IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 4, 2021, accepted November 12, 2021, date of publication November 16, 2021,
date of current version November 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3128572

Opportunistic Relay in Multicast Channels With Generalized Shadowed Fading Effects: A Physical Layer Security Perspective

S. M. SAUMIK SHAHRIYER[1], A. S. M. BADRUDDUZA[1], (Member, IEEE), SARJANA SHABAB[2], (Member, IEEE), MILTON KUMAR KUNDU[3], (Member, IEEE), AND HEEJUNG YU[4], (Senior Member, IEEE)

[1]Department of Electronics and Telecommunication Engineering, Rajshahi University of Engineering and Technology (RUET), Rajshahi 6204, Bangladesh
[2]Department of Electrical and Electronic Engineering, RUET, Rajshahi 6204, Bangladesh
[3]Department of Electrical and Computer Engineering, RUET, Rajshahi 6204, Bangladesh
[4]Department of Electronics and Information Engineering, Korea University, Sejong 30019, South Korea

Corresponding author: Heejung Yu (heejungyu@korea.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korean Government (Ministry of Science and ICT) under Grant 2019R1A2C1083988; in part by the Basic Science Research Program through the NRF funded by the Ministry of Education under Grant 2021R1I1A3041887; and in part by the MSIT, South Korea, through the Information Technology Research Center (ITRC) Support Program supervised by the Institute for Information & Communications Technology Promotion (IITP) under Grant IITP-2021-2016-0-00313.

ABSTRACT Through ordinary transmissions over wireless multicast networks are greatly hampered due to the simultaneous presence of fading and shadowing of wireless channels, secure transmissions can be enhanced by properly exploiting random attributes of the propagation medium. This study focuses on the utilization of those attributes to enhance the physical layer security (PLS) performance of a dual-hop wireless multicast network over $\kappa - \mu$ shadow-fading channel under the wiretapping attempts of multiple eavesdroppers. In order to improve the secrecy level, the best relay selection strategy among multiple relays is employed. Performance analysis is carried out based on the mathematical modeling in terms of analytical expressions of non-zero secrecy capacity probability, secure outage probability, and ergodic secrecy capacity over multicast relay networks. Capitalizing on those expressions, the effects of system parameters, i.e., fading, shadowing, the number of antennas, destination receivers, eavesdroppers, and relays, on the secrecy performance are investigated. Numerical results show that the detrimental impacts caused by fading and shadowing can be remarkably mitigated using the well-known opportunistic relaying technique. Moreover, the proposed model unifies secrecy analysis of several classical models, thereby exhibiting enormous versatility than the existing works. Finally, all the numerical results are authenticated utilizing Monte-Carlo simulations.

INDEX TERMS $\kappa - \mu$ shadowed fading, opportunistic relaying, physical layer security, secure outage probability, wireless multicasting.

I. INTRODUCTION

A. BACKGROUND AND RELATED WORKS

Data-carrying radio waves, which propagate through communication channels, experience several constraints, such as diffraction, scattering of waves on the object surface, shadowing, fading, limited bandwidth, and vulnerable nature of the wireless medium, etc. Especially, random shadowing caused by obstacles in the local scenarios or human body exhibits some variations in the interaction pattern of radio wave propagation. Therefore, the aim to build a fortified network not only involves the enhancement of communicating link performance but also the use of optimized protocols in transmitter and receiver circuitry to prevent shadowing and swift variations in multipath propagation conditions.

To understand the effect of dominant and scattered components of the dual shadowing process, the authors in [1] derived expressions of probability density function (PDF), cumulative distribution function (CDF), and Moment Generating Function (MGF) of Rician-fading envelopes. In [2], the

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

authors analyzed outage performance over compound $\eta - \mu$ fading-log-normal shadowing radio channels and derived a formula for the PDF of $\eta - \mu$ fading distribution. With a view to unifying all classic fading models, the authors of [3] investigated the ergodic capacity (EC) and flexibility of channels. Similarly, a trade-off between mathematical complexity and flexibility was represented in [4] by varying different fading parameters under Rayleigh fading distribution. An optimal rate adaptation (ORA) scheme under composite $\kappa - \mu$ / Inverse Gamma (I-Gamma) and $\eta - \mu$ / I-Gamma [5] fading models was investigated in [6], where the analysis incorporated expressions of channel capacity (CP) with a view to developing highly attractive wireless communication systems. The authors in [7] studied average symbol error probability (SEP), the CP under ORA, channel inversion with fixed-rate (CIFR), and truncated CIFR under I-Gamma shadowed fading channels. A qualified analysis among Log-Normal, Inverse Gaussian [8], Gamma, and I-Gamma distribution was also depicted. Apart from these fading channels, the $\kappa - \mu$ shadowed fading channel gained much popularity because of its broad spectrum of flexibility and general characterization. The researchers in [9] proposed a $\kappa - \mu$ shadowed fading model to improve network quality, capacity, and spectral efficiency taking human body shadowing under consideration. Maximum ratio combining (MRC) and square-law combining schemes over $\kappa - \mu$ shadowed fading channel was performed in [10] to observe energy detection in wireless communication scenarios. The $\kappa - \mu$ shadowed model was also employed in [11] to investigate the bit error rate (BER) considering user mobility instead of static user position. The outage probability (OP), average bit error probability and the effective capacity was analyzed in [12] considering double shadowed $\kappa - \mu$ fading model. With the interest of investigating the effective rate of the multiple-input multiple-output (MIMO) systems, the authors in [13], [14] performed higher-order statistics analysis and proved that the properties of the considered fading distribution could be approximated by Gamma distribution. Multiplicative shadowing was investigated in many works such as [15], [16], where the authors showed the superiority of $\kappa - \mu$ / Gamma composite fading model over $\kappa - \mu$ / log-normal line-of-sight (LOS) shadowed fading model in an indoor off-body communication system.

Presently, the need for security enhancement between communicating devices in wireless medium has become a major concern [17]. To compensate for the consequences due to several hindrances such as shadowing, fading, wiretapping, various studies have been introduced to build reliable wireless networks to make it impossible for any eavesdropper to decode any information from the communicating network. Wyner's classic wiretap structure is known as the leading model which recapitulates the importance of security enhancement over different fading channels. Among them, shadow-fading distribution is more admissible for being amenable than any other modern fading model and vast span of propagation conditions. In an extension of this fact, outage performance over log-normal shadowed Rayleigh fading channel was analyzed [18], [19], where the authors prosecuted the Gaussian-Hermite integration approach to show that outage performance significantly enhances standard deviations of shadowing. Authors in [20] analyzed the impact of shadowing on numbers of antennas and propagation conditions over secrecy performance deriving several secrecy measures. Free space optical (FSO) links undergoing shadowed Rician and $\alpha - \mu$ fading in [21] were analyzed to achieve a perfect secrecy level despite severe channel constraints. To get the more generalized picture, security over $\kappa - \mu$ shadowed fading model at a physical layer was examined in [22]–[24], where the authors demonstrated that MIMO system diversity manifests superior performance over MRC and selecting diversity in case of security. The authors in [25] considered $\kappa - \mu$ shadow-fading channels to observe the effect of correlation and drew a conclusion on the fact that a correlation coefficient works as a propitious parameter in case of improving secrecy performance at a lower signal-to-noise ratio (SNR).

Cooperative relaying is another proficient technology to enhance security in wireless systems [26]. The impact of shadowing is inevitably minimized using the dual-hop network which in turn helps to improve wireless links. The authors in [27] analyzed the OP over a non-identical log normal fading channel employing the "best relay" selection scheme. A multi-branch-multi-hop cooperative relaying system in the presence of co-channel interferers was considered in [28], [29] over shadowed Nakagami-m channel, where the authors evinced that a fading parameter affects the system performance greater than the shadowing parameter. A multiple cooperative relay-based satellite-terrestrial system over non-identical shadowed Rician and Nakagami-m fading channels was studied in [30], [31], whether the authors came to a conclusion that EC of the system decreases with the number of relay nodes between satellite and ground users. The best relay selection scheme was employed in the performance analysis of $\kappa - \mu$ shadowed fading channel with multiple relays in [32]. The authors examined the expressions of outage probability (OP), EC, and average BER to manifest the superiority of multiple relay systems over all other transmission techniques. The performance of a $\kappa - \mu$ shadowed fading model with beamforming and amplify-and-forward (AF) relaying technique was demonstrated in [33], [34]. The author validated the fact that the increment in the number of antennas at the transmitting earth station (ES) provides better performance than the increment in the number of antennas at the receiving ES.

Recently, multicast channels have earned much popularity in wireless communication due to its versatile nature to transmit data to multiple destinations accommodating fewer network supplies [35]. Due to such wide spread of wireless multicast networks, lots of researches have been are undertaken to enhance the secrecy performance. Physical layer security (PLS) in a multicasting scenario was analyzed in [36] over quasi-static Rayleigh fading channel where the authors derived the expressions of the probability of non-zero secrecy multicast capacity (PNSMC) and secure outage probability for multicasting (SOPM). A virtual MIMO antenna array scheme was employed in a multiple relay system in [37], where the authors provided a completed description on cooperative spatial multiplexing and derived analytical expressions of SOPM and ergodic secrecy multicast capacity (ESMC). The authors proved that the secrecy performance of a cooperative network completely outweighs that of a direct network.

B. MOTIVATION AND CONTRIBUTIONS

According to the aforementioned works, most of the researches was performed to investigate the system improvement applying numerous technologies over various fading channels, i.e., both generalized and multipath fading. However, there are few works that considered wireless multicasting scenarios and the impact of shadowing on the secure wireless multicast schemes with opportunistic relaying and multiple eavesdroppers over multipath/generalized shadowed fading channels has not been investigated yet. Motivated from this perspective, this paper investigates the mathematical modeling of a secure wireless multicasting scheme over $\kappa - \mu$ shadow-fading channels with an opportunistic relaying technique. Here, a single sender communicates with a set of multiple destination receivers via a set of multiple cooperative relays in the existence of multiple eavesdroppers. $\kappa - \mu$ shadow model assumes random fluctuations of ling of sight (LOS) component and also matches well with experimental data of land mobile satellite (LMS) communication channel. Moreover, a $\kappa - \mu$ fading channel is a generalized fading model, and hence a number of classical fading models, e.g., one-sided Gaussian, Nakagami-m, Rayleigh, Rician-K, and shadowed Rician, can be obtained as particular cases of the proposed model. The prime contributions of the authors are as follows:

- We derive the PDF and CDF of SNRs for multicast and eavesdropper channels by first realizing the PDF of SNRs of each individual hop and then obtaining the PDF of dual-hop SNR with the best relay selection algorithm. To the best of the authors' knowledge, the derived PDF and CDF are absolutely novel and have not been reported yet in any existing literature.
- We analyze the secrecy performance utilizing novel expressions of some well-known secrecy metrics i.e. PNSMC, SOPM, and ESMC, and quantify the effects of each system parameter, i.e., fading parameters, shadowing, number of receive antennas, relays, destination receivers, and eavesdroppers, etc. In comparison to the previous literature, only the proposed work demonstrates how the detrimental impact of shadowing on secure multicasting can be mitigated by employing an opportunistic relaying strategy.
- Finally, we verify all the numerical results corresponding to the derived analytical expressions of secrecy metrics via Monte-Carlo simulations.

C. ORGANIZATION

The organization of this paper is summarized as follows: Section II discusses the proposed system model and problem formulation. The derivations of the expressions of secrecy metrics i.e. PNSMC, SOPM, and ESMC are demonstrated in Section III. Section IV provides the numerical results analysis. Finally, the conclusion of this work is illustrated in section V.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A secure wireless multicast network is shown in Fig.1, where a source, S with a single antenna sends secret information to a set of Q destination receivers via P relays. A set of W eavesdroppers are also present in that network which is intended to decipher the secret messages. Each relay has a single antenna while each destination receiver and each eavesdropper are equipped with G_Q and G_W antennas, respectively. In this particular communication scenario, we assume that the distances of Q and W from S are too large and due to masking effect and severe shadowing there are no direct communication paths between S to Q as well as S to W. Hence the only communication path that exists is through the relay. The overall process is performed in two phases. In the first-hop, S sends messages to the relay. Then, in the second-hop, desired messages are received by the destination receivers from the best relay only. It is noteworthy that AF variable gain relaying scheme has been adopted in this work. Meanwhile, at the same time slot, the eavesdroppers also try to steal information from a best relay.

The best relay selection is performed using the method of distributed timers, where all the relays use their timers to estimate own instantaneous channel gains and compete to access the wireless medium according to their own channel conditions. In an opportunistic relaying scheme, competition among cooperative relays offers diversity benefits in the direction of destination that enhances secrecy rate (i.e. minimises secure outage probability) and adhere to the 'opportunistic' cooperation rule giving priority to the 'best' available relay even when they are not chosen to transmit but rather chosen to cooperatively listen.

