mathematics

MDPI

Article

On the Physical Layer Security Peculiarities of Wireless Communications in the Presence of the Beaulieu-Xie Shadowed Fading

Aleksey S. Gvozdarev * and Tatiana K. Artemova

Department of Intelligent Radiophysical Information Systems (IRIS), P.G. Demidov Yaroslavl State University, 150003 Yaroslavl, Russia

* Correspondence: asg.rus@gmail.com

Abstract: The article presents an analysis of the physical layer security of a wireless communication system functioning in the presence of multipath fading and a wiretap. Under the assumption of the equal propagation conditions (both for the legitimate receiver and the eavesdropper) described by the shadowed Beaulieu–Xie model, a closed-form expression for the secrecy outage probability was derived. The correctness of the obtained expression was numerically verified via comparison with the direct numerical integration. The truncated version of the obtained expression was analyzed for various channel parameters to establish the requirements for numerically efficient implementation (in terms of the number of summands delivering the desired precision). An in-depth study of the secrecy outage probability dependence from all the possible channel parameters for different fading scenarios was performed, including heavy fading and light fading, with and without strong dominant and multipath components. The performed research demonstrated the existence of the secrecy outage probability non-uniqueness with the respect to the average signal-to-noise ratio in the main channel and the relative distance between the legitimate and wiretap receivers.

Keywords: fading channel; shadowed Beaulieu–Xie; physical layer security; secrecy outage probability

MSC: 94A40; 94A05

Citation: Gvozdarev, A.S.; Artemova, T.K. On the Physical Layer Security Peculiarities of Wireless Communications in the Presence of the Beaulieu-Xie Shadowed Fading. *Mathematics* **2022**, *10*, 3724. https://doi.org/10.3390/math10203724

Academic Editors: Zhongyun Hua and Yushu Zhang

Received: 31 August 2022
Accepted: 7 October 2022
Published: 11 October 2022

1. Introduction

With the ever-increasing number of wireless communication technologies, the problem of personal data security is of great importance. Classically, this has been solved via coding and ciphering usually employed at the upper layer of the protocol stack [1], but starting from the mid-2000s, physical layer security (PLS) algorithms [2,3] have gained specific ground. Not opposing the classical approach, but rather assisting it, they help to exploit the specific traits of the physical wireless propagation phenomena to increase the security of the communication link.

Dating back to the pioneering work [4], the communication link between the transmitter and the legitimate receiver is assumed to be accompanied by the passive wiretap link. From a practical perspective, in the case of wireless links, one of the most critical situations occurs when the wiretap device is subtly present nearby the receiver. In this case, the propagation conditions can be assumed equal for both of the devices and the channels exhibit physical and statistical symmetry. Later, we will resort to this case as "the symmetric communication system with a wiretap". Since we are mainly after legitimate link security maximization, the general goal of PLS algorithms can be regarded as breaking this symmetry in favor of the main link (leading to asymmetry in the results). At this state, it is evident that the PLS heavily relies upon the statistical description of the channel used. Thus, the more profound the model, the better its predictive capabilities, and the higher the adequacy of the expected security.

Nowadays, alongside the classical channel models, such as Rayleigh [5], Rice [6], Nakagami-m [6], log-normal [7], Hoyt [8], Weibull [9], which are commonly limited in applicability, the so-called generalized models have gained wide acceptance: generalized gamma [10], generalized K [11], $\alpha - \mu$ [12], $\kappa - \mu$ [13], $\kappa - \mu$ shadowed [14], fluctuating Beckmann [15], Beaulieu–Xie [16], and the combination of those channels [17]. At the same time, the increasing complexities of the novel models have led to the loss of simplicity in mathematical derivations. Recently, a new model (shadowed Beaulieu–Xie [18]) was proposed; it generalizes a wide range of simplified ones (allowing to derive closed-form representations).

The shadowed Beaulieu–Xie fading model was initially proposed in [18], where the statistical and physical models were presented, and several statistical functions were derived: an envelope probability density and cumulative distribution function, characteristic and moment-generating functions, and arbitrary-order moments. By relating the envelope probability functions with that of the instantaneous power, the expressions for the outage probability and the bit error probability for coherent/non-coherent binary frequency shift keying modulations were derived. Later on, in [16], the capacity analysis was carried out and the error rate analysis for various modulations was performed in [19]. In [20], an alternative expression for the moment-generating function of the instantaneous signal-to-noise ratio was proposed and applied to the derived average probability of the energy-based detection, receiver operating characteristic, and area under its curve. To date, the physical layer security analysis is absent. Although such an analysis was performed for the classical Beaulieu–Xie channel model (see [21]), the way the shadowing was introduced in [18] prevents a direct derivation of secrecy metrics (for instance, the secrecy outage probability (SOP)) for a shadowed channel from the results obtained in [21]. A simple attempt was performed by the authors in [22], where a numerical analysis was executed for only a single fading scenario corresponding to the experimental results given in [18], which demonstrate some existing peculiarities of the shadowed Beaulieu–Xie model SOP, but no profound analysis is present.

Thus, motivated by the problem stated above, the present research performs the closed-form analysis of the secrecy outage probability in the presence of multipath fading represented by the shadowed Beaulieu–Xie model. The major contributions of this work can be summarized as follows:

- A closed-form expression was derived for the secrecy outage probability of a symmetric wireless wiretap system functioning in the presence of multipath fading subjected to the shadowed Beaulieu–Xie model.
- A numerical simulation of the obtained expression was performed: *(a)* to demonstrate the correctness of the analytical work and *(b)* to establish the specifications required for numerical implementation (i.e., the number of summands in the truncated version of the derived solution) for various channel parameters.
- A thorough analysis of the secrecy outage probability dependence from all possible channel parameters for different fading scenarios: heavy fading and light fading, with and without strong dominant and multipath components.
- A discovered non-uniqueness of the secrecy outage probability with respect to the average signal-to-noise ratio and relative distance between the legitimate and wiretap receivers from the transmitter.

The remainder of the paper is organized as follows: Section 2 provides some preliminary results of the assumed: *(a)* symmetric wireless wiretap system and its description in terms of the average and instantaneous signal-to-noise ratios (SNR) for the main and the wiretap links, *(b)* secrecy outage probability as the metric used to quantify the security of the communication process, and *(c)* statistical channel models for both links; Section 3 derives the closed-form expression of the SOP and studies the aspects of its numerical implementations; Section 4 presents a thorough numerical analysis of the derived expression depending on various channel parameter values; the conclusions are drawn in Section 5.

2. The Assumed Model Description

2.1. System Model

In accordance with the classical Wyner model [4], the assumed SISO (single input single output) communication system is comprised of the main (further denoted by the index "M") wireless transmission channel between the transmitter (Alice) and the legitimate recipient (Bob), and the wiretap channel (further denoted by the index "W"), formed between the transmitter and eavesdropper (Eve). The elements of the message $x(j)$, $j = 1, \ldots, n$, (n—the length of the code word) are transmitted through a multipath fading channel and sensed simultaneously by Bob ($y_M(j)$) and Eve ($y_W(j)$). In this case, the mathematical model of the system for the *jth* symbol being transmitted is described by the expressions:

$$\begin{cases} y_M(j) = h_M(j)x(j) + n_M(j), \\ y_W(j) = h_W(j)x(j) + n_W(j). \end{cases} \tag{1}$$

Here, it is assumed that both legal and wiretap receptions are conducted by the presence of the zero-mean complex Gaussian noise ($n_M(j)$ and $n_W(j)$, respectively), and the transmission coefficients ($h_M(j)$ and $h_W(j)$) are stochastic with arbitrary distributions in a general case, and will be defined specifically for the problem under analysis in Section 2.3.

With the fixed transmission/reception methods and signal processing algorithms, the values of the transmission coefficients $h_M(j)$ and $h_W(j)$ are determined by the total combination of physical propagation phenomena: the transmitter's angle spectrum, attenuation, and diffraction on various obstacles along various paths, various re-reflections from the underlying surface and nearby objects, and energy losses during propagation. Since most of the factors are random, the expected communication link secrecy will fluctuate.

In the current study, we will adopt the following assumptions about the channels' properties:

1. The main and the wiretap channels are considered statistically independent.
2. Both channels are described by the same generalized model with the same sets of model parameters.
3. The security analysis of the considered communication systems is performed for the critically important case when the legitimate and wiretap receivers are located close to each other. This corresponds to the similarity of the signal propagation conditions in both channels and, consequently, the proximity of the values of the model parameters.
4. The transmission coefficients are considered constant over the duration interval of the message, i.e., $h_M(j) \approx h_M$ and $h_W(j) \approx h_W$ [5], which corresponds to the typical case of slow fading or, equivalently, channels that are quasi-static over the time interval under consideration.

The signal receptions in the presence of noise in the main channel and the wiretap channel are characterized by instantaneous signal-to-noise ratios:

$$\begin{cases} \gamma_M(j) = \dfrac{P|h_M(j)|^2}{\sigma_M^2} = \dfrac{P|h_M|^2}{\sigma_M^2} = \gamma_M, \\ \gamma_W(j) = \dfrac{P|h_W(j)|^2}{\sigma_W^2} = \dfrac{P|h_W|^2}{\sigma_W^2} = \gamma_W, \end{cases} \tag{2}$$

where $\sigma_M^2 and\ \sigma_W^2$ represent the noise power in each channel, P is the average power of the transmitter, and the second equality takes into account the quasi-static nature of the channels in accordance with the fourth of the above assumptions.

Due to the stochastic nature of (2), the instantaneous signal-to-noise ratios (2) are mainly described in terms of their average values (for the main channel and the wiretap channel), and for further analysis, will act as independent parameters of the system model:

$$\begin{cases} \bar{\gamma}_M(j) = \dfrac{P\mathbb{E}\left\{|h_M(j)|^2\right\}}{\sigma_M^2} = \dfrac{P\mathbb{E}\left\{|h_M|^2\right\}}{\sigma_M^2} = \bar{\gamma}_M, \\ \bar{\gamma}_W(j) = \dfrac{P\mathbb{E}\left\{|h_W(j)|^2\right\}}{\sigma_W^2} = \dfrac{P\mathbb{E}\left\{|h_W|^2\right\}}{\sigma_W^2} = \bar{\gamma}_W, \end{cases} \tag{3}$$

here $\mathbb{E}\{\cdot\}$ is the expectation operator.

Due to the propagation attenuation of the signal (as a result of energy dissipation during the expansion of the wavefront with the distance from the source, as well as at scattering or absorption inside obstacles) the communication system must also be characterized by the distances from the transmitter to the legitimate receiver (d_M) and the wiretap receiver (d_W).

Further on, the propagation medium is characterized with the help of the so-called path loss exponent [23]. Since it is a random variable, its effective value α is used (for example, $\alpha = 2$ for propagation in free space without fading).

