On the Secrecy Performance of a Hybrid RF/VLC System

I. W. Gomes da Silva, D. P. Moya Osorio, E. E. Benitez Olivo, I. Ahmed, and M. Katz

***Abstract*— This paper evaluates the secrecy outage probability of a hybrid radio frequency (RF) and visible light communication (VLC) network in the presence of an eavesdropper. We assume that data is transmitted over the RF and VLC links following a proposed multiplexing scheme in which the data sent by the source is split with a certain allocation ratio. Furthermore, the legitimate and eavesdropper users are assumed to have multihoming capabilities, so that they are able to receive data from both RF and VLC access points, simultaneously. We derive integral-form exact expression, as well as a closed-form asymptotic expression for the secrecy outage probability and validate them via Monte Carlo simulations. Our results show that multiplexing the information signal by both links leads to an enhancement of the secrecy performance since it opportunistically takes advantages of the best characteristics of both domains.**

***Keywords*— Hybrid RF/VLC, physical layer security, secrecy outage probability, Visible light communications.**

I. Introduction

As the fifth-generation (5G) of wireless communications is globally introduced, research efforts are carried out for the development of its successor, the sixth-generation (6G), which is expected to provide extremely high data throughput, virtually zero-latency services and immense cognition capabilities [1]. Although 6G is still in early stages of research, it is expected that it will be required to exploit frequencies beyond 100 GHz to alleviate the scarcity of spectrum. Thus, with an unlicensed frequency range from 400-800 THz, visible-light communications (VLCs) have attracted considerable attention as an enabling technology for 6G networks due to the advancement in white light-emitting diodes (LEDs) and the capability of providing illumination and data transmission simultaneously, in addition to high energy efficiency and longer lifespan [2]. However, numerous challenges must be addressed for the deployment of VLC in practical scenarios. Among them, we can cite the limited coverage and instability of the link quality [3], which can severely impact the performance. To overcome those limitations, hybrid scenarios have been proposed in order to combine the benefits of VLC and radio-frequency (RF) communications [4], [5]. For instance, in [5], a reconfigurable optical and RF wireless network was presented, in which the system is capable of dynamically adopting the best mode for transmission based on predefined handover rules, e.g., link failures or local policies. In [4], a comparison between a hybrid RF/VLC system and a stand-alone VLC network was performed. It was shown a remarkable gain in terms of average connectivity and system throughput.

Moreover, with the introduction of disruptive technologies and novel services, 6G networks must assure a high level of security and privacy, so that traditional cryptography-based techniques might not be suitable or enough for some applications, especially those of constrained scenarios, e.g. limited hardware and restricted computing power [6] . Hence, physical layer security (PLS) techniques might found a new horizon on 6G to provide security by efficiently exploiting the randomness of wireless channels.In this regard, there exists special interest in investigating PLS techniques on VLC networks under secrecy constraints [7], [8]. Particularly, in [7], upper and lower bounds for the secrecy capacity of an indoor VLC network in the presence of an eavesdropper were derived. In [8], the secrecy outage probability (SOP) of a VLC network with imperfect channel state information (CSI) in the presence of an eavesdropper was investigated. Hybrid VLC/RF scenarios under secrecy constraints have been investigated in [9], [10]. The work in [9] investigated the secrecy performance in terms of the average secrecy capacity of a hybrid RF/VLC network in the presence of an eavesdropper. To ensure security, therein it was proposed a link-selection scheme based on the availability of a positive secrecy rate on the VLC link. In [10], a PLS algorithm was proposed based on zero-forcing beamforming to mitigate the eavesdropper from receiving data from both VLC and RF.

Despite the research efforts so far, security issues for hybrid RF/VLC systems have been barely investigated. Therefore, this paper intends to contribute in filling this gap by investigating the SOP of an indoor hybrid RF/VLC network in the presence of an eavesdropper. The main contributions of the paper are: i) We propose a multiplexing scheme where the data sent by the source is split according to an allocation ratio; ii) An integral-form expression for the SOP was derived to assess the key system parameters' effect on the network performance; iii) A closed-form asymptotic expression of the SOP is obtained to assess the diversity order of the system. Moreover, we corroborate our analytical expressions via Monte Carlo simulations.

