Received 3 February 2024; accepted 23 February 2024. Date of publication 5 March 2024; date of current version 13 May 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3373476

Physical-Layer Security in Mixed UOWC-RF Networks With Energy Harvesting Relay Against Multiple Eavesdroppers

MOLOY KUMAR GHOSH[1], MILTON KUMAR KUNDU[1] (Member, IEEE), MD. IBRAHIM[2] (Graduate Student Member, IEEE), A. S. M. BADRUDDUZA[3] (Member, IEEE), MD. SHAMIM ANOWER[4], IMRAN SHAFIQUE ANSARI[5] (Senior Member, IEEE), ANNIE SOLOMON[6], SUMIT CHAKRAVARTY[7] (Member, IEEE), IMTIAZ AHMED[8] (Senior Member, IEEE), AND HEEJUNG YU[9] (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, Rajshahi University of Engineering and Technology, Rajshahi 6204, Bangladesh

[2]Institute of Information and Communication Technology, Rajshahi University of Engineering and Technology, Rajshahi 6204, Bangladesh

[3]Department of Electronics and Telecommunication Engineering, Rajshahi University of Engineering and Technology, Rajshahi 6204, Bangladesh

[4]Department of Electrical and Electronic Engineering, Rajshahi University of Engineering and Technology, Rajshahi 6204, Bangladesh

[5]James Watt School of Engineering, University of Glasgow, G12 8QQ Glasgow, U.K.

[6]Department of Mechanical Engineering, Kennesaw State University, Kennesaw, GA 30144, USA

[7]Department of Electrical and Computer Engineering, Kennesaw State University, Kennesaw, GA 30144, USA

[8]Department of Electrical Engineering and Computer Science, Howard University, Washington, DC 20059, USA

[9]Department of Electronics and Information Engineering, Korea University, Sejong 30019, South Korea

CORRESPONDING AUTHOR: S. CHAKRAVARTY (e-mail: Schakra2@kennesaw.edu)

This work was supported by the College of Engineering of Kennesaw State University and Howard University's NSF Grant under Award 2200640.

ABSTRACT In this study, physical layer security (PLS) in a dual-hop underwater optical wireless communication (UOWC)-radio frequency (RF) network under the intruding attempts of multiple eavesdroppers via RF links is considered. An intermediate decode-and-forward (DF) relay node between an underwater source and a destination transforms the optical signal into an electrical form and forwards it to the destination node with the help of harvested energy by the relay from an integrated power beacon within the system. The source-to-relay link, i.e., a UOWC link, is assumed to follow a mixture of exponential generalized Gamma turbulence with pointing error impairments whereas all the remaining links, i.e., RF links, are assumed to undergo $\kappa - \mu$ shadowed fading. Here, two eavesdropping scenarios are considered depending on the types of intruders, i.e., colluding (*Scenario-I*) and non-colluding (*Scenario-II*) eavesdropping operations. The analytical expressions of secrecy outage probability (SOP), probability of strictly positive secrecy capacity (SPSC), and effective secrecy throughput (EST) are derived for each scenario. Furthermore, the impacts of UOWC and RF channel parameters as well as detection techniques on secrecy capacity are demonstrated. A comparative study between two scenarios demonstrates that the collusion between the eavesdroppers imposes the most harmful threat on secrecy throughput but a better secrecy level can be attained by adopting diversity at the destination and power beacon nodes along with heterodyne detection rather than intensity modulation and direct detection technique. Finally, all the derived expressions are verified with the numerical results.

INDEX TERMS Effective secrecy throughput, underwater optical communication, secure outage probability, energy harvesting, colluding and non-colluding eavesdroppers.

I. INTRODUCTION

WIRELESS communication technologies have been expanding at a rapid rate along with the diverse needs for connectivity between individuals and machine-type devices. As the fifth generation (5G) of cellular networks is expanded over the world, researchers have

already begun contemplating and subsequently performing research for the beyond 5G (B5G) and the sixth generation (6G) communication networks [1], [2], [3]. Ubiquitous connectivity is one of the key features of B5G and 6G networks. To this end, non-terrestrial networks (NTNs) and underwater communication networks are regarded as new service domains. For underwater communication, an underwater cable was regarded as the only viable way for underwater communication. In general, the deployment and maintenance of wired underwater communication is not a realistic solution due to the cost and complexity of the system. To achieve network scalability and flexibility, underwater wireless communication has gathered more and more attention from academia and industries. Even though acoustic waves and radio frequency electromagnetic waves can have been investigated, they have limitations such as bandwidth, coverage, propagation delay, and hardware size. Alternatively, underwater optical wireless communication (UOWC) has been regarded as a promising technology due to the merits of sufficient bandwidth, high security, compact footprint, and low time latency. According to the researchers, one of the most important features of a 6G communication system will be the spectral and energy efficiencies [4], [5], [6], [7], [8]. Energy harvesting can play a vital role in achieving the energy efficiency feature in a wireless communication network and unravel a variety of problems that are impossible to solve by conventional battery-powered communication operations such as untethered mobility, monitoring in rural areas, and developed medical applications [7], [9].

A. BACKGROUND

Wireless communication terminals can harvest energy from radio frequency (RF) signals. The harvested power depends significantly on the changes in the number of RF sources and channel condition [10]. Energy harvesting schemes can be achieved by considering various possibilities (e.g., single/two-hop model, finite/infinite energy capacity, perfect/imperfect channel state information, etc.) and employing the optimal policy (e.g., offline or online optimal policy) [11]. Another scheme named energy cooperation save-then-transmit was proposed in [12] where the maximum throughput and outage probability (OP) were derived in a closed-form solution under additive white Gaussian noise (AWGN) channels with deterministic energy arrival rate and Rayleigh block fading channels with stochastic energy arrival rate. A general approximation framework was introduced in [13] for real-life energy harvesting setups for both single and multiple users to provide an effective solution to the throughput and outage problems. A piece-wise linear approximation model was proposed in [14] considering practical harvesting scenarios such as limited harvesting efficiency and sensitivity. This model is proclaimed to match the actual condition whereas the infinite sensitivity model (both linear and non-linear) deviates from reality. The 2D and 3D position of the energy harvesters plays a significant role in harvesting energy to different nodes of a wireless network. If we presume a system with concurrent energy transfer, the received and interference power follows the log-normal distribution while the harvested voltage exhibits the Rayleigh distribution [15].

Energy harvesting can also be boosted by using multiple antennas at the transmitter due to its non-linear characteristics, even if the channel state information (CSI) is unavailable at the transmitter [16]. Energy harvesting technology is frequently considered in mixed communication networks, e.g., RF/free-space optical (FSO) networks and RF/UOWC networks because it requires a large amount of energy to convert the signal from one form to another. In [17], the authors analyzed the OP and diversity order of an FSO/RF network considering the physical limitations like pointing error, atmospheric turbulence, and saturation threshold of the energy harvester, whereas in [18], the authors considered an RF/FSO network with a multi-antenna source that harvests energy from a relay and determined the OP of the system. The RF/UOWC is another popular model to explore underwater activities such as ocean surveillance and exploration, climate monitoring, etc. [19]. The researchers in [20], [21], [22], [23] considered an RF/UOWC network to evaluate the OP and bit error rate (BER) assuming different combinations of RF and UOWC channels. The application of unmanned aerial vehicle (UAV) as a source was considered in [24] where the authors analyzed similar performance parameters (OP and BER) and also deduced the optimal altitude of the UAV for performance maximization. In another research, the authors assumed a RIS-assisted RF/UOWC network and derived the OP, BER, and average channel capacity of the system [25].

Another important feature of the 6G wireless communication model is data security and privacy [26]. Since the beginning of the wireless network, this issue has been thoroughly analyzed for RF communication systems. With the rise of mixed networks and advanced eavesdropping technologies, the physical layer security of these types of communication schemes is threatened and needs to be evaluated extensively [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38]. In [37], authors analyzed the secrecy of a RF/FSO network considering a single eavesdropper trying to overhear information from the RF link. The authors in [38] investigated the hybrid free-space optical and radio frequency (FSO/RF) communication system's physical layer secrecy (PLS) performance utilizing a modified selection combining scheme. The researchers in [39] analyzed energy harvested RF/FSO network assuming the relaying protocol to be decode-and-forward (DF) with the simultaneous wireless information and power transfer (SWIPT) technology and revealed that security of the proposed network can be enhanced by lowering the power splitting fraction parameter. The effect of atmospheric turbulence and pointing error on the security of the RF/FSO model was analyzed in [40], [41]. A multi-relay network was considered in [42] with imperfect channel state information (CSI) and non-linear energy harvesters where the authors

derived secure outage probability (SOP) to evaluate the system performance. The researchers concluded that further improvement in SOP is impossible if the saturation threshold is higher than a certain value. However, the secrecy performance of an FSO/RF system was investigated in [43] considering an energy harvesting-dependent relay scheme. The authors of [44] considered a mixed RF/UOWC model with a single antenna source and destination in the presence of a relay equipped with multiple antennas and derived the SOP performance of the system. In [45], [46], the authors analyzed three main secrecy parameters i.e., SOP, average secrecy capacity (ASC), and strictly positive secrecy capacity (SPSC), assuming an RF/UOWC model where the underwater signal undergoes frequent underwater turbulence (UWT) due to the temperature gradient, bubble level, and salinity gradient of the ocean.

The security of the wireless communication model also depends on the behavior of eavesdroppers, i.e., the types of eavesdropping operation. If there are multiple eavesdroppers in the system, they can work together to decode a message coming from the source. This scenario is known as colluding eavesdropping. On the other hand, eavesdroppers can try to decode confidential information independently without help from other eavesdroppers. This is known as a non-colluding eavesdropping scenario. It is evident that the former scenario is more threatening for wireless communication than the latter [47]. Keeping this in mind, many researchers have started to analyze the colluding eavesdropping scenario and how it can jeopardize our secure communication network. The authors in [48], [49] analyzed the SOP of a wireless network considering colluding eavesdroppers were present in the system. In [50], [51], the authors analyzed the secrecy performance with an assumption of non-colluding eavesdroppers. To compare the detrimental effect caused by colluding and non-colluding eavesdroppers on the secure wireless network, the authors of [52], [53], [54] considered both eavesdropping scenarios and concluded that the increasing number of eavesdroppers degrades the security of the system whereas colluding eavesdroppers have the most harmful effects.

B. MOTIVATION AND CONTRIBUTIONS

Recently, researchers have made some excellent advancements in mixed communication systems. Despite their efforts, a few important considerations such as energy harvesting at the relay node along with the presence of multiple eavesdroppers (both colluding and non-colluding) in the system are not available in any literature and thus are considered an open problem. In this study, therefore, an energy harvesting relay-based mixed UOWC-RF network with multiple eavesdroppers has been analyzed assuming that the UOWC channel link follows a mixture exponential generalized Gamma (mEGG) fading model whereas the RF link undergoes $\kappa - \mu$ shadowed fading channel. The proposed mEGG model is mostly favored by the researchers due to its capability to mathematically represent all the physical constraints such as air bubbles, UWT, water salinity, and temperature gradient [55], [56] along with being a generalized model that can be reduced to an EGG model as one of its special cases [57]. On the other hand, the $\kappa - \mu$ shadowed fading model is another generalized model that represents a number of practical fading channels [58, Table I]. The goal of this study is to analyze the secrecy of such a system considering multiple eavesdroppers present in the system and trying to decode transmitted information individually or as a group as well as measure the impact of energy harvesting on data security. Although a few research has considered colluding and non-colluding eavesdropping operations [54], [59], [60] and energy harvesting in mixed wireless optical-RF channels [39], [57], [61], no study is available considering both of these scenarios. Thus, this study represents a novel system model and provides some unique results. The key contributions of this work are as follows:

- At first, we derive the cumulative density function (CDF) of the dual-hop signal-to-noise ratio (SNR) considering an energy-harvesting relay in a UOWC-RF network for both source-to-relay as well as eavesdroppers. Note that, unlike [39], [57], which only considered a single eavesdropper, the scenarios with multiple eavesdroppers (both colluding and non-colluding) are analyzed in this study. As our model represents a novel structure, the derived CDFs are also novel.
- The secrecy performance of the proposed network is demonstrated with respect to the secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC), and effective secrecy throughput (EST) expressions for both eavesdropping conditions in the closed forms and further verified via Monte-Carlo (MC) simulations. To the best of the authors' knowledge, these expressions can be utilized to unify versatile classical existing models as given in [57] and [58, Table I].
- Capitalizing on the derived expressions, noticeable impacts of air bubbles and temperature gradients-based UWTs for both salty and fresh water along with the energy harvesting parameters are demonstrated. Finally, the effects of two types of detection techniques, i.e., intensity modulation/direct detection (IM/DD) and heterodyne detection (HD) techniques, are also analyzed.

C. PAPER ORGANIZATION

The rest of the paper is organized as follows: Section II describes the system model in detail while Section III portrays the channel models. Expression of the performance measures, e.g., SOP, SPSC, and EST, are derived in Section IV followed by numerical results discussed in Section V. Finally, concluding remarks on the work are provided in Section VI.

II. SYSTEM MODEL

In Figure 1, an energy-harvested relay-based mixed UOWC-RF system is illustrated that consists of a single aperture

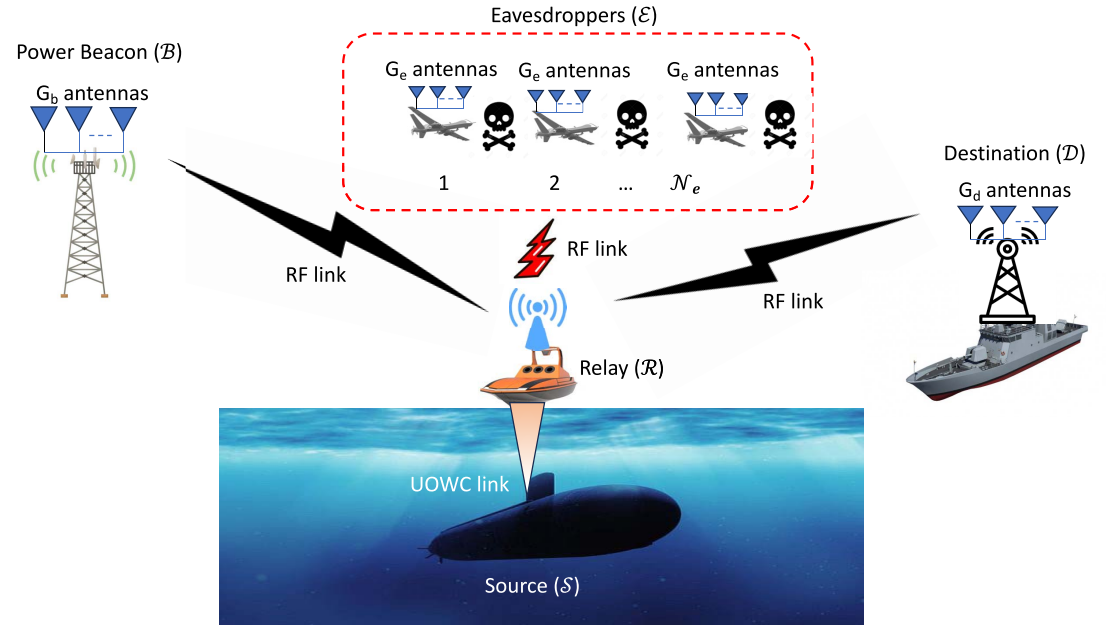

FIGURE 1. Proposed system model for physical layer security in mixed UOWC-RF networks with energy harvesting relay against multiple eavesdroppers.

source node, which is denoted by $\mathcal{S}$, (e.g., submarine), an energy-harvested relay node represented by $\mathcal{R}$ (e.g., a small unmanned boat or floating buoy) with a single receive aperture and a single transmit antenna, a destination node, $\mathcal{D}$, (e.g., a large ship) having G_d antennas, a power beacon, $\mathcal{B}$, with G_b antennas, and multiple eavesdropper nodes, $\mathcal{E}$s, (e.g., unmanned aerial vehicles) with G_e antennas. Herein, $\mathcal{S}$ connected to an underwater optics-based network transmits secret information, e.g., military information, to $\mathcal{D}$ in the RF network while $\mathcal{E}$ tries to decode the secret information by overhearing the illegitimate RF link. The UOWC link experiences mEGG turbulence with pointing error impairments, while all the RF links undergo $\kappa - \mu$ shadowed fading channels. We take into consideration two scenarios that correspond to the two types of eavesdropping operation with multiple eavesdroppers, i.e., colluding and non-colluding [36]. In *scenario-I*, the colluding eavesdroppers combine and share their receptions utilizing the maximum ratio combining (MRC) technique in order to decode the private data wiretapped from $\mathcal{R}$. In *scenario-II*, on the other hand, each non-colluding eavesdropper individually examines the wiretapped private data from $\mathcal{R}$. Exploiting the broadcast nature of RF signals, any prototype in the RF system can serve as a power beacon in the proposed framework. Hence, the integration of a power beacon is possible without any additional cost. Because an optical network is unable to directly connect with an RF network, an energy-harvesting relay needs to act as an intermediary to facilitate this communication. It is noteworthy that the decode-and-forward (DF) protocol is utilized to process the received signals at $\mathcal{R}$ because it has the advantage of reducing the first hop's channel impacts on the received signals on the second hop. It is also noted that the proposed framework can be utilized in real-world scenarios such as monitoring biological and ecological processes in ocean environments, investigation of climate change, unmanned underwater vehicles used to control and maintain oil production facilities, etc.

