Performance Analysis of Physical Layer Security Over k-Shadowed Fading Channels

Citation for published version:

Digital Object Identifier (DOI):
10.1049/iet-com.2017.1268

Link:
Link to publication record in Heriot-Watt Research Portal

Document Version:
Peer reviewed version

Published In:
IET Communications

Publisher Rights Statement:
This paper is a postprint of a paper submitted to and accepted for publication in IET Communications and is subject to Institution of Engineering and Technology Copyright. The copy of record is available at the IET Digital Library.

General rights
Copyright for the publications made accessible via Heriot-Watt Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
Heriot-Watt University has made every reasonable effort to ensure that the content in Heriot-Watt Research Portal complies with UK legislation. If you believe that the public display of this file breaches copyright please contact open.access@hw.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
Performance Analysis of Physical Layer Security Over $k$-$\mu$ Shadowed Fading Channels

Jiangfeng Sun\textsuperscript{1}, Xingwang Li\textsuperscript{2},\textsuperscript{3}, Mengyan Huang\textsuperscript{2}, Yuan Ding\textsuperscript{3}, Jin Jin\textsuperscript{5}, Gaofeng Pan\textsuperscript{4,6}

\textsuperscript{1} College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo, 45400, China
\textsuperscript{2} School of Physics and Electronic Information Engineering, Henan Polytechnic University, Jiaozuo 45400, China
\textsuperscript{3} Institute of Sensors, Signals, and Systems, Heriot-Watt University, Edinburgh, EH14 4AS, United Kingdom
\textsuperscript{4} School of Information and Engineering, Zhengzhou University, Zhengzhou 450001, China
\textsuperscript{5} Chongqing Key Laboratory of Nonlinear Circuits and Intelligent Information Processing, Southwest University, Chongqing, China
\textsuperscript{6} School of Computing and Communications, Lancaster University, Lancaster, U.K.

\textsuperscript{4} E-mail: corresponding lijingwangbupt@gmail.com

Abstract: In this paper, the secrecy performance of the classic Wyner’s wiretap model over $k$-$\mu$ shadowed fading channels is studied. More specifically, we derive two analytical expressions for the lower bound of secure outage probability at high signal-to-noise ratio regime and the probability of strictly positive secrecy capacity over $k$-$\mu$ shadowed fading channels, respectively. As there exist infinite series in the two derived expressions, we further obtain two simple and explicit approximate expressions for the lower bound of secure outage probability and the probability of strictly positive secrecy capacity with the aid of the moment matching method. It is shown that the match between the analytical results and simulations is very excellent for all parameters under considerations.

1 Introduction

Physical layer security (PLS) has emerged as a promising technique to provide trustworthiness and reliability for the future wireless communication \cite{1, 2}. Unlike the traditional encryption algorithms, as well as the conventional security mechanisms with encryption processing, the key feature of PLS is to exploit the physical layer characteristics of wireless channels. Recently, the secure performance of communication systems over fading channels has been studied in the corresponding literatures \cite{3-7}. Authors in \cite{3} defined the secrecy capacity and characterized the secrecy capacity of a quasi-static Rayleigh fading channel in terms of outage probability. The exact closed-form expressions for the secure outage probability (SOP) and the probability of the strictly positive secrecy capacity (SPSC) of multiple-input multiple-output (MIMO) system over Nakagami-$m$ fading channels have been investigated in \cite{13}. Authors in \cite{14} extended the work of \cite{12} to derive approximate expressions for outage probability and channel state information (CSI) of the main channel were known. In \cite{17}, the performance analysis of the SOP lower bound and exact SPSC over Nakagami-$m$ fading channels was presented in \cite{17}. Authors in \cite{18} investigated the effective rate of multiple-input single-output (MISO) systems over independent and identically distributed (i.i.d.) $k$-$\mu$ shadowed fading channels. The performance of energy detection over $k$-$\mu$ shadowed fading was analysed in \cite{19}. To the best of the authors’ knowledge, the performance of the physical layer security over $k$-$\mu$ shadowed fading channels has not been presented in the open technical literature, which motivates us to develop this treatise.

