Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 48-4 (2015) 234–239

Security issues in visible light communication systems

Grzegorz Blinowski*

** Institute of Computer Science, Warsaw University of Technology, Nowowiejska 15/19, 00-665 Warszawa; Poland (Tel: 0048222347184; e-mail: g.blinowski@ii.pw.edu.pl).*

Abstract: Visible light communication (VLC) has been recently proposed as an alternative standard to radio-based wireless networks. 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 modification. We also discuss MAC-level security mechanisms as defined in the IEEE 802.15.7 standard.

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

1. INTRODUCTION

Solid-state lighting is a rapidly developing field. White-light (and tri-color) LEDs are more energy efficient, and have better reliability than traditional incandescent and fluorescent light sources. Visible light communication (VLC) is a wireless optical communication technology through which baseband signals are modulated on the light emitted by an LED - Nakagawa (2007), Kraemer (2009), Elgala (2011), Hranilovic (2013), Tsiatmas (2014). 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 such as Wi-Fi, Bluetooth and others. An important adoption factor in favor of VLC is the increasing "pollution" of the radio spectrum. Radio wireless devices, ranging from IEEE 802.3 (Wi-Fi) compatible equipment, PAN (personal area network) devices, to child monitors, generate interference and clog up the available spectrum. VLC data transmission networks (sometimes referred to as "Li-Fi") provide an attractive alternative to traditional wireless techniques, since:

- they 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.

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 transmit data within a closed 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 (Conti (2008)).

Since history likes to repeat itself - 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), 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 directed the developers' focus away from security issues.

In this paper we address the classic security triad of: confidentiality, authenticity and integrity in VLC communications. As far as VLC standards are concerned, we will refer to the IEEE Standard 802.15.7 (IEEE (2011)); 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 the remaining part of this section we will discuss the VLC channel structure and properties, as well as most important practical applications of VLC. In section 2 we discuss security risk in various aspects of in-door VLC communication. In section 3 we further analyze security risks at the physical and MAC layer - especially with respect to IEEE 802.15.7 standard. The work is summarized in section 4.

1.1 The VLC Data-Link

A VLC data-link consists of: the transmitter, the propagation channel and the receiver. Their properties are as follows:

Transmitter – There are two types of white-light LEDs 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 popular in illumination due to its energy efficiency and lower complexity (when compared to RGB

10.1016/j.ifacol.2015.07.039

emitters). 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. Single-chip LEDs driven by a single modulation source achieve a bandwidth of approx. 2.5 MHz for the white and 14 MHz for the blue component (O'Brien (2008a)) (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). Data throughput of up to 40 Mb/s has been demonstrated in a single-emitter–single-receiver scenario – Grubor (2007). With techniques such as simple analogue equalization on the receiving side, a transfer rate of 100 Mb/s was achieved (Le Minh (2008)). High data rates exceeding 100 Mb/s are also attainable with multiple-subcarrier modulation techniques such as OFDM. With arrays of separately driven light sources and OFDM, a data throughput of up to 1Gbit/s was demonstrated, techniques similar to radio frequency MIMO are used in such a case – see Helmi (2013).

The receiver collects and concentrates the incoming light on a photo-detecting element. Both imaging and non-imaging receivers may be used. Generated photocurrent is amplified and fed to the D/A circuitry. 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). Currently in devices such as smartphones, tablets, etc., low cost photodiodes or typical optical sensors are used as photodetectors for the VLC channel. As these devices work in an Intensity Modulation/Direct Detection (IM/DD) regime, the photodetector produces a signal proportional to the intensity (not the amplitude) of the incident wave: the detector works as a squarer.

The propagation channel in the case of indoor environments communication may be characterized by six different link configurations, as originally defined by Kahn and Barry (1997) 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 the 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.