The direct channel coefficients for S to ath ($a = 1, 2, 3, \ldots, P$) relay link is $f_{s,a} \in \mathcal{C}^{1\times 1}$, for ath relay to bth ($b = 1, 2, 3, \ldots, Q$) destination receiver link is $\mathbf{g}_{a,b} \in \mathcal{C}^{G_Q\times 1}$ (i.e. $\mathbf{g}_{ab} = [g_{1ab} \quad g_{2ab} \quad g_{3ab} \quad \ldots \quad g_{G_Qab}]^T$) and for ath relay to cth ($c = 1, 2, 3, \ldots, W$) eavesdropper link is $\mathbf{h}_{a,c} \in \mathcal{C}^{G_W\times 1}$ (i.e. $\mathbf{h}_{ac} = [h_{1ac} \quad h_{2ac} \quad h_{3ac} \quad \ldots \quad h_{G_Wac}]^T$).

In the first-hop, the received signal at ath relay is expressed as

$$y_{s,a} = f_{s,a}x + z_a, \tag{1}$$

where $x \sim \widetilde{\mathcal{N}}(0, T_s)$ is the transmitted message signal from S, T_s is the transmit power, $\widetilde{\mathcal{N}}$ is circularly symmetric complex Gaussian distribution with mean 0 and variance T_s, $z_a \sim \widetilde{\mathcal{N}}(0, N_a)$ indicates the additive white gaussian noise (AWGN) imposed on ath relay with noise power N_a.

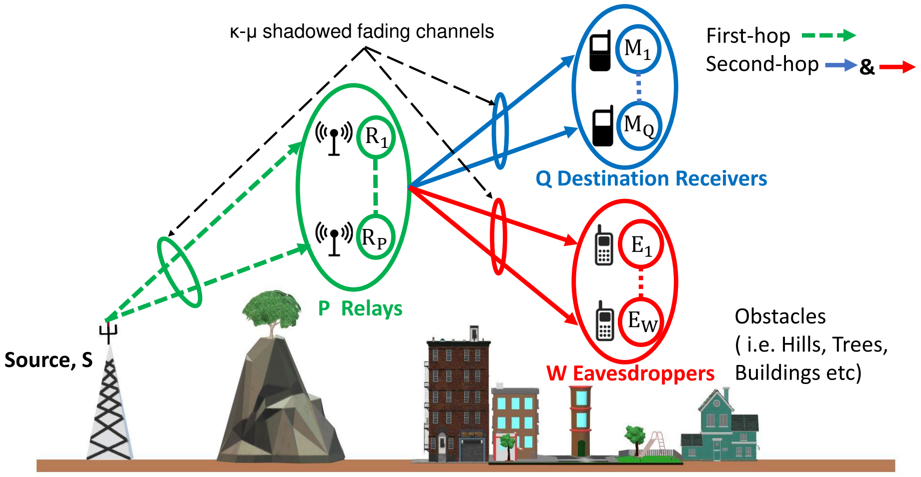


FIGURE 1. Proposed system model.

In the second-hop, the received signal of the ath best relay will be forwarded to the receivers. Hence, the received signals at the bth receiver is denoted as

$$\begin{aligned}\mathbf{y}_{a,b} &= \mathbf{g}_{a,b}y_{s,a} + \mathbf{j}_b = \mathbf{g}_{a,b}(f_{s,a}x + z_a) + \mathbf{j}_b \\ &= \mathbf{d}_{ab}x + \mathbf{u}_b, \end{aligned} \tag{2}$$

whereas the received signal at cth eavesdropper can be written as

$$\begin{aligned}\mathbf{y}_{a,c} &= \mathbf{h}_{a,c}y_{s,a} + \mathbf{k}_c = \mathbf{h}_{ac}(f_{s,a}x + z_a) + \mathbf{k}_c \\ &= \mathbf{d}_{ac}x + \mathbf{v}_c. \end{aligned} \tag{3}$$

Here, $\mathbf{u}_b \triangleq \mathbf{g}_{a,b}z_a + \mathbf{j}_b$, $\mathbf{v}_c \triangleq \mathbf{h}_{a,c}z_a + \mathbf{k}_c$, $\mathbf{d}_{a,b} = \mathbf{g}_{a,b}f_{s,a}$, $\mathbf{d}_{a,c} = \mathbf{h}_{a,c}f_{s,a}$, $\mathbf{j}_b \sim \tilde{\mathcal{N}}(0, N_b\mathbf{I}_{G_Q})$ and $\mathbf{k}_c \sim \tilde{\mathcal{N}}(0, N_c\mathbf{I}_{G_W})$ symbolize the noises imposed on the bth receiver and cth eavesdropper, N_b and N_c represent noise powers, and $\mathbf{I}_G(.)$ is the identity matrix of order $G \times G$.

We assume all the channels between source to relays ($S \rightarrow P$ links), relays to destination receivers ($P \rightarrow Q$ links), and relays to eavesdroppers ($P \rightarrow W$ links) undergo independent and identically distributed (i.i.d.) $\kappa - \mu$ shadowed fading i.e. all the LOS components are subjected to shadowing. This channel is widely used to model land mobile satellite communication systems. Moreover, this model exhibits extreme versatility since a wide number of multipath/generalized fading models can be obtained as special cases from this particular model as shown in Table 1.

A. CHANNEL MODEL

The instantaneous SNRs of $S \rightarrow P$, $P \rightarrow Q$ and $P \rightarrow W$ links are respectively given by $\lambda_{s,a} = \frac{T_s}{N_a}\|f_{s,a}\|^2$, $\lambda_{a,b} = \frac{P_a}{N_b}\|\mathbf{g}_{a,b}\|^2$, and $\lambda_{a,c} = \frac{P_a}{N_c}\|\mathbf{h}_{a,c}\|^2$, where P_a is the transmit signal power from the relay. The PDF of respective SNRs are shown below.

TABLE 1. Special Cases of $\kappa - \mu$ shadowed fading channel [38].

Fading Channels	$\kappa - \mu$ Shadowed Fading Parameters		
	$\kappa_b{=}\kappa_c{=}\kappa_a$	$\mu_b{=}\mu_c{=}\mu_a$	$m_b{=}m_c{=}m_a$
One Sided Gaussian	0	0.5	∞
Rayleigh	0	1	∞
Nakagami-m	0	m	∞
Shadowed Rician	K	1	m
Rician-K	K	1	∞

1) PDF OF $\lambda_{s,a}$

The PDF of $\lambda_{s,a}$ is given by [39, eq. 1]

$$f_{s,a}(\lambda) = \alpha_1 e^{-\mathcal{A}_2\lambda}\lambda^{\mu_a-1}{}_1F_1(m_a, \mu_a; \alpha_3\lambda), \tag{4}$$

where $\alpha_1 = \frac{\mu_a^{\mu_a}m_a^{m_a}(1+\kappa_a)^{\mu_a}}{\Gamma(\mu_a)\bar{\lambda}_{sa}^{\mu_a}(\mu_a\kappa_a+m_a)^{m_a}}$, $\mathcal{A}_2 = \frac{\mu_a(1+\kappa_a)}{\bar{\lambda}_{sa}}$, $\alpha_3 = \frac{\mu_a^2\kappa_a(1+\kappa_a)}{(\mu_a\underline{\kappa}_a+m_a)\bar{\lambda}_{sa}}$, the average SNR of $S \rightarrow P$ link channel is $\bar{\lambda}_{sa}$, κ_a is the ratio of the powers between dominant and scattered components, μ_a is the number of clusters, m_a is the Nakagami-m faded shadowing component and ${}_1F_1(.,.;.)$ is the confluent hyper-geometric function which can be expressed as ${}_1F_1(x_1, y_1; z_1) = \frac{\Gamma(y_1)}{\Gamma(x_1)}\sum_{d_1=0}^{\infty}\frac{\Gamma(x_1+d_1)z_1^{d_1}}{\Gamma(y_1+d_1)d_1!}$ [40, eq. 13]. Hence, finally $f_{s,a}(\lambda)$ can be written as

$$f_{s,a}(\lambda) = \sum_{e_1=0}^{\infty}\mathcal{A}_1 e^{-\mathcal{A}_2\lambda}\lambda^{\mathcal{A}_3}, \tag{5}$$

where $\mathcal{A}_1 = \alpha_1\alpha_{e_1}$, $\alpha_{e_1} = \frac{\Gamma(\mu_a)\Gamma(m_a+e_1)\alpha_3^{e_1}}{\Gamma(m_a)\Gamma(\mu_a+e_1)e_1!}$, and $\mathcal{A}_3 = \mu_a - 1 + e_1$.

2) PDF OF $\lambda_{a,b}$

Similar to (5), PDF of $\lambda_{a,b}$ can be written as [39, eq. 1]

$$f_{a,b}(\lambda) = \sum_{e_2=0}^{\infty}\mathcal{B}_1 e^{-\mathcal{B}_2\lambda}\lambda^{\mathcal{B}_3}, \tag{6}$$

where $\mathcal{B}_1 = \beta_1\beta_{e_2}, \beta_1 = \frac{(G_Q\mu_b)^{G_Q\mu_b}(G_Qm_b)^{G_Qm_b}(1+\kappa_b)^{G_Q\mu_b}}{\Gamma(G_Q\mu_b)(\bar{\lambda}_{ab})^{G_Q\mu_b}(G_Q\mu_b\kappa_b+G_Qm_b)^{G_Qm_b}}$, $\beta_{e_2} = \frac{\Gamma(G_Q\mu_b)\Gamma(G_Qm_b+e_2)\beta_2^{e_2}}{\Gamma(G_Qm_b)\Gamma(G_Q\mu_b+e_2)e_2!}$, $\beta_2 = \frac{G_Q^2\mu_b^2\kappa_b(1+\kappa_b)}{(G_Q\mu_b\kappa_b+G_Qm_b)\bar{\lambda}_{ab}}$, $\mathcal{B}_2 = \frac{G_Q\mu_b(1+\kappa_b)}{\bar{\lambda}_{ab}}$, $\mathcal{B}_3 = G_Q\mu_b - 1 + e_2$, the average SNR of $P \rightarrow Q$ link channel is $\bar{\lambda}_{ab}$ and shape parameters corresponding to $P \rightarrow Q$ link are denoted by κ_b, μ_b and m_b.

3) PDF OF $\lambda_{a,c}$

The PDF of $\lambda_{a,c}$ can be expressed as [39, eq. 1]

$$f_{a,c}(\lambda) = \sum_{e_3=0}^{\infty} \mathcal{C}_1 e^{-\mathcal{C}_2\lambda}\lambda^{\mathcal{C}_3}, \tag{7}$$

where $\mathcal{C}_1 = \iota_1\iota_{e_3}, \iota_1 = \frac{(G_W\mu_c)^{G_W\mu_c}(G_Wm_c)^{G_Wm_c}(1+\kappa_c)^{G_W\mu_c}}{\Gamma(G_W\mu_c)(\bar{\lambda}_{ac})^{G_W\mu_c}(G_W\mu_c\kappa_c+G_Wm_c)^{G_Wm_c}}$, $\iota_{e_3} = \frac{\Gamma(G_W\mu_c)\Gamma(G_Wm_c+e_3)\iota_2^{e_3}}{\Gamma(G_Wm_c)\Gamma(G_Wu_c+e_3)e_3!}$, $\iota_2 = \frac{G_W^2\mu_c^2\kappa_c(1+\kappa_c)}{(G_W\mu_c\kappa_c+G_Wm_c)\bar{\lambda}_{ac}}$, $\mathcal{C}_2 = \frac{G_W\mu_c(1+\kappa_c)}{\bar{\lambda}_{ac}}$, $\mathcal{C}_3 = G_W\mu_c - 1 + e_3$, the average SNR of $P \rightarrow W$ link is $\bar{\lambda}_{ac}$ and κ_c, μ_c and m_c symbolize the shape parameters corresponding to $P \rightarrow W$ link.

