Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 4094096, 6 pages
https://doi.org/10.1155/2017/4094096

WILEY | Hindawi

Research Article

Secrecy Dimming Capacity in Multi-LED PAM-Based Visible Light Communications

Byung Wook Kim

Department of ICT Automotive Engineering, Hoseo University, 201 Sandan 7-ro, Seongmun-myeon, Dangjin-si, Chungcheongnam-do 31702, Republic of Korea

Correspondence should be addressed to Byung Wook Kim; philip0110@gmail.com

Received 8 June 2017; Accepted 31 July 2017; Published 28 August 2017

Academic Editor: Shingo Yamaguchi

Recently, mobile cloud computing (MCC) has gained a lot of interest for researchers building the next-generation mobile applications. Because unauthorized access may cause serious problems, security and privacy with MCC have become significant issues. This paper addresses the secrecy dimming capacity of secure transmission in MCC over visible light communication (VLC) channels. By obtaining the entropy-maximizing symbol probability of multiple light emitting diode- (LED-) based pulse amplitude modulation (PAM), mathematical analysis of the secrecy dimming capacity of VLC was derived. Simulation results show that the secure transmission ability of multi-LED-based VLC is determined according to the number of activated LEDs and target dimming level. This can be a guideline for practical VLC-based mobile network designers intending to secure wireless transmission and to decide on the number of activated LEDs at target dimming level to operate.

1. Introduction

With the proliferation of smart mobile devices and cloud computing technologies, mobile cloud computing (MCC) has emerged as one of the most important technologies for next-generation mobile services [1–4]. MCC is a technology that combines mobile devices and cloud computing to perform both data storage and data processing outside the mobile device. The use of MCC can offer ubiquitous on-demand network access to a shared pool of configurable data processing resources that can be rapidly provided with minimal management effort on the user side and for the service provider.

As the radio frequency spectrum of mobile devices becomes increasingly crowded and light emitting diodes (LEDs) are more widely used for various incident light applications, visible light communication (VLC) is gaining appeal as an alternative to conventional radio frequency (RF) for billions of mobile devices that need to be networked [5–9]. A VLC system can transmit information by modulating the intensity of LEDs at high frequencies (≥150 Hz) so that LED flickering is unnoticeable to the human eye. Due to VLC's large spectral availability and the free unlicensed spectrum, mobile phone-based VLC can be an important candidate for MCC applications. By adapting multiple-input multiple-output (MIMO) technology in VLC, where multiple LEDs and multiple photo-detectors (PDs) are utilized, independent data streams are simultaneously transmitted from all light sources and thus it promises a further increase in bandwidth for MCC networks.

Although the widespread use of mobile devices can contribute to the improvement of standard of living, anxiety about the leakage of personal information is increasing. While the large spectral availability of the visible light spectrum is certainly the main reason for the growing interest in VLC, the inherent security that stems from line-of-sight propagation and the nonpenetrating nature of light waves is also an important issue and the most captivating difference compared to RF. This vulnerability may be even worse for RF communications due to the nature of the broadcast of the radio propagation and the inherent random nature of the radio channel. Although VLC channel exhibits perfect security in a private-room, security of the transmitted signal in public areas such as hotels, stations, libraries, or planes cannot be guaranteed, and thus it makes transmissions over VLC channel vulnerable to unexpected wiretappers' attacks.

Because user's privacy and integrity of data are important, secure communication for VLC becomes a significant topic for both academia and industry.

Recently, there have been several studies that address security in VLC systems. Mostafa and Lampe addressed secure VLC link at the physical layer [10] by investigating the achievable secrecy rates of a Gaussian wiretap channel. Cho et al. [11] investigated secrecy outage probability of the downlink for VLC. Zhang et al. [12] proposed a secure system for barcode-based VLC, that is, for secure transmission between a screen and a camera. To support secure data exchange, however, the system requires a fully duplex VLC channel. To the best of our knowledge, the secrecy dimming capacity of VLC using multiple LEDs has not been studied in the literature.