The entire communication process, which we denote as T, can be divided into two time slots. In this scenario, the fraction of the block time during which the relay harvests energy from $\mathcal{B}$ is represented by α $(0 \leq \alpha \leq 1)$. The remaining block time is then split into two equal parts, namely $(1-\alpha)T/2$, for transmitting information from $\mathcal{S}$ to $\mathcal{R}$ and from $\mathcal{R}$ to $\mathcal{D}$, respectively. In the first time slot, $\mathcal{S}$ transmits the confidential information to $\mathcal{R}$ through a legitimate UOWC link. At $\mathcal{R}$, the instantaneous electrical signal-to-noise ratio (SNR) is expressed as

$$\gamma_{sr} = \frac{\eta_{sr}^2 \urcorner_{sr}^2 I_{sr}^2}{\vartheta_{sr}^2}, \tag{1}$$

where η_{sr} represents an optical conversion ratio, $\urcorner_{sr}$ indicates a photoelectric conversion factor, I_{sr} denotes an optical irradiance, and ϑ_{sr} denotes an AWGN. Because $\mathcal{R}$ harvests RF energy from $\mathcal{B}$, the harvested energy at $\mathcal{R}$ is expressed as [62]

$$E_r = \eta_r P_b |\mathbf{h}_{br}|^2 \alpha T, \tag{2}$$

where P_b defines the transmit power at $\mathcal{B}$, $\mathbf{h}_{br} \in \mathbb{C}^{1\times G_b}$ is the channel gain of $\mathcal{B}-\mathcal{R}$ link, and an energy conversion efficiency is indicated by $\eta_r (0 \leq \eta_r \leq 1)$, which is mainly controlled by a harvesting circuitry.

In the second time slot, $\mathcal{R}$ firstly decodes the received optical signal and then transforms it into the RF signal. To

facilitate the information transfer from $\mathcal{R}$ to $\mathcal{D}$, $\mathcal{R}$ utilizes all of the harvested energy with an output power of

$$P_r = \eta_r P_b |\mathbf{h}_{br}|^2. \tag{3}$$

The signals received at $\mathcal{D}$ is given as

$$\mathbf{y}_d = \sqrt{P_r}\mathbf{h}_{rd} z + \mathbf{n}_d, \tag{4}$$

where z represents the transmitted signal, $\mathbf{h}_{rd} \in \mathbb{C}^{G_d \times 1}$ is the channel gain of $\mathcal{R}-\mathcal{D}$ link, and an AWGN with a noise power, P_{dn}, is represented by $\mathbf{n}_d \sim \mathcal{N}(0, P_{dn}\mathbf{I}_{G_d})$. Here, $\mathbf{I}_N$ is an $N \times N$ identity matrix. We consider $\mathcal{E}$ trying to wiretap the confidential information signals via an illicit $\mathcal{R}-\mathcal{E}$ link. Hence, the received signals at jth eavesdropper in the second time slot are given as

$$\mathbf{y}_{e,j} = \sqrt{P_r}\mathbf{h}_{re,j} z + \mathbf{n}_{e,j}, \tag{5}$$

where $\mathbf{h}_{re,j} \in \mathbb{C}^{G_e \times 1}$ is the channel gain of $\mathcal{R} \to j$th ($j = 1, 2, \ldots, \mathcal{N}_e$) link and the AWGN with zero mean and noise power, P_{en}, is represented by $\mathbf{n}_{e,j} \sim \mathcal{N}(0, P_{en}\mathbf{I}_{G_e})$. The instantaneous SNRs for the $\mathcal{R}-\mathcal{D}$ and $\mathcal{R}-\mathcal{E}$ links are, respectively, defined as

$$\gamma_{rd} = \frac{P_r|\mathbf{h}_{rd}|^2}{P_{dn}} = \frac{\eta_r P_b}{P_{dn}}|\mathbf{h}_{br}|^2|\mathbf{h}_{rd}|^2, \tag{6}$$

$$\gamma_{re,j} = \frac{P_r|\mathbf{h}_{re,j}|^2}{P_{en}} = \frac{\eta_r P_b}{P_{en}}|\mathbf{h}_{br}|^2|\mathbf{h}_{re,j}|^2. \tag{7}$$

III. CHANNEL MODEL

In this section, the channel modeling of UOWC ($\mathcal{S}-\mathcal{R}$) and RF ($\mathcal{R}-\mathcal{D}$, $\mathcal{R}-\mathcal{E}$, $\mathcal{B}-\mathcal{R}$) links are realized for further mathematical analysis.

A. PDF AND CDF OF SNR FOR $\mathcal{S}-\mathcal{R}$ LINK

The PDF of γ_{sr} can be defined as [46, eq. (11)]

$$f_{\gamma_{sr}}(\gamma) = \sum_{i=1}^{2} B_i \gamma^{-1} G_{1,2}^{2,0}\left(Z_i \gamma^{V_i} \middle| \begin{matrix} W_i \\ S_i, K_i \end{matrix}\right), \tag{8}$$

where $B_1 = \frac{\omega\xi^2}{\epsilon}$, $B_2 = \frac{\xi^2(1-\omega)}{\epsilon\Gamma(a)}$, $Z_1 = \frac{1}{\mho A_0 \psi_\epsilon^{1/\epsilon}}$, $Z_2 = \frac{1}{A_0^c \sigma^c \psi_\epsilon^{c/\epsilon}}$, $V_1 = \frac{1}{\epsilon}$, $V_2 = \frac{c}{\epsilon}$, $W_1 = \xi^2 + 1$, $W_2 = \frac{\xi^2}{c} + 1$, $S_1 = 1$, $S_2 = a$, $K_1 = \xi^2$, $K_2 = \frac{\xi^2}{c}$, $\psi_1 = \Phi_{sr}$, $\psi_2 = \frac{\Phi_{sr}}{2\omega\mho^2 + \sigma^2(1-\omega)\frac{\Gamma(a+\frac{2}{c})}{\Gamma(a)}}$, the average SNR of $\mathcal{S}-\mathcal{R}$ link is indicated by Φ_{sr}, $\mathcal{S}-\mathcal{R}$ link's electrical SNR is defined by ψ_ϵ, and ϵ represents the detection technique (e.g., $\epsilon = 1$ indicates HD technique and $\epsilon = 2$ implies IM/DD technique). The exponential distribution parameter is represented by $\mho$, three GG distributed constraints are symbolized by a, σ, and c, the weight of the mixture is denoted by $0 < \omega < 1$, and the pointing error is indicated by ξ whereas A_0 is a constant corresponding to ξ. The values of ω, $\mho$, a, σ, and c are determined experimentally based on varying UWT (mild to severe) due to varying levels of air bubbles, temperature gradients, and water salinity. According to [55, Table I], increasing the temperature gradient and/or the level of air bubbles causes mild to severe UWT, which significantly raises the scintillation index. Reference [55, Table II] further displays several UWT scenarios in a thermally uniform UOWC network for fresh and salty waters. Therefore, the CDF of γ_{sr} is given as

$$F_{\gamma_{sr}}(\gamma) = \int_0^{\gamma} f_{\gamma_{sr}}(\gamma) d\gamma. \tag{9}$$

Substituting (8) into (9), $F_{\gamma_{sr}}(\gamma)$ is obtained finally as

$$F_{\gamma_{sr}}(\gamma) = \sum_{i=1}^{2} Y_i G_{2,3}^{2,1}\left(Z_i \gamma^{V_i} \middle| \begin{matrix} 1, W_i \\ S_i, K_i, 0 \end{matrix}\right), \tag{10}$$

where $Y_1 = \omega\xi^2$ and $Y_2 = \frac{\xi^2(1-\omega)}{c\Gamma(a)}$.

B. PDF AND CDF OF SNR FOR $\mathcal{R}-\mathcal{D}$ LINK

The PDF of γ_{rd} is defined as [63, eq. (4)]

$$f_{\gamma_{rd}}(\gamma) = \alpha_1 e^{-\Xi_2\gamma} \gamma^{\mu_d - 1} {}_1F_1(m_d, \mu_d; \alpha_2\gamma), \tag{11}$$

where

$$\alpha_1 = \frac{(G_d\mu_d)^{G_d\mu_d}(G_d m_d)^{G_d m_d}(1+\kappa_d)^{G_d\mu_d}}{\Gamma(G_d\mu_d)(\Phi_{rd})^{G_d\mu_d}(G_d\mu_d\kappa_d + G_d m_d)^{G_d m_d}},$$
$$\Xi_2 = \frac{G_d\mu_d(1+\kappa_d)}{\Phi_{rd}},$$
$$\alpha_2 = \frac{G_d^2\mu_d^2\kappa_d(1+\kappa_d)}{(G_d\mu_d\kappa_d + G_d m_d)\Phi_{rd}},$$

the average SNR of $\mathcal{R}-\mathcal{D}$ link is denoted by Φ_{rd}, G_d indicates the number of antennas of each user, the ratio of the powers of the dominant and scattered components, the number of clusters, and the Nakagami-m faded shadowing parameter are symbolized by κ_d, μ_d, and m_d, respectively. Here, ${}_1F_1(.,.;.)$ represents the confluent hypergeometric function that can be expressed as ${}_1F_1(l_4, l_5; l_6) = \frac{\Gamma(l_5)}{\Gamma(l_4)}\sum_{i_1=0}^{\infty}\frac{\Gamma(i_1+l_4)l_6^{i_1}}{\Gamma(i_1+l_5)i_1!}$ [64, eq. (13)]. Finally, $f_{\gamma_{rd}}(\gamma)$ can be written as [63, eq. (5)]

$$f_{\gamma_{rd}}(\gamma) = \sum_{e_1=0}^{\infty} \Xi_1 e^{-\Xi_2\gamma}\gamma^{\Xi_3}, \tag{12}$$

where $\Xi_1 = \alpha_1\alpha_3$, $\alpha_3 = \frac{\Gamma(G_d\mu_d)}{\Gamma(G_d m_d)}\frac{\Gamma(G_d m_d + e_1)\alpha_2^{e_1}}{\Gamma(G_d\mu_d + e_1)e_1!}$, and $\Xi_3 = G_d\mu_d - 1 + e_1$. Similar to (9), utilizing the formula [65, eq. (3).351.1], the CDF of γ_{rd} is formulated as

$$F_{\gamma_{rd}}(\gamma) = \sum_{e_1=0}^{\infty}\Xi_1\left(\frac{\Xi_3!}{\Xi_2^{\Xi_3+1}} - \sum_{e_2=0}^{\Xi_3}\frac{\Xi_3!}{e_2!\Xi_2^{\Xi_3-e_2+1}}e^{-\Xi_2\gamma}\gamma^{e_2}\right). \tag{13}$$

C. PDF AND CDF OF SNR FOR $\mathcal{R}-\mathcal{E}$ LINK

The PDF of $\gamma_{re,j}$ can be expressed as [63, eq. (5)]

$$f_{\gamma_{re,j}}(\gamma) = \sum_{f_1=0}^{\infty} \Xi_4 e^{-\Xi_5\gamma}\gamma^{\Xi_6}, \tag{14}$$

where

$$\Xi_4 = \beta_1\beta_3,$$
$$\Xi_5 = \frac{G_e\mu_e(1+\kappa_e)}{\Phi_{re}},$$
$$\Xi_6 = G_e\mu_e - 1 + f_1,$$
$$\beta_1 = \frac{(G_e\mu_e)^{G_e\mu_e}(G_em_e)^{G_em_e}(1+\kappa_e)^{G_e\mu_e}}{\Gamma(G_e\mu_e)(\Phi_{re})^{G_e\mu_e}(G_e\mu_e\kappa_e + G_em_e)^{G_em_e}},$$
$$\beta_2 = \frac{G_e^2\mu_e^2\kappa_e(1+\kappa_e)}{(G_e\mu_e\kappa_e + G_em_e)\Phi_{re}},$$
$$\beta_3 = \frac{\Gamma(G_e\mu_e)}{\Gamma(G_em_e)}\frac{\Gamma(G_em_e+f_1)\beta_2^{f_1}}{\Gamma(G_e\mu_e+f_1)f_1!},$$

Φ_{re} is the average SNR of $\mathcal{R}-\mathcal{E}$ link, G_e indicates the number of antennas of each eavesdropper, and the fading and shadowing parameters regarding $\mathcal{R}-\mathcal{E}$ link are indicated by κ_e, μ_e, and m_e. The CDF of $\gamma_{re,j}$ can be derived from (14) making use of [65, eq. (3).351.2] as

$$F_{\gamma_{re,j}}(\gamma) = 1 - \sum_{f_1=0}^{\infty}\sum_{p_1=0}^{\Xi_6}\frac{\Xi_6!}{p_1!\Xi_5^{\Xi_6-p_1+1}}\Xi_4 e^{-\Xi_5\gamma}\gamma^{p_1}. \quad (15)$$

1) SCENARIO-I

For the colluding eavesdroppers, we substitute Φ_{re}, G_e, μ_e, and m_e with $\mathcal{N}_{eI}\Phi_{re}$, $\mathcal{N}_{eI}G_e$, $\mathcal{N}_{eI}\mu_e$, and $\mathcal{N}_{eI}m_e$, respectively, based on the MRC technique [66]. Here, $\mathcal{N}_{eI}$ indicates the number of colluding eavesdroppers. For this scenario, the PDF of the instantaneous SNR of $\mathcal{R}-\mathcal{E}$ link denoted by γ_{re} is obtained as

$$f^{I}_{\gamma_{re}}(\gamma) = \sum_{f_2=0}^{\infty}\widetilde{\Xi}_4 e^{-\widetilde{\Xi}_5\gamma}\gamma^{\widetilde{\Xi}_6}, \quad (16)$$

where

$$\widetilde{\Xi}_4 = \tilde{\beta}_1\tilde{\beta}_3,$$
$$\widetilde{\Xi}_5 = \frac{\mathcal{N}_{eI}G_e\mu_e(1+\kappa_e)}{\mathcal{N}_{eI}\Phi_{re}},$$
$$\widetilde{\Xi}_6 = \mathcal{N}_{eI}G_e\mu_e - 1 + f_2,$$
$$\tilde{\beta}_1 = \frac{(\mathcal{N}_{eI}G_e\mu_e)^{\mathcal{N}_{eI}G_e\mu_e}(\mathcal{N}_{eI}G_em_e)^{\mathcal{N}_{eI}G_em_e}}{\Gamma(\mathcal{N}_{eI}G_e\mu_e)(\mathcal{N}_{eI}\Phi_{re})^{\mathcal{N}_{eI}G_e\mu_e}} \times \frac{(1+\kappa_e)^{\mathcal{N}_{eI}G_e\mu_e}}{(\mathcal{N}_{eI}G_e\mu_e\kappa_e + \mathcal{N}_{eI}G_em_e)^{\mathcal{N}_{eI}G_em_e}},$$
$$\tilde{\beta}_2 = \frac{(\mathcal{N}_{eI}G_e)^2\mu_e^2\kappa_e(1+\kappa_e)}{(\mathcal{N}_{eI}G_e\mu_e\kappa_e + \mathcal{N}_{eI}G_em_e)\mathcal{N}_{eI}\Phi_{re}},$$
$$\tilde{\beta}_3 = \frac{\Gamma(\mathcal{N}_{eI}G_e\mu_e)}{\Gamma(\mathcal{N}_{eI}G_em_e)}\frac{\Gamma(\mathcal{N}_{eI}G_em_e+f_2)(\tilde{\beta}_2)^{f_2}}{\Gamma(\mathcal{N}_{eI}G_e\mu_e+f_2)f_2!}.$$