Assuming that the propagation conditions in both channels are similar, the average values of the SNR can be considered inversely proportional to the distances from the transmitter to the receiver with the same power α: $\bar{\gamma}_M \sim 1/d_M^\alpha$, $\bar{\gamma}_W \sim 1/d_W^\alpha$ [5]:

$$\frac{\bar{\gamma}_M}{\bar{\gamma}_W} = \left(\frac{d_W}{d_M}\right)^\alpha. \tag{4}$$

Therefore, under the assumed conditions, we will consider four parameters of the communication system model: the SNR in the main channel $\bar{\gamma}_M$ (which can be controlled, for example, by changing the processing algorithm in a legitimate receiver), the SNR in the wiretap channel $\bar{\gamma}_W$ (which participants in a legitimate link session cannot control), the average value of the path loss exponent α and the ratio of the distances from the transmitter to the wiretap and legitimate receivers d_W/d_M.

2.2. Secrecy Metric

For further analysis, it is important to define the metric that quantifies the level of the communication link secrecy. Among the plethora of such metrics (see, for instance, [24–28]) one of the most prominent roles (in various applications) is given to the secrecy outage probability [29–33]. Classically it is defined as the probability that the instantaneous capacity C falls below some pre-specified threshold value C_{th}:

$$\begin{aligned} P_{out}(C_{th}) &= \mathbb{P}(C < C_{th}) = \mathbb{P}\Big(\gamma_M < (1+\gamma_W)2^{C_{th}} - 1\Big) = \\ &= \int_0^\infty \int_0^{(1+z_W)2^{C_{th}}-1} f_{\gamma_M,\gamma_W}(z_M, z_W)\mathrm{d}z_M\mathrm{d}z_W, \end{aligned} \tag{5}$$

where the second equality follows from the definition of the secrecy capacity [5].

2.3. Fading Channel Model

In this state, it is evident that for a fading channel, SOP heavily relies on the channel model. Thus, as mentioned earlier, it is important that such a model be complex enough to incorporate most of the physically meaningful effects, and at the same time can yield closed-form results. Within the research, we will adopt the shadowed Beaulieu–Xie channel model [18,34], which defines the probability density function of the instantaneous signal-to-noise ratio in the following form:

$$f_{\gamma_i}(z_i) = \frac{e^{-\frac{m_X(\Omega_X+\Omega_Y)}{\bar{\gamma}_i\Omega_X}z_i}}{\Gamma(m_X)\sqrt{\frac{z_i\bar{\gamma}_i}{\Omega_X+\Omega_Y}}}\left(\frac{m_X}{\Omega_X}\right)^{m_X}\left(\frac{z_i(\Omega_X+\Omega_Y)}{\bar{\gamma}_i}\right)^{m_X-\frac{1}{2}}\left(\frac{m_Y\Omega_X}{m_Y\Omega_X+m_X\Omega_Y}\right)^{m_Y}\times$$
$$\times {}_1F_1\left(m_Y; m_X; \frac{m_X^2(\Omega_X+\Omega_Y)\Omega_Y}{\bar{\gamma}_i\Omega_X(m_Y\Omega_X+m_X\Omega_Y)}z_i\right), \quad (6)$$

here, the index $i = \{M; W\}$ enumerates the channel, with index M denoting the main and W the wiretap channels, respectively; $\bar{\gamma}_i$ stands for the average signal-to-noise ratio in each channel, ${}_1F_1(\cdot)$ is the confluent hypergeometric function [35], and $\Gamma(\cdot)$ is the Euler gamma function [35]. The model is parameterized with four characteristics: m_X and m_Y, which define the shadowing coefficients of the overall and dominant components; Ω_X and Ω_Y, which define the energy of the non-line-of-sight (NLoS) and line-of-sight (LoS) components respectively.

Further on, we will assume only the case of the symmetric wiretap, when the main and the wiretap channels have the same parameters, thus m_X, m_Y, Ω_X, and Ω_Y will not be indexed with $i = \{M; W\}$, contrary to the signal-to-noise ratios (instantaneous and average). This choice corresponds to the practical situation when the eavesdropper is located nearby the legitimate receiver, which is by far one of the most important for indoor communications with a crowded environment.

Thus, it is required to derive the closed-form representation of the assumed metric (i.e., SOP) (5) within the framework of the adopted symmetric communication system (1) with a wiretap for the case of shadowed Beaulieu–Xie fading channel models (6).

3. Derived Closed-Form Results

3.1. Secrecy Outage Probability Derivation

To evaluate the closed-form expression for the SOP, it can be noticed that due to the independence of the main and the wiretap channels, their joint probability density function can be factorized, i.e., $f_{\gamma_M,\gamma_W}(z_1, z_2) = f_{\gamma_M}(z_1)f_{\gamma_W}(z_2)$.

Thus, combining SOP (5) with the assumed channel models (6) yields:

$$P_{out}(C_{th}) = \int_0^\infty \int_0^{(1+z_W)2^{C_{th}}-1} f_{\gamma_M}(z_M)f_{\gamma_W}(z_W)\mathrm{d}z_M\mathrm{d}z_W = \frac{\left(\frac{m_Y\Omega_X}{m_Y\Omega_X+m_X\Omega_Y}\right)^{2m_Y}\left(\frac{m_X}{\Omega_X}(\Omega_X+\Omega_Y)\right)^{2m_X}}{\Gamma^2(m_X)\bar{\gamma}_M^{m_X}\bar{\gamma}_W^{m_X}}\times$$
$$\times \int_0^\infty \int_0^{(1+z_W)2^{C_{th}}-1} z_W^{m_X-1}z_M^{m_X-1}e^{-\frac{m_X(\Omega_X+\Omega_Y)}{\bar{\gamma}_W\Omega_X}z_W}{}_1F_1\left(m_Y; m_X; \frac{m_X^2(\Omega_X+\Omega_Y)\Omega_Y}{\bar{\gamma}_M\Omega_X(m_Y\Omega_X+m_X\Omega_Y)}z_M\right)\times$$
$$\times e^{-\frac{m_X(\Omega_X+\Omega_Y)}{\bar{\gamma}_M\Omega_X}z_M}{}_1F_1\left(m_Y; m_X; \frac{m_X^2(\Omega_X+\Omega_Y)\Omega_Y}{\bar{\gamma}_W\Omega_X(m_Y\Omega_X+m_X\Omega_Y)}z_W\right)\mathrm{d}z_M\mathrm{d}z_W. \quad (7)$$

At this point, one can use the classical series expansion of the confluent hypergeometric function ${}_1F_1(\cdot)$ (see Equation (13.2.2) in [35]):

$${}_1F_1(a, b, z) = \sum_{s=0}^{\infty}\frac{(a)_s}{(b)_s s!}z^s, \quad (8)$$

where $(\cdot)_s$ is the Pochhammer symbol [35].

Rearranging the terms and switching the order of summation and integration operation delivers:

$$P_{out}(C_{th}) = \frac{\left(\frac{m_Y\Omega_X}{m_Y\Omega_X+m_X\Omega_Y}\right)^{2m_Y}\left(\frac{m_X}{\Omega_X}(\Omega_X+\Omega_Y)\right)^{2m_X}}{\Gamma^2(m_X)\bar{\gamma}_M^{m_X}\bar{\gamma}_W^{m_X}}\sum_{p=0}^{\infty}\sum_{q=0}^{\infty}\frac{(m_Y)_q}{(m_X)_q}\frac{(m_Y)_p}{(m_X)_p}\frac{\left(\frac{m_X^2(\Omega_X+\Omega_Y)\Omega_Y}{\Omega_X(m_Y\Omega_X+m_X\Omega_Y)}\right)^{p+q}}{q!p!\bar{\gamma}_W^p\bar{\gamma}_M^q}\times$$
$$\times\int_0^{\infty} z_W^{m_X+p-1}e^{-\frac{m_X(\Omega_X+\Omega_Y)}{\bar{\gamma}_W\Omega_X}z_W}\left\{\int_0^{(1+z_W)2^{C_{th}}-1} z_M^{m_X+q-1}e^{-\frac{m_X(\Omega_X+\Omega_Y)}{\bar{\gamma}_M\Omega_X}z_M}\mathrm{d}z_M\right\}\mathrm{d}z_W. \quad (9)$$

To evaluate the inner integral, one can apply the definition of the lower incomplete gamma function (see Equation (8.2.1) in [35]):

$$\gamma(n+1,z) = \int_0^z t^n e^{-t}\mathrm{d}t = \quad (10)$$
$$= n!\left(1-e^{-z}\sum_{k=0}^{n}\frac{z^k}{k!}\right), \quad (11)$$

where the second equality follows from the series expansion of $\gamma(a,z)$ (see Equations (8.4.7) and (8.4.11) in [35]).

Let us combine (9) with (11) and simplify the obtained expression with the help of the following identities:

$$\frac{1}{(m_X)_p}\Gamma(m_X+p) = \Gamma(m_X), \quad (12)$$

$$\sum_{p=0}^{\infty}\frac{(m_Y)_p}{p!}\left(\frac{m_X\Omega_Y}{(m_Y\Omega_X+m_X\Omega_Y)}\right)^p = {}_2F_1\left(m_Y,b\,;\,b\,;\frac{m_X\Omega_Y}{(m_Y\Omega_X+m_X\Omega_Y)}\right) =$$
$$= \left(1-\frac{m_X\Omega_Y}{(m_Y\Omega_X+m_X\Omega_Y)}\right)^{-m_Y}, \quad (13)$$

where (12) follows from the definition of the Pochhammer function [35], and (13) from the definition of the Gauss hypergeometric function (see Equation (15.4.6) in [35]).

