A Method for Improving Physical Layer Security in Visible Light Communication Networks

Zhe Chen, *Member*, *IEEE* and Xin Wang, *Member*, *IEEE*
Fujitsu R&D Centre Co., Ltd.
Beijing, China
Email: {chenzhe, wangxin}@cn.fujitsu.com

***Abstract*—In this paper, a method is proposed for improving the physical layer security for indoor visible light communication (VLC) networks with angle diversity transmitters. An angle diversity transmitter usually consists of multiple narrow-beam light-emitting diode (LED) elements with different orientations. Angle diversity transmitters are suitable for confidential data transmission, since data transmission via narrow light beams can effectively avoid the leakage of messages. In order to improve security performance, protection zones are introduced to the systems with angle diversity transmitters. Simulation results show that over 50% performance improvement can be obtained by adding protection zones.**

***Index Terms*—physical layer security; angle diversity transmitter; visible light communication; secrecy capacity.**

I. Introduction

Over the last decade, the number of mobile devices has been increasing exponentially. As predicted in the latest Cisco Visual Networking Index (VNI), overall mobile data traffic is expected to rise to 24.3 exabytes per month by 2019 [1]. In order to meet such high levels of data traffic, the incoming 5-th generation of communication system (5G) is striving for 1000-fold system capacity improvement over 4G. In order to achieve this, techniques including the use of densely deployed cells, mmWave spectrum and other unlicensed spectrum was being discussed in the recent 5G standardization meeting [2]. However, the aforementioned techniques cannot perfectly work in indoor scenarios. In order to achieve high data rate as well as fast coverage in indoor environment, it is inevitable to use expensive devices including advanced antenna arrays, high resolution analogue-to-digital converters etc. Also, the cost of deploying indoor RF cellular networks is high.

In order to improve system capacity in a cost-efficient manner, visible light communication (VLC) has emerged as one of the competitive candidates. VLC system employs light-emitting diodes (LEDs) for transmission and photodiodes (PDs) for reception. With the advancement of the LED technology, LEDs can now fulfil two functions at low cost: illumination and high-speed wireless communication. Taking an important step beyond the current 5G unlicensed spectrum access, high speed wireless networking solution using the aggregation of RF spectrum and visible light spectrum are envisaged.

In a typical indoor scenario, each lighting fixture can act as an optical access point (AP), and multiple lighting fixtures in a room can be connected as a VLC network. Since the coverage of LEDs is usually confined [3], the size of optical cells can be much smaller than the size of radio frequency (RF) cells. Hence, VLC networks facilitate more effective frequency reuse and higher data density than small-cell RF networks. Research showed that VLC networks significantly outperform RF femtocell networks [4].

With the increasing amount of wireless communication and the advent of Internet of Things (IoT), wireless communication security becomes increasingly important. Typically, wireless communication security is achieved by network layer protocols. These protocols include data encryption and password-protected access. However, since state-of-the-art wireless communication systems are of multiple layers, network layer protection alone cannot ensure end-to-end security. Hence, physical layer security is taken into account which is as important as the network layer security [5].

VLC is promising in enhancing physical layer security due to the following reasons: 1) since data transmission is via a different media, confidential messages conveyed by visible light cannot be wire-tapped by RF eavesdroppers; 2) as visible light cannot penetrate opaque objects, there is no leakage of confidential messages outside a confined area; 3) since LED can be easily designed with directionality, the coverage of an optical transmitter can be within a specific area. This feature can prevent the wire-tapping from distant eavesdroppers.

In previous researches, VLC physical layer security was studied from different aspects. A mechanism of generating security key was proposed for optical orthogonal frequency division multiplexing (OFDM) system in [6]. This mechanism was shown to achieve significant improvement in terms of system confidentiality. The secrecy rate of VLC links via transmitter beam-forming is evaluated in [7]. Apart from link level study, physical layer security of VLC are further studied in system level [8], [9]. In specific, angle diversity transmitters are used in VLC networks to improve security performance of the system [8].

