IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 26 September 2022, accepted 22 October 2022, date of publication 28 October 2022, date of current version 9 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3218049

RESEARCH ARTICLE

Security Performance Analysis of a NOMA-Assisted Underwater VLC System Under Imprecise Channel Estimations

AMBRISH KUMAR[1], SAIF AL-KUWARI[2], (Senior Member, IEEE), DUSHANTHA NALIN K. JAYAKODY[1,3], (Senior Member, IEEE), AND REEM ALKANHEL[4], (Member, IEEE)

[1]Center for Telecommunication Research, School of Postgraduate Studies and Research, Sri Lanka Technological Campus, Padukka 110007, Sri Lanka
[2]Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, Doha, Qatar
[3]COPELABS, Lusófona University, 1749-024 Lisbon, Portugal
[4]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia

Corresponding author: Dushantha Nalin K. Jayakody (nalin.jayakody@ieee.org)

This work was supported in part by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R323), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia; by the Fundação para a Ciência e a Tecnologia, Portugal under Grant No.: UIDB / 04111/2020 (COPELABS); and in part by the Sri Lanka Technological Campus, Sri Lanka, under Grant RRSG.22.0714.1 and Grant RRSG.22.0612.2.

ABSTRACT The accurate estimation of underwater Visible Light Communication (VLC) channel conditions is challenging due to its widespread attenuation and scattering effects. The channel attenuation is a linear function of frequency and causes exponential signal power loss whereas due to the scattering effect, numerous photons are statistically generated as light beams strike water molecules and there arise security concerns. Assuming realistic underwater conditions, this paper investigates the security performance of a typical Non-Orthogonal Multiple Access (NOMA)-assisted underwater VLC system. It consists of a Floating Vehicle Transmitter (FVT), equipped with multiple Light Emitting Diodes (LEDs) to transmit the signal to two legitimate near-end and far-end Underwater Vehicles (UVs) in presence of an active/passive eavesdropper. The Channel State Information (CSI) of each transmitting link is estimated with the use of a Minimum Mean Square Error (MMSE) technique. Furthermore, we propose a LED selection mechanism to select an LED that can achieve the highest secrecy rate defined under the constraints of known and unknown CSI of legitimate and/or eavesdropping links. Using the Successive Interference Cancellation (SIC) technique, a novel closed-form secrecy outage probability expressions for the conventional single-LED and multi-LED NOMA-VLC links for both known and unknown CSI scenarios is derived. The security performance of the proposed multi-LED NOMA-VLC system is compared with the conventional single-LED NOMA-VLC system under the effect of air bubbles for both fresh and salty water. Finally, we verify the validity of the numerical results through Monte-carlo simulation analysis.

INDEX TERMS Non-orthogonal multiple access, physical layer security, secrecy capacity, secrecy outage probability and underwater visible light communication.

I. INTRODUCTION

Underwater Optical Wireless Communication (OWC) is rapidly gaining popularity among both academia and industry due to the expansion of underwater activities, such as underwater scientific data collection, underwater sensor networks, unmanned underwater vehicles, etc. [1]. Unlike traditional acoustic communications, underwater Visible Light Communication (VLC) is expected to provide a high-speed data transmission rate with reliable, secure, and low-latency metrics. However, attenuation and scattering are two widespread concerns the OWC networks, which affect the overall

The associate editor coordinating the review of this manuscript and approving it for publication was Hassan Omar.

performance of the underwater VLC system. Therefore, in [3], a modified Beer-Lambert formula was derived especially for the underwater VLC link that incorporates both *attenuation* and *scattering* effects unlike the conventional Beer-Lambert formula derived in [4] which did not include the scattering effect. Indeed, the attenuation effect causes signal power loss whereas due to the scattering effect, when a light beam (i.e. operating at blue/green light wavelength band 450 nm to 550 nm) originated at VLC transmitter strikes a water molecule, numerous photons are statistically generated and start traveling in random directions [1], [2], [3], [4], [5], [6]. This as a consequence may cause an insecurity issue in the underwater VLC system because a scattered photon may received by an illegitimate receiver (or eavesdropper). Considering the security as a key metric, it is important to track the scattered photon location, which indeed requires the channel estimations of realistic underwater conditions.

The overall attenuation effect in the realistic underwater channel conditions, not only causes signal power loss but also moderates the VLC channel connectivity with mobile end-users [7]. In order to improve the user connectivity between transceivers, Multiple Input Multiple Output (MIMO) technology that utilizes multiple Light Emitting Diodes (LEDs) can be used [8]. However, due to small-area transmission coverage of VLC technology [9], each transmitting LED cannot be accessed by a mobile user. Then, for further improvement in the underwater VLC network connectivity, the transmitter can select a number of LEDs that are perfectly aligned with the receiver terminal. However, it again depends on the channel estimation analysis to know the exact user location [10].

Recently, Non-Orthogonal Multiple Access (NOMA) has emerged as another potential technology that can serve multiple users at the same time/frequency/code by minimizing the attenuation effect [4]. The fundamental concept of NOMA is based on superposition coding and successive decoding where the superposition coding of multiple users' signals can be done over the same subcarrier with different power levels. As a consequence, it enables the receiver to decode the signal by using the Successive Interference Cancellation (SIC) technique [11]. At the receiver terminal, the SIC starts by decoding the data of the user that have the strongest channel connectivity with the transmitter. Once the strongest user's signal is decoded, then the detected data is passed through to an iterative SIC method. Then, the other user's signal is reconstructed based on the prior knowledge of the CSI of this next user after the first user's signal is subtracted from the superimposed signal [12]. This indeed avoids the interference caused by the first user's signal and increases accuracy in decoding another user's signal. In particular, in the NOMA scheme, the power coefficients among multiple users can either be arbitrarily chosen or power can be intentionally allocated to optimize a preferable performance e.g. minimizing the secrecy outage probability and/or maximizing the capacity, secrecy capacity, and other objectives [13], [14].

On the other hand, due to the scattering effect, less number of scattered photons enter the Field-of-View (FOV) of the authenticated (legitimate) user while there is a high probability that some of the scattered photons might be incident on the FOV of the unauthenticated user (eavesdropper) [15], [16], [17], [18]. Thus, the underwater VLC systems have a requirement for security performance analysis. The security in OWC systems can be provided through either the conventional Cryptographic technique that can be applied at the network layer or the Physical Layer Security (PLS) technique, which is applicable at the physical layer itself [19]. More specifically, the PLS technique provides Information Theoretic Security (ITS) at a quantum level by exploiting the properties of the physical layer whereas the Cryptographic technique is based on encryption and decryption methods following a secrete code. Therefore, Wyner [20] first time used the PLS technique and proposed a wiretapper channel model by defining a positive secrecy rate metric that can provide the optimum guarantee to prevent eavesdropping attacks up at this particular rate [21], [22]. However, the major limitation of the Wyner model was the assumption that the legitimate channel conditions are always stronger than the eavesdropping channel conditions and the transmitter can easily obtain a positive secrecy rate. In fact, this assumption is not reliable in underwater communication scenarios because here scattering is a major cause of insecurity occurrence and hence, eavesdroppers can also realize the stronger channel conditions. Therefore, in PLS analysis instantaneous CSI estimation analysis is a key requirement in order to track the light propagation paths that are approaching the legitimate and/or eavesdropper's FOVs.

In the OWC systems, due to the fact that the user node which might be either a legitimate node or an eavesdropper one, can estimate the CSI of its receiving link during the pilot symbol transmission process. In this process, some known pilot symbols are been sent by the transmitter over each transmitting link [23]. Then, whenever the transmitter demands, the user may or may not send its estimated CSI knowledge to it. In practice, it can be assumed that a legitimate user always sends its CSI to the transmitter [24]. Whereas, an eavesdropper will send its CSI to the transmitter depending on whether it is an active user (i.e. a legitimate node of the adjacent network that sends its CSI to the transmitter) or a passive user (i.e. a malicious node that never shares its CSI with transmitter) [25]. Recently, in [26], a secure NOMA-assisted multi-LED underwater VLC network is presented where the secrecy rate metric is defined against both active and passive eavesdropping attacks with an assumption that an error-free CSI estimation is possible at the receiver node. However, due to the variable underwater channel conditions and the occurrence of Gaussian distribution errors, the precise error-free CSI estimation at the receiver node is practically impossible [27]. Therefore, in the PLS, it is important to formulate the secrecy rate according to imprecise channel estimations so that the transmitter can prevent both active and passive eavesdropping attacks in a strategic manner. To the

best of our knowledge, no prior research has been conducted that address the adverse scattering effects from a security perspective, specifically for underwater VLC system.

In this paper, we assume that due to the scattering phenomenon, the underwater VLC system is vulnerable in the presence of an active/passive eavesdropper. In order to estimate the exact knowledge of the eavesdropper's availability, imprecise channel estimations are needed in each transmission time interval. The main contributions of this paper can be summarized as follows:

- Present the geometry of the light propagation mechanism of the underwater VLC model and derive the approximate channel gain expressions for both direct and scattered paths, respectively.
- Derive the Probability Density Function (PDF) and Cumulative Distribution Function (CDF) expressions of the received end-to-end signal-to-interference noise ratio (SINR) of each legitimate and eavesdropper links.
- A Minimum Mean Square Error (MMSE) technique is used to estimate the CSI knowledge of CSI of both legitimate and eavesdropping links. Then, according to the availability or non-availability of CSI of both legitimate and eavesdropping links, a LED selection mechanism is defined to select the LED with the highest secrecy rate.
- This paper considers the Exponential Generalized Gamma (EGG) distribution to model to measure the received signal fluctuations while considering the underwater turbulence effects because it can provide the excellent agreement between the theoretical and experimental results.
- Derive novel closed-form secrecy outage probability expressions for conventional single-LED as well as multi-LED transmission strategies, for both eavesdropping scenarios.
- Finally, computer-based simulation analysis is performed to validate each plotted numerical result.

