future internet

MDPI

Article

Cascaded κ-μ Fading Channels with Colluding and Non-Colluding Eavesdroppers: Physical-Layer Security Analysis

Deemah Tashman *,† **and Walaa Hamouda** †

Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H3G 1M8, Canada; hamouda@ece.concordia.ca

* Correspondence: d_tashma@ece.concordia.ca

† Both authors contributed equally to this work.

Abstract: In this paper, the physical-layer security for a three-node wiretap system model is studied. Under the threat of multiple eavesdroppers, it is presumed that a transmitter is communicating with a legitimate receiver. The channels are assumed to be following cascaded κ-μ fading distributions. In addition, two scenarios for eavesdroppers' interception and information-processing capabilities are investigated: colluding and non-colluding eavesdroppers. The positions of these eavesdroppers are assumed to be random in the non-colluding eavesdropping scenario, based on a homogeneous Poisson point process (HPPP). The security is examined in terms of the secrecy outage probability, the probability of non-zero secrecy capacity, and the intercept probability. The exact and asymptotic expressions for the secrecy outage probability and the probability of non-zero secrecy capacity are derived. The results demonstrate the effect of the cascade level on security. Additionally, the results indicate that as the number of eavesdroppers rises, the privacy of signals exchanged between legitimate ends deteriorates. Furthermore, in this paper, regarding the capabilities of tapping and processing the information, we provide a comparison between colluding and non-colluding eavesdropping.

Keywords: cascaded general fading channels; physical-layer security; probability of non-zero secrecy capacity; secrecy outage probability

Citation: Tashman, D.; Hamouda, W. Cascaded κ-μ Fading Channels with Colluding and Non-Colluding Eavesdroppers: Physical-Layer Security Analysis. *Future Internet* **2021**, *13*, 205. https://doi.org/10.3390/fi13080205

Academic Editors: Khalid Elgazzar, Aboelmagd Noureldin, Mohamed El-Tarhuni and Mohamed Hassan

Received: 29 June 2021
Accepted: 31 July 2021
Published: 4 August 2021

1. Introduction

This work is an extension for a previous paper that has been presented in 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA) [1]. Security is one of the fundamental challenges that must be addressed in all types of networks, particularly with the tremendous number of connections and services planned in 5G and beyond. In this context, physical-layer security (PLS) has emerged as a critical and reliable approach to effectively addressing the security concern [2,3]. PLS does not depend on the exchange of security keys between authorized endpoints since there is no necessity for decryption and encryption operations, as in higher-layer security techniques [4,5]. As a result, PLS is more suitable for use in 5G networks and beyond. That is, there is no additional complexity introduced to the current complicated networks. Shannon was the first to propose the notion of PLS [6], which was then expanded upon by Wyner [7]. The PLS notion claimed that the confidentiality of private information is assured when the main channel (the link between the transmitter and the legitimate receiver) is more reliable than the wiretap channel (the one between the transmitter and the eavesdropper) [8].

κ-μ fading model is one of the general fading distributions, which have been confirmed by field measurement campaigns to better suit the experimental data compared to other known distributions, such as Rayleigh, Rician, and Nakagami-m fading [9]. κ-μ distribution

suits the line-of-sight (LOS) applications with the two physical parameters; κ and μ. $\kappa > 0$ is recognized as the ratio between the total power of the dominant components and the power of the scattered waves, while $\mu > 0$ demonstrates the number of the multipath clusters. κ-μ fading channel includes some of the well-known channels as special cases, which is a reason for its flexibility property, such as Rician ($\mu = 1$ and κ = LOS component in the Rician channel), Rayleigh ($\kappa = 0, \mu = 1$), Nakagami-m ($\kappa = 0, \mu = m$), and the one-sided Gaussian ($\kappa = 0, \mu = 0.5$) distributions [9].

Recently, various forms of networks have been investigated under the premise of cascaded channels rather than single regular channels. These channels presume that the entities in the networks are moving or that they reside in dense scattering regions [10]. The principle of cascaded channels suggests that the signal that leaves the transmitter does not travel directly to the receiver without encountering objects and obstacles along the way. In addition, the received signal is composed of the multiplication of multiple rays reflected from the objects obstructing the path [11]. Cascaded channels have a variety of applications, which has made them intriguing for recent research in signal propagation modeling. These applications include mobile-to-mobile/vehicle-to-vehicle communications (M2M/V2V) [12], the multi-hop relaying systems, and the keyhole channels in multiple-input–multiple-output (MIMO) system models [13,14].

Physical-layer security performance over cascaded fading channels has recently been thoroughly investigated. PLS was studied for a system model consisting of a transmitter, a receiver, and one eavesdropper in terms of the secrecy outage probability (SOP) and the strictly positive secrecy capacity (SPSC) over double Rayleigh fading channel in [15] and over double Nakagami-m fading channel in [16]. Similar analyses were performed in [17] over cascaded $\alpha - \mu$ fading channel and in [12,18] over cascaded Nakagami-m fading channel. In [18], the secrecy performance was explored for two scenarios of one eavesdropper and two eavesdroppers. Secrecy was investigated over cascaded Fisher-Snedecor $\mathcal{F}$ fading channels using stochastic geometry in [19] in the presence of randomly distributed eavesdroppers. Intercept probability is evaluated in this model, where two different cases are considered, which are the k^{th} nearest and k^{th} best eavesdropper. PLS was studied over cascaded κ-μ fading channels over the main link only in [20].

To the best of the authors' knowledge, no prior works studied the physical-layer security (PLS) for a three-node wiretap system model over cascaded κ-μ fading channels at the main and the wiretap links and under the threat of multiple eavesdroppers. Moreover, no previous research has investigated the difference between colluding and non-colluding eavesdroppers with multiple antennas. Therefore, in this work, we explore the PLS of a system model consisting of a transmitter interacting with a legitimate receiver in the presence of multiple eavesdroppers. In one scenario, these eavesdroppers are considered to be colluding to intercept the information effectively, whereas in another, the eavesdroppers are considered to be non-colluding and have random positions. In the case of colluding eavesdroppers, it is assumed that each has a single antenna. These eavesdroppers can be replaced by a single eavesdropper equipped with several antennas. This assumption is valid since these colluding eavesdroppers can perform cooperative processing on the gathered intercepted information by sending it to a centralized processor [21–25]. The PLS is investigated in terms of the secrecy outage probability (OP_{sec}), the probability of non-zero secrecy capacity (P_{nsc}), and the intercept probability (P_{int}). Exact and asymptotic equations for the OP_{sec} and the P_{nsc} are derived. The results demonstrate the influence of multiple eavesdroppers on information privacy. Moreover, the impact of the cascade levels of the main and the wiretap channels over the security is addressed. This paper also investigates the effect of distances on security. Finally, a comparison between the two scenarios of the eavesdroppers' capabilities on degrading the main channel's privacy is provided.

2. Materials and Methods

2.1. Physical-Layer Security Analysis: Colluding Eavesdroppers

A three-node wiretap system model is shown in Figure 1. In the presence of an eavesdropper (E) equipped with several antennas, it is assumed that the transmitter (Alice) is communicating with a legitimate receiver (Bob) over the main channel. This eavesdropper replaces the multiple colluding eavesdroppers, each equipped with a single antenna [20,21,25]. Moreover, the eavesdropper utilizes the maximal ratio combining (MRC) technique over the received messages to improve the received signal-to-noise ratio (SNR). Through the wiretap channel, E is attempting to capture the messages conveyed between Alice and Bob. Both the main and wiretap channels follow the cascaded κ-μ fading model.

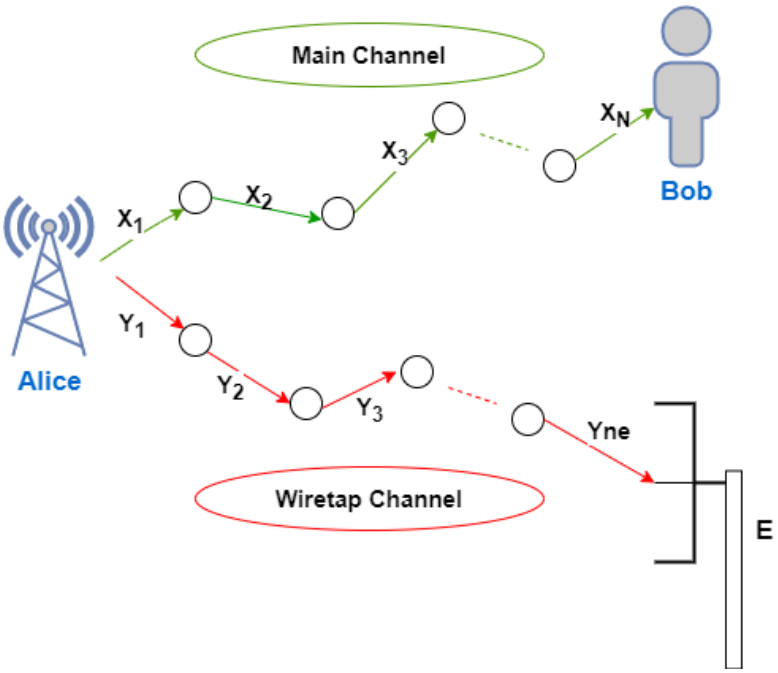

Figure 1. The system model.