2) SCENARIO-II

In the scenario of non-colluding eavesdroppers, the PDF of instantaneous SNR is obtained utilizing the *max* algorithm of order statistics as [54, eq. (4)]

$$f^{II}_{\gamma_{re}}(\gamma) = \mathcal{N}_{eII}\Big[F_{\gamma_{re,J}}(\gamma)\Big]^{\mathcal{N}_{eII}-1} f_{\gamma_{re,J}}(\gamma), \quad (17)$$

where $\mathcal{N}_{eII}$ indicates the number of non-colluding eavesdroppers. Substituting (14) and (15) into (17), $f^{II}_{\gamma_{re}}(\gamma)$ is outlined as

$$f^{II}_{\gamma_{re}}(\gamma) = \mathcal{N}_{eII}\Bigg[1 - \sum_{f_1=0}^{\infty}\sum_{p_4=0}^{\Xi_6}\frac{\Xi_6!}{p_4!\Xi_5^{\Xi_6-p_4+1}}\Xi_4 e^{-\Xi_5\gamma}\gamma^{p_4}\Bigg]^{\mathcal{N}_{eII}-1} \times \sum_{f_1=0}^{\infty}\Xi_4 e^{-\Xi_5\gamma}\gamma^{\Xi_6}. \quad (18)$$

Utilizing the binomial theorem [65, eq. (1).111] and performing some mathematical manipulations, Eq. (18) is formulated as

$$f^{II}_{\gamma_{re}}(\gamma) = \mathcal{N}_{eII}\sum_{f_1=0}^{\infty}\Xi_4 e^{-\Xi_5\gamma}\gamma^{\Xi_6}\Bigg[\sum_{h_1=0}^{\mathcal{N}_{eII}-1}\binom{\mathcal{N}_{eII}-1}{h_1}(-1)^{h_1} \times \Bigg(\sum_{f_1=0}^{\infty}\sum_{p_4=0}^{\Xi_6}\frac{\Xi_6!}{p_4!\Xi_5^{\Xi_6-p_4+1}}\Xi_4 e^{-\Xi_5\gamma}\gamma^{p_4}\Bigg)^{h_1}\Bigg]$$
$$= \mathcal{N}_{eII}\sum_{f_1=0}^{\infty}\Xi_4 e^{-\Xi_5\gamma}\gamma^{\Xi_6}\Bigg[\sum_{h_1=0}^{\mathcal{N}_{eII}-1}\binom{\mathcal{N}_{eII}-1}{h_1}(-1)^{h_1} \times \Bigg(\sum_{f_1=0}^{\infty}\Xi_4 e^{-\Xi_5\gamma}\Bigg)^{h_1}\Bigg(\sum_{p_4=0}^{\Xi_6}\frac{\Xi_6!}{p_4!}\frac{\gamma^{p_4}}{\Xi_5^{\Xi_6-p_4+1}}\Bigg)^{h_1}\Bigg]. \quad (19)$$

Since $(\sum_{p_4=0}^{\Xi_6}\frac{\Xi_6!}{p_4!}\frac{\gamma^{p_4}}{\Xi_5^{\Xi_6-p_4+1}})^{h_1}$ portion of (19) is normally difficult to solve, we use the multinomial theorem [67] to it. Applying the multinomial theorem, we write $(\sum_{p_4=0}^{\Xi_6}\frac{\Xi_6!}{p_4!}\frac{\gamma^{p_4}}{\Xi_5^{\Xi_6-p_4+1}})^{h_1}$ portion as

$$\Bigg(\sum_{p_4=0}^{\Xi_6}\frac{\Xi_6!}{p_4!}\frac{\gamma^{p_4}}{\Xi_5^{\Xi_6-p_4+1}}\Bigg)^{h_1} = \sum_{q_0+q_1+\ldots+q_{\Xi_6}=h_1}\binom{h_1}{q_0,q_1,\ldots,q_{\Xi_6}} \times \prod_{p_4}\Bigg(\frac{\Xi_6!}{p_4!\Xi_5^{\Xi_6-p_4+1}}\Bigg)^{q_{p_4}}\gamma^{\sum_{p_4}p_4q_{p_4}}. \quad (20)$$

Substituting (20) in (19) and performing some mathematical manipulations, $f^{II}_{\gamma_{re}}(\gamma)$ is finally derived as

$$f^{II}_{\gamma_{re}}(\gamma) = \mathcal{N}_{eII}\sum_{f_1=0}^{\infty}\sum_{h_1=0}^{\mathcal{N}_{eII}-1}\sum_{q_0+q_1+\ldots+q_{\Xi_6}=h_1}\prod_{p_4}\binom{\mathcal{N}_{eII}-1}{h_1} \times \binom{h_1}{q_0,q_1,\ldots,q_{\Xi_6}}\Bigg(\frac{\Xi_6!}{p_4!\Xi_5^{\Xi_6-p_4+1}}\Bigg)^{q_{p_4}}\Bigg(\sum_{f_1=0}^{\infty}\Xi_4\Bigg)^{h_1} \times (-1)^{h_1}\Xi_4 e^{-\gamma(\Xi_5+\Xi_5h_1)}\gamma^{\mathcal{X}_3}, \quad (21)$$

where $\mathcal{X}_3 = \sum_{p_1}p_1q_{p_1} + \Xi_6$.

D. PDF AND CDF OF SNR FOR $\mathcal{B}-\mathcal{R}$ LINK

The PDF of γ_{br} can be addressed as [63, eq. (5)]

$$f_{\gamma_{br}}(\gamma)=\sum_{g_1=0}^{\infty}\Xi_7 e^{-\Xi_8\gamma}\gamma^{\Xi_9}, \tag{22}$$

where

$$\begin{aligned}
\Xi_7&=\lambda_1\lambda_3,\\
\Xi_8&=\frac{G_b\mu_b(1+\kappa_b)}{\Phi_{br}},\\
\Xi_9&=G_b\mu_b-1+g_1,\\
\lambda_1&=\frac{(G_b\mu_b)^{G_b\mu_b}(G_bm_b)^{G_bm_b}(1+\kappa_b)^{G_b\mu_b}}{\Gamma(G_b\mu_b)(\Phi_{br})^{G_b\mu_b}(G_b\mu_b\kappa_b+G_bm_b)^{G_bm_b}},\\
\lambda_2&=\frac{G_b^2\mu_b^2\kappa_b(1+\kappa_b)}{(G_b\mu_b\kappa_b+G_bm_b)\Phi_{br}},\\
\lambda_3&=\frac{\Gamma(G_b\mu_b)}{\Gamma(G_bm_b)}\frac{\Gamma(G_bm_b+g_1)\lambda_2^{g_1}}{\Gamma(G_b\mu_b+g_1)g_1!},
\end{aligned}$$

the average SNR of $\mathcal{B}-\mathcal{R}$ link is defined by Φ_{br}, G_b indicates the number of antennas of the beacon, and similar to $\mathcal{R}-\mathcal{D}$ link, the channel parameters corresponding to $\mathcal{B}-\mathcal{R}$ link are denoted by κ_b, μ_b, and m_b. Therefore, the CDF of γ_{br} is expressed as

$$F_{\gamma_{br}}(\gamma)=\sum_{g_1=0}^{\infty}\Xi_7\left(\frac{\Xi_9!}{\Xi_8^{\Xi_9+1}}-\sum_{g_2=0}^{\Xi_9}\frac{\Xi_9!}{g_2!\Xi_8^{\Xi_9-g_2+1}}e^{-\Xi_8\gamma}\gamma^{g_2}\right). \tag{23}$$

IV. PERFORMANCE METRICS

SOP, SPSC, and EST are three key performance parameters that are frequently utilized to evaluate physical layer secrecy performance. This section demonstrates closed-form expressions for those performance metrics.

A. SECRECY OUTAGE PROBABILITY ANALYSIS

For the first and second hops, the instantaneous secrecy capacities (SC) are defined, respectively, as

$$C_{sr}=\frac{1}{2}\log_2(1+\gamma_{sr}), \tag{24}$$

$$C_{rd}=\left\{\frac{1}{2}\left[\log_2(1+\gamma_{rd})-\log_2\left(1+\gamma_{re,j}\right)\right]\right\}^{+}, \tag{25}$$

where $\{z\}^+=\max(z,0)$. Furthermore, the well-known *max-flow min-cut* theory states that the system's instantaneous capability (C_m) is restricted by the nominal capacity of the two hops and it is defined as [68, eq. (14)]

$$C_m=\min(C_{sr},C_{rd}). \tag{26}$$

The SOP is the probability of C_m falling below a target secrecy rate, R_s ($R_s>0$), expressed as

$$\begin{aligned}
\text{SOP}&=\Pr\{C_m<R_s\}\\
&=\Pr\{\min(C_{sr},C_{rd})<R_s\}\\
&=1-\Pr\{\min(C_{sr},C_{rd})\geq R_s\}\\
&=1-\Pr\{C_{sr}\geq R_s\}\Pr\{C_{rd}\geq R_s\},
\end{aligned} \tag{27}$$

where

$$\begin{aligned}
\Pr\{C_{sr}\geq R_s\}&=1-\Pr\{C_{sr}<R_s\}\\
&=1-\Pr\left\{\frac{1}{2}\log_2(1+\gamma_{sr})<R_s\right\}\\
&=1-\Pr\{\gamma_{sr}<\theta-1\}\\
&=1-F_{\gamma_{sr}}(\theta-1),
\end{aligned} \tag{28}$$

by defining $\theta=2^{2R_s}$. Substituting (10) into (28), $\Pr\{C_{sr}\geq R_s\}$ is formulated as

$$\Pr\{C_{sr}\geq R_s\}=1-\sum_{i=1}^{2}Y_iG_{2,3}^{2,1}\left(Z_i(\theta-1)^{V_i}\middle|\begin{matrix}1,W_i\\S_i,K_i,0\end{matrix}\right), \tag{29}$$

and

$$\begin{aligned}
&\Pr\{C_{rd}\geq R_s\}\\
&=\Pr\left\{\frac{1}{2}\left[\log_2(\gamma_{rd}+1)-\log_2\left(\gamma_{re,j}+1\right)\right]\geq R_s\right\}\\
&=\Pr\left\{\gamma_{rd}\geq\theta\gamma_{re,j}(\theta-1)\right\}\\
&=\Pr\left\{\frac{\eta_rP_b|\mathbf{h}_{br}|^2}{P_{dn}}\left(|\mathbf{h}_{rd}|^2-\theta\left|\mathbf{h}_{re,j}\right|^2\right)\geq\theta-1\right\}\\
&=\Pr\left\{|\mathbf{h}_{br}|^2w\geq D_0\right\},
\end{aligned} \tag{30}$$

where $D_0=\frac{(\theta-1)P_{dn}}{\eta_rP_b}$ and $w=|\mathbf{h}_{rd}|^2-\theta|\mathbf{h}_{re,j}|^2$. Here, the term P_{dn} is set to 1. To hold the inequality $|\mathbf{h}_{br}|^2w\geq D_0$, it has $w>0$. Hence, we obtain

$$\begin{aligned}
\Pr\{C_{rd}\geq R_s\}&=\Pr\left\{|\mathbf{h}_{br}|^2w\geq D_0,w>0\right\}\\
&=\int_0^{\infty}\int_{\frac{D_0}{w}}^{\infty}f_{\gamma_{br}}(\gamma)f_w(w)\,d\gamma\,dw,
\end{aligned} \tag{31}$$

where

$$f_w(w)=\int_0^{\infty}f_{\gamma_{rd}}(w+x)\frac{1}{\theta}f_{\gamma_{re,j}}\left(\frac{x}{\theta}\right)dx. \tag{32}$$

1) SCENARIO-I

In the scenario of colluding eavesdroppers, (31) is expressed as

$$\begin{aligned}
\Pr\left\{|\mathbf{h}_{br}|^2w\geq D_0,w>0\right\}&=\int_0^{\infty}\int_{\frac{D_0}{w}}^{\infty}f_{\gamma_{br}}(\gamma)f_w^I(w)\\
&\quad\times d\gamma\,dw,
\end{aligned} \tag{33}$$

where

$$f_w^I(w)=\int_0^{\infty}f_{\gamma_{rd}}(w+x)\frac{1}{\theta}f_{\gamma_{re}}^I\left(\frac{x}{\theta}\right)dx. \tag{34}$$

Placing (22), (12), and (16) into (33), Eq. (33) is finally derived as

$$\begin{aligned}
&\Pr\left\{|\mathbf{h}_{br}|^2w\geq D_0,w>0\right\}\\
&=\sum_{e_1=0}^{\infty}\sum_{f_2=0}^{\infty}\sum_{g_1=0}^{\infty}\sum_{t_1=0}^{\Xi_3}\sum_{t_2=0}^{\Xi_9}\binom{\Xi_3}{t_1}\left(\Xi_2+\frac{\widetilde{\Xi}_5}{\theta}\right)^{-(\widetilde{\Xi}_6+t_1+1)}\\
&\quad\times\frac{(\widetilde{\Xi}_6+t_1)!\mathcal{X}_2}{\theta^{\widetilde{\Xi}_6+1}}\frac{\Xi_9!D_0^{t_2}}{t_2!\Xi_8^{\Xi_9-t_2+1}}\left(\frac{\Xi_8D_0}{\Xi_2}\right)^{\frac{\Xi_3-t_1-t_2+1}{2}}
\end{aligned}$$

$$\times (\Xi_2\Xi_8 D_0)^{-\frac{(\Xi_3+t_1+t_2+1)}{2}} \times G_{0,2}^{2,0}\left(\Xi_2\Xi_8 D_0 \middle| \begin{matrix} - \\ \Xi_3+1, t_1+t_2 \end{matrix}\right). \quad (35)$$

Proof: See Appendix A. ■

Now, substituting (29) and (35) into (27), we finally obtain the SOP expression for Scenario-I that is presented in (36), shown at the bottom of the page.

Asymptotic Analysis: In the case of scenario-I, a tight asymptotic expression of SOP at high SNR can be obtained by means of using [69, eq. (2.9.1)] and [69, eq. (1.8.4)] as demonstrated in (37), shown at the bottom of the page, where $b_{j_1} = (\Xi_3+1, t_1+t_2)$, $\alpha_{k_1} = \beta_{j_1} = 1$ for the values of $k_1 = 1, \ldots, p_1$; $j_1 = 1, \ldots, m_1$, $a_{k_2} = (1, W_i)$, $b_{j_2} = (S_i, K_i, 0)$, and $\alpha_{k_2} = \beta_{j_2} = 1$ for the values of $k_2 = 1, \ldots, p_2$; $j_2 = 1, \ldots, m_2$.

2) SCENARIO-II

In the scenario with non-colluding eavesdroppers, Eq. (31) is expressed as

$$\Pr\left\{|\mathbf{h}_{br}|^2 w \geq D_0, w > 0\right\} = \int_0^\infty \int_{\frac{D_0}{w}}^\infty f_{\gamma_{br}}(\gamma) f_w^{II}(w) \times d\gamma\, dw, \quad (38)$$

where

$$f_w^{II}(w) = \int_0^\infty f_{\gamma_{rd}}(w+x)\frac{1}{\theta} f_{\gamma_{re}}^{II}\left(\frac{x}{\theta}\right) dx. \quad (39)$$

Substituting (22), (12), and (21) into (38), Eq. (38) is finally derived as shown in (40), shown at the bottom of the page, where $\mathcal{X}_5 = \Xi_1\Xi_4\Xi_7$.

Proof: See Appendix B. ■

Finally, placing (29) and (40) into (27), we obtain the SOP formula for scenario-II which is expressed in (41), shown at the bottom of the next page.

Asymptotic Analysis: In the case of scenario-II, following the similar procedure as utilized for scenario-I, a tight asymptotic expression of SOP at high SNR can be obtained as presented in (42), shown at the bottom of the page, where $b_{j_3} = (\Xi_3+1, t_3+t_4)$, and $\alpha_{k_3} = \beta_{j_3} = 1$ for the values of $k_3 = 1, \ldots, p_3$; $j_3 = 1, \ldots, m_3$.