The remainder of the paper is organized as follows. The system and channel model are presented in Section II. Additionally, a detailed description of the light propagation underwater VLC model and LED selection mechanism are presented in the same section. The performance metrics of the conventional single-LED and the proposed multi-LED transmission strategies are defined in Section III. In Section IV, the numerical results are demonstrated for the security performance of the proposed NOMA-assisted underwater VLC system and Section V concludes the findings of this paper.

II. SYSTEM AND CHANNEL MODEL

Suppose a floating vehicle transmitter (T_x) transmits signals towards legitimate near-end (M_1) and far-end (M_2) underwater vehicles (UVs), in the presence of an active and/or passive eavesdropping UV (E_k). Let T_x be equipped with N transmitting LEDs, whereas M_1 and M_2 are equipped with a photo-detector (PD) node, as shown in Fig. 1. In NOMA scheme, two signals X_1 and X_2 overlap with different power

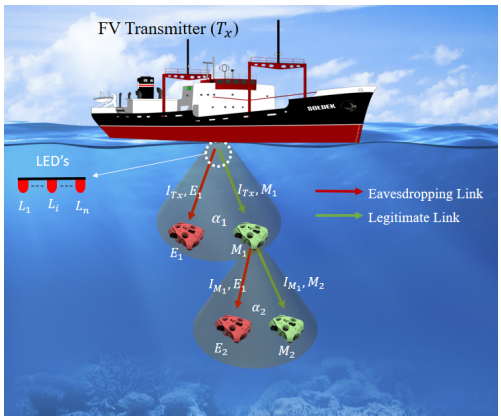

FIGURE 1. System model of underwater visible light communication.

levels. Each signal is encoded as $(R_{b,k}, R_{s,k})$, when $R_{b,k}$ is defined as a fixed transmission rate parameter and $R_{s,k}$ is defined as a desired secrecy rate quantity. The signal received at the UVs can be expressed as

$$Y_{z_1}(t) = \eta I^r \left(\sqrt{\alpha_1 P_s} X_1 + \sqrt{\alpha_2 P_s} X_2\right) h_{z_1}(t) + W_{z_1}(t), \quad (1a)$$

$$Y_{z_2}(t) = \eta I^r \sqrt{\alpha_2 P_s} X_2 h_{z_2}(t) + W_{z_2}(t), \quad (1b)$$

where $z_k \in \{M_k, E_k\}$ and $k \in \{1, 2\}$, $\hat{h}_{z_k}$ is the imprecise channel gain, α_1 and α_2 are the power allocation coefficients. From the security perspective, the confidential signal of user M_1 should be hidden below the signal of user M_2. Also, more power is allocated to user M_2 under the condition that $\alpha_2 > \alpha_1$ when $\alpha_1 + \alpha_2 = 1$, with transmit power P_s at T_x. η denotes the responsivity and I is denoted as the real valued irradiance fluctuations of the corresponding link. The value of r is related to the used detection technique at the user terminal, which means that $r = 1$ when Heterodyne Detection (HD) technique is used whereas $r = 2$ when Intensity Modulation/Direct Detection (IM/DD) technique is used by the receiving UV terminal [3]. Finally, W_z is defined as a complex Additive White Gaussian Noise (AWGN) parameter with zero-mean and variance $\sigma_{z_k}^2$.

A. LIGHT PROPAGATION MODEL

The geometry of light propagation VLC model is depicted in Fig. 2, which illustrates that the optical signal at z_k^{th} UV can be received via two separate paths, namely Line-of-Sight (LoS) (or direct) path and scattering (indirect or NLoS) path following FVT-to-Scatterer and Scatterer-to-Z_k links. Let minimum mean square error (MMSE) estimation technique is used to estimate the CSI of each transmitting links under imprecise channel conditions. According to light propagation geometry, the channel-gain at the z_k^{th} UV can be given as [24]

$$\hat{h}_{z_k} = \beta_{z_k} h_{z_k}^g h_{z_k}^s + \sqrt{1 - \beta_{z_k}^2} w_{z_k}, \quad (2)$$

where β_{z_k} is denoted as correlation coefficient between $h_{z_k}^{g/s}$ and $\hat{h}_{z_k}$, here, $h_{z_k}^g$ is the geometric underwater VLC link channel gain in fresh water when no turbulence is present

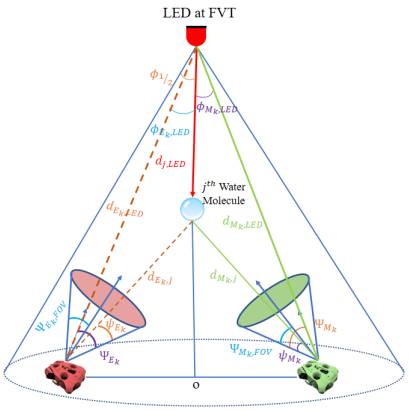

FIGURE 2. Geometry of light propagation VLC model, where light propagated over a direct path under fresh water conditions while follows scattered path under turbulent (or salty) water conditions.

whereas $h^s_{z_k}$ is the scattered link channel gain obtained under error-free channel conditions and w_{z_k} is the Gaussian random error independent to $\hat{h}_{z_k}$ with zero-mean and unit variance. Moreover, the β_{z_k} can be given as [25]

$$\beta_{z_k} = \frac{1}{1+\alpha P_s T_t}, \tag{3}$$

where T_t is the length of pilot symbol transmission and α is the normalized pilot power. When $T_t = 1$ and hence, the effect of channel estimation solely characterized by α.

1) CHANNEL GAIN UNDER FRESH WATER CONDITIONS

The direct underwater VLC link gain $h^g_{z_k}$ can be given by [25]

$$h^g_{z_k} = \Xi^{\text{LoS}}_{z_k,L_i} \cos^m(\phi_{z_k,L_i}) \cos^m(\psi_{z_k,L_i}), \tag{4}$$

for $0 \le \psi_{z_k,LED} \ge \Psi_{i,LED}$ and 0 otherwise, where

$$\Xi^{\text{LoS}}_{z_k,L_i} = \frac{A(m+1)}{2\pi d^2_{z_k,L_i}} \text{U}(\psi_{z_k}) \text{g}(\psi_{z_k}), \tag{5}$$

where $\text{U}(\psi_{z_k})$ is denoted as optical filter gain and $\text{g}(\psi_{z_k})$ is the gain of the optical concentrator given by

$$\text{g}(\psi_{z_k}) = \begin{cases} \frac{n^2}{\sin^2 \Psi_{z_k}}, & 0 \le \psi_{z_k} \ge \Psi_{z_k,\text{FoV}} \\ 0, & \text{Otherwise}, \end{cases} \tag{6}$$

where n denotes the refractive index, $\Psi_{z_k,\text{FoV}}$ denotes the FOV of the z^{th}_k UV, A is the detector area, m is the Lambertian radiation pattern which can be given by $m = -\frac{1}{\log(\cos(\phi_{1/2}))}$, where $\phi_{1/2}$ is the semi-angle of each transmitting LED. Therefore, the directivity of the transmitting LED is related to semi-angle $\phi_{1/2}$ and at $\phi_{1/2} = 60°$, m becomes unity, which corresponds to ideal LED. d_{z_k,L_i} is the Euclidian depth from the FVT to z^{th}_k.

2) CHANNEL GAIN OVER TURBULENT CONDITIONS

The scattering effect in underwater medium causes two major effects: i) the light beam deviates from its original path which means that it may or may not incident on the legitimate user's FOV and causes probability of eavesdropping occurrence, and ii) it reduces the mean irradiance of light beam at the receiver terminal that indeed reduces the received signal strength at the UV and might deteriorate the system performance. As a consequence, two paths between transceivers can be constructed i.e. LED-to-Scatterer and Scatterer-to-Z^{th}_k receiver path. Therefore, an approximate expression for scattering channel gain $h^s_{z_k}$ can be derived as

$$h^s_{z_k} = \Xi^{\text{Scatter}}_{z_k,j,L_i} \text{U}(\psi_{z_k}) \text{g}(\psi_{z_k}) \cos^m(\phi_{j,L_i}) \cos^m(\psi_{z_k,j}), \tag{7}$$

for $0 \le \psi_{z_k,j} \le \Psi_{z_k}$ and 0 otherwise, where

$$\Xi^{\text{Scatter}}_{z_k,j,L_i} = \frac{A(m+1)\exp\left[-c\left(d_{j,L_i} + d_{z_k,j}\right)\right]}{2\pi\left(d_{j,L_i} + d_{z_k,j}\right)^2}, \tag{8}$$

where d_{j,L_i} and $d_{z_k,j}$ are the Euclidian depth from the FVT to the j^{th} scattering molecule and scattering molecule to the z^{th}_k user. Moreover, the overall attenuation effect in transmitting light beam can be defined by extinction coefficient c denoted as $c = a + b$, here, a is defined as an absorption coefficient, and b is defined as a scattering coefficient and their values can be chosen as constant for a particular wavelength of the signal during performance analysis of the proposed underwater VLC network.