The received signal at the legitimate receiver (Bob) is given by

$$y_m = \sqrt{P} Z_N x + w_m, \tag{1}$$

where P is the transmit power. x is the transmitted symbol at Alice and w_m is the additive white Gaussian noise (AWGN) at the receiver with zero mean and variance N_0. Z_N is the channel gain for the main link, which is defined by $Z_N = \prod_{i=1}^{N} X_i$. X_i is a set of independent κ-μ random variables (RVs) with the parameters κ_i and μ_i $(i \in \{1, 2, \cdots, N\})$. Therefore, Z_N follows cascaded $\kappa - \mu$ fading with the following probability density function (PDF) [20]

$$f_{Z_N}(z) = \sum_{v_1=0}^{\infty} \sum_{v_2=0}^{\infty} \cdots \sum_{v_N=0}^{\infty} a_1 z^{2\mu_1 + 2v_1 - 1} G_{N\ 0}^{0\ N} \left(\begin{matrix} \epsilon \\ - \end{matrix} \middle| \frac{1}{z^2 \prod_{i=1}^{N} \mu_i (1+\kappa_i)} \right), \tag{2}$$

where $G_{p\ q}^{m\ n}\left(\begin{matrix} a_r \\ b_s \end{matrix} \middle| z \right)$ is the Meijer G-function defined in [26] (Equation 9-301), $\epsilon = \mu_1 - \mu_2 + v_1 - v_2 + 1, \cdots, \mu_1 - \mu_N + v_1 - v_N + 1, 1$, and

$$a_1 = 2 \prod_{i=1}^{N} \left[\frac{[\mu_i(1+\kappa_i)]^{\mu_1 - \mu_i + v_1 - v_i} \mu_i (1+\kappa_i)^{\frac{\mu_i + 1}{2}}}{\kappa_i^{\frac{\mu_i - 1}{2}} \exp(\kappa_i \mu_i) \Gamma(v_i + \mu_i)} \right] \prod_{i=1}^{N} \left[\frac{\left[2\mu_i \sqrt{\kappa_i (1+\kappa_i)} \right]^{2v_i + \mu_i - 1}}{(v_i)! 2^{2v_i + \mu_i - 1}} \right].$$

The cumulative distribution function (CDF) of the RV Z_N is given by [20]

$$F_{Z_N}(z) = \sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\frac{a_1}{2}z^{2(\mu_1+v_1)}G_{1\ N+1}^{N\ 1}\left(\begin{matrix}1-\mu_1-v_1\\ \rho\end{matrix}\middle| z^2\prod_{i=1}^{N}\mu_i(1+\kappa_i)\right), \tag{3}$$

where $\rho = -\mu_1+\mu_2-v_1+v_2,\cdots,-\mu_1+\mu_N-v_1+v_N,0,-\mu_1-v_1$. The intercepted message at E is given by

$$y_{E,k} = \sqrt{P}Z_{E,k}x + w_{E,k}, \tag{4}$$

where $w_{E,k}$ is the AWGN at the k^{th} antenna of E with zero mean and variance N_0. $Z_{E,k}$ is the channel gain for the wiretap link, which is the one between Alice and the k^{th} antenna of E for $k = 1,2,\cdots,K$. K is the total number of eavesdroppers, which also represents the number of antennas at E. $Z_{E,k}$ is defined by $Z_{E,k} = \prod_{j=1}^{n_e} Y_j^{(k)}$. $Y_j^{(k)}$ is a set of independent κ-μ RVs with the parameters $\kappa_{ej}^{(k)}$ and $\mu_{ej}^{(k)}$ $(j \in \{1,2,\cdots,n_e\})$ for the k^{th} link. Hence, $Z_{E,k}$ follows the cascaded $\kappa-\mu$ fading distribution with the following PDF

$$f_{Z_{E,k}}(z_e) = \sum_{r_1^{(k)}=0}^{\infty}\sum_{r_2^{(k)}=0}^{\infty}\cdots\sum_{r_{n_e}^{(k)}=0}^{\infty}a_2^{(k)}z_e^{2\mu_{e1}^{(k)}+2r_1^{(k)}-1}G_{\ n_e^{(k)}\ 0}^{0\ n_e^{(k)}}\left(\begin{matrix}\beta_e^{(k)}\\ -\end{matrix}\middle|\frac{1}{z_e^2\prod_{j=1}^{n_e^{(k)}}\mu_{ej}^{(k)}\left(1+\kappa_{ej}^{(k)}\right)}\right), \tag{5}$$

where $\beta_e^{(k)} = \mu_{e1}^{(k)}-\mu_{e2}^{(k)}+r_1^{(k)}-r_2^{(k)}+1,\cdots,\mu_{e1}^{(k)}-\mu_{en_e}^{(k)}+r_1^{(k)}-r_{n_e}^{(k)}+1,1$ and

$$a_2^{(k)} = 2\prod_{j=1}^{n_e^{(k)}}\left[\frac{\left[\mu_{ej}^{(k)}\left(1+\kappa_{ej}^{(k)}\right)\right]^{\mu_{e1}^{(k)}-\mu_{ej}^{(k)}+r_1^{(k)}-r_j^{(k)}}\mu_{ej}^{(k)}}{{\kappa_{ej}^{(k)}}^{\frac{\mu_{ej}^{(k)}-1}{2}}\exp\left(\kappa_{ej}^{(k)}\mu_{ej}^{(k)}\right)\Gamma\left(r_j^{(k)}+\mu_{ej}^{(k)}\right)}\right]\prod_{j=1}^{n_e^{(k)}}\left[\frac{\left[2\mu_{ej}^{(k)}\sqrt{\kappa_{ej}^{(k)}\left(1+\kappa_{ej}^{(k)}\right)}\right]^{2r_j^{(k)}+\mu_{ej}^{(k)}-1}}{(r_j^{(k)})!2^{2r_j^{(k)}+\mu_{ej}^{(k)}-1}}\right]$$
$$\times\prod_{j=1}^{n_e^{(k)}}\left[\left(1+\kappa_{ej}^{(k)}\right)^{\frac{\mu_{ej}^{(k)}+1}{2}}\right].$$

The CDF of the RV $Z_{E,k}$ is expressed as

$$F_{Z_{E,k}}(z_e) = \sum_{r_1^{(k)}=0}^{\infty}\sum_{r_2^{(k)}=0}^{\infty}\cdots\sum_{r_{n_e}^{(k)}=0}^{\infty}\frac{a_2^{(k)}}{2}z_e^{2\left(\mu_{e1}^{(k)}+r_1^{(k)}\right)}G_{\ 1\ n_e^{(k)}+1}^{n_e^{(k)}\ 1}\left(\begin{matrix}1-\mu_{e1}^{(k)}-r_1^{(k)}\\ s^{(k)}\end{matrix}\middle| z_e^2\prod_{j=1}^{n_e^{(k)}}\mu_{ej}^{(k)}\left(1+\kappa_{ej}^{(k)}\right)\right), \tag{6}$$

where $s^{(k)} = -\mu_{e1}^{(k)}+\mu_{e2}^{(k)}-r_1^{(k)}+r_2^{(k)},\cdots,-\mu_{e1}^{(k)}+\mu_{en_e}^{(k)}-r_1^{(k)}+r_{n_e}^{(k)},0,-\mu_{e1}-r_1^{(k)}$. The SNR at Bob is given by $\gamma_B = |Z_N|^2\frac{P}{N_\circ}$ with the following being the PDF and the CDF of γ_B

$$f_{\gamma_B}(\gamma) = \sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\frac{a_1}{2}\left(\frac{\prod_{i=1}^{N}E\left[X_i^2\right]}{\bar{\gamma_B}}\right)^{\mu_1+v_1}G_{N\ 0}^{0\ N}\left(\begin{matrix}\epsilon\\ -\end{matrix}\middle|\frac{\bar{\gamma_B}}{\gamma\prod_{i=1}^{N}E\left[X_i^2\right]\mu_i(1+\kappa_i)}\right)\times\gamma^{\mu_1+v_1-1}, \tag{7}$$

$$F_{\gamma_B}(\gamma) = \sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\frac{a_1}{2}\left(\gamma\frac{\prod_{i=1}^{N}E\left[X_i^2\right]}{\bar{\gamma_B}}\right)^{\mu_1+v_1}$$
$$\times G_{1\ N+1}^{N\ 1}\left(\begin{matrix}1-\mu_1-v_1\\ \rho\end{matrix}\middle|\frac{\gamma\prod_{i=1}^{N}E\left[X_i^2\right]\mu_i(1+\kappa_i)}{\bar{\gamma_B}}\right), \tag{8}$$