B. STRICTLY POSITIVE SECRECY CAPACITY ANALYSIS

The probability of SPSC refers to the probability when $C_m > 0$. SPSC is a significant aspect of the system's secrecy transmission. Although analytical representation of the probability of SPSC can be simply generated from the SOP formulation, its physical significance is different from SOP. Hence, it can be defined as [70, eq. (48)]

$$\begin{aligned} \text{SPSC} &= \Pr\{C_m > 0\} \\ &= \Pr\{\min(C_{sr}, C_{rd}) > 0\} \\ &= \Pr\{C_{sr} > 0\}\Pr\{C_{rd} > 0\}, \end{aligned} \quad (43)$$

$$\text{SOP}^I = 1 - \left[\sum_{e_1=0}^{\infty}\sum_{f_2=0}^{\infty}\sum_{g_1=0}^{\infty}\sum_{t_1=0}^{\Xi_3}\sum_{t_2=0}^{\Xi_9}\binom{\Xi_3}{t_1}\left(\Xi_2+\frac{\widetilde{\Xi_5}}{\theta}\right)^{-(\widetilde{\Xi_6}+t_1+1)}\frac{(\widetilde{\Xi_6}+t_1)!\mathcal{X}_2}{\theta^{\widetilde{\Xi_6}+1}}\frac{\Xi_9! D_0^{t_2}}{t_2!\Xi_8^{\Xi_9-t_2+1}}\left(\frac{\Xi_8 D_0}{\Xi_2}\right)^{\frac{\Xi_3-t_1-t_2+1}{2}} \times (\Xi_2\Xi_8 D_0)^{-\frac{(\Xi_3+t_1+t_2+1)}{2}} G_{0,2}^{2,0}\left(\Xi_2\Xi_8 D_0 \middle| \begin{matrix} - \\ \Xi_3+1, t_1+t_2 \end{matrix}\right)\right]\left[1 - \sum_{i=1}^{2} Y_i G_{2,3}^{2,1}\left(Z_i(\theta-1)^{V_i} \middle| \begin{matrix} 1, W_i \\ S_i, K_i, 0 \end{matrix}\right)\right] \quad (36)$$

$$\text{SOP}_{(\infty)}^I = 1 - \left[\sum_{e_1=0}^{\infty}\sum_{f_2=0}^{\infty}\sum_{g_1=0}^{\infty}\sum_{t_1=0}^{\Xi_3}\sum_{t_2=0}^{\Xi_9}\sum_{j_1=1}^{m_1=2}\binom{\Xi_3}{t_1}\left(\Xi_2+\frac{\widetilde{\Xi_5}}{\theta}\right)^{-(\widetilde{\Xi_6}+t_1+1)}\frac{(\widetilde{\Xi_6}+t_1)!\mathcal{X}_2}{\theta^{\widetilde{\Xi_6}+1}}\frac{\Xi_9! D_0^{t_2}}{t_2!\Xi_8^{\Xi_9-t_2+1}}\left(\frac{\Xi_8 D_0}{\Xi_2}\right)^{\frac{\Xi_3-t_1-t_2+1}{2}} \times (\Xi_2\Xi_8 D_0)^{-\frac{(\Xi_3+t_1+t_2+1)}{2}}(\Xi_2\Xi_8 D_0)^{\frac{b_{j_1}}{\beta_{j_1}}}\frac{\prod_{k_1=1;k_1\neq j_1}^{m_1=2}\Gamma\left(b_{k_1}-b_{j_1}\frac{\beta_{k_1}}{\beta_{j_1}}\right)}{\beta_{j_1}}\right]\left[1 - \sum_{i=1}^{2}\sum_{j_2=1}^{m_2=2} Y_i \frac{1}{\beta_{j_2}}\left(Z_i(\theta-1)^{V_i}\right)^{\frac{b_{j_2}}{\beta_{j_2}}} \times \frac{\prod_{k_2=1;k_2\neq j_2}^{m_2=2}\Gamma\left(b_{k_2}-b_{j_2}\frac{\beta_{k_2}}{\beta_{j_2}}\right)\prod_{k_2=1}^{n_2=1}\Gamma\left(1-a_{k_2}+b_{j_2}\frac{\alpha_{k_2}}{\beta_{j_2}}\right)}{\prod_{k_2=n_2+1}^{p_2=2}\Gamma\left(a_{k_2}-b_{j_2}\frac{\alpha_{k_2}}{\beta_{j_2}}\right)\prod_{k_2=m_2+1}^{q_2=3}\Gamma\left(1-b_{k_2}+b_{j_2}\frac{\beta_{k_2}}{\beta_{j_2}}\right)}\right] \quad (37)$$

$$\Pr\left\{|\mathbf{h}_{br}|^2 w \geq D_0, w > 0\right\} = \mathcal{N}_{eII}\sum_{e_1=0}^{\infty}\sum_{f_1=0}^{\infty}\sum_{g_1=0}^{\infty}\sum_{h_1=0}^{\mathcal{N}_{eII}-1}\sum_{t_3=0}^{\Xi_3}\sum_{t_4=0}^{\Xi_9}\sum_{q_0+q_1+\ldots+q_{\Xi_6}=h_1}\prod_{p_4}\binom{\mathcal{N}_{eII}-1}{h_1}\binom{\Xi_3}{t_3}\binom{h_1}{q_0, q_1, \ldots, q_{\Xi_6}} \times \left(\frac{\Xi_6!}{p_4!\Xi_5^{\Xi_6-p_4+1}}\right)^{q_{p_4}}\left(\sum_{f_1=0}^{\infty}\Xi_4\right)^{h_1}\left(\Xi_2+\frac{\Xi_5 h_1}{\theta}+\frac{\Xi_5}{\theta}\right)^{-(\mathcal{X}_4+1)}(-1)^{h_1}\frac{\mathcal{X}_4!\mathcal{X}_5}{\theta^{\mathcal{X}_3+1}}\frac{\Xi_9! D_0^{t_4}}{t_4!\Xi_8^{\Xi_9-t_4+1}} \times \left(\frac{\Xi_8 D_0}{\Xi_2}\right)^{\frac{\Xi_3-t_3-t_4+1}{2}}(\Xi_2\Xi_8 D_0)^{-\frac{(\Xi_3+t_3+t_4+1)}{2}} G_{0,2}^{2,0}\left(\Xi_2\Xi_8 D_0 \middle| \begin{matrix} - \\ \Xi_3+1, t_3+t_4 \end{matrix}\right) \quad (40)$$

where

$$\Pr\{C_{sr} > 0\} = \Pr\left\{\frac{1}{2}\log_2(1+\gamma_{sr}) > 0\right\} = \Pr\{\gamma_{sr} > 0\} = 1, \tag{44}$$

and

$$\begin{aligned}\Pr\{C_{rd} > 0\} &= \Pr\left\{\frac{1}{2}\left[\log_2(1+\gamma_{rd}) - \log_2\left(1+\gamma_{re,j}\right)\right] > 0\right\} \\ &= 1 - \Pr\left\{\gamma_{rd} \le \gamma_{re,j}\right\} \\ &= 1 - \Pr\left\{|\mathbf{h}_{rd}|^2 \le \left|\mathbf{h}_{re,j}\right|^2\right\} \\ &= 1 - \int_0^{\infty}\int_0^{v} f_{\gamma_{rd}}(u) f_{\gamma_{re,j}}(v) du dv. \end{aligned} \tag{45}$$

1) SCENARIO-I

For the scenario of colluding eavesdroppers, (45) is expressed as

$$\Pr\{C_{rd} > 0\} = 1 - \int_0^{\infty}\int_0^{v} f_{\gamma_{rd}}(u) f^{I}_{\gamma_{re}}(v) du dv. \tag{46}$$

Placing (12) and (16) into (46), Eq. (46) is formulated as

$$\begin{aligned}&\Pr\{C_{rd} > 0\} \\ &= 1 - \left[\sum_{e_1=0}^{\infty}\sum_{f_2=0}^{\infty} \mathcal{X}_1 \left(\frac{\Xi_3!\widetilde{\Xi}_6!}{\Xi_2^{\Xi_3+1}}\widetilde{\Xi}_5^{-(\widetilde{\Xi}_6+1)} - \sum_{t_5=0}^{\Xi_3}\frac{\Xi_3!}{t_5!}\right.\right. \\ &\quad \left.\left. \times \frac{(\widetilde{\Xi}_6+t_5)!}{\Xi_2^{\Xi_3-t_5+1}}(\Xi_2+\widetilde{\Xi}_5)^{-(\widetilde{\Xi}_6+t_5+1)}\right)\right]. \end{aligned} \tag{47}$$

where $\mathcal{X}_1 = \Xi_1\widetilde{\Xi}_4$.

Proof: See Appendix C. ■

Placing (44) and (47) into (43), The formula of SPSC for the scenario-I is expressed as

$$\begin{aligned}\mathrm{SPSC}^{I} = 1 - \left[\sum_{e_1=0}^{\infty}\sum_{f_2=0}^{\infty} \mathcal{X}_1 \left(\frac{\Xi_3!\widetilde{\Xi}_6!}{\Xi_2^{\Xi_3+1}}\widetilde{\Xi}_5^{-(\widetilde{\Xi}_6+1)} - \sum_{t_5=0}^{\Xi_3}\frac{\Xi_3!}{t_5!}\right.\right. \\ \left.\left. \times \frac{(\widetilde{\Xi}_6+t_5)!}{\Xi_2^{\Xi_3-t_5+1}}(\Xi_2+\widetilde{\Xi}_5)^{-(\widetilde{\Xi}_6+t_5+1)}\right)\right]. \end{aligned} \tag{48}$$

2) SCENARIO-II

In the scenario of non-colluding eavesdroppers, $\Pr\{C_{rd} > 0\}$ is expressed as

$$\Pr\ \{C_{rd} > 0\} = 1 - \int_0^{\infty}\int_0^{v} f_{\gamma_{rd}}(u) f^{II}_{\gamma_{re}}(v) du dv. \tag{49}$$

Substituting (12) and (21) into (49), following the similar formulation procedure as utilized for scenario-I with some mathematical manipulations and simplifications, $\Pr\{C_{rd} > 0\}$ is derived as

$$\begin{aligned}&\Pr\{C_{rd} > 0\} \\ &= 1 - \left[\mathcal{N}_{eII}\sum_{e_1=0}^{\infty}\sum_{f_1=0}^{\infty}\sum_{h_1=0}^{\mathcal{N}_{eII}-1}\sum_{q_0+q_1+\ldots+q_{\Xi_6}=h_1}\prod_{p_4}\binom{\mathcal{N}_{eII}-1}{h_1}\right. \\ &\quad \left.\times \binom{h_1}{q_0, q_1, \ldots, q_{\Xi_6}}\left(\frac{\Xi_6!}{p_4!\Xi_5^{\Xi_6-p_4+1}}\right)^{q_{p_4}}\left(\sum_{f_1=0}^{\infty}\Xi_4\right)^{h_1}(-1)^{h_1}\right. \end{aligned}$$

$$\begin{aligned}\mathrm{SOP}^{II} = 1 - \left[\mathcal{N}_{eII}\sum_{e_1=0}^{\infty}\sum_{f_1=0}^{\infty}\sum_{g_1=0}^{\infty}\sum_{h_1=0}^{\mathcal{N}_{eII}-1}\sum_{t_3=0}^{\Xi_3}\sum_{t_4=0}^{\Xi_9}\sum_{q_0+q_1+\ldots+q_{\Xi_6}=h_1}\prod_{p_4}\binom{\mathcal{N}_{eII}-1}{h_1}\binom{\Xi_3}{t_3}\binom{h_1}{q_0, q_1, \ldots, q_{\Xi_6}}\right. \\ \times \left(\frac{\Xi_6!}{p_4!\Xi_5^{\Xi_6-p_4+1}}\right)^{q_{p_4}}\left(\sum_{f_1=0}^{\infty}\Xi_4\right)^{h_1}\left(\Xi_2 + \frac{\Xi_5 h_1}{\theta} + \frac{\Xi_5}{\theta}\right)^{-(\mathcal{X}_4+1)}(-1)^{h_1}\frac{\mathcal{X}_4!\mathcal{X}_5}{\theta^{\mathcal{X}_3+1}}\frac{\Xi_9!D_0^{t_4}}{t_4!\Xi_8^{\Xi_9-t_4+1}}\left(\frac{\Xi_8 D_0}{\Xi_2}\right)^{\frac{\Xi_3-t_3-t_4+1}{2}} \\ \left.\times (\Xi_2\Xi_8 D_0)^{-\frac{(\Xi_3+t_3+t_4+1)}{2}} G^{2,0}_{0,2}\left(\Xi_2\Xi_8 D_0 \middle| \begin{matrix} - \\ \Xi_3+1, t_3+t_4 \end{matrix}\right)\right]\left[1 - \sum_{i=1}^{2} Y_i G^{2,1}_{2,3}\left(Z_i(\theta-1)^{V_i}\middle| \begin{matrix} 1, W_i \\ S_i, K_i, 0 \end{matrix}\right)\right] \end{aligned} \tag{41}$$

$$\begin{aligned}\mathrm{SOP}^{II}_{(\infty)} = 1 - \left[\mathcal{N}_{eII}\sum_{e_1=0}^{\infty}\sum_{f_1=0}^{\infty}\sum_{g_1=0}^{\infty}\sum_{h_1=0}^{\mathcal{N}_{eII}-1}\sum_{t_3=0}^{\Xi_3}\sum_{t_4=0}^{\Xi_9}\sum_{j_3=1}^{m_3=2}\sum_{q_0+q_1+\ldots+q_{\Xi_6}=h_1}\prod_{p_4}\binom{\mathcal{N}_{eII}-1}{h_1}\binom{\Xi_3}{t_3}\binom{h_1}{q_0, q_1, \ldots, q_{\Xi_6}}\right. \\ \times \left(\frac{\Xi_6!}{p_4!\Xi_5^{\Xi_6-p_4+1}}\right)^{q_{p_4}}\left(\sum_{f_1=0}^{\infty}\Xi_4\right)^{h_1}\left(\Xi_2 + \frac{\Xi_5 h_1}{\theta} + \frac{\Xi_5}{\theta}\right)^{-(\mathcal{X}_4+1)}(-1)^{h_1}\frac{\mathcal{X}_4!\mathcal{X}_5}{\theta^{\mathcal{X}_3+1}}\frac{\Xi_9!D_0^{t_4}}{t_4!\Xi_8^{\Xi_9-t_4+1}}\left(\frac{\Xi_8 D_0}{\Xi_2}\right)^{\frac{\Xi_3-t_3-t_4+1}{2}} \\ \times (\Xi_2\Xi_8 D_0)^{-\frac{(\Xi_3+t_3+t_4+1)}{2}}(\Xi_2\Xi_8 D_0)^{\frac{b_{j_3}}{\beta_{j_3}}}\frac{\prod_{k_3=1;k_3\neq j_3}^{m_3=2}\Gamma\left(b_{k_3} - b_{j_3}\frac{\beta_{k_3}}{\beta_{j_3}}\right)}{\beta_{j_3}}\left]\left[1 - \sum_{i=1}^{2}\sum_{j_2=1}^{m_2=2} Y_i \frac{1}{\beta_{j_2}}\left(Z_i(\theta-1)^{V_i}\right)^{\frac{b_{j_2}}{\beta_{j_2}}}\right.\right. \\ \left.\left. \times \frac{\prod_{k_2=1;k_2\neq j_2}^{m_2=2}\Gamma\left(b_{k_2} - b_{j_2}\frac{\beta_{k_2}}{\beta_{j_2}}\right)\prod_{k_2=1}^{n_2=1}\Gamma\left(1-a_{k_2}+b_{j_2}\frac{\alpha_{k_2}}{\beta_{j_2}}\right)}{\prod_{k_2=n_2+1}^{p_2=2}\Gamma\left(a_{k_2} - b_{j_2}\frac{\alpha_{k_2}}{\beta_{j_2}}\right)\prod_{k_2=m_2+1}^{q_2=3}\Gamma\left(1-b_{k_2}+b_{j_2}\frac{\beta_{k_2}}{\beta_{j_2}}\right)}\right] \end{aligned} \tag{42}$$

$$\times \mathcal{X}_6 \left(\frac{\Xi_3! \mathcal{X}_3!}{\Xi_2^{\Xi_3+1}} (\Xi_5 + \Xi_5 h_1)^{-(\mathcal{X}_3+1)} - \sum_{t_6=0}^{\Xi_3} \frac{\Xi_3! \mathcal{X}_7!}{t_6! \Xi_2^{\Xi_3-t_6+1}} \times (\Xi_2 + \Xi_5 h_1 + \Xi_5)^{-(\mathcal{X}_7+1)} \right) \Bigg], \tag{50}$$

where $\mathcal{X}_6 = \Xi_1 \Xi_4$ and $\mathcal{X}_7 = \mathcal{X}_3 + t_6$. Substituting (44) and (50) into (43), we can finally demonstrate the formula of SPSC for scenario-II as presented in (51), shown at the bottom of the page.