In order to extract the relevant information from the overlapped signal X_k, the UV utilizes the SIC technique. In this technique, when demodulating the X_2 signal, the X_1 signal is viewed as an interference signal. However, when demodulating the signal X_1, the X_2 signal is first demodulated and then re-modulated after subtracting the interfering signal from the overlapped signal. Assuming that both E_k and M_k UVs are having the same decoding capabilities, then, by using (1a), Signal-to-Interference plus Noise Ratio (SINR) obtained at M_1 and E_1, can be defined as

$$\gamma^{X_2}_{M_1} = \frac{\alpha_2 \rho \hat{h}_{M_2}}{\wp \alpha_1 \rho \hat{h}_{M_1} + 1}, \gamma^{X_1}_{M_1} = \frac{\alpha_1 \rho \hat{h}_{M_1}}{\wp \alpha_2 \rho \hat{h}_{M_2} + 1}, \tag{9a}$$

$$\gamma^{X_1}_{E_1} = \frac{\alpha_1 \rho \hat{h}_{E_1}}{\wp \rho \hat{h}_{E_1} + 1}. \tag{9b}$$

where $\rho = \frac{\eta I^r P_s}{2\sigma^2}$ and level is residual interference is denoted by $\wp = \in (0, 1]$. Let both M_2 and E_2 can access the second transmission phase, which is an interference-free signal then, by using (1b), the SNR received at M_2 and E_2, can be defined as

$$\gamma^{X_2}_{M_2} = \alpha_2 \rho \hat{h}_{M_2}. \tag{10a}$$

$$\gamma^{X_2}_{E_2} = \alpha_2 \rho \hat{h}_{E_2}. \tag{10b}$$

B. LED SELECTION MECHANISM

Any LED available at the transmitter can transmit the information. During pilot symbol transmission process, some known pilot symbols are been transmitted by the FVT T_x over each transmitting link. Then, the MMSE technique is used to receive the CSI information from each receiving legitimate and/or eavesdropping UV terminal. Based on availability

and/or non-availability of CSI information at T_x, two know and unknown CSI scenarios are defined. In particular, known CSI scenario is defined against active eavesdropper, which shares its CSI with the transmitter and unknown CSI scenario is defined against a passive eavesdropper, which never shares its CSI with the transmitter. The above assumptions on both scenarios are valid because in wireless communication, during pilot symbol transmission process, the receiver first receives the instantaneous CSI of its receiving link and then, when the transmitter demands, the receiver sends its estimated CSI to the transmitter. The CSI estimation is performed by using each transmitting LED. However, from a security perspective, the transmitter T_x selects an LED that provides the optimum guarantee of security against both active and passive eavesdroppers. Therefore, the transmit LED selection mechanism is further divided into the following two scenarios;

1) SCENARIO-I: AGAINST ACTIVE EAVESDROPPER

Let E_k be an active user. Hence, T_x knows the instantaneous CSI of both legitimate and eavesdropping VLC links. Then similar to the Wyner wiretapper channel model [20], the positive secrecy rate can be formulated as

$$C_{s,k} = \left[\log_2\left(1+\gamma_{M_k}^{X_k}\right) - \log_2\left(1+\gamma_{E_k}^{X_k}\right)\right]^+, \quad (11)$$

where $[.]^+$ is used to denoted a non-negative quantity. Moreover, $\gamma_{M_k}^{X_k}$ and $\gamma_{E_k}^{X_k}$ are the instantaneous SINRs of the legitimate and eavesdropping links given by (9) and (10), respectively. Then, the secrecy rate under scenario-I, can be defined as

$$C_{s,k}^{i\text{OLS}} = \max_{i\in N}\left\{C_{s,k}\right\}, \quad (12)$$

where $i \in \{1, 2, \ldots N\}$. A pseudo-code of the scenario-I can be given by Algorithm-1.

Algorithm 1 LED Selection in Scenario-I

1: **Initialization:** Instantaneous CSIs of both M_k and E_k links;
2: **Decision:** Link decision indicator I_i, where $i \in \{1, 2, 3, \ldots N\}$ for N number of LEDs;
3: **for** $i = 1; i \leq N : i++$ do
4: Calculate $C_{M_1}^i$ and $C_{E_1}^i$;
5: **if** $C_{M_1} \geq C_{E_1} \wedge C_{s,1}(i) = \max_{i\in N}\left\{C_{s,k}\right\}$ **then**
6: $I_i = 0$, An optimal LED is selected for M_1 user;
7: **else if** $C_{M_2}^i \geq C_{E_2}^i \wedge C_{s,2}^i > 0$ **then**
8: $I_i = 1$, A random LED is selected for M_2 user;
9: **else**
10: $I_i = -1$, The system outage occurs;
11: **end if**
12: **end for**

2) SCENARIO-II: AGAINST PASSIVE EAVESDROPPER

Let E_k is now a passive user and T_x does not know the CSI of eavesdropping link. Then, it transmits the signal with a predetermined transmission rate $R_{b,k}$. The selection of $R_{b,k}$ is constrained with the channel capacity of the legitimate link i.e. $C_{M_k} = \log_2(1+\gamma_{M_k}^{X_k})$. Furthermore, T_x can transmit the information under the certain condition that $C_{M_k} \geq R_{b,k}$ because it cannot transmit the information beyond the channel capacity of the respected link. Otherwise, when $C_{M_k} < R_{b,k}$, connection outage occurs and T_x remains silent. In order to transmit the signal to M_k, T_x selects an LED which can achieve the maximum channel capacity C_{M_k}; that is $C_{M_k}^i = \log_2(1+\gamma_{M_k}^{i,X_k})$, where $\gamma_{M_k}^{i,X_k}$ is the received SINR at M_k^{th} user from the i^{th} antenna at T_x. Then, the secrecy rate for scenario-II, can be formulated as

$$C_{s,k}^{i\text{SLS}} = \max_{1<i\leq N}\left\{C_{M_k}^i - R_{b,k}\right\}. \quad (13)$$

A pseudo-code of scenario-II can be given by Algorithm-2.

Algorithm 2 LED Selection in Scenario-II

1: **Initialization:** Instantaneous CSIs of M_k link and define $R_{b,k}$;
2: **Decision:** Indicator I_i, here $i \in \{1, 2, 3, \ldots N\}$;
3: **for** $i = 1; i \leq T : i++$ do
4: Calculate $C_{M_1}^i$;
5: **if** $C_{M_1}^i \geq R_{b,1} \wedge C_{s,1}^{i\text{SLS}} = \max_{1<i\leq N}\left\{C_{M_1}^i - R_{b,1}\right\}$ **then**
6: $I_i = 0$, A LED is selected for M_1 user;
7: **else if** $C_{M_2}^i \geq R_{b,2} \wedge C_{s,2}^i > 0$ **then**
8: $I_i = 1$; A random LED is selected for M_2 user;
9: **else**
10: $I_i = -1$, The system outage occurs;
11: **end if**
12: **end for**

Remark-1: Using (13), it can be defined that in order to achieve the highest security against a passive eavesdropper, the value of $R_{b,k}$ should be high or very close to $\gamma_{M_k}^{X_k}$. However, when $R_{b,k}$ increases, the secrecy rate $C_{s,k}^{i\text{SLS}}$ decreases. As a consequence, using (12) and (13), it can be concluded that secrecy rate $C_{s,k}^{i\text{SLS}}$ can never be greater than $C_{s,k}^{i\text{OLS}}$, which means that knowledge of instantaneous CSI of both legitimate and eavesdropping links at the transmitter can provide better or higher security against the eavesdropping attacks.

In order to model the irrandiance light beam intensity fluctuations $I_{z_k}^r$ given in (1), a mixed exponential generalized Gamma (EGG) distribution is distribution is used. Then, utilizing (9), (10) and [5, eqn. (21)], the cumulative distribution function (CDF) of $\gamma_{z_k}^{X_k}$ can be given by

$$F_{\gamma_{z_k}}(\gamma) = \omega G_{1,2}^{1,1}\left[\frac{1}{\lambda}\left(\frac{\gamma}{\varphi_z^k \mu_{z_k}^r}\right)^{\frac{1}{r}}\Bigg|_{1,0}^{1}\right] + \frac{1-\omega}{\Gamma(a)} G_{1,2}^{1,1}\left[\frac{1}{b^c}\left(\frac{\gamma}{\varphi_z^k \mu_{z_k}^r}\right)^{\frac{c}{r}}\Bigg|_{a,0}^{1}\right], \quad (14)$$

where $z_k \in (M_k, E_k)$. Using (14) and [28, eqn. (8.2.2.31)], the probability density function (PDF) of $\gamma_{z_k}^{X_k}$ can be given by

$$f_{\gamma_{z_k}}(\gamma) = \frac{\omega}{r\gamma\lambda} G_{0,1}^{1,0}\left[\frac{1}{\lambda}\left(\frac{\gamma}{\varphi_z^k \mu_{z_k}^r}\right)^{\frac{1}{r}}\Bigg|_1^-\right] + \frac{c(1-\omega)}{r\gamma\Gamma(a)} G_{0,1}^{1,0}\left[\frac{1}{b^c}\left(\frac{\gamma}{\varphi_z^k \mu_{z_k}^r}\right)^{\frac{c}{r}}\Bigg|_a^-\right], \quad (15)$$

where

$$\mu_{z_k}^1 = \overline{\gamma}_{z_k}^{X_k}, \quad (16a)$$

$$\mu_{z_k}^2 = \frac{\overline{\gamma}_{z_k}^{X_k}}{2\omega\lambda^2 + b^2(1-\omega)\Gamma(a+2/c)/\Gamma(a)}, \quad (16b)$$

where $\overline{\gamma}_{z_k}^{X_k} = \mathbb{E}(\gamma_{z_k}^{X_k})$ denotes the average electrical SINR, ω denotes the mixture coefficient and λ is the scale parameter of exponential distribution. Moreover, a, b and c quantities are representing the EGG distribution parameters for different underwater scenarios and $\Gamma(.)$ represents the Gamma function. More specifically, the CDF and PDF expressions given in (14) and (15) are valid for (9), when $\varphi_z^1 = \alpha_1\rho_{z_1}$. However, for (9) and (10), both expressions are valid when $\varphi_z^2 = (\alpha_2 - \alpha_1\gamma)\rho_{z_2}$ under the condition that $\gamma \leq \frac{\alpha_2}{\alpha_1}$. Otherwise, when $\gamma > \frac{\alpha_2}{\alpha_1}$, then the CDF expression becomes unity i.e. $F_{\gamma_{z_k}}(\gamma) = 1$ and the PDF expression becomes zero i.e. $f_{\gamma_{z_k}}(\gamma) = 0$.

