ANALYSIS OF DATA TRANSMISSION METHODS USING VISIBLE LIGHT FOR INFORMATION SECURITY

Shvyrev B.A. PhD. (Phys.-Math.)[1], PhD student Timonov D.A.[1]
Kuban State University of Technology, Krasnodar, the Russian Federation [1]
bor2275@yandex.ru, dmitrii-timonov@bk.ru

Abstract: *We consider modern methods of transmitting messages by means of modulating the intensity of the flux of visible light from LEDs. The structure of data transmission and existing standards are analyzed. The possibility of using technology to organize a channel of information leakage has been determined. Discusses methods for countering information leakage by modulating the intensity of the light output of LEDs.*

Keywords: LI-FI, VLC, MODULATION OF VISIBLE LIGHT, LED, INFORMATION LEAKAGE CHANNEL.

1. Introduction

Room lighting can be used to organize data transmission. This method of transmitting information can be used to form information leakage channels by means of modulating the visible light produced by the LEDs. This leakage channel allows you to transfer information from physically isolated from the communication lines of computing systems.

The transmission of information on the means of modulation of visible light has been known since 2011, when Professor Haar introduced the concept of Li-Fi [1,2]. This type of data transfer uses the transmission of information on the means of controlling the LEDs of lighting devices (chandeliers, lamps, etc., Figure 1).

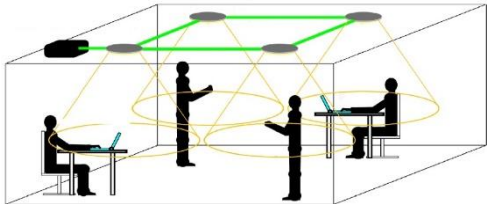

Fig. 1. *The organization of communication systems using visible light*

The data transmission network based on this modulation of visible light is called Visible Light Communication (VLC) and is a new and promising communication method due to its high bandwidth and immunity to interference from electromagnetic sources [3-6]. The revolution in solid-state lighting leads to the replacement of fluorescent lamps with light-emitting diodes (LEDs), which further stimulates the use of VLC. Consider potential capabilities, organization architecture, modulation and standardization methods in VLC.

2. Overview of communication systems using visible light

Visible light communication systems (VLC) use visible light for communications, which occupies a spectrum from 380 nm to 750 nm, corresponding to a frequency spectrum from 430 THz to 790 THz.

The VLC receiver only receives signals if it is in the same room as the transmitter, so receivers outside the VLC source room will not be able to receive signals, which ensures the potential security of data transmission. Since the source of visible light can be used both for lighting and for communication, therefore, it saves additional power, which increases the transmission efficiency and increases the secrecy for outsiders, data transmission. VLC has high throughput and low power consumption.

When implementing VLC, there are a number of problems associated with interference from surrounding third-party light sources, interference between VLC devices, and VLC integration with existing wireless technologies. To overcome the identified problems, four JEITA CP-1221, JEITA Cp-1222, JEITA Cp-1223 and IEEE 802.15.7 standards have been developed.

In 802.15.7, only the channel and physical layers are defined for communication over a short distance using visible light. On the transmitter side, white light is generated at the wavelength of the LED. White light based on LEDs is generated in dichromatic, trichromatic and tetrachromatic modes. Data on the transmitter side is modulated by modulating the light; however, the modulation must be done in such a way as to avoid flicker. In addition, the dimming level selected for modulation must be such that it is supported by luminous LEDs. A typical VLC receiver consists of a gain circuit, an optical filter, and an optical hub.

The two integral parts of a VLC system: the transmitter and the receiver usually consist of three general levels. This is the physical layer, the link layer and the application layer. The reference model of the VLC communication system is shown in the figure. 2 [5]. In IEEE 802.15.7, only two layers (such as physical and channel) are defined for simplicity [6].

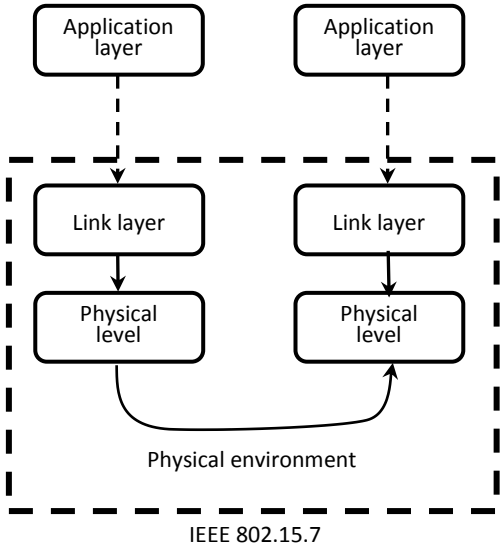

Fig. 2. *Layered VLC architecture.*

Tasks performed by the link level access control environment include [7]: support mobility, support dimming the LED, support visibility, support security, reduce flicker, support color functions, support network beacons, support installation and disconnection of the network, ensuring reliable communication between equal level link objects. Topologies supported by the link layer are peer-to-peer, broadcast and star-shaped

The physical layer provides the physical specification of the device, as well as the relationship between the device and the carrier.