Notation: Herein, we use $f_X(\cdot)$ and $F_X(\cdot)$ to denote the probability density function (PDF) and cumulative density function (CDF) of a random variable X, and $\mathbb{E}[\cdot]$ to denote expectation; $I_0(\cdot)$ and $Q_1(\cdot;\cdot)$ stands for the zero-order modified Bessel function of the first kind [11, Eq. 8.447.1] and the first order Marcum Q function [12, Eq. 4.34], respectively; and $[x]^+ = \max(x, 0)$.

I. W. Gomes da Silva and E. E. Benitez Olivo are with the São Paulo State University (UNESP), Campus of São João da Boa Vista, São João da Boa Vista-SP, Brazil, E-mails: iwg.silva@unesp.br, edgar.olivo@unesp.br.;

D. P. Moya Osorio, I. Ahmed and M. Katz are with the Centre of Wireless Communications, University of Oulu, Oulu, Finland, E-mails: diana.moyaosorio@oulu.fi, iqrar.ahmed@oulu.fi, marcos.katz@oulu.fi.

II. System Model

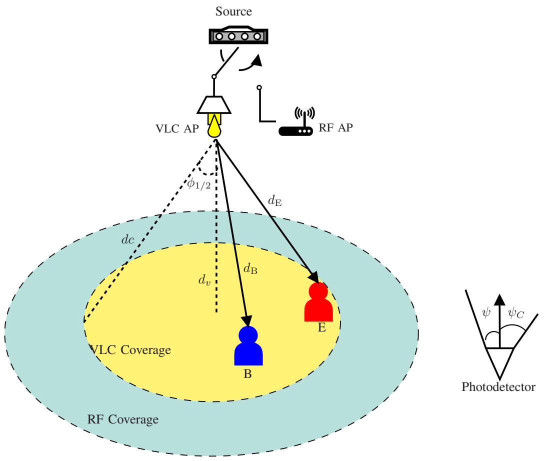

Fig. 1: System Model

We assume an indoor downlink hybrid VLC/RF communication network under secrecy constraints, as illustrated in Fig. 1. In our model, we consider a source S that communicates with a legitimate user B in the presence of an eavesdropper user E through RF or VLC access points (APs). B and E are assumed to be equipped with an RF front-end and a photodetector (PD), as well as having multihoming capabilities, i.e., these users can receive data from both APs simultaneously. Furthermore, the VLC and RF coverage area are assumed to overlap [13].

A. RF Channel Model

To account for the possible Line-of-Sight (LoS) component in an indoor scenario, all RF links are considered to undergo Rician Fading [14]. Hence, the channel coefficients between S→B and S→E, denoted by $h_{\rm B}^{\rm rf}$ and $h_{\rm E}^{\rm rf}$, respectively, are modeled with shape factor K_i and scale parameter equal to the average channel gain of the corresponding link, $\Omega_i{=}\mathbb{E}\{|h_i^{\rm rf}|^2\}$, with $i \in \{{\rm B},{\rm E}\}$. Under these considerations, the received signal at B and E are expressed as

$$y_i^{\rm rf}(t) = \sqrt{P^{\rm rf}}s^{\rm rf}(t)h_i^{\rm rf}(t) + n_i^{\rm rf}(t) \tag{1}$$

where $s^{\rm rf}(t)$ is the information signal and $P^{\rm rf}$ is the total transmit power of the RF AP, $n_i^{\rm rf}(t)$ is the additive white Gaussian noise (AWGN) at the RF front-end of the receivers, with average power N_0. The noise samples $\{n^{\rm rf}(t)\}$ are assumed to be independent and identically distributed. Moreover, we assume that the information signal $s^{\rm rf}(t)$ has mean power normalized to unity, that is $\mathbb{E}\{|{\rm s}^{\rm rf}(t)|^2\}{=}1$. We also consider a block-fading channels, so that $h_i^{\rm rf}(t)$ stays fixed during one transmission frame and changes independently from one frame to another. For notation simplicity, consider $g_i^{\rm rf}{\triangleq}|h_i^{\rm rf}|^2$ for $i \in \{{\rm B},{\rm E}\}$ as the channel gains. Hence, the signal-to-noise ratio (SNR) received at B and E are given by $\gamma_i^{\rm rf}{=}\gamma_P g_i^{\rm rf}$ with $i \in \{{\rm B},{\rm E}\}$, where $\gamma_P{=}P^{\rm rf}/N_0$ is the total transmit system SNR with respect to the RF transmitter.