III. PERFORMANCE ANALYSIS

In order to compare the performance of the proposed underwater multi-LED-VLC system with the conventional underwater single-LED-VLC system, in this section, we derive closed-form secrecy outage probability (SOP) expressions for both single-LED and multi-LED transmission strategies. The SOP is the probability that the secrecy capacity $C_{s,k}$ is less than a target secrecy rate $R_{s,k}$. Therefore, the security is now constrained with the $R_{s,k}$ parameter which means that the proposed system must provide guaranteed secure communication against eavesdropping attacks up to the desired target secrecy rate $R_{s,k}$. Otherwise, the system outage condition occurs and the transmitter stops information transmission.

A. SOP OF UNDERWATER SINGLE-LED VLC SYSTEM

In this strategy, we consider that only the LED is transmitting the information and hence, in the first transmission phase for $k = 1$, the SOP at M_1 can be expressed as

$$P_{\text{out},M_1}^{\text{Single LED}} = Pr\left(C_{s,k} < R_{s,k}\right) = \int_0^\infty F_{\gamma_{M_1}}[\tau_1(1+\gamma) - 1] f_{\gamma_E}(\gamma_E) d\gamma, \quad (17)$$

where $\tau_1 = 2^{R_{s,1}}$. Using [29, eqn.(2.24.1.1)], [28, eqn.(8.2.2.15)], (15), (14) and (17), the derived SOP expression for M_1 UV is given in (18), as shown at the bottom of the next page, where $G(.)$ is the Meijer G function [28].

For $k = 2$, the SOP at M_2 can be defined as

$$P_{\text{out},M_2}^{\text{Single LED}} = \int_0^\vartheta F_{\gamma_{M_2}}[\tau_2(1+\gamma) - 1] f_{\gamma_E}(\gamma) d\gamma + \int_\vartheta^{\frac{\alpha_2}{\alpha_1}} f_{\gamma_E}(\gamma) d\gamma, \quad (19)$$

where $\tau_2 = 2^{R_{s,2}}$ and $\vartheta = \frac{1}{\alpha_1\tau_2} - 1 \leq \frac{\alpha_2}{\alpha_1}$. Using [29, eqn.(2.24.1.1)], (15), (14) and (17), the SOP at M_2 is derived and given in (20), as shown at the bottom of the next page.

In practice, the FV transmitter T_x does not know the exact location of E_k. Therefore, we assume that E_k can eavesdrop the information of either M_1 or M_2. Therefore, the eavesdropping occurrence in both the transmission phases is equal and then, the SOP of the single-LED VLC system can be given as

$$P_{\text{out}} = P_{\text{out},M_1} \times \Pr\left[E \text{ eavesdrops } M_1\right] + P_{\text{out},M_2} \times \Pr\left[E \text{ eavesdrops } M_2\right], \quad (21)$$

where $\Pr\left[E \text{ eavesdrops } M_1\right]$ and $\Pr\left[E \text{ eavesdrops } M_2\right]$ can be obtained according to the practical scenarios. We assume that $\Pr\left[E \text{ eavesdrops } M_1\right] = \Pr\left[E \text{ eavesdrops } M_2\right] = 1/2$. Then, the SOP can be expressed as

$$P_{\text{out}} = \frac{1}{2}\left(P_{\text{out},M_1} + P_{\text{out},M_2}\right). \quad (22)$$

B. SOP OF UNDERWATER MULTI-LED VLC SYSTEM

As stated above, the proposed system model is equipped with multiple LEDs and eavesdropping is possible via either an active and/or passive eavesdropper. Hence, in this section, the closed-form SOP expressions are derived for both scenario-I and scenario-II, respectively.

1) SOP ANALYSIS FOR SCENARIO-I

We first consider the case where security of M_1 is more important than M_2. Then, the SOP at M_1 of the Multi-LED underwater NOMA-VLC transmission against active eavesdropping, can be defined as

$$P_{\text{out},M_1}^{\text{OLS}} = \Pr\left[\max_{i\in N}\left(C_{s,1}^{i\text{OLS}}\right) \leq R_{s,1}\right] = \prod_{i=1}^{N} \Pr\left[C_{s,1}^{i\text{OLS}} \leq R_{s,1}\right] = \left(P_{\text{out},M_1}^{i\text{OLS}}\right)^N. \quad (23)$$

It is clear here that once an optimal LED is selected for transmitting the signal to M_1, the SOP at M_1 can be given as $P_{\text{out},M_1}^{i\text{OLS}} = P_{\text{out},M_1}$. Then, a random LED can be selected for transmitting the signal to M_2. Moreover, the SOP at M_2 can be given by (19) and the overall SOP for the VLC link can be given by

$$P_{\text{out}}^{\text{OLS},1} = \frac{1}{2}\left(\left(P_{\text{out},M_1}\right)^N + P_{\text{out},M_2}\right). \quad (24)$$

Similarly, when the optimal LED is selected for M_2, the overall SOP can be given by

$$P_{\text{out}}^{\text{OLS},2} = \frac{1}{2}\left(P_{\text{out},M_1} + \left(P_{\text{out},M_2}\right)^N\right). \quad (25)$$

2) SOP ANALYSIS FOR SCENARIO-II

The SOP at M_1 against passive eavesdropping attacks, can be defined as

$$P_{\text{out},M_1}^{\text{SLS}} = \left(P_{\text{out},M_1}^{i\text{SLS}}\right)^N, \tag{26}$$

where $P_{\text{out},M_1}^{i\text{SLS}}$ can be given by

$$\begin{aligned} P_{\text{out},M_1}^{i\text{SLS}} &= \Pr\left\{C_{s,1}^{i\text{SLS}} \leq R_{s,1}\right\} \\ &= \int_0^{\tau_1(1+\gamma_{\text{th},1})-1} f_{\gamma_{M,1}}(\gamma)d\gamma, \end{aligned} \tag{27}$$

where $\gamma_{\text{th},1} = 2^{R_{b,1}} - 1$. Using (15), the SOP can be derived and given in (28), as shown at the bottom of the next page. As an LED is already selected to transmit the signal to M_1 and hence, T_x can select any random LED to transmit the signal to M_2. Then, the SOP at M_2 can be defined as

$$P_{\text{out},M_2}^{i\text{SLS}} = \int_0^{\varpi} f_{\gamma_{M,2}}(\gamma)d\gamma + \int_{\varpi}^{\frac{\alpha_2}{\alpha_1}} f_{\gamma_{M,2}}(\gamma)d\gamma, \tag{29}$$

where $\varpi = \tau_2(1+\gamma_{\text{th},2}) - 1 \leq \frac{\alpha_2}{\alpha_1}$ and $\gamma_{\text{th},2} = 2^{R_{b,2}} - 1$. Using (15), SOP can be derived and given in (30), as shown at the bottom of the next page. The SOP that maximizes the channel capacity of the M_1 link can be defined as

$$P_{\text{out}}^{\text{SLS},1} = \frac{1}{2}\left(\left(P_{\text{out},M_1}^{i\text{SLS}}\right)^N + P_{\text{out},M_2}^{i\text{SLS}}\right) \tag{31}$$

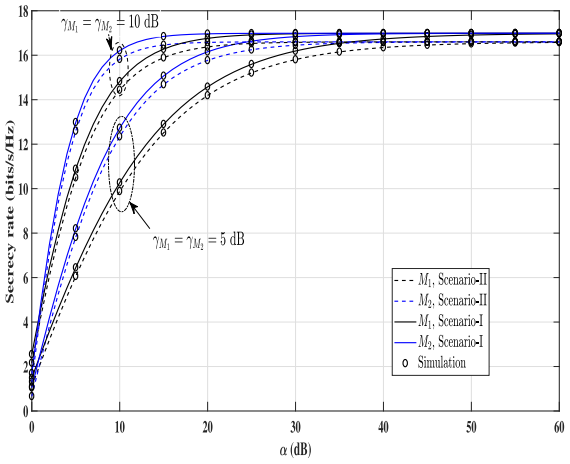

FIGURE 3. Secrecy-rate vs α for varying $\overline{\gamma}_M$ with known and unknown imprecise CSI scenarios.