This paper investigates the secrecy dimming capacity of pulse amplitude modulation- (PAM-) based VLC using multiple LEDs. To derive a secrecy dimming capacity, the entropy-maximizing PAM symbol probabilities were mathematically derived. Then the secrecy dimming capacity for multiple LED-based VLC systems was analyzed. Simulation results demonstrated the baseline information of the secrecy dimming capacity of multi-LED PAM-based VLC systems. To obtain robust secure transmission under VLC, the number of activated LEDs should be decided according to the target dimming level.

The main contribution of this paper is the analytical derivation of secrecy dimming capacity in the presence of the wiretapper. The curves of secrecy dimming capacity were plotted against the SNR and target dimming ratio of the main channel in the presence of the wiretappers channel. This can be a guideline for practical VLC-based mobile network designers intending to secure wireless transmission and to decide on the number of activated LEDs at target dimming level to operate. This paper paves the way for a new study on the secrecy dimming capacity when both the main and wiretapper VLC channels are considered.

The remainder of this paper is organized as follows. The system model of a multi-LED PAM-based VLC scheme is presented in Section 2. Section 3 addresses derivation of entropy-maximizing PAM symbol probabilities. Section 4 reports analysis of secrecy dimming capacity and evaluation. Section 5 presents the conclusions.

2. System Model of Multi-LED PAM-Based VLC

A VLC scenario with one transmitter and one legitimate receiver in the presence of a wiretapper, where the solid and dash lines represent the main channel (from transmitter to legitimate receiver) and the wiretap channel (from transmitter to wiretapper), respectively, is shown in Figure 1. When a transmitter sends its signal to a legitimate receiver, a wiretapper may overhear such transmission due to the nature of wireless medium. Considering the fact that recent mobile devices are highly standardized, wiretappers can easily acquire communication parameters such as signal waveform, coding, modulation scheme, and encryption algorithm. In addition, the secret key can be accessed by the wiretapper through the exhaustive search. In this scenario, the transmitted signal can be interpreted at the wiretapper by decoding its overheard signal, leading the legitimate transmission to be insecure.

The number of activated LEDs, N_t, at the transmitter is assumed to be same as the number of PDs at legitimate and wiretap receivers. When the sender transmits $N_t \times 1$ symbol vector $\mathbf{X}$, the $N_t \times 1$ received symbol vectors $\mathbf{Y}_1$ and $\mathbf{Y}_2$ at the legitimate receiver and the wiretapper, respectively, are given by

$$\begin{aligned} \mathbf{Y}_1 &= \mathbf{X} + \mathbf{Z}_1, \\ \mathbf{Y}_2 &= \mathbf{X} + \mathbf{Z}_2. \end{aligned} \tag{1}$$

$\mathbf{Z}_q$, $q = 1, 2$, is $N_t \times 1$ additive white Gaussian noise (AWGN) vector following $\mathbf{Z}_q \sim N(\mathbf{0}, \mathbf{K}_q)$, where

$$\mathbf{K}_q = \begin{bmatrix} \sigma_q^2 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_q^2 \end{bmatrix}, \tag{2}$$

which satisfies

$$\mathbf{0} < \mathbf{K}_1 < \mathbf{K}_2. \tag{3}$$

Because the goal of the transmitter here is not just to convey information reliably to the legitimate receiver, but also to perfectly secure the data from the wiretap receiver, the condition in (3) should be satisfied.

Note that intensity modulation with direct detection (IM/DD) is typically used in VLC systems where signals are transmitted through an LED in the form of optical power. In the receiver, a PD is employed to convert the optical power signal into electrical signals. By applying MIMO technology to VLC, independent data streams are simultaneously emitted from multiple LEDs.

