Survey on Physical Layer Security in Optical Wireless Communication Systems

Mohanad Obeed*, Anas M. Salhab*, Mohamed-Slim Alouini+, and Salam A. Zummo*

*King Fahd University of Petroleum & Minerals, Dhahran, Eastern Province, Saudi Arabia
Email: {g201106250, salhab, zummo}@kfupm.edu.sa
+King Abdullah University of Science and Technology, Thuwal, Makkah Province, Saudi Arabia
Email: slim.alouini@kaust.edu.sa

***Abstract*—As the existing radio-frequency (RF) networks cannot meet the ever-increasing data rate demand, the optical wireless communication (OWC), which uses a wide untapped unregulated spectrum, has been proposed as a promising technology to overcome the RF spectrum limitations. On the other hand, with the increasing demand for high data rate and the prevalence of the broadcast-nature networks, researchers have recently come up with new mechanisms to improve secure communication using physical layer techniques. Compared to RF networks, the OWC networks are more secure and less susceptible to the interception because of the small coverage provided by LEDs, and because they work properly only in the presence of the line-of-sight (LoS) components. However, the security in OWC networks is still an issue, especially in visible light communication (VLC) when the transmitted information can be accessed by multiple users as in public areas, meeting rooms, laboratories, and libraries. That means potential eavesdroppers may be existing to gather confidential messages. This paper reviews all the conducted work on physical layer security (PLS) in two types of OWC networks, which are the VLC and free space optical (FSO) networks. Furthermore, the paper proposes several open problems in these networks to optimize and enhance the security performance.**

***Index Terms*—Physical layer security, visible light communication, free space optical communication.**

I. Introduction

The evolving explosion in high data rate services and applications has pushed the attention in the research community to utilize the untapped abundant unregulated voptical spectrum for communications to meet the fifth-generation (5G) and beyond traffic demand. The radio-frequency (RF) networks are proving to be scarce to cover the escalation in data rate services [1], and therefore, optical wireless communication (OWC) has emerged as a great potential solution or as a complementary to the existing RF networks to support the predicted traffic demand. Compared to their RF counterparts, OWC technologies can offer several advantages such as providing high data rates, rejecting RF interference, and providing energy-efficient wireless systems. Another additional unique feature of OWC is that the transmission can work properly only when the line-of-sight (LoS) component is available. In other words, the channel is deteriorated significantly if the LoS component is absent. Therefore, compared to RF networks, VLC networks are more secured and less susceptible to the interception because of the small coverage provided by LEDs, and because they work properly only in the presence of LoS components. However, the security in VLC networks is still an issue, especially, when the transmitted information can be accessed by multiple users as in public areas, meeting rooms, laboratories, shoping malls, and libraries. That means potential eavesdroppers may be existing to gather confidential messages [2].

Usually, the physical layer is used to provide a reliable communication to the legitimate destinations, while the upper layers of wireless networks are used to protect and secure the transmitted information [3]. However, due to the spread of the broadcast networks, new techniques using the physical layer have been emerged to improve the secure communications. Physical layer security (PLS) has been emerged as a promising technique to reduce the attained information at the eavesdroppers by exploiting the randomness of noise, channel-state-information (CSI), and different resources (like multi-antenna, and cooperative nodes) [4], [5]. The eavesdropper is an unauthorized user that tries to attain confessional information that is transmitted to an authorized user. The secrecy capacity metric was presented by Wyner [6] to evaluate the systems secrecy performance, and was defined as the highest information rate that can be attained at the legitimate destination with keeping the eavesdropper ignorant. To guarantee an accurate evaluation, eavesdroppers were assumed to have the complete knowledge of the network's parameters and have a sufficient computational capability.

OWC systems can use the spectrum of visible light, infrared, or ultraviolet as a propagation media. The systems that use the visible light are known as the visible light communication (VLC) systems, while the free space optical (FSO) systems use the spectrum of visible light, infrared, or ultraviolet for terrestrial point-to-point communications. Lasers or light emitting diodes are usually used as transmitters in OWC systems, while the receivers must be equipped with photo-detectors that can convert the received light intensity into a current signal.