C. EFFECTIVE SECRECY THROUGHPUT ANALYSIS

Another secrecy performance metric is EST, which assures confidential average throughput measurements. EST is calculated by multiplying the target secrecy rate with the probability of successful data transmission that is defined as

$$\text{EST} = R_s(1 - \text{SOP}). \tag{52}$$

1) SCENARIO-I

For colluding eavesdroppers, the formula of EST is expressed as

$$\text{EST}^I = R_s(1 - \text{SOP}^I). \tag{53}$$

2) SCENARIO-II

For non-colluding eavesdroppers, the formula of EST is expressed as

$$\text{EST}^{II} = R_s(1 - \text{SOP}^{II}). \tag{54}$$

V. NUMERICAL RESULTS

Selected simulation results due to mixed UOWC-RF model with the considered two different eavesdropping scenarios (colluding and non-colluding) are demonstrated and analyzed in this section, utilizing the obtained closed-form expressions of (36), (37), (41), (42), (48), (51), (53), and (54). In the simulation analysis, the impacts of detection techniques, various UWT scenarios, pointing error, fading and shadowing severity, number of diversity branches, number of eavesdroppers, energy conversion efficiency, power of power beacon, target secrecy rate, and average SNR values on secrecy performance are investigated. Similar to [71], we assume that the RF links have the following parameters: $G_d = G_b = G_e = 2$, $\kappa_d = \kappa_b = \kappa_e = 1$, $\mu_d = \mu_b = \mu_e = 1$, $m_d = m_b = m_e = 2$, $\eta_r = 0.7$, $P_b = 20$ dB, and $R_s = 0.05$ bits/sec/Hz, unless specified otherwise. On the other hand,

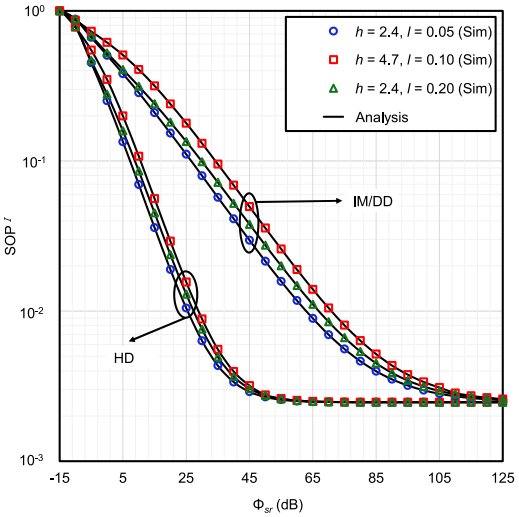

FIGURE 2. The SOP^I versus Φ_{sr} for selected values of h, l, and ϵ with $\mathcal{N}_{el} = 1$, $\Phi_{rd} = 15$ dB, $\Phi_{br} = 1$, and $\Phi_{re} = 0$ dB.

the values of h and l utilized in the first hop (UOWC link) are set according to [55] and inherited from Table 1 and Table 2. Unless otherwise mentioned, We also assume that the UOWC link has the following parameters: $h = 2.4$, $l = 0.05$, $\epsilon = 1$ (HD technique) or $\epsilon = 2$ (IM/DD technique), $A_0 = 1$, and $\xi = 0.8$. Note that Figs. 2-5 and Figs. 7-15 are illustrated for scenario-I (colluding eavesdropping mode) whereas Figs. 6 and 14 are depicted for scenario-II (non-colluding eavesdropping mode). Moreover, a fair comparison between colluding and non-colluding eavesdropping attacks is also presented in Figs. 16 and 17 in terms of EST and SOP analysis, respectively. In addressing the computational complexity inherent in the infinite series, we employ a strategic approach by truncating them to the first 25 terms. The Monte-Carlo (MC) simulated results, with 10^8 channel realizations and the analytical results, are utilized to generate all the graphs. Furthermore, the validity of our developed expressions is confirmed by the excellent match between theoretical and simulated results.

A. IMPACT OF UOWC LINK PARAMETERS

To assess the severity level of different turbulence (i.e., air bubbles level and temperature gradients) conditions, SOP^I is plotted as a function of Φ_{sr} in Fig. 2. It can be observed that secrecy performance decreases as the values of h and l increase. This is because an increase in the level of air bubbles and/or temperature gradient adversely affects the

$$\text{SPSC}^{II} = 1 - \Bigg[\mathcal{N}_{eII} \sum_{e_1=0}^{\infty} \sum_{f_1=0}^{\infty} \sum_{h_1=0}^{\mathcal{N}_{eII}-1} \sum_{q_0+q_1+\ldots+q_{\Xi_6}=h_1} \prod_{p_4} \binom{\mathcal{N}_{eII}-1}{h_1} \binom{h_1}{q_0, q_1, \ldots, q_{\Xi_6}} \left(\frac{\Xi_6!}{p_4! \Xi_5^{\Xi_6-p_4+1}} \right)^{q_{p_4}} \left(\sum_{f_1=0}^{\infty} \Xi_4 \right)^{h_1} \times (-1)^{h_1} \mathcal{X}_6 \left(\frac{\Xi_3! \mathcal{X}_3!}{\Xi_2^{\Xi_3+1}} (\Xi_5 + \Xi_5 h_1)^{-(\mathcal{X}_3+1)} - \sum_{t_6=0}^{\Xi_3} \frac{\Xi_3! \mathcal{X}_7!}{t_6! \Xi_2^{\Xi_3-t_6+1}} (\Xi_2 + \Xi_5 h_1 + \Xi_5)^{-(\mathcal{X}_7+1)} \right) \Bigg] \tag{51}$$

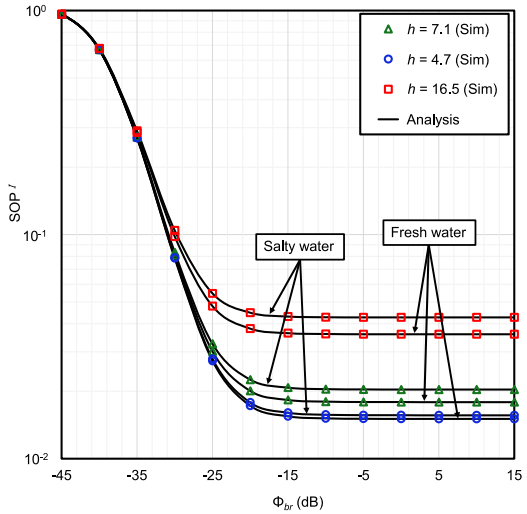

FIGURE 3. The SOP^I versus Φ_{br} for selected values of h for both salty and fresh water with $\epsilon = 1$, $\mathcal{N}_{el} = 1$, $\Phi_{sr} = 20$ dB, $\Phi_{rd} = 10$ dB, and $\Phi_{re} = -10$ dB.

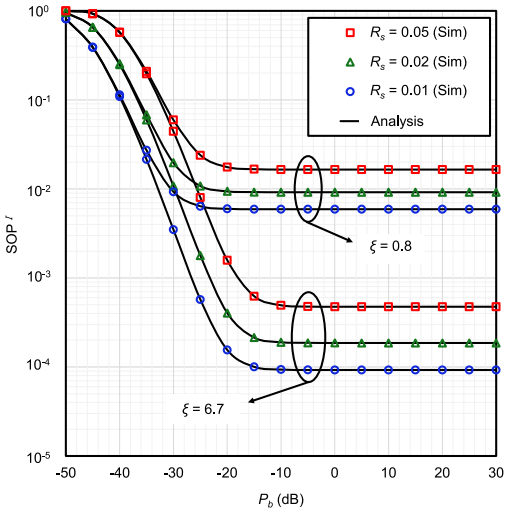

FIGURE 4. The SOP^I versus P_b (dB) for selected values of ξ and R_s with $\epsilon = 1$, $\mathcal{N}_{el} = 1$, $\Phi_{sr} = 20$ dB, $\Phi_{rd} = 30$ dB, $\Phi_{br} = 1$ dB, and $\Phi_{re} = -10$ dB.

scintillation index, which has a negative effect on the SOP performance. Therefore, it can be observed that utilizing the HD technique instead of the IM/DD technique significantly improves secrecy performance. This is as expected since the HD technique, relative to the IM/DD technique, can more easily overcome the impacts of turbulence conditions as testified in [46]. As noticed from the figure, the analytical results perfectly match with the MC simulation (denoted by markers). Additionally, it is demonstrated that SOP declines as Φ_{sr} increases proving that increasing Φ_{sr} enhances the secrecy performance.

In Fig. 3, SOP^I performance is analyzed graphically concerning Φ_{br} under uniform temperature conditions and varying air bubbles levels due to the UOWC link.

It is possible to conclude that secrecy performance increases as the turbulence severity decreases. Water salinity also has an impact on secrecy performance though it is not as significant as the UWT scenarios. Increased value of Φ_{br} results in a considerable decline of SOP. This is because as Φ_{br} increases, the strength of $\mathcal{B} - \mathcal{R}$ link improves, leading to a better SOP performance. However, a secrecy outage floor is observed in the figure after a certain value of Φ_{br}. This is due to the fact that the secrecy performance is influenced by the worse hop in the mixed UOWC-RF model implying the secrecy capacity is affected by the second hop in such a situation, which is not enhanced.

Fig. 4 depicts SOP^I against P_b under varying values of R_s to address the influence of pointing errors in the UOWC link.

As expected, the higher value of ξ (i.e., ξ=6.7) exhibits a better SOP performance than that of lower ξ (i.e., ξ=0.8). This is due to the fact that smaller ξ produces larger pointing errors in the receiver, which significantly distorts the signal that is received. As a result, the signal strength of $\mathcal{S} - \mathcal{R}$ link deteriorates and the system's secrecy performance weakens.

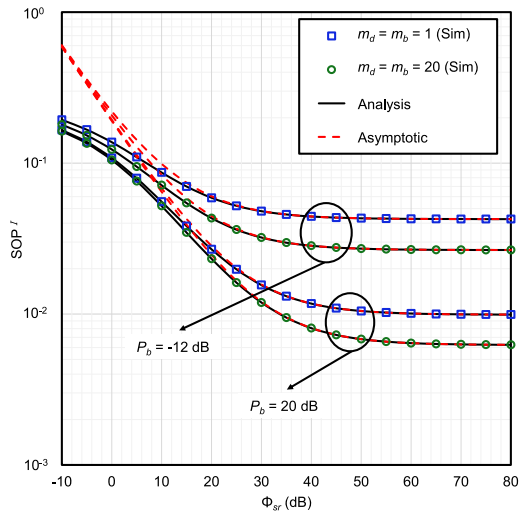

FIGURE 5. The SOP^I versus Φ_{sr} for selected values of m_d, m_b, and P_b with $\epsilon = 2$, $\xi \to \infty$, $m_e = 2$, $\mathcal{N}_{el} = 2$, $\Phi_{rd} = 15$ dB, $\Phi_{br} = 1$ dB, and $\Phi_{re} = 0$ dB.

In a similar context, it is realized that the SOP value falls significantly with decreasing R_s. This is because C_{sr} must be greater than R_s to achieve secure networking over the UOWC-RF link. However, increasing R_s increases the probability that C_{sr} will fall below R_s thereby raising the SOP value and as a result deteriorating the secrecy performance.

B. IMPACT OF RF LINK PARAMETERS

The performance analysis of SOP^I has been elucidated in Fig. 5 to analyze the impacts of shadowing severity and beacon's power for the considered UOWC-RF mixed model.

It is noticed that SOP^I increases as the value of m_d and m_b decreases. It is due to the fact that lowering the values of m_d and m_b reflects a stronger shadowing impact on the legitimate channel; hence the secrecy performance behaves inversely. Similarly, it is observed that SOP performance is greatly improved with increasing P_b from -12 dB to 20 dB.

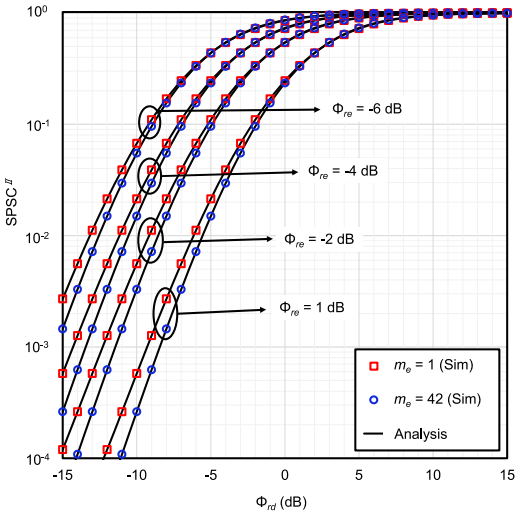

FIGURE 6. The SPSC^{II} versus Φ_{rd} for selected values of Φ_{re} and m_e with $\mathcal{N}_{eII} = 2$, $G_d = G_e = 2$, $\kappa_d = \kappa_e = 1$, $\mu_d = \mu_e = 1$, and $m_d = 2$.

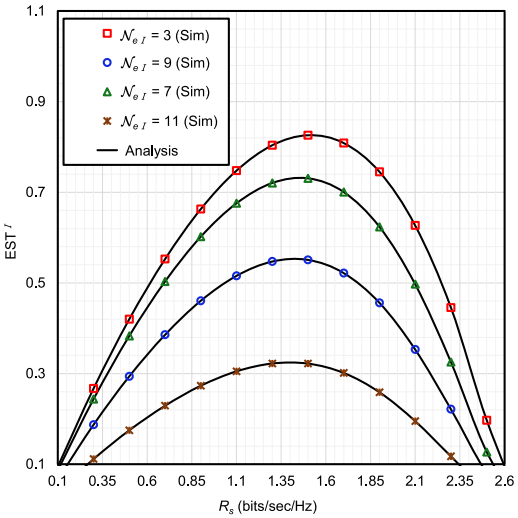

FIGURE 7. The EST^{I} versus R_s for selected values of $\mathcal{N}_{eI}$ with $\epsilon = 1$, $\Phi_{sr} = 15$ dB, $\Phi_{rd} = 25$ dB, $\Phi_{br} = 1$ dB, and $\Phi_{re} = 0$ dB.

This increase enhances the possibility of improved energy harvesting at the relay with higher transmission capacity. However, as Φ_{sr} increases, the SOP value declines noticeably demonstrating that increasing the value of Φ_{sr} improves secrecy performance. It is also observed that in high SNR, the asymptotic expression demonstrated in (37), converges quite fast to the exact result proving this asymptotic approximation to be tight enough.

In Fig. 6, SPSC^{II} is plotted against Φ_{rd} demonstrating the effects of the shadowing parameter of the eavesdropper channel.

It can be observed that the lower the value of m_e, the better the SOP performance. This is because the SNR values of $\mathcal{R} - \mathcal{E}$ link improve with the m_e as the impact of shadowing is reduced while all other parameters remain constant. It is also realized that reducing the value of Φ_{re} provides better secrecy performance of the system. On the other hand, Fig. 7 demonstrates the EST^{I} of the UOWC-RF mixed system for selected values of $\mathcal{N}_{eI}$ under various turbulence conditions to address the impact of colluding eavesdroppers and UWT severity.

Increasing the number of eavesdroppers decreases the secrecy performance, as noticed in the figure. It is expected since the probability of information leakage is enhanced drastically with the increase in eavesdroppers. Furthermore, the results of this figure reveal that EST improves with an increase in R_s to a specific threshold ($R_s = 1.55$ bits/sec/Hz) and subsequently declines with a further rise in R_s as shown in TABLE 1. This is because when R_s is lower, it is possible to achieve the desired secrecy performance with fewer resources. However, as R_s increases, greater resources are needed to counter the increased security risks, leading to decreased EST performance. In summary, the graph along with TABLE 1 illustrate stronger security measures offer diminishing returns in terms of EST performance.

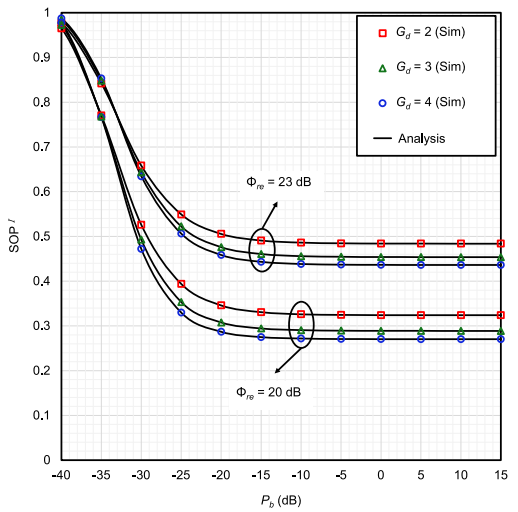

FIGURE 8. The SOP^{I} versus P_b for selected values of G_d and Φ_{re} with $\epsilon = 2$, $G_b = G_e = 2$, $\mathcal{N}_{eI} = 1$, $\Phi_{sr} = 15$ dB, $\Phi_{rd} = 25$ dB, and $\Phi_{br} = 1$ dB.

The influence of G_d and G_b on secrecy performance is investigated in Figs. 8-10. Under both scenarios, it is observed that the proposed model exhibits better secrecy as the values of G_d and G_b increase. In other words, having more antennas at the destination and power-beacon is beneficial to strengthen the secrecy behavior. This is owing to the fact that implementing antenna diversity at the $\mathcal{D}$ and $\mathcal{B}$ ensures reliable communication, which leads to improved security. More importantly, an increase in G_b increases the probability of exploiting more energy from the power-beacon to $\mathcal{R}$. On the other hand, it can be demonstrated that the higher value of P_b ensures a good reception with a higher probability at $\mathcal{D}$. Note that when $P_b > -15$ dB, all such curves flatten out due to the dominance of the system's first hop. It is also inspected in Fig. 9 that the asymptotic results tightly approximate with the closed form results. The theoretical and simulation results of SOP^{I} are compared in

TABLE 1. The EST^I versus R_s for selected values of $\mathcal{N}_{el}$.