The PAM modulation method is considered for data modulation, where the information is encoded in the amplitude of a series of signal pulses. Applying MIMO concept to VLC, the independent PAM-modulated signals are transmitted from activated LEDs. As this method simultaneously emits the identical signal from several activated LEDs, the optical transmission power is assumed to be equally distributed across all LEDs. For the individual LED, the intensities of PAM with Mth order modulation are given by

$$I_n = \frac{2In}{M+1}, \quad n = 1, 2, \ldots, M, \tag{4}$$

where I is medium intensity of PAM signal candidates. Signals with intensity $I_n = 0$ at an individual LED are not used for the signal modulation so that activated and nonactivated LEDs can be distinguished.

3. Entropy-Maximizing Symbol Probability of Multi-LED PAM

To use LEDs in a mobile device as an illumination source, the target dimming level should be determined according to various illuminating applications. To meet the target dimming

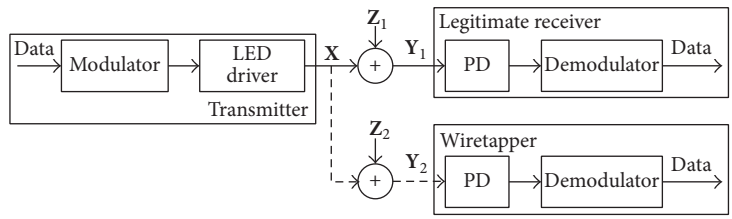


Figure 1: The system model of VLC in the presence of wiretapper.

level of multiple LED-based VLC systems, symbol probability of various PAM-levels should be different. Because there are many possible alternatives for meeting the given target dimming level, each will result in a different entropy. Therefore, an entropy-maximizing probability distribution is derived to determine secrecy dimming capacity. The entropy of PAM at an individual LED is given by

$$-\sum_{n=1}^{M} p(n) \log_2 p(n), \tag{5}$$

where M is the order of modulation and $p(n)$ is the nth symbol probability.

To meet the total transmit power constraint, that is, the dimming level constraint, each respective emitted intensity is the total power divided by the number of activated LEDs. By doing this, the total optical power emitted is constant regardless of the number of activated LEDs. Using the normalization constraint associated with the definition of a probability density, the intensity of an individual LED considering dimming constraint is written as

$$\sum_{n=1}^{M} \frac{2In}{M+1} p(n) = \frac{D_t}{N_t} 2I, \tag{6}$$

where D_t is the target dimming ratio and N_t is the number of activated LEDs. Note that the range of the target dimming ratio is $0 \le D_t \le 1$ and target dimming level is set to $D_t \times 100$. Due to the sum-power constraint on the transmitting LEDs, the intensity is divided by N_t. Using the symbol probability set $(p(1), p(2), \ldots, p(n))$, satisfying (6), we obtain symbol probability that maximizes (5) by using Lagrange multipliers. Note that objective function (5) is concave, and the constraint function (6) is linear. Therefore, the Lagrange equation is presented as

$$\begin{aligned} &L(p(1), p(2), \ldots, p(M), \beta, \gamma) \\ &= -\sum_{n=1}^{M} p(n) \log_2 p(n) - \beta \left(\sum_{n=1}^{M} p(n) - 1 \right) \\ &\quad - \gamma \left(\sum_{n=1}^{M} \frac{2In}{M+1} p(n) - 2I \frac{D_t}{N_t} \right), \end{aligned} \tag{7}$$

where β and γ are the scalar Lagrange coefficients. The problem of maximizing (7) is solved by converting the problem to an optimization problem with independent variables. The variables to this problem are $p(n), \beta, \gamma$, and three equations are obtained from the gradient with respect to these variables. Having the same number of equations and variables makes the problem determined and can be solved. To calculate the gradient of the Lagrange equation, the functional derivative on (7) with respect to the variables [13], $p(n), \beta, \gamma$, is taken as follows:

$$\frac{\partial L}{\partial p(n)} = -\log_2 p(n) - \frac{1}{\ln 2} - \beta - \gamma \frac{2In}{N_t (M+1)} = 0, \tag{8}$$

$$\frac{\partial L}{\partial \beta} = \sum_{n=1}^{M} p(n) - 1 = 0, \tag{9}$$

$$\frac{\partial L}{\partial \gamma} = \sum_{n=1}^{M} \frac{2In}{M+1} p(n) - 2I \frac{D_t}{N_t} = 0. \tag{10}$$