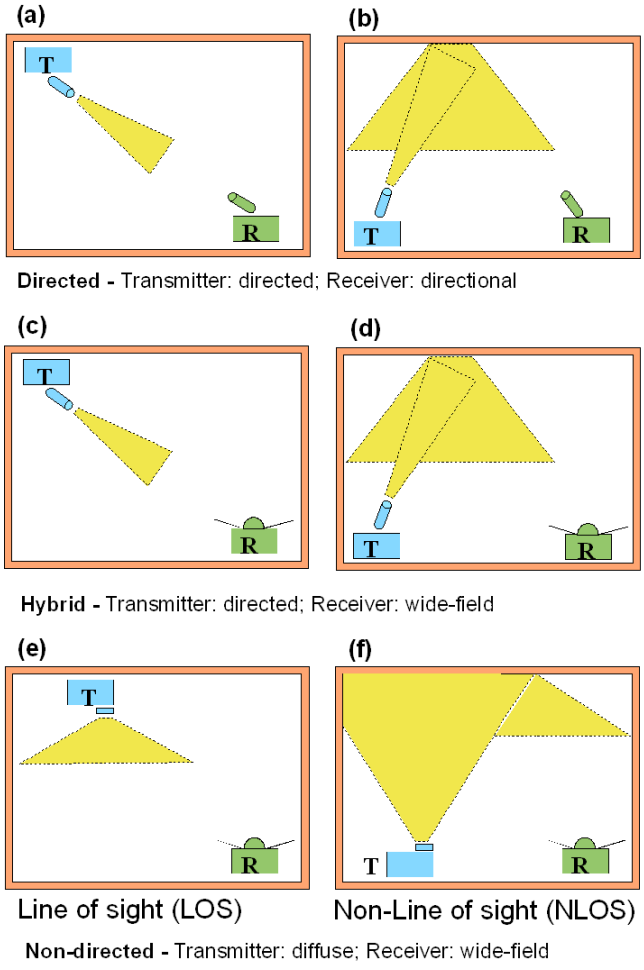

Fig 1. Classification of links according to LOS/NLOS (line-of-sight) and directionality of transmitter and receiver.

1.2 Applications of VLC

VLC was proposed both for in-door and out-door applications – see Samsung (2008) and Elgala (2011). 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 – Rahaim (2011), multimedia conferencing – Chen (2014), peer-to-peer data exchange, data broadcasting – especially multimedia such as home-audio and video streams, see Javaudin (2008), Langer (2008), O'Brien (2008b, 2009) to positioning – Yoshino (2008), Ren (2014) Because of their physical characteristics, VLC systems permit very close spacing between nodes, providing higher data density which results in increased network capacity.

Currently available commercial 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 "smartcarts" 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) – GBI Research (2011).

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 Samsung Electronics 2008. 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 BLC based vehicle-to-vehicle ("VANETs" – Vehicle Area Networks) and vehicle-to-roadside communications have become a reality – Cailean 2012 VLC also provides a viable solution for short-range communications underwater where, due to strong signal absorption, RF use is impractical – Farr (2010). In this work we will focus only on in-door applications.

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.

Table 1 – 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
Formfactor	Unconstrained	Constrained	Critically-constrained
Light source	Intense	Weak – moderate	Weak
Mobility	No	No	Yes
Source	High	moderate	moderate
dispersion	(ambient)		
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)

Indoor VLC modes are sumarized on figure 2.

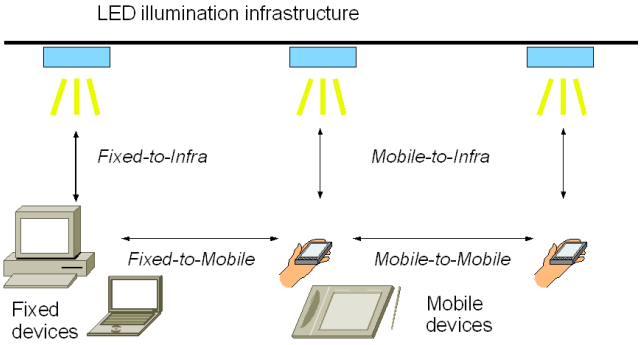

Fig 2. Indoor VLC modes

2. SECURITY IN VARIOUS ASPECTS OF VLC COMMUNICATION

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 30 to 60 degrees for mobile and fixed devices; when infrastructure ambient lighting is used we consider the angle to be "high". (Narrow radiation angles which may be achieved with laser or highly focused transmitter optics are not currently popular.)

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
	M	**F**	**I**

Power (P)

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

Radiation 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: $S = P \cdot A$ (2)

Data modification: $M = J \cdot S = R \cdot A$ (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.

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

Jamming J

I	2	4	-
F	2	4	9
M	2	4	9
	M	**F**	**I**

Snooping S

I	6	6	-
F	4	4	9
M	2	4	9
	M	**F**	**I**

Modification M

Fig. 4 - Qalitative estimation of risk of: jamming, snooping nad data modification of communication between: mobile, fixed and infrastructure devices. Sender are grouped by columns, receivers by rows.

3. PHYSICAL AND MAC LAYER SECURITY

The risk estimation results are consistent with our intuition: the greatest risk of violating VLC security arises when communication with infrastructure is concerned. We should therefore focus mainly on this aspect of communication. 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*." Clearly, however, this is not always true: in the case of the NLOS channel and LOS communication with the infrastructure, 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, especially in the case of communication with infrastructure.

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. Optical beamforming in a VLC system was demonstrated in practice with a solid-state spatial light modulator (Kim (2013)).

