Optics Communications 344 (2015) 81–85

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Secure communication zone for white-light LED visible light communication

Chi-Wai Chow [a], Yang Liu [b], Chien-Hung Yeh [c,*], Chung-Yen Chen [a], Chao-Nan Lin [a], Dar-Zu Hsu [d]

[a] Department of Photonics and Institute of Electro-Optical Engineering, National Chiao Tung University, Hsinchu 30010, Taiwan
[b] Philips Electronics Ltd., Hong Kong
[c] Department of Photonics, Feng Chia University, Seatwen, Taichung 40724, Taiwan
[d] Information and Communications Research Laboratories, Industrial Technology Research Institute (ITRI), Hsinchu 31040, Taiwan

ARTICLE INFO

Article history:
Received 2 January 2015
Received in revised form
16 January 2015
Accepted 19 January 2015
Available online 21 January 2015

Keywords:
Visible light communication (VLC)
Optical wireless communication (OWC)
Secure communication

ABSTRACT

As visible light communication (VLC) can be one of the promising wireless communication technologies in the future, improving the transmission security in VLC is highly desirable. We propose and demonstrate a secure VLC system using data superposition of different light emitting diodes (LEDs). The eavesdroppers can receive similar illumination but cannot obtain enough signal-to-noise ratio (SNR) for communication. The channel model and simulation parameters are presented. Analysis of the secure VLC zone forming using practical in-home scenarios is also discussed, showing the flexibly control the size and shift of secure VLC zone. A proof-of-concept experiment is performed, and there is a good match in trend between the experimental and simulation results.

1. Introduction

Comparing with the traditional lighting sources, such as compact fluorescent lamp (CFL) and incandescent lamp, white-light light-emitting-diode (LED) has many attractive features, including long life-time, low power consumption and high power efficiency. Besides, LED can be used as the transmitter (Tx) for visible light communication (VLC). VLC can provide many attractive features, such as high directionality, license-free and electromagnetic interference (EMI) free. White-light LED illumination system with the value-added functionality of VLC enables the deployment of a communication system with very little extra cost. As a result, the researches of VLC have been extensively performed in recent years, including improving the VLC transmission performances and data rates [1–8], reduction of the influence of optical background noises [9,10], using spatial arrangement to reduce the VLC signal-to-noise (SNR) fluctuation [11,12], etc. As VLC is one of the promising wireless communication technologies in the future, improving the transmission security in VLC is highly desirable.

VLC is generally considered as a more secure communication link when compared with radio-frequency (RF) communication, since it is based on light-of-sight (LOS) communication and optical signal does not penetrate wall. As the primary function of the LED system is for lighting, it is not possible to increase or reduce the illumination level for controlling the users' access.

In this work, we first propose and demonstrate a secure VLC system using data-superposition of different LEDs. Hence, a secure VLC zone can be created, and this can protect the information from being detected by adjacent users with similar light illumination. Most importantly, our proposed scheme will not affect the home illumination when the secure communication zone is formed; hence eavesdroppers will receive similar light illumination but cannot obtain enough SNR for communication. The channel model and simulation parameters are presented. Analysis of the secure VLC zone forming using practical in-home scenarios is also discussed, showing flexible control of the size and shift of secure VLC zone. A proof-of-concept experiment is performed, and there is a good match in trend between the experimental and simulation results.

2. Architecture of secure VLC system

Fig. 1 shows the proposed architecture of secure VLC system. A standard room size of 4 m × 4 m × 3 m is used. The distance between the ceiling lamp and the working space is 2 m. 8 white-light LED lamps, in which 4 LEDs at the center (referred as signal-LEDs) are for VLC. The other 4 LEDs (referred as intrusion-LEDs) send intrusion signal. The 4 intrusion-LEDs are located at a distance of 0.5 m away from the center. The modulation formats of both data

* Corresponding author.
E-mail address: yehch@fcu.edu.tw (C.-H. Yeh).