Equation (8) is rearranged as

$$p(n) = 2^{-1/\ln 2 - \beta - \gamma(2In/(M+1))}. \tag{11}$$

Equations (9) and (11) give

$$2^a = \frac{r\left(1 - r^M\right)}{1 - r}, \tag{12}$$

where

$$\begin{aligned} a &= \frac{1}{\ln 2} + \beta, \\ r &= 2^{-\gamma 2I/(M+1)}. \end{aligned} \tag{13}$$

Equations (10) and (11) are simplified as

$$\begin{aligned} &D_t \\ &= \frac{N_t 2^{-a}}{(M+1)} \left(\frac{r\left(1 - r^{M-1}\right)}{(1-r)^2} - \frac{(M-1) r^M}{(1-r)} + M r^M \right). \end{aligned} \tag{14}$$

From (12) and (13), multiple solutions for (β, γ) are obtained. Then, β and γ solutions are carefully chosen to make the group of symbol probabilities $(p(1), p(2), \ldots, p(n))$ non-negative and real. This yields (11) providing PAM symbol probabilities that maximize entropy while satisfying the given target dimming level.

Figure 2 presents PAM symbol probabilities maximizing entropy when 4-PAM is considered. To meet the constraint of target dimming ratio, turn-on probability maximizing entropy for each PAM signal level is different except when target dimming ratio is 0.5.

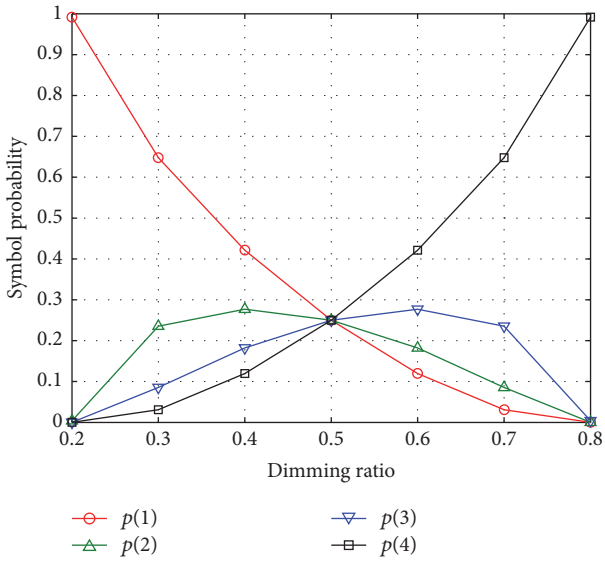


Figure 2: Entropy-maximizing symbol probability (4-PAM).

4. Analysis of Secrecy Dimming Capacity for Multi-LED PAM-Based VLC

In this section, the secrecy dimming capacity for multi-LED PAM-based VLC is analyzed. The dimming capacity means the achievable data rate obtained by a specific modulation and dimming condition and expressed as mutual information. The secrecy dimming capacity is the difference in the dimming capacities of the main channel and the wiretapper's channel under the constraint of target dimming level [14]. When the main channel is less noisy compared to the wiretapper's channel, the secrecy dimming capacity is given by

$$C_d = \max_{p(n)} \left[I\left(\mathbf{X}; \mathbf{Y}_1\right) - I\left(\mathbf{X}; \mathbf{Y}_2\right) \right]. \tag{15}$$