To resolve the remaining integral over z_W one can make use of the Tricomi confluent hypergeometric function definition (see Equation (13.4.4) in [35]):

$$U(a,b,z) = \frac{1}{\Gamma(a)}\int_0^{\infty} e^{-zt}t^{a-1}(1+t)^{b-a-1}\mathrm{d}t, \quad (14)$$

which is valid when $\Re a > 0$ and $|\arg z| < \pi/2$ (it can be verified that those conditions are satisfied), thus delivering the following form of the secrecy outage capacity:

$$P_{out}(C_{th}) = 1 - \frac{\left(\frac{2^{C_{th}}-1}{2^{C_{th}}}\right)^{m_X}\left(\frac{m_Y\Omega_X}{m_Y\Omega_X+m_X\Omega_Y}\right)^{2m_Y}}{\left(\frac{m_X}{\bar{\gamma}_W\Omega_X}(\Omega_X+\Omega_Y)\right)^{-m_X}}e^{-\frac{m_X}{\bar{\gamma}_M\Omega_X}(\Omega_X+\Omega_Y)\left(2^{C_{th}}-1\right)}\times$$
$$\times\sum_{p=0}^{\infty}\sum_{q=0}^{\infty}\frac{(m_Y)_q(m_Y)_p}{q!p!\bar{\gamma}_W^p\bar{\gamma}_M^q}\frac{\left(\frac{m_X^2(\Omega_X+\Omega_Y)\Omega_Y}{\Omega_X(m_Y\Omega_X+m_X\Omega_Y)}\right)^p}{\left(\frac{2^{C_{th}}-1}{2^{C_{th}}}\right)^{-p}}\left(\frac{m_X\Omega_Y}{m_Y\Omega_X+m_X\Omega_Y}\right)^q m_X+q-1\sum_{k=0}^{}\frac{\left[\left(\frac{m_X(\Omega_X+\Omega_Y)}{\bar{\gamma}_M\Omega_X}\right)\left(2^{C_{th}}-1\right)\right]^k}{k!}\times$$
$$\times U\left(m_X+p;m_X+p+1+k;\left(\frac{2^{C_{th}}-1}{2^{C_{th}}}\right)\left(\frac{m_X(\Omega_X+\Omega_Y)}{\Omega_X}\left(\frac{1}{\bar{\gamma}_W}+2^{C_{th}}\frac{1}{\bar{\gamma}_M}\right)\right)\right). \quad (15)$$

It is worth noting that for the obtained specific arguments of the Tricomi hypergeometric function, it can be represented in terms of the finite sum (see Equation (13.2.8) in [35]):

$$U\left(m_X+p;m_X+p+1+k;\left(\frac{2^{C_{th}}-1}{2^{C_{th}}}\right)\left(\frac{m_X(\Omega_X+\Omega_Y)}{\Omega_X}\left(\frac{1}{\bar{\gamma}_W}+2^{C_{th}}\frac{1}{\bar{\gamma}_M}\right)\right)\right)=$$
$$=\frac{\sum_{s=0}^{k}\binom{k}{s}(m_X+p)_s\left[\left(\frac{2^{C_{th}}-1}{2^{C_{th}}}\right)\left(\frac{m_X(\Omega_X+\Omega_Y)}{\Omega_X}\left(\frac{1}{\bar{\gamma}_W}+2^{C_{th}}\frac{1}{\bar{\gamma}_M}\right)\right)\right]^{-s}}{\left[\left(\frac{2^{C_{th}}-1}{2^{C_{th}}}\right)\left(\frac{m_X(\Omega_X+\Omega_Y)}{\Omega_X}\left(\frac{1}{\bar{\gamma}_W}+2^{C_{th}}\frac{1}{\bar{\gamma}_M}\right)\right)\right]^{m_X+p}}, \tag{16}$$

thus (15) can be rewritten as

$$P_{out}(C_{th})=1-\frac{\left(\frac{2^{C_{th}}-1}{2^{C_{th}}}\right)^{m_X}\left(\frac{m_Y\Omega_X}{m_Y\Omega_X+m_X\Omega_Y}\right)^{2m_Y}e^{-\frac{m_X}{\bar{\gamma}_M\Omega_X}(\Omega_X+\Omega_Y)\left(2^{C_{th}}-1\right)}\times}{\left(\frac{m_X}{\bar{\gamma}_W\Omega_X}(\Omega_X+\Omega_Y)\right)^{-m_X}}\times$$
$$\times\sum_{p=0}^{\infty}\sum_{q=0}^{\infty}\frac{(m_Y)_q(m_Y)_p}{q!p!\bar{\gamma}_W^p\bar{\gamma}_M^q}\frac{\left(\frac{m_X^2(\Omega_X+\Omega_Y)\Omega_Y}{\Omega_X(m_Y\Omega_X+m_X\Omega_Y)}\right)^p}{\left(\frac{2^{C_{th}}-1}{2^{C_{th}}}\right)^{-p}}\left(\frac{m_X\Omega_Y}{m_Y\Omega_X+m_X\Omega_Y}\right)^q\sum_{k=0}^{m_X+q-1}\frac{\left[\left(\frac{m_X(\Omega_X+\Omega_Y)}{\bar{\gamma}_M\Omega_X}\right)\left(2^{C_{th}}-1\right)\right]^k}{k!}\times$$
$$\times\frac{\sum_{s=0}^{k}\binom{k}{s}(m_X+p)_s\left[\left(\frac{2^{C_{th}}-1}{2^{C_{th}}}\right)\left(\frac{m_X(\Omega_X+\Omega_Y)}{\Omega_X}\left(\frac{1}{\bar{\gamma}_W}+2^{C_{th}}\frac{1}{\bar{\gamma}_M}\right)\right)\right]^{-s}}{\left[\left(\frac{2^{C_{th}}-1}{2^{C_{th}}}\right)\left(\frac{m_X(\Omega_X+\Omega_Y)}{\Omega_X}\left(\frac{1}{\bar{\gamma}_W}+2^{C_{th}}\frac{1}{\bar{\gamma}_M}\right)\right)\right]^{m_X+p}}. \tag{17}$$

Reorganizing the terms, and performing the summation over p, i.e.,

$$\sum_{p=0}^{\infty}\frac{(m_Y)_p(m_X+p)_s}{p!}\left[\frac{m_X\Omega_Y}{(m_Y\Omega_X+m_X\Omega_Y)\left(1+2^{C_{th}}\frac{\bar{\gamma_W}}{\bar{\gamma_W}}\right)}\right]^p=$$
$$=(m_X)_s\,{}_2F_1\left(m_Y,m_X+s;m_X;\frac{m_X\Omega_Y}{(m_Y\Omega_X+m_X\Omega_Y)\left(1+2^{C_{th}}\frac{\bar{\gamma_W}}{\bar{\gamma_W}}\right)}\right), \tag{18}$$

yields the expression for the secrecy outage probability:

$$P_{out}(C_{th})=1-e^{-\frac{m_X(\Omega_X+\Omega_Y)\left(2^{C_{th}}-1\right)}{\bar{\gamma}_M\Omega_X}}\sum_{q=0}^{\infty}\sum_{k=0}^{m_X+q-1}\sum_{s=0}^{k}\frac{(m_Y)_q}{q!}\left(\frac{m_Y\Omega_X}{m_Y\Omega_X+m_X\Omega_Y}\right)^{q+2m_Y}\times$$
$$\times\binom{k}{s}\left[\frac{\left(2^{C_{th}}-1\right)m_X(\Omega_X+\Omega_Y)}{\Omega_X}\right]^{k-s}\left(1+2^{C_{th}}\frac{\bar{\gamma_W}}{\bar{\gamma_W}}\right)^{-s-m_X}\frac{\left(2^{C_{th}}\bar{\gamma_W}\right)^s(m_X)_s}{\bar{\gamma_M}^k k!}\times$$
$$\times{}_2F_1\left(m_Y,m_X+s;m_X;\frac{m_X\Omega_Y}{(m_Y\Omega_X+m_X\Omega_Y)\left(1+2^{C_{th}}\frac{\bar{\gamma_W}}{\bar{\gamma_W}}\right)}\right). \tag{19}$$

It is worth noting that (19) is given in terms of a single infinite series (compared to (15)), which can be successfully truncated with the desired accuracy. The derived expression (19) is novel, and has not been presented in the technical scientific literature.

3.2. Derived Expression Numerical Analysis and Discussion

Although the derived expression is closed-form, from a practical point of view, it is clear that the series should be truncated. Thus, it is important to understand the number of summands required to reach the desired accuracy.

To achieve that goal and demonstrate the correctness of the derived solution, a numerical simulation was performed, and the results are illustrated in Figures 1 and 2 and Tables 1 and 2.

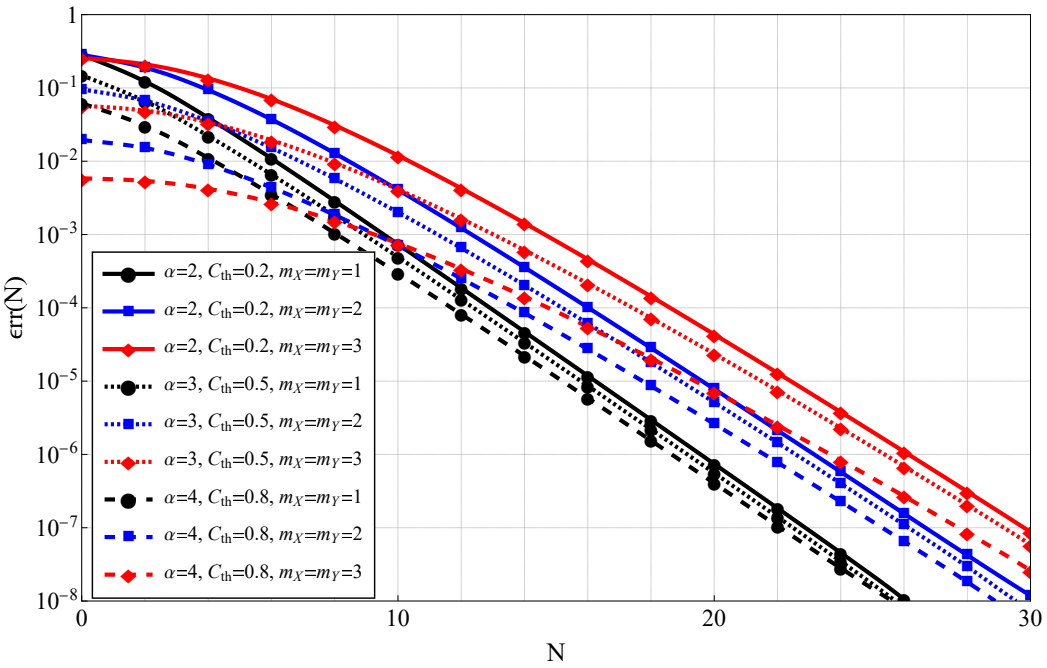

Figure 1. Error analysis of the derived expression (19) with $\Omega_X = \Omega_Y = 0$ dB, $\bar{\gamma}_M = 10$ dB and $d_W/d_M = 1$.