Three different types of physical VLC implementations are given in IEEE 802.15.7. The capacity of the first, second, and third implementations, respectively, is 11.67–266.6 Kbps, 1.25–96 Mbps, and 12–96 Mbps, respectively.

3. Countermeasures for information leakage

The main countermeasures consist of organizational and technical measures.

Organizational measures include prohibiting the use of video cameras in the office, closing the LEDs, using more inertial incandescent or energy-saving neon lamps, and shielding windows. Separately, it is necessary to monitor compliance with the imposed administrative restrictions and regularly check them.

In most cases, organizational measures to counter information leakage are not enough to ensure the required effectiveness of information protection. It is necessary to carry out a set of technical measures to protect information, providing for the use of special technical means, as well as the implementation of technical solutions. Technical measures are aimed at closing information leakage channels by reducing the signal-to-noise ratio in places where portable acoustic intelligence devices or their sensors can be placed to values that ensure that the information signal cannot be extracted by the intelligence tool. Depending on the technical means used, passive and active methods of protecting information can be used.

Acoustic masking is effectively used to protect speech information from leakage through the direct acoustic channel by suppressing by means of acoustic noise (noise) microphones of reconnaissance equipment installed in such structural elements of the protected premises as the doorway, ventilation duct, space behind the suspended ceiling, etc. Vibroacoustic masking is used to protect speech information from leakage through acousto-vibrational and acousto-optic (opto-electronic) channels and consists in creating vibration noise in elements of building structures, window panes, engineering communications, etc. Vibroacoustic masking is effectively used to suppress electronic and radio-stethoscope as well as laser acoustic intelligence systems.

The creation of electromagnetic masking including optical low-frequency interference (low-frequency masking interference method) is used to exclude the possibility of intercepting speech information from allocated rooms using passive and active acoustoelectric information leakage channels, suppressing the channel by modulating visible light.

The ban on the use of LED lighting lamps is easily implemented, but leads to an increase in energy costs. It is worth noting that for the organization of office workplaces, open-air premises are often used, which involve the separation of workplaces only by partitions or the use of glass walls and partitions all this allows surveillance surveillance cameras to receive an optical signal from LEDs of lighting equipment and computers. Therefore, it is necessary to provide shielding of computer technology from getting into the field of view of video surveillance systems.

It is advisable to use technical systems of counteraction, including the monitoring of the state of the LEDs using a software or optical method. Detection of the use of LEDs for transmitting messages by external sensors is an ideal method, without informing the attacker of any information about the measures taken to ensure the protection of information. Such monitoring is passive and not detectable by an intruder. External detection of transmission is usually apparently very informative, but for a high probability of detection, it is necessary to know the frequency range and the type of modulation and coding of the transmitted message. We have to admit that the considered hidden optical channels of information leakage are unlikely, but they still remain difficult to detect.

4. Conclusion

The development of LEDs has made semiconductor lighting a growing area [8]. LEDs surpassed incandescent light sources in terms of reliability, power consumption and light output. The efficiency of LEDs is 20 lm / W more than incandescent efficiency [9]. LEDs and lasers are used as transmission sources for VLC. The LED should be used when communications and lighting should be performed using the same device.

The technical features of the considered transmission method such as high bandwidth, the absence of interference from radio wave radiation, the absence of harmful effects on the human body made communication in visible light an attractive promising technology and at the same time carrying the danger of organizing an information leakage channel.

Given the pace at which attackers use modern technology to breach information security, the area of VLC research in the interests of information security for its detection and suppression is relevant. All of these applications have made VLC an attractive area of research.

5. Literature

1. ⟨http://purelifi.com/what_is_li-fi/the-lifi-story/⟩

2. Anurag Sarkar, Shalabh Agarwal, Asoke Nath, Li-Fi technology: data transmission through visible light, Int. J. Adv. Res. Comput. Sci. Manag. Stud. 3 (6) (2015).

3. Y. Wang, N. Chi, Y. Wang, L. Tao, J. Shi, Network architecture of a high-speed visible light communication local area network, IEEE Photonics Technol. Lett. 27 (2) (2015) 197–200p.

4. ⟨https://mentor.ieee.org/802.15/dcn/08/15-08-0171-00-0vlc-10mbps-visible-light-transmission-system.pdf⟩.

5. S. Schmid, G. Corbellini, S. Mangold, T.R. Gross, LED-to-LED visible light communication networks, in: Proceedings of the fourteenth ACM international symposium on Mobile ad hoc networking and computing, 2013, pp.1–9.

6. C. Ley-Bosch, I. Alonso-González, D. Sánchez-Rodríguez, C. Ramírez-Casañas, Evaluation of the effects of hidden node problems in IEEE 802.15. 7 uplink performance, Sensors 16 (2) (2016).

7. IEEE, P802.15.7 – Standard for Short-Range Wireless Optical Communication, 2011.

8. Zukauskas, M.S. Shur, R. Gaska, Introduction to Solid-state Lighting, J. Wiley, United States, 2002.