where $\bar{\gamma_B}$ is the average received SNR at Bob. The eavesdropper utilizes the MRC on the received messages. Hence, the received SNR at E is given by $\gamma_E = \sum_{i=1}^{K} \gamma_{E,i} = \sum_{i=1}^{K} |Z_{E,i}|^2 \frac{P}{N_0}$. Using [27] and (5), the PDF of γ_E is given by

$$f_{\gamma_E}(\gamma_e) = \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_{n_e}=0}^{\infty} \frac{c_{x,e}}{2} \left(\frac{\prod_{j=1}^{n_e} E\left[X_j^2\right]}{\bar{\gamma_E} K} \right)^{\mu_{e1}K + r_1} \gamma_e^{\mu_{e1}K + r_1 - 1} \times G_{n_e\ 0}^{0\ n_e} \left(\begin{matrix} \beta'_e \\ - \end{matrix} \middle| \frac{\bar{\gamma_E} K}{\gamma_e \prod_{j=1}^{n_e} E\left[X_j^2\right] \mu_{ej} K_j (1 + \kappa_{ej})} \right), \quad (9)$$

where $\bar{\gamma_E}$ is the average received SNR at E, $\beta'_e = \mu_{e1}K - \mu_{e2}K + r_1 - r_2 + 1, \cdots, \mu_{e1}K - \mu_{en_e}K + r_1 - r_{ne} + 1, 1$, and

$$c_{x,e} = 2 \prod_{j=1}^{n_e} \left[\frac{\left[2\mu_{ej} K_j \sqrt{\kappa_{ej}(1 + \kappa_{ej})} \right]^{2r_j + \mu_{ej}K_j - 1}}{(r_j)! 2^{2r_j + \mu_{ej}K_j - 1}} \right] \prod_{j=1}^{n_e} \left[\frac{\left[\mu_{ej} K_j (1 + \kappa_{ej}) \right]^{\mu_{e1}K - \mu_{ej}K_j + r_1 - r_j}}{\kappa_{ej}^{\frac{\mu_{ej}K_j - 1}{2}} \exp(\kappa_{ej} \mu_{ej} K_j)} \right] \times \prod_{j=1}^{n_e} \left[\frac{\mu_{ej} K_j (1 + \kappa_{ej})^{\frac{\mu_{ej}K_j + 1}{2}}}{\Gamma(r_j + \mu_{ej} K_j)} \right].$$

Proving the accuracy of (9), the PDF of γ_E is plotted in Figure 2 with Monte-Carlo simulations.

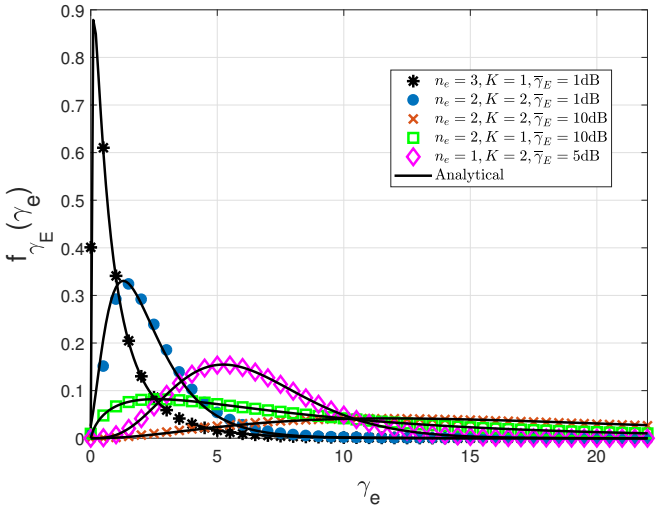

Figure 2. The PDF of the received SNR at the eavesdropper (γ_E) for multiple values of cascade level of the wiretap channel (n_e) and multiple number of antennas at E (K). $\kappa_e = 1$ and $\mu_e = 2$.

Using (9) and ([28] Equation (26)), the CDF of γ_E can be given by

$$F_{\gamma_E}(\gamma_e) = \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_{n_e}=0}^{\infty} \frac{c_{x,e}}{2} G_{1\ n_e+1}^{n_e\ 1} \left(\begin{matrix} \epsilon' \\ \eta'_e \end{matrix} \middle| \frac{A\gamma_e}{\bar{\gamma_E} K} \right) \left(\gamma_e \frac{\prod_{j=1}^{n_e} E\left[X_j^2\right]}{\bar{\gamma_E} K} \right)^{\mu_{e1}K + r_1}, \quad (10)$$

where $\epsilon' = 1 - \mu_{e1}K - r_1$, $\eta'_e = -\mu_{e1}K + \mu_{e2}K - r_1 + r_2, \cdots, -\mu_{e1}K + \mu_{e'n_e}K - r_1 + r_{n_e}, 0$, $-\mu_{e1}K - r_1$, and $A = \prod_{j=1}^{n_e} E\left[X_j^2\right] \mu_{ej} K_j (1 + \kappa_{ej})$.

2.1.1. Secrecy Outage Probability

The secrecy outage probability (OP_{sec}) is defined as the probability that the secrecy capacity C_s is less than a predetermined threshold C_{th}. The secrecy capacity can be expressed as [29]

$$C_s = \begin{cases} C_m - C_e, & \text{if } \gamma_B > \gamma_E \\ 0, & \text{if } \gamma_B \leq \gamma_E \end{cases}, \tag{11}$$

where C_m and C_e are the capacities of the main and the wiretap channels, respectively. OP_{sec} is expressed as

$$\begin{aligned} OP_{sec} &= P_r(C_s < C_{th}) \\ &= \int_0^\infty f_{\gamma_E}(\gamma_e) F_{\gamma_B}\left(2^{C_{th}}(1+\gamma_e) - 1\right) d\gamma_e, \end{aligned} \tag{12}$$

Due to the complexity of the expression in (12), a lower bound for the secrecy outage probability is obtained instead (OP_{sec}^L). Hence, OP_{sec}^L is given by [30]

$$OP_{sec}^L = \int_0^\infty f_{\gamma_E}(\gamma_e) F_{\gamma_B}\left(2^{C_{th}}\gamma_e\right) d\gamma_e. \tag{13}$$

Using (8) and (9) with the help of ([31] Equation (2.3.31)) and ([26] Equation (7.813-1)) yields

$$OP_{sec}^L = \sum_{v_1=0}^{\infty} \sum_{v_2=0}^{\infty} \cdots \sum_{v_N=0}^{\infty} \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_{n_e}=0}^{\infty} c_a G_{\,n_e+1}^{\,N}{}_{N+1}^{\,n_e+1}\left(\begin{matrix}\xi \\ \rho\end{matrix}\middle| D\right), \tag{14}$$

where $\xi = 1 - \mu_1 - v_1, 1 - \mu_1 - v_1 - \mu_{e2}K - r_2, \cdots, 1 - \mu_1 - v_1 - \mu_{en_e}K - r_{n_e}, 1 - \mu_{e1}K - r_1 - \mu_1 - v_1, D = \frac{2^{C_{th}}\bar{\gamma}_E K \prod_{i=1}^{N} E\left[X_i^2\right]\mu_i(1+\kappa_i)}{\bar{\gamma}_B \prod_{j=1}^{n_e} E[X_j^2]\mu_{ej}K_j\left(1+\kappa_{ej}\right)}$, and

$$\begin{aligned} c_a = \frac{a_1 c_{x,e}}{4} 2^{C_{th}(\mu_1+v_1)} &\left(\frac{\prod_{i=1}^{N} E\left[X_i^2\right]}{\bar{\gamma}_B}\right)^{\mu_1+v_1} \left(\frac{\prod_{j=1}^{n_e} E[X_j^2]\mu_{ej}K(1+\kappa_{ej})}{\bar{\gamma}_E K}\right)^{-\mu_{e1}K-r_1-\mu_1-v_1} \\ &\times \left(\frac{\prod_{j=1}^{n_e} E[X_j^2]}{\bar{\gamma}_E K}\right)^{\mu_{e1}K+r_1}. \end{aligned}$$