Motivated by the above discussion, in this study, we investigate the secrecy performance over the $k$-$\mu$ shadowed fading channels. The analytical expressions of the SOP lower bound and exact SPSC for the classic Wyner’s wiretap model are derived. However, the derived expressions contain infinite series, which makes challenge to analyze the influence of fading parameters on system performance. To solve this problem, the approximate expressions of the asymptotic lower bound of SOP and the asymptotic SPSC are derived with the aid of a moment matching method. Two explicit asymptotic expressions are easy to be numerically evaluated because they provide a unified form in terms of well-known Gamma function and Meijer G-function. Moreover, our theoretical analysis is confirmed by Monte-Carlo simulation results.
The remainder of this paper is organised as follows: In Section 2, we introduce the system model and the statistics for the $k$-$\mu$ shadowed distribution. Section 3 derives the exact analytical expressions for the lower bound of the SOP and the SPSC over the $k$-$\mu$ shadowed fading channels based on the classic Wyner’s wiretap model, respectively. In Section 4, we provide asymptotic expressions of the lower bound of SOP and SPSC by using the moment matching method. Section 5 showcases numerical results according to the Monte-Carlo simulations to validate the correctness of our analyses. Finally, the paper is concluded in Section 6.

2 System model and statistics for the $k$-$\mu$ shadowed distribution

2.1 System Model

In this subsection, the classic Wyner’s wiretap model consisting of three entities is considered: a legitimate transmitter ($S$), a legitimate receiver ($D$), and an eavesdropper ($E$). As shown in Fig. 1, the communication occurs over the main channel between $S$ and $D$, while $E$ is able to intercept the signal from the eavesdropper channels. We have the following assumption that both the main and eavesdropper channels experience independent and non-identical $k$-$\mu$ shadowed fading. Two channels are block fading channels where the channels vary independently from one block to another while remaining constant during a block period. Additionally, it is assumed that $S$ has the perfect CSI of both main and eavesdropper channels. In practice, it is very difficult to obtain perfect CSI, which is obtained by channel estimation. This problem will be as our future research content. The received signals at the receiver ($D$ and $E$) can be written as

$$y_i = h_i x + n_i, i \in \{D, E\}$$

where $h_i$ denotes the $k$-$\mu$ shadowed fading channels between the transmitter and the single receiver, $i \in \{D, E\}$ means the parameter belongs to the main channel or the eavesdropper channel; $x$ is the transmitted signal; $n$ represents the additive white Gaussian noise having zero mean and fixed variance $\sigma_n^2$.

2.2 Statistics for The $k$-$\mu$ Shadowed Distribution

In the following, the main and eavesdropper channels undergo independent and non-identical $k$-$\mu$ shadowed fading, and the probability density function (PDF) of the SNR over $k$-$\mu$ shadowed fading channels is given as [15]

$$f_1(\gamma) = \frac{\mu_i^{\mu_i} m_i^{m_i} (1 + k_i)^{m_i} \Gamma(\mu_i)\Gamma(\mu_j) m_i^{m_i} \gamma^{\mu_i-1}}{\Omega_i \mu_i \Gamma(\mu_i) \Gamma(\mu_j) m_i^{m_i} \gamma^{\mu_i-1}} \times \frac{\gamma}{\mu_i (1 + k_i)^{m_i} \Omega_i}$$

$$\times F_1(\mu_i, m_i; \frac{\mu_i (1 + k_i)^{m_i} \gamma}{\mu_i (1 + k_i)^{m_i} \Omega_i})$$

where $\Omega_i = E[\gamma_i]$ is the average SNR at $D$ or $E$, $\mu_i$ and $m_i$ are channel’s parameters of $D$ or $E$ with the meanings of the ratio between the total power of the dominant components and the total power of the scattered waves, the number of clusters, and the shaping parameter of the Nakagami-$m$ random variable (RV), respectively. $\Gamma(\cdot)$ and $F_1(\cdot)$ are the Gamma function [20, Eq. (8.310.1)] and the confluent hypergeometric function [20, Eq. (9.14.1)], respectively.