Similarly, the SOP that maximizes the channel capacity of the M_2 link can be defined as

$$P_{\text{out}}^{\text{SLS},2} = \frac{1}{2}\left(P_{\text{out},M_1}^{i\text{SLS}} + \left(P_{\text{out},M_2}^{i\text{SLS}}\right)^N\right) \tag{32}$$

IV. NUMERICAL RESULTS

As stated above, the underwater OWC networking systems are mainly affected by air bubbles, which cause attenuation and scattering effects. In previous section, performance metrics of system were defined by considering EGG distribution.

$$\begin{aligned} P_{\text{out},M_1}^{\text{Single LED}} = \frac{\omega}{r\ell_1\lambda}&\left[\omega G_{2,2}^{2,1}\left(\frac{\delta_1}{\ell_1}\middle|\begin{matrix}-1,0\\-1,1\end{matrix}\right) + \frac{1-\omega}{\Gamma(a)}G_{2,2}^{2,1}\left(\frac{\delta_2}{\ell_1}\middle|\begin{matrix}-a,0\\-1,1\end{matrix}\right)\right] \\ &+\frac{1-\omega}{r\ell_2\Gamma(a)}\left[\omega c G_{2,2}^{2,1}\left(\frac{\delta_1}{\ell_2}\middle|\begin{matrix}-1,0\\-1,a-1\end{matrix}\right) + \frac{1-\omega}{\Gamma(a)}G_{2,2}^{2,1}\left(\frac{\delta_2}{\ell_2}\middle|\begin{matrix}-a,1\\-1,a-1\end{matrix}\right)\right], \end{aligned} \tag{18}$$

where $\ell_1 = \frac{1}{\lambda(\varphi_E^1\mu_E^r)^{\frac{1}{r}}}$, $\ell_2 = \frac{1}{b^c(\varphi_E^1\mu_E^r)^{\frac{c}{r}}}$, $\delta_1 = \sum_{p_1=0}^{\frac{1}{r}} \frac{\tau_1^{p_1}(\tau_1-1)^{\frac{1}{r}-p_1}}{\lambda(\varphi_{M_1}^1\mu_{M_1}^r)^{\frac{1}{r}}}$ and $\delta_2 = \sum_{p_2=0}^{\frac{c}{r}} \frac{\tau_1^{p_2}(\tau_1-1)^{\frac{c}{r}-p_2}}{b^c(\varphi_{M_1}^1\mu_{M_1}^r)^{\frac{c}{r}}}$.

$$\begin{aligned} P_{\text{out},M_2}^{\text{Single LED}} = \frac{\omega}{r\lambda}&\left[\frac{1}{r\ell_3^r}\left\{\omega G_{1+p_3,2+p_3}^{1,1+p_3}\left(\vartheta^{p_3}\delta_3\middle|\begin{matrix}\frac{r}{p_3},1\\1,0,-\frac{r+1}{p_3}\end{matrix}\right) + \frac{1-\omega}{\Gamma(a)}G_{1+p_4,2+p_4}^{1,1+p_4}\left(\vartheta^{p_4}\delta_4\middle|\begin{matrix}\frac{r}{p_4},1\\a,0,-\frac{r+1}{p_4}\end{matrix}\right)\right\}\right. \\ &\left.+\frac{r^{\frac{3}{2}}\delta_3}{\omega(2\pi)^{\frac{r-1}{2}}}\left\{G_{1,r+1}^{r+1,1}\left(\frac{\ell_3^r}{r^r}\middle|\begin{matrix}0\\0,\frac{1}{r},0\end{matrix}\right) - \frac{\alpha_1}{\alpha_2}G_{1,r+1}^{r+1,1}\left(\frac{\ell_3^r}{r^r}\middle|\begin{matrix}0\\\frac{1}{r},-1,0\end{matrix}\right) - \vartheta G_{1,r+1}^{r+1,0}\left(\frac{\ell_3^r}{r^r}\middle|\begin{matrix}0\\-1,\frac{1}{r},0\end{matrix}\right)\right\}\right] \\ &+\frac{c(1-\omega)}{r\Gamma(a)}\left[\frac{1}{r\ell_4^r}\left\{\omega G_{1+p_3,2+p_3}^{1,1+p_3}\left(\vartheta^{p_3}\delta_3\middle|\begin{matrix}\frac{1-r}{p_3},1\\1,0,-\frac{r}{p_3}\end{matrix}\right) + \frac{1-\omega}{\Gamma(a)}G_{1+p_4,2+p_4}^{1,1+p_4}\left(\vartheta^{p_4}\delta_4\middle|\begin{matrix}\frac{1-r}{p_4},1\\a,0,-\frac{r}{p_4}\end{matrix}\right)\right\}\right. \\ &\left.+\frac{\sqrt{c}(2\pi)^{\frac{c-1}{2}}}{\omega}\left\{G_{1,r+1}^{r+1,1}\left(\frac{\ell_4^r}{r^r}\middle|\begin{matrix}0\\0,\frac{a}{r},0\end{matrix}\right) - \frac{\alpha_1}{\alpha_2}G_{1,r+1}^{r+1,1}\left(\frac{\ell_4^r}{r^r}\middle|\begin{matrix}0\\\frac{a}{r},-1,0\end{matrix}\right) - \vartheta G_{1,r+1}^{r+1,0}\left(\frac{\ell_4^r}{r^r}\middle|\begin{matrix}0\\-1,\frac{a}{r},0\end{matrix}\right)\right\}\right], \end{aligned} \tag{20}$$

where $\ell_3 = \frac{1}{\lambda(\varphi_E^2\mu_E^r)^{\frac{1}{r}}}$, $\ell_4 = \frac{1}{b^c(\varphi_E^2\mu_E^r)^{\frac{c}{r}}}$, $\delta_3 = \sum_{p_3=0}^{\frac{1}{r}} \frac{\tau_2^{p_3}(\tau_2-1)^{\frac{1}{r}-p_3}}{\lambda(\varphi_M^2\mu_{M_2}^r)^{\frac{1}{r}}}$ and $\delta_4 = \sum_{p_4=0}^{\frac{c}{r}} \frac{\tau_2^{p_4}(\tau_2-1)^{\frac{c}{r}-p_4}}{b^c(\varphi_M^2\mu_{M_2}^r)^{\frac{c}{r}}}$.

In this section, we will now observe the effect of different air bubble levels, on the security performance of the proposed underwater VLC system. Indeed, we consider the two types of water conditions namely i) *fresh water* when no (or moderate) turbulence is present and ii) *salty water* when strong turbulence is present. Turbulence effect variation is estimated by varying the air bubble levels (BL) using different values of ω, λ, a, b, and c, as listed in [5, Tables 1 and 2]. Other parameters such as refractive index of water $n = 1.5$, gain of optical filter $\mathrm{U}(\psi_k) = 1$, effective area $A = 1.0$ cm^2, FOV angle of both M_1 and M_2 UV terminals i.e. $\psi_{z_k} = 70°$ and $\phi_{1/2} = 60°$ are kept fixed. For Monte-Carlo simulation analysis, 10^5 random samples are generated and their values are correlated with the numerically obtained values. Moreover, we consider $\overline{\gamma}_{M_1} = \overline{\gamma}_{M_2} = \overline{\gamma}_M$ and $R_{s,1} = R_{s,2} = 1$ bit/sec/Hz.

Using (12) and (13), we first quantify two optimal values of normalized pilot power α that can provide the highest secrecy-rate for transmitting the information to M_1 and/or M_2 UVs for both scenario-I and scenario-II. Fig. 3 demonstrates the achievable secrecy-rate against the normalized pilot signal power α, at $\overline{\gamma}_E = 0$ dB and $R_b = 0.6781$ bits/s/Hz. In scenario-I, it can be observed from the curves of $\overline{\gamma}_M = 5$ dB and $\overline{\gamma}_M = 10$ dB that the secrecy-rate increases fast to a peak value at $\alpha = 29$ for $\overline{\gamma}_M = 5$ dB, and at $\alpha = 19$ for $\overline{\gamma}_M = 10$ as α increases. Similarly, in scenario-II, the secrecy-rate increases to its peak value $\alpha = 28$ for $\overline{\gamma}_M = 5$ dB, and at $\alpha = 18$ for $\overline{\gamma}_M = 10$ dB. Moreover, it is to noticeable from the figure that it is not always good to impose a high pilot power to achieve a maximum secrecy rate because secrecy rate saturates after a certain value of α. This is happening due to the fact that we cannot transmit the information over a VLC link beyond its channel capacity. Hence, for further improvement in the security performance of the system, we need to focus on the other parameters i.e. attenuation, scattering effects, noise, and CSI estimations, etc. With this observation,

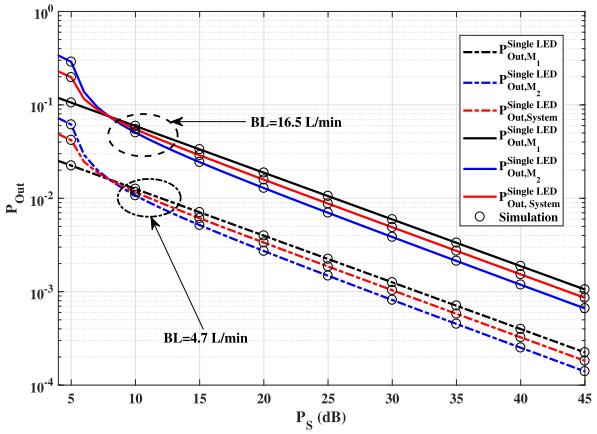

FIGURE 4. SOP vs. P_S for the single-LED transmission scheme at different bubble levels.