In this study, we introduce a method of adding protection zones in VLC networks with angle diversity transmitters. This method can improve the security performance of the networks.

The remainder of this paper is organised as follows. In Section II, the system model of VLC networks is introduced. VLC networks with angle diversity transmitters are introduced

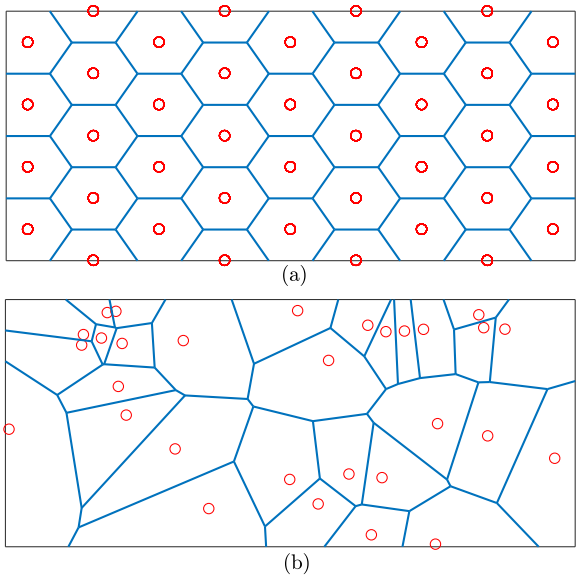

Fig. 1. The layout of (a) HEX deployment and (b) PPP deployment. Red circles represent optical APs in a room. Blue lines represent the boundaries of optical cells.

in Section III. The method of adding protection zones is given in Section IV. Simulation results are illustrated and discussed in Section V. Finally, Section VI concludes the paper.

II. System Models

A. Network Model

In a VLC network, optical APs can be deployed in different ways to meet the illumination requirement. In this study, two deployments are assumed and discussed as follows.

The first deployment is hexagonal (HEX) deployment. In this deployment, optical APs are deployed so that their service area can be divided into hexagonal shaped cells, as illustrated in Fig. 1(a). HEX deployment is assumed since this deployment can achieve the best system throughput in VLC networks [10].

The second deployment is poisson point process (PPP) deployment. In this deployment, the position of optical APs follows 2-D homogeneous PPP, as illustrated in Fig. 1(b). The density of PPP is defined as Λ. Compared with HEX deployment, PPP deployment can be regarded as worst-case scenario due to the randomness of AP positions [10].

B. Channel Model

In this study, the downlink direct current (DC) gain of the Line-of-sight (LOS) link is calculated as follows [11]:

$$H_0 = \frac{(n+1)A_{\text{eff}}}{2\pi d^2}\cos^n(\phi)\cos(\psi)\text{rect}\left(\frac{\psi}{\Psi_{\text{fov}}}\right), \quad (1)$$

where d is the distance between an optical AP and its corresponding receiver; Ψ_{fov} is the field-of-view (FOV) of the optical receiver; n is the Lambertian order of the LED element and it is also a function of the transmitter half-intensity radiation angle Φ_{tx} as $n = -1/\log_2(\cos(\Phi_{\text{tx}}))$; ϕ is the angle of irradiance; ψ is the angle of light incidence at the receiver; $\text{rect}(\cdot)$ is a rectangular function.

C. Secrecy Capacity

In typical wireless communication secrecy model, all users can be classified as legitimate users and eavesdroppers. Legitimate users exchange confidential messages with their desired APs with the existence of eavesdroppers. The widely used metric to evaluate communication secrecy is secrecy capacity. Secrecy capacity is defined as the maximum data rate that the information can be decoded with arbitrarily small error by the legitimate user, while the eavesdropper's error probabilities of decoding approach to maximum. The secrecy capacity of a legitimate user k is [12]:

$$C_{\text{secret}} = \left[\log_2(1+\gamma_k^{\text{legi}}) - \log_2\left(1+\tilde{\gamma}_k^{\text{eav}}\right)\right]^+, \quad (2)$$

where γ_k^{legi} is the signal-to-interference-plus-noise-ratio (SINR) of the legitimate user; $\tilde{\gamma}_k^{\text{eav}}$ is the SINR of the worst-case eavesdropper; $[a]^+$ denotes the $\max\{0, a\}$. Note that worst-case eavesdropper is the eavesdropper that can achieve the best SINR performance in the candidate eavesdroppers.