Then, the cumulative distribution function (CDF) of $k$-$\mu$ shadowed distribution of SNR is given as [15]

$$F_1(\gamma) = \frac{\mu_i^{\mu_i-1} m_i^{m_i} (1 + k_i)^{m_i} \Gamma(\mu_i)}{\Gamma(\mu_i) \mu_i \Gamma(\mu_i) \Gamma(\mu_j) m_i^{m_i} \gamma^{\mu_i-1}} \times \Phi_2(\mu_i - m_i, m_i, \mu_i + 1 ;$$

$$- \mu_i (1 + k_i)^{m_i} \gamma \Omega_i, \mu_i (1 + k_i)^{m_i} \gamma \Omega_i)$$

$$, i \in \{D, E\}$$

where $\Phi_2(\cdot)$ is the confluent multivariate hypergeometric function [20].

3 Analyses for secure outage probability and probability of strictly positive secrecy capacity

In this section, the exact analytical closed-form expressions for the lower bound of the SOP and the SPSC over $k$-$\mu$ shadowed fading channels are derived in the following theorems, respectively.

3.1 SOP Analysis

As an important performance metric to characterize wireless communications, SOP is the probability that the instantaneous secrecy capacity is smaller than the target rate [3, 21], which is defined as

$$P_{out}(R_S) = P(C_S \leq R_S)$$

where $C_S = C_m - C_w$, $C_S$ is the instantaneous secrecy capacity for the wireless fading channels; $C_m$ and $C_w$ denote the capacity of the main channel and the eavesdropper channel, respectively; $R_S$ represents a target secrecy rate.

Theorem 1. For $k$-$\mu$ shadowed fading channels, the closed-form expression for the lower bound of the SOP is given as

$$SOP = \frac{\mu_i^{\mu_i} m_i^{m_i} (1 + k_i)^{m_i} \Gamma(\mu_i)}{\Gamma(\mu_i) \Gamma(\mu_j) m_i^{m_i} \gamma^{\mu_i-1}} \times \Phi_2(\mu_i - m_i, m_i, \mu_i + 1 ;$$

$$- \mu_i (1 + k_i)^{m_i} \gamma \Omega_i, \mu_i (1 + k_i)^{m_i} \gamma \Omega_i)$$

$$, i \in \{D, E\}$$

where $\Omega_i = E[\gamma_i]$ is the average SNR at $D$ or $E$, $\mu_i$ and $m_i$ are channel’s parameters of $D$ or $E$ with the meanings of the ratio between the total power of the dominant components and the total power of the scattered waves, the number of clusters, and the shaping parameter of the Nakagami-$m$ random variable (RV), respectively. $\Gamma(\cdot)$ and $F_1(\cdot)$ are the Gamma function [20, Eq. (8.310.1)] and the confluent hypergeometric function [20, Eq. (9.14.1)], respectively.

Proof: The detailed proof is provided in Appendix

3.2 SPSC Analysis

In this subsection, we consider another benchmark, SPSC, which is the probability of existence of strictly positive secrecy capacity [3, 21]. In secure communications, SPSC is an essential metric to characterize the system performance, which is defined as

$$P_{out} = P(C_S > 0)$$

\[\text{Fig. 1: System model}\]
Theorem 2. For k-μ shadowed fading channels, the closed-form expression for SPSC is given as
\[ \text{SPSC} = 1 - \frac{\rho_D}{\mu_D} \left[ \frac{\Gamma(\mu_D)}{\mu_D} \right]_{p,q=0}^{\infty} \frac{\Gamma(p+1)}{\Gamma(p+q+1)} \frac{\Gamma(m_D)}{\mu_D} \frac{E_{p+q+\mu_D}^m (a_D)^{p+q}}{e^{a_D}} \]
(7)

Proof: According to (6), SPSC can be obtained as
\[ \text{SPSC} = P \{ C_S(\gamma_D, \gamma_E) > 0 \} = 1 - P \{ \ln(1 + \gamma_D) - \ln(1 + \gamma_E) \leq 0 \} = 1 - P \{ \gamma_D \leq \gamma_E \}
= 1 - \int_0^\infty F_D(\gamma_E) f_E(\gamma_E) d\gamma_E
= 1 - \frac{\rho_D}{\mu_D} \left[ \frac{\Gamma(\mu_D)}{\mu_D} \right]_{p,q=0}^{\infty} \frac{\Gamma(p+1)}{\Gamma(p+q+1)} \frac{\Gamma(m_D)}{\mu_D} \frac{E_{p+q+\mu_D}^m (a_D)^{p+q}}{e^{a_D}} \]
(8)