we have calculated two optimum values of α under which T_x achieves the highest secrecy rates. It can also be seen from the plot that the achieved secrecy-rates of both M_1 and M_2 UVs for scenario-I is greater than the achieved rates for scenario-II. More specifically, the secrecy rate of M_2 is higher than the M_1 UV because the allocated power coefficient $\alpha_2 = 0.6$ at M_2 is higher than the coefficient $\alpha_1 = 0.4$ at M_1. Next, we analyze the SOP performance of a conventional single-LED VLC system with the variation in the transmitting signal power P_s for two air bubble levels. Also, we assume that the parameters $r = 2$, $\overline{\gamma}_M = 10$ dB and $\overline{\gamma}_E = 5$ dB as fixed quantities. One can notice from (9) and (10) that the received SINRs at M_k is directly proportional to P_s, which means that when we increase the value of P_s, the received SINRs at M_k will also increase and their consequence effects will also improve secrecy rates $C_{s,k}$ under both scenarios, see eqns. (12) and (13). Therefore, plotted results in Fig. 4 are quite intuitive and validate the equation derived in (17)

$$P^{i\mathrm{SLS}}_{\mathrm{out},M_1} = \frac{(2\pi)^{\frac{1-r}{2}}}{\tau_1(1+\gamma_{\mathrm{th},1})-1}\left[\frac{\omega\sqrt{r}}{\lambda}G^{r+1,1}_{1,r+1}\left(\frac{\ell_5^r}{r^r}\middle|^{0}_{\frac{1}{r},-1,0}\right)+\frac{c(1-\omega)r^{a-\frac{1}{2}}}{\Gamma(a)}G^{r+1,1}_{1,r+1}\left(\frac{\ell_6^r}{r^r}\middle|^{0}_{\frac{a}{r},-1,0}\right)\right], \tag{28}$$

where $\ell_5 = \frac{1}{\lambda\left(\varphi^1_{M_1}\mu^r_{M_1}\right)^{\frac{1}{r}}}$ and $\ell_6 = \frac{1}{b^c\left(\varphi^1_{M_1}\mu^r_{M_1}\right)^{\frac{c}{r}}}$.

$$\begin{aligned}P^{i\mathrm{SLS}}_{\mathrm{out},M_2} = \frac{1}{(2\pi)^{\frac{r-1}{2}}}\Bigg[&\frac{\omega\sqrt{r}}{\lambda}\left\{G^{r+1,1}_{1,r+1}\left(\frac{\ell_7^r}{r^r}\middle|^{0}_{0,\frac{1}{r},0}\right)+\left(\frac{1}{2^{R_{b,2}}-1}-\frac{\alpha_1}{\alpha_2}\right)G^{r+1,1}_{1,r+1}\left(\frac{\ell_7^r}{r^r}\middle|^{0}_{\frac{1}{r},-1,0}\right)\right.\\&\left.-\frac{1}{2^{R_{b,2}}-1}G^{r+1,0}_{1,r+1}\left(\frac{\ell_7^r}{r^r}\middle|^{0}_{-1,\frac{1}{r},0}\right)\right\}+\frac{c(1-\omega)r^{a-\frac{1}{2}}}{\Gamma(a)}\left\{G^{r+1,1}_{1,r+1}\left(\frac{\ell_8^r}{r^r}\middle|^{0}_{0,\frac{a}{r},0}\right)\right.\\&\left.+\left(\frac{1}{2^{R_{b,2}}-1}-\frac{\alpha_1}{\alpha_2}\right)G^{r+1,1}_{1,r+1}\left(\frac{\ell_8^r}{r^r}\middle|^{0}_{\frac{a}{r},-1,0}\right)-\frac{1}{2^{R_{b,2}}-1}G^{r+1,0}_{1,r+1}\left(\frac{\ell_8^r}{r^r}\middle|^{0}_{-1,\frac{a}{r},0}\right)\right\}\Bigg],\end{aligned} \tag{30}$$

where $\ell_7 = \frac{1}{\lambda\left(\varphi^2_{M_2}\mu^r_{M_2}\right)^{\frac{1}{r}}}$ and $\ell_8 = \frac{1}{b^c\left(\varphi^2_{M_2}\mu^r_{M_2}\right)^{\frac{c}{r}}}$.

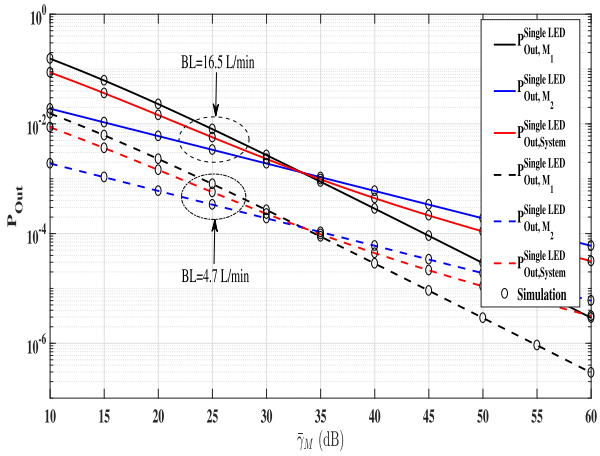

FIGURE 5. SOP vs. $\overline{\gamma}_M$ for the single-LED transmission scheme at different bubble levels.

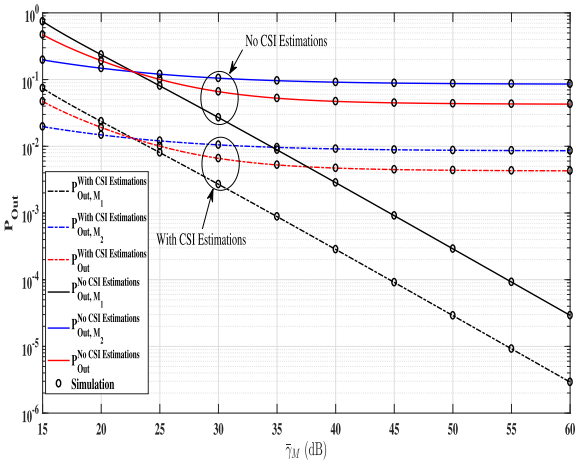

FIGURE 6. SOP vs. $\overline{\gamma}_M$ with imprecise channel estimations using MMSE and without channel estimations.

i.e. increasing the value of P_s should deteriorate the secrecy outage effect. Moreover, as power coefficients α_1 and α_2 are different for both UVs and in fact, more power is allocated to M_2 UV than M_1 UV. Hence, the plotted results are also representing that before the floor point, the value of SOP for M_2 UV remains higher than the SOP value for the M_1 UV and then, after the floor point, it represents the opposite effects i.e. higher SOP value for M_1 than M_2 UV. Here, the floor point is occurring when both M_1 and M_2 UVs are having equal power allocation coefficients i.e., $\alpha_1 = \alpha_2$. On the other hand, it can also be observed from the same figure that the SOP value is high at air bubble level BL = 16.5 L/min (i.e., for salty water) than the SOP value at BL = 4.7 L/min (i.e., for freshwater) for each individual value of P_s. This occurs due to the fact that as the turbulence effect increases, the scattering effect increases, and its consequence effect decreases the value of SOPs for both UVs. Using (22), it can be seen that the total SOP of the system is an average value of the SOPs obtained for M_1 and M_2 UVs, respectively. Therefore, the curve for total SOP approaches near the SOP of M_2 UV before the floor point and then approaches near the SOP value of M_1 UV after the floor point. This complete observation is also indicating that the overall security performance of the system deteriorates when the scattering effect becomes severe.

Based on the above-illustrated explanation, one can easily find that Fig. 3 concludes that we cannot increase the normalized power value α after a certain limit whereas Fig. 4 concludes that an increase in value of P_s can improve the system performance. Therefore, it is now important to obtain the SOP against the average instantaneous SINR of the legitimate link i.e., $\overline{\gamma}_M$ because it can quantify the effect the power of a signal received at M_k UV on the security performance of the system. We again take $r = 2$ and $\overline{\gamma}_E = 5$ dB parameters as fixed quantities. Fig. 5 illustrates the results of the equations derived in (18) and (20), respectively, which represents that when we increase $\overline{\gamma}_M$ value, the SOP for M_2 UV remains lower than the SOP value of M_1 UV until it reaches to a floor point and then, as expected, after the floor point, the SOP value for M_2 UV becomes higher than the SOP value obtained for M_1 UV. Here, the floor point exists at around $\overline{\gamma}_M = 33$ dB SINR value because we now keep the P_s value fixed at 2 dB and it can neglect the turbulence effects and increase the security over a noticeable region. It can also be observed from the same plot that the SOP value is high for air bubble level BL = 16.5 L/min than the SOP value of BL = 4.7 L/min, which is again illustrating the similar effect as described above. Moreover, the total SOP value given by (22) and (24) are also imposing the desired changes, and accordingly, the total SOP curve is approaching the SOP curves of M_1 and M_2 UVs, respectively. Interestingly, it can further be noticed from Figs. 4 and 5 that when $\overline{\gamma}_M$ increases, it decreases the SOP of M_1 (or M_2) in a much faster rate than when P_s value increases. The reason is that the secrecy rate becomes a constant at a large value of P_s and does not produce any significant contribution in improving the security performance analysis of the system beyond a certain limit.

Fig. 6 represents and compares the advantage of imprecise channel estimations over the SOP analysis against when no estimations are performed with correlation coefficient $\beta_{z_k} = 0.31$, $r = 2$ and $\overline{\gamma}_E = 5$ dB. It can be observed from the plot that CSI estimations represent lower SOP than the SOP with no CSI estimations for both the M_1 and M_2 UVs at each individual value of $\overline{\gamma}_M$ in dB. The results are pretty obvious because the estimated channel gain defined in (2) is directly proportional to the product of the channel gain parameters of direct and scattered paths that enhances the overall received signal strength at the receiver terminal. The another advantage of using the MMSE technique over LSE is that it avoids the error that occurred during channel estimations. Therefore, the overall SOP performance of the proposed underwater VLC system with imprecise estimations is better than the SOP performance evaluated without CSI estimations.