B. VLC Channel Model

For VLC, we consider an intensity modulation/direct detection (IM/DD) scheme. Besides, both B and E are equipped with PDs, responsible to generate an electrical current proportional to the intensity of the collected light. Moreover, as pointed out in [15], in typical indoor scenarios, the majority of the collected energy at the VLC PD comes from the LoS component. Therefore, we assume that the VLC channel is flat with a dominant line-of-sight component, and the channel gain does not vary during the data transmission as long as the receivers remain stationary. Accordingly, the received signal at the PD of B and E at a time instant t is given as follows

$$y_i^{\rm vlc}(t) = s^{\rm vlc}(t)h_i^{\rm vlc} + n_i^{\rm vlc}(t), \tag{2}$$

where $s^{\rm vlc}(t) \in \mathbb{R}^+$ is the emitted intensity by the LED, whose average value is upper bounded as $\mathbb{E}\{s^{\rm vlc}\}{=}P^{\rm vlc}$ due to safety concerns. Moreover, $h^{\rm vlc} \in \mathbb{R}^+$ is the optical channel gain which is time invariant and depends only on the users positions, and $n_i^{\rm vlc}(t)$ is the noise component. Thus, the channel gain of the VLC link can be expressed as [16]

$$h_i^{\rm vlc} = \frac{(m+1)AD(\psi)r^2 d_v^{m+1}}{2\pi \sin^2(\psi_C)\, d_i^{m+3}}, \tag{3}$$

where d_i, with $i \in \{{\rm B},{\rm E}\}$ is the distance from the transmitter to the receiver, d_v is the vertical distance between the AP and the floor, A denotes the physical detector area, ψ and ψ_C are the angle of incidence with respect to the normal axis of the receiver plane, and the field of view (FOV) angle of the PD, respectively, $D(\psi)$ is the gain of the optical filter, r is the refractive index, and $m{=}{-}1/\log_2(\cos(\phi_{1/2}))$ represents the order of Lambertian emission, with $\phi_{1/2}$ being the LED half intensity view angle. Considering the optical-to-electrical conversion, the SNR received at B and E through the VLC AP is given by [17]

$$\gamma_i^{\rm vlc} = \frac{\left(\rho P^{\rm vlc} h_i^{\rm vlc}\right)^2}{k^2 N_0}, \tag{4}$$

where ρ is the optical-to-electrical conversion efficiency of the PD, and k is the ratio between the average optical power and the average electrical power of the transmitted signal.

III. Performance Analysis

In this section, we present an analytical expression for the exact secrecy outage probability of the considered hybrid RF/VLC system. To this end, we begin revising the definition of the secrecy capacity C_s as the difference between the channel capacities of the legitimate and wiretap channels. Thus, the secrecy capacity for the RF and VLC channel are given, respectively, by [18], [19]

$$C_s^{\rm rf} = [C_{\rm L}^{\rm rf} - C_{\rm E}^{\rm rf}]^+ = \log_2\left(\frac{1+\gamma_{\rm B}^{\rm rf}}{1+\gamma_{\rm E}^{\rm rf}}\right), \tag{5}$$

$$C_s^{\rm vlc} = \frac{1}{2}[C_{\rm L}^{\rm vlc} - C_{\rm E}^{\rm vlc}]^+ = \frac{1}{2}\left[\log_2\left(\frac{1+c^2\gamma_{\rm B}^{\rm vlc}}{1+c^2\gamma_{\rm E}^{\rm vlc}}\right)\right]^+, \tag{6}$$

where c is a constant, related to the distribution of the VLC signal, $s^{\rm vlc}$ [20].

A. Secrecy Outage Probability

For the proposed setup, the system secrecy is in outage if the secrecy capacity C_s is less than a target secrecy rate, $\mathcal{R}_s$. As both users are assumed to have multihoming capabilities, we propose a multiplexing-based transmission scheme in which the data streams are split according to the ratio δ:$(1{-}\delta)$, with $\delta \in (0,1)$, and transmitted over the RF and VLC links simultaneously in each frame. This is feasible since the light and RF waves do not cause interference on each other [21]. We further consider that, for both links, the maximum achievable rate is set as the channel secrecy capacity, that is, $\mathcal{R}^i{=}C_s^i$, with $i \in \{\mathrm{rf}, \mathrm{vlc}\}$. Accordingly, the total transmission rate in each frame is given by the sum of the transmission rates of both links. Thus, the SOP can be written from (5) and (6) as