In general, two metrics can be used to describe the security performance of a VLC network. The first one is the cumulative distribution function (CDF) of the secrecy capacity of legitimate user represents the probability of the secrecy capacity of a legitimate user is larger than a secrecy capacity threshold C_{T}, which can be expressed as follows:

$$F(C_{\text{T}}) = \Pr(C_{\text{secret}} > C_{\text{T}}). \quad (3)$$

The second one is the ergodic secrecy capacity of legitimate user, which can be expressed as follows:

$$\overline{C} = \mathbb{E}(C_{\text{secret}}). \quad (4)$$

In this paper, the VLC networks are evaluated by this two metrics.

III. Networks with Angle Diversity Transmitters

A. Angle Diversity Transmitter

In previous studies [8], angle diversity transmitters are introduced to improve physical layer security in VLC networks.

Each of the angle diversity transmitters considered in this study consists of several LED elements. In terms of multi-element LED, the first LED element is installed at the centre of a semi-sphere base. Then, rings of LED elements are installed around the central LED element with increasing radius. In this study, 7-element and 18-element angle diversity transmitters are considered.

With the use of angle diversity transmitters, narrow beam optical signals can be generated without complex beamforming algorithms. Parallel directional data transmissions can be realised by activating LED elements that cover only the areas occupied by active users. The remaining LED elements

generate constant light to provide room illumination. Therefore, angle diversity transmitters can fulfil the requirement for both uniform illumination and data communication to multiple users.

B. Performance Evaluation

In the system with angle diversity transmitters, in order to evaluate the SINR performance for each legitimate user, both intra-cell interference and inter-cell interference (ICI) are considered. Intra-cell interference originates from the active LED elements in the desired optical cell. ICI is the interference generated by the active LED elements in other optical cells. Hence, the SINR of the legitimate user k can be expressed as follows:

$$\gamma_k^{\text{legi}} = \frac{\left(\tau P_{\text{tx}} H_{k,m,\hat{c}}\right)^2}{\sigma^2 + \mathcal{I}_k^{\text{intra}} + \mathcal{I}_k^{\text{inter}}}, \tag{5}$$

where $H_{k,m,\hat{c}}$ is the channel attenuation between the desired LED element m and an active user k in the desired cell $\hat{c}$; $\mathcal{I}_{\text{intra}}$ denotes intra-cell interference and can be defined as follows:

$$\mathcal{I}_k^{\text{intra}} = \sum_{m' \neq m} \left(\tau P_{\text{tx}} H_{k,m'}\right)^2; \tag{6}$$

and $\mathcal{I}_{\text{inter}}$ denotes ICI and can be defined as follows:

$$\mathcal{I}_k^{\text{inter}} = \sum_{c'} \sum_{\hat{m}} \left(\tau P_{\text{tx}} H_{k,\hat{m},c'}\right)^2, \tag{7}$$

where m' is the index of active LED elements in the desired cell; $\hat{m}$ is the index of active LED elements in each interfering cell; c' is the index of the interfering cell. The SINR of the worst-case eavesdropper, γ_k^{eav}, can be described as follows:

$$\tilde{\gamma}_k^{\text{eav}} = \max_j \left(\frac{\left(\tau P_{\text{tx}} H_{j,m,\hat{c}}\right)^2}{\sigma^2 + \mathcal{I}_j^{\text{intra}} + \mathcal{I}_j^{\text{inter}}} \right), \tag{8}$$

where σ^2 is the noise power at an optical receiver.

IV. Networks with Protection Zone

In [13], the concept of 'protection zone' is proposed to enhance the physical layer security of wireless communication systems. In this study, in order to enhance the security performance, the concept of protection zone is adopted to the network using angle diversity transmitters. As shown in Fig. 2, each AP has its own protection zone. The protection zone is a round-shaped area which is defined as follows: the horizontal distance an AP and an arbitrary point inside the corresponding protection zone is less than D. Here, D is named as the radius of the protection zone.