Fig. 7 compares the secrecy outage performance of the proposed underwater VLC system with the conventional single-LED VLC system. Here, we define how the number of LEDs can play an important role in improving the security performance of the system and also present the effect

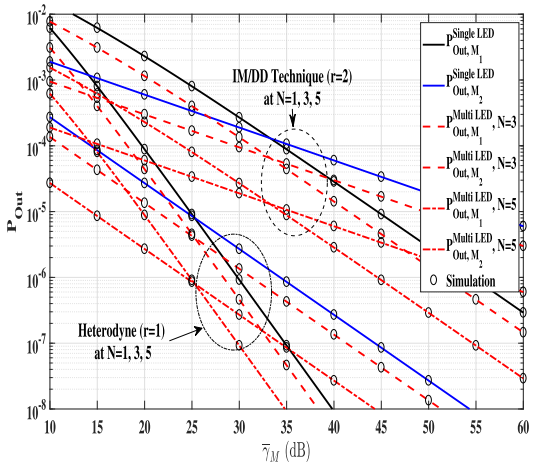

FIGURE 7. SOP vs. $\overline{\gamma}_M$ w.r.t. different values of r and N for both single LED and multi-LED VLC networks.

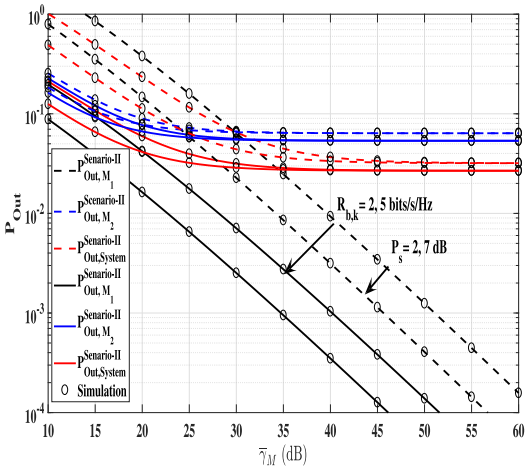

FIGURE 8. SOP vs. $\overline{\gamma}_M$ for different values of $R_{b,k}$ and P_s for scenario-II.

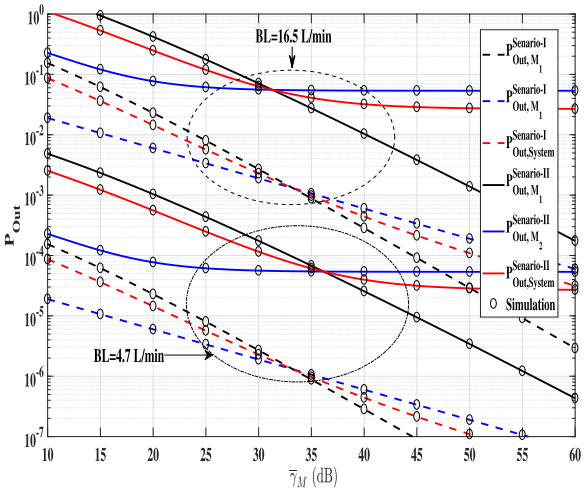

FIGURE 9. SOP vs. $\overline{\gamma}_M$ vs. different bubble levels for both scenario-I and scenario-II.

of choosing the detection techniques illustrated before in Section IIA i.e. heterodyne ($r = 1$) and IM/DD ($r = 2$) detection techniques. The SOP values are obtained by considering the equations given by (24) and (25) at different values of $\overline{\gamma}_M$ received at M_k UV while considering $P_s = 2$ dB and $\overline{\gamma}_E = 5$ dB as constant quantities. At $N = 1$, we plot the results of a single LED system. It can be seen from the plot that the SOP values of M_1 (or M_2) decrease when we increase the value of $N = 1$ to $N = 3$ and/or $N = 5$. In particular, the SOP value of M_2 UV remains less than the SOP value of M_1 UV until it reaches a floor point, but after floor point, the SOP value M_2 UV becomes greater than the SOP value of M_1 UV. Again, the results are quite intuitive and represent that when the value of N increases from $N = 3$ or $N = 5$, it can significantly improve the secrecy performance of the proposed system. An important point here is to notice with the same plot that the SOP values for $r = 2$ are always higher than the values for $r = 1$, which means that in contrast to the IM/DD detection technique, the heterodyne detection technique can not only improve the decoding ability of the respective UV but it can provide higher security against eavesdropping attacks too.

In Fig. 8, we presents how imprecise channel estimations can affect the overall security performance of the proposed system. The SOP values are obtained by using (28) and (30) for different $\overline{\gamma}_M$ values while varying the predefined transmission rate $R_{b,k}$ (i.e. illustrated in Section IIB for scenario-II) and P_s. We set $r = 2$, $\alpha_1 = 0.4$, $N = 5$ and $\overline{\gamma}_E = 5$ dB as fixed quantities. It can be observed from the figure that as data transmission rate $R_{b,k}$ (here, we choose equal data transmission rate in both transmission phases i.e. $R_{b,1} = R_{b,2}$) increases from 2 bits/s/Hz to 5 bits/s/Hz, the SOP value of M_1 (or M_2) decreases. On the other hand, when we increase P_s from 2 dB to 7 dB, the SOP value of M_1 (or M_2) further decreases. It defines the fact that a large quantity of either $R_{b,k}$ or P_s can improve the secrecy performance of the proposed system in the presence of a passive eavesdropper. However, the overall SOP performance of M_2 UV is lower than the M_1 user as the figure illustrates that the secrecy outage for M_2 UV occurs earlier than M_1 UV. The reason is that $R_{b,k}$ is defined under the constraints of channel capacity of the legitimate M_k UV only and its value can never exceed the value of C_{M_k} value, as stated in the Section-IIB. Indeed, this reason was discussed earlier in scenario-II, T_x has to compromise with the security performance of the system. This observation defines that the CSI estimation process plays an important role in order to identify the eavesdropping UV node presence as well as in defining the strategies to prevent eavesdropping attacks.

Finally, Fig. 9 illustrates a comparison between the results plotted for secrecy outage performance of the proposed NOMA-assisted VLC system in both scenario-I and scenario-II. The results are plotted for the SOP values obtained for different values of $\overline{\gamma}_M$ by using equations given by (18), (20), (28) and (30), respectively. We take $r = 2$, $\alpha_1 = 0.4$, $N = 5$, $\overline{\gamma}_E = 5$ dB, and $R_{b,k}$ i.e. $R_{b,1} = R_{b,2} = 2$ bits/sec/Hz, $P_s = 2$ dB as constant parameters. It can be observed from the plots of both the scenarios that the SOP value of M_2 UV remains lower than the SOP value of M_1 UV at each identical

value of $\overline{\gamma}_M$. The figure is also representing that under strong turbulence condition (i.e. BL = 16.5 L/min) or moderate (i.e. BL = 4.7 L/min) turbulence condition, the scenario-I is always better than the scenario-II, as we cannot track a scattered photon location when it reaches at the FOV of a passive eavesdropper. Also, it is very clear from the figure that with the use of the heterodyne technique (at $r = 1$), we can improve the security performance of the proposed underwater VLC system.

V. CONCLUSION

In this paper, according to the geometry of the light propagation mechanism, we have derived the direct and scattered paths' channel gain expressions for an underwater VLC environment. Using the MMSE technique under imprecise underwater channel conditions, we have formulated the secrecy rate for both known CSI scenario-I and unknown CSI scenario-II. Then, the closed-form SOP expressions are derived for both single-LED and proposed multi-LED VLC links. Furthermore, the performance of both systems is evaluated through a variety of different parameters such as underwater turbulence effects, transmit signal power, desired secrecy rate, and predefined transmission rate. The obtained results are validating the fact that the performance of the underwater VLC system in scenario-I is superior to the performance of scenario-II, which means that the CSI knowledge of all transmitting links at the transmitter can improve the security performance of the VLC network. Finally, the validity of the plotted numerical results is verified through a computer-based Monte-Carlo simulation analysis. In the future, investigating optimization algorithms to estimate an optimal pre-determined transmission rate and/or transmitted power values in a underwater VLC scenario with multiple users is an interesting extension to this work. Also, the simulated results can be verified through the experimental setups designed to perform in realistic underwater channel conditions.

ACKNOWLEDGMENT

The authors express their gratitude to Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R323), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCES

[1] Z. Zeng, S. Fu, H. Zhang, Y. Dong, and J. Cheng, "A survey of underwater optical wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 204–238, 1st Quart., 2017, doi: 10.1109/COMST.2016.2618841.

[2] Q. Hu, C. Gong, T. Lin, J. Luo, and Z. Xu, "Secrecy performance analysis for water-to-air visible light communication," *J. Lightw. Technol.*, vol. 40, no. 14, pp. 4607–4620, Jul. 15, 2022, doi: 10.1109/JLT.2022.3168258.

[3] M. Elamassie, F. Miramirkhani, and M. Uysal, "Performance characterization of underwater visible light communication," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 543–552, Jan. 2019, doi: 10.1109/TCOMM.2018.2867498.

[4] D. C. Mobley, B. Gentili, R. H. Gordon, Z. Jin, W. G. Kattawar, A. Morel, P. Reinersman, K. Stamnes, and H. R. Stavn, "Comparison of numerical models for computing underwater light fields," *Appl. Opt.*, vol. 32, pp. 7484–7504, Dec. 1993.

[5] E. Zedini, H. M. Oubei, A. Kammoun, M. Hamdi, B. S. Ooi, and M.-S. Alouini, "Unified statistical channel model for turbulence-induced fading in underwater wireless optical communication systems," *IEEE Trans. Commun.*, vol. 67, no. 4, pp. 2893–2907, Apr. 2019, doi: 10.1109/TCOMM.2019.2891542.