$$\begin{aligned}\mathrm{SOP} &= \Pr(C_s < \mathcal{R}_s) = \Pr(\delta C_s^{\mathrm{rf}} + (1-\delta) C_s^{\mathrm{vlc}} < \mathcal{R}_s) \\ &= \Pr\Big(C_s^{\mathrm{rf}} < \alpha\Big) = \Pr\Big(\frac{1+\gamma_{\mathrm{B}}^{\mathrm{rf}}}{1+\gamma_{\mathrm{E}}^{\mathrm{rf}}} < 2^{\alpha}\Big). \end{aligned} \tag{7}$$

where $\alpha{=}\frac{\mathcal{R}_s-(1-\delta)C_s^{\mathrm{vlc}}}{\delta}$.

Proposition 1. *The exact SOP of a hybrid RF-VLC system in the presence of an eavesdropper is given by*

$$\begin{aligned}\mathrm{SOP} = 1 - \int_0^{\infty} Q_1\left(\sqrt{2\mathrm{K}_{\mathrm{B}}}, \sqrt{\frac{2\Big((\gamma_P g_{\mathrm{E}}^{\mathrm{rf}}+1)2^{\alpha}-1\Big)}{(\mathrm{K}_{\mathrm{B}}+1)^{-1}\gamma_P \Omega_{\mathrm{B}}}}\right) \\ \times \frac{(\mathrm{K}_{\mathrm{E}}+1) e^{-\frac{g_{\mathrm{E}}^{\mathrm{rf}}(\mathrm{K}_{\mathrm{E}}+1)}{\Omega_{\mathrm{E}}} - \mathrm{K}_{\mathrm{E}}} I_0\left(2\sqrt{\frac{g_{\mathrm{E}}^{\mathrm{rf}} \mathrm{K}_{\mathrm{E}}(\mathrm{K}_{\mathrm{E}}+1)}{\Omega_{\mathrm{E}}}}\right)}{\Omega_{\mathrm{E}}} dg_{\mathrm{E}}^{\mathrm{rf}}. \end{aligned} \tag{8}$$

Proof: To obtain the integral-form expression for the SOP of the system, we first rewrite (7) as

$$\begin{aligned}\mathrm{SOP} &= \Pr\Big(g_{\mathrm{B}}^{\mathrm{rf}} < \frac{\big(\gamma_P g_{\mathrm{E}}^{\mathrm{rf}}+1\big)2^{\alpha}-1}{\gamma_P} | g_{\mathrm{E}}^{\mathrm{rf}} > 0\Big) \Pr(g_{\mathrm{E}}^{\mathrm{rf}} > 0) \\ &= \int_0^{\infty} F_{g_{\mathrm{B}}^{\mathrm{rf}}}\left(\frac{2^{\alpha}\left(\gamma_P g_{\mathrm{E}}^{\mathrm{rf}}+1\right)}{\gamma_P} - \frac{1}{\gamma_P}\right) f_{g_{\mathrm{E}}^{\mathrm{rf}}}(g_{\mathrm{E}}^{\mathrm{rf}}) dg_{\mathrm{E}}^{\mathrm{rf}}. \end{aligned} \tag{9}$$

Given that h_i^{rf}, $i \in \{\mathrm{B}, \mathrm{E}\}$ undergo Rician fading, the respective channel gains g_i^{rf} $i \in \{\mathrm{B}, \mathrm{E}\}$, follow a non-central chi-squared distribution. Thus, after some simplifications, (8) can be achieved.

B. Asymptotic SOP

To gain a better insight into the secrecy diversity order attained by the investigated system, its secrecy outage behavior at high SNR is determined in the following proposition.

Proposition 2. *An asymptotic closed-form expression for the SOP of a hybrid RF-VLC system in the presence of an eavesdropper is given by* (10)*, shown at the top of the next page.*

Proof: By considering the high SNR regime (i.e., as $\gamma_P{\rightarrow}\infty$) (9) can be rewritten as

Table I: Simulation Parameters

RF subsystem	
Transmit SNR, γ_P	20 dB
Path Loss Exponent, φ	1.8
VLC subsystem	
Vertical distance, d_v	2.5 m
Field of view (FOV) at PD, ψ_C	90°
Average emitted power, P^{vlc}	9 W
Physical area of PD, A	1 cm^2
Responsivity of PD, ρ	0.53 A/W
Refractive index, r	1.5
Optical filter gain, $D(\psi)$	1
LED half intensity view angle, $\phi_{1/2}$	60°
Noise power spectral density,N^{vlc}	10^{-21} A^2/ Hz
Elect./opt. power conversion, k	3
Constant c	$\sqrt{e/2\pi}$

$$\mathrm{SOP}^{\infty} = \int_0^{\infty} F_{g_B^{\mathrm{rf}}}\left(2^{\alpha} g_E^{\mathrm{rf}}\right) f_{g_E^{\mathrm{rf}}}(g_E^{\mathrm{rf}}) dg_E^{\mathrm{rf}}. \tag{11}$$

Thus, based on [22, Eq. 3.5] and after the proper substitutions and some simplifications, (10) can be obtained.