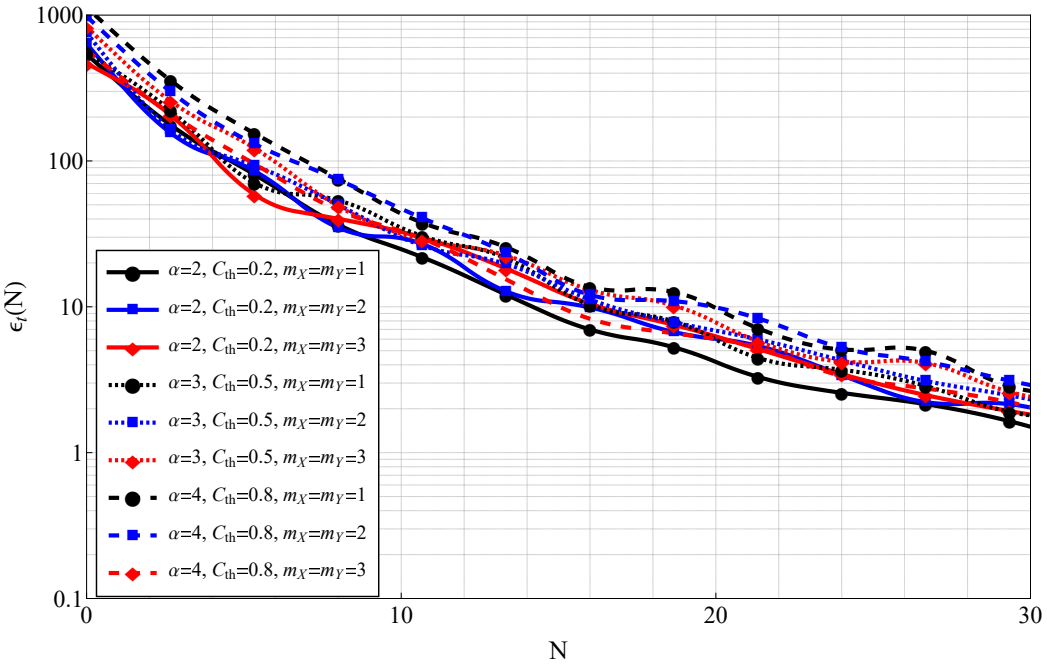

Figure 2. Computational time gain analysis of the derived expression (19) with $\Omega_X = \Omega_Y = 0$ dB, $\bar{\gamma}_M = 10$ dB and $d_W/d_M = 1$.

First, the obtained closed-form solution (19) was truncated by N terms (denoted as P_{out}^{cf}), and the calculated results for various systems and channel parameters were compared with the results obtained via brute-force numeric integration of (7) (denoted as P_{out}^{num}). The relative error $err(N) = \left| \frac{P_{out}^{num} - P_{out}^{cf}}{P_{out}^{num}} \right|$ as a function of the number of terms is presented in Figure 1 and the resultant computational speedup $\epsilon_t(N)$ (defined as the ratio between the times required to compute P_{out}^{cf} and P_{out}^{num}) is presented in Figure 2.

It can be observed that the increase in the path loss and the threshold capacity improved the residual error (see Figure 1), whereas the improvement of the shadowing conditions (greater m) impaired it. If the 1% error is tolerable then, for example, for the heavy path loss scenario with light shadowing, even the 0-term truncation gives the result. For most of the cases, 10–15 terms are enough to yield the sub-percent error.

On the other hand, the computational speedup (see Figure 2) that can be obtained with the help of the proposed solution is at least 10 times for $N \geq 14$. Moreover, it can be seen that even though $\epsilon_t(N)$ decreases as a function of N, P_{out}^{cf} is always superior over P_{out}^{num} (i.e., $\epsilon_t(N) > 1$). It should be noted that, in practice, in the sphere of wireless communications, the relative error of 10^{-8} is way below the necessity. Thus, it can be seen that depending on the desired accuracy and computational time, one can choose the number of terms, respectively.

Table 1. A comparison between the numerical and closed-form solutions for $C_{th} = 0.3$, $\bar{\gamma}_W = 10$ dB, $m_X = m_Y = 1, \Omega_X = \Omega_Y = 0$ dB with various numbers of terms N.

$\bar{\gamma}_M$, dB	P_{out}^{num}	$N = 10$	$N = 20$	$N = 30$
		P_{out}^{cf}	P_{out}^{cf}	P_{out}^{cf}
0	0.94038	0.940572	0.940381	0.94038
5	0.855632	0.855978	0.855632	0.855632
10	0.705207	0.705664	0.705208	0.705207
15	0.503409	0.503896	0.50341	0.503409
20	0.306428	0.306916	0.306428	0.306428
25	0.163436	0.163924	0.163437	0.163436
30	0.0800201	0.0805084	0.0800206	0.0800201
35	0.0373851	0.0378734	0.0373856	0.0373851
40	0.0170628	0.0175511	0.0170633	0.0170628

Table 1 presents the comparison for 10, 20, and 30 terms as functions of the average SNR in the main channel. It can be observed that although the precision drops with the increase of $\bar{\gamma}_M$, even $N = 10$ can provide three-digit precision (for reasonably high SNR $\simeq 40$ dB), and $N = 30$ delivers seven-digit precision, which is excessive for practical applications.

Limiting ourselves to $N = 20$ (yielding in most cases five-digit precision) an analysis of the fading conditions impart was performed (see Table 2).

Table 2. A comparison between numerical and closed-form solutions for $N = 20$, $\bar{\gamma}_M = \bar{\gamma}_W = 10$ dB, $\Omega_X = \Omega_Y = 0$ dB, with various C_{th} and shadowing coefficients.

C_{th}	$m_X = m_Y = 1$		$m_X = m_Y = 2$		$m_X = m_Y = 3$	
	P_{out}^{num}	P_{out}^{cf}	P_{out}^{num}	P_{out}^{cf}	P_{out}^{num}	P_{out}^{cf}
0.1	0.571434	0.571434	0.600792	0.600797	0.623793	0.623825
0.2	0.640469	0.640469	0.695150	0.695155	0.735766	0.735798
0.3	0.705207	0.705208	0.777915	0.777920	0.827489	0.827519
0.4	0.764140	0.764141	0.846028	0.846033	0.895670	0.895697
0.5	0.816242	0.816243	0.898699	0.898704	0.941763	0.941786
0.6	0.860981	0.860982	0.937004	0.937008	0.970142	0.970159
0.7	0.898269	0.898270	0.963189	0.963192	0.986044	0.986055
0.8	0.928373	0.928374	0.979962	0.979964	0.994121	0.994128
0.9	0.951825	0.951826	0.989965	0.989967	0.997806	0.997811

It was observed that the improvement in shadowing conditions (greater m_X and m_Y) impairs the precision (up to four digits), but it must be stressed that the overall values of SOP are high and such precision is more than enough. On the other hand, increasing the requirements implied on the C_{th} does not affect the quality of the obtained result.

It should be noted that in the case of a fixed number of terms, extra precision is sought, one can successfully apply well-established convergence-increasing algorithms, for instance, Shanks' transformation (see [36]).

As the result of the numerical implementation of the derived expression for various values of the channel and the system parameters, it was decided to truncate the series in (15) for further calculations by twenty terms, delivering at least five-digit precision.

4. Simulation and Results

4.1. Simulation Setup

To analyze the dependence of the secrecy outage probability on the values of the channel and system parameters, the numeric simulation was carried out.

The assumed ranges of the parameter values are presented in Table 3.

Table 3. System and channel parameters assumed for simulation.

Parameter	Parameter Value
Shadowing coefficients of the total and LoS components (m_X, m_Y)	$1 \ldots 10$
Energy of NLoS and LoS components (Ω_X, Ω_Y), dB	$-10 \ldots 10$
Average SNR for the main and the wiretap channels ($\bar{\gamma}_M, \bar{\gamma}_W$), dB	$0 \ldots 50$
The relative distance between the receiver, the eavesdropper, and the transmitter (d_W/d_M)	$0.1 \ldots 10$
Path loss exponent (α)	$1.5 \ldots 5$
Normalized threshold capacity (C_{th})	$0.01 \ldots 0.99$

Several notes should be pointed out:

- The range of path loss exponent was chosen in accordance with the existent real-life measurements performed for various scenarios [37,38].
- The threshold channel capacity corresponding to the secrecy outage was normalized by the capacity of the non-fading Gaussian channel with Gaussian input (see [5]).
- The d_W/d_M range was chosen in a way to cover the possible cases when the eavesdropper was further and closer to the transmitter compared to the main receiver.
- In accordance with [18], $2m_Y$ equals the number of LoS components; thus, the analysis was performed for the scenarios with possible multiple LoS components.

- The average SNR range was set so to account for the requirements of the shadowed Beaulieu–Xie channel modulation techniques (see [18]).

It is worth mentioning that the problem under analysis was a multiparametric one; thus, a single-argument cut of a multi-argument function (as widely used) cannot give a full description. So, for further analysis, we will resort to the contour plots that give descriptions in terms of several joint parameters.

4.2. Simulation Results and Analysis

Figures 3 and 4 demonstrate the influence of the system model parameters (the ratio of the distances d_W/d_M and the average SNR in the main channel $\bar{\gamma}_M$) on the secrecy outage probability P_{out}, depending on the channel model parameters: the average power of multipath Ω_X, line-of-sight components Ω_Y, shadowing coefficients of the overall m_X, and the line-of-sight components m_Y. Figure 3 was obtained with significant shadowing ($m_X = m_Y = 1$), and Figure 4—with weak shadowing ($m_X = m_Y = 5$). Both figures show four situations covering the most indicative combinations of the average powers of LoS and NLoS components: in the case of *a*, both components are weak ($\Omega_X = \Omega_Y = -10$ dB), in the case of *b*, multipath components predominate in the signal ($\Omega_X \gg \Omega_Y$), in the case of *c*, the line-of-sight components are strong, and multipath components are weakened ($\Omega_X \ll \Omega_Y$), and finally, in the case of *d*, both components are strong ($\Omega_X = \Omega_Y = 10$ dB). With the color scheme used, low values P_{out} (and, therefore, a greater degree of link secrecy) correspond to dark blue; high values correspond to yellow.

A comparison of Figures 3 and 4 shows that the amount of shadowing $m_X = m_Y$ has a more pronounced effect than the combination of the signal component powers Ω_X, Ω_Y. One of the main features of P_{out} is related to the size and shape of the desirable values region of the secrecy outage probability ($P_{out} < 0.2$), shown in Figures 3 and 4 by the dark blue. It contains the existing global extremum of the P_{out} with respect to the variables d_W/d_M and $\bar{\gamma}_M$. This area corresponds to the most favorable transmission in terms of security. In Figure 3 it is observed for $d_W/d_M > 8$ and $13 < \bar{\gamma}_M < 26$, and in Figure 4 it occupies a fairly significant part of the plot area: $d_W/d_M > 2.5$ and $\bar{\gamma}_M < 35$. Thus, the range of system parameters at which the secrecy outage probability will be small is narrower at lower m, i.e., in a situation of larger shadowing. This suggests that in a situation when the shadowing is large, care is needed in choosing the employed transmitting/receiving strategy, optimizing the average SNR. In addition, at small $m_X = m_Y$ a communication link becomes secure only when the wiretap receiver is removed from the legitimate one by a large distance, while at large, $m_X = m_Y$, a secure scenario, can be achieved even for the situation in which both receivers are at almost the same distance from the transmitter.

In Figure 3 for small $m_X = m_Y$, the region with $P_{out} < 0.2$ is such that for all combinations of Ω_X, Ω_Y for a fixed d_W/d_M there are two values of $\bar{\gamma}_M$ (which practically do not depend on Ω_X, Ω_Y), which means that the choice of system parameters is non-unique. For large $m_X = m_Y$, as illustrated in Figure 4, the shape of such an area changes significantly and is also dependent on Ω_X, Ω_Y. With the equal average powers of multipath components and line-of-sight components $\Omega_X = \Omega_Y$ (Figure 4a,d), there are $3 < d_W/d_M < 3.5$, which correspond to the ambiguity of the choice of $\bar{\gamma}_M$. With large differences between the power of the components, regardless of the sign, i.e., at $\Omega_X \gg \Omega_Y$ (Figure 4b) or $\Omega_X \ll \Omega_Y$ (Figure 4c), such ambiguity is not observed.