2.1.2. Asymptotic Secrecy Outage Probability as $\bar{\gamma}_E \to \infty$

In this section, the asymptotic OP_{sec}^L is evaluated when $\bar{\gamma}_E \to \infty$. Rewriting (14) with the help of ([32] Equation (2.2.1)) and ([32] Equation (3.11.3)) yields

$$OP_{sec}^L = \sum_{v_1=0}^{\infty} \sum_{v_2=0}^{\infty} \cdots \sum_{v_N=0}^{\infty} \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_{n_e}=0}^{\infty} c_a c_b H_{\,n_e+1}^{\,N}{}_{N+1}^{\,n_e+1}\left(\begin{matrix}\epsilon_d \\ \eta_d\end{matrix}\middle| D\right), \tag{15}$$

where $H_{\,p}^{\,m}{}_{q}^{\,n}\left(\begin{matrix}a \\ b\end{matrix}\middle|\cdot\right)$ is the H-function defined in ([32] (Equation 3.11.1)), $\epsilon_d = \{1,1\}, \{1-\mu_{e2}K-r_2,1\}, \cdots, \{1-\mu_{en_e}K-r_{n_e},1\}, \{1-\mu_{e1}K-r_1,1\}, \eta_d = \{\mu_2+v_2,1\}, \cdots, \{\mu_N+v_N,1\}, \{\mu_1+v_1,1\}, \{0,1\}$, and $c_b = \left(\frac{\bar{\gamma}_B \prod_{j=1}^{n_e} E[X_j^2]\mu_{ej}K_j\left(1+\kappa_{ej}\right)}{2^{C_{th}}K\prod_{i=1}^{N} E\left[X_i^2\right]\mu_i(1+\kappa_i)}\right)^{\mu_1+v_1}$. Furthermore, the H-function can be rewritten again using its integral representation. Hence, (15) is given by

$$\begin{aligned} OP_{sec}^L = &\sum_{v_1=0}^{\infty} \sum_{v_2=0}^{\infty} \cdots \sum_{v_N=0}^{\infty} \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_{n_e}=0}^{\infty} \frac{c_a c_b}{2\pi i} \\ &\times \int_C \frac{\Gamma[s]\prod_{i=1}^{N}\Gamma[\mu_i+v_i-s]}{\Gamma[1+s]} \prod_{j=1}^{n_e} \Gamma[\mu_{ej}K + r_j + s] D^s ds. \end{aligned} \tag{16}$$

To obtain the asymptotic expression for OP_{sec}^{L}, the residue method is utilized [33]. Hence, as $\bar{\gamma_E} \to \infty$, D $\to \infty$ with the asymptotic expression of OP_{sec}^{L} given by

$$\begin{aligned} OP_{sec,E}^{L} &\approx \sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty}\frac{c_a c_b}{2\pi i}\mathrm{Res}\{g(s),0\} \\ &\approx \sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} c_a c_b \prod_{i=1}^{N}\Gamma[\mu_i+v_i]\prod_{j=1}^{n_e}\Gamma[\mu_{ej}K+r_j], \end{aligned} \tag{17}$$

where $g(s)$ is given by

$$g(s) = D^s \frac{\Gamma[s]\prod_{i=1}^{N}\Gamma[\mu_i+v_i-s]\prod_{j=1}^{n_e}\Gamma[\mu_{ej}K+r_j+s]}{\Gamma[1+s]}.$$

It is evident from (17) that the diversity order is zero since the expression is independent of $\bar{\gamma}$. This implies that the secrecy is completely compromised when the wiretap channel's conditions are highly improved ($\bar{\gamma_E} \to \infty$). In such circumstances, the confidential information can be overheard and decoded successfully by E.

2.1.3. Asymptotic Secrecy Outage Probability as $\bar{\gamma_B} \to \infty$

In this section, we assess the impact of having very reliable conditions on the main link in terms of the average received SNR over the security. That is, the asymptotic OP_{sec}^{L} as $\bar{\gamma_B} \to \infty$ is evaluated. The secrecy outage probability in (14) can be rewritten as

$$\begin{aligned} OP_{sec}^{L} &= \sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty}\frac{c_a c_d^{-\mu_1-v_1}}{2\pi i} \\ &\times \int_C \frac{\prod_{j=1}^{N}\Gamma[\mu_j+v_j-s]\Gamma[s]\prod_{j=1}^{n_e}\Gamma[\mu_{ej}K_j+r_j+s]\Gamma[s]}{\Gamma[1+s]} M^s ds, \end{aligned} \tag{18}$$

where $c_d = \frac{2^{C_{th}}\bar{\gamma_E}K\prod_{i=1}^{N}E[X_i^2]\mu_i(1+\kappa_i)}{\prod_{j=1}^{n_e}\mu_{ej}K_j(1+\kappa_{ej})}$ and $M = \frac{c_d}{\bar{\gamma_B}}$. Similar to the previous section, using the residue method [33], the asymptotic secrecy outage probability can be finally given by

$$\begin{aligned} OP_{sec,B}^{L} &\approx \sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} c_a c_d^{-\mu_1-v_1}\prod_{j=1,j\neq I}^{N}\Gamma[\mu_j+v_j-\mu_I-v_I]\} \\ &\times \prod_{j=1}^{n_e}\Gamma[\mu_{ej}K_j+r_j+\mu_I+v_I]M^{\mu_I+v_I}, \end{aligned} \tag{19}$$

where $\mu_I + v_I = \min \mu_j + v_j$, for $j = 1, 2, \cdots, N$, which represents the minimum pole at which the residue method is evaluated.

2.1.4. Probability of Non-Zero Secrecy Capacity

The probability of non-zero secrecy capacity (P_{nsc}) is recognized as the probability that the main channel's capacity is larger than the wiretap channel's capacity. This implies that the main channel is more reliable than the wiretap channel. Mathematically, P_{nsc} is expressed as

$$\begin{aligned} P_{nsc} &= P_r(C_s > 0) \\ &= 1 - P_r(\gamma_B \leq \gamma_E) \\ &= 1 - \int_0^{\infty} F_{\gamma_B}(y) f_{\gamma_E}(y), \end{aligned} \tag{20}$$

Substituting (8) and (9) into (20) and with the help of ([34] Equation (2.24.1.1)), P_{nsc} is solved as

$$P_{nsc} = 1 - \sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty}\sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\frac{c_{x,e}a_1}{4}\left(\frac{\prod_{i=1}^{N}E\left[X_i^2\right]}{\bar{\gamma_B}}\right)^{\mu_1+v_1}\left(\frac{\prod_{j=1}^{n_e}E\left[X_j^2\right]}{\bar{\gamma_E}K}\right)^{\mu_{e1}K+r_1}$$
$$\times\left(\frac{\prod_{i=1}^{N}E\left[X_i^2\right]\mu_i(1+\kappa_i)}{\bar{\gamma_B}}\right)^{-\mu_1-v_1-\mu_{e1}K-r_1}G_{N+1\ n_e+1}^{n_e+1\ N}\left(\begin{matrix}\psi\\ \psi'\end{matrix}\middle|\frac{\bar{\gamma_B}\prod_{j=1}^{n_e}E[X_j^2]\mu_{ej}K_j(1+\kappa_{ej})}{\bar{\gamma_E}K\prod_{i=1}^{N}E\left[X_i^2\right]\mu_i(1+\kappa_i)}\right), \quad (21)$$

where $\psi = 1-\mu_{e1}K-r_1-\mu_2-v_2,\cdots,1-\mu_{e1}K-r_1-\mu_N-v_N,1-\mu_1-v_1-\mu_{e1}K-r_1,1-\mu_{e1}K-r_1$ and $\psi' = -\mu_{e1}K+\mu_{e2}K-r_1+r_2,\cdots,-\mu_{e1}K+\mu_{en_e}K-r_1+r_{n_e},0,-\mu_{e1}K-r_1$.

2.1.5. Asymptotic Probability of Non-Zero Secrecy Capacity

To study the impact of enhancing the wiretap channel's conditions over the privacy of the shared information, asymptotic P_{nsc} is evaluated as $\bar{\gamma_E}\to\infty$. Following the same approach used to find the asymptotic secrecy outage probability, the asymptotic probability of non-zero secrecy capacity is expressed as

$$P_{nsc} \approx 1 - \sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty}c_{x,e}a_1c_c\prod_{i=1}^{N}\Gamma[\mu_i+v_i]\prod_{j=1}^{n_e}\Gamma[\mu_{ej}K+r_j], \quad (22)$$

where $c_c = \dfrac{\prod_{j=1}^{n_e}E[X_j^2]}{4\prod_{i=1}^{N}E[X_i^2]\left(\prod_{j=1}^{n_e}\mu_{ej}K_j(1+\kappa_{ej})\right)^{\mu_{e1}K+r_1}\left(\prod_{i=1}^{N}\mu_i(1+\kappa_i)\right)^{\mu_1+v_1}}$.

Equation (22) demonstrates that the eavesdropper taps the information and decodes it effectively since the characteristics of the wiretap channel are extremely strong in terms of the average received SNR $(\bar{\gamma_E})$. A similar scenario is attainable when the eavesdropper is relatively close to the transmitter, enabling it to effectively decode the intercepted information.

2.1.6. Intercept Probability

The intercept probability (P_{int}) estimates the probability that the eavesdropper is able to intercept the information. This occurs when the wiretap channel conditions are more reliable than the main channel conditions. Mathematically, P_{int} is expressed as

$$P_{int} = P_r(C_s<0) = P_r(\gamma_B<\gamma_E) = 1-P_{nsc}. \quad (23)$$

Substituting (21) and (22) into (23) yields the exact and asymptotic intercept probability, respectively. It is worth mentioning that while the probability of non-zero secrecy capacity highlights the reliability level of the main channel, the intercept probability measures the intercept capabilities of the eavesdropper instead. This aids in comprehending the security implications of both channels.