Remark 1. Note from (10) that the asymptotic outage performance of the system is independent of γ_P. Consequently, the system's secrecy diversity order is zero.

IV. Numerical results and discussions

In this section, the analytical expressions derived in Section III are evaluated through illustrative samples and validated via Monte Carlo simulations. For this purpose, we considered that the users' positions are given by $d_i{=}d_v/\cos(\phi_i)$, with $i \in \{\mathrm{B}, \mathrm{E}\}$. Moreover, the average channel gains of the RF links are assumed to be determined by the path loss, i.e., $\Omega_i{=}d_i^{-\varphi}, i \in \{\mathrm{B}, \mathrm{E}\}$, and the target secrecy rate is set to $\mathcal{R}_s{=}1$ bps/Hz. Furthermore, unless otherwise specified, Table I summarises the considered values for the system parameters.

Fig. 2 illustrates the SOP as a function of the transmit SNR at the RF AP, γ_P, for two different splitting ratios $\delta{=}0.2, 0.8$ and different combinations of the K-factors K_{B} and K_{E}, with $d_{\mathrm{B}}/d_{\mathrm{E}}{=}0.6$. Moreover, we fixed the position of E at the edge of the VLC AP coverage. Note that our analytical expression perfectly matches the simulation results. Also, our derived asymptotic expression in (10) is independent of γ_P, so that the SOP presents a saturation baseline at high SNR. Interestingly, note that, for $K_{\mathrm{B}}{=}K_{\mathrm{E}}{=}20$ dB, that is, when both B and E have stronger LoS components, the best secrecy performance is achieved for both values of δ. Furthermore, as expected, the worst secrecy performance is observed when K_{B}=0 dB. On the other hand, we can also note that, in terms of δ, there is an enhancement in secrecy by allocating more rate to the VLC link if both RF channels have a strong LoS component, while for the other cases, the difference is minimal.

In Fig. 3, it is illustrated the SOP vs. the splitting ratio, δ for different combinations of the K-factors, K_{E} and K_{B}, with $d_{\mathrm{B}}/d_{\mathrm{E}}{=}0.6$ and 1. As previously observed in Fig. 2, with B closer to the source, better performance is achieved

$$\mathrm{SOP}^{\infty}=\frac{\exp\left(-\frac{(\mathrm{K_B}+1)\mathrm{K_E}\Omega_{\mathrm{E}}2^{\alpha}+\mathrm{K_B}(\mathrm{K_E}+1)\Omega_{\mathrm{B}}}{(\mathrm{K_B}+1)\Omega_{\mathrm{E}}2^{\alpha}+(\mathrm{K_E}+1)\Omega_{\mathrm{B}}}\right)I_0\left(\frac{2\sqrt{\frac{\mathrm{K_B}(\mathrm{K_B}+1)\mathrm{K_E}(\mathrm{K_E}+1)2^{\alpha}}{\Omega_{\mathrm{B}}\Omega_{\mathrm{E}}}}}{\frac{(\mathrm{K_B}+1)2^{\alpha}}{\Omega_{\mathrm{B}}}+\frac{\mathrm{K_E}+1}{\Omega_{\mathrm{E}}}}\right)}{(\Omega_{\mathrm{B}}(\mathrm{K_E}+1))^{-1}((\mathrm{K_B}+1)\Omega_{\mathrm{E}}2^{\alpha}+(\mathrm{K_E}+1)\Omega_{\mathrm{B}})}-Q_1\left(\sqrt{\frac{2\mathrm{K_E}}{\frac{(\mathrm{K_E}+1)\Omega_{\mathrm{B}}2^{-\alpha}}{(\mathrm{K_B}+1)\Omega_{\mathrm{E}}}+1}},\sqrt{\frac{2\mathrm{K_B}(\mathrm{K_E}+1)\Omega_{\mathrm{B}}}{(\mathrm{K_B}+1)\Omega_{\mathrm{E}}2^{\alpha}+(\mathrm{K_E}+1)\Omega_{\mathrm{B}}}}\right) \tag{10}$$