In this paper, we review the conducted works on securing the FSO and VLC systems using the PLS mechanisms. Because of the unique properties of these technologies, the solutions that were provided in RF systems cannot be applied directly in OWC systems. Hence, many researchers focused their work on how to enhance the PLS in OWC systems with considering these properties. Up to our knowledge, there is no paper reviewed the security issue in OWC systems using the PLS mechanisms. For the PLS in the RF networks, we

refer the readers to the works in [7] and [8].

II. PLS IN FSO SYSTEMS

FSO systems use the optical spectrum to transmit high data rates between two fixed points over distances up to 10 Kilometers [9]. Compared to RF links, FSO links are characterized with much higher available bandwidth, resulting in high data rates. In addition, FSO systems are license-free systems, because they use the frequency greater than 300 GHz that is unlicensed. Because they use confined laser beams for transmitting data, FSO-based systems are more secure than both RF and VLC, more interference rejection, and the frequency can be reused with high reuse factor. However, the atmospheric turbulences, pointing error, scattering channels, and laser-beam divergence provide an opportunity to the eavesdroppers to have a version of the transmitted data. Hence, some researchers investigated the use of PLS to secure the FSO systems [10]–[19].

Lopez-Martinez *et al.* [10] characterized the PLS in point-to-point transmission with the presence of an eavesdropper. Because of the effects of both the laser-beam divergence and the turbulence-induces fading, possible eavesdropping mechanisms were discussed. They concluded that the eavesdropper can compromise the communication if he is close to the legitmate receiver or transmitter. Based on an experimental FSO link testbed that consists of one transmitter, one receiver, and one eavesdropper, authors of [11] estimated the secrecy rate, secrecy outage probability, and the expected code lengths that required for achieving a predefined secrecy rate. With such system model, authors of [12] evaluated the secure performance of the FSO link with IM/DD over Malaga turbulence channels. In [13], authors derived expressions for a lower bound of the instantaneous secrecy capacity, the average secrecy capacity and its lower bound, when on-off keying (OOK) IM/DD was applied and the FSO links suffered from turbulence-induced fading. With the eavesdropper being located outside the laser beam, authors of [14] studied the possibility of attaining the information by the eavesdropper through a non-LoS scattering channel.

To enhance the aggregated secrecy rate, Sun and Djordjevic [15] used the angular momentum multiplexing to improve the system performance under medium and weak turbulence scenarios. The acousto-optic deflectors were proposed in [16] to enhance the security, where the optical messages are sent through multiple beam paths between the transmitter and the legitimate receiver. The authors showed that the security is directly affected by the received intensity signal and the radius of the received beam. The authors in [17] evaluated the effective secrecy throughput (EST) of an FSO system that is consisted of multiple-aperture transmitter, multiple-aperture receiver, and multiple-aperture eavesdropper. They showed that the use of multiple-aperture at the transmitter is crucial to approach the optimal EST. In [18], authors verified that Bessel-Gaussian orbital angular momentum beams have more resiliency to atmospheric turbulence effects than Laguerre-Gaussian orbital angular momentum beams and concluded that optimizing the quality of these beams can provide a more secure communications. Authors of [19] fragmented the transmitted data and distributed the resulted fragments into different atmospheric channels, aiming at protecting confidential messages and improving the secure FSO systems.

PLS has also been investigated in mixed RF/FSO systems [20]–[25] using relaying schemes. Relaying schemes are an effective way to improve the secure communication systems [26], [27]. There are two scenarios of mixed RF/FSO systems, which are the uplink and downlink scenarios. In the uplink scenario, the information signals are transmitted from users through RF link to the relay node that converts the received signals to optical signals, multiplexes them, and forwards them through FSO link to the data center. In the downlink scenario, the information signals are transmitted through FSO link to the relay node that converts the received optical signals to RF signals and forwards them through RF link to the users. In both scenarios, authors assumed that the eavesdroppers target only the weakest link which is the RF link.