R_s (bits/sec/Hz)	1.1	1.15	1.2	1.25	1.3	1.35	1.4	1.45	1.5	1.55	1.6	1.65	1.7
$\mathcal{N}_{eI}=3$ (Sim)	0.74785	0.76471	0.77969	0.79272	0.80373	0.81264	0.81937	0.82383	0.82593	0.82558	0.82268	0.81710	0.80876
$\mathcal{N}_{eI}=7$ (Sim)	0.67581	0.68993	0.70215	0.71239	0.72057	0.72660	0.73038	0.73183	0.73083	0.72730	0.72114	0.71224	0.70051
$\mathcal{N}_{eI}=9$ (Sim)	0.51565	0.52592	0.53466	0.54181	0.54728	0.55100	0.55291	0.55291	0.55094	0.54692	0.54076	0.53242	0.52181
$\mathcal{N}_{eI}=11$ (Sim)	0.30500	0.31078	0.31561	0.31945	0.32224	0.32394	0.32451	0.32389	0.32204	0.31891	0.31447	0.30868	0.30151

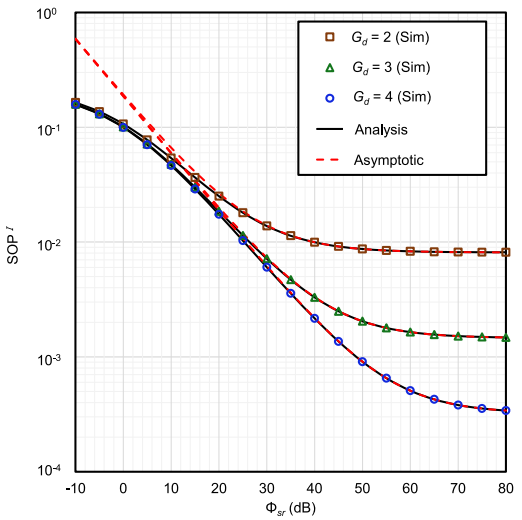

FIGURE 9. The SOP^I versus Φ_{sr} for selected values of G_d with $\epsilon = 2$, $\xi \to \infty$, $G_b = G_e = 2$, $\mathcal{N}_{el} = 2$, $\Phi_{rd} = 15$ dB, $\Phi_{br} = 1$ dB, and $\Phi_{re} = 0$ dB.

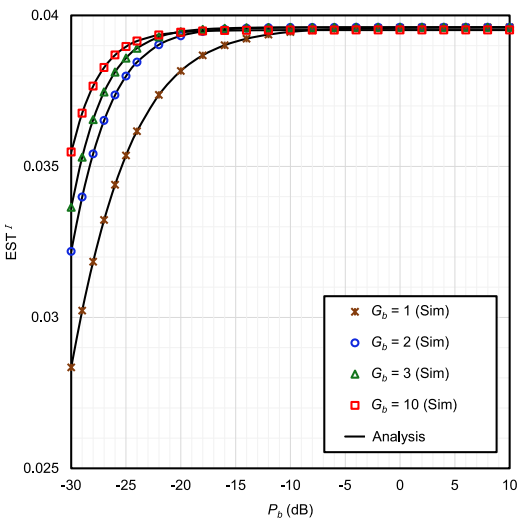

FIGURE 10. The EST^I versus P_b for selected values of G_b with $\epsilon = 2$, $G_d = G_e = 2$, $m_d = m_e = 2$, $m_b = 15$, $\mathcal{N}_{el} = 2$, $\Phi_{sr} = 15$ dB, $\Phi_{rd} = 25$ dB, $\Phi_{br} = 1$ dB, and $\Phi_{re} = 0$ dB.

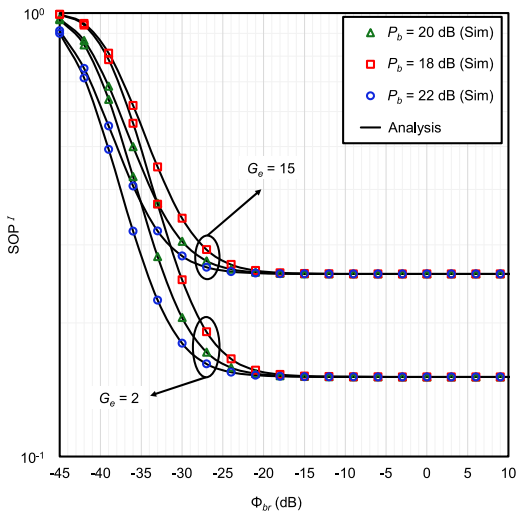

FIGURE 11. The SOP^I versus Φ_{br} for selected values of P_b and G_e with $\epsilon = 2$, $G_d = G_b = 2$, $\mathcal{N}_{el} = 2$, $\Phi_{sr} = 20$ dB, $\Phi_{rd} = 10$ dB, and $\Phi_{re} = -10$ dB.

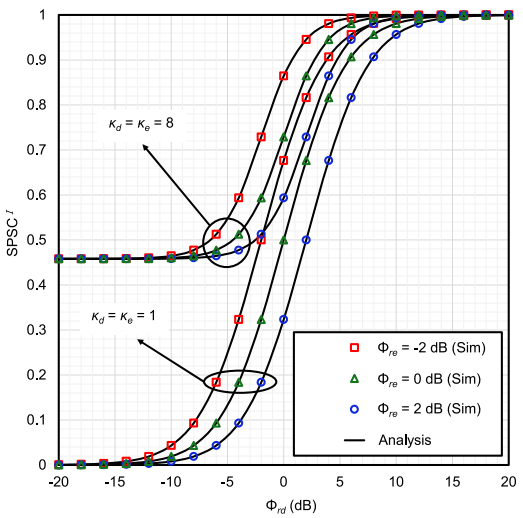

FIGURE 12. The SPSC^I versus Φ_{rd} for selected values of Φ_{re}, κ_d, and κ_e with $G_d = G_e = 2$, $\mu_d = \mu_e = 1$, $m_d = m_e = 2$, and $\mathcal{N}_{el} = 1$.

Fig. 11 to analyze the impact of G_e on secrecy performance. A clear decrease in the SOP performance is noticed with the increase of G_e. This is because when G_e increases, more confidential information is susceptible to the eavesdroppers thereby increasing the chances of eavesdropping.

The effect of various fading conditions on secrecy performance is investigated in Figs. 12-15, which are graphically represented in terms of the probability of SPSC and EST analysis. The results in Fig. 12 reveal that the probability of SPSC^I greatly improves as the combination of

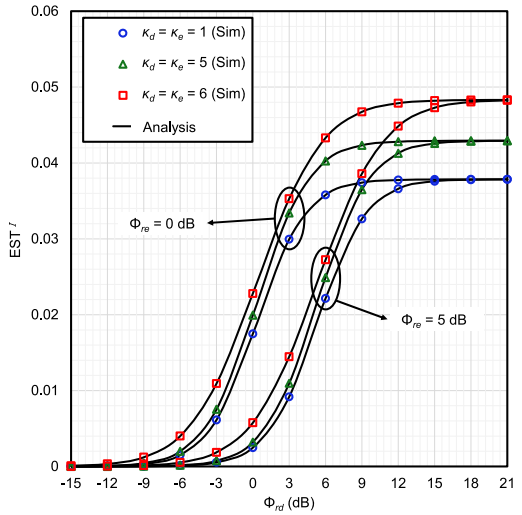

FIGURE 13. The EST^{I} versus Φ_{rd} for selected values of Φ_{re}, κ_d, and κ_e with $\epsilon = 1$, $\mathcal{N}_{el} = 1$, $\kappa_b = 1$, $\Phi_{sr} = 15$ dB, and $\Phi_{br} = 1$ dB.

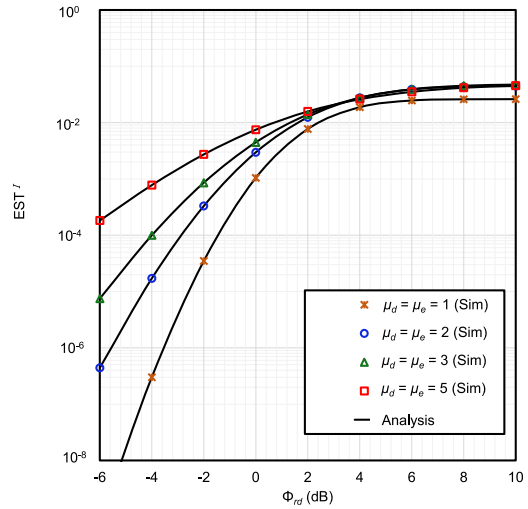

FIGURE 15. The EST^{I} Φ_{rd} for selected values of Φ_{re}, μ_d, and μ_e with $\epsilon = 1$, $\mathcal{N}_{el} = 2$, $\mu_b = 1$, $\Phi_{sr} = 15$ dB, and $\Phi_{br} = 1$ dB.

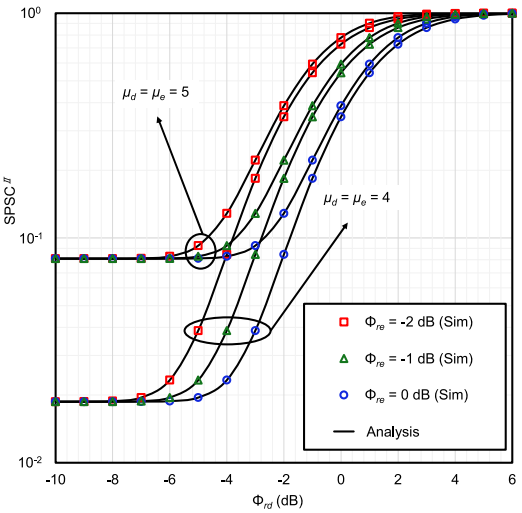

FIGURE 14. The SPSC^{II} Φ_{rd} for selected values of Φ_{re}, μ_d, and μ_e with $G_d = G_e = 2$, $\kappa_d = \kappa_e = 1$, $m_d = m_e = 4$, and $\mathcal{N}_{ell} = 2$.

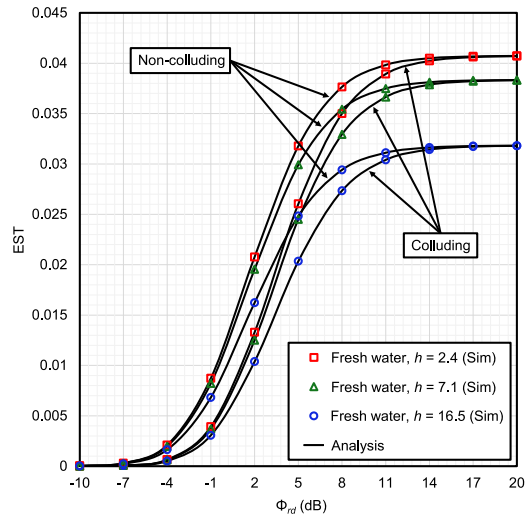

FIGURE 16. The EST versus Φ_{rd} for selected values of h for fresh water with $\epsilon = 2$, $\mathcal{N}_{el} = \mathcal{N}_{ell} = 2$, $\Phi_{sr} = 15$ dB, $\Phi_{br} = 1$ dB, and $\Phi_{re} = 0$ dB.

κ_d and κ_e increases. Therefore, it is observed from figure 13 that the value of EST becomes higher while the value of κ is increased. This indicates that communication between $\mathcal{R}$ to $\mathcal{D}$ can be established more securely due to the increased fading severity. This is expected since the SNR of $\mathcal{R}-\mathcal{D}$ link is dependent on fading parameters as demonstrated in (48). Similar outcomes are also observed while comparing the results in Fig. 14-15 since a good reception is obtained at $\mathcal{D}$ as the levels of μ_d and μ_e increase.

C. COMPARISON OF COLLUDING AND NON-COLLUDING EAVESDROPPERS ATTACK

Fig. 16 demonstrates the EST analysis to compare the secrecy performance of colluding and non-colluding eavesdropping modes under numerous UWT conditions in thermally uniform freshwater. Since the non-colluding eavesdroppers obtain a greater EST value than the colluding mode, it can be inferred that the colluding eavesdropping scenario is more severe than that of the non-colluding scenario. In other words, due to the colluding scenario, eavesdropper's capabilities are improved, which leads to poorer secrecy performance. The reason for this is that while colluding eavesdroppers collaborate and corroborate their opinions to decode sensitive information, non-colluding eavesdroppers explore the confidential message independently. Furthermore, EST is greater in the presence of weaker UWT relative to stronger UWT conditions. The reason is the same as it was in Fig. 3.

The SOP vs Φ_{rd} is illustrated in Fig. 17, which exhibits the impact of energy conversion efficiency (η_r). It can be concluded that an increase in η_r triggers a noticeable improvement in SOP performance. This is predictable since

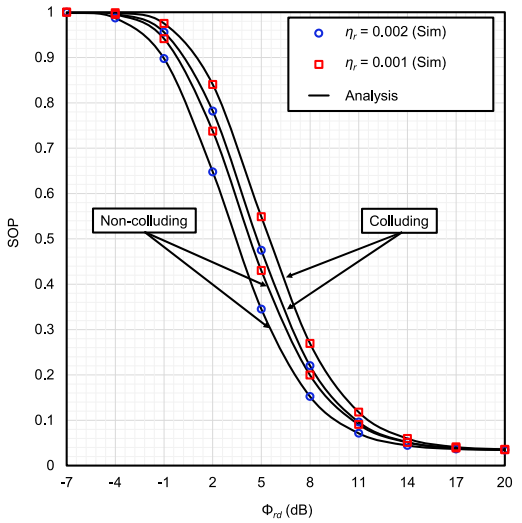

FIGURE 17. The SOP versus Φ_{rd} for selected values of η_r with $\epsilon = 1$, $\mathcal{N}_{el} = \mathcal{N}_{ell} = 2$, $\Phi_{sr} = 15$ dB, $\Phi_{br} = 1$, and $\Phi_{re} = 0$ dB.

more harvested energy can be utilized due to the reliable information transfer in the second time slot. Moreover, it is observed that secrecy performance degrades significantly in the scenario of colluding eavesdroppers relative to the non-colluding eavesdroppers scenario.

VI. CONCLUSION

In this study, the secrecy performance of UOWC-RF mixed networks including an energy harvesting relay against multiple eavesdroppers which operate in colluding (*Scenario-I*) and non-colluding (*Scenario-II*) manners is analyzed. We derive the closed-form expressions of SOP, probability of SPSC and EST, and then validate them via computer simulations. Numerical results reveal that whereas the secrecy performance is drastically influenced by UWT (based on air bubble level, temperature gradient, and water salinity), and pointing errors, the HD technique can guarantee a better secrecy throughput as opposed to the IM/DD technique. Besides, the secrecy performance is always dominated by the worse hop but it can be significantly enhanced by exploiting diversity at the power beacon and/or the destination along with increasing the power of the power beacon to facilitate more harvested energy at the relay. Finally, a comparative analysis between the two scenarios concludes that the attacks led by colluding eavesdroppers are more detrimental than that of non-colluding eavesdroppers, and preventing such collusion between the eavesdroppers must be given top-most priority by the design engineers while designing secure communication system networks.