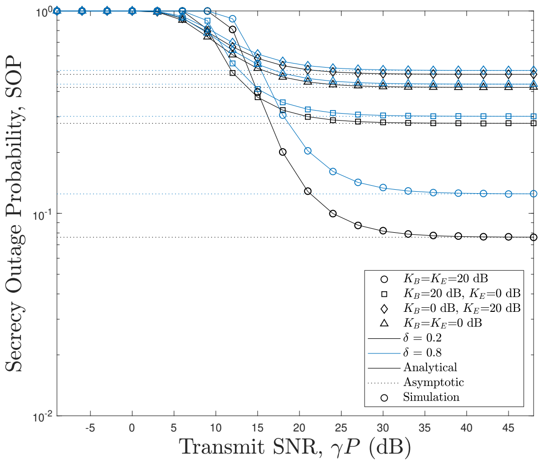

Fig. 2: Secrecy Outage Probability, SOP vs transmit SNR, for different combinations of the K-factor K_{E} and K_{B} and δ=$0.2, 0.8$ with $d_{\mathrm{B}}/d_{\mathrm{E}}$=$0.6$.

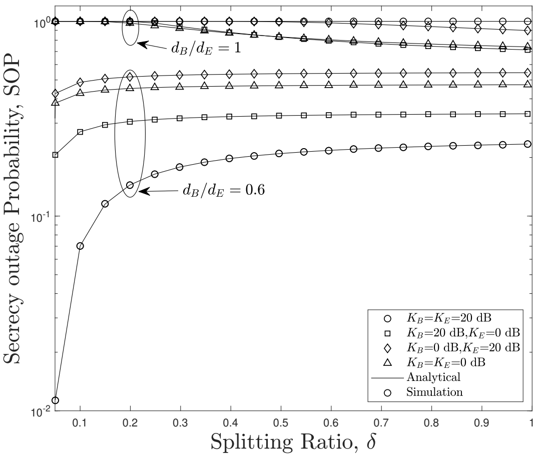

Fig. 3: Secrecy Outage Probability, SOP vs Rate allocation ratio, δ for different combinations of the K-factor K_{E} and K_{B} and $d_{\mathrm{B}}/d_{\mathrm{E}}$=$0.6, 1$.

when the K-factor of both channels is high. Also note that, for lower values of δ, the impact of LoS available on the RF links, especially on B, is more significant, as expected given that, in those conditions, the RF link is the main source of leakage to E. Moreover, it can be observed that, it is better to allocate more rate for the VLC link in terms of secrecy. On the other hand, with both B and E located at the edge of the VLC coverage, better performance is obtained as more data rate is allocated to the RF link, since according to (6), the secrecy capacity of the VLC link is based on the position of the nodes and it is only positive if B is closer to the source than E. In this case, the performance is slightly improved when E has a smaller LoS component.

Fig. 4 illustrates the SOP vs. the distance ratio between receiver nodes, $d_{\mathrm{B}}/d_{\mathrm{E}}$, for different splitting ratios δ=$0.2, 0.5, 0.8$. We also consider K_{B}=K_{E}=10 dB. As expected, when B is much closer to the source than E, that is for distance ratios lower than 0.6, more rate being allocated to the VLC AP results in a better secrecy performance. On the other hand, with 0.6<$d_{\mathrm{B}}/d_{\mathrm{E}}$<$1$ and γ_P=30 dB, there is an inversion on the behaviour, and it becomes better for the secrecy of the system to transmit more data rate through the RF link, highlighting the advantages of combining both techniques for transmission. However, as B leaves the VLC coverage, the system is always in outage. Moreover, the scenario with γ_P=10 dB presents a better performance only when B is positioned beneath the source and δ=0.2, since, for this case, the RF link acts mostly as a source of leakage to E.