For the uplink scenario, Abd El-Malek *et al.* [20] analyzed the security-reliabiliy trad-off and derived some closed-form expressions, like the outage probability and average symbol error probability. The same authors studied the impact of the RF co-channel interference on the secrecy performance and optimized the transmit RF power [21], [28]. With considering the main and wiretap channels jointly, authors, in [22], studied the secrecy performance and derived expressions for the secrecy outage probability. The effects of imperfect CSI, misalignment, detection schemes, and relaying schemes on the secrecy outage performance were studied in [23]. With considering imperfect CSI for both RF and FSO links, Authors of [29] analyzed the secrecy outage performance for the SIMO RF/FSO, when the RF and FSO links were characterized as a Rayleigh and Gamma-Gamma channel, respectively. The same authors generalized their own work in [29] by modeling the FSO link by a Malaga distribution, and proposed transmit antenna selection schemes to improve the secrecy performance [30]. In [31], with the presence of multiple eavesdroppers, colluding and non-colluding eavesdropping scenarios were considered, where their CSI are unknown at the transmitter. Closed-form expressions were derived for the lower bound security outage probability and the strictly positive secrecy capacity.

For the dwnlink scenario, authors of [24] evaluated the secrecy capacity and the secrecy outage probability of the proposed system. In [25], authors studied the mixed FSO/RF system when both the legitimate receiver and eavesdropper decode the information and harvest the energy simultaneously from the second hop RF link. They analyzed the effects of the energy harvesting, pointing error, atmospheric turbulence, path loss, and the detection technology.

III. PLS IN VLC SYSTEMS

In this section, we focus the review on the PLS in VLC systems. VLC systems in indoor environment have two dual functions, which are the illumination and communication. Therefor, the illumination requirements should be considered in developing solution for PLS. In other words, unlike the RF channels, the optical intensity must be considered for the illumination requirements. Hence, in VLC channels, the

optical intensity is the constraint which is directly proportional to the electrical signal amplitude, not to the squared signal as in the RF channel.

Several articles have appeared in the literature to tackle the PLS in VLC networks, and many techniques have been proposed to evaluate and enhance the secure communications. Authors in [32] established examining the PLS in multiple-input single-output (MISO) VLC system with one authorized receiver and one eavesdropper. By exploiting the eavesdropper's CSI, the sources can cooperate to eliminate the received information at the eavesdropper, using zero-forcing precoding, while if the eavesdropper's CSI is unavailable, the transmitters devote a portion of the optical power for jamming the eavesdropper without confusing the authorized user. The same authors, in [33], assigned one LED for transmitting data while the other LEDs are assigned to transmit jamming signals that must be eliminated at the legitimate user. To strengthen the jamming signal, authors of [34] assigned multiple LEDs to build a protected zone, where the eavesdropper receives a poor SNR.

Authors of [35] found the optimal weighting vector at the light source transmitters by transforming the nonconvex problem into a solvable quasiconvex line search algorithm that provides a slightly better performance than the simpler zero-forcing algorithm [36], when CSI of the eavesdropper is known. On the other hand, if the eavesdropper's CSI is unknown, they estimated the channel of the eavesdropper and used the same approach used when the CSI is available. In [37], the beamforming and jamming vectors were optimized jointly to enhance the PLS in MISO-VLC-multiple eavesdropper system.

In [38], authors used massive low-intensity LEDs to design a beamformer the can steer the main lobes toward the ligetimate users and minimize it elsewhere. Authors of [39] and [40] studied how to transmit confidential information to two receivers in a MISO-VLC system with the presence of an eavesdropper. They applied the zero-forcing approach to eliminate the messages at the unauthorized users. In [41], authors proposed a new precoding scheme rather than the zero-forcing precoding approach for maximizing the secrecy sum rate in a multi-user MISO VLC system, when the transmitter wants to transmit K confidential messages to K users, and compared it with the zero-forcing precoding scheme to show the superiority. The proposed precoding scheme is to find the beamforming matrix from the eigenvectors related to the highest eigenvalues of the different K MISO-VLC channels.