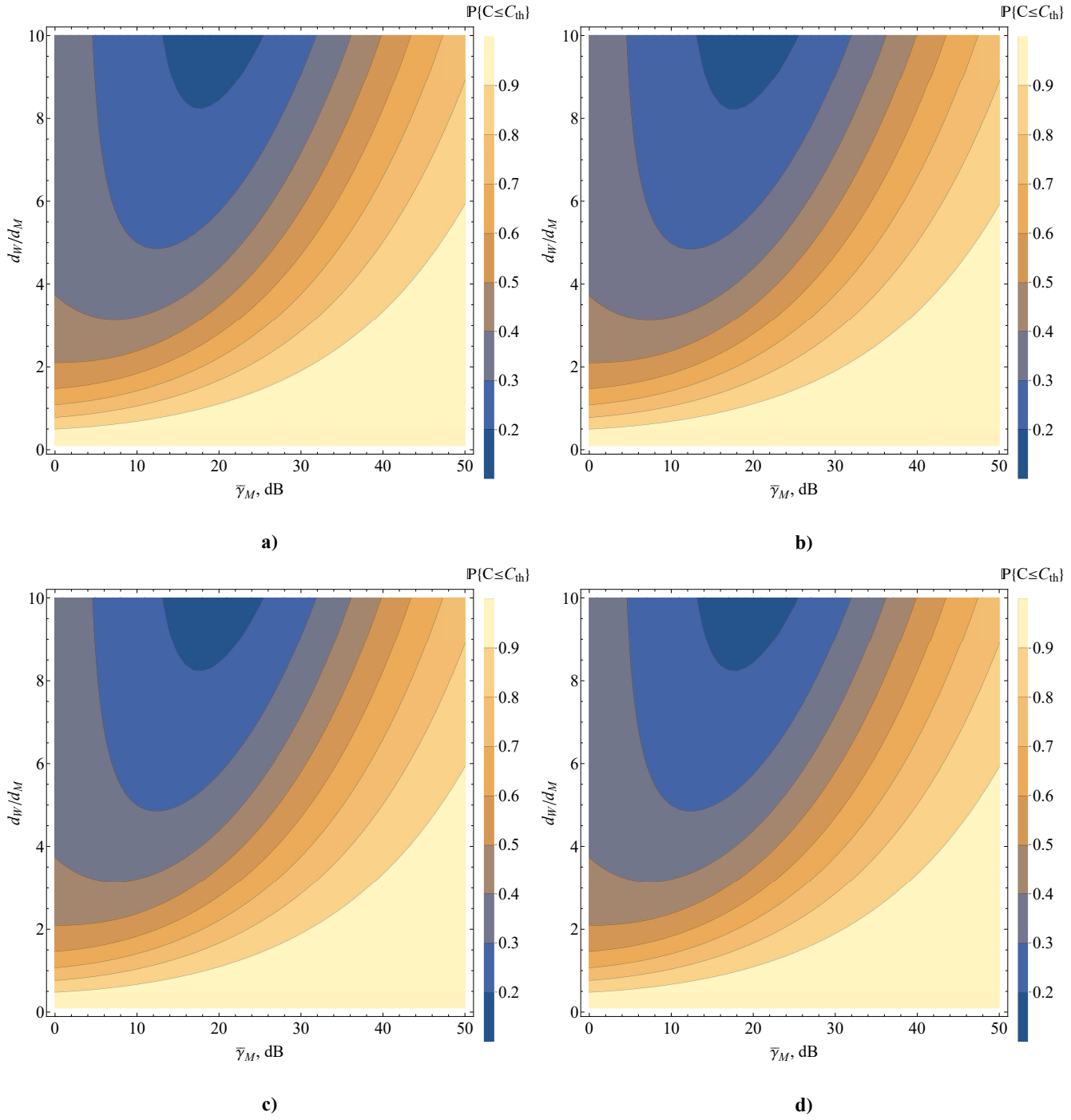

Figure 3. Secrecy outage capacity of the shadowed Beaulieu–Xie model for $m_X = 1$, $m_Y = 1$, $C_{th} = 0.5$, $\alpha = 2$ with: (**a**) $\Omega_X = -10$ dB, $\Omega_Y = -10$ dB; (**b**) $\Omega_X = 10$ dB, $\Omega_Y = -10$ dB; (**c**) $\Omega_X = -10$ dB, $\Omega_Y = 10$ dB; (**d**) $\Omega_X = 10$ dB, $\Omega_Y = 10$ dB.

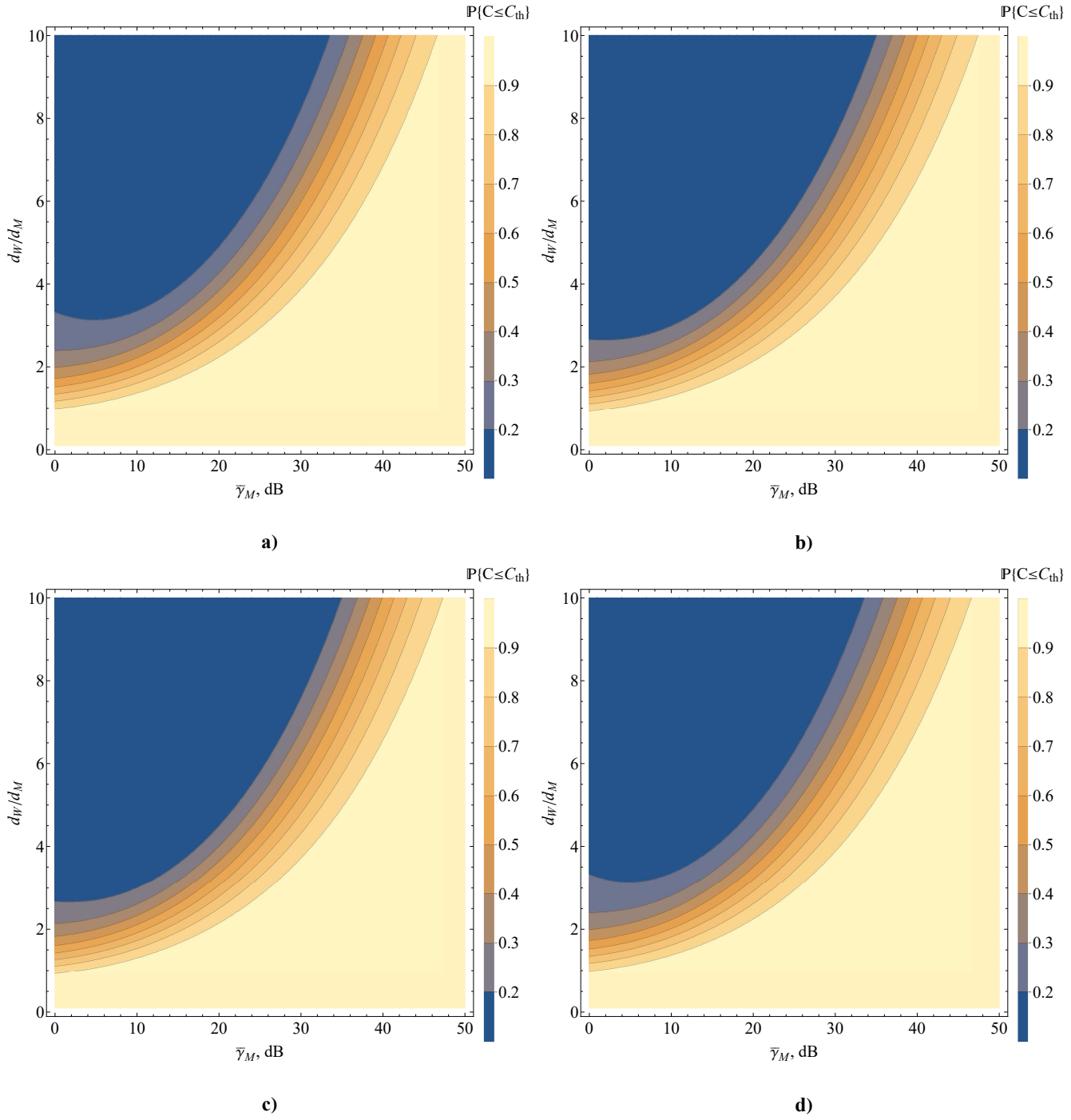

Figure 4. Secrecy outage capacity of the shadowed Beaulieu–Xie model for $m_X = 5$, $m_Y = 5$, $C_{th} = 0.5$, $\alpha = 2$ with: (**a**) $\Omega_X = -10$ dB, $\Omega_Y = -10$ dB; (**b**) $\Omega_X = 10$ dB, $\Omega_Y = -10$ dB; (**c**) $\Omega_X = -10$ dB, $\Omega_Y = 10$ dB; (**d**) $\Omega_X = 10$ dB, $\Omega_Y = 10$ dB.

Analyzing contour plots with one of the arguments being constant, one should keep in mind the relationship (4) between the parameters of the system model. With a constant ratio $d_W/d_M = const$ we have $\sqrt[\alpha]{\bar{\gamma}_M/\bar{\gamma}_W} = const$, this means that the increase in $\bar{\gamma}_M$ corresponds to either a proportional increase of $\bar{\gamma}_W$ (i.e., facilitating the reception for the wiretap receiver), or an increase in the path loss exponent α (i.e., increasing attenuation and worsening the overall signal propagation conditions). Thus, while maintaining $d_W/d_M < 3$ and d_W/d_M fixed, the increase of $\bar{\gamma}_M$ leads to the increase of P_{out}, which corresponds to the impairment of the predicted security. For the constant average main channel SNR

$\bar{\gamma}_M = const$, (4) evaluates to $\bar{\gamma}_W \left(d_W/d_M\right)^{\alpha} = const$, i.e., the increase of d_W/d_M (the withdrawal of the eavesdropper from the transmitter with a legitimate receiver being fixed) corresponds either to the reduction of $\bar{\gamma}_W$ (i.e., hardening the reception for the wiretap), or to the decrease of α (i.e., approaching the propagation conditions to the free space). Thus, while maintaining fixed $\bar{\gamma}_M$, the increase of d_W/d_M yields the reduction of P_{out}, which corresponds to the improvement of the predicted security.