B. PDFs OF DUAL-HOP SNRs

Denoting SNRs of $S \rightarrow Q$ and $S \rightarrow W$ links by $\lambda_{s,b}$ and $\lambda_{s,c}$, respectively, the PDFs of $\lambda_{s,b}$ and $\lambda_{s,c}$ are defined as

$$f_{s,b}(\lambda) = \frac{dF_{s,b}(\lambda)}{d\lambda}, \tag{8}$$

$$f_{s,c}(\lambda) = \frac{dF_{s,c}(\lambda)}{d\lambda}, \tag{9}$$

where $F_{s,b}(\lambda)$, and $F_{s,c}(\lambda)$ express the CDFs of $\lambda_{s,b}$, and $\lambda_{s,c}$. The CDF of $\lambda_{s,b}$ is defined as

$$F_{s,b}(\lambda) = 1 - Pr(\lambda_{s,a} > \lambda_{s,b})Pr(\lambda_{a,b} > \lambda_{s,b}), \tag{10}$$

where $Pr(\lambda_{s,a} > \lambda_{s,b})$ and $Pr(\lambda_{a,b} > \lambda_{s,b})$ are the complementary cumulative distribution functions (CCDFs) of $\lambda_{s,a}$ and $\lambda_{a,b}$, and the CCDFs are respectively defined as

$$Pr(\lambda_{s,a} > \lambda_{s,b}) = \int_{\lambda_{s,b}}^{\infty} f_{s,a}(\lambda)d\lambda, \tag{11}$$

$$Pr(\lambda_{a,b} > \lambda_{s,b}) = \int_{\lambda_{s,b}}^{\infty} f_{a,b}(\lambda)d\lambda. \tag{12}$$

Substituting (5) into (11) and executing integration using the following identity of [41, eq. 3.351.2], we get

$$Pr(\lambda_{s,a} > \lambda_{s,b}) = \sum_{e_1=0}^{\infty} \mathcal{A}_1\mathcal{A}_2^{-\mu_a-e_1}\Gamma(\mu_a + e_1, \mathcal{A}_2\lambda_{s,b}), \tag{13}$$

where $\Gamma(.,.)$ denotes the upper incomplete gamma function. Further, substituting (6) into (12) and performing integration, we have

$$Pr(\lambda_{a,b} > \lambda_{s,b}) = \sum_{e_2=0}^{\infty} \mathcal{B}_1\mathcal{B}_2^{-G_Q\mu_b-e_2}\Gamma(G_Q\mu_b + e_2, \mathcal{B}_2\lambda_{s,b}). \tag{14}$$

Deploying (13) and (14) into (10), the CDF of $\lambda_{s,b}$ is obtained as

$$F_{s,b}(\lambda) = 1 - \sum_{e_2=0}^{\infty}\sum_{e_1=0}^{\infty} \lambda_{e_2}\Gamma(\mu_a + e_1, \mathcal{A}_2\lambda) \times\Gamma(G_Q\mu_b + e_2, \mathcal{B}_2\lambda), \tag{15}$$

where $\lambda_{e_2} = \mathcal{A}_1\mathcal{B}_1\mathcal{A}_2^{-\mu_a-e_1}\mathcal{B}_2^{-G_Q\mu_b-e_2}$. Now, substituting (15) into (8) and performing differentiation with respect to $\lambda_{s,b}$, the PDF of $\lambda_{s,b}$ is found as

$$f_{s,b}(\lambda) = \sum_{s_2=0}^{\infty}\sum_{e_4=0}^{\infty} \frac{\lambda_{e_4}\lambda^{\mu_a+s_2-1}}{e^{\mathcal{A}_2\lambda}}\Gamma(G_Q\mu_b + e_4, \mathcal{B}_2\lambda) + \sum_{s_3=0}^{\infty}\sum_{e_5=0}^{\infty} \frac{\lambda_{e_5}\lambda^{G_Q\mu_b+e_5-1}}{e^{\mathcal{B}_2\lambda}}\Gamma(\mu_a + s_3, \mathcal{A}_2\lambda), \tag{16}$$

where $\lambda_{e_4} = \mathcal{A}_1\mathcal{B}_1\mathcal{A}_2^{-\mu_a-s_2}\mathcal{B}_2^{-G_Q\mu_b-e_4}$ and $\lambda_{e_5} = \mathcal{A}_1\mathcal{B}_1\mathcal{A}_2^{-\mu_a-s_3}\mathcal{B}_2^{-G_Q\mu_b-e_5}$. Similarly, the CDF of $\lambda_{s,c}$ can be obtained as

$$F_{s,c}(\lambda) = 1 - \sum_{e_3=0}^{\infty}\sum_{e_1=0}^{\infty} \lambda_{e_3}\Gamma(\mu_a + e_1, \mathcal{A}_2\lambda) \times\Gamma(G_W\mu_c + e_3, \mathcal{C}_2\lambda), \tag{17}$$

where $\lambda_{e_3} = \mathcal{A}_1\mathcal{C}_1\mathcal{A}_2^{-\mu_a-e_1}\mathcal{C}_2^{-G_W\mu_c-e_3}$. Furthermore, replacing (17) into (9), the PDF of $\lambda_{s,c}$ is obtained as

$$f_{s,c}(\lambda) = \sum_{s_4=0}^{\infty}\sum_{e_6=0}^{\infty} \frac{\lambda_{e_6}\lambda^{\mu_a+s_4-1}}{e^{\mathcal{A}_2\lambda}}\Gamma(G_W\mu_c + e_6, \mathcal{C}_2\lambda) + \sum_{s_5=0}^{\infty}\sum_{e_7=0}^{\infty} \frac{\lambda_{e_7}\lambda^{G_W\mu_c+e_7-1}}{e^{\mathcal{C}_2\lambda}}\Gamma(\mu_a + s_5, \mathcal{A}_2\lambda), \tag{18}$$

where $\lambda_{e_6} = \mathcal{A}_1\mathcal{C}_1\mathcal{A}_2^{-\mu_a-s_4}\mathcal{C}_2^{-G_W\mu_c-e_6}$ and $\lambda_{e_7} = \mathcal{A}_1\mathcal{C}_1\mathcal{A}_2^{-\mu_a-s_5}\mathcal{C}_2^{-G_W\mu_c-e_7}$.

C. BEST RELAY SELECTION

Let λ_b^* denote the SNR between best relay and bth receiver which is expressed as

$$\lambda_b^* = arg_{a\in\varpi}^{max} min(\lambda_{s,a}, \lambda_{a,b}), \tag{19}$$

where $\varpi = 1, 2, \ldots, P$ is the relay set. The CDF of λ_b^* is demonstrated as

$$F_{*,b}(\lambda) = [F_{s,b}(\lambda)]^P. \tag{20}$$

Hence, substituting (15) into (20), the CDF of λ_b^* is derived as

$$F_{*,b}(\lambda) = \left[1 - \sum_{e_2=0}^{\infty}\sum_{e_1=0}^{\infty} \lambda_{e_2}\Gamma(\mu_a + e_1, \mathcal{A}_2\lambda) \times\Gamma(G_Q\mu_b + e_2, \mathcal{B}_2\lambda)\right]^P. \tag{21}$$

Differentiating (20) with respect to $\lambda_{s,b}$, the PDF of λ_b^* is obtained as

$$f_{*,b}(\lambda) = Pf_{s,b}(\lambda)[F_{s,b}(\lambda)]^{P-1}. \tag{22}$$

Again, deploying (15) and (16) into (22), $f_{*,b}(\lambda)$ is given by

$$\begin{aligned} &f_{*,b}(\lambda) \\ &= P\Bigg[\sum_{s_2=0}^{\infty}\sum_{e_4=0}^{\infty}\frac{\lambda_{e_4}\lambda^{\mu_a+s_2-1}}{e^{\mathcal{A}_2\lambda}}\Gamma(G_Q\mu_b+e_4,\mathcal{B}_2\lambda) \\ &\quad+\sum_{s_3=0}^{\infty}\sum_{e_5=0}^{\infty}\frac{\lambda_{e_5}\lambda^{G_Q\mu_b+e_5-1}}{e^{\mathcal{B}_2\lambda}}\Gamma(\mu_a+s_3,\mathcal{A}_2\lambda)\Bigg]\Bigg[1 \\ &\quad-\sum_{e_2=0}^{\infty}\sum_{e_1=0}^{\infty}\lambda_{e_2}\Gamma(\mu_a+e_1,\mathcal{A}_2\lambda)\Gamma(G_Q\mu_b+e_2,\mathcal{B}_2\lambda)\Bigg]^{P-1}. \end{aligned} \tag{23}$$

Similar to (19), the SNR between best relay and cth eavesdropper denoted by λ_c^* is explained as

$$\lambda_c^* = arg_{a\in\varpi}^{max} min(\lambda_{s,a},\lambda_{a,c}), \tag{24}$$

the CDF of which is given by

$$F_{*,c}(\lambda) = [F_{s,c}(\lambda)]^{P}. \tag{25}$$

Substituting (17) into (25), the CDF of λ_c^* is obtained as

$$\begin{aligned} F_{*,c}(\lambda) = \Bigg[1-\sum_{e_3=0}^{\infty}\sum_{e_1=0}^{\infty}\lambda_{e_3}\Gamma(\mu_a+e_1,\mathcal{A}_2\lambda) \\ \times\Gamma(G_W\mu_c+e_3,\mathcal{C}_2\lambda)\Bigg]^{P}. \end{aligned} \tag{26}$$

Further, differentiating (25) with respect to $\lambda_{s,c}$, and substituting (17) and (18) into it, the PDF of λ_c^* is derived as

$$\begin{aligned} &f_{*,c}(\lambda) \\ &= P\Bigg[\sum_{s_4=0}^{\infty}\sum_{e_6=0}^{\infty}\frac{\lambda_{e_6}\lambda^{\mu_a+s_4-1}}{e^{\mathcal{A}_2\lambda}}\Gamma(G_W\mu_c+e_6,\mathcal{C}_2\lambda) \\ &\quad+\sum_{s_5=0}^{\infty}\sum_{e_7=0}^{\infty}\frac{\lambda_{e_7}\lambda^{G_W\mu_c+e_7-1}}{e^{\mathcal{C}_2\lambda}}\Gamma(\mu_a+s_5,\mathcal{A}_2\lambda)\Bigg] \\ &\quad\Bigg[1-\sum_{e_3=0}^{\infty}\sum_{e_1=0}^{\infty}\lambda_{e_3}\Gamma(\mu_a+e_1,\mathcal{A}_2\lambda)\Gamma(G_W\mu_c+e_3,\mathcal{C}_2\lambda)\Bigg]^{P-1}. \end{aligned} \tag{27}$$

D. MODELING OF MULTICAST CHANNELS

Note that we consider multiple destination receivers (Q) each of which can receive the multicast messages at the same instant. To ascertain a secure communication with each receiver, we demonstrate secrecy analysis considering the worst possible scenario which includes taking into consideration the minimum SNR among all receivers as denoted by $\lambda_{min} = min_{1<b<Q}\lambda_b^*$. Hence, it is clear from this consideration that if the proposed system is capable of protecting multicast information from being eavesdropped for the worst case, then for all other cases (i.e. better than worst case), the system will undoubtedly be secure. Since, $\lambda_1^*, \lambda_2^*, \ldots, \lambda_Q^*$ are all independent, using order statistics, the PDF of λ_{min} can be defined as [42]

$$f_{\lambda_{min}}(\lambda) = Qf_{*,b}(\lambda)[1-F_{*,b}(\lambda)]^{Q-1}. \tag{28}$$

Now, substituting (21) and (23) into (28), $f_{\lambda_{min}}(\lambda)$ is obtained as

$$\begin{aligned} &f_{\lambda_{min}}(\lambda) \\ &= PQ\Bigg[\sum_{s_2=0}^{\infty}\sum_{e_4=0}^{\infty}\frac{\lambda_{e_4}\lambda^{\mu_a+s_2-1}}{e^{\mathcal{A}_2\lambda}}\Gamma(G_Q\mu_b+e_4,\mathcal{B}_2\lambda) \\ &\quad+\sum_{s_3=0}^{\infty}\sum_{e_5=0}^{\infty}\frac{\lambda_{e_5}\lambda^{G_Q\mu_b+e_5-1}}{e^{\mathcal{B}_2\lambda}}\Gamma(\mu_a+s_3,\mathcal{A}_2\lambda)\Bigg]\Bigg[1 \\ &\quad-\sum_{e_2=0}^{\infty}\sum_{e_1=0}^{\infty}\lambda_{e_2}\Gamma(\mu_a+e_1,\mathcal{A}_2\lambda)\Gamma(G_Q\mu_b+e_2,\mathcal{B}_2\lambda)\Bigg]^{P-1} \\ &\quad\times\Bigg[1-\Bigg[1-\sum_{e_2=0}^{\infty}\sum_{e_1=0}^{\infty}\lambda_{e_2}\Gamma(\mu_a+e_1,\mathcal{A}_2\lambda) \\ &\quad\times\Gamma(G_Q\mu_b+e_2,\mathcal{B}_2\lambda)\Bigg]^{P}\Bigg]^{Q-1}. \end{aligned} \tag{29}$$