The stochastic geometry were used to characterize the secure system and to derive analytical expressions for the secure communication metrics [42]–[45]. In [42], using the stochastic geometry method, authors derived the average secrecy rate and the secrecy outage probability in a single circle VLC cell containing multiple eavesdroppers that are randomly distributed based on the Poisson point process (PPP). A LED selection scheme was proposed in [43] to enhance the secrecy outage probability, using the PPP to model the randomness of the eavesdroppers locations. Using the PPP eavesdroppers' location modeling, in [44], authors analyzed the performance and optimized the beamforming vector for MISO-VLC system to improve the system secrecy. Due to the limited coverage area inherited in VLC systems, the beamforming vector optimizing for secrecy maximizing can be approximated by a LED selection, especially if the distance between the user and the eavesdropper is high [44]. Authors of [45] investigated the secrecy, when multiple eavesdroppers fuse their received signals using maximum ratio combining (MRC) for maximizing their total information-rate. The stochastic geometry was used to predict the secure communication performance under a predefined density of eavesdroppers. Authors of [46] characterized the ergodic secrecy rate and the secrecy outage probability for multi-user multi-cell VLC systems. They modeled the APs in the cieling as a two-dimensional homogeneous PPP, while another independent two-dimensional homogeneous PPP was used to model the users and the eavesdroppers at the floor.

Authors of [47] focused their work on the effect of the reflected in a MISO-VLC network and proposed an eavesdropping-resilient framework. In [48], authors showed that a small gap under the door, keyholes, or the window can be sufficient sources for eavesdropping. Authors of [49] showed how the non-LOS components have an impact on the secrecy outage probability with the presence of multiple randomly distributed eavesdroppers. It was shown that the secrecy performance affected by the legitimate user's location, LED transmitters' design, and the eavesdroppers' locations.

MIMO-VLC systems were investigated for secur communications [50]–[52]. A MIMO technology was applied to build a secure communication zone and minimize the bit-error-rate (BER) in the secured zone [50]. Authors of [51] optimized the covariance matrix and the signaling scheme for maximizing the achievable secrecy rate. The authors also derived an upper bound for the secrecy capacity. Authors of [52] used angle diversity transmitters, which are able to transmit signals in narrow beams, to effectively reduce the leakage of the confidential messages. They deduced that the the PPP optical network deployment is the worst in terms of secrecy, while the hexagonal deployment is the best.

Hybrid VLC/RF systems were investigated for the secure communication [53]–[55]. In [53], authors studied the PLS when both the eavesdropper and the legitimate user can aggregate the information from RF and VLC networks at the same time, when the RF and the VLC APs were multi-antenna and multi-LEDs, respectively. They optimized the power of transmission and the beamforming vectors at both APs to minimize the sum-power under rates constraints with having the eavesdropper's information rate nulled. Authors of [54] and [55] presented an exact and symptomatic secrecy outage probability for the uplink transmission in a system containing a single user and an eavesdropper. The VLC AP used for the downlink transmission, the legitimate user and the eavesdropper harvest the energy using the light intensity, and used it to transmit data by the RF link. The eavesdropper aimed at attain the transmitted information through the RF link. The authors showed that decreasing the LED height or increasing the circle area improves the secrecy performance. For more clarification and comparison between the proposed techniques in PLS of VLC systems, readers can refer to [56].

IV. Open Research Problems in PLS-OWC

Despite of all the aforementioned works that have been done in literature on PLS in OWCs, there are still some open problems and challenges that can be addressed in the future work. In the following, we suggest some ideas and open problems that help in improving the PLS in OWC systems:

- Evaluating the PLS in the downlink FSO/VLC systems. In these systems, the information is transmitted through FSO link to the relay node. This relay node must be equipped with LED and able to convert the received optical signal to other form of optical signal that meets the illumination requirements and the linear operational range of the transmitted LED. Because of the unique properties of VLC, studying the PLS in FSO/VLC systems is different from that in FSO/RF systems.
- Optimizing the beamforming vectors at relays in the mixed FSO/RF and FSO/VLC systems to maximize the secrecy rate. The optimization problem may depend on the distribution of RF or VLC APs and on the distribution of the legitimate users and eavesdroppers.
- Studying the PLS in hybrid RF/VLC networks, where the users and the eavesdroppers can be connected to either RF network or VLC network. In hybrid RF/VLC networks, the users are served either by RF APs or VLC APs, and each user must associate to the appropriate AP that maximize the system utility [57], [58]. Hence, from the security aspect, it is important to investigate and study this system model, where the proposed PLS techniques in the literature can be used and integrated with the problem of network assignment.
- Securing the newly emerging non-orthogonal multiple access (NOMA) technique in VLC networks is a new open research problem. Several new articles have been dedicated for securing NOMA in RF networks using PLS, but to date, no work has investigated the PLS in NOMA-VLC networks. Because of the unique features of VLC systems, optimizing and characterizing the PLS in NOMA-VLC systems is required.
- Employing the PLS to secure other OWC systems such as ultraviolet and infrared communication systems.

Acknowledgment

This work was supported by the Deanship of Scientific Research in King Fahd University of Petroleum & Minerals through grant number KAUST004. The authors would like also to acknowledge the KFUPM-KAUST research initiative resulted from this research work.

References

[1] M. Obeed, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Joint optimization of power allocation and load balancing for hybrid VLC/RF networks," *IEEE/OSA J. Opt. Commun. and Netw.*, 2018.

[2] A. Mostafa and L. Lampe, "Enhancing the security of VLC links: Physical-layer approaches," in *Summer Topicals Meeting Series (SUM), 2015*. IEEE, 2015, pp. 39–40.

[3] J. L. Massey, "An introduction to contemporary cryptology," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 533–549, 1988.

[4] X. Zhou, Y. Zhang, and L. Song, *Physical layer security in wireless communications*. Crc Press, 2016.

[5] M. Obeed and W. Mesbah, "Efficient algorithms for physical layer security in two-way relay systems," *Physical Communication*, vol. 28, pp. 78–88, 2018.

[6] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[8] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2017.

[9] M. A. Khalighi and M. Uysal, "Survey on free space optical communication: A communication theory perspective," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2231–2258, 2014.

[10] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photonics Journal*, vol. 7, no. 2, pp. 1–14, 2015.

[11] H. Endo, M. Fujiwara, M. Kitamura, T. Ito, M. Toyoshima, Y. Takayama, H. Takenaka, R. Shimizu, N. Laurenti, G. Vallone *et al.*, "Free-space optical channel estimation for physical layer security," *Optics express*, vol. 24, no. 8, pp. 8940–8955, 2016.

[12] M. J. Saber and S. M. S. Sadough, "On secure free-space optical communications over málaga turbulence channels," *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 274–277, 2017.

[13] J. Zhu, Y. Chen, and M. Sasaki, "Average secrecy capacity of free-space optical communication systems with on-off keying modulation and threshold detection," in *Information Theory and Its Applications (ISITA), 2016 International Symposium on*. IEEE, 2016, pp. 616–620.

[14] D. Zou and Z. Xu, "Information security risks outside the laser beam in terrestrial free-space optical communication," *IEEE Photonics Journal*, vol. 8, no. 5, pp. 1–9, 2016.

[15] X. Sun and I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," *IEEE Photonics Journal*, vol. 8, no. 1, pp. 1–10, 2016.

[16] M. Eghbal and J. Abouei, "Security enhancement in free-space optics using acousto-optic deflectors," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 6, no. 8, pp. 684–694, 2014.

[17] M. E. P. Monteiro, J. L. Rebelatto, R. D. Souza, and G. Brante, "Maximum secrecy throughput of MIMOME FSO communications with outage constraints," *IEEE Transactions on Wireless Communications*, vol. 17, no. 5, pp. 3487–3497, 2018.

[18] T.-L. Wang, J. A. Gariano, and I. B. Djordjevic, "Employing bessel-gaussian beams to improve physical-layer security in free-space optical communications," *IEEE Photonics Journal*, 2018.