The influence of the path loss exponent α on the secrecy outage probability has the following features at different relative distances from the transmitter to the wiretap and legitimate receivers (see Figure 5):

1. If the location of the eavesdropper is too close to the transmitter compared to the legitimate receiver (for example, $d_W/d_M = 0.1$ in Figure 5a), the higher the path loss exponent α, the greater the secrecy outage probability P_{out}, since in this case $\bar{\gamma}_M < \bar{\gamma}_W$ and the reception conditions for the legitimate receiver compared to the wiretap are worse, as follows from (4). In the analyzed range of parameters α and C_{th}, P_{out} does not fall below 0.96.
2. At the unit relative distances (see $d_W/d_M = 1$ in Figure 5b) the signal propagation conditions in the main and the wiretap channels are equal, as $m_X = m_Y$, $\Omega_X = \Omega_Y$ and $\bar{\gamma}_M = \bar{\gamma}_W$ from (4). Hence, the secrecy outage probability is determined primarily by the required threshold capacity C_{th}: the higher C_{th}, the more likely the loss of link secrecy.
3. Finally, in cases when the eavesdropper is further from the transmitter than the legitimate receiver (see, for instance, $d_W/d_M = 10$ in Figure 5c), with the growth of the path loss exponent α there is a confrontation between two multidirectional factors. On the one hand, the reception conditions for a legitimate receiver are improving (the inequality $\bar{\gamma}_M > \bar{\gamma}_W$ becomes stronger), on the other hand, the conditions for signal propagation are worsening due to the increase of α similarly for both receivers. This leads to the fact that the equiprobability lines run along the horizontal axis in the area $\alpha > 3$ (Figure 5c); in this region, the values of P_{out} are determined by the value of C_{th}, as in Figure 5b. Thus, the existence and the shape of the area of α and C_{th}, which provides a low secrecy outage probability, depends on the relative distance between the receivers and the transmitter.

There is no acceptable threshold capacity C_{th} (for instance, greater than 0.1) for either $d_W/d_M \approx 1$ or even $d_W/d_M < 1$ that would guarantee the required probability of $P_{out} < 0.2$. If the relative distance satisfied the condition $d_W/d_M > 8$, then, by decreasing C_{th}, it is possible to ensure a safe link with a given probability of outage, and better propagation conditions (with smaller α)—with a greater decrease in C_{th}.

Considering the influence of the channel parameters (i.e., average powers of NLoS Ω_X and LoS Ω_Y components for various combinations of shadowing conditions m_X, m_Y), demonstrated in Figure 6, it is evident that the contour lines of constant P_{out} can be approximated on a logarithmic scale as $\Omega_Y = \Omega_X + b$, where b is a constant term representing the LoS–NLoS component power imbalance. As b increases, P_{out} also increases, and the link becomes insecure. The area corresponding to the least secrecy is located in the lower right corner of the plot at any m_X, m_Y. This corresponds to scenarios $\Omega_Y < \Omega_X + b$ and even $\Omega_Y << \Omega_X + b$, which practically means that secure communication is easier to provide with strong NLoS, rather than LoS components. The specific value of the admissible power imbalance depends on the shadowing conditions of the components. The specific area of $P_{out} < 0.2$ is maximized for the case of $m_X = 1$, $m_Y = 5$ (see Figure 6b), which constitutes to the situation when security is guaranteed for the greater range of power imbalances, and minimized for the case of $m_X = 5$, $m_Y = 1$ (see Figure 6c). From the point of view of the overall area of $P_{out} < 0.2$ the situations depicted in Figure 6a,d are in between. The gradient of P_{out} is the greatest in the cases depicted in Figure 6b,d. Thus, even a small change in Ω_X, Ω_Y can cause a serious increase of P_{out} making the link not secure.

An analysis of the results obtained for varying m_X, m_Y, and distinct combinations of Ω_X, Ω_Y (see Figure 7) made it possible to conclude that in the cases of equal powers of

LoS and NLoS components (i.e., $\Omega_X = \Omega_Y = -5$ dB in Figure 7a, or $\Omega_X = \Omega_Y = 5$ dB in Figure 7c) the difference of P_{out} as a function of m_X, m_Y is almost intractable. In those cases, the area with $P_{out} < 0.1$ (where the secrecy constraints are satisfied) is concentrated where m_X, m_Y are large, which corresponds to the small overall and LoS component shadowing, and the equiprobability contours are almost parallel to the m_Y axis (thus the values m_Y do not impact) for $m_X < 4$, $m_Y > 6$ in case of $P_{out} = 0.2$ and for $m_X < 2$, $m_Y > 3$ in case of $P_{out} = 0.3$. On the other hand, for large values of m_X and small m_Y the lines of $P_{out} = const$ are almost parallel to m_X, thus m_Y does not have any impact on the link security.

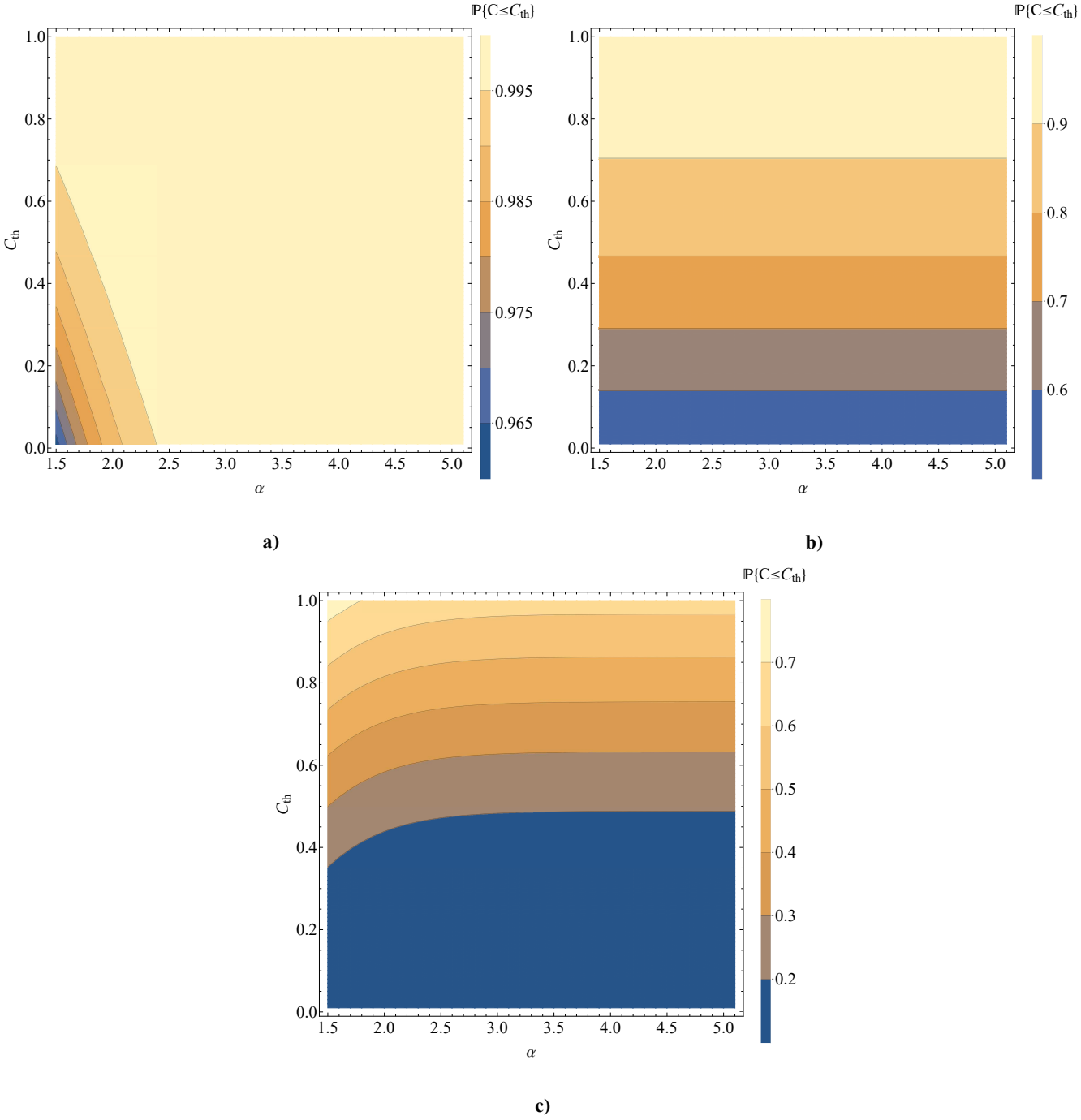

Figure 5. Secrecy outage capacity of the shadowed Beaulieu–Xie model for $m_X = 1$, $m_Y = 1$, $\Omega_X = -10$ dB, $\Omega_Y = -10$ dB, $\bar{\gamma}_M = 10$ dB with: (**a**) $d_W/d_M = 0.1$, (**b**) $d_W/d_M = 1$, and (**c**) $d_W/d_M = 10$.

For the cases of unequal LoS/NLoS powers (see Figure 7b,c), the greater impact has the part of the channel spatial structure that exhibits stronger shadowing. From the results, presented in Figure 7b, which correspond to the case with strong NLoS ($\Omega_X = 5$ dB) and weak LoS ($\Omega_Y = -5$ dB) components, it is evident that $P_{out} = const$ contours are almost parallel to the m_Y axis for arbitrary m_X, which means that it does not have any impact in those conditions. Strictly the opposite is the case with strong LoS ($\Omega_Y = 5$ dB) and weak NLoS ($\Omega_X = -5$ dB) components (see Figure 7c), when $P_{out} = const$ lines, starting from some threshold m_Y, are parallel to the m_X axis. The increase of P_{out} shifts this threshold to the region with smaller m_Y, e.g., $m_Y \approx 4$ for $P_{out} = 0.2$, and $m_Y \approx 2$ for $P_{out} = 0.3$.