Using (A.14), we can derive SPSC as (7) after some simplifications. \( \square \)

We can finally derive the approximate expression for the lower bound SOP as
\[ \text{SOP} = \frac{1}{\Gamma(\Delta_D)} \left[ \frac{\Omega_E \Delta_D}{\Omega_D} \right]_{1,1}^{\infty} \frac{1}{\Delta_D, 0} \]
(11)

Proof: SOP can be presented as
\[ \text{SOP} = \Pr \{ C_S(\gamma_D, \gamma_E) \leq C_{th} \} = \frac{1}{\Gamma(\Delta_D)} \left[ \frac{\Omega_E \Delta_D}{\Omega_D} \right]_{1,1}^{\infty} \frac{1}{\Delta_D, 0} \]
(12)

For \( \text{SOP} \), the lower bound of SOP can be given by
\[ \text{SOP} = \frac{1}{\Gamma(\Delta_D)} \left[ \frac{\Omega_E \Delta_D}{\Omega_D} \right]_{1,1}^{\infty} \frac{1}{\Delta_D, 0} \]
(13)

Then, using (A.11), the lower bound of SOP can be given by
\[ \text{SOP} = \frac{1}{\Gamma(\Delta_D)} \left[ \frac{\Omega_E \Delta_D}{\Omega_D} \right]_{1,1}^{\infty} \frac{1}{\Delta_D, 0} \]
(14)

The integral in (14) contains a power function, an exponential function and a lower incomplete gamma function. Using [23, Eq. (11)] and the integral in [24, Eq. (8.4.16.1)], we can rewrite the exponential function and the lower incomplete gamma function in the form of MeijerG-function as
\[ \exp \left( \frac{\Delta_E}{\Omega_E} \gamma_E \right) = G_{1,0}^{0,1} \left[ \frac{\Delta_E}{\Omega_E} \gamma_E \right]_{0}^{1} \]
(15)

\[ \text{Y}(\Delta_D, \frac{\Delta_D \Theta \gamma_E}{\Omega_D}) = G_{1,1}^{1,1} \left[ \frac{\Delta_D \Theta \gamma_E}{\Omega_D} \right]_{1,0}^{1} \]
(16)

Then, by substituting (15) and (16) into (14), and utilizing (A.14), we can finally derive the approximate expression for the lower bound of SOP as
\[ \text{SOP} = \frac{1}{\Gamma(\Delta_D)} \left[ \frac{\Omega_E \Delta_D}{\Omega_D} \right]_{1,1}^{\infty} \frac{1}{\Delta_D, 0} \]
(17)

\( \square \)
Theorem 4. For $k$-$\mu$ shadowed fading channels, the approximate expression for the SPSC is given as

$$SPSC = 1 - \frac{1}{\Gamma(\Delta_D)} \frac{1}{\Gamma(\Delta_E)} \left[ \frac{\Omega E \Delta D}{\Omega D \Delta E} \right]^{1,1-\Delta_E}_{1,0}$$

Proof: Referring to (8), SPSC can be obtained as

$$SPSC = P \{ C_S(\gamma_D, \gamma_E) > 0 \}$$

$$= 1 - P \{ \gamma_D \leq \gamma_E \}$$

$$= 1 - \int_0^\infty F_D(\gamma_E) f_E(\gamma_E) d\gamma_E$$

$$= 1 - \frac{\Omega E \Delta E}{\Gamma(\Delta_D) \Gamma(\Delta_E)} \int_0^\infty \gamma_E^{\Delta_E-1}$$

$$\times G_{0,1}^{1,0} \left[ \frac{\Delta E}{\Omega E} \gamma_E \right]_0^{\infty} G_{1,2}^{1,1} \left[ \frac{\Delta D \gamma_E}{\Omega D} \right]_0^{\Delta_D} d\gamma_E$$

In (19), the integral consists of three terms: a power function and two exponential functions. As suggested by (A.14), we can finally derive the expression of (18) after some algebraic operations. $\square$