[19] Q. Huang, D. Liu, Y. Chen, Y. Wang, J. Tan, W. Chen, J. Liu, and N. Zhu, "Secure free-space optical communication system based on data fragmentation multipath transmission technology," *Optics express*, vol. 26, no. 10, pp. 13 536–13 542, 2018.

[20] A. H. A. El-Malek, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Security-reliability trade-off analysis for multiuser SIMO mixed RF/FSO relay networks with opportunistic user scheduling," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 5904–5918, 2016.

[21] ——, "Physical layer security enhancement in multiuser mixed RF/FSO relay networks under RF interference," in *Wireless Communications and Networking Conference (WCNC), 2017 IEEE*. IEEE, 2017, pp. 1–6.

[22] H. Lei, Z. Dai, I. S. Ansari, K.-H. Park, G. Pan, and M.-S. Alouini, "On secrecy performance of mixed RF-FSO systems," *IEEE Photonics Journal*, vol. 9, no. 4, pp. 1–14, 2017.

[23] H. Lei, H. Luo, K. Park, Z. Ren, G. Pan, and M.-S. Alouini, "Secrecy outage analysis of mixed RF-FSO systems with channel imperfection," *IEEE Photonics Journal*, 2018.

[24] A. Kumar and P. Garg, "Physical layer security for dual-hop FSO/RF system using generalized $\gamma\gamma/\eta$- μ fading channels," *International Journal of Communication Systems*, vol. 31, no. 3, p. e3468, 2018.

[25] H. Lei, Z. Dai, K.-H. Park, W. Lei, G. Pan, and M.-S. Alouini, "Secrecy outage analysis of mixed RF-FSO downlink SWIPT systems," *arXiv preprint arXiv:1806.01895*, 2018.

[26] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE transactions on signal processing*, vol. 58, no. 3, pp. 1875–1888, 2010.

[27] M. Obeed and W. Mesbah, "Efficient algorithms for physical layer security in one-way relay systems," *Wireless Networks*, pp. 1–13, 2018.

[28] A. H. A. El-Malek, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Effect of rf interference on the security-reliability tradeoff analysis of

multiuser mixed rf/fso relay networks with power allocation," *Journal of Lightwave Technology*, vol. 35, no. 9, pp. 1490–1505, 2017.

[29] H. Lei, Z. Dai, I. S. Ansari, K. Park, M.-S. Alouini *et al.*, "On secrecy performance of mixed rf-fso systems," *IEEE Photonics Journal*, 2017.

[30] H. Lei, H. Luo, K.-H. Park, G. Pan, I. S. Ansari, and M.-S. Alouini, "On secure mixed rf-fso systems with tas and imperfect csi," *arXiv preprint arXiv:1809.01503*, 2018.

[31] K. O. Odeyemi and P. A. Owolawi, "Physical layer security in mixed rf/fso system under multiple eavesdroppers collusion and non-collusion," *Optical and Quantum Electronics*, vol. 50, no. 7, p. 298, 2018.

[32] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Communications (ICC), 2014 IEEE International Conference on*. IEEE, 2014, pp. 3342–3347.

[33] ——, "Securing visible light communications via friendly jamming," in *Globecom Workshops (GC Wkshps), 2014*. IEEE, 2014, pp. 524–529.

[34] C.-W. Chow, Y. Liu, C.-H. Yeh, C.-Y. Chen, C.-N. Lin, and D.-Z. Hsu, "Secure communication zone for white-light LED visible light communication," *Optics Communications*, vol. 344, pp. 81–85, 2015.

[35] A. Mostafa and L. Lampe, "Optimal and robust beamforming for secure transmission in MISO visible-light communication links," *IEEE Trans. Signal Processing*, vol. 64, no. 24, pp. 6501–6516, 2016.

[36] ——, "Physical-layer security for MISO visible light communication channels," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1806–1818, 2015.

[37] H. Shen, Y. Deng, W. Xu, and C. Zhao, "Secrecy-oriented transmitter optimization for visible light communication systems," *IEEE Photonics Journal*, vol. 8, no. 5, pp. 1–14, 2016.