Note that the secrecy dimming capacity can be expressed in even simpler terms in certain cases. When $I(\mathbf{X}; \mathbf{Y}_1)$ and $I(\mathbf{X}; \mathbf{Y}_2)$ can be individually maximized by the same $p(n)$, the secrecy capacity is simply the difference in channel capacities [15]. As the mutual information between two random variables is a measure of the amount of information they contain about each other, the difference $I(\mathbf{X}; \mathbf{Y}_1) - I(\mathbf{X}; \mathbf{Y}_2)$ represents the extra information that $\mathbf{Y}_1$ shares with $\mathbf{X}$ over that which $\mathbf{X}$ and $\mathbf{Y}_2$ share. Because this approach specializes the setting to less noisy main channel by imposing the restriction of $\mathbf{K}_2 > \mathbf{K}_1$, secrecy dimming capacity is always positive. If the secrecy capacity falls below zero, the transmission from transmitter to legitimate receiver becomes insecure and the wiretapper would succeed in intercepting the transmitted information. In order to enhance transmission security against a wiretapper's attack, it is of importance to reduce the probability of occurrence of an intercept event through enlarging the secrecy dimming capacity.

The expression of secrecy dimming capacity becomes just the difference in the mutual information of the main and the wiretapper's channel. Because the mutual information is defined as differential entropy, the secrecy dimming capacity is presented as

$$\begin{aligned} C_d &= I\left(\mathbf{X}; \mathbf{Y}_1\right) - I\left(\mathbf{X}; \mathbf{Y}_2\right) \\ &= h\left(\mathbf{Y}_1\right) - h\left(\mathbf{Y}_1 \mid \mathbf{X}\right) - h\left(\mathbf{Y}_2\right) - h\left(\mathbf{Y}_2 \mid \mathbf{X}\right) \\ &= h\left(\mathbf{Y}_1\right) - h\left(\mathbf{Z}_1\right) - h\left(\mathbf{Y}_2\right) - h\left(\mathbf{Z}_2\right) \\ &= -\int_{-\infty}^{\infty} P_Y\left(\mathbf{Y}_1\right) \log_2 P_Y\left(\mathbf{Y}_1\right) d\mathbf{Y}_1 \\ &\quad - \frac{1}{2} \log_2 \left(2\pi e\right)^{N_t} \left|\mathbf{K}_1\right| \\ &\quad - \int_{-\infty}^{\infty} P_Y\left(\mathbf{Y}_2\right) \log_2 P_Y\left(\mathbf{Y}_2\right) d\mathbf{Y}_2 \\ &\quad - \frac{1}{2} \log_2 \left(2\pi e\right)^{N_t} \left|\mathbf{K}_2\right|. \end{aligned} \tag{16}$$