It is also assumed that eavesdroppers can be detected in protection zone. In order to achieve this, sensors (such as motion sensors, heat sensors or HD camera) can be used to search the protection zone periodically. Alternatively, each protection zone can be surrounded by physical barrier such as glass walls, shelves etc. Sensors can be installed at the entrances of the barrier. These sensors can monitor and determine if any eavesdroppers enter/leave the protection zone.

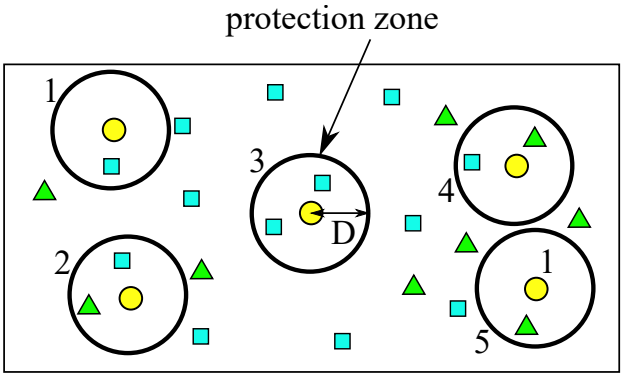

Fig. 2. A VLC network with protection zone. Each AP has a round-shaped protection zone. Yellow dot represents the AP with angle diversity transmitter. Blue rectangle represents legitimate user. Green triangle represents an eavesdropper. The indexes of APs are labelled in the figure. In this example, only the APs without eavesdroppers inside the protection zone (AP 1 & 3) are data-active and communicate with legitimate users.

TABLE I
Simulation Parameters

Optical transmission power of an AP, P_{tx}	2 W
Radius of a hexagonal cell, R_{cell}	4 m
Responsivity, τ	0.5 A/W
Gain of the optical filter, G	1
Refractive index, n	1.5
FOV of each optical receiver, Φ_{fov}	90^{o}
Physical area of a PD, A_{p}	0.1 cm^2
Receiver noise power, σ^2	-103.98 dBm

If eavesdroppers are detected inside the protection zone, all LED elements on the corresponding AP will stop data communication until eavesdroppers are no longer detected within the protection zone.

In this study, we assumed a practical backhaul-limited network. This means that each AP can only acquire the knowledge of eavesdroppers from its own protection zone. Each AP cannot acquire the knowledge of the eavesdroppers inside the protection zones from other APs.

With the use of protection zone, the area that eavesdroppers can perform wire-tapping is limited. It is expected that security performance of legitimate users in VLC networks can be improved by adding protection zones.

V. Results and Discussions

A. Simulation Setup

In the simulation, VLC networks with 7-element and 18-element angle diversity transmitters are evaluated. The half-intensity radiance angle of them is assumed to be 17^{o} and 10^{o}, respectively. These parameters ensure that the combined half-intensity radiance angle for all transmitters are identical. It is also ensured that the total transmission power of all transmitters are the same irrespective of the number of elements. Moreover, HEX and PPP deployment are evaluated in the simulation. All deployment are bounded by a $20 \times 10 \times 4$ m room where all APs are placed on the ceiling and all optical