[38] A. Mostafa and L. Lampe, "Pattern synthesis of massive LED arrays for secure visible light communication links," in *Communication Workshop (ICCW), 2015 IEEE International Conference on*. IEEE, 2015, pp. 1350–1355.

[39] T. V. Pham and A. T. Pham, "On the secrecy sum-rate of MU-VLC broadcast systems with confidential messages," in *Communication Systems, Networks and Digital Signal Processing (CSNDSP), 2016 10th International Symposium on*. IEEE, 2016, pp. 1–6.

[40] ——, "Secrecy sum-rate of multi-user MISO visible light communication systems with confidential messages," *Optik-International Journal for Light and Electron Optics*, vol. 151, pp. 65–76, 2017.

[41] M. A. Arfaoui, A. Ghrayeb, and C. Assi, "Achievable secrecy sum-rate of the MISO VLC broadcast channel with confidential messages," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.

[42] G. Pan, J. Ye, and Z. Ding, "On secure VLC systems with spatially random terminals," *IEEE Communications Letters*, vol. 21, no. 3, pp. 492–495, 2017.

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

[44] ——, "Securing visible light communication systems by beamforming in the presence of randomly distributed eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. PP, no. 99, pp. 1–1, 2018.

[45] ——, "Physical layer security in visible light communication systems with randomly located colluding eavesdroppers," *IEEE Wireless Communications Letters*, 2018.

[46] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 1, pp. 162–174, 2018.

[47] X. Liu, X. Wei, L. Guo, Y. Liu, and Y. Zhou, "A new eavesdropping-resilient framework for indoor visible light communication," in *Global Communications Conference (GLOBECOM), 2016 IEEE*. IEEE, 2016, pp. 1–6.

[48] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The spy next door: Eavesdropping on high throughput visible light communications," in *Proceedings of the 2Nd International Workshop on Visible Light Communications Systems*. ACM, 2015, pp. 9–14.

[49] S. Cho, G. Chen, H. Chun, J. P. Coon, and D. OBrien, "Impact of multipath reflections on secrecy in VLC systems with randomly located eavesdroppers," 2018.

[50] H. Le Minh, A. T. Pham, Z. Ghassemlooy, and A. Burton, "Secured communications-zone multiple input multiple output visible light communications," in *Globecom Workshops (GC Wkshps), 2014*. IEEE, 2014, pp. 505–511.

[51] M. A. Arfaoui, A. Ghrayeb, and C. Assi, "On the achievable secrecy rate of the mimo vlc gaussian wiretap channel," in *Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017 IEEE 28th Annual International Symposium on*. IEEE, 2017, pp. 1–5.

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

[53] M. F. Marzban, M. Kashef, M. Abdallah, and M. Khairy, "Beamforming and power allocation for physical-layer security in hybrid RF/VLC wireless networks," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International*. IEEE, 2017, pp. 258–263.

[54] G. Pan, J. Ye, and Z. Ding, "Secure hybrid VLC-RF systems with light energy harvesting," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4348–4359, 2017.

[55] ——, "Secrecy outage analysis of hybrid VLC-RF systems with light energy harvesting," in *Signal Processing Advances in Wireless Communications (SPAWC), 2017 IEEE 18th International Workshop on*. IEEE, 2017, pp. 1–5.

[56] M. Obeed, A. M. Salhab, M.-S. Alouini, and S. A. Zummo, "On optimizing vlc networks for downlink multi-user transmission: A survey," *arXiv preprint arXiv:1808.05089*, 2018.

[57] M. Obeed, A. M. Salhab, S. A. Zummo, and M.-S. Alouini, "Joint load balancing and power allocation for hybrid VLC/RF networks," in *Proc. IEEE Global Commun. Conf. (Globecom)*, Singapore, 2017.

[58] X. Li, R. Zhang, and L. Hanzo, "Cooperative load balancing in hybrid visible light communications and WiFi," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1319–1329, 2015.