Article | Received 21 May 2026; Revised 4 June 2026; Accepted 9 June 2026; Published 24 July 2026
https://doi.org/10.55092/aic20260010

Performance analysis and prediction of physical layer security over α-Beaulieu-Xie shadowed fading channels

Jiangfeng Sun* and Shuiwang Niu

College of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China

* Correspondence author; E-mail: sunjiangfeng@hpu.edu.cn.

Highlights:

- This paper studies the security performance analysis based on α-Beaulieu-Xie shadowed fading channels, and closed-form expressions of two security benchmarks for SOP and SPSC are derived.
- To enhance the real-time performance of security performance evaluation, this paper proposes the Self-LSTM algorithm for predicting SOP and SPSC.
- The impacts of fading parameters on the secrecy performance of Wyner's model are investigated.

Abstract: This paper investigates the secrecy performance of α-Beaulieu-Xie shadowed fading channels based on the Wyner's wiretap model. In particular, the lower bound expression of secure outage probability (SOP) and the exact expression of strictly positive secrecy capacity (SPSC) are derived. Monte Carlo simulation verifies the accuracy of theoretical analysis. The results indicate that the larger α_D, m_{DX} and m_{DY} or smaller Ω_{DX} can enhance the performance of model. Moreover, to predict the security performance of the model, the self long short-term memory (Self-LSTM) algorithm is proposed. We found that the Self-LSTM algorithm has better prediction performance by comparing with LSTM, DenseNet and convolutional neural network (CNN) network. Compared with the LSTM, the prediction accuracy of Self-LSTM is increased by 55.95%, the time complexity is decreased by 81.03%. Comparing to the DenseNet network, the precision of the Self-LSTM algorithm is improved by 64.20%. It can be concluded that the proposed Self-LSTM has higher prediction accuracy and lower time complexity.

Keywords: physical layer security; α-BX shadowed fading channels; performance analysis; security prediction

1. Introduction

With the fast development of information technology, wireless communication has become the main ways of the signal transmission. During the process of communication between users, the signals are exposed to external environment, which bring the challenge to secrecy. The conventional security schemes are encryption and decryption technology based on cryptography. However, the solution can't meet the needs for high efficiency and secure communication. Compared to the complex cryptographic scheme, physical layer security (PLS) has the characteristic of low power and high efficiency. As an emerging energy-saving technology, PLS has been favored by many scholars [1–4]. The authors of [1] explored the PLS over generalized gamma fading from two perspectives of secure outage probability (SOP) and strictly positive secrecy capacity (SPSC). Sun *et al.* in [2] discussed the security performance on κ-μ shadowed distribution. The work in [3] analyzed the system security of the Multi-Hop amplify and forward (AF) relay network. Li *et al.* in [4] studied the PLS of Ambient Backscatter cooperative communication networks by deriving the accurate and approximate expressions of SOP.

In the actual communication scenarios, the signals will experience various fading, including α-μ, κ-μ shadowed, Nakagami-*m*, Beaulieu-Xie (BX), Rayleigh, BX shadowed and α-BX fading and so on. Yadav *et al.* in [5] summarized the security performance of cognitive radio networks (CRN) on α-μ fading channels. The authors of [6] studied the security capability of single-input–multiple-output (SIMO) models over κ-μ shadowed distribution. The work in [7] evaluated the bit error rate (BER) performance with direct link on Nakagami-*m* distribution. The secrecy capacity of relaying non-orthogonal multiple access (NOMA) models was explored in [8] on BX fading channels. Li *et al.* in [9] discussed the effect of residual hardware impairments on the secrecy performance over Rayleigh distribution. The BX shadowed model was used for exploring the communication system's average BER [10], the performance of PLS [11], and capacity analysis [12]. The authors of [13] presented the statistics of the classical α-BX model.