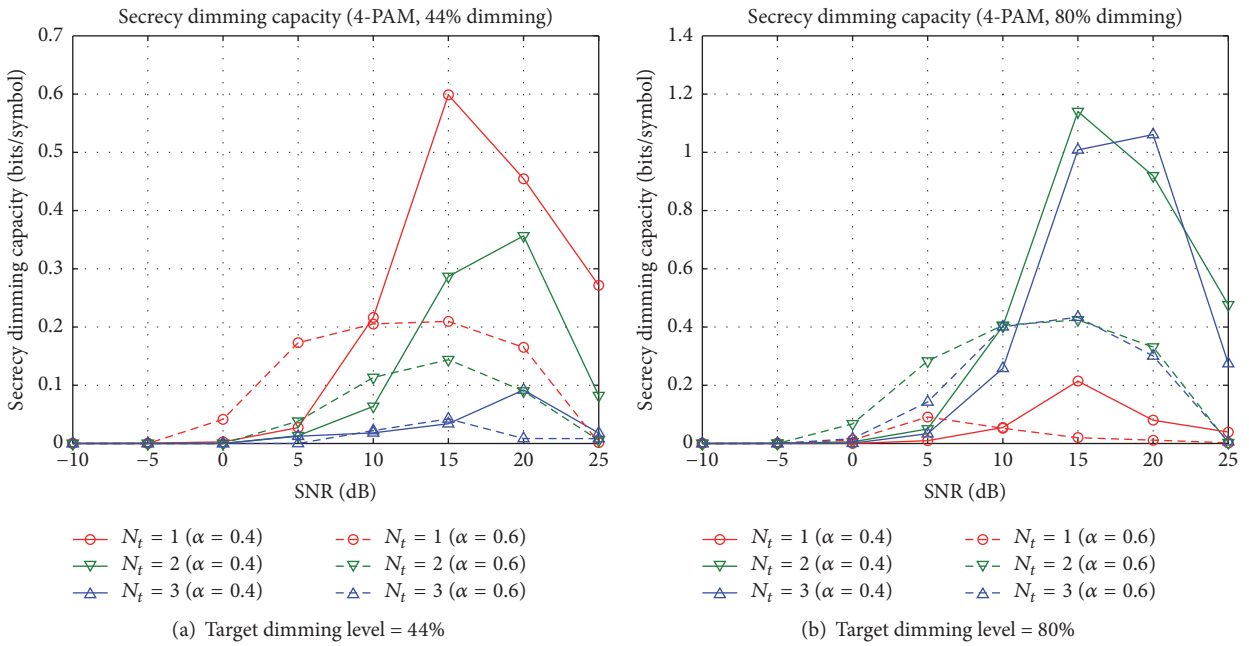
The probability distribution functions of the transmitted signal $P_X(\mathbf{X})$, the received signal via main channel, $P_Y(\mathbf{Y}_1)$, the received signal via wiretap channel, $P_Y(\mathbf{Y}_2)$, AWGN via main channel, $P_Z(\mathbf{Z}_1)$, and AWGN via wiretap channel, $P_Z(\mathbf{Z}_2)$, are expressed as

$$\begin{aligned} P_X\left(\mathbf{X}\right) &= \sum_{n=1}^{M} p\left(n\right) \delta\left(\mathbf{X} - \mathbf{b}_n\right), \\ P_Y\left(\mathbf{Y}_1\right) &= \sum_{n=1}^{M} p\left(n\right) P_Z\left(\mathbf{Y}_1 - \mathbf{b}_n\right), \\ P_Y\left(\mathbf{Y}_2\right) &= \sum_{n=1}^{M} p\left(n\right) P_Z\left(\mathbf{Y}_2 - \mathbf{b}_n\right), \\ P_Z\left(\mathbf{Z}_1\right) &= \frac{1}{\pi^{N_t} \det\left(\mathbf{C}_Z\right)} \exp\left(-\mathbf{Z}_1{}^T \mathbf{C}_Z^{-1} \mathbf{Z}_1\right), \\ P_Z\left(\mathbf{Z}_2\right) &= \frac{1}{\pi^{N_t} \det\left(\mathbf{C}_Z\right)} \exp\left(-\mathbf{Z}_2{}^T \mathbf{C}_Z^{-1} \mathbf{Z}_2\right), \end{aligned} \tag{17}$$

where $\mathbf{b}_n$ is the $N_t \times 1$ intensity vector with elements of I_n. From (16), the secrecy dimming capacity, with the maximum information rate of the main channel (transmitter-to-legitimate receiver) with the ignorance at the wiretapper, can be obtained.

Figure 3 shows the secrecy dimming capacity of 4-PAM versus SNR values with different target dimming level. The ratio of average legitimate noise variance to wiretappers average noise variance is defined as $\alpha = \sigma_1^2/\sigma_2^2$. We can see that secrecy dimming capacity for $\alpha = 0.4$ is larger than that of $\alpha = 0.6$. This means that the more the noise on wiretap channel is, the greater the secrecy dimming capacity can be achieved. When dimming level is 44%, a single activated LED shows a robust secrecy dimming capacity compared to multiple activated LEDs. For 80% dimming level scenario, however, multiple activated LEDs, that is, $N_t = 2, 3$, result in better performance of secrecy dimming capacity than the scenario with single activated LED.