5 Numerical results

In this section, the proposed analytical derivations are validated against the simulation results, and the effects of various channel parameters on the secrecy performance are discussed. According to Eq. (2), the $k$-$\mu$ shadowed RVs are generated in $10^5$ realizations. These random RVs are used to obtain the simulation results of the SOP and SPSC. Unless otherwise specified, we have the following assumption: $C_{ib} = 1$dB, $\Omega_D = \lambda \Omega_E$. SOP simulation: $\Omega_E = 20$dB, SPSC simulation: $\Omega_E = 1$dB, where $\lambda$ represents the ratio of the received SNR between the main and the eavesdropper channels.

In Figs. 2 and 3, the approximated lower bound of the SOP in (11) and approximate SPSC in (18) are compared with the simulation results versus $\lambda$ for parameters $(k_D,k_E)$, respectively. The specific parameters are set as follows: $\mu_D = \mu_E = 2$, $m_D = m_E = 1$. It is clearly shown that the simulation results sufficiently match with analysis results. A higher $\lambda$ causes a smaller SOP and a bigger SPSC since a higher $\lambda$ represents that the quality of main channel outperforms the one of eavesdropper channel. In addition, when $\lambda > 2$dB, SOP increases and SPSC decreases while $k_D$ increasing, because $k$ is the ratio between the total power of the dominant components and the total power of the scattered waves. Finally, we can observe that small $k_D$ is beneficial to enhance the secrecy performance of the considered system.

Fig. 2: SOP with changing $(k_D,k_E)$ versus $\lambda$, $(k_D,k_E) = \{(0.5,2),(2,2),(10,2)\}$

Fig. 3: SPSC with changing $(k_D,k_E)$ versus $\lambda$, $(k_D,k_E) = \{(10,2),(2,2),(0.5,2)\}$

Fig. 4: SOP with changing $(\mu_D,\mu_E)$ versus $\lambda$, $(\mu_D,\mu_E) = \{(10,2),(2,2),(1,2)\}$

Fig. 5: SPSC with changing $(\mu_D,\mu_E)$ versus $\lambda$, $(\mu_D,\mu_E) = \{(1,2),(2,2),(10,2)\}$
large value of $\mu_2$ yields lower SOP and higher SPSC, which means that large $\mu_2$ is beneficial for enhancing SOP and SPSC, since $\mu$ is the number of clusters.

In Figs. 6 and 7, we compare simulation and approximate analysis results of the SOP and SPSC over $k$-$\mu$ shadowed fading channels versus $\lambda$ for different parameters $(m_D, m_E)$. The parameter sets are given as follows: $k_D = k_E = 2, \mu_D = \mu_E = 2$. The close match between analysis and simulation results verifies the correctness of our proposed analytical models. Moreover, we can see that SOP decreases and SPSC increases by increasing $m_D$ with $\lambda > -2\text{dB}$, where $m$ is the shaping parameter of Nakagami-$m$ RV. Finally, we can observe that large $m_D$ is helpful in improving the performance of PLS.

6 Conclusion

In this paper, we investigate the secrecy performance of the classic Wyner's wiretap model over $k$-$\mu$ shadowed channels. The closed-form expressions for the SOP lower bound followed by high SNR analysis and the exact SPSC are derived. However, the derived expressions involve infinite series which is a challenge to further analysis. In order to solve this problem, we obtain two simple and explicit approximate expressions for the lower bound of the SOP and the SPSC by using a moment matching method. Finally, the asymptotic expressions are validated through the simulation results.

7 Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grant 61501404, in part by China Scholarship Council Grant 201608410318, in part by the Doctoral Scientific Funds of Henan Polytechnic University under Grant B2016-34, and in part by the Henan Scientific and Technological Research Project under Grant 172102210023.