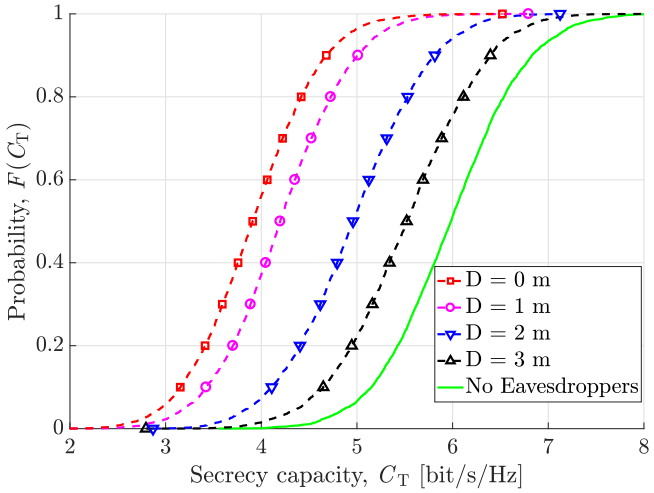

Fig. 3. The CDF of secrecy capacity of legitimate users in HEX networks with 7-element transmitters when different radius of protection zones are considered. The density of legitimate users and eavesdroppers is assumed as Λ_0. As the baseline, the scenario without eavesdroppers is also evaluated.

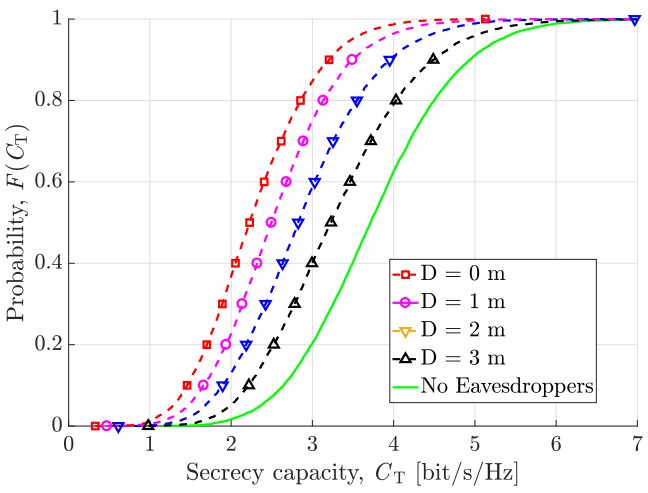

Fig. 4. The CDF of secrecy capacity of legitimate users in PPP networks with 7-element transmitters when different radius of protection zones are considered. The density of legitimate users and eavesdroppers is assumed as Λ_0. As the baseline, the scenario without eavesdroppers is also evaluated.

receivers are placed at the desk height, which is 1 m. For the purpose of fairness, the density of the APs in both deployments are the same, which is $\Lambda_0 = 1/A_{\mathrm{HEX}}$, where A_{HEX} is the area of an hexagonal cell. Also, legitimate users and eavesdroppers are assumed to follow 2-D homogeneous PPP with the density of Λ_{legi} and Λ_{eav}, respectively. Other simulation parameters are listed in Table I.

B. Results Analysis

The system performance of VLC networks are evaluated on the basis of over $100,000$ realisations of Monte Carlo simulations. The metrics used for the system analysis are the same metrics mentioned in Sec. II-C.

Fig. 3 shows the CDF of secrecy capacity of legitimate users in HEX networks equipped with 7-element transmitters. As a baseline, the scenario without eavesdroppers is also evaluated. It is notable that the security performance, as expected, improves when the radius of protection zones increases. This is because eavesdroppers are more likely to be detected if larger protection zones are used. Hence, legitimate users are safer to communicate with their desired APs. It can also be observed that when the radius of the protection zone increases from 0 m to 1 m, the improvement of secrecy capacity is marginal. When the radius of the protection zone increases from 1 m to 2 m, the improvement of secrecy capacity is significant. Moreover, when the radius of the protection zone is 3 m, the secrecy capacity of legitimate user is close to the secrecy capacity of the system without eavesdroppers. If we consider the scenario that $F(C_{\mathrm{T}}) = 0.5$, the system with protection zones ($D = 3$ m) achieves 40% secrecy capacity improvement over the same system without protection zones.

Fig. 4 shows the CDF of secrecy capacity of legitimate users in PPP networks equipped with 7-element transmitters. It is notable that, for PPP model, the secrecy capacity of all cases is lower than the secrecy capacity in HEX model. This is because, when APs follows Poisson point distribution, the interference degrades the overall system performance. Also, similar to HEX model, the security performance improves when the radius of protection zones increases. If we consider the scenario that $F(C_{\mathrm{T}}) = 0.5$, the system with protection zones ($D = 3$ m) achieves almost 50% secrecy capacity improvement over the same system without protection zones. In comparison with HEX network, PPP network can achieve more secrecy capacity improvement with the protection zones of the same size.