Utilizing the identity of [41, eq. 1.111], (29) can be simplified as

$$\begin{aligned} &f_{\lambda_{min}}(\lambda) \\ &= PQ\sum_{e_8=0}^{Q-1}\sum_{e_9=0}^{P+Pe_8-1}\lambda_{e_9}\Bigg[\sum_{s_3=0}^{\infty}\sum_{e_5=0}^{\infty}\frac{\lambda_{e_5}\lambda^{G_Q\mu_b+e_5-1}}{e^{\mathcal{B}_2\lambda}} \\ &\quad\times\Gamma(\mu_a+s_3,\mathcal{A}_2\lambda)+\sum_{s_2=0}^{\infty}\sum_{e_4=0}^{\infty}\frac{\lambda_{e_4}\lambda^{\mu_a+s_2-1}}{e^{\mathcal{A}_2\lambda}} \\ &\quad\times\Gamma(G_Q\mu_b+e_4,\mathcal{B}_2\lambda)\Bigg]\Bigg[\sum_{e_2=0}^{\infty}\sum_{e_1=0}^{\infty}\lambda_{e_2}\Gamma(\mu_a+e_1,\mathcal{A}_2\lambda) \\ &\quad\times\Gamma(G_Q\mu_b+e_2,\mathcal{B}_2\lambda)\Bigg]^{e_9}, \end{aligned} \tag{30}$$

where $\lambda_{e_9} = \frac{\binom{Q-1}{e_8}\binom{P+Pe_8-1}{e_9}}{(-1)^{-e_8-e_9}}$. Applying the identity of [41, eq. 8.352.7], (30) is further simplified as

$$\begin{aligned} f_{\lambda_{min}}(\lambda) = PQ\sum_{e_8=0}^{Q-1}\sum_{e_9=0}^{P+Pe_8-1}\lambda_{e_9}e^{-(\mathcal{A}_2+\mathcal{B}_2)\lambda}\big[\gamma_1(\lambda)\big]^{e_9} \\ \times\Bigg[\sum_{s_3=0}^{\infty}\sum_{e_5=0}^{\infty}\sum_{e_{11}=0}^{\mu_a+s_3-1}\lambda_{e_{11}}\lambda^{G_Q\mu_b+e_5+e_{11}-1} \\ +\sum_{s_2=0}^{\infty}\sum_{e_4=0}^{\infty}\sum_{e_{10}=0}^{G_Q\mu_b+e_4-1}\lambda_{e_{10}}\lambda^{\mu_a+s_2+e_{10}-1}\Bigg], \end{aligned} \tag{31}$$

where $\lambda_{e_{10}} = \frac{\lambda_{e_4}\Gamma(e_4+G_Q\mu_b)}{e_{10}!\mathcal{B}_2^{-e_{10}}}$ and $\lambda_{e_{11}} = \frac{\lambda_{e_5}\Gamma(e_5+\mu_a)}{e_{11}!\mathcal{A}_2^{-e_{11}}}$. Here $\gamma_1(\lambda)$ is denoted as

$$\gamma_1(\lambda) = \sum_{e_1=0}^{\infty}\sum_{e_2=0}^{\infty}\sum_{e_{12}=0}^{\mu_a+e_1-1}\sum_{e_{13}=0}^{G_Q\mu_b+e_2-1} \lambda_{e_{13}}\lambda^{(e_{12}+e_{13})} \times e^{-(\mathcal{A}_2+\mathcal{B}_2)\lambda}, \tag{32}$$

where $\lambda_{e_{13}} = \frac{\mathcal{A}_1\mathcal{B}_1\Gamma(e_1+\mu_a)\mathcal{B}_2^{-G_Q\mu_b-e_2+e_{13}}\Gamma(e_2+G_Q\mu_b)}{e_{12}!e_{13}!\mathcal{A}_2^{\mu_a+e_1-e_{12}}}$. Applying the multinomial theorem of [43, eq. 7], we obtain

$$[\gamma_1(\lambda)]^{e_9} = \sum_{\varpi_{e_9}} \binom{e_9}{g_{0,0,0,0},\cdots,g_{e_1,e_2,e_{12},e_{13}},\cdots,e_{\infty,\infty,\mu_a+e_1-1,G_Q\mu_b+e_2-1}} \times \Omega_{\varpi_{e_9}} e^{-\Lambda_{\varpi_{e_9}}\lambda}\lambda^{\Psi_{\varpi_{e_9}}}, \tag{33}$$

where $\binom{i}{i_1,i_2,\cdots,i_m} = \frac{i!}{i_1!i_2!\cdots i_m!}$ symbolizes the multinomial coefficients, $\Omega_{\varpi_{e_9}} = \prod_{e_1,e_2,e_{12},e_{13}} \lambda_{e_{13}}^{g_{e_1,e_2,e_{12},e_{13}}}$, $\Psi_{\varpi_{e_9}} = \sum_{e_1}\sum_{e_2}\sum_{e_{12}}\sum_{e_{13}}(e_{12}+e_{13})g_{e_1,e_2,e_{12},e_{13}}$ and $\Lambda_{\varpi_{e_9}} = \sum_{e_1}\sum_{e_2}\sum_{e_{12}}\sum_{e_{13}}(\mathcal{A}_2+\mathcal{B}_2)g_{e_1,e_2,e_{12},e_{13}}$. For each element of ϖ_{e_9}, the sum in (33) is to be performed, which can be defined as

$$\begin{aligned}\varpi_{e_9} &= [(g_{0,0,0,0},\cdots,g_{e_1,e_2,e_{12},e_{13}},\cdots, \\ &\quad e_{\infty,\infty,\mu_a+e_1-1,G_Q\mu_b+e_2-1}): \\ &\quad g_{e_1,e_2,e_{12},e_{13}} \in \mathbb{N}, 0 \le e_1 \le \infty, 0 \le e_2 \le \infty, \\ &\quad 0 \le e_{12} \le \mu_a + e_1 - 1, 0 \le e_{13} \le G_Q\mu_b + e_2 - 1; \\ &\quad \sum_{e_1,e_2,e_{12},e_{13}} g_{e_1,e_2,e_{12},e_{13}} = e_9].\end{aligned} \tag{34}$$

Finally, substituting (33) into (31), we get

$$f_{\lambda_{min}}(\lambda) = \sum_{e_8=0}^{Q-1}\sum_{e_9=0}^{P+Pe_8-1}\sum_{\varpi_{e_9}}\Big(\sum_{s_2=0}^{\infty}\sum_{e_4=0}^{\infty}\sum_{e_{10}=0}^{G_Q\mu_b+e_4-1} \mathcal{J}_1\lambda^{\mathcal{J}_3} + \sum_{s_3=0}^{\infty}\sum_{e_5=0}^{\infty}\sum_{e_{11}=0}^{\mu_a+s_3-1} \mathcal{J}_2\lambda^{\mathcal{J}_4}\Big)e^{-\mathcal{J}_5\lambda}, \tag{35}$$

where $\lambda_{\varpi_{e_9}} = \binom{e_9}{g_{0,0,0,0},\cdots,g_{e_1,e_2,e_{12},e_{13}},\cdots,e_{\infty,\infty,\mu_a+e_1-1,G_Q\mu_b+e_2-1}} \times \Omega_{\varpi_{e_9}}$, $\mathcal{J}_1 = PQ\lambda_{e_9}\lambda_{e_{10}}\lambda_{\varpi_{e_9}}$, $\mathcal{J}_2 = PQ\lambda_{e_9}\lambda_{e_{11}}\lambda_{\varpi_{e_9}}$, $\mathcal{J}_3 = \mu_a+\Psi_{\varpi_{e_9}}+s_2+e_{10}-1$, $\mathcal{J}_4 = G_Q\mu_b+\Psi_{\varpi_{e_9}}+e_5+e_{11}-1$, and $\mathcal{J}_5 = \mathcal{A}_2+\mathcal{B}_2+\Lambda_{\varpi_{e_9}}$.

E. MODELING OF EAVESDROPPER CHANNELS

In order to perform the secrecy analysis assuming the worst possible case (i.e. maximum strength of the eavesdroppers), we herein, consider maximum SNR among W eavesdroppers as denoted by $\lambda_{max} = max_{1<c<W}\lambda_c^*$. Similar to the multicast channels, λ_1^*, λ_2^*, …, λ_W^* are independent, and by means of order statistics, the PDF of λ_{max} is defined as [42]

$$f_{\lambda_{max}}(\lambda) = Wf_{*,c}(\lambda)[F_{*,c}(\lambda)]^{W-1}. \tag{36}$$

Hence, substituting (26) and (27) into (36), and after some mathematical manipulation, $f_{\lambda_{max}}(\lambda)$ is obtained as

$$\begin{aligned}f_{\lambda_{max}}(\lambda) = PW\Bigg[&\sum_{s_4=0}^{\infty}\sum_{e_6=0}^{\infty}\frac{\lambda_{e_6}\lambda^{\mu_a+s_4-1}}{e^{\mathcal{A}_2\lambda}}\Gamma(G_W\mu_c+e_6,\mathcal{C}_2\lambda) \\ &+\sum_{s_5=0}^{\infty}\sum_{e_7=0}^{\infty}\frac{\lambda_{e_7}\lambda^{G_W\mu_c+e_7-1}}{e^{\mathcal{C}_2\lambda}}\Gamma(\mu_a+s_5,\mathcal{A}_2\lambda)\Bigg] \\ &\times\Bigg[1-\sum_{e_3=0}^{\infty}\sum_{e_1=0}^{\infty}\lambda_{e_3}\Gamma(\mu_a+e_1,\mathcal{A}_2\lambda) \\ &\times\Gamma(G_W\mu_c+e_3,\mathcal{C}_2\lambda)\Bigg]^{PW-1}.\end{aligned} \tag{37}$$

Simplifying (37) similar to (31), we get

$$\begin{aligned}f_{\lambda_{max}}(\lambda) = PW&\sum_{e_{14}=0}^{PW-1}\lambda_{e_{14}}e^{-(\mathcal{A}_2+\mathcal{C}_2)\lambda}[\gamma_3(\lambda)]^{e_{14}}\Bigg[\sum_{s_4=0}^{\infty}\sum_{e_6=0}^{\infty} \\ &\times\sum_{e_{15}=0}^{G_W\mu_c+e_6-1}\lambda_{e_{15}}\lambda^{\mu_a+s_4+e_{15}-1}+\sum_{s_5=0}^{\infty}\sum_{e_7=0}^{\infty} \\ &\times\sum_{e_{16}=0}^{\mu_a+s_5-1}\lambda_{e_{16}}\lambda^{G_W\mu_c+e_7+e_{16}-1}\Bigg],\end{aligned} \tag{38}$$

where $\lambda_{e_{14}} = (-1)^{e_{14}}\binom{PR-1}{e_{14}}$, $\lambda_{e_{15}} = \frac{\lambda_{e_6}\Gamma(e_6+G_W\mu_c)}{e_{15}!\mathcal{C}_2^{-e_{15}}}$ and $\lambda_{e_{16}} = \frac{\lambda_{e_7}\Gamma(s_5+\mu_a)}{e_{16}!\mathcal{A}_2^{-e_{16}}}$. Here,

$$\gamma_3(\lambda) = \sum_{e_1=0}^{\infty}\sum_{e_3=0}^{\infty}\sum_{e_{17}=0}^{\mu_a+e_1-1}\sum_{e_{18}=0}^{G_W\mu_c+e_3-1}\lambda_{e_{18}}\lambda^{e_{17}+e_{18}} \times e^{-(\mathcal{A}_2+\mathcal{C}_2)\lambda}, \tag{39}$$

where $\lambda_{e_{18}} = \frac{\mathcal{A}_1\mathcal{C}_1\Gamma(e_1+\mu_a)\mathcal{C}_2^{-G_W\mu_c-e_3+e_{18}}\Gamma(e_3+G_W\mu_c)}{e_{17}!e_{18}!\mathcal{A}_2^{\mu_a+e_1-e_{17}}}$.

Implementing multinomial theorem, we get

$$[\gamma_3(\lambda)]^{e_{14}} = \sum_{\varpi_{e_{14}}}\lambda_{\varpi_{e_{14}}}e^{-\Lambda_{\varpi_{e_{14}}}\lambda}\lambda^{\Psi_{\varpi_{e_{14}}}}, \tag{40}$$

where $\lambda_{\varpi_{e_{14}}} = \sum_{\varpi_{e_{14}}}\binom{e_{14}}{h_{0,0,0,0},\cdots,h_{e_1,e_3,e_{17},e_{18}},\cdots,e_{\infty,\infty,\mu_a+s_5-1},G_W\mu_c+e_3-1}\Omega_{\varpi_{e_{14}}}$, $\Omega_{\varpi_{e_{14}}} = \prod_{e_1,e_3,e_{17},e_{18}}\lambda_{e_{18}}^{h_{e_1,e_3,e_{17},e_{18}}}$, $\Psi_{\varpi_{e_{14}}} = \sum_{e_1}\sum_{e_3}\sum_{e_{17}}\sum_{e_{18}}(e_{17}+e_{18})h_{e_1,e_3,e_{17},e_{18}}$, $\Lambda_{\varpi_{e_{14}}} = \sum_{e_1}\sum_{e_3}\sum_{e_{17}}\sum_{e_{18}}(\mathcal{A}_2+\mathcal{C}_2)h_{e_1,e_3,e_{17},e_{18}}$.