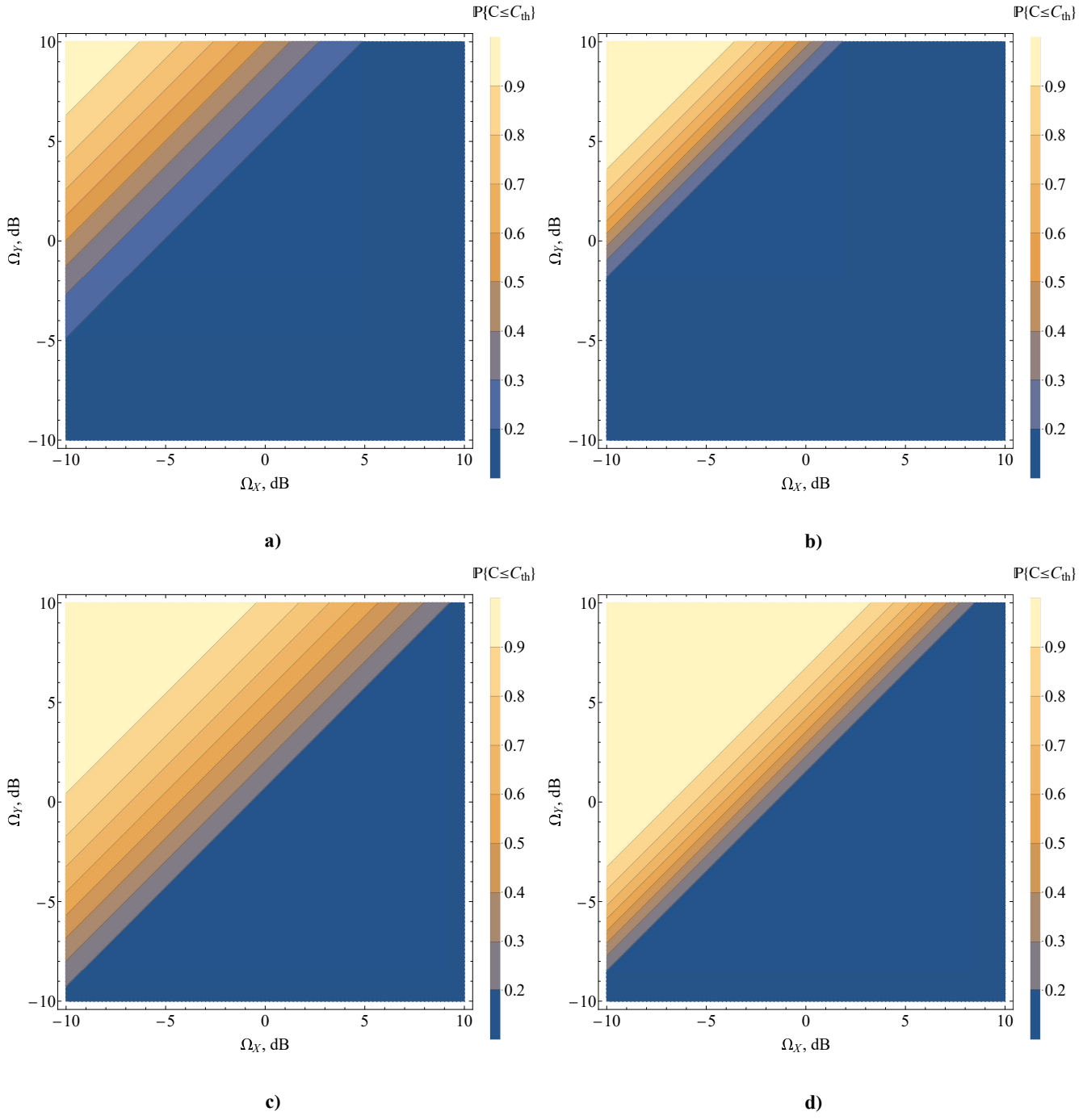

Figure 6. Secrecy outage capacity of the shadowed Beaulieu–Xie model for $d_W/d_M = 3$, $\alpha = 2$, $C_{th} = 0.1$, and $\bar{\gamma}_M = 10$ dB with: (**a**) $m_X = 1$, $m_Y = 1$, (**b**) $m_X = 1$, $m_Y = 5$, (**c**) $m_X = 5$, $m_Y = 1$, and (**d**) $m_X = 5$, $m_Y = 5$.

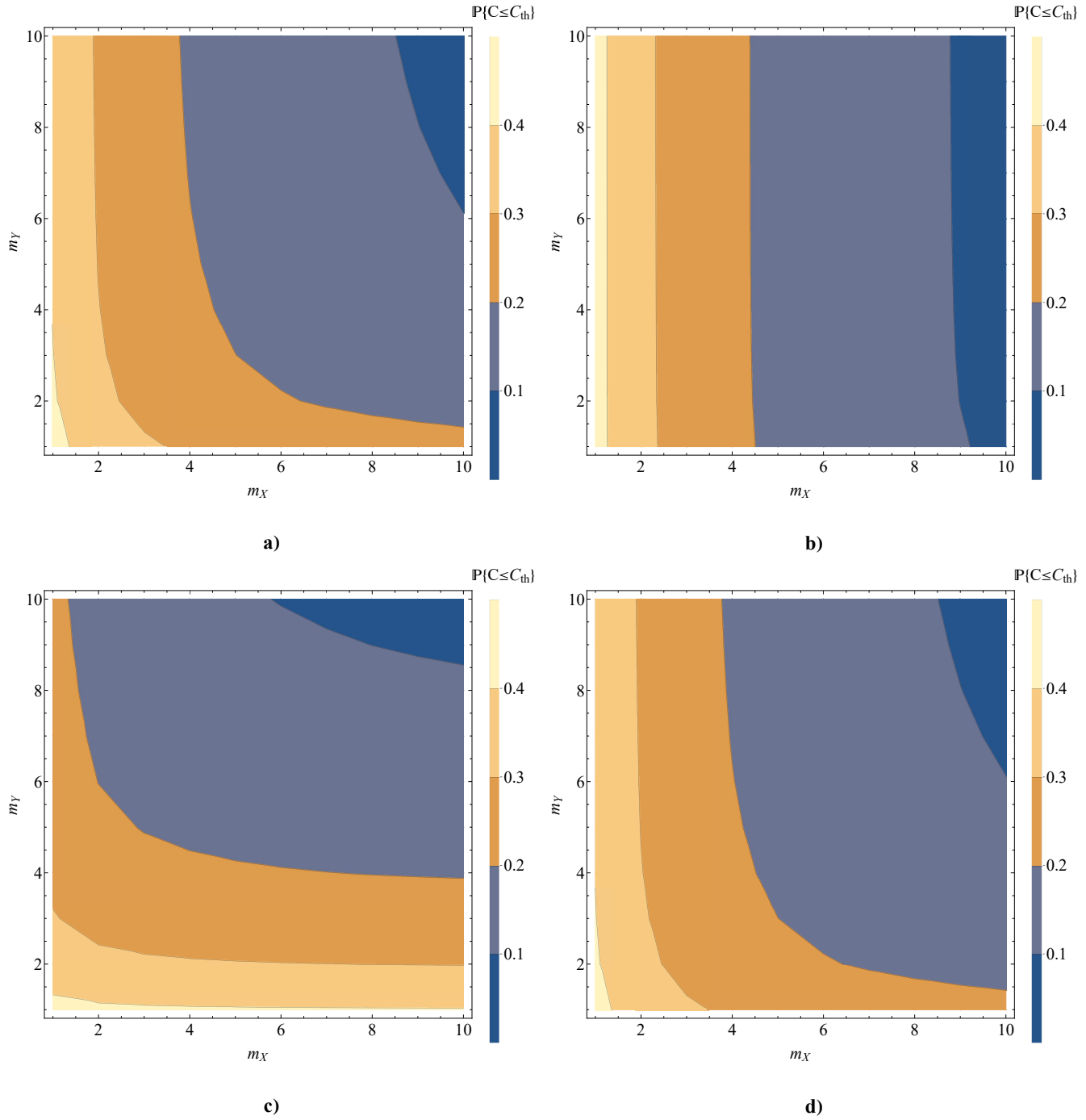

Figure 7. Secrecy outage capacity of the Beaulieu–Xie shadowed model for $d_W/d_M = 2$, $\alpha = 3$, $C_{th} = 0.5$, and $\bar{\gamma}_M = 5$ dB with: (**a**) $\Omega_X = -5$ dB, $\Omega_Y = -5$ dB; (**b**) $\Omega_X = 5$ dB, $\Omega_Y = -5$ dB; (**c**) $\Omega_X = -5$ dB, $\Omega_Y = 5$ dB; (**d**) $\Omega_X = 5$ dB, $\Omega_Y = 5$ dB.

4.3. Discussion and Analysis Summary

The performed analysis makes it possible to find specific propagation conditions (i.e., channel parameters), which deliver the desired level of link security. On the other hand, recently, a novel and very promising technology—reconfigurable intelligent surfaces [39]—demonstrated the ability of communication assistance [40,41]. Such surfaces are designed in such a way to change and control the propagation channel properties. A classic example is the controlled variation of its reflection coefficient [42], thus creating new clusters of multipath waves or suppressing the existing ones [43]. This means that the effective value of the path loss exponent, shadowing coefficients and LoS/NLoS power imbalance can be

possibly controlled or manipulated. The possible further deployment of the reconfigurable intelligent surfaces (or other technologies that can help to control channel parameters) allows us to reformulate the performed descriptive analysis into specific recommendations for communication system design.

Summarizing all of the above, several general conclusions can be drawn and recommendations can be given:

- First, the recommended values of channel parameters m_X, m_Y should constitute to the light shadowing, and the values of Ω_X, greater than that of Ω_Y (i.e., favoring the multipath components of a fading channel, rather than line-of-sight components). Second, the following system parameters are recommended: $d_W/d_M > 1$ or even $d_W/d_M >> 1$ (i.e., exploiting the situation when the legitimate receiver is closer than the eavesdropper), the values of the path loss exponent α and average signal-to-noise ratio in the main channel should correspond to the ranges, depicted in Figures 3–5, the threshold capacities C_{th} should be lowered down up to the lowest values that are still admissible for information transfer.
- The overall parameter values for which there is no way to achieve communication link secrecy corresponds to the following propagation scenarios: the eavesdropper is closer to the transmitter than the legitimate receiver (i.e., $d_W/d_M \leq 0.1$, see Figure 3a), the overall signal propagation conditions are too severe (large path loss exponent α values), large values of the average SNR in the wiretap channel $\bar{\gamma}_W$ (the wiretap receiver has an advantage over the legitimate one).
- Contour lines of the constant secrecy outage probability exhibit a specific minimum in case of heavy shadowing, i.e., small m_X, m_Y, and eavesdropper displaced at least twice further than the legitimate receiver, i.e., $d_W/d_M > 2$, see Figure 3. This results in non-uniqueness of the possible guidelines in the choice of main channel average SNR $\bar{\gamma}_M$.
- Although from the physical perspective, the meanings of several parameters are identical (m_X, m_Y and Ω_X, Ω_Y), their impacts on the P_{out} greatly differ. To reach the smaller values of P_{out}, it is desirable to have $\Omega_Y < \Omega_X$, and the overall shadowing m_X has a stronger impact, than the LoS shadowing m_Y; moreover, the cases with $m_X > 6$ are preferable, and recommendations about the choice of m_Y greatly depend on the required level of secrecy.

5. Conclusions

The presented research studies the problem of the physical layer security of a wireless communication system functioning in the presence of a multipath fading channel and a wiretap. The analysis was performed under the following assumptions: *a* the communication system was symmetric, meaning that the physical propagation conditions are equal for the legitimate receiver and the eavesdropper; *b* both channels are assumed to be statistically independent; *c* both channels are described by the shadowed Beaulieu–Xie fading model. The link secrecy was characterized by the secrecy outage probability defined for a fixed target secrecy capacity level. For the model under consideration, the closed-form expression of the SOP is presented, and its correctness is numerically verified. It is demonstrated that the proposed expression delivers practically reasonable results (in terms of the desired precision) from all the possible channel parameters. An in-depth study of the secrecy performance was carried out for all practically meaningful fading scenarios, including heavy and light fading, with and without strong dominant and multipath components. The performed research demonstrated the existence of the secrecy outage probability non-uniqueness with respect to the average signal-to-noise ratio in the main channel and the relative distance between the legitimate and wiretap receivers.