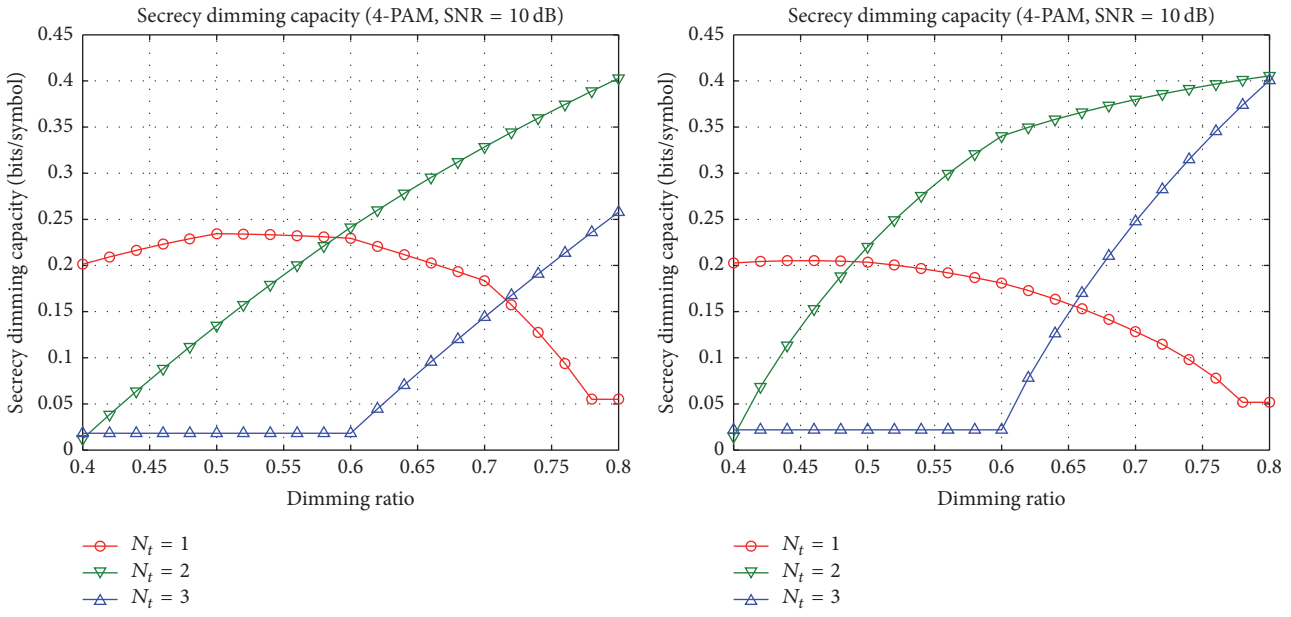
Figure 4 shows the secrecy dimming capacity of 4-PAM versus target dimming ratio. For $\alpha = 0.6$, the single



(a) Target dimming level = 44%

(b) Target dimming level = 80%

FIGURE 3: Secrecy dimming capacity with 44% and 80% of target dimming level.



(a) $\alpha = 0.4$

(b) $\alpha = 0.6$

FIGURE 4: Secrecy dimming capacity with $\alpha = 0.4$ and $\alpha = 0.6$.

activated LED shows best performance when target dimming ratio is ≤0.48. When target dimming ratio is larger than 0.48, the performance with dual activated LEDs outperforms other scenarios. As the target dimming ratio approaches 0.8, the use of two and three activated LEDs shows similar secrecy dimming capacity performance. For $\alpha = 0.4$, the single activated LED shows best performance when target dimming ratio is ≤0.58. If the target dimming ratio is set to a value larger than 0.58, best secrecy dimming capacity performance can be achieved when dual activated LEDs are considered. From Figures 4(a) and 4(b), we see that the use of multiple activated LEDs results in robust secrecy dimming capacity performance when target dimming ratio is set to high value. When low dimming is required, the use of a single activated LED guarantees best secrecy dimming capacity.

