design to take a appear at such troubles as multi-user and more than one eavesdroppers' scenarios, protection with recognize to client mobility and anti-jamming techniques.

REFERENCES

[1] Blinowski, Grzegorz J. "Practical aspects of physical and MAC layer security in visible light communication systems." International Journal of Electronics and Telecommunications 62.1 (2016): 7-13.
[2] Kraemer, Rolf, and Marcos Katz, eds. Short-range wireless communications: Emerging technologies and applications. John Wiley & Sons, 2009.
[3] Elgala, Hany, Raed Mesleh, and Harald Haas. "Indoor optical wireless communication: potential and state-of-the-art." IEEE Communications Magazine 49.9 (2011).
[4] Hranilovic, Steve, Lutz Lampe, and Srinath Hosur. "Visible light communications: the road to standardization and commercialization (Part 1)[Guest Editorial]." IEEE Communications Magazine 51.12 (2013): 24-25.
[5] Blinowski, Grzegorz J. "Practical aspects of physical and MAC layer security in visible light communication systems." International Journal of Electronics and Telecommunications 62.1 (2016): 7-13.
[6] Blinowski, Grzegorz. "Security issues in visible light communication systems." IFAC-PapersOnLine 48.4 (2015): 234-239.
[7] Rahaim, Michael B., Anna Maria Vegni, and Thomas DC Little. "A hybrid radio frequency and broadcast visible light communication system." GLOBECOM Workshops (GC Wkshps), 2011 IEEE. IEEE, 2011.
[8] Chen, Liang-Bi, et al. "Development of a dual-mode visible light communications wireless digital conference system." Consumer electronics (ISCE 2014), The 18th IEEE international symposium on. IEEE, 2014.
[9] Javaudin, Jean-Philippe, et al. "OMEGA ICT project: Towards convergent Gigabit home networks." Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on. IEEE, 2008.
[10] Langer, Klaus-Dieter, et al. "Optical wireless communications for broadband access in home area networks." Transparent Optical Networks, 2008. ICTon 2008. 10th Anniversary International Conference on. Vol. 4. IEEE, 2008.
[11] O'Brien, Dominic C., et al. "Home access networks using optical wireless transmission." Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on. IEEE, 2008.
[12] O'Brien, Dominic C., et al. "Gigabit optical wireless for a home access network." Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on. IEEE, 2009.
[13] Yoshino, Masaki, Shinichiro Haruyama, and Masao Nakagawa. "High-accuracy positioning system using visible LED lights and image sensor." Radio and Wireless Symposium, 2008 IEEE. IEEE, 2008.

[14] Ren, Zhe Xin, et al. "A high precision indoor positioning system based on VLC and smart handheld." Applied mechanics and materials. Vol. 571. Trans Tech Publications, 2014.
[15] Burchardt, Harald, et al. "VLC: Beyond point-to-point communication." IEEE Communications Magazine 52.7 (2014): 98-105.
[16] Arnon, Shlomi, ed. Visible light communication. Cambridge University Press, 2015.
[17] Farr, N., et al. "An integrated, underwater optical/acoustic communications system." OCEANS 2010 IEEE-Sydney. IEEE, 2010.
[18] Dede, Georgia, et al. "Evaluation of technological and socio-economic issues affecting the deployment of home networks: evidence from the ICT-OMEGA project." NETNOMICS: Economic Research and Electronic Networking 11.2 (2010): 181-200.
[19] Wang, Qing, Domenico Giustiniano, and Daniele Puccinelli. "OpenVLC: software-defined visible light embedded networks." Proceedings of the 1st ACM MobiCom workshop on Visible light communication systems. ACM, 2014.
[20] Conti, Juan Pablo. "What you see is what you send-[comms visible light]." Engineering & Technology 3.19 (2008): 66-69.
[21] Blinowski, Grzegorz J. "Practical aspects of physical and MAC layer security in visible light communication systems." International Journal of Electronics and Telecommunications 62.1 (2016): 7-13.
[22] O'Brien, Dominic C., et al. "Visible light communications: Challenges and possibilities." Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on. IEEE, 2008.
[23] Le Minh, Hoa, et al. "High-speed visible light communications using multiple-resonant equalization." IEEE Photonics Technology Letters 20.14 (2008): 1243-1245.
[24] Zeng, Lubin, et al. "Equalisation for high-speed visible light communications using white-leds." Communication Systems, Networks and Digital Signal Processing, 2008. CNSDSP 2008. 6th International Symposium on. IEEE, 2008.
[25] Blinowski, Grzegorz J. "Practical aspects of physical and MAC layer security in visible light communication systems." International Journal of Electronics and Telecommunications 62.1 (2016): 7-13.
[26] Azhar, Ahmad Helmi, Thomas Tran, and Dominic O'Brien. "A gigabit/s indoor wireless transmission using MIMO-OFDM visible-light communications." IEEE photonics technology letters 25.2 (2013): 171-174.
[27] Kahn, Joseph M., and John R. Barry. "Wireless infrared communications." Proceedings of the IEEE 85.2 (1997): 265-298.
[28] Wyner, Aaron D. "The wire-tap channel." Bell system technical journal 54.8 (1975): 1355-1387.
[29] Csiszár, Imre, and Janos Korner. "Broadcast channels with confidential messages." IEEE transactions on information theory 24.3 (1978): 339-348.
[30] Khisti, Ashish, and Gregory W. Wornell. "Secure transmission with multiple antennas I: The MISOME wiretap channel." IEEE Transactions on Information Theory 56.7 (2010): 3088-3104.
[31] Khisti, Ashish, and Gregory Wornell. "Secure transmission with multiple antennas II: The MIMOME wiretap channel." arXiv preprint arXiv:1006.5879 (2010).
[32] Negi, Rohit, and Satashu Goel. "Secret communication using artificial noise." IEEE Vehicular Technology Conference. Vol. 62. No. 3. IEEE; 1999, 2005.

[33] Swindlehurst, A. Lee. "Fixed SINR solutions for the MIMO wiretap channel." Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on. IEEE, 2009.
[34] Le Minh, Hoa, et al. "Secured communications-zone multiple input multiple output visible light communications." Globecom Workshops (GC Wkshps), 2014. IEEE, 2014.
[35] Mostafa, Ayman, and Lutz Lampe. "Physical-layer security for indoor visible light communications." Communications (ICC), 2014 IEEE International Conference on. IEEE, 2014.
[36] Chow, Chi-Wai, et al. "Secure communication zone for white-light LED visible light communication." Optics Communications 344 (2015): 81-85.
[37] Classen, Jiska, et al. "The spy next door: Eavesdropping on high throughput visible light communications." Proceedings of the 2nd International Workshop on Visible Light Communications Systems. ACM, 2015.