Finally, substituting (40) into (38), we obtain

$$f_{\lambda_{max}}(\lambda) = \sum_{e_{14}=0}^{PW-1}\sum_{\varpi_{e_{14}}}\Big(\sum_{s_4=0}^{\infty}\sum_{e_6=0}^{\infty}\sum_{e_{15}=0}^{G_W\mu_c+e_6-1}\mathcal{J}_6\lambda^{\mathcal{J}_8} + \sum_{s_5=0}^{\infty}\sum_{e_7=0}^{\infty}\sum_{e_{16}=0}^{\mu_a+s_5-1}\mathcal{J}_7\lambda^{\mathcal{J}_9}\Big)e^{-\mathcal{J}_{10}\lambda}, \tag{41}$$

where $\mathcal{J}_6 = PW\lambda_{e_{14}}\lambda_{e_{15}}\lambda_{\varpi_{e_{14}}}$, $\mathcal{J}_7 = PW\lambda_{e_{14}}\lambda_{e_{16}}\lambda_{\varpi_{e_{14}}}$, $\mathcal{J}_8 = \mu_a+\Psi_{\varpi_{e_{14}}}+s_4+e_{15}-1$, $\mathcal{J}_9 = G_W\mu_c+\Psi_{\varpi_{e_{14}}}+e_7+e_{16}-1$ and $\mathcal{J}_{10} = \mathcal{A}_2+\mathcal{C}_2+\Lambda_{\varpi_{e_{14}}}$.

III. PERFORMANCE METRICS

In the following parts, we utilize $f_{\lambda_{min}}(\lambda)$ and $f_{\lambda_{max}}(\lambda)$ of (35) and (41) to derive analytical expressions of three performance metrics i.e. SOPM, PNSMC, and ESMC.

A. SOPM ANALYSIS

Signifying the target secrecy rate by ξ_s, and the secrecy multicast capacity as $\mathcal{C}_{s,m}$ [44], the SOPM is denoted as

$$\begin{aligned} P_{out}(\xi_s) &= \Pr(\mathcal{C}_{s,m} < \xi_s) \\ &= 1 - \int_0^\infty \int_{\psi_s}^\infty f_{\lambda_{min}}(\lambda_b^*) f_{\lambda_{max}}(\lambda_c^*) d\lambda_b^* d\lambda_c^*, \end{aligned} \tag{42}$$

where $\psi_s = 2^{\xi_s}(1+\lambda_c^*)-1$ and $\xi_s > 0$. This definition specifies that, reliable transmission is achievable only if $\mathcal{C}_{s,m} > \xi_s$, otherwise the security cannot be guaranteed. Substituting (35) and (41) into (42), we get

$$\begin{aligned} &P_{out}(\xi_s) \\ &= \int_0^\infty \int_{\psi_s}^\infty \sum_{e_8=0}^{Q-1} \sum_{e_9=0}^{P+Pe_8-1} \sum_{\varpi_{e_9}} \Big(\sum_{s_2=0}^{\infty} \sum_{e_4=0}^{\infty} \sum_{e_{10}=0}^{G_Q\mu_b+e_4-1} \mathcal{J}_1 \lambda_b^{*\mathcal{J}_3} \\ &\quad + \sum_{s_3=0}^{\infty} \sum_{e_5=0}^{\infty} \sum_{e_{11}=0}^{\mu_a+s_3-1} \mathcal{J}_2 \lambda_b^{*\mathcal{J}_4} \Big) e^{-\mathcal{J}_5 \lambda_b^*} \sum_{e_{14}=0}^{PW-1} \sum_{\varpi_{e_{14}}} \Big(\sum_{s_4=0}^{\infty} \sum_{e_6=0}^{\infty} \\ &\quad \times \sum_{e_{15}=0}^{G_W\mu_c+e_6-1} \mathcal{J}_6 \lambda_c^{*\mathcal{J}_8} + \sum_{s_5=0}^{\infty} \sum_{e_7=0}^{\infty} \sum_{e_{16}=0}^{\mu_a+s_5-1} \mathcal{J}_7 \lambda_c^{*\mathcal{J}_9} \Big) \\ &\quad \times e^{-\mathcal{J}_{10}\lambda_c^*} d\lambda_c^* d\lambda_b^*. \end{aligned} \tag{43}$$

Now, performing integration making use of [41, (eq. 3.351.2, 3.351.3)] in (43), the closed form expression for the SOPM is given in (44), as shown at the bottom of this page, where $p_{\psi_s} = 2^{\xi_s} - 1$, $q_{\psi_s} = 2^{\xi_s}$, $\omega_5 = \frac{\mathcal{J}_1 \mathcal{J}_3! \binom{f_2}{f_4} p_{\psi_s}^{f_2-f_4}}{f_2! \mathcal{J}_5^{\mathcal{J}_3-f_2+1} q_{\psi_s}^{-f_4} e^{\mathcal{J}_5 p_{\psi_s}}}$ and $\omega_6 = \frac{\mathcal{J}_2 \mathcal{J}_4! \binom{f_3}{f_5} p_{\psi_s}^{f_3-f_5}}{f_3! \mathcal{J}_5^{\mathcal{J}_4-f_3+1} q_{\psi_s}^{-f_5} e^{\mathcal{J}_5 p_{\psi_s}}}$.

1) SIGNIFICANCE OF SOPM EXPRESSION

It can be seen that, (44) comprises of all the system parameters of the proposed network which helps to evaluate the secrecy outage behaviour of the proposed system. Hence (44) can explain and quantify the secrecy trade-off in terms of the secrecy outage probability utilizing opportunistic relaying mechanism. Besides, (44) also exhibits generic characteristics which helps the design engineers to model more practical networks. Note that, as a special case of the proposed network with $\kappa_a = K$, $\mu_a = 1$ and $m_a = m$, we obtain Shadowed Rician fading distribution for satellite links and for $\kappa_b = \kappa_c = 0$, $\mu_b = \mu_c = m$ and $m_b = m_c \to \infty$, we obtain Nakagami-m fading distribution for terrestrial links. For this particular case our results with (44) totally matches with [45, eq. 45]. Likewise, for a special case with ($\kappa_b = \kappa_c = \kappa_a = 0$, $\mu_b = \mu_c = \mu_a = m$, and $m_b = m_c = m_a \to \infty$), our results with (44) can be shown similar to uncorrelated (correlation coefficient $\to 0$) Nakagami-m fading channel in [26].

B. PNSMC ANALYSIS

The PNSMC can be expressed as

$$\Pr(\mathcal{C}_{s,m} > 0) = \int_0^\infty \int_0^{\lambda_b^*} f_{\lambda_{min}}(\lambda_b^*) f_{\lambda_{max}}(\lambda_c^*) d\lambda_c^* d\lambda_b^*. \tag{45}$$

Substituting (35) and (41) into (45), $\Pr(\mathcal{C}_{s,m} > 0)$ can be easily derived. But PNSMC can also be derived from the SOPM expression as the following.

$$\Pr(\mathcal{C}_{s,m} > 0) = 1 - P_{out}(\xi_s)|_{\xi_s=0}. \tag{46}$$

Hence we first substitute $P_{out}(\xi_s)$ from (44) into (46), then set $\xi_s = 0$, and finally obtain the expression of PNSMC.

C. ESMC ANALYSIS

The ESMC can be defined as

$$\begin{aligned} \langle \mathcal{C}_{s,m} \rangle = &\int_0^\infty \log_2(1+\lambda_b^*) f_{\lambda_{min}}(\lambda_b^*) d\lambda_b^* \\ &- \int_0^\infty \log_2(1+\lambda_c^*) f_{\lambda_{max}}(\lambda_c^*) d\lambda_c^*. \end{aligned} \tag{47}$$

Replacing (35) and (41) into (47) and integrating by making use of [41, eq. 4.222.8], the novel expression for the ESMC is exhibited in (48), as shown at the top of the next page, where $D_1 = \mathcal{J}_3 - d_2$, $D_2 = \mathcal{J}_4 - d_4$, $D_3 = \mathcal{J}_8 - d_6$, $D_4 = \mathcal{J}_9 - d_8$, $D_5 = \frac{\mathcal{J}_1 \mathcal{J}_3!}{D_1! \mathcal{J}_5^{\mathcal{J}_3+1}}$, $D_6 = \frac{\mathcal{J}_2 \mathcal{J}_4!}{D_2! \mathcal{J}_5^{\mathcal{J}_4+1}}$, $D_7 = \frac{\mathcal{J}_6 \mathcal{J}_8!}{D_3! \mathcal{J}_{10}^{\mathcal{J}_8+1}}$, and $D_8 = \frac{\mathcal{J}_7 \mathcal{J}_9!}{D_4! \mathcal{J}_{10}^{\mathcal{J}_9+1}}$.

$$\begin{aligned} P_{out}(\xi_s) = 1 - &\sum_{e_8=0}^{Q-1} \sum_{e_9=0}^{P+Pe_8-1} \sum_{\varpi_{e_9}} \sum_{e_{14}=0}^{PW-1} \sum_{\varpi_{e_{14}}} \Bigg[\sum_{s_2=0}^{\infty} \sum_{e_4=0}^{\infty} \sum_{e_{10}=0}^{G_Q\mu_b+e_4-1} \sum_{f_2=0}^{\mathcal{J}_3} \sum_{f_4=0}^{f_2} \Bigg[\sum_{s_4=0}^{\infty} \sum_{e_6=0}^{\infty} \sum_{e_{15}=0}^{G_W\mu_c+e_6-1} \frac{\mathcal{J}_6 \omega_5 (\mathcal{J}_8 + f_4)!}{(\mathcal{J}_{10} + \mathcal{J}_5 q_{\psi_s})^{\mathcal{J}_8+f_4+1}} \\ &+ \sum_{s_5=0}^{\infty} \sum_{e_7=0}^{\infty} \sum_{e_{16}=0}^{\mu_a+s_5-1} \frac{\mathcal{J}_7 \omega_5 (\mathcal{J}_9 + f_4)!}{(\mathcal{J}_{10} + \mathcal{J}_5 q_{\psi_s})^{\mathcal{J}_9+f_4+1}} \Bigg] - \sum_{s_3=0}^{\infty} \sum_{e_5=0}^{\infty} \sum_{e_{11}=0}^{\mu_a+s_3-1} \sum_{f_3=0}^{\mathcal{J}_4} \sum_{f_5=0}^{f_3} \Bigg[\sum_{s_4=0}^{\infty} \sum_{e_6=0}^{\infty} \sum_{e_{15}=0}^{G_W\mu_c+e_6-1} \\ &\times \frac{\mathcal{J}_6 \omega_6 (\mathcal{J}_8 + f_5)!}{(\mathcal{J}_{10} + \mathcal{J}_5 q_{\psi_s})^{\mathcal{J}_8+f_5+1}} + \sum_{s_5=0}^{\infty} \sum_{e_7=0}^{\infty} \sum_{e_{16}=0}^{\mu_a+s_5-1} \frac{\mathcal{J}_7 \omega_6 (\mathcal{J}_9 + f_5)!}{(\mathcal{J}_{10} + \mathcal{J}_5 q_{\psi_s})^{\mathcal{J}_9+f_5+1}} \Bigg]\Bigg]. \end{aligned} \tag{44}$$

$$\begin{aligned}\langle \mathcal{C}_{s,m}\rangle = &\sum_{e_8=0}^{Q-1}\sum_{e_9=0}^{P+Pe_8-1}\sum_{\varpi_{e_9}}\Bigg[\sum_{s_2=0}^{\infty}\sum_{e_4=0}^{\infty}\sum_{e_{10}=0}^{G_Q\mu_b+e_4-1}\Bigg[\sum_{d_2=0}^{\mathcal{J}_3}\frac{D_5}{ln(2)}\frac{(-1)^{D_1-1}Ei(-\mathcal{J}_5)}{(\frac{1}{\mathcal{J}_5})^{D_1}e^{-\mathcal{J}_5}}+\sum_{d_3=1}^{D_1}\frac{(d_3-1)!}{(-\frac{1}{\mathcal{J}_5})^{D_1-d_3}}\Bigg]\\ &+\sum_{s_3=0}^{\infty}\sum_{e_5=0}^{\infty}\sum_{e_{11}=0}^{\mu_a+s_3-1}\Bigg[\sum_{d_4=0}^{\mathcal{J}_4}\frac{D_6}{ln(2)}\frac{(-1)^{D_2-1}Ei(-\mathcal{J}_5)}{(\frac{1}{\mathcal{J}_5})^{D_2}e^{-\mathcal{J}_5}}+\sum_{d_5=1}^{D_2}\frac{(d_5-1)!}{(-\frac{1}{\mathcal{J}_5})^{D_2-d_5}}\Bigg]\Bigg]\\ &-\sum_{e_{14}=0}^{PW-1}\sum_{\varpi_{e_{14}}}\Bigg[\sum_{s_4=0}^{\infty}\sum_{e_6=0}^{\infty}\sum_{e_{15}=0}^{G_W\mu_c+e_6-1}\Bigg[\sum_{d_6=0}^{\mathcal{J}_8}\frac{D_7}{ln(2)}\frac{(-1)^{D_3-1}Ei(-\mathcal{J}_{10})}{(\frac{1}{\mathcal{J}_{10}})^{D_3}e^{-\mathcal{J}_{10}}}+\sum_{d_7=1}^{D_3}\frac{(d_7-1)!}{(-\frac{1}{\mathcal{J}_{10}})^{D_3-d_7}}\Bigg]\\ &-\sum_{s_5=0}^{\infty}\sum_{e_7=0}^{\infty}\sum_{e_{16}=0}^{\mu_a+s_5-1}\Bigg[\sum_{d_8=0}^{\mathcal{J}_9}\frac{D_8}{ln(2)}\frac{(-1)^{D_4-1}Ei(-\mathcal{J}_{10})}{(\frac{1}{\mathcal{J}_{10}})^{D_4}e^{-\mathcal{J}_{10}}}+\sum_{d_9=1}^{D_4}\frac{(d_9-1)!}{(-\frac{1}{\mathcal{J}_{10}})^{D_4-d_9}}\Bigg]\Bigg].\end{aligned} \quad (48)$$