5. Conclusions

Because of the increased demand for processing and storage capabilities for mobile devices, MCC is gaining popularity. As MCC makes data storage and data processing possible outside of a mobile device, security risk becomes a significant issue. This paper investigates the secrecy dimming capacity of PAM in VLC with multiple LED arrays. By obtaining entropy-maximizing symbol probabilities based on multiple LED arrays, the secrecy dimming capacity considering the presence of wiretapper is mathematically derived. Simulation results showed the baseline information of secure capacity performance of PAM-based VLC systems. According to the target dimming ratio, the number of activated LEDs should be decided to guarantee robust secrecy dimming capacity. The result can be a guideline to practical VLC-based mobile systems intending to secure wireless transmission.

Most of the existing works of secure transmission of VLC have neglected the joint consideration of various forms of the wireless attacks, including both eavesdropping and denial-of-service (DoS) behaviors. It will be very important to explore new techniques of joint defense and maximizing secrecy dimming capacity against multiple different wireless attacks. Furthermore, it will be important to consider joint optimization of security and throughput of the VLC system, which is a problem to be solved in the future.

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIP) (2016R1C1B1013942).

References

[1] Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya, "Heterogeneity in mobile cloud computing: taxonomy and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 369– 392, 2014.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Communications and Mobile Computing*, vol. 13, no. 18, pp. 1587–1611, 2013.

[3] J. Bou Abdo, T. Bourgeau, J. Demerjian, and H. Chaouchi, "Extended privacy in crowdsourced location-based services using mobile cloud computing," *Mobile Information Systems*, vol. 2016, Article ID 7867206, 13 pages, 2016.

[4] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baaaharun, and K. Sakurai, "Authentication in mobile cloud computing: A survey," *Journal of Network and Computer Applications*, vol. 61, pp. 59–80, 2016.

[5] D. Karunatilaka, F. Zafar, V. Kalavally, and R. Parthiban, "LED based indoor visible light communications: state of the art," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 3, pp. 1649–1678, 2015.

[6] A. Nuwanpriya, S.-W. Ho, and C. S. Chen, "Indoor MIMO Visible Light Communications: Novel Angle Diversity Receivers for Mobile Users," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1780–1792, 2015.

[7] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, "Visible light communication, networking, and sensing: a survey, potential and challenges," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2047–2077, 2015.

[8] L. Yin, W. O. Popoola, X. Wu, and H. Haas, "Performance evaluation of non-orthogonal multiple access in visible light communication," *IEEE Transactions on Communications*, vol. 64, no. 12, 2016.

[9] A. C. Boucouvalas, P. Chatzimisios, Z. Ghassemlooy, M. Uysal, and K. Yiannopoulos, "Standards for indoor Optical Wireless Communications," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 24–31, 2015.

[10] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Proceedings of the 1st IEEE International Conference on Communications (ICC '14)*, pp. 3342–3347, Sydney, Australia, June 2014.

[11] S. Cho, G. Chen, and J. P. Coon, "Secrecy analysis in visible light communication systems with randomly located eavesdroppers," in *Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 475–480, Paris, France, May 2017.

[12] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, "SBVLC: Secure barcode-based visible light communication for smartphones," *IEEE Transactions on Mobile Computing*, vol. 15, no. 2, pp. 432–446, 2016.

[13] D. P. Bertsekas, *Constrained Optimization and Lagrange Multiplier Methods*, Academic Press, New York, NY, USA, 1982.

[14] Y. Zou, J. Zhu, X. Wang, and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

[15] M. Van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 43, no. 2, pp. 712–714, 1997.