[6] P. Saxena and M. R. Bhatnagar, "A simplified form of beam spread function in underwater wireless optical communication and its applications," *IEEE Access*, vol. 7, pp. 105298–105313, 2019, doi: 10.1109/ACCESS.2019.2929738.

[7] A. Amantayeva, M. Yerzhanova, and R. C. Kizilirmak, "Multiuser MIMO for underwater visible light communication," in *Proc. Int. Conf. Comput. Netw. Commun. (CoCoNet)*, Aug. 2018, pp. 164–168.

[8] S. Tang, Y. Dong, and X. Zhang, "Impulse response modeling for underwater wireless optical communication links," *IEEE Trans. Commun.*, vol. 62, no. 1, pp. 226–234, Jan. 2014, doi: 10.1109/TCOMM.2013.120713.130199.

[9] A. Stamoulis, S. N. Diggavi, and N. Al-Dhahir, "Intercarrier interference in MIMO OFDM," *IEEE Trans. Signal Process.*, vol. 50, no. 10, pp. 2451–2464, Oct. 2002, doi: 10.1109/TSP.2002.803347.

[10] H. Lei, J. Zhang, K.-H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017, doi: 10.1109/ACCESS.2017.2737330.

[11] Y. Liu, W. Yi, Z. Ding, X. Liu, O. A. Dobre, and N. Al-Dhahir, "Developing NOMA to next generation multiple access (NGMA): Future vision and research opportunities," *IEEE Wireless Commun.*, early access, Jun. 24, 2022, doi: 10.1109/MWC.007.2100553.

[12] Z. Ding, R. Schober, and H. V. Poor, "Unveiling the importance of SIC in NOMA systems—Part 1: State of the art and recent findings," *IEEE Commun. Lett.*, vol. 24, no. 11, pp. 2373–2377, Nov. 2020.

[13] M. Elamassie, L. Bariah, M. Uysal, S. Muhaidat, and P. C. Sofotasios, "Capacity analysis of NOMA-enabled underwater VLC networks," *IEEE Access*, vol. 9, pp. 153305–153315, 2021, doi: 10.1109/ACCESS.2021.3122399.

[14] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016, doi: 10.1109/LCOMM.2016.2539162.

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

[16] Y. H. Chung, "Secure NLOS ultraviolet communication against active/passive eavesdropping attacks," *Opt. Commun.*, vol. 501, Dec. 2021, Art. no. 127378, doi: 10.1016/J.OPTCOM.2021.127378.

[17] D. Zou, C. Gong, and Z. Xu, "Secrecy rate of MISO optical wireless scattering communications," *IEEE Trans. Commun.*, vol. 66, no. 1, pp. 225–238, Jan. 2018.

[18] M. A. Arfaoui, H. Zaid, Z. Rezki, A. Ghrayeb, A. Chaaban, and M. Alouini, "Artificial noise-based beamforming for the MISO VLC wiretap channel," *IEEE Trans. Commun.*, vol. 67, no. 4, pp. 2866–2879, Apr. 2019.

[19] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Sep. 1949.

[20] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[21] A. Kumar and P. Garg, "Physical layer security for dual-hop FSO/RF system using generalized $\Gamma\Gamma/\eta$-μ fading channels," *Int. J. Commun. Syst.*, vol. 31, no. 3, pp. 1099–1131, Feb. 2018.

[22] A. Kumar, P. Garg, and P. K. Sharma, "Secured selected cooperative communication analysis in cognitive relay networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2018, pp. 1–6.

[23] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.

[24] J. Hu, W. Yang, N. Yang, X. Zhou, and Y. Cai, "On–off-based secure transmission design with outdated channel state information," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6075–6088, Aug. 2016.

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

[26] A. Kumar and D. N. K. Jayakody, "Secure NOMA-assisted multi-LED underwater visible light communication," *IEEE Trans. Veh. Technol.*, vol. 71, no. 7, pp. 7769–7779, Jul. 2022, doi: 10.1109/TVT.2022.3167992.

[27] A. Kumar, P. Garg, P. K. Sharma, and A. Gupta, "Secure information broadcasting analysis in an indoor VLC system with imperfect CSI," *IET Commun.*, vol. 15, no. 4, pp. 526–536, Dec. 2020.

[28] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. New York, NY, USA: Academic, 2014.
[29] A. Prudnikov, Y. Brychkov, and O. Marichev, *Integrals and Series: More Special Functions*, vol. 3. Boca Raton, FL, USA: CRC Press, 1999.

AMBRISH KUMAR received the M.Tech. degree in optical and wireless communication technologies from the Jaypee University of Information Technology, Solan, Himachal Pradesh, India, and the Ph.D. degree in wireless communication from the University of Delhi, New Delhi, India. He was a Network Engineer at Tata Communication Pvt. Ltd., New Delhi, and a Lecturer at Amity University, Rajasthan, Jaipur, India. He was a Teaching-Cum Research Fellow (TRF) at the Netaji Subhas University of Technology [formerly Netaji Subhas Institute of Technology (NSIT)], New Delhi. He was a Researcher with the Department of Information and Communications Engineering, Pukyong National University (PKNU), Busan, South Korea. He is currently a Postdoctoral Researcher at the Centre for Telecommunications Research (CTR), Sri Lanka Technological Campus, Padukka, Sri Lanka. His research interests include physical layer security, visible light communication, underwater VLC, ultraviolet communication, free-space-optics, and cognitive radio networks.

SAIF AL-KUWARI (Senior Member, IEEE) received the Bachelor of Engineering degree in computers and networks from the University of Essex, U.K., in 2006, the Ph.D. degree from the University of Bath and Royal Holloway, in 2011, and the Ph.D. degree in computer science from the University of London, in 2011. He is currently an Assistant Professor at the College of Science and Engineering, Hamad Bin Khalifa University. His research interests include applied cryptography, quantum computing, computational forensics, and their connections with machine learning. He is an IET and BCS Fellow and an ACM Senior Member.

DUSHANTHA NALIN K. JAYAKODY (Senior Member, IEEE) received the M.Sc. degree in electronics and communications engineering from the Department of Electrical and Electronics Engineering, Eastern Mediterranean University, Turkey (under the University Full Graduate Scholarship), and the Ph.D. degree in electronics and communications engineering from the University College Dublin, Ireland, in 2013.

He held visiting and/or sabbatical positions at the Center for Telecommunications Research, The University of Sydney, Australia, in 2015, and Texas A&M University, in 2018. He was a Visiting Professor at the University of Jyvaskyla, Finland, in 2019 and 2022, within the framework of the Academy of Finland. He also served as a Visiting Professor at the University of Juiz de Fora, Brazil, in 2019. From 2019 to 2022, he was a Resource Person/Visiting Professor with the Department of Electronics and Communication Engineering, National Institute of Tiruchirappalli, India, within the SPARC Project of the Ministry of Human Resources in India. From 2014 to 2016, he was a Postdoctoral Research Fellow at the University of Tartu, Estonia, and the University of Bergen, Norway. From 2016 to 2021, he was a Professor at the School of Computer Science and Robotics, National Research Tomsk Polytechnic University (TPU), Russia. He has been serving as the Head of the School of Postgraduate and Research, Sri Lanka Technological Campus (SLTC), Padukka, Sri Lanka, and the Founding Head of the Centre of Telecommunication Research, SLTC, since January 2019. Since 2021, he has been with the Autonoma TechLab, Portugal, and the Department of Engineering and Computer Science, Universidade Autónoma de Lisboa, Portugal. He is supervising/supervised 15 Ph.D. students and many master's and undergraduate students and five postdoctoral researchers. In his career, so far, he has attracted nearly 6M$ research funding from many international grant agencies such as the European Commission, the Russian Science foundation, and the Ministry of Human Resource India. He has published nearly 200 international peer reviewed journals and conference papers and books. His research interests include PHY and NET layer prospective of 5G communications technologies such as NOMA for 5G, cooperative wireless communications, device to device communications, LDPC codes, and unmanned aerial vehicle.

Prof. Jayakody is a fellow of IET. He has received the Best Paper Award from the IEEE International Conference on Communication, Management and Information Technology (ICCMIT), in 2017, and the International Conference on Emerging Technologies of Information and Communications, Bhutan, in March 2019. In July 2019, he received the Education Leadership Award from the World Academic Congress, in 2019. From 2017 to 2018, he received the Outstanding Faculty Award by the National Research Tomsk Polytechnic University, Russia. He also received the Distinguished Researcher in wireless communications, Chennai, India, in 2019. He also received the Presidential Award for Outstanding Research Performance, in 2021. He also received the ''Best Publication Award'' at SLTC, in 2019 and 2020. He has organized or co-organized more than 30 workshops, special sessions, and IEEE conferences. He currently serves as an Area Editor for the *Physical Communication* journal (Elsevier), *Information* journal (MDPI), *Sensors* (MDPI), and *Internet of Technology Letters* (Wiley). Also, he serves on the Advisory Board of *MDPI Multidisciplinary Journal Sci*. In addition, he serves as a reviewer for various IEEE TRANSACTIONS and other journals.

REEM ALKANHEL (Member, IEEE) received the B.S. degree in computer sciences from King Saud University, Riyadh, Saudi Arabia, in 1996, the M.S. degree in information technology (computer networks and information security) from the Queensland University of Technology, Brisbane, Australia, in 2007, and the Ph.D. degree in information technology (networks and communication systems) from Plymouth University, Plymouth, U.K., in 2019. She has been with Princess Nourah bint Abdulrahman University, Riyadh, since 1997. She is currently an Assistant Professor at the College of Computer and Information Sciences. Her current research interests include communication systems, networking, the Internet of Things, software-defined networking, and information security.