1) SIGNIFICANCE OF ESMC EXPRESSION

It is clear that how do the physical properties of the channels as well as the system parameters affects the secrecy capacity, can be easily quantified with (48). Besides, how does the cooperative diversity provided by the relays help to enhance secrecy capacity in spite of harsh channel conditions can also be evaluated easily. Since (48) is a generalized expression, it also represents secrecy analysis over several classical models. It is noted that, as a special case of Shadowed Rician fading distribution with ($P = 0$, $Q = W = 1$ $\kappa_b = \kappa_c = \kappa_a = K$, $\mu_b = \mu_c = \mu_a = 1$ and $m_b = m_c = m_a \rightarrow m$), our obtained results with (48) are equivalent with the analysis in [46, eq. 51]. In parallel, utilizing (48), another special scenario i.e. Shadowed Rician fading distribution for satellite links and Rayleigh fading distribution ($Q = W = 1$, $\kappa_b = \kappa_c = \kappa_a = 0$, $\mu_b = \mu_c = \mu_a = 1$ and $m_b = m_c = m_a \rightarrow \infty$) for terrestrial links can be shown as a special case of our model [47].

IV. NUMERICAL RESULTS

In this section, the numerical results concerning the expressions of SOPM, PNSMC, and ESMC as given in (44), (46), and (48), respectively are demonstrated graphically in order to gain some useful insights regarding the enhancement of security by taking the advantages of the physical properties of the propagation medium. Since the infinite series converges rapidly after a few terms, we take the first 25 terms to obtain the numerical results. Additionally, the validity of the analytical expressions as described in the previous sections are justified by Monte-Carlo (MC) simulations.[1] In each figure, we observe a close agreement between the analytical and simulation results which clearly justifies the validity of our analysis.

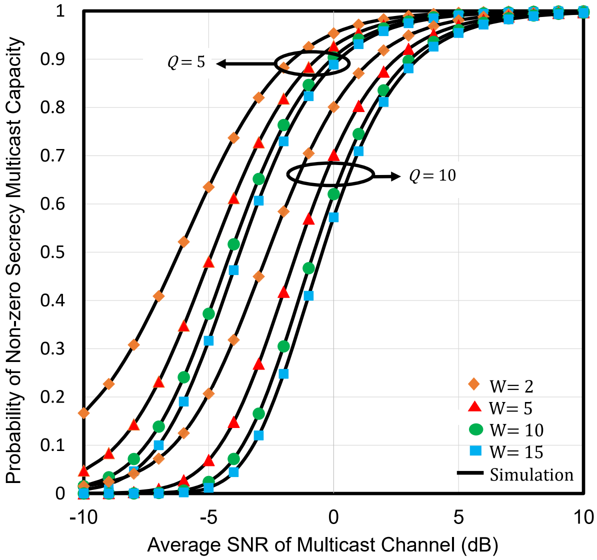


FIGURE 2. **The PNSMC versus $\bar{\lambda}_{ab}$ for selected values of Q and W when $\bar{\lambda}_{ac} = -10dB$,$G_Q = G_W = 2$,$\mu_a = \mu_b = \mu_c = 2$,$\kappa_a = \kappa_b = \kappa_c = 2$, and $m_a = m_b = m_c = \infty$.**

Figure 2 presents the PNSMC against $\bar{\lambda}_{ab}$ in which the impact of the multicast receivers (Q) and eavesdroppers (W) are illustrated. We assume two scenarios considering $Q =$ 5 and 10. Both the scenarios clearly dictate that the PNSMC decreases with increasing values of Q, and W. In the multicast scenario, due to the increase in Q, the bandwidth per user is reduced which causes a reduction in the received SNR at the user node. Hence the PNSMC performance degrades remarkably which is testified in [26]. On the contrary, increasing W escalates the strength of the eavesdroppers by ensuring the maximum SNR at the eavesdropper node (since increasing W indicates an increasing probability of obtaining maximum SNR at the eavesdropper channel) and thus PNSMC is degraded. It is also observed from Fig. 2 that the MC and analytical simulation are in a good agreement, which clearly indicates the exactness of our PNSMC expression in (46).

In Fig. 3, the PNSMC is plotted against $\bar{\lambda}_{ab}$ in which the effect of different number of clusters of relay channel (μ_a), multicast channels (μ_b) as well as eavesdropper channel (μ_c) are shown. It is observed from the figure that the increment in the number of clusters of relay (μ_a) and multicast channels

[1] To accomplish this task, we generate $\kappa - \mu$ shadowed random variables in MATLAB and 10^6 realizations of the channels are averaged to calculate each value of the secrecy parameters. The analytical results are shown using markers and corresponding simulation results are shown using solid lines.

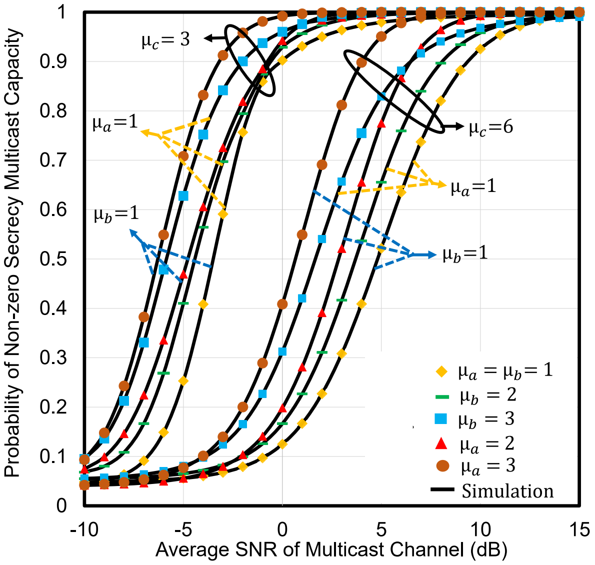


FIGURE 3. The PNSMC versus $\bar{\lambda}_{ab}$ for selected values of μ_b, μ_a, and μ_c when $m_a = m_b = m_c = \infty$, $\kappa_a = \kappa_b = \kappa_c = 1$, and $\bar{\lambda}_{ac} = 0dB$.

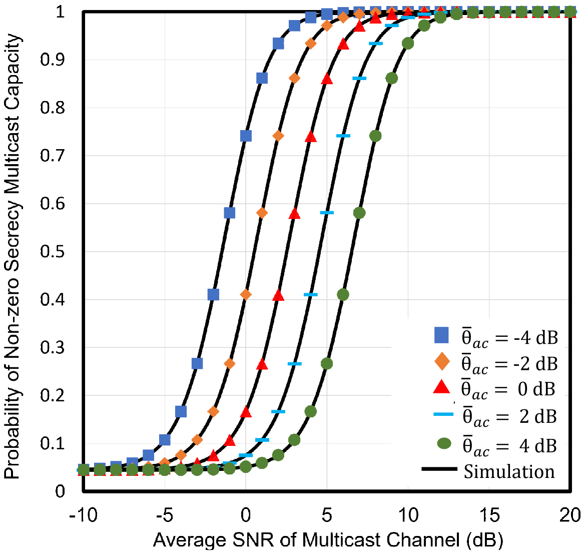


FIGURE 4. The PNSMC versus $\bar{\lambda}_{ab}$ for selected values of $\bar{\lambda}_{ac}$ when $G_Q = G_W = 2$, $\mu_a = \mu_b = \mu_c = 2$, $\kappa_a = \kappa_b = \kappa_c = 1$, and $m_a = m_b = m_c = \infty$.

(μ_b) enhances the PNSMC of the proposed model. Because, with increasing values of μ_a and μ_b, we are increasing the end-to-end SNR indirectly by including more incoming signals based on various diversity schemes. As a result, the total fading of the multicast channels reduces which ensures the increment of the PNSMC. Due to this similar reason, the PNSMC of the system degrades with μ_c. It is noteworthy that the impact of μ_a upgrading the secrecy performance is much superior than that of μ_b. The outcomes from [25] and [48] exhibits the same characteristics which validate our result convincingly.

The MC simulation and analytical results of PNSMC as a function of $\bar{\lambda}_{ab}$ is shown in Fig. 4, where the outcomes due to the variation in average SNR of the eavesdropper channel ($\bar{\lambda}_{ac}$) are depicted. It is noted that the PNSMC is degraded with the increase of $\bar{\lambda}_{ac}$ because an increase in $\bar{\lambda}_{ac}$ indicates a higher SNR at the eavesdropper terminals which enhances the strength of the wiretap channels in terms of secrecy performance as shown in [49].

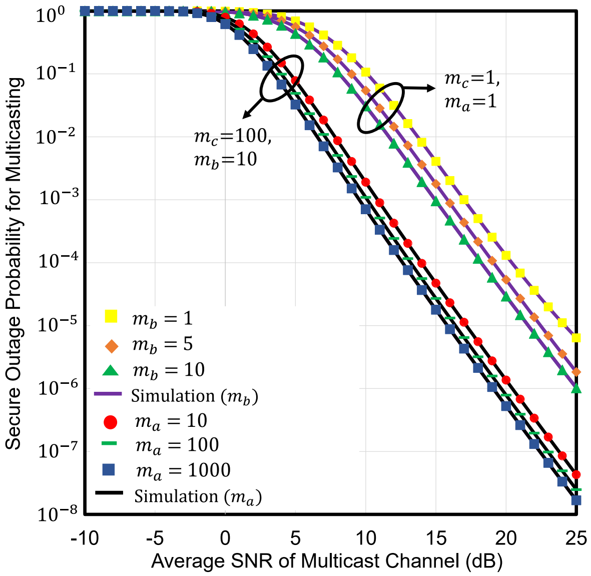


FIGURE 5. The SOPM versus $\bar{\lambda}_{ab}$ for selected values of m_b, m_a, and m_c when $\bar{\lambda}_{ac} = -5dB$, $G_Q = G_W = 2$, $\mu_a = \mu_b = \mu_c = 1$, and $\kappa_a = \kappa_b = \kappa_c = 1$.

Figure 5 demonstrates the SOPM as a function of $\bar{\lambda}_{ab}$, where the consequences of variation in the shadowing parameter for multicast channels (m_b) and relay channel (m_a) are represented. From the figure, it is recognized that increment in m_b and m_a minimize the shadowing effect of the multicast channel, and thus the SOPM of the model decrease. So superior secrecy performance can be achieved if the shadowing present in the multicast network is comparatively lower. Our numerical result is also confirmed by MC simulation. A similar conclusion (related to shadowing) was also drawn in [25].

Figure 6 depicts SOPM versus $\bar{\lambda}_{ab}$ to represent the effect of target secrecy rate (ξ_s) on the secure outage performance. We consider two cases herein with $\bar{\lambda}_{ac} = 0$ and -10 dB. It is noted that the SOPM increases with ξ_s for both cases of $\bar{\lambda}_{ac}$ as shown in [17]. It is also noticeable that the impact of ξ_s in case of $\bar{\lambda}_{ac} = -10$ dB is more significant than that of $\bar{\lambda}_{ac} = 0$ dB. Moreover, the SOPM performance improves when the eavesdropper channel becomes worse (i.e. $\bar{\lambda}_{ac} = -10$ dB). A good agreement between MC and analytical outcomes proves that the SOPM derived in (44) is accurate.