2.2. Physical-Layer Security Analysis: Non-Colluding Eavesdroppers

This section considers the second scenario, in which the eavesdroppers are expected to process the intercepted information independently without the messages being jointly processed. In this context, the eavesdroppers' locations are assumed to be random according to a homogeneous Poisson point process (HPPP) with a density of λ_e. We assume that the eavesdroppers are distributed in an unbounded Euclidean space of dimension U. The eavesdroppers' information regarding the positions related to Alice can be obtained by assuming that the eavesdroppers are users in the network but are untrusted and do not have the authorization to access the channel [35,36]. Our analyses are based on selecting the i^{th} closest eavesdropper to the transmitter Alice, once the distances between Alice and the eavesdroppers have been ordered in an ascending manner [19].

2.2.1. Probability of Non-Zero Secrecy Capacity

To explore the physical-layer security for the three-node wiretap system model under the threat of non-colluding eavesdroppers, the probability of non-zero secrecy capacity is utilized. From (20), the probability of non-zero secrecy capacity is expressed as

$$P_{nsc} = 1 - \int_0^\infty F_{\gamma_B}(y) f_Y(y) dy, \tag{24}$$

where $Y = \frac{\gamma_E}{d^\alpha}$, in which d is the distance between the transmitter (Alice) and the i^{th} closest eavesdropper and α is the path loss exponent. The PDF of the path loss d^α is distributed as [37]

$$f_{d^\alpha}(x) \quad = \quad \exp\left(-A_e x^\delta\right) \frac{\delta A_e^i x^{\delta i - 1}}{\Gamma(i)}, \tag{25}$$

where $A_e = \pi\lambda_e$, $\delta = \frac{U}{\alpha}$, and $\Gamma(\cdot)$ is the gamma function. First, one needs to obtain the PDF of Y as

$$f_Y(y) \quad = \quad \int_0^\infty y_b f_{\gamma_E}(y y_b) f_{d^\alpha}(y_b) dy_b. \tag{26}$$

Substituting (9) and (25) and with the help of ([34] Equation (2.24.3.1)) yields

$$f_Y(y) = \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_{n_e}=0}^{\infty} C_1 y^{-1-\delta i} G_{\delta n_e \; 1}^{\; 1 \; \delta n_e} \left(\begin{matrix} F \\ F' \end{matrix} \middle| \frac{A_e \delta^{\delta n_e} (\bar{\gamma_E} K)^\delta}{y^\delta \left(\prod_{j=1}^{n_e} E\left[X_j^2\right] \mu_{ej} K_j (1+\kappa_{ej}) \right)^\delta} \right), \tag{27}$$

where

$$C_1 = \left(\frac{\prod_{j=1}^{n_e} E\left[X_j^2\right]}{\bar{\gamma_E} K} \right)^{\mu_{e1} K + r_1} \frac{c_{x,e} A_e^i \delta^{n_e(\delta i + \mu_{e1} K + r_1) + \rho^*}}{2\Gamma(i)(2\pi)^{\frac{(\delta-1)n_e}{2}}} \left(\frac{\prod_{j=1}^{n_e} E\left[X_j^2\right] \mu_{ej} K_j (1+\kappa_{ej})}{\bar{\gamma_E} K} \right)^{-\delta i - \mu_{e1} K - r_1},$$

$F = \frac{1-\delta i-\mu_{e2}K-r_2}{\delta}, \cdots, \frac{1-\delta i-\mu_{en_e}K-r_{n_e}}{\delta}, \frac{1-\delta i-\mu_{e1}K-r_1}{\delta}$, $F' = 0$, and $\rho^* = \sum_{j=1}^{n_e} 1 - \beta_e' + 1 - \frac{n_e}{2}$. Using (8), (27), and ([34] Equation (2.24.3.1)), the probability of non-zero secrecy capacity given in (24) is solved as

$$P_{nsc} = 1 - \sum_{r_1=0}^{\infty} \sum_{r_2=0}^{\infty} \cdots \sum_{r_{n_e}=0}^{\infty} \sum_{v_1=0}^{\infty} \sum_{v_2=0}^{\infty} \cdots \sum_{v_N=0}^{\infty} C_2 G_{\delta N+1+\delta \; \delta n_e+\delta}^{\; \delta n_e+\delta \; \delta N+1} \left(\begin{matrix} \zeta \\ \zeta' \end{matrix} \middle| \phi \right), \tag{28}$$

where

$$C_2 = \frac{C_1 a_1}{2} \left(\frac{\prod_{i=1}^{N} E\left[X_i^2\right]}{\bar{\gamma_B}} \right)^{\mu_1 + v_1} \frac{\delta^{N(\mu_1+v_1-\delta i)-1+q}}{(2\pi)^{\frac{(\delta-1)N}{2}}} \left(\frac{\prod_{i=1}^{N} E\left[X_i^2\right] \mu_i (1+\kappa_i)}{\bar{\gamma_B}} \right)^{\delta i - \mu_1 - v_1},$$

$q = \sum_{j=1}^{N+1} \rho + \mu_1 + v_1 - \frac{N}{2}$, $\zeta = 1, \frac{1+\delta i-\mu_2-v_2}{\delta}, \cdots, \frac{1+\delta i-\mu_N-v_N}{\delta}, \frac{1+\delta i-\mu_1-v_1}{\delta}, \frac{1+\delta i}{\delta}$, $\zeta' = 1 - F, i$, and $\phi = \frac{\left(\prod_{j=1}^{n_e} E\left[X_j^2\right] \mu_{ej} K_j \left(1+\kappa_{ej}\right) \right)^\delta}{A_e \delta^{\delta n_e} \left(\bar{\gamma_E} K\right)^\delta} \Big/ \left(\frac{\prod_{i=1}^{N} E\left[X_i^2\right] \mu_i (1+\kappa_i)}{\bar{\gamma_B}} \right)^\delta$.

2.2.2. Asymptotic Probability of Non-Zero Secrecy Capacity

In this section, the security is evaluated as the wiretap channel's conditions are extremely strong. Particularly, we evaluate the probability of non-zero secrecy capacity as $\bar{\gamma_E} \to \infty$. Hence, (28) is rewritten as

$$P_{nsc} = 1 - \sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty}\frac{C_2 c_f^i}{2\pi j} \times \int_C \frac{\prod_{j=1}^{\delta n_e}\Gamma\left[-i+\frac{\delta i+\mu_{ej}K_j+r_j}{\delta}-s\right]\Gamma[-s]\prod_{j=1}^{\delta N}\Gamma\left[1+i+\frac{-1-\delta i+\mu_j+r_j}{\delta}+s\right]\Gamma[i+s]}{\Gamma\left[\frac{1}{\delta}+s\right]} T^s ds, \quad (29)$$

where $c_f = \frac{\frac{(\prod_{j=1}^{n_e} E[X_j^2]\mu_{ej}K_j(1+\kappa_{ej}))^{\delta}}{A_e \delta^{\delta n_e}(\bar{\gamma_E}K)^{\delta}}}{(\prod_{i=1}^{N} E[X_i^2]\mu_i(1+\kappa_i))^{\delta}}$ and $T = \frac{c_f}{\bar{\gamma_E}^{\delta}}$. Using the residue method [33], the probability of non-zero secrecy capacity can be finally approximated as

$$P_{nsc} \approx 1 - \sum_{v_1=0}^{\infty}\sum_{v_2=0}^{\infty}\cdots\sum_{v_N=0}^{\infty}\sum_{r_1=0}^{\infty}\sum_{r_2=0}^{\infty}\cdots\sum_{r_{n_e}=0}^{\infty} C_2 c_f^i \prod_{j=1}^{N}\Gamma\left[1-\frac{1}{\delta}+\frac{\mu_j+v_j}{\delta}\right]\} \times \prod_{j=1}^{\delta n_e}\Gamma\left[\frac{\mu_{ej}K_j+r_j}{\delta}\right]\frac{\Gamma[i]}{\Gamma[1/\delta]}. \quad (30)$$

It is worth mentioning that according to (30), the security is independent of the average received SNR at the eavesdropper ($\bar{\gamma_E}$). This indicates that the probability of achieving a positive secrecy capacity under such conditions is extremely low. This represents the scenario where the wiretap channel is very reliable and the eavesdropper has a very strong reception level as opposed to the legitimate receiver reception quality.

2.2.3. Intercept Probability

Intercept probability is evaluated with the help of (28) as

$$P_{int} = 1 - P_{nsc}. \quad (31)$$

Moreover, the asymptotic P_{int} can be directly attained from (30) as $\bar{\gamma_E} \to \infty$.

3. Results and Discussion

In this section, the results and Monte-Carlo simulations are given. The analytical curves are plotted by truncating the infinite series summations (v and r) to the first twenty terms.