In Fig. 5, the SOP is illustrated as a function of the VLC access point LED half intensity view angle, $\phi_{1/2}$, from 30° (minimum diffusion) to 70° (maximum diffusion) [23], considering different rate allocation ratios δ=$0.2, 0.5, 0.8$ and γ_P=10 and 30 dB, with K_{B}=K_{E}=10 dB. We have considered d_{B}=d_v. It is worth reminding that the distance between the source and the nodes is also related to $\phi_{1/2}$. Therefore, we assumed E fixed, with the distance between S and E given by d_{E}=$d_v/\cos(\pi/4)$ m, thus being out of the VLC link coverage for values of $\phi_{1/2}$<$\pi/4$ and within coverage for the rest values. Therein, Note that lower values of $\phi_{1/2}$ result in a reduced field of view for VLC and provides a better secrecy performance for smaller values of δ, that is, with more rate being allocated to the VLC link as E is outside the VLC coverage. Also, a lower value of $\phi_{1/2}$ results in a higher optical concentrator gain, which, consequently, enhances the signal strength of the receiver. Furthermore, as previously observed in Fig. 4, the case with γ_P=10 dB achieves a better secrecy performance when $\phi_{1/2}$ is very small ($< 35°$). Finally, except for the case with δ=0.2, for larger values of $\phi_{1/2}$, the scenario with γ_P=30 dB presents a better secrecy performance for all the cases studied, as expected.

V. Conclusion

This paper investigated the performance of a hybrid RF/VLC system in terms of the secrecy outage probability in the presence of an eavesdropper by assuming a multiplexing-based scheme, where the rate is split between RF and VLC links according to a splitting ratio. Furthermore, the legitimate and eavesdropper users are assumed to have multihoming

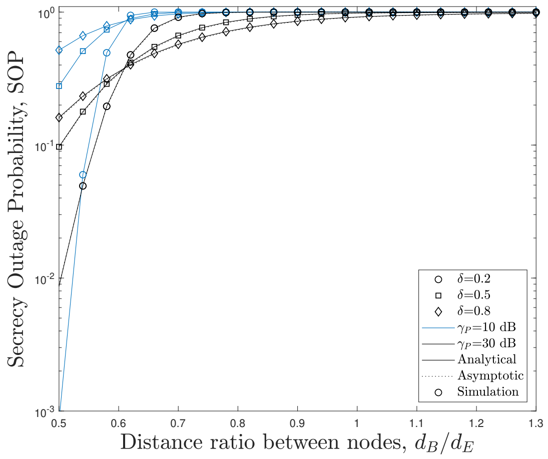

Fig. 4: Secrecy Outage Probability, SOP vs Distance ratio between nodes, $d_{\mathrm{B}}/d_{\mathrm{E}}$ for different splitting ratios δ=0.2, 0.5, 0.8 and γ_P=10,30 dB, with K_{B}=K_{E}=10 dB.

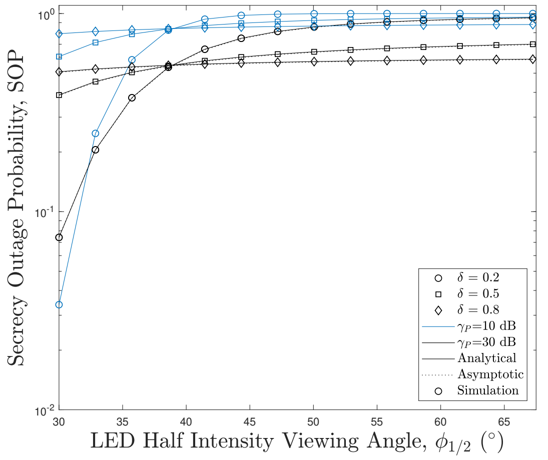

Fig. 5: Secrecy Outage Probability, SOP vs LED half intensity view angle, $\phi_{1/2}$ for different rate allocation ratios δ=0.2, 0.5, 0.8 and γ_P=10, 30 dB, with K_{B}=K_{E}=10 dB.

capabilities, so that they are able to receive data from both APs simultaneously. Exact and asymptotic analytical expressions for the SOP were derived and validated via Monte Carlo simulations. The results showed that when B is located closer to the source, a better performance is attained by allocating more data rate to the VLC link. However, the LoS component of the RF channel can highly impact the secrecy performance. Furthermore, different values of the transmit power at the RF link, γ_P, the LED half intensity view angle, $\phi_{1/2}$, and the position of the legitimate receiver regarding the eavesdropper greatly impact on the secrecy performance of the system. This can be explored by sending more bits via the RF or VLC link, thus reinforcing the advantages of combining both transmission technologies to enhance the secrecy performance.

References

[1] G. Wikström, J. Peisa, P. Rugeland, N. Johansson, S. Parkvall, M. Girnyk, G. Mildh, and I. L. Da Silva, "Challenges and technologies for 6G," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5.