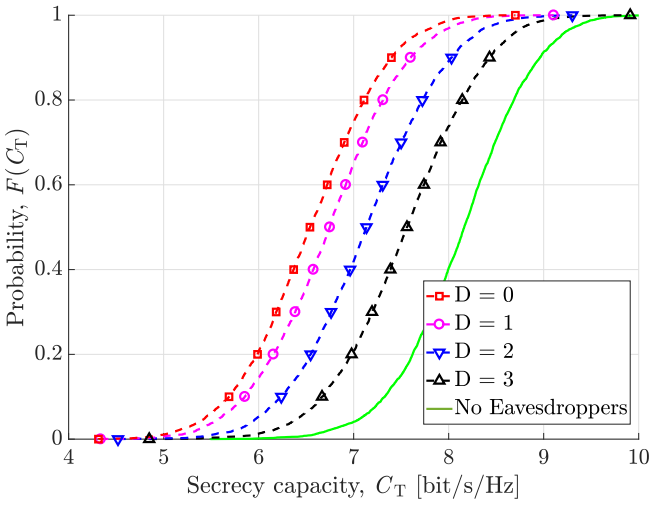

Fig. 5. The CDF of secrecy capacity of legitimate users in HEX networks with 18-element transmitters when different radius of protection zones are considered. The density of legitimate users and eavesdroppers is assumed as Λ_0. As the baseline, the scenario without eavesdroppers is also evaluated.

Fig. 5 shows the CDF of secrecy capacity of legitimate users in HEX networks equipped with 18-element transmitters.

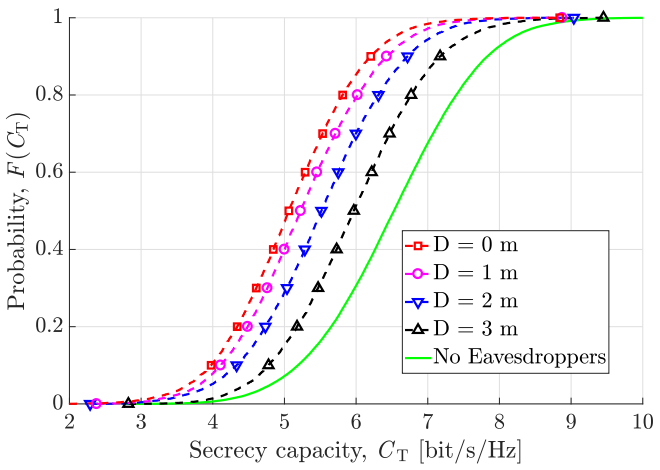

Fig. 6. The CDF of secrecy capacity of legitimate users in PPP networks with 18-element transmitters when different radius of protection zones are considered. The density of legitimate users and eavesdroppers is assumed as Λ_0. As the baseline, the scenario without eavesdroppers is also evaluated.

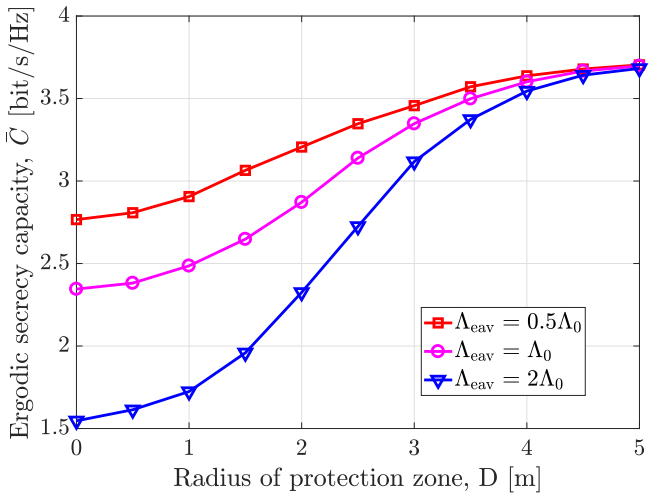

Fig. 7. The ergodic secrecy capacity of legitimate user in PPP networks with with 7-element transmitters. Three values of eavesdropper density are assumed, which are $0.5\Lambda_0$, Λ_0 and $2\Lambda_0$, respectively.