Author Contributions: Conceptualization, A.S.G.; formal analysis, A.S.G.; funding acquisition, A.S.G.; investigation, A.S.G.; methodology, A.S.G. and T.K.A.; software, A.S.G.; supervision, A.S.G.; validation, A.S.G. and T.K.A.; visualization, A.S.G.; writing—original draft preparation, A.S.G. and T.K.A.; writing—review and editing A.S.G. and T.K.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Russian Science Foundation under grant 22-29-01458 (https://rscf.ru/en/project/22-29-01458/, accessed date: 10 October 2022).

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Wang, L. *Physical Layer Security in Wireless Cooperative Networks*; Springer International Publishing: Berlin/Heidelberg, Germany, 2018. [CrossRef]
2. Bloch, M.; Barros, J. *Physical-Layer Security*; Cambridge University Press: Cambridge, UK, 2011. [CrossRef]
3. Zhou, X.; Song, L.; Zhang, Y. (Eds.) *Physical Layer Security in Wireless Communications*; CRC Press: Boca Raton, FL, USA, 2016. [CrossRef]
4. Wyner, A.D. The Wire-Tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
5. Barros, J.; Rodrigues, M.R.D. Secrecy Capacity of Wireless Channels. In Proceedings of the 2006 IEEE International Symposium on Information Theory, Seattle, WA, USA, 9–14 July 2006. [CrossRef]
6. Iwata, S.; Ohtsuki, T.; Kam, P.Y. Performance Analysis of Physical Layer Security over Rician/Nakagami-m Fading Channels. In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, NSW, Australia, 4–7 June 2017. [CrossRef]
7. Liu, X. Secrecy capacity of wireless links subject to log-normal fading. In Proceedings of the 7th International Conference on Communications and Networking in China, Kunming, China, 8–10 August 2012. [CrossRef]
8. Jameel, F.; Haider, M.A.; Butt, A.A. Physical layer security under Rayleigh/Weibull and Hoyt/Weibull fading. In Proceedings of the 2017 13th International Conference on Emerging Technologies (ICET), Islamabad, Pakistan, 27–28 December 2017. [CrossRef]
9. Liu, X. Average secrecy capacity of the Weibull fading channel. In Proceedings of the 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2016. [CrossRef]
10. Lei, H.; Gao, C.; Guo, Y.; Pan, G. On Physical Layer Security Over Generalized Gamma Fading Channels. *IEEE Commun. Lett.* **2015**, *19*, 1257–1260. [CrossRef]
11. Lei, H.; Zhang, H.; Ansari, I.S.; Gao, C.; Guo, Y.; Pan, G.; Qaraqe, K.A. Performance Analysis of Physical Layer Security Over Generalized-K Fading Channels Using a Mixture Gamma Distribution. *IEEE Commun. Lett.* **2016**, *20*, 408–411. [CrossRef]
12. Kong, L.; Tran, H.; Kaddoum, G. Performance analysis of physical layer security over α-μ fading channel. *Electron. Lett.* **2016**, *52*, 45–47. [CrossRef]
13. Bhargav, N.; Cotton, S.L.; Simmons, D.E. Secrecy Capacity Analysis Over κ-μ Fading Channels: Theory and Applications. *IEEE Trans. Commun.* **2016**, *64*, 3011–3024. [CrossRef]
14. Al-Hmood, H.; Al-Raweshidy, H. Exact closed-form capacity and outage probability of physical layer security in shadowed fading channels. *IET Commun.* **2019**, *13*, 3235–3243. [CrossRef]
15. Al-Hmood, H.; Al-Raweshidy, H. Performance Analysis of Physical-Layer Security Over Fluctuating Beckmann Fading Channels. *IEEE Access* **2019**, *7*, 119541–119556. [CrossRef]
16. Silva, H.S.; Almeida, D.B.; Queiroz, W.J.; Silva, H.T.; Fonseca, I.E.; Oliveira, A.S.; Madeiro, F. Capacity analysis of shadowed Beaulieu–Xie fading channels. *Digit. Signal Process.* **2022**, *122*, 103367. [CrossRef]
17. Bhargav, N.; Cotton, S.L. Secrecy capacity analysis for α-μ/κ-μ and κ-μ/α-μ fading scenarios. In Proceedings of the 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, Spain, 4–8 September 2016. [CrossRef]
18. Olutayo, A.; Cheng, J.; Holzman, J.F. A New Statistical Channel Model for Emerging Wireless Communication Systems. *IEEE Open J. Commun. Soc.* **2020**, *1*, 916–926. [CrossRef]
19. Hawaibam, S.; Singh, A.D. Error Rate Analysis of Different Modulation Schemes Over Shadowed Beaulieu-Xie Fading Channels. *IETE J. Res.* **2022**, 1–7. [CrossRef]
20. Gvozdarev, A.S. A Novel Unified Framework for Energy-Based Spectrum Sensing Analysis in the Presence of Fading. *Sensors* **2022**, *22*, 1742. [CrossRef] [PubMed]
21. Chauhan, P.S.; Kumar, S.; Soni, S.K. On the physical layer security over Beaulieu-Xie fading channel. *AEU—Int. J. Electron. Commun.* **2020**, *113*, 152940. [CrossRef]
22. Gvozdarev, A.S.; Artemova, T.K.; Murin, D.M.; Patralov, P.E. Reconfigurable Intelligent Surfaces' Impact on the Physical Layer Security of the Beaulieu-Xie Shadowed Fading Channel. In Proceedings of the 2022 International Symposium on Networks, Computers and Communications (ISNCC), Shenzhen, China, 19–22 July 2022. [CrossRef]

23. Cho, Y.S.; Kim, J.; Yang, W.Y.; Kang, C.G. *MIMO-OFDM Wireless Communications with MATLAB®*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2010. [CrossRef]
24. Bloch, M.; Barros, J.; Rodrigues, M.R.D.; McLaughlin, S.W. Wireless Information-Theoretic Security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534. [CrossRef]
25. Gopala, P.K.; Lai, L.; Gamal, H.E. On the Secrecy Capacity of Fading Channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 4687–4698. [CrossRef]
26. He, B.; Zhou, X.; Swindlehurst, A.L. On Secrecy Metrics for Physical Layer Security Over Quasi-Static Fading Channels. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 6913–6924. [CrossRef]
27. Hyadi, A.; Rezki, Z.; Alouini, M.S. An Overview of Physical Layer Security in Wireless Communication Systems With CSIT Uncertainty. *IEEE Access* **2016**, *4*, 6121–6132. [CrossRef]
28. Li, S.; Yang, L.; Hasna, M.O.; Alouini, M.S.; Zhang, J. Amount of Secrecy Loss: A Novel Metric for Physical Layer Security Analysis. *IEEE Commun. Lett.* **2020**, *24*, 1626–1630. [CrossRef]
29. Lei, H.; Zhang, H.; Ansari, I.; Pan, G.; Qaraqe, K. Secrecy Outage Analysis for SIMO Underlay Cognitive Radio Networks over Generalized-K Fading Channels. *IEEE Signal Process. Lett.* **2016**, *23*, 1106–1110. [CrossRef]
30. Duong, T.Q.; Zhou, X.; Poor, H.V. (Eds.) *Trusted Communications with Physical Layer Security for 5G and Beyond*; Institution of Engineering and Technology: London, UK, 2017. [CrossRef]
31. Ye, J.; Lei, H.; Liu, Y.; Pan, G.; da Costa, D.B.; Ni, Q.; Ding, Z. Cooperative Communications With Wireless Energy Harvesting Over Nakagami-m Fading Channels. *IEEE Trans. Commun.* **2017**, *65*, 5149–5164. [CrossRef]
32. Lei, H.; Luo, H.; Park, K.H.; Ansari, I.S.; Lei, W.; Pan, G.; Alouini, M.S. On Secure Mixed RF-FSO Systems with TAS and Imperfect CSI. *IEEE Trans. Commun.* **2020**, *68*, 4461–4475. [CrossRef]
33. Li, T.; Ye, J.; Dai, J.; Lei, H.; Yang, W.; Pan, G.; Chen, Y. Secure UAV-to-Vehicle Communications. *IEEE Trans. Commun.* **2021**, *69*, 5381–5393. [CrossRef]
34. Olutayo, A.; Cheng, J.; Holzman, J.F. Performance bounds for diversity receptions over a new fading model with arbitrary branch correlation. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 97. [CrossRef]
35. Olver, F.W.J. *NIST handbook of Mathematical Functions*; Cambridge University Press: Cambridge, UK, 2010.
36. Bender, C.M.; Orszag, S.A. *Advanced Mathematical Methods for Scientists and Engineers I*; Springer: New York, NY, USA, 1999. [CrossRef]
37. Maccartney, G.R.; Rappaport, T.S.; Sun, S.; Deng, S. Indoor Office Wideband Millimeter-Wave Propagation Measurements and Channel Models at 28 and 73 GHz for Ultra-Dense 5G Wireless Networks. *IEEE Access* **2015**, *3*, 2388–2424. [CrossRef]
38. MacCartney, G.R.; Rappaport, T.S. Rural Macrocell Path Loss Models for Millimeter Wave Wireless Communications. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 1663–1677. [CrossRef]
39. Yildirim, I.; Uyrus, A.; Basar, E. Modeling and Analysis of Reconfigurable Intelligent Surfaces for Indoor and Outdoor Applications in Future Wireless Networks. *IEEE Trans. Commun.* **2021**, *69*, 1290–1301. [CrossRef]
40. de Figueiredo, F.A.P.; Facina, M.S.P.; Ferreira, R.C.; Ai, Y.; Ruby, R.; Pham, Q.V.; Fraidenraich, G. Large Intelligent Surfaces With Discrete Set of Phase-Shifts Communicating Through Double-Rayleigh Fading Channels. *IEEE Access* **2021**, *9*, 20768–20787. [CrossRef]
41. Zhi, K.; Pan, C.; Ren, H.; Wang, K. Statistical CSI-Based Design for Reconfigurable Intelligent Surface-Aided Massive MIMO Systems With Direct Links. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1128–1132. [CrossRef]
42. Yildirim, I.; Kilinc, F.; Basar, E.; Alexandropoulos, G.C. Hybrid RIS-Empowered Reflection and Decode-and-Forward Relaying for Coverage Extension. *IEEE Commun. Lett.* **2021**, *25*, 1692–1696. [CrossRef]
43. Kubota, A.; Sampei, S.; Takahashi, T. A Study on Conversion of NLoS to LoS conditions using Sidelink in Smart Factory Environments. In Proceedings of the 2021 IEEE VTS 17th Asia Pacific Wireless Communications Symposium (APWCS), Osaka, Japan, 30–31 August 2021. [CrossRef]