APPENDIX

A. APPENDIX A

Substituting (12) and (16) into (34), $f_w^I(w)$ is expressed as

$$f_w^I(w) = \int_0^\infty \sum_{e_1=0}^{\infty} \Xi_1 e^{-\Xi_2(w+x)}(w+x)^{\Xi_3} \frac{1}{\theta} \sum_{f_2=0}^{\infty} \widetilde{\Xi}_4 \times e^{-\widetilde{\Xi}_5\left(\frac{x}{\theta}\right)} \left(\frac{x}{\theta}\right)^{\widetilde{\Xi}_6} dx. \tag{55}$$

Applying the binomial theorem to $(w+x)^{\Xi_3}$ term, utilizing the formula [65, eq. (3).351.3] along with some mathematical manipulations and simplifications, (55) is derived as

$$\begin{aligned} f_w^I(w) &= \sum_{e_1=0}^{\infty} \sum_{f_2=0}^{\infty} \sum_{t_1=0}^{\Xi_3} \binom{\Xi_3}{t_1} \frac{\mathcal{X}_1}{\theta^{\widetilde{\Xi}_6+1}} e^{-\Xi_2 w} w^{\Xi_3-t_1} \\ &\quad \times \int_0^\infty e^{-(\Xi_2+\frac{\widetilde{\Xi}_5}{\theta})x} x^{\widetilde{\Xi}_6+t_1} dx \\ &= \sum_{e_1=0}^{\infty} \sum_{f_2=0}^{\infty} \sum_{t_1=0}^{\Xi_3} \binom{\Xi_3}{t_1} \left(\Xi_2 + \frac{\widetilde{\Xi}_5}{\theta}\right)^{-(\widetilde{\Xi}_6+t_1+1)} \\ &\quad \times \frac{(\widetilde{\Xi}_6+t_1)!\mathcal{X}_1}{\theta^{\widetilde{\Xi}_6+1}} e^{-\Xi_2 w} w^{\Xi_3-t_1}, \end{aligned} \tag{56}$$

where $\mathcal{X}_1 = \Xi_1 \widetilde{\Xi}_4$. Now, substituting (22) and (56) into (33), utilizing the formula [65, eq. (3).351.2], and performing some mathematical manipulations and simplifications, $\Pr\{|\mathbf{h}_{br}|^2 w \geq D_0, w > 0\}$ is formulated as

$$\begin{aligned} &\Pr\left\{|\mathbf{h}_{br}|^2 w \geq D_0, w > 0\right\} \\ &= \sum_{e_1=0}^{\infty} \sum_{f_2=0}^{\infty} \sum_{g_1=0}^{\infty} \sum_{t_1=0}^{\Xi_3} \binom{\Xi_3}{t_1} \left(\Xi_2 + \frac{\widetilde{\Xi}_5}{\theta}\right)^{-(\widetilde{\Xi}_6+t_1+1)} \\ &\quad \times \frac{(\widetilde{\Xi}_6+t_1)!\mathcal{X}_2}{\theta^{\widetilde{\Xi}_6+1}} \int_0^\infty e^{-\Xi_2 w} w^{\Xi_3-t_1} dw \int_{\frac{D_0}{w}}^\infty e^{-\Xi_8 \gamma} \gamma^{\Xi_9} d\gamma \\ &= \sum_{e_1=0}^{\infty} \sum_{f_2=0}^{\infty} \sum_{g_1=0}^{\infty} \sum_{t_1=0}^{\Xi_3} \sum_{t_2=0}^{\Xi_9} \binom{\Xi_3}{t_1} \left(\Xi_2 + \frac{\widetilde{\Xi}_5}{\theta}\right)^{-(\widetilde{\Xi}_6+t_1+1)} \\ &\quad \times \frac{(\widetilde{\Xi}_6+t_1)!\mathcal{X}_2}{\theta^{\widetilde{\Xi}_6+1}} \frac{\Xi_9!}{t_2!\Xi_8^{\Xi_9-t_2+1}} \int_0^\infty \left(\frac{D_0}{w}\right)^{t_2} \\ &\quad \times e^{-\Xi_2 w - \frac{\Xi_8 D_0}{w}} w^{\Xi_3-t_1} dw, \end{aligned} \tag{57}$$

where $\mathcal{X}_2 = \mathcal{X}_1 \Xi_7$. Applying [65, eq. (3).471.9] and [72, eq. (07).34.03.0605.01] after performing some mathematical simplifications, (57) is finally implemented as shown in (35).

B. APPENDIX B

Substituting (12) and (21) into (39), $f_w^{II}(w)$ is expressed as

$$\begin{aligned} f_w^{II}(w) &= \int_0^\infty \sum_{e_1=0}^{\infty} \Xi_1 e^{-\Xi_2(w+x)}(w+x)^{\Xi_3} \frac{1}{\theta} \mathcal{N}_{eII} \\ &\quad \times \sum_{f_1=0}^{\infty} \sum_{h_1=0}^{\mathcal{N}_{eII}-1} \sum_{q_0+q_1+\ldots+q_{\Xi_6}=h_1} \prod_{p_4} \binom{\mathcal{N}_{eII}-1}{} \\ &\quad \times h_1 \binom{h_1}{q_0, q_1, \ldots, q_{\Xi_6}} \left(\frac{\Xi_6!}{p_4!\Xi_5^{\Xi_6-p_4+1}}\right)^{q_{p_4}} \left(\sum_{f_1=0}^{\infty} \Xi_4\right)^{h_1} \\ &\quad \times (-1)^{h_1} \Xi_4 e^{-\frac{x}{\theta}(\Xi_5+\Xi_5 h_1)} \left(\frac{x}{\theta}\right)^{\mathcal{X}_3} dx. \end{aligned} \tag{58}$$

Now, according to the similar formulation procedure as utilized for scenario-I with some mathematical simplifications, $f_w^{II}(w)$ is finally derived as follows:

$$f_w^{II}(w) = \mathcal{N}_{eII} \sum_{e_1=0}^{\infty} \sum_{f_1=0}^{\infty} \sum_{h_1=0}^{\mathcal{N}_{eII}-1} \sum_{q_0+q_1+\ldots+q_{\Xi_6}=h_1} \sum_{t_3=0}^{\Xi_3} \prod_{p_4} \times \binom{\mathcal{N}_{eII}-1}{h_1} \binom{\Xi_3}{t_3} \binom{h_1}{q_0, q_1, \ldots, q_{\Xi_6}} \times \left(\frac{\Xi_6!}{p_4! \Xi_5^{\Xi_6-p_4+1}} \right)^{q_{p_4}} \left(\sum_{f_1=0}^{\infty} \Xi_4 \right)^{h_1} (-1)^{h_1} \frac{\mathcal{X}_4!}{\theta^{\mathcal{X}_3+1}} \times \left(\Xi_2 + \frac{\Xi_5 h_1}{\theta} + \frac{\Xi_5}{\theta} \right)^{-(\mathcal{X}_4+1)} \Xi_1 \Xi_4 e^{-\Xi_2 w} w^{\Xi_3-t_1}, \tag{59}$$

where $\mathcal{X}_4 = \mathcal{X}_3 + t_3$.

Substituting (22) and (59) into (38) and implementing the similar approach as utilized for scenario-I along with some algebraic manipulations and simplifications, $\Pr\{|\mathbf{h}_{br}|^2 w \geq D_0, w > 0\}$ is obtained as in (40) and the proof is completed.

C. APPENDIX C

Substituting (12) and (16) into (46), utilizing the identity [65, eq. (3).351.1], and performing some mathematical manipulations and simplifications, $\Pr\{C_{rd} > 0\}$ is formed as

$$\begin{aligned} &\Pr\{C_{rd} > 0\} \\ &= 1 - \left[\sum_{e_1=0}^{\infty} \sum_{f_2=0}^{\infty} \mathcal{X}_1 \left(\int_0^{\infty} e^{-\widetilde{\Xi}_5 v} v^{\widetilde{\Xi}_6} dv \int_0^{v} e^{-\Xi_2 u} u^{\Xi_3} du \right) \right] \\ &= 1 - \left[\sum_{e_1=0}^{\infty} \sum_{f_2=0}^{\infty} \mathcal{X}_1 \left(\int_0^{\infty} \frac{\Xi_3!}{\Xi_2^{\Xi_3+1}} e^{-\widetilde{\Xi}_5 v} v^{\widetilde{\Xi}_6} dv \right. \right. \\ &\quad \left. \left. - \int_0^{\infty} \sum_{t_5=0}^{\Xi_3} \frac{\Xi_3!}{t_5! \Xi_2^{\Xi_3-t_5+1}} e^{-(\Xi_2+\widetilde{\Xi}_5) v} v^{\widetilde{\Xi}_6+t_5} dv \right) \right], \end{aligned} \tag{60}$$

Now, applying the formula [65, eq. (3).351.3], $\Pr\{C_{rd} > 0\}$ is finally derived as shown in (47) and hence the proof is concluded.

REFERENCES

[1] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nat. Electron.*, vol. 3, no. 1, pp. 20–29, 2020.

[2] M. Shahjalal et al., "Enabling technologies for AI empowered 6G massive radio access networks," *ICT Exp.*, vol. 9, no. 3, pp. 341–355, Jun. 2023.

[3] H. Yu, H. Lee, and H. Jeon, "What is 5G? Emerging 5G mobile services and network requirements," *Sustainability*, vol. 9, no. 10, p. 1848, 2017.

[4] M. R. A. Ruku, M. Ibrahim, A. Badrudduza, and I. S. Ansari, "Effects of co-channel interference on RIS empowered wireless networks amid multiple eavesdropping attempts," 2023, *arXiv:2302.10876*.

[5] J. Joung, H. Yu, and J. Zhao, "Bandwidth design for energy-efficient unmanned aerial vehicle using space–time line code," *IEEE Syst. J.*, vol. 15, no. 2, pp. 3154–3157, Jun. 2021.

[6] S. Kim and H. Yu, "Energy-efficient HARQ-IR for massive MIMO systems," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 3892–3901, Sep. 2018.

[7] S. Lee, H. Yu, and H. Lee, "Multiagent Q-learning-based multi-UAV wireless networks for maximizing energy efficiency: Deployment and power control strategy design," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6434–6442, May 2022.

[8] C.-B. Le et al., "Joint design of improved spectrum and energy efficiency with backscatter NOMA for IoT," *IEEE Access*, vol. 10, pp. 7504–7519, 2022.

[9] S. Ulukus et al., "Energy harvesting wireless communications: A review of recent advances," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 3, pp. 360–381, Mar. 2015.

[10] D. Altinel and G. Karabulut Kurt, "Energy harvesting from multiple RF sources in wireless fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 8854–8864, Nov. 2016.

[11] Y. He, X. Cheng, W. Peng, and G. L. Stuber, "A survey of energy harvesting communications: Models and offline optimal policies," *IEEE Wireless Commun. Mag.*, vol. 53, no. 6, pp. 79–85, Jun. 2015.

[12] W. Ni and X. Dong, "Energy harvesting wireless communications with energy cooperation between transmitter and receiver," *IEEE Trans. Commun.*, vol. 63, no. 4, pp. 1457–1469, Apr. 2015.

[13] H. Li, J. Xu, R. Zhang, and S. Cui, "A general utility optimization framework for energy-harvesting-based wireless communications," *IEEE Wireless Commun. Mag.*, vol. 53, no. 4, pp. 79–85, Apr. 2015.

[14] P. N. Alevizos and A. Bletsas, "Sensitive and nonlinear far-field RF energy harvesting in wireless communications," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3670–3685, Jun. 2018.

[15] M. Y. Naderi, K. R. Chowdhury, and S. Basagni, "Wireless sensor networks with RF energy harvesting: Energy models and analysis," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2015, pp. 1494–1499.

[16] B. Clerckx and J. Kim, "On the beneficial roles of fading and transmit diversity in wireless power transfer with nonlinear energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7731–7743, Nov. 2018.

[17] J. Zhang, H. Ran, X. Pan, G. Pan, and Y. Xie, "Outage analysis of wireless-powered relaying FSO-RF systems with nonlinear energy harvesting," *Opt. Commun.*, vol. 477, Dec. 2020, Art. no. 126309. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0030401820307264

[18] K. O. Odeyemi and P. A. Owolawi, "Wireless energy harvesting based asymmetric RF/FSO system with transmit antenna selection and receive diversity over M-distribution channel and non-zero boresight pointing error," *Opt. Commun.*, vol. 461, Apr. 2020, Art. no. 125219. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0030401819311812

[19] P. N. Ramavath, S. A. Udupi, and P. Krishnan, "Co-operative RF-UWOC link performance over hyperbolic tangent log-normal distribution channel with pointing errors," *Opt. Commun.*, vol. 469, Aug. 2020, Art. no. 125774. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0030401820302832

[20] S. Anees and R. Deka, "On the performance of DF based dual-hop mixed RF-UWOC system," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC)*, 2019, pp. 1–5.

[21] S. Li, L. Yang, D. B. da Costa, J. Zhang, and M.-S. Alouini, "Performance analysis of mixed RF-UWOC dual-hop transmission systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 14043–14048, Nov. 2020.

[22] I. S. Ansari, L. Jan, Y. Tang, L. Yang, and M. H. Zafar, "Outage and error analysis of dual-hop TAS/MRC MIMO RF-UOWC systems," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 10093–10104, Oct. 2021.

[23] H. Lei, Y. Zhang, K.-H. Park, I. S. Ansari, G. Pan, and M.-S. Alouini, "On the performance of dual-hop RF-UWOC system," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2020, pp. 1–6.

[24] S. Yadav, A. Vats, M. Aggarwal, and S. Ahuja, "Performance analysis and altitude optimization of UAV-enabled dual-hop mixed RF-UWOC system," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12651–12661, Dec. 2021.

[25] S. Li, L. Yang, D. B. d. Costa, M. D. Renzo, and M.-S. Alouini, "On the performance of RIS-assisted dual-hop mixed RF-UWOC systems," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, no. 2, pp. 340–353, Jun. 2021.

[26] M. Ibrahim, M. Z. I. Sarkar, A. S. M. Badrudduza, M. K. Kundu, and S. Dev, "Impact of correlation on the security in multicasting through $\kappa - \mu$ shadowed fading channels," in *Proc. IEEE Reg. 10 Symp. (TENSYMP)*, 2020, pp. 1396–1399.

[27] W. Khalid, H. Yu, R. Ali, and R. Ullah, "Advanced physical-layer technologies for beyond 5G wireless communication networks," *Sensors*, vol. 21, no. 9, p. 3197, 2021.

[28] M. A. Rakib et al., "A RIS empowered THz-UWO relay system for air-to-underwater mixed network: Performance analysis with pointing errors," *IEEE Internet Things J.*, early access, Jan. 23, 2024, doi: 10.1109/JIOT.2024.3357596.

[29] H. Yu and I.-G. Lee, "Physical layer security based on NOMA and AJ for MISOSE channels with an untrusted relay," *Future Gener. Comput. Syst.*, vol. 102, pp. 611–618, Jan. 2020.

[30] M. M. Rahman, A. S. M. Badrudduza, N. A. Sarker, M. Ibrahim, I. S. Ansari, and H. Yu, "RIS-aided mixed RF-FSO wireless networks: Secrecy performance analysis with simultaneous eavesdropping," *IEEE Access*, vol. 11, pp. 126507–126523, 2023.

[31] H. Yu and T. Kim, "Training and data structures for AN-aided secure communication," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2869–2872, Sep. 2019.

[32] H. Yu and J. Joung, "Design of the power and dimension of artificial noise for secure communication systems," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 4001–4010, Jun. 2021.

[33] H. Yu and J. Joung, "Secure IoT communications using HARQ-based beamforming for MISOSE channels," *IEEE Internet Things J.*, vol. 8, no. 23, pp. 17211–17226, Dec. 2021.

[34] W. Khalid, H. Yu, D.-T. Do, Z. Kaleem, and S. Noh, "RIS-aided physical layer security with full-duplex jamming in underlay D2D networks," *IEEE Access*, vol. 9, pp. 99667–99679, 2021.

[35] T. Ahmed et al., "Enhancing physical layer secrecy performance for RIS-assisted RF-FSO mixed wireless system," *IEEE Access*, vol. 11, pp. 127737–127753, 2023.

[36] H. Yu, T. Kim, and H. Jafarkhani, "Wireless secure communication with beamforming and jamming in time-varying wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 2087–2100, 2018.

[37] S. H. Islam et al., "On secrecy performance of mixed generalized Gamma and Málaga RF-FSO variable gain relaying channel," *IEEE Access*, vol. 8, pp. 104127–104138, 2020.

[38] Y. Ai, A. Mathur, H. Lei, M. Cheffena, and I. S. Ansari, "Secrecy enhancement of RF backhaul system with parallel FSO communication link," *Opt. Commun.*, vol. 475, Nov. 2020, Art. no. 126193. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0030401820306106

[39] M. J. Saber, J. Mazloum, A. M. Sazdar, A. Keshavarz, and M. J. Piran, "On secure mixed RF-FSO decode-and-forward relaying systems with energy harvesting," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4402–4405, Sep. 2020.

[40] N. A. Sarker et al., "On the intercept probability and secure outage analysis of mixed (α–κ–μ)-shadowed and Málaga turbulent models," *IEEE Access*, vol. 9, pp. 133849–133860, 2021.

[41] N. H. Juel et al., "Secrecy performance analysis of mixed α-μ and exponentiated Weibull RF-FSO cooperative relaying system," *IEEE Access*, vol. 9, pp. 72342–72356, 2021.

[42] J. Zhang, G. Pan, and Y. Xie, "Secrecy analysis of wireless-powered multi-antenna relaying system with nonlinear energy harvesters and imperfect CSI," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 2, pp. 460–470, Jun. 2018.