[2] N. Chi, Y. Zhou, Y. Wei, and F. Hu, "Visible light communication in 6G: Advances, challenges, and prospects," *IEEE Vehicular Technology Magazine*, vol. 15, no. 4, pp. 93–102, 2020.

[3] D. A. Basnayaka and H. Haas, "Design and analysis of a hybrid radio frequency and visible light communication system," *IEEE Trans. on Commun.*, vol. 65, no. 10, pp. 4334–4347, 2017.

[4] H. Chowdhury and M. Katz, "Cooperative data download on the move in indoor hybrid (radio-optical) WLAN-VLC hotspot coverage," *Trans. on Emerging Telecommun. Technol.*, vol. 25, no. 6, pp. 666–677, 2014.

[5] M. S. Saud, I. Ahmed, T. Kumpuniemi, and M. Katz, "Reconfigurable optical-radio wireless networks: Meeting the most stringent requirements of future communication systems," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 2, p. e3562, 2019.

[6] D. P. M. Osorio, E. E. B. Olivo, H. Alves, and M. Latva-Aho, "Safeguarding MTC at the physical layer: Potentials and challenges," *IEEE Access*, vol. 8, pp. 101 437–101 447, 2020.

[7] J. Wang, C. Liu, J. Wang, Y. Wu, M. Lin, and J. Cheng, "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," *IEEE Trans. on Commun.*, vol. 66, no. 12, pp. 6423–6436, 2018.

[8] J. Y. Wang, Y. Qiu, S. H. Lin, J. B. Wang, M. Lin, and C. Liu, "On the secrecy performance of random VLC networks with imperfect CSI and protected zone," *IEEE Systems Journal*, vol. 14, no. 3, pp. 4176–4187, 2020.

[9] A. Kumar, P. Garg, and A. Gupta, "PLS analysis in an indoor heterogeneous VLC/RF network based on known and unknown CSI," *IEEE Systems Journal*, vol. 15, no. 1, pp. 68–76, 2021.

[10] 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 *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2017, pp. 258–263.

[11] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. Elsevier/Academic Press, Amsterdam, 2007.

[12] M. K. Simon and M.-S. Alouini, *Digital communication over fading channels*. John Wiley & Sons, 2005, vol. 95.

[13] F. Wang, Z. Wang, C. Qian, L. Dai, and Z. Yang, "Efficient vertical handover scheme for heterogeneous VLC-RF systems," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 7, no. 12, pp. 1172–1180, 2015.

[14] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. on Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, 2012.

[15] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights," *IEEE Trans. on Consumer Electronics*, vol. 50, no. 1, pp. 100–107, 2004.

[16] J. R. Barry, J. M. Kahn, W. J. Krause, E. A. Lee, and D. G. Messerschmitt, "Simulation of multipath impulse response for indoor wireless optical channels," *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 3, pp. 367–379, 1993.

[17] Y. Wang and H. Haas, "Dynamic load balancing with handover in hybrid li-fi and wi-fi networks," *Journal of Lightwave Technology*, vol. 33, no. 22, pp. 4671–4682, 2015.

[18] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. on Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[19] A. Chaaban, Z. Rezki, and M. Alouini, "Fundamental limits of parallel optical wireless channels: Capacity results and outage formulation," *IEEE Trans. on Commun.*, vol. 65, no. 1, pp. 296–311, 2017.

[20] A. Lapidoth, S. M. Moser, and M. A. Wigger, "On the capacity of free-space optical intensity channels," *IEEE Trans. on Inf. Theory*, vol. 55, no. 10, pp. 4449–4461, 2009.

[21] M. Hammouda, S. Akln, A. M. Vegni, H. Haas, and J. Peissig, "Hybrid RF/VLC systems under QoS constraints," in *2018 25th International Conference on Telecommunications (ICT)*, 2018, pp. 312–318.

[22] R. Price, "Some non-central F-distributions expressed in closed form," *Biometrika*, vol. 51, no. 1/2, pp. 107–122, 1964. [Online]. Available: http://www.jstor.org/stable/2334200

[23] M. H. Khadr, A. Abd El Aziz, H. A. Fayed, and M. Aly, "Bandwidth and BER improvement employing a pre-equalization circuit with white LED arrays in a MISO VLC system," *Applied Sciences*, vol. 9, no. 5, 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/5/986