In Fig. 7, the SOPM is varied against $\bar{\lambda}_{ab}$ to illustrate the consequences of differing the number of relays (P). From the figure, it can be seen that an increment in P offers a remarkable improvements in system's SOPM performance. As the number of relays are increased, the P relays compete among themselves to be the best one. Additionally, the cooperative diversity provided by multiple relays also play a notable role

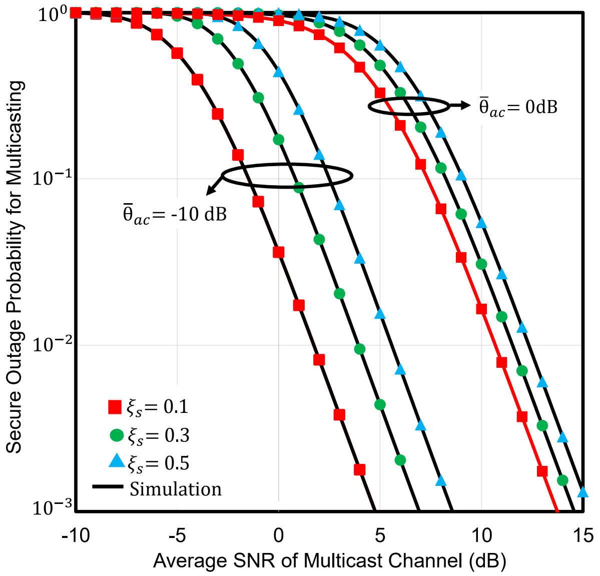


FIGURE 6. The SOPM versus $\bar{\lambda}_{ab}$ for selected values of ξ_S and $\bar{\lambda}_{ac}$.

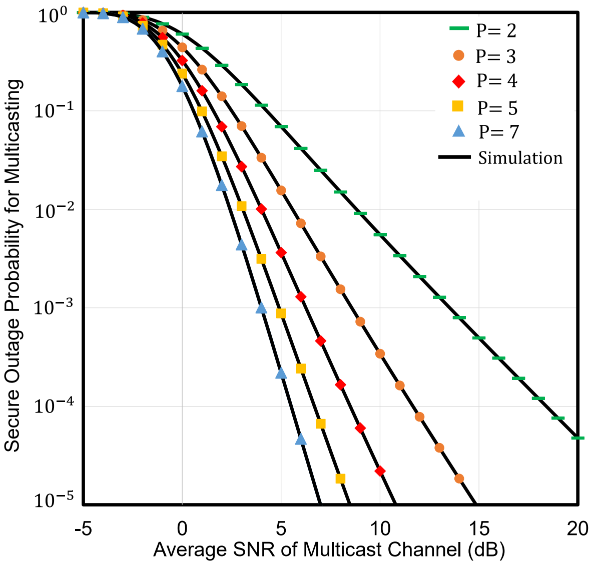


FIGURE 7. The SOPM versus $\bar{\lambda}_{ab}$ for selected values of P when $\bar{\lambda}_{ac} = -10dB$, $G_Q = G_W = 2$, $\mu_a = \mu_b = \mu_c = 1$, $\kappa_a = \kappa_b = \kappa_c = 1$, and $m_a = m_b = m_c = \infty$.

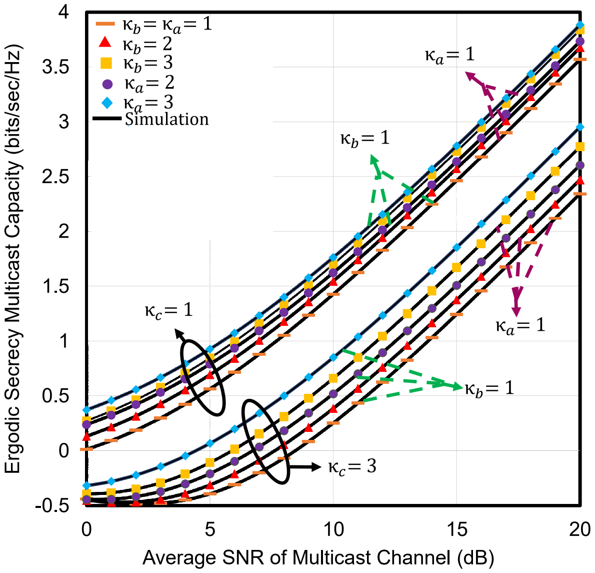


FIGURE 8. The ESMC versus $\bar{\lambda}_{ab}$ for selected values of κ_b, κ_a, and κ_c when $\mu_a = \mu_b = \mu_c = 1$, $m_a = m_b = m_c = \infty$ and $\bar{\lambda}_{ac} = -5dB$.

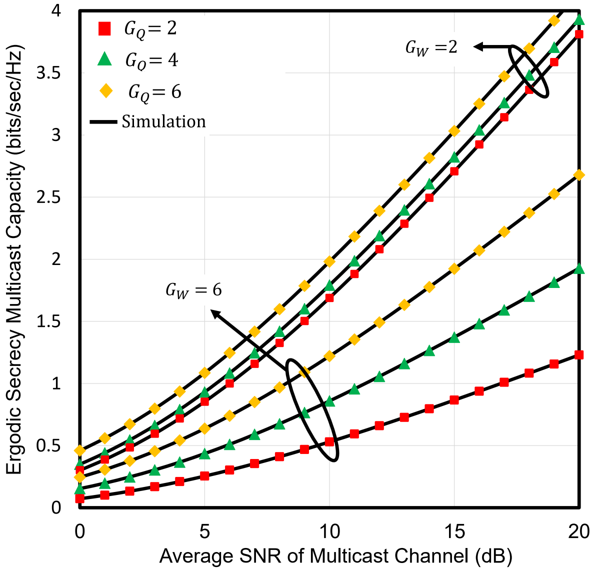


FIGURE 9. The ESMC versus $\bar{\lambda}_{ab}$ for selected values of G_Q and G_W when $\bar{\lambda}_{ac} = -10dB$, $\kappa_a = \kappa_b = \kappa_c = 1$, $\mu_a = \mu_b = \mu_c = 1$, and $m_a = m_b = m_c = \infty$.

in reducing the impacts of fading and shadowing of multicast links.

Figure. 8 represents ESMC with respect to $\bar{\lambda}_{ab}$ for different values of κ_a, κ_b and κ_c. It is evident from the figure that both κ_a and κ_b increases the secrecy capacity of the proposed system. The increment of κ_a and κ_b enhances the dominant component as well as reduces the scattering component of the multicast channel which results in higher SNR at the receiver and ESMC of the proposed model. But, the capacity degrades sharply with κ_c as it upgrades the SNR of the eavesdropper channel. Same results were obtained in [25], and [48] which undoubtedly confirms our analysis. The MC simulation also has a tight agreement with the analytical result.

In Fig. 9, ESMC is plotted against $\bar{\lambda}_{ab}$ with a view to observing the impacts due to the variation in number of antennas of each user (G_Q) and eavesdropper (G_W). From the figure, it is observed that the ESMC escalates if G_Q increases. This is because an increase in G_Q significantly reduce the fading of multicast channels by enhancing the antenna diversity at the receiver. On the other hand, it is also noted that, ESMC degrades if G_W is increased. In that case, the eavesdroppers are capable of overhearing more confidential messages from the multicast channels due to increase in antenna diversity at the eavesdropper terminals. Even ESMC degrades dramatically when the eavesdroppers are equipped with large number of antennas (i.e. $G_W = 6$).

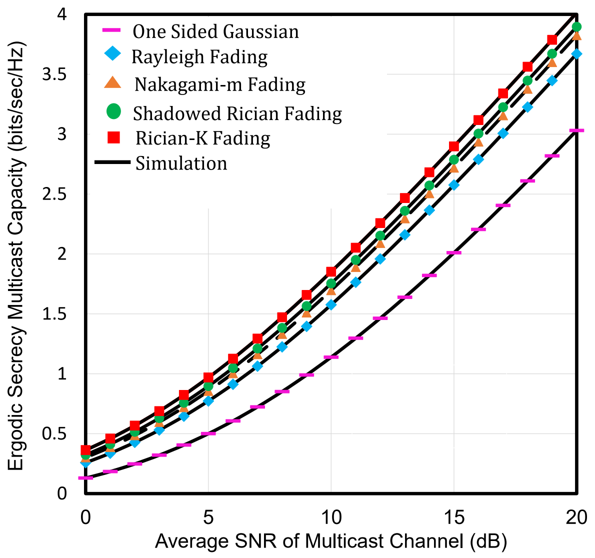


FIGURE 10. The ESMC versus $\bar{\lambda}_{ab}$ for comparing performance of different classical fading channels as a special cases of $\kappa-\mu$ shadowed fading channel when $\bar{\lambda}_{ac} = -10dB$, $G_Q = G_W = 2$, and $P = Q = W = 2$.

Similar outcomes are also presented in [39] which manifest the exactness of our results.

Figure 10 exhibits a graphical representation in which the generic characteristics of the proposed scenario is illustrated by plotting ESMC against $\bar{\lambda}_{ab}$. Note that the secrecy analysis over generalized shadowed model using opportunistic relaying is absent in the previous studies. Moreover, simply reorienting the system parameters, we can generate some existing models as special cases which is a clear indication of superiority of our proposed work. Hence, the conclusive remarks based on the aforementioned discussion is that this novel proposed work is more purposeful than all the conventional multipath/ shadowed secure models.

A. COMPARATIVE ANALYSIS WITH EXISTING RELATED LITERATURE

We consider generalized distribution (i.e. $\kappa-\mu$ shadowed fading) at $S \rightarrow P, P \rightarrow Q$, and $P \rightarrow W$ links in the proposed dual-hop scheme that encompasses a number of well-known fading distributions which can be acquired as special cases of our model as shown in Table 1. Hence, it is noteworthy that the derived expressions in (46), (44), and (48) regarding our proposed scenario are also generalized, and can be utilized to unify the secrecy performances of the mentioned channels in Table 1.

V. CONCLUSION

This paper considers PLS in the dual-hop secure wireless multicast relay networks over $\kappa-\mu$ shadow-fading channels with multiple eavesdroppers. Under this scenario, secrecy enhancement is ensured by choosing the best relay among multiple relays. The effect of all the system parameters on the secrecy performance of the proposed model is thoroughly observed by deriving the exact and analytical expressions of the performance metrics, i.e., PNSMC, SOPM, and ESMC. Also, these analytical results are numerically verified with Monte-Carlo simulations. Form such analyses, it is shown that the secrecy performance of this dual-hop relay communication model mostly affected by the channel environment of the first hop, i.e., source-to-relay link, than that of the second hops, i.e., relay-to-destination and relay-to-eavesdropper links. Shadowing is an important aspect of this study. The security of this proposed scenario can be improved by increasing the shadowing effect in relay-to-eavesdropper link. The proposed generalized shadowing model with opportunistic relay operation can also be employed to improve the security of different classical fading scenarios irrespective of the harsh channel conditions in the presence of a large number of multicast receivers and eavesdroppers. The proposed model can also be extended to non-terrestrial networks where shadowing is one of the major impairments.

REFERENCES

[1] N. Simmons, C. R. N. da Silva, S. L. Cotton, P. C. Sofotasios, and M. D. Yacoub, "Double shadowing the Rician fading model," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 344–347, Apr. 2019.

[2] N. Y. Ermolova and O. Tirkkonen, "Outage probability over composite η-μ fading–shadowing radio channels," *IET Commun.*, vol. 6, no. 13, pp. 1898–1902, Sep. 2012.

[3] J. Zhang, L. Dai, W. H. Gerstacker, and Z. Wang, "Effective capacity of communication systems over κ-μ shadowed fading channels," *Electron. Lett.*, vol. 51, no. 19, pp. 1540–1542, 2015.

[4] F. J. Lopez-Martinez, J. F. Paris, and J. M. Romero-Jerez, "The κ-μ shadowed fading model with integer fading parameters," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 7653–7662, 2017.

[5] S. K. Yoo, N. Bhargav, S. L. Cotton, P. C. Sofotasios, M. Matthaiou, M. Valkama, and G. K. Karagiannidis, "The κ-μ/inverse gamma and η-μ/inverse gamma composite fading models: Fundamental statistics and empirical validation," *IEEE Trans. Commun.*, vol. 69, no. 8, pp. 5514–5530, Aug. 2017.

[6] D. Pant, P. S. Chauhan, S. K. Soni, and S. Naithani, "Channel capacity analysis of wireless system under ORA scheme over $\kappa-\mu/$-inverse gamma and $\eta-\mu/$-inverse gamma composite fading models," in *Proc. Int. Conf. Electr. Electron. Eng.*, Mar. 2020, pp. 425–430.