http://dx.doi.org/10.1016/j.optcom.2015.01.055
0030-4018/

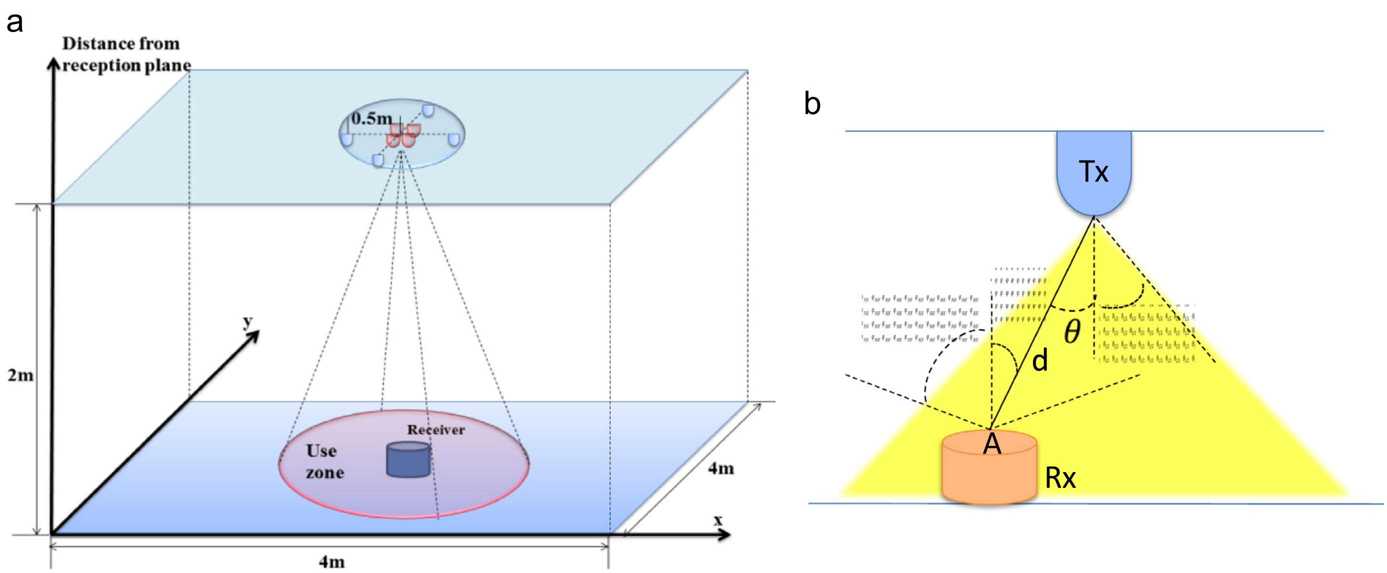

Fig. 1. (a) Proposed secure VLC system. 4 signal-LEDs (marked red) and 4 intrusion-LEDs (marked blue). (b) System model with simulation parameters. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

and intrusion signals are non-return-to-zero (NRZ) on–off keying (OOK). By control the powers and beam-angles of the LEDs, the secure VLC zone can be adjusted, and they will be discussed in the following sections.

First, we discuss the channel model and simulation parameters. The LED is assumed to have a Lambertian radiant intensity [13] as in the following equation:

$$R(\theta) = (m+1)\cos^{m}(\theta)/(2\pi) \tag{1}$$

where m is the order of Lambertian emission defined by the LED's semi-angle at half power $\theta_{1/2}$, so that the order of Lambertian emission can be described in the following equation:

$$m = -\frac{\ln 2}{\ln(\cos(\theta_{1/2}))} \tag{2}$$

Here θ and φ are the irradiance and incidence angles respectively, as shown in Fig. 1(b). Light propagates from LED to Rx via the LOS since the LED is located at the center of the room. The direct-current (DC) gain can be expressed by the channel transfer function

$$h = \begin{cases} \dfrac{(m+1)A\cos^{m}(\theta)\cos(\varphi)}{2\pi d^2} & \varphi \le \varphi_{FOV} \\ 0 & \varphi > \varphi_{FOV} \end{cases} \tag{3}$$

where A is the Rx area, d is the LOS distance between the LED and Rx. As shown in Eq. (3), the incidence angle φ should be less than the field-of-view (FOV) incidence angle φ_{FOV}, otherwise, the channel transfer function is zero. After modulation, the output signal power $P_o(t)$ from the LED can be described as

$$P_o(t) = P_{LED}[1 + M_i x(t)] \tag{4}$$

where P_{LED} is the LED optical power, M_i is the modulation index and $x(t)$ is the NRZ OOK signal. The signal detected by the Rx is equal to

$$s'(t) = RP_o(t)h \tag{5}$$

where R is the responsivity of the Rx, h is the channel transfer function described in Eq. (3).

When the detected signal is DC-blocked, the output signal $s(t)$ from the Rx can be derived as

$$s(t) = RP_{LED}M_i x(t)h \tag{6}$$

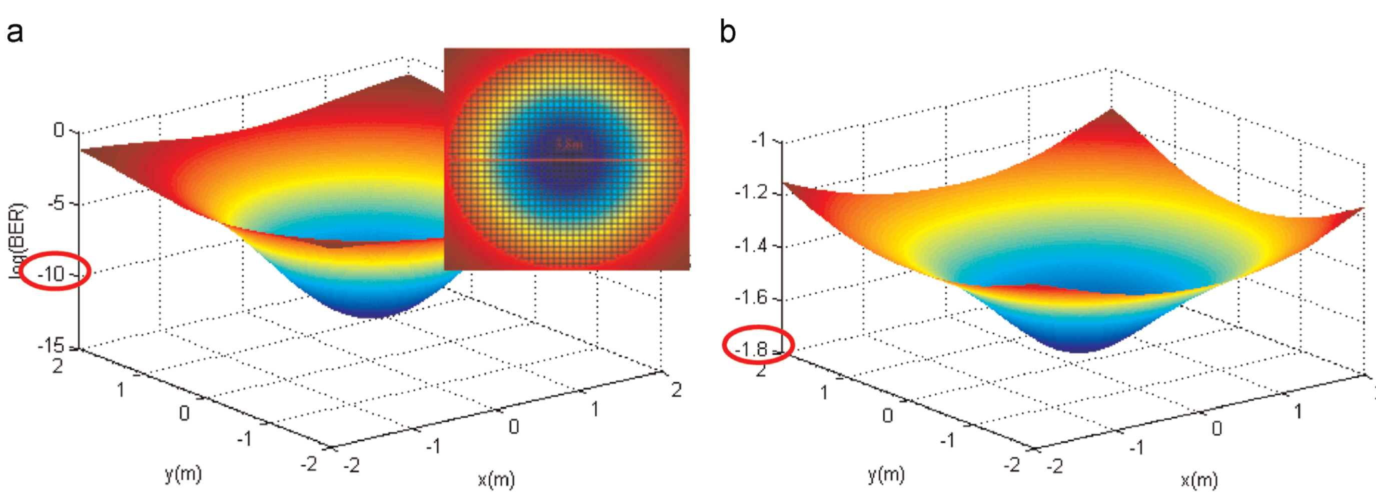

Fig. 2. BER distribution of (a) without and (b) with the intrusion signal; illustrating the secure VLC zone.