Figure 3 shows the secrecy outage probability versus the average received SNR at Bob ($\bar{\gamma_B}$). In this figure, setting the fading channel parameters for the main and the wiretap channels to $\kappa = 0$ and $\mu = 1$ results in the Rayleigh fading as a special case of the κ-μ fading model. The impact of the cascade levels (number of keyholes) for the main channel (N) and for the wiretap channel (n_e) is provided in this figure. Indeed, privacy worsens as the cascade level grows in the main channel or reduces in the wiretap channel. The fact is that a greater N signifies a larger number of scatters and obstacles in the main channel, resulting in a more severe fading. Additionally, it is noted that the probability of an outage in the security of the transmitted messages is higher as the eavesdropper channel's circumstances improve by increasing the average received SNR ($\bar{\gamma_E}$). Moreover, the figure includes the asymptotic secrecy outage probability derived in (17) as $\bar{\gamma_E}$ becomes very high. At the highest value of $\bar{\gamma_E}$, a zero slope appears, and a value of one for the secrecy outage probability is provided. This demonstrates that for these parameters, the secrecy is completely compromised and the information will be certainly intercepted by E irrespective of the value of $\bar{\gamma_B}$. Finally, the results show that the information may be delivered more securely regardless of the cascade levels as the main channel conditions improve in terms of $\bar{\gamma_B}$. Finally, the asymptotic secrecy outage probability derived in (19) as $\bar{\gamma_B} \to \infty$ is included, and it is clear that it matches the results as $\bar{\gamma_B}$ takes high values.

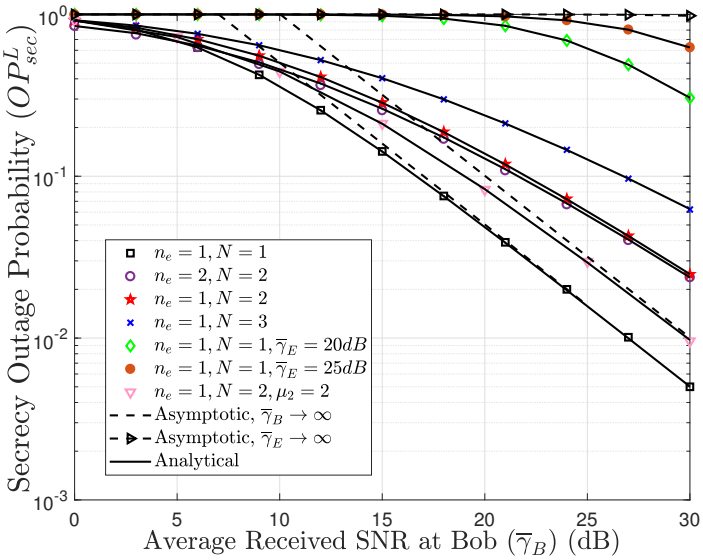

Figure 3. The lower bound of the secrecy outage probability (OP_{sec}^{L}) versus the average received SNR at Bob $(\overline{\gamma}_B)$. For the main channel, $\kappa = 0, \mu = 1$, and for the wiretap channel, $\kappa_e = 0, \mu_e = 1$ (Rayleigh). $C_{th} = 1$, $K = 2$, and $\overline{\gamma}_E = 1$ dB.

Figure 4 depicts the effect of varying the number of antennas at E (K) over the security. It can be seen that increasing the number of antennas improves the eavesdropper's reception capabilities and aids in effectively decoding the tapped messages owing to the use of the MRC method. Hence, the shared information's privacy is compromised. Additionally, the figure illustrates that improving the wiretap channel conditions in terms of the average received SNR at E $(\overline{\gamma}_E)$ will eventually result in an extremely low probability of non-zero secrecy capacity. This indicates the P_{nsc} asymptotic case derived in (22). However, the privacy of shared information may be enhanced by raising the value of $\overline{\gamma}_B$, which can be achieved by having fewer scatters (N) obstructing the main channel path.

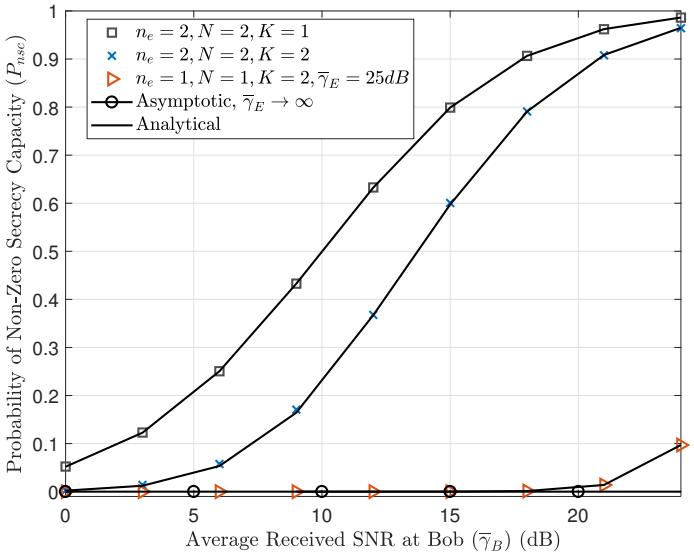

Figure 4. The probability of non-zero secrecy capacity (P_{nsc}) versus the average received SNR at Bob $(\overline{\gamma}_B)$. For the main channel, $\kappa = 1, \mu = 2$, and for the wiretap channel, $\kappa_e = 1, \mu_e = 2$. $\overline{\gamma}_E = 10$ dB.

To take the path loss effect over the secrecy into considerations, Figure 5 shows a two-dimensional (2D) graph where the transmitter Alice (A) is the reference location. That

is, Alice is located at $(0,0)$ and the other receivers (B and E) have different distances from Alice, and B stands for the legitimate receiver Bob. Assume $d_{XY}^{-\beta} = \frac{1}{2\lambda_J}$, where β is the path loss exponent, $X \in \{A, p_1, p_2, \cdots\}$, $Y \in \{B, E, p_1, p_2, \cdots\}$, and $J \in \{B, E\}$. $\lambda_J = \frac{1}{2\sigma_J^2}$ is the Rayleigh fading parameter, and σ_J is the scale parameter of the distribution. d_{XY} represents the distance from node X to node Y in meters (m). p_i (for $i = 1, 2, \cdots, N-1$) are the locations of the obstacles in the main channel. This is to note the effect of the cascade level between A and B. Figure 6 corresponds to the 2D graph and it indicates that regardless of the number of antennas at E and the effectiveness of the MRC technique, as the eavesdropper moves further away from the transmitter Alice, i.e., as d_{AE} becomes larger, the privacy of the transferred information improves. This can be interpreted by the fact that as d_{AE} rises, the wiretap channel's conditions worsen and the received SNR at E deteriorates accordingly. This graph demonstrates the importance of considering the impact of distances between nodes on privacy.

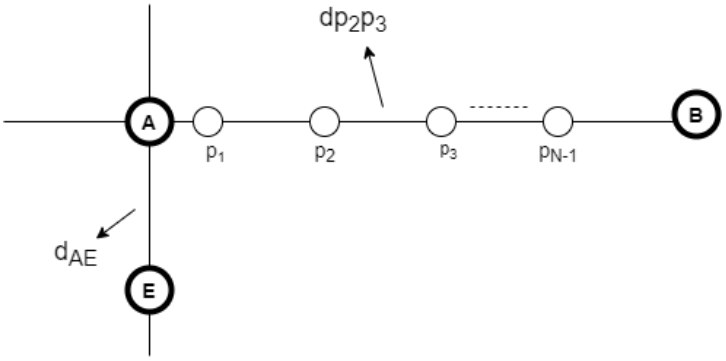

Figure 5. The 2D graph.

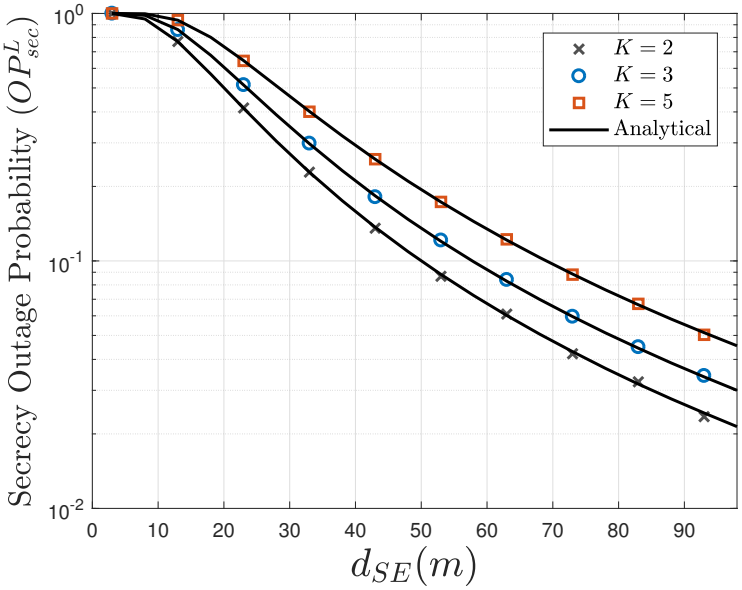

Figure 6. The lower bound of the secrecy outage probability (OP_{sec}^{L}) versus the distance between Alice and E for different number of antennas K. For the main channel, $\kappa = 0, \mu = 1$, and for the wiretap channel, $\kappa_e = 0, \mu_e = 1$. $\bar{\gamma_E} = 1$ dB, $\bar{\gamma_B} = 10$ dB, $C_{th} = 1$, $N = 2$, $n_e = 1$, $\beta = 3$, $d_{Ap_1} = 5$ m, and $d_{p_{1B}} = 5$ m.