[7] D. Pant, P. S. Chauhan, and S. K. Soni, "Error probability and channel capacity analysis of wireless system over inverse gamma shadowed fading channel with selection diversity," *Int. J. Commun. Syst.*, vol. 32, no. 16, p. e4083, Nov. 2019.

[8] P. Raghuwanshi and K. Kumar, "$\alpha-\eta-\mu$/IG composite fading model for body-centric communication," in *Advances in VLSI, Communication, and Signal Processing*. Singapore: Springer, 2021, pp. 263–269.

[9] Y. J. Chun, S. L. Cotton, H. S. Dhillon, F. J. Lopez-Martinez, J. F. Paris, and K. S. Yoo, "A comprehensive analysis of 5G heterogeneous cellular systems operating over κ-μ shadowed fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 6995–7010, Dec. 2017.

[10] H. Al-Hmood and H. S. Al-Raweshidy, "Analysis of energy detection with diversity receivers over non-identically distributed κ-μ shadowed fading channels," *Electron. Lett.*, vol. 53, no. 2, pp. 83–85, Jan. 2017.

[11] V. A. Aalo, P. S. Bithas, and G. P. Efthymoglou, "On the impact of user mobility on the performance of wireless receivers," *IEEE Access*, vol. 8, pp. 197300–197311, 2020.

[12] H. Al-Hmood and H. Al-Raweshidy, "Unified composite distribution with applications to double shadowed $\kappa-\mu$ fading channels," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 7182–7186, Jul. 2021.

[13] X. Li, J. Li, L. Li, J. Jin, J. Zhang, and D. Zhang, "Effective rate of MISO systems over κ-μ shadowed fading channels," *IEEE Access*, vol. 5, pp. 10605–10611, 2017.

[14] J. Zhang, X. Chen, K. P. Peppas, X. Li, and Y. Liu, "On high-order capacity statistics of spectrum aggregation systems over κ-μ and κ-μ shadowed fading channels," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 935–944, Dec. 2016.

[15] S. K. Yoo, S. L. Cotton, P. C. Sofotasios, and S. Freear, "Shadowed fading in indoor off-body communication channels: A statistical characterization using the κ-μ/gamma composite fading model," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5231–5244, Mar. 2016.

[16] A. Subhash, M. Srinivasan, and S. Kalyani, "Asymptotic maximum order statistic for SIR in κ-μ shadowed fading," *IEEE Trans. Commun.*, vol. 67, no. 9, pp. 6512–6526, Jun. 2019.

[17] A. Badrudduza, S. Islam, M. Kundu, and I. Ansari, "Secrecy performance of $\alpha-\kappa-\mu$ shadowed fading channel," *ICT Exp.*, Oct. 2021.

[18] L. Han and J. Mu, "Outage probability of opportunistic decode-and-forward relaying over correlated shadowed fading channels," *Wireless Pers. Commun.*, vol. 91, no. 1, pp. 453–462, Nov. 2016.

[19] J. Zhang and G. Pan, "Secrecy outage analysis with *Kth* best relay selection in dual-hop inter-vehicle communication systems," *AEU-Int. J. Electron. Commun.*, vol. 71, pp. 139–144, Jan. 2017.

[20] J. Vegasanchez, D. P. M. Osorio, F. J. Lopez-Martinez, M. C. P. Paredes, and L. Urquiza-Aguiar, "Information-theoretic security of MIMO networks under-shadowed fading channels," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 6302–6318, Jul. 2021.

[21] A. S. Sumona, M. K. Kundu, and A. Badrudduza, "Security analysis in multicasting over shadowed rician and $\alpha-\mu$ fading channels: A dual-hop hybrid satellite terrestrial relaying network," *arXiv preprint arXiv:2105.12071*, 2021.

[22] S. Jiang-Feng, L. Xing-Wang, D. Yuan, and D. Jian-He, "Physical layer security over SIMO κ-μ shadowed fading channels," *Recent Adv. Electr. Electron. Eng.*, vol. 13, no. 6, pp. 871–878, 2020.

[23] M. Nunes and U. S. Dias, "On the physical layer security under κ-μ shadowed fading channels with diversity approaches," in *Proc. Symp. Telecommun. Process. Sig. (BSTPS)*, 2017, pp. 373–377.

[24] Y. Ai, L. Kong, and M. Cheffena, "Secrecy outage analysis of double shadowed rician channels," *Electron. Lett.*, vol. 55, no. 13, pp. 765–767, Jun. 2019.

[25] J. Sun, H. Bie, X. Li, J. Zhang, G. Pan, and K. M. Rabie, "Secrecy performance analysis of SIMO systems over correlated κ-μ shadowed fading channels," *IEEE Access*, vol. 7, pp. 86090–86101, 2019.

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

[27] A. Kalantari, M. Mohammadi, and M. Ardebilipour, "Performance analysis of opportunistic relaying over imperfect non-identical log-normal fading channels," in *Proc. IEEE 22nd Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2011, pp. 1909–1913.

[28] H. Yu and G. L. Stuber, "General decode-and-forward cooperative relaying with co-channel interference in shadowed Nakagami fading channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4318–4327, Dec. 2012.

[29] Y. Feng, V. C. M. Leung, and F. Ji, "Performance study for SWIPT cooperative communication systems in shadowed Nakagami fading channels," *IEEE Trans. Wireless Commun.*, vol. 17, no. 2, pp. 1199–1211, Feb. 2018.

[30] A. Iqbal and K. M. Ahmed, "Integrated satellite-terrestrial system capacity over mix shadowed Rician and Nakagami channels," *Int. J. Commun. Netw. Inf. Secur.*, vol. 5, no. 2, pp. 104–109, 2013.

[31] L. Fan, R. Zhao, F.-K. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, Jul. 2017.

[32] J. Zhang, X. Li, I. S. Ansari, Y. Liu, and K. A. Qaraqe, "Performance analysis of dual-hop DF satellite relaying over κ-μ shadowed fading channels," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.

[33] M. Arti, "Beamforming and combining based scheme over κ-μ shadowed fading satellite channels," *IET Commun.*, vol. 10, no. 15, pp. 2001–2009, 2016.

[34] Y. Zou, J. Zhu, X. Li, and L. Hanzo, "Relay selection for wireless communications against eavesdropping: A security-reliability trade-off perspective," *IEEE Netw.*, vol. 30, no. 9, pp. 74–79, Sep. 2016.

[35] A. S. M. Badrudduza and M. K. Kundu, "Enhancing security in wireless multicasting over $\kappa-\mu$ fading channel," in *Proc. 22nd Int. Conf. Comput. Inf. Technol. (ICCIT)*, Dec. 2019, pp. 1–5.

[36] A. P. Shrestha, J. Jung, and K. S. Kwak, "Secure wireless multicasting in presence of multiple eavesdroppers," in *Proc. 13rd Int. Symp. Commun. Inf. Technol. (ISCIT)*, 2013, pp. 814–817.

[37] X. Wang, M. Tao, and Y. Xu, "Outage analysis of cooperative secrecy multicast transmission," *IEEE Wireless Commun. Lett.*, vol. 3, no. 2, pp. 161–164, Apr. 2014.

[38] J. F. Paris, "Statistical characterization of κ-μ shadowed fading," *IEEE Trans. Veh. Technol.*, vol. 63, no. 2, pp. 518–526, Mar. 2013.

[39] M. Srinivasan and S. Kalyani, "Secrecy capacity of κ-μ shadowed fading channels," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1728–1731, 2018.

[40] 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, Oct. 2017.

[41] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

[42] A. S. M. Nafis, A. S. M. Badrudduza, Z. I. Borshon, M. K. Kundu, and M. Z. I. Sarkar, "Secrecy trade-off at the physical layer over mixed fading multicast channels employing antenna diversity," *Wireless Pers. Commun.*, vol. 15, pp. 1–18, Sep. 2021.

[43] J. P. Pena-Martin, J. M. Romero-Jerez, and C. Tellez-Labao, "Performance of selection combining diversity in η-μ fading channels with integer values of μ," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 834–839, 2014.

[44] A. S. M. Badrudduza, M. Z. I. Sarkar, M. K. Kundu, and D. K. Sarker, "Performance analysis of multicasting over Rician-K fading channels: A secrecy tradeoff," in *Proc. Int. Conf. Comput., Commun., Chem., Mater. Electron. Eng.*, Jul. 2019, pp. 1–4.

[45] V. Bankey and P. K. Upadhyay, "Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2488–2501, Mar. 2019.

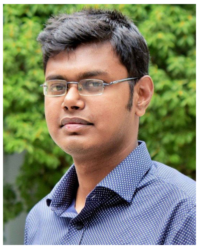
[46] K. An, T. Liang, X. Yan, and G. Zheng, "On the secrecy performance of land mobile satellite communication systems," *IEEE Access*, vol. 6, pp. 39606–39620, 2018.

[47] K. Guo, K. An, B. Zhang, Y. Huang, and D. Guo, "Physical layer security for hybrid satellite terrestrial relay networks with joint relay selection and user scheduling," *IEEE Access*, vol. 6, pp. 55815–55827, 2018.

[48] J. Sun, X. Li, Y. Ding, and J. Du, "On physical layer security over SIMO κ-μ shadowed fading channels," *Recent Adv. Electr. Electron. Eng.*, vol. 13, no. 6, pp. 871–878(8), Nov. 2020.

[49] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy capacity analysis over κ-μ fading channels: Theory and applications," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3011–3024, Jul. 2016.

S. M. SAUMIK SHAHRIYER received the Bachelor of Science (B.Sc.) degree in electronics and telecommunication engineering (ETE) from the Rajshahi University of Engineering and Technology (RUET), Rajshahi, Bangladesh, in March 2021. His research interests include information theoretic physical layer security in multicast, cellular, and wireless networks. He has received one Best Paper Award in IEEE 3rd International Conference on Telecommunication and Photonics (ICTP 2019).



A. S. M. BADRUDDUZA (Member, IEEE) received the Bachelor of Science (B.Sc.) and Master of Science (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 September 2016 to July 2017, he was a Lecturer with the Department of EEE, Bangladesh Army University of Engineering and Technology (BAUET), Natore, Rajshahi. From July 2017 to June 2020, he was a Lecturer with the Department of Electronics and Telecommunication Engineering (ETE), RUET. Since June 2020, he has been working as an Assistant Professor with the Department of ETE, RUET. He has authored/coauthored more than 40 international journals/conference publications. His research interests include physical layer security in multicast, cellular and cooperative networks, free space optics (FSO), underwater optics (UWO), and NOMA systems.

Mr. Badrudduza has been affiliated with IEEE and is an active reviewer for several IEEE journals, since 2020. He 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 two Best Paper Awards for two different research articles from IEEE Region 10 Symposium (TENSYMP2020), and IEEE 3rd International Conference on Telecommunication and Photonics (ICTP2019).

SARJANA SHABAB (Member, IEEE) received the Bachelor of Science degree in electrical and electronic engineering (EEE) from the Rajshahi University of Engineering and Technology (RUET), in September 2019, where she is currently pursuing the master's degree with the Department of EEE.

From November 2019 to February 2021, she worked as a Lecturer with the Department of EEE, North Bengal International University (NBIU), Rajshahi. Since February 2021, she has been working as a Lecturer with the Department of EEE, RUET. Her research interests include underwater optics and modeling secured communication in cellular, multicasting, and cooperative networks.

Ms. Shabab has received one Best Paper Award in IEEE 3rd International Conference on Telecommunication and Photonics (ICTP 2019).

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), Kajla, Rajshahi, Bangladesh, in 2016.

From May 2017 to February 2019, he worked as a Lecturer with the Department of EEE, North Bengal International University, Rajshahi, and also performed his duty as a Lecturer with the Department of Electrical and Computer Engineering (ECE), RUET, from February 2019 to May 2021. Since May 2021, he has been working as an Assistant Professor with the Department of ECE, RUET. He is currently an Advisor of IEEE RUET Industry Applications Society (IAS) Student Branch Chapter. His research interests include security aspects of cooperative and physical-layer networks and wireless communication (both RF and optical).

Mr. Kundu has received 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, two Best Paper Awards for two different research articles from IEEE Region 10 Symposium (TENSYMP 2020), and IEEE 3rd International Conference on Telecommunication and Photonics (ICTP 2019).

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 (KAIST), Daejeon, South Korea, in 2001 and 2011, respectively. From 2001 to 2012, he was with the Electronics and Telecommunications Research Institute (ETRI), Daejeon. From 2012 to 2019, he was with Yeungman University, South Korea. He is currently an Associate Professor with the Department of Electronics and Information Engineering, Korea University, Sejong, South Korea. His research interests include statistical signal processing and communication theory.