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 Cui, Quan and Xu (2013). 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 by Wilhelm (2011), real time reactive jamming is easily in reach of attackers with the use of software defined radio (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.

3.1 Security at the physical level

What are the security aspects of VLC in terms of the communication channel? 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.

From our perspective the multi-access Poisson channel model introduced by Lapidoth and Shamai (1998) is of interest. In the MAC model 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 $\lambda_1(t)$; $\lambda_2(t)$; ... $\lambda_K(t)$ the output of the channel is an inhomogeneous Poisson process ν(t), with intensity:

$$\lambda(t) = \sum_{i=1}^{K} \lambda_i(t) \quad (4)$$

In the general case of *K* users, it was shown by Lapidoth and Shamai (1998) that the maximum total throughput of the Poisson MAC monotonically increases with the number of users 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 users. 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 and modifying are 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.

3.2 Security at the MAC level

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 reinitialization 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.

4. CONCLUSIONS

Security aspects of VLC have so far attracted little attention. Current research in this field is mainly focused on achieving higher transmission rates (novel modulation schemes, MIMO, etc.). In our opinion, as was the case with other wireless network technologies, VLC is also not free from its own security issues. VLC infrastructure is particularly prone to data-security risks. The current IEEE standard 802.15.7 does not provide adequate MAC-level protection against physical level risks. Further research is needed to analyze and improve current VLC technologies as far as channel-level security is concerned.

REFERENCES

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

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

Conti, J.P. (2008). What you see is what you send, *Engineering & Technology*, pp 66-67.

Cui, K., Quan, J., & Xu, Z. (2013). Performance of indoor optical femtocell by visible light communication. *Optics Communications,* 298, pp. 59-66.

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

Farr, N., et al. (2010). An integrated, underwater optical/acoustic communications system. *OCEANS 2010*, IEEE-Sydney, pp. 1-6.

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

Grubor, J., et al. (2007). Wireless high-speed data transmission with phosphorescent white-light LEDs,. *Proc. Eur. Conf. Optical Communications (ECOC 2007)*, Berlin, Germany.

Helmi, A., et al. (2013). A Gigabit/s Indoor Wireless Transmission Using MIMO-OFDM Visible-Light Communications, *IEEE Photonics Technology Letters*, VOL. 25, NO. 2.

Hranilovic, S., Lampe, L. Hosur, S. (2013) Visible light communications: the road to standardization and commercialization. *IEEE Communications Magazine*, Volume:51, Issue: 12, ISSN: 0163-6804, pp. 24-54.

IEEE. (2011) 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*.

Javaudin, J.-P., et al. (2008) OMEGA ICT Project: Towards Convergent Gigabit Home Networks. *International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008)*. Cannes, France.

Kahn J., Barry, J. (1997) Wireless infrared communications. *Proceedings of the IEEE*, vol. 85, no. 2, pp. 265–298.

Kim, S. M., & Kim, S. M. (2013) Wireless visible light communication technology using optical beamforming. *Optical Engineering*, 52(10), pp. 106101-106101.

Kraemer, R., Katz, M. D. (2009) Short-range wireless communications – Emerging technologies and applications. Wireless World Research Forum. Hoboken, NJ: Wiley.

Langer, K.-D., et al. (2008) Optical Wireless Communications for Broadband Access in Home Area Networks. *Proc. International Conference on Transparent Optical Networks, ICTON*, pp. 149 - 154.

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

Le Minh, H., et al. (2009), 100-Mb/s NRZ Visible Light Communications Using a Postequalized White LED. *IEEE Photonics Technology Letters*, vol. 21, no. 15.

Nakagawa, M. (2007) Visible Light Communications. Proc. *Conference on Lasers and Electro- Optics/Quantum Electronics and Laser Science Conference and Photonic Applications Systems Technologies.*

O'Brien, D., et al. (2008) Visible Light Communications: challenges and possibilities, *International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2008)*. Cannes, France.

O'Brien, D., et al. (2008) Home access networks using optical wireless transmission. *Proc. PIMRC.*

O'Brien, D., et al. (2009) Gigabit Optical Wireless for a Home Access Network. *IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1-5.

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

Ren, Z. X., et al. (2014) A High Precision Indoor Positioning System Based on VLC and Smart Handheld. *Applied Mechanics and Materials*, Vol. 571, pp. 183-186.

Tsiatmas, A., et al. (2014). An illumination perspective on visible light communications. *Communications Magazine, IEEE,* 52.7. pp. 64-71.

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

Wilhelm, M., et al. (2011). Short paper: reactive jamming in wireless networks: how realistic is the threat? *Proceedings of the fourth ACM conference on Wireless network security* (pp. 47-52). ACM.

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