[43] J. Zhang, W. He, G. Pan, and Y. Xie, "On secrecy analysis of wireless-powered relaying FSO-RF systems," *Opt. Eng.*, vol. 60, no. 6, pp. 1–13, 2021. [Online]. Available: https://doi.org/10.1117/1.OE.60.6.066102

[44] E. Illi et al., "On the physical layer security of a regenerative relay-based mixed RF/UOWC," in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, 2019, pp. 1–7.

[45] A. S. M. Badrudduza et al., "Security at the physical layer over GG fading and mEGG turbulence induced RF-UOWC mixed system," *IEEE Access*, vol. 9, pp. 18123–18136, 2021.

[46] M. Ibrahim, A. S. M. Badrudduza, M. S. Hossen, M. K. Kundu, and I. S. Ansari, "Enhancing security of TAS/MRC-based mixed RF-UOWC system with induced underwater turbulence effect," *IEEE Syst. J.*, vol. 16, no. 4, pp. 5584–5595, Dec. 2022.

[47] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 3, pp. 1281–1293, Jul. 2016.

[48] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: The case of colluding eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory*, 2009, pp. 2442–2446.

[49] S. Cho, G. Chen, and J. P. Coon, "Physical layer security in visible light communication systems with randomly located colluding eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 768–771, Oct. 2018.

[50] T. M. Hoang, L. T. Dung, B. C. Nguyen, X. N. Tran, and T. Kim, "Secrecy outage performance of FD-NOMA relay system with multiple non-colluding eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12985–12997, Dec. 2021.

[51] X. Xuan Tang, W. Yang, Y. Cai, W. Yang, and Y. Huang, "Security of full-duplex jamming SWIPT system with multiple non-colluding eavesdroppers," in *Proc. 7th IEEE Int. Conf. Electron. Inf. Emerg. Commun. (ICEIEC)*, 2017, pp. 66–69.

[52] M. Ragheb and S. M. S. Hemami, "Secure communication for millimeter-wave systems with randomly located non-colluding eavesdroppers," in *Proc. 28th Iran. Conf. Electr. Eng. (ICEE)*, 2020, pp. 1–6.

[53] D. Tashman and W. Hamouda, "Cascaded $\kappa - \mu$ fading channels with colluding and non-colluding eavesdroppers: Physical-layer security analysis," *Future Internet*, vol. 13, no. 8, p. 205, 2021. [Online]. Available: https://www.mdpi.com/1999-5903/13/8/205

[54] K. O. Odeyemi and P. A. Owolawi, "Physical layer security in mixed RF/FSO system under multiple eavesdroppers collusion and non-collusion," *Opt. Quantum Electron.*, vol. 50, no. 7, pp. 1–19, Jul. 2018.

[55] 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.

[56] T. Hossain, S. Shabab, A. S. M. Badrudduza, M. K. Kundu, and I. S. Ansari, "On the physical layer security performance over RIS-aided dual-hop RF-UOWC mixed network," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2246–2257, Feb. 2023.

[57] E. Illi, F. El Bouanani, and F. Ayoub, "Physical layer security of an amplify-and-forward energy harvesting-based mixed RF/UOW system," in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, 2019, pp. 1–8.

[58] J. F. Paris, "Statistical characterization of $\kappa - \mu$ shadowed fading," *IEEE Trans. Veh. Technol.*, vol. 63, no. 2, pp. 518–526, Feb. 2014.

[59] W. M. R. Shakir, "Physical layer security performance analysis of hybrid FSO/RF communication system," *IEEE Access*, vol. 9, pp. 18948–18961, 2021.

[60] J. Xia et al., "Secure cache-aided multi-relay networks in the presence of multiple eavesdroppers," *IEEE Trans. Commun.*, vol. 67, no. 11, pp. 7672–7685, Nov. 2019.

[61] J. Chen et al., "A novel energy harvesting scheme for mixed FSO-RF relaying systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8259–8263, Aug. 2019.

[62] Y. Gu and S. Aïssa, "RF-based energy harvesting in decode-and-forward relaying systems: Ergodic and outage capacities," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6425–6434, Nov. 2015.

[63] S. M. S. Shahriyer, A. S. M. Badrudduza, S. Shabab, M. K. Kundu, and H. Yu, "Opportunistic relay in multicast channels with generalized shadowed fading effects: A physical layer security perspective," *IEEE Access*, vol. 9, pp. 155726–155739, 2021.

[64] S. Al-Juboori and X. N. Fernando, "Multiantenna spectrum sensing over correlated Nakagami-*m* channels with MRC and EGC diversity receptions," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2155–2164, Mar. 2018.

[65] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Cambridge, MA, USA: Academic, 2007.

[66] J. D. V. Sánchez, D. P. M. Osorio, F. J. López-Martínez, M. C. P. Paredes, and L. F. Urquiza-Aguiar, "Information-theoretic security of MIMO networks under κ-μ shadowed fading channels," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 6302–6318, Jul. 2021.

[67] A. Badrudduza, M. Sarkar, and M. Kundu, "Enhancing security in multicasting through correlated Nakagami-*m* fading channels with opportunistic relaying," *Phys. Commun.*, vol. 43, Dec. 2020, Art. no. 101177.

[68] X. Pan, H. Ran, G. Pan, Y. Xie, and J. Zhang, "On secrecy analysis of DF based dual hop mixed RF-FSO systems," *IEEE Access*, vol. 7, pp. 66725–66730, 2019.
[69] A. A. Kilbas, *H-Transforms: Theory and Applications*. Boca Raton, FL, USA: CRC Press, 2004.
[70] M. Ibrahim, A. S. M. Badrudduza, M. S. Hossen, M. K. Kundu, I. S. Ansari, and I. Ahmed, "On effective secrecy throughput of underlay spectrum sharing α-μ/ málaga hybrid model under interference-and-transmit power constraints," *IEEE Photon. J.*, vol. 15, no. 2, pp. 1–13, Apr. 2023.
[71] M. Tania, M. Ibrahim, M. Hossen, A. Badrudduza, and M. Kundu, "Combined impacts of co-channel interference and correlation on secrecy performance over κ-μ shadowed fading channel," in *Proc. Int. Conf. Adv. Electr. Electron. Eng. (ICAEEE)*, 2022, pp. 1–6.
[72] "MeijerG." wolfram. Accessed: Jul. 31, 2023. [Online]. Available: https://functions.wolfram.com/HypergeometricFunctions/MeijerG/

MOLOY KUMAR GHOSH received the B.Sc. degree in electrical and computer engineering (ECE) from the Rajshahi University of Engineering and Technology, Rajshahi, Bangladesh, in 2022, where he is currently working as a Lecturer with the Department of ECE. He led an IoT-based disaster management project which got the most popular project award at IEEE YESIST12 Maker Fair Track, Thailand, in 2019. His research interests include free-space optics communication, physical-layer security, underwater communication, and energy harvesting.

MILTON KUMAR KUNDU (Member, IEEE) received the B.Sc. degree in electrical and electronic engineering (EEE) from the Rajshahi University of Engineering and Technology (RUET), Rajshahi, Bangladesh, in 2016.

He has worked as the Lecturer with the Department of EEE, North Bengal International University, Rajshahi, from 20 May 2017 to 14 February 2019. He has been working as a Lecturer with the Department of Electrical and Computer Engineering, RUET since 16 February 2019. He is also the Advisor of the IEEE RUET Industry Applications Society Student Branch Chapter. His research interests are centered around the security aspects of cooperative and physical-layer networks and wireless multicasting.

Mr. Kundu has won several awards, including the 2nd Runner-Up Award in Regional Mathematical Olympiad and EEE Association Award (Student of the Year Award) from RUET for his outstanding academic performances in the 3rd year examinations while pursuing B.Sc. engineering degree. He has also won two Best Paper Awards for two different research papers from IEEE Region 10 Symposium (TENSYMP 2020) and IEEE 3rd International Conference on Telecommunication and Photonics (ICTP 2019).

MD. IBRAHIM (Graduate Student Member, IEEE) received the B.Sc. degree in electrical and electronic engineering (EEE) from the Rajshahi University of Engineering and Technology (RUET), Rajshahi, Bangladesh, in 2021. From 1 September 2021 to 10 December 2021, he was a Lecturer with the Department of EEE, Varendra University, Rajshahi. He has been working as a Lecturer with the Institute of Information and Communication Technology, RUET since 12 December 2021. His current research interests include free-space optics communication, physical-layer security, underwater communications, cognitive radio network, and NOMA systems. He has been affiliated with IEEE since 2022 and is an active reviewer for several IEEE journals.

A. S. M. BADRUDDUZA (Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical and electronic engineering (EEE) from the Rajshahi University of Engineering and Technology (RUET), Rajshahi, Bangladesh, in 2016 and 2019, respectively.

From 16 September 2016 to 22 July 2017, he was a Lecturer with the Department of EEE, Bangladesh Army University of Engineering and Technology, Qadirabad Cantonment, Natore, Bangladesh. From 23 July 2017 to 29 June 2020, he was a Lecturer with the Department of Electronics and Telecommunication Engineering (ETE), RUET. He has been working as an Assistant Professor with the Department of ETE, RUET since 30 June 2020. He has authored/coauthored 50+ international journals/conference publications. His research interests include physical-layer security, optical wireless communication, NOMA systems, reflecting intelligent surfaces, UAVs, and machine learning.

Mr. Badrudduza was a recipient of two EEE Association Awards (Student of the Year Award) from RUET for his outstanding academic performances in the 1st and 4th-year examinations while pursuing his B.Sc. engineering degree and three Best Paper Awards for three different research papers from ICTP 2019, TENSYMP 2020, and ECCE 2023. He has been affiliated with IEEE since 2020 and is an active reviewer for several IEEE, Elsevier, Springer, OSA, IET, and SPIE journals.

MD. SHAMIM ANOWER received the B.Sc. and M.Sc. degrees in electrical and electronic engineering (EEE) from the Rajshahi University of Engineering and Technology (RUET), Rajshahi, Bangladesh, in 2002 and 2007, respectively, and the Ph.D. degree in electrical engineering from the University of New South Wales, Australia, in 2012.

From 22 April 2003 to 24 September 2006, he was a Lecturer with the Department of EEE, RUET. From 25 September 2006 to 4 June 2015, he was an Assistant Professor with the Department of EEE, RUET. From 5 January 2015 to 18 June 2016, he was an Associate Professor with the EEE Department, RUET. Since 19 January 2016, he has been working as a Professor with the Department of EEE, RUET. Basically, his field of specialization is Underwater Acoustic Signal processing: Theory and Applications. Besides, his field of researches are photonics, power system stability, biomedical engineering, cyber security, and wireless communication. He has over 100 refereed publications, including journal (16 Q1 ranked in Scimago) and conference papers with H-index 18, i10-index 29, and 954 citations. These cover the target sectors: "Energy and Mining Technology," "Quantum Information, Advanced Digital, Data Science and ICT," and "Cyber Security." Scopus Ranking: 1st in RUET and 6th in Bangladesh (2015–2019 and 2015–2020). He has got BOG Gold Medal for being 1st in B.Sc. Engineering.

IMRAN SHAFIQUE ANSARI (Senior Member, IEEE) received the B.Sc. degree (with First-Class Hons.) in computer engineering from the King Fahd University of Petroleum and Minerals in 2009, and the M.Sc. and Ph.D. degrees from the King Abdullah University of Science and Technology (KAUST) in 2010 and 2015, respectively.

Since August 2018, he has been a Lecturer (Assistant Professor) with the University of Glasgow, Glasgow, U.K. Prior to this, from November 2017 to July 2018, he was a Lecturer (Assistant Professor) with the Global College of Engineering and Technology (affiliated with the University of the West of England, Bristol, U.K.). From April 2015 to November 2017, he was a Postdoctoral Research Associate with Texas A&M University at Qatar (TAMUQ). From May 2009 to August 2009, he was a Visiting Scholar with Michigan State University, East Lansing, MI, USA, and from June 2010 to August 2010, he was a Research Intern with Carleton University, Ottawa, ON, Canada. He has authored/coauthored 100+ journal and conference publications. He has co-organized the GRASNET'2016, 2017, and 2018 workshops in conjunction with IEEE WCNC'2016 and 2017 and IEEE Globecom 2018. His current research interests include free-space optics, underwater communications, physical-layer secrecy issues, full-duplex systems, and secure D2D applications for 5G+ systems.

Dr. Ansari is a recipient of appreciation for an Exemplary Reviewer for IEEE TRANSACTION ON COMMUNICATIONS in 2018 and 2016, a recipient of appreciation for an Exemplary Reviewer for IEEE WIRELESS COMMUNICATIONS LETTERS in 2017 and 2014, a recipient of TAMUQ ECEN Research Excellence Award in 2016 and 2017, a recipient of recognized reviewer certificate by Elsevier *Optics Communications* in 2015, a recipient of recognized reviewer certificate by OSA Publishing in 2014, a recipient of the Postdoctoral Research Award (first cycle) with Qatar National Research Foundation in 2014, a recipient of the KAUST Academic Excellence Award in 2014, and a recipient of the IEEE Richard E. Merwin Student Scholarship Award in July 2013. He has been affiliated with IEEE and IET since 2007 and has served in various capacities. He has been serving on the IEEE Nominations and Appointments Committee since 2020–2021 and IEEE Communication Society Young Professionals Board since April 2016. He is part of the IEEE 5G Tech Focus Publications Editorial Board since February 2017. He is serving as the Past-Chair of the IET Young Professionals Communities Committee from October 2020 to September 2021. He has served on the IET Satellites Technical Network from March 2016 to September 2020. He has served on the IET CC-EMEA (Communities Committee-Europe, Middle-East and Africa) for two complete terms from October 2015 to September 2018 and October 2010 to September 2013. He is an active reviewer for various IEEE TRANSACTIONS and various other journals. He has served as a TPC for various IEEE conferences.

ANNIE SOLOMON is currently pursuing the undergraduate degree in mechanical engineering with Kennesaw State University (KSU), with a strong interest in the fields of robotics, automobile manufacturing, radar systems, and microcontroller systems. In her previous professional experiences, she has served as an Engineering Intern with the Georgia Institute of Technology. She approaches her academic and career pursuits with unwavering dedication and passion, supported by a diverse range of technical competencies. Her technical proficiencies encompass, among others, an extensive background in Arduino microcontroller systems and SOLIDWORKS. Furthermore, she possesses a solid foundation in physics and calculus, enhancing her engineering knowledge and problem-solving skills. Today, she is accruing practical experience through an internship within KSU.

SUMIT CHAKRAVARTY (Member, IEEE) received the bachelor's, master's, and Ph.D. degrees in electrical and computer engineering. He has an extensive background in electrical and computer engineering. He served as a Postdoctoral Researcher with the University of Pennsylvania. He has used his expertise in signal processing machine learning and communications in his role as a principal scientist in industry as well as a faculty member in academia. He is currently an Associate Professor of ECE with Kennesaw State University. He has published multiple journals and peer-reviewed conference papers in venues like *Pattern Recognition*, IEEE SENSORS JOURNAL, and *Journal of Medical Imaging*. His academic experiences include working for NASA-Goddard, the University of Maryland, and the New York Institute of Technology. His industry experience in engineering and research include working in various roles, such as an Instrumentation Engineer and a Research Intern with Siemens CAD and Apex Eclipse Communications, and a Principal Scientist with SGT Inc., Honeywell Research (Automatic Control Solutions-Advanced Technology Labs). He has served as a Guest Editor for *Electronics* journal Special Issue on "Signal Processing in Wireless Communications" and Special Issue on "Towards Reliable and Scalable Smart Cities: Internet of Things Meets Big Data and AI."

IMTIAZ AHMED (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of British Columbia, Vancouver, BC, Canada. He is currently working as an Assistant Professor with the Department of Electrical Engineering and Computer Science, Howard University, Washington, DC, USA. He works in the areas of wireless communications, signal processing, and computer networks. After finishing his Ph.D. degree, he worked with Intel Corporation, San Diego, CA, USA, as a Wireless Systems Engineer and Marshall University, Huntington, WV, USA, as an Assistant Professor. His research interests include communications with intelligent reflecting surface, THz-band communications, cell-free communication systems, aerial–terrestrial integrated network, and design of hybrid RF/FSO communication systems.

HEEJUNG YU (Senior Member, IEEE) received the B.S. degree in radio science and engineering from Korea University, Seoul, South Korea, in 1999, and the M.S. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology, Daejeon, South Korea, in 2001 and 2011, respectively. From 2001 to 2012, he was with the Electronics and Telecommunications Research Institute, Daejeon. From 2012 to 2019, he was with Yeungman University, South Korea. He is currently a Professor with the Department of Electronics and Information Engineering, Korea University, Sejong, South Korea. His areas of interest include statistical signal processing and communication theory.