Compared with the scenario using 7-element transmitters, the secrecy capacity of this scenario improves. Also, the trend of secrecy capacity is similar to the previous scenarios. If we consider the scenario that $F(C_T) = 0.5$, the system with protection zones ($D = 3$ m) achieves 15% secrecy capacity improvement over the same system without protection zones.

Fig. 6 illustrates the CDF of secrecy capacity of legitimate users in PPP network equipped with 18-element transmitters. If we consider the scenario that $F(C_T) = 0.5$, the system with protection zones ($D = 3$ m) achieves 20% secrecy capacity improvement over the same system without protection zones.

Finally, Fig. 7 illustrates the ergodic secrecy capacity of legitimate user in PPP networks equipped with 7-element transmitters. Three values of eavesdropper density are evaluated. It can be observed that the ergodic secrecy capacity of all cases saturates at the same value (3.7 bit/s/Hz). This is because, if the protection zone is large enough, eavesdroppers can only wire-tap from a long distance which will not affect the security performance of legitimate users. Also, it is notable that, with the increase of the protection zone radius, the ergodic secrecy capacity increases more rapidly when eavesdropper density is higher. This means that the method of adding protection zones is more effective when the density of eavesdroppers is high.

VI. Conclusion

In this paper, we enhanced the physical layer security for VLC networks with angle diversity transmitters by adding protection zones. According to Monte Carlo simulation results, adding protection zones can significantly improve the secrecy capacity of legitimate users. In specific, 50% secrecy capacity improvement can be obtained by adding protection zones in the PPP network with 7-element angle diversity transmitters. Compared with the transmitter with more LED elements, transmitters with less LED elements can achieve more security improvement by adding protection zones. Also, it can be concluded that the system with PPP deployment can achieve more security improvement than the system with HEX deployment by adding protection zones. Finally, the method of adding protection zone to angle diversity transmitter systems is proven to be more effective when the density of eavesdroppers is high.

References

[1] Cisco Visual Networking Index, "Global Mobile Data Traffic Forecast Update, 2014-2019," White Paper, Feb. 2015. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html

[2] 3GPP, "RAN1 Chairmans Notes," Busan, Korea, 3GPP TSG RAN WG1 Meeting 93, May 2018.

[3] T. Borogovac, M. Rahaim, and J. B. Carruthers, "Spotlighting for Visible Light Communications and Illumination," in *IEEE Global Communications Conference (GLOBECOM 2010) Workshops*, 6-10 Dec 2010, pp. 1077–1081.

[4] H. Haas, L. Yin, Y. Wang, and C. Chen, "What is LiFi?" *J. Lightw. Technol.*, vol. 34, no. 6, pp. 1533–1544, March 2016.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[6] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Robust Key Generation From Optical OFDM Signal in Indoor VLC Networks," *IEEE Photon. Technol. Lett.*, vol. 28, no. 22, pp. 2629–2632, Nov 2016.

[7] A. Mostafa and L. Lampe, "Physical-Layer Security for MISO Visible Light Communication Channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, Sept 2015.

[8] Z. Chen and H. Haas, "Physical layer security for optical attocell networks," in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6.

[9] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 1, pp. 162–174, Jan 2018.

[10] C. Chen, D. A. Basnayaka, and H. Haas, "Downlink Performance of Optical Attocell Networks," *J. Lightwave Technol.*, vol. 34, no. 1, pp. 137–156, Jan 2016.

[11] J. M. Kahn and J. R. Barry, "Wireless Infrared Communications," *Proc. IEEE*, vol. 85, no. 2, pp. 265–298, Feb. 1997.

[12] I. Csiszár and J. Körner, "Broadcast Channels With Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[13] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "Phy layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2013.