Recently, with the rapid development of artificial intelligence technology, deep learning (DL) algorithms has been extensively applied in mobile communication scenarios. Liang *et al.* in [14] discussed the motivation and obstacles of wireless resource allocation and applied DL to vehicular networks. The authors of [15] first analyzed the channel estimation of the multiple antenna systems based on DL. Chen *et al.* in [16] developed an energy-saving offloading strategy for intelligent Internet of Things (IoT) systems based on deep neural network (DNN). The authors in [17] presented a practical method for DL-based end-to-end wireless communication systems. To improve the reliability and efficiency of signal reception, the work of [18] proposed a novel receiver architecture using deep recurrent neural networks (RNNs) in Time-varying fading channels. The authors in [19] discussed the application of emerging DL technologies in future wireless communication networks.

Compared with conventional fading models such as Rayleigh, Nakagami-*m*, α-μ, and κ-μ shadowed fading, the α-BX shadowed fading model provides a more flexible description of wireless channels by jointly considering nonlinear propagation, multipath fading, and shadowing effects. The parameter α characterizes the nonlinearity of the propagation medium, while the BX shadowed structure can model the coexistence of dominant and scattered components under different shadowing conditions. Therefore, this model is suitable for complex propagation environments where the line-of-sight and non-line-of-sight components experience different fading severities, such as emerging mobile communication systems, millimeter-wave communications, terahertz communications, 6G wireless networks, and satellite/terrestrial links with severe blockage or shadowing.

To the best of the author's knowledge, the performance of PLS based on Wyner's wiretap model over α-BX shadowed fading channels has not been explored in the available databases. On the basis, this paper mainly studies and predicts the secrecy performance over α-BX shadowed fading channels under Wyner model. The primary contributions of this paper are as below:

- According to the characteristic of α-BX shadowed distribution, the lower bound expression of SOP and the exact expression of SPSC are derived. The Monte Carlo simulation verifies the correctness of theoretical derivation. Furthermore, the impacts of fading parameters on the secrecy performance of Wyner's system are investigated.
- The Closed-form analytical formulas for SOP and SPSC obtained through consistent Meijer's G-function. The complex operations of infinite series are avoided by using the function.
- This paper proposes the Self-LSTM algorithm to analyze and predict the security performance of considered system. As far as prediction accuracy and time complexity, we compare three algorithms, including LSTM, DenseNet and CNN. The experimental results demonstrate that the Self-LSTM excels in both real-time performance and accuracy.

The remainder of this paper is organized as follows. Section 2 presents Wyner's system model and the statistical characteristics of the α-Beaulieu-Xie shadowed fading distribution. Section 3 derives and validates the closed-form expressions for the SOP and SPSC. Section 4 describes the proposed Self-LSTM algorithm. Section 5 analyzes the theoretical research and security prediction. Section 6 concludes this paper.

Notations: The symbols are displayed in Table 1.

Table 1. Notations.

Notation	Meaning
$\Gamma(\cdot)$	Gamma function
$\exp(\cdot)$	Exponential function
$\sum$	Sum function
$(a)_b$	Pochhammer function
$(\cdot)!$	Factorial operator
$\Upsilon(\cdot)$	Lower incomplete Gamma function
${}_2F_1(\cdot)$	Gauss hypergeometric function
$G(\cdot)$	Meijer's G-function

2. System model and α-BX shadowed fading chanels

2.1. System model

The Wyner's wiretap model consists of a signal source (S), a legal node (D) and an eavesdropper (E). h_D and h_E express the fading coefficients for legal and wiretap channels, respectively. Both legal and wiretap links suffer the α-BX shadowed fading. In addition, the complex additive white Gaussian noise (AWGN) also interfere the transmission process of signals. Assuming that all channels has optimal channel state information, the signals of the D and E are represented by

$$y_i = h_i x + n_i, i \in \{D, E\}, \tag{1}$$

where h_i stands for the fading coefficients between S and i, x denotes the transmission signals, n_i is the complex AWGN.

The considered Wyner's wiretap model can represent a practical secure wireless transmission scenario, where a legitimate transmitter sends confidential information to an intended receiver in the presence of a passive eavesdropper. Such a model is applicable to mobile communication networks, Internet of Things systems, satellite/terrestrial communication links, and future 6G networks, where confidential information may be intercepted due to the broadcast nature of wireless channels. Therefore, analyzing SOP and SPSC over α-BX shadowed fading channels is valuable for evaluating and improving the secrecy performance of practical wireless systems under complex propagation and shadowing environments.