Figure 7 illustrates the intercept probability (P_{int}) versus the density of eavesdroppers (λ_e) for two different values of i, in which i represents the selection of the closest eavesdropper. For example, $i = 1$ denotes choosing the first nearest eavesdropper to the transmitter, and thus the wiretap channel will be the one between Alice and this selected eavesdropper.

We assume a 2D area $(U = 2)$, and we generate 10^5 realizations of the positions of the eavesdroppers in a square area of 20 m^2. The figure shows that the probability of the information interception grows as the density of eavesdroppers increases. This is owing to the fact that the probability of a more harmful eavesdropper is rising as the λ_e grows. That is, as λ_e rises, there is a greater probability of having a closer eavesdropper to Alice. Additionally, the privacy of the shared information is under a higher risk when selecting the first closest eavesdropper $(i = 1)$ as opposed to selecting the second closest one $(i = 2)$. The reason is that the first closest eavesdropper is more probable to have better channel conditions compared to the other farther eavesdroppers. This figure proves the significance of considering random locations for the eavesdroppers, rather than being fixed at specific locations and distances from the transmitter.

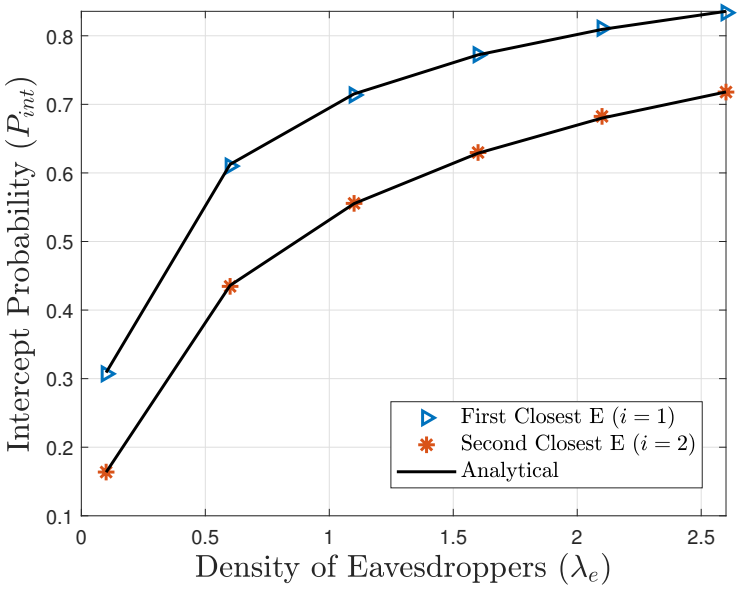

Figure 7. The intercept probability (P_{int}) versus the density of E for different values of i. For the main channel, $\kappa = 1, \mu = 1$, and for the wiretap channel, $\kappa_e = 1, \mu_e = 1$. $\bar{\gamma}_E = 1$ dB, $\bar{\gamma}_B = 5$ dB, $N = 2$, $n_e = 2$, $\alpha = 2$, $K = 1$.

Figure 8 presents a comparison between colluding and non-colluding eavesdroppers with a density of $\lambda_e = 0.1$. In the case of non-colluding eavesdroppers, the security declines as the number of antennas rise. Moreover, comparing the case of non-colluding eavesdroppers for $K = 2$ with the colluding eavesdroppers case, it is noted that although the number of non-colluding eavesdroppers is greater, the interception and decoding ability of the colluding eavesdroppers is stronger. Hence, the privacy of information is more vulnerable when colluding eavesdroppers exist in the network. This leads to the realization that further countermeasures should be adopted at the main channel in the presence of colluding eavesdroppers.

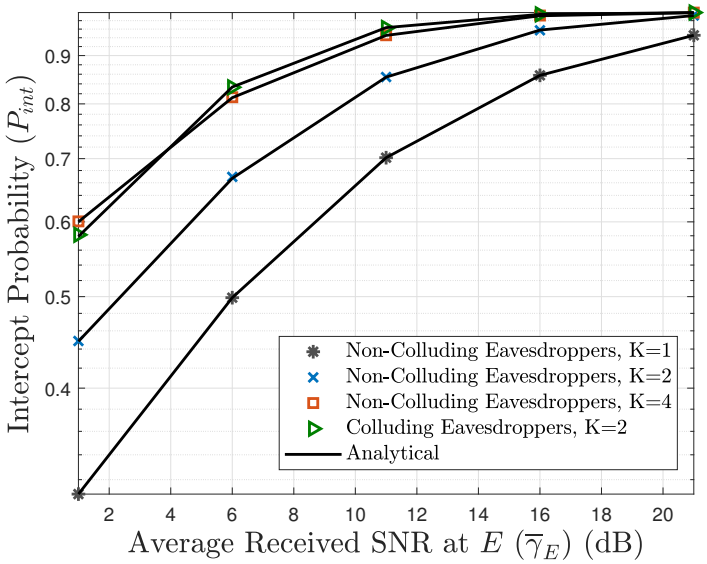

Figure 8. The intercept probability (P_{int}) versus the average received SNR at E. For the main channel, $\kappa = 1, \mu = 1$, and for the wiretap channel, $\kappa_e = 1, \mu_e = 1$. $\overline{\gamma}_B = 5$ dB, $N = 2$, $n_e = 1$, $\alpha = 2$, $\lambda_e = 0.1$, and $i = 1$.

As a final investigation, Figure 9 demonstrates the probability of non-zero secrecy capacity for different values of the average received SNR at E ($\overline{\gamma}_E$) for the non-colluding eavesdroppers case. The results clearly demonstrate how the system's privacy behaves as the eavesdroppers' channel quality improves. Particularly, fixing the legitimate receiver received SNR, the privacy of the shared information is severely compromised as $\overline{\gamma}_E$ takes high values. After a certain limit, the P_{nsc} approaches its asymptotic degree, i.e., lowest value. That is, the curve reaches a value of zero as $\overline{\gamma}_E \to \infty$. Indeed, this is in agreement with the asymptotic results obtained in (30).

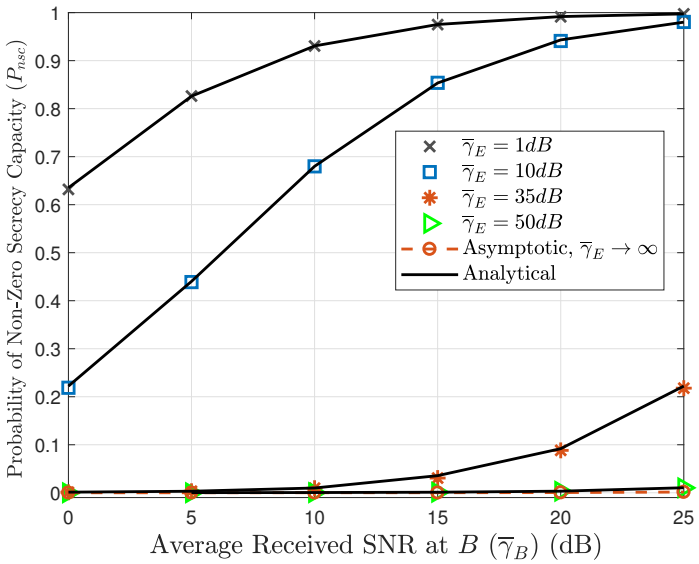

Figure 9. The probability of non-zero secrecy capacity (P_{nsc}) for different values of the average received SNR at E ($\overline{\gamma}_E$). For the main channel, $\kappa = 2, \mu = 2$, and for the wiretap channel, $\kappa_e = 0$, $\mu_e = 1$. $N = 2$, $n_e = 1$, $K = 1$, $\alpha = 2$, $\lambda_e = 0.1$, and $i = 1$.