8 References


9 Appendix

In this section, the proof of theorem 1 is given.
Proof: Based on the definition in (4), SOP can be provided as

\[ SOP = P \{ C_S(\gamma_D, \gamma_E) \leq C_{th} \} \]

\[ = P \{ \ln(1 + \gamma_D) - \ln(1 + \gamma_E) \leq C_{th} \} \]

\[ = P \left\{ \frac{1 + \gamma_D}{1 + \gamma_E} \leq \Theta \right\} \]

\[ = P \{ \gamma_D \leq \Theta \gamma_E + \theta - 1 \} \]

\[ = \int_0^\infty f_D(\gamma_D) d\gamma_D \int_0^{\gamma_D} f_E(\gamma_E) d\gamma_E \]

\[ = \int_0^\infty F_D(\Theta \gamma_E + \theta - 1) f_E(\gamma_E) d\gamma_E \]

According to [25], we can obtain the following formula as

\[ pF_q \left( \frac{\mu}{a} \right) = \frac{\Gamma(b_\mu)}{\Gamma(a)} G_{p+1}^{1,1} \left[ -x \middle| \begin{array}{c} a_1, \ldots, a_p \\ b_\mu \end{array} \right] \]

Employing the following identity [24, Eq. (7.111.2)],

\[ 1F_1(a, b; x) = e^x F_1(b - a, b; -x) \]

and after some algebraic manipulations, the confluent hypergeometric function in (2) can be rewritten as

\[ 1F_1 \left( \frac{m_1}{\mu}, \mu, \frac{2}{\mu}k_m(1 + k_m) \right) \]

Theorem, (2) can be rewritten as

\[ f_i(\gamma) = \frac{a_i^{\mu_i}}{b_i \mu_i} \Gamma(\mu_i) \exp(-\gamma \gamma) \]

Substituting the following identity [20, Eq. (9.261.2)] into (3),

\[ \Phi_2(\alpha, \beta, \gamma; x) = \sum_{p,q=0}^\infty \frac{(\gamma)^{p+q}}{(\gamma)^{p+q}} y^q \]

the CDF of \( k\)-\( \mu \) shadowed distribution can be simplified as

\[ F_i(\gamma) = \frac{a_i^{\mu_i}}{\mu_i \Gamma(\mu_i)} \sum_{p,q=0}^\infty \frac{(\gamma)^{p+q}}{(\gamma)^{p+q}} \exp(-\gamma^{p+q+1}) \]

Then, substituting (A.5) and (A.7) into (A.1), SOP can be further expressed as

\[ SOP = \frac{a_i^{\mu_i}}{\mu_i \Gamma(\mu_i)} \sum_{p,q=0}^\infty \frac{(\gamma)^{p+q}}{(\gamma)^{p+q}} \exp(-\gamma^{p+q+1}) \]

\[ \times \left( \frac{\gamma^{p+q+1}}{\mu_i \Gamma(\mu_i)} \right) \]

The integral term contained in (A.8) is more complex, which will cause difficulty in integral operation. Considering that \( \Theta = \exp(C_{th}) \) is a finite value, we utilize the similar method adopted in [26], with the assumption of \( \gamma_E \to \infty \), the formula can be obtained as

\[ (\Theta \gamma_E + \theta - 1)^{p+q+\mu D} \approx (\Theta \gamma_E)^{p+q+\mu D} \]

Then, by using the following inequality [21, Eq. (6)],

\[ SOP = P \{ \gamma_D \leq \Theta \gamma_E + \theta - 1 \} \]

the lower bound of SOP can be given by

\[ SOP^L = P \{ \gamma_D \leq \Theta \gamma_E \} \]

Here, the remaining task is to calculate the integral in the (A.11). The integrand contains a power function, an exponential function and a lower incomplete gamma function. Using [23, Eq. (11)], we can rewrite the exponential function in the form of Meijer-G function as

\[ \exp(-\frac{\gamma_E}{b_E}) = G_{0,1}^{1,0} \left[ \frac{\gamma E}{b_E} \right] \]

So the integral in Eq. (A.11) is transformed into

\[ \int_0^{\gamma_E} \gamma^{d-1} \int_0^{1} \frac{a E}{b_E} \gamma E \]

With the aid of the identity [23, Eq. (21)], setting the parameters:

\[ l = 1 \text{ and } k = 1 \text{, we can obtain:} \]

\[ \int_0^{x^{\alpha=-1}} G_{m,n}^{l} \left[ \frac{\alpha x}{(b\alpha)} \right] \]