2.2. *Statistics for the α-Beaulieu-Xie shadowed distribution*

All channels experience α-BX shadowed distribution. The probability density function (PDF) of instantaneous signal-to-noise ratio (SNR) over α-BX shadowed fading channels [20] can be written by

$$\begin{aligned} f_i(\gamma) = &\frac{\alpha_i(1-\xi_i)^{m_{iY}}}{2(\lambda_{\alpha_i})^{m_{iX}}\Gamma(m_{iX})\Psi_i}\left(\frac{\gamma}{\Psi_i}\right)^{\frac{\alpha_i m_{iX}}{2}-1} \\ &\times \exp\left(-\lambda_{\alpha_i}{}^{-1}\left(\frac{\gamma}{\Psi_i}\right)^{\frac{\alpha_i}{2}}\right) \\ &\times \sum_{p_i=0}^{\infty}\frac{(m_{iY})_{p_i}\left(\frac{\xi_i}{\lambda_{\alpha_i}}\right)^{p_i}\left(\frac{\gamma}{\Psi_i}\right)^{\frac{\alpha_i p_i}{2}}}{(m_{iX})_{p_i}p_i!}, \end{aligned} \tag{2}$$

according to the relevant knowledge of probability theory and Equation (3.381.8) [21], the cumulative distribution function (CDF) of α-BX shadowed distribution is calculated by

$$\begin{aligned} F_i(\gamma) &= \int_0^{\gamma} f_i(x)\,dx \\ &= \frac{\alpha_i(1-\xi_i)^{m_{iY}}(\Psi_i)^{-\frac{\alpha_i m_{iX}}{2}}}{2(\lambda_{\alpha_i})^{m_{iX}}\Gamma(m_{iX})} \\ &\quad \times \sum_{p_i=0}^{\infty}\frac{(m_{iY})_{p_i}\left(\frac{\xi_i}{\lambda_{\alpha_i}}\right)^{p_i}\left(\frac{1}{\Psi_i}\right)^{\frac{\alpha_i p_i}{2}}}{(m_{iX})_{p_i}p_i!} \\ &\quad \times \int_0^{\gamma} x^{\frac{\alpha_i(m_{iX}+p_i)}{2}-1} e^{-\frac{1}{\lambda_{\alpha_i}(\Psi_i)^{\frac{\alpha_i}{2}}}x^{\frac{\alpha_i}{2}}}\,dx \\ &= \frac{\alpha_i(1-\xi_i)^{m_{iY}}(\Psi_i)^{-\frac{\alpha_i m_{iX}}{2}}}{2(\lambda_{\alpha_i})^{m_{iX}}\Gamma(m_{iX})} \\ &\quad \times \sum_{p_i=0}^{\infty}\frac{(m_{iY})_{p_i}\left(\frac{\xi_i}{\lambda_{\alpha_i}}\right)^{p_i}\left(\frac{1}{\Psi_i}\right)^{\frac{\alpha_i p_i}{2}}}{(m_{iX})_{p_i}p_i!} \\ &\quad \times \frac{\Upsilon\left(m_{iX}+p_i, \frac{1}{\lambda_{\alpha_i}(\Psi_i)^{\frac{\alpha_i}{2}}}\gamma^{\frac{\alpha_i}{2}}\right)}{\frac{\alpha_i}{2}\left(\frac{1}{\lambda_{\alpha_i}(\Psi_i)^{\frac{\alpha_i}{2}}}\right)^{m_{iX}+p_i}}, \end{aligned} \tag{3}$$

where $\lambda_{\alpha_i} = \left[\frac{\Gamma(m_{iX})}{\Gamma\left(m_{iX}+\frac{2}{\alpha_i}\right){}_2F_1\left(m_{iY},-\frac{2}{\alpha_i};m_{iX};-\frac{m_{iX}\Omega_{iY}}{m_{iY}\Omega_{iX}}\right)}\right]^{\frac{\alpha_i}{2}}$, $\xi_i = \frac{m_{iX}\Omega_{iY}}{m_{iY}\Omega_{iX}+m_{iX}\Omega_{iY}}$. m_{iX}, m_{iY}, Ω_{iX}, Ω_{iY} and $\alpha_i\,(\alpha_i \geq 0)$ are the fading parameters. γ represents instantaneous SNR, Ψ indicates the average SNR, $\Gamma(\cdot)$ denotes the Gamma function Equation (8.310.1) [21], $(a)_b = a(a+1)\ldots(a+b-1) = \Gamma(a+b)/\Gamma(a)$ means the pochhammer function [22], $(\cdot)!$ is the factorial function, $\Upsilon(\alpha, x) = \int_0^x e^{-t} t^{\alpha-1} dt$ expresses the lower incomplete Gamma function Equation (8.350.1) [21], ${}_2F_1(\cdot)$ is the Gauss hypergeometric function Equation (9.14.1) [21].

3. Performance analysis

SOP and SPSC are the key performance indicators for analyzing the PLS over α-BX shadowed fading channels. The analytical expressions of SOP and SPSC are obtained in this section. SOP and SPSC are adopted because they are two fundamental and widely used metrics for evaluating physical layer security. SOP measures the probability that the instantaneous secrecy capacity is lower than a given target secrecy rate, and thus reflects the reliability of secure transmission under a secrecy requirement. In contrast, SPSC measures the probability that the instantaneous secrecy capacity is strictly larger than zero, which indicates whether a positive secrecy transmission can be achieved. Therefore, SOP characterizes the secrecy outage behavior for a prescribed threshold, while SPSC describes the basic existence probability of secure communication. When the target secrecy rate approaches zero, the SPSC can be regarded as the complementary event of secrecy outage, *i.e.*, $P_{SPSC} = 1 - P_{SOP}|_{C_{th}=0}$.

3.1. SOP analysis

As the significant indicator of wireless communication systems, SOP expresses the probability that the instantaneous confidentiality ability is smaller than the target rate [23,24]. Therefore, the SOP is defined by

$$P_{SOP} = \Pr(C_S \le C_{th}), \tag{4}$$

where C_S means the instantaneous secrecy ability of fading channels and $C_S = C_D - C_E$. C_D and C_E are the capacity of the main channel and eavesdropper channel, respectively. C_{th} denotes the target rate.

Theorem 1: For the α-BX shadowed fading channels, the closed-form expression for the lower bound of the SOP is gained by

$$\begin{aligned} P_{SOP}^{L} = {} & \frac{\alpha_D (1-\xi_D)^{m_{DY}} (\Psi_D)^{-\frac{\alpha_D m_{DX}}{2}}}{2(\lambda_{\alpha_D})^{m_{DX}} \Gamma(m_{DX})} \\ & \times \frac{\alpha_E (1-\xi_E)^{m_{EY}} (\Psi_E)^{-\frac{\alpha_E m_{EX}}{2}}}{2(\lambda_{\alpha_E})^{m_{EX}} \Gamma(m_{EX})} \\ & \times \sum_{p_D=0}^{\infty} \frac{(m_{DY})_{p_D} \left(\frac{\xi_D}{\lambda_{\alpha_D}}\right)^{p_D} \left(\frac{1}{\Psi_D}\right)^{\frac{\alpha_D p_D}{2}}}{(m_{DX})_{p_D} p_D! \frac{\alpha_D}{2} (\mathrm{I}_D)^{m_{DX}+p_D}} \\ & \times \sum_{p_E=0}^{\infty} \frac{(m_{EY})_{p_E} \left(\frac{\xi_E}{\lambda_{\alpha_E}}\right)^{p_E} \left(\frac{\gamma_E}{\Psi_E}\right)^{\frac{\alpha_E p_E}{2}}}{(m_{EX})_{p_E} p_E!} \\ & \times \frac{2{\alpha_E}^{m_{DX}+p_D+\Theta-\frac{3}{2}} \left(\mathrm{I}_D \Lambda^{\frac{\alpha_D}{2}}\right)^{-\Theta}}{\sqrt{\alpha_D} (2\pi)^{\frac{\alpha_D+\alpha_E}{2}-1}} \\ & \times G_{2\alpha_E, \alpha_D+\alpha_E}^{\alpha_D+\alpha_E, \alpha_E} \left(\frac{(\mathrm{I_E})^{\alpha_D} {\alpha_E}^{\alpha_E}}{\left(\mathrm{I_D} \Lambda^{\frac{\alpha_D}{2}}\right)^{\alpha_E} {\alpha_D}^{\alpha_D}} \middle| \begin{matrix} \Delta(\alpha_E, N), \Delta(\alpha_E, 1-\Theta) \\ \Delta(\alpha_D, 0), \Delta(\alpha_E, -\Theta) \end{matrix} \right), \end{aligned} \tag{5}$$

where $\mathrm{I}_i=\left(\lambda_{\alpha_i}(\Psi_i)^{\frac{\alpha_i}{2}}\right)^{-1}$, $i\in\{D,E\}$, $\Theta=\frac{\alpha_E(m_{EX}+p_E)}{\alpha_D}$, $N=1-\Theta-m_{DX}-p_D$, $C_{th}\geq 0$, $\Lambda=\exp\left(C_{th}\right)\geq 1$, $\Delta(x,y)=\frac{y}{x},\frac{y+1}{x},\ldots,\frac{y+x-1}{x}$, $G(\cdot)$ is the Meijer's G-function, Equation (9.301) [21].

Convergence and numerical evaluation: The infinite series in the derived SOP and SPSC expressions originate from the series representation of the PDF and CDF of the α-BX shadowed fading distribution. For the considered physical channel parameters, *i.e.*, $m_{iX}>0$, $m_{iY}>0$, $\alpha_i>0$, $\Omega_{iX}>0$, $\Omega_{iY}>0$, and $\Psi_i>0$, the involved series are absolutely convergent. Specifically, by applying the ratio test to the general term containing the Pochhammer symbols and the factorial term, the ratio between two adjacent terms tends to zero as the summation index approaches infinity. Therefore, the double infinite series in the SOP and SPSC expressions can be accurately evaluated by finite truncation. In the numerical evaluation, the summations are truncated when the difference between two successive truncated results is less than 10^{-6}. It is observed that when the summation index exceeds approximately 50 terms, the values of SOP and SPSC remain stable and no longer change, indicating that the series converge rapidly and a small truncation order is sufficient to obtain stable results.

Proof: Combining Equation (2) and Equation (3), the analytical expression of SOP is given by

$$\begin{aligned}
P_{SOP}&=\Pr\left(C_S\leq C_{th}\right)\\
&=\Pr\left(C_D-C_E\leq C_{th}\right)\\
&=\Pr\left\{\frac{1+\gamma_D}{1+\gamma_E}\leq e^{C_{th}}\right\}\\
&=\Pr\left\{\gamma_D\leq\Lambda\gamma_E+\Lambda-1\right\}\\
&=\int_0^\infty\int_0^{\Lambda\gamma_E+\Lambda-1}f_D\left(\gamma_D\right)d\gamma_D f_E\left(\gamma_E\right)d\gamma_E\\
&=\frac{\alpha_D(1-\xi_D)^{m_{DY}}(\Psi_D)^{-\frac{\alpha_D m_{DX}}{2}}}{2(\lambda_{\alpha_D})^{m_{DX}}\Gamma\left(m_{DX}\right)}\\
&\times\frac{\alpha_E(1-\xi_E)^{m_{EY}}(\Psi_E)^{-\frac{\alpha_E m_{EX}}{2}}}{2(\lambda_{\alpha_E})^{m_{EX}}\Gamma\left(m_{EX}\right)}\\
&\times\sum_{p_D=0}^{\infty}\frac{(m_{DY})_{p_D}\left(\frac{\xi_D}{\lambda_{\alpha_D}}\right)^{p_D}\left(\frac{1}{\Psi_D}\right)^{\frac{\alpha_D p_D}{2}}}{(m_{DX})_{p_D}p_D!\frac{\alpha_D}{2}(\mathrm{I}_D)^{m_{DX}+p_D}}\\
&\times\sum_{p_E=0}^{\infty}\frac{(m_{EY})_{p_E}\left(\frac{\xi_E}{\lambda_{\alpha_E}}\right)^{p_E}\left(\frac{\gamma_E}{\Psi_E}\right)^{\frac{\alpha_E p_E}{2}}}{(m_{EX})_{p_E}p_E!}\\
&\times\int_0^\infty Z\times\gamma_E^{\frac{\alpha_E(m_{EX}+p_E)}{2}-1}e^{-\mathrm{I}_E\gamma_E^{\frac{\alpha_E}{2}}}d\gamma_E,
\end{aligned}\tag{6}$$

where $Z=\Upsilon\left(m_{DX}+p_D,\mathrm{I}_D(\Lambda\gamma_E+\Lambda-1)^{\frac{\alpha_D}{2}}\right)$, $\mathrm{I}_D=\left(\lambda_{\alpha_D}(\Psi_D)^{\frac{\alpha_D}{2}}\right)^{-1}$, $\mathrm{I}_E=\left(\lambda_{\alpha_E}(\Psi_E)^{\frac{\alpha_E}{2}}\right)^{-1}$.

To the convenience of calculation, the related formula is recorded as

$$Q=\int_0^\infty Z\times\gamma_E^{\frac{\alpha_E(m_{EX}+p_E)}{2}-1}e^{-\mathrm{I}_E\gamma_E^{\frac{\alpha_E}{2}}}d\gamma_E,\tag{7}$$

considering Equation (7) relates to complicated power exponential integration, to be specific, the lower bound expression of SOP [25] can be gained.

When $\gamma_E \to \infty$, Z is rewritten as

$$
\begin{aligned}
Z &= \Upsilon\left(m_{DX}+p_D, \mathrm{I_D}(\Lambda\gamma_E+\Lambda-1)^{\frac{\alpha_D}{2}}\right) \\
&= \Upsilon\left(m_{DX}+p_D, \mathrm{I_D}(\Lambda\gamma_E)^{\frac{\alpha_D}{2}}\left(1+\frac{\Lambda-1}{\Lambda\gamma_E}\right)^{\frac{\alpha_D}{2}}\right) \\
&\xrightarrow{\gamma_E\to\infty} \Upsilon\left(m_{DX}+p_D, \mathrm{I_D}(\Lambda\gamma_E)^{\frac{\alpha_D}{2}}\right),
\end{aligned} \tag{8}
$$

then, the lower bound of SOP is defined by

$$
\begin{aligned}
P_{SOP} &= \Pr\{\gamma_D \le \Lambda\gamma_E+\Lambda-1\} \\
&\ge P_{SOP}^{L} = \Pr\{\gamma_D \le \Lambda\gamma_E\},
\end{aligned} \tag{9}
$$

with the aids of Equation (8.4.16.1) [26] and Equation (11) [27], letting $\gamma_E^{\frac{\alpha_D}{2}} = t$ and using Equation (2.24.1.1) [26], after a series of mathematical operations, we can get the accurate expression of Equation (7) as

$$
\begin{aligned}
Q^L &= \int_0^\infty Z^L \times \gamma_E^{\frac{\alpha_E(m_{EX}+p_E)}{2}-1} e^{-\mathrm{I_E}\gamma_E^{\frac{\alpha_E}{2}}} d\gamma_E \\
&= \frac{2}{\alpha_D}\int_0^\infty t^{\frac{\alpha_E(m_{EX}+p_E)}{\alpha_D}-1} \\
&\times G_{1,2}^{1,1}\left(\mathrm{I_D}\Lambda^{\frac{\alpha_D}{2}} t \,\middle|\, \begin{matrix} 1 \\ m_{DX}+p_D, 0 \end{matrix}\right) \\
&\times G_{0,1}^{1,0}\left(\mathrm{I_E} t^{\frac{\alpha_E}{\alpha_D}} \,\middle|\, \begin{matrix} - \\ 0 \end{matrix}\right) dt \\
&= \frac{2{\alpha_E}^{m_{DX}+p_D+\Theta-\frac{3}{2}}\left(\mathrm{I_D}\Lambda^{\frac{\alpha_D}{2}}\right)^{-\Theta}}{\sqrt{\alpha_D}(2\pi)^{\frac{\alpha_D+\alpha_E}{2}-1}} \\
&\times G_{2\alpha_E,\alpha_D+\alpha_E}^