4. Conclusions

In this paper, the physical-layer security for a three-node wiretap system model with multiple eavesdroppers over cascaded κ-μ fading channels is investigated. The secrecy was assessed in terms of the secrecy outage probability, the probability of non-zero secrecy capacity, and the intercept probability. Two scenariosw were examined for the way in which eavesdroppers tap and analyze the information: colluding and non-colluding eavesdroppers. Results reveal that the cascade level has a significant impact over the privacy of the shared information. In addition, the results show that the security can be improved by enhancing the average received SNR at the main channel. However, confidentiality is reduced by the increasing number of antennas for the two eavesdroppers' scenarios. Additionally, the effect of the distances between the nodes is investigated, suggesting that the privacy deteriorates significantly as the eavesdropper draws closer to the transmitter. Moreover, our results prove that having colluding eavesdroppers in the network is more threatening and challenging to combat than having non-colluding eavesdroppers. This is maintained even when the density of non-colluding eavesdroppers is larger.

Author Contributions: Formal analysis, D.T.; Supervision, W.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Tashman, D.H.; Hamouda, W. Cascaded κ-μ Fading Channels with Colluding Eavesdroppers: Physical-Layer Security Analysis. In Proceedings of the 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Sharjah, United Arab Emirates, 16–18 March 2021; pp. 1–6. [CrossRef]
2. Moualeu, J.M.; Hamouda, W.; Takawira, F. Secrecy Performance of Generalized Selection Diversity Combining Scheme with Gaussian Errors. In Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 27–30 August 2018; pp. 1–5. [CrossRef]
3. Moualeu, J.M.; Hamouda, W. Performance analysis of secure communications over α-μ/κ-μ fading channels. In Proceedings of the 2017 12th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 19–20 Decwmber 2017; pp. 473–478. [CrossRef]
4. Jameel, F.; Wyne, S.; Kaddoum, G.; Duong, T.Q. A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2734–2771. [CrossRef]
5. Moualeu, J.M.; Sofotasios, P.C.; da Costa, D.B.; Muhaidat, S.; Hamouda, W.; Dias, U.S. Physical-Layer Security of SIMO Communication Systems over Multipath Fading Conditions. *IEEE Trans. Sustain. Comput.* **2021**, *6*, 105–118.[CrossRef]
6. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
7. Ozarow, L.H.; Wyner, A.D. Wire-tap channel II. *AT&T Bell Lab. Tech. J.* **1984**, *63*, 2135–2157.
8. Tashman, D.H.; Hamouda, W. An Overview and Future Directions on Physical-Layer Security for Cognitive Radio Networks. *IEEE Netw.* **2020**, *35*, 205–211. [CrossRef]
9. Yacoub, M.D. The κ-μ distribution and the η-μ distribution. *IEEE Antennas Propag. Mag.* **2007**, *49*, 68–81. [CrossRef]
10. Tashman, D.H.; Hamouda, W. Physical-Layer Security on Maximal Ratio Combining for SIMO Cognitive Radio Networks over Cascaded κ-μ Fading Channels. *IEEE Trans. Cogn. Commun. Netw.* **2021**. [CrossRef]
11. Tashman, D.H.; Hamouda, W. Physical-Layer Security for Cognitive Radio Networks over Cascaded Rayleigh Fading Channels. In Proceedings of the GLOBECOM 2020—2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6. [CrossRef]
12. Ata, S.Ö. Secrecy performance analysis over cascaded fading channels. *IET Commun.* **2019**, *13*, 259–264. [CrossRef]
13. Eshteiwi, K.; Kaddoum, G.; Selim, B.; Gagnon, F. Impact of Co-Channel Interference and Vehicles as Obstacles on Full-Duplex V2V Cooperative Wireless Network. *IEEE Trans. Veh. Technol.* **2020**, *69*, 7503–7517. [CrossRef]
14. Ghareeb, I.; Tashman, D. Statistical analysis of cascaded Rician fading channels. *Int. J. Electron. Lett.* **2018**, *8*, 46–59. [CrossRef]
15. Ata, S.Ö. Physical layer security over cascaded Rayleigh fading channels. In Proceedings of the 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, Turkey, 2–5 May 2018; pp. 1–4. [CrossRef]

16. Ata, S.Ö. Secrecy Performance Analysis Over Double Nakagami-m Fading Channels. In Proceedings of the 2018 41st International Conference on Telecommunications and Signal Processing (TSP), Athens, Greece, 4–6 July 2018; pp. 1–4. [CrossRef]
17. Kong, L.; Kaddoum, G.; da Costa, D.B. Cascaded $\alpha - \mu$ Fading Channels: Reliability and Security Analysis. *IEEE Access* **2018**, *6*, 41978–41992. [CrossRef]
18. Singh, R.; Rawat, M. Unified Analysis of Secrecy Capacity Over N∗Nakagami Cascaded Fading Channel. In Proceedings of the 2018 18th International Symposium on Communications and Information Technologies (ISCIT), Bangkok, Thailand, 26–29 September 2018; pp. 422–427. [CrossRef]
19. Kong, L.; Ai, Y.; He, J.; Rajatheva, N.; Kaddoum, G. Intercept Probability Analysis over the Cascaded Fisher-Snedecor $\mathcal{F}$ Fading Wiretap Channels. In Proceedings of the 2019 16th International Symposium on Wireless Communication Systems (ISWCS), Oulu, Finland, 27–30 August 2019; pp. 672–676. [CrossRef]
20. Tashman, D.H.; Hamouda, W.; Dayoub, I. Secrecy Analysis Over Cascaded $\kappa - \mu$ Fading Channels With Multiple Eavesdroppers. *IEEE Trans. Veh. Technol.* **2020**, *69*, 8433–8442. [CrossRef]
21. Jia, S.; Zhang, J.; Zhao, H.; Zhang, R. Relay Selection for Improved Security in Cognitive Relay Networks With Jamming. *IEEE Wireless Commun. Lett.* **2017**, *6*, 662–665. [CrossRef]
22. Wang, H.; Wang, C.; Ng, D.W.K.; Lee, M.H.; Xiao, J. Artificial Noise Assisted Secure Transmission for Distributed Antenna Systems. *IEEE Trans. Signal Process.* **2016**, *64*, 4050–4064. [CrossRef]
23. Zhou, X.; McKay, M.R. Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3831–3842. [CrossRef]
24. Goel, S.; Negi, R. Secret communication in presence of colluding eavesdroppers. In Proceedings of the MILCOM 2005—2005 IEEE Military Communications Conference, Atlantic City, NJ, USA, 17–20 October 2005; Volume 3, pp. 1501–1506. [CrossRef]
25. Jiang, K.; Jing, T.; Huo, Y.; Zhang, F.; Li, Z. SIC-Based Secrecy Performance in Uplink NOMA Multi-Eavesdropper Wiretap Channels. *IEEE Access* **2018**, *6*, 19664–19680. [CrossRef]
26. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*; Academic Press: Cambridge, MA, USA, 2007.
27. Milisic, M.; Hamza, M.; Hadzialic, M. Outage and symbol error probability performance of L-branch maximal-ratio combiner for generalized κ-μ fading. In Proceedings of the 2008 50th International Symposium ELMAR, Borik Zadar, Croatia, 10–12 September 2008; Volume 1, pp. 231–236.
28. Adamchik, V.; Marichev, O. The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system. In Proceedings of the International Symposium on Symbolic and Algebraic Computation, Tokyo, Japan, 20–24 August 1990; pp. 212–224.
29. Kamel, M.; Hamouda, W.; Youssef, A. Physical Layer Security in Ultra-Dense Networks. *IEEE Commun. Lett.* **2017**, *6*, 690–693. [CrossRef]
30. Moualeu, J.M.; Hamouda, W. On the Secrecy Performance Analysis of SIMO Systems Over κ-μ Fading Channels. *IEEE Commun. Lett.* **2017**, *21*, 2544–2547. [CrossRef]
31. Proakis, J.; Salehi, M. *Digital Communications*, 5th ed.; McGraw-Hill: New York, NY, USA, 2008.
32. Mathai, A.M. *A Handbook of Generalized Special Functions for Statistical and Physical Sciences*; Oxford University Press: Oxford, MI, USA, 1993.
33. Chergui, H.; Benjillali, M.; Saoudi, S. Performance Analysis of Project-and-Forward Relaying in Mixed MIMO-Pinhole and Rayleigh Dual-Hop Channel. *IEEE Commun. Lett.* **2016**, *20*, 610–613. [CrossRef]
34. Prudnikov, A.; Brychkov, Y.; Marichev, O. *Integrals Series: More Special Functions, Volume III of Integrals and Series*; Gordon and Breach Science Publishers: New York, NY, USA, 1990.
35. Singh, A.; Bhatnagar, M.R.; Mallik, R.K. Secrecy Outage of a Simultaneous Wireless Information and Power Transfer Cognitive Radio System. *IEEE Wirel. Commun. Lett.* **2016**, *5*, 288–291. [CrossRef]
36. Su, R.; Wang, Y.; Sun, R. Destination-assisted jamming for physical-layer security in SWIPT cognitive radio systems. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6. [CrossRef]
37. Haenggi, M. On distances in uniformly random networks. *IEEE Trans. Inf. Theory* **2005**, *51*, 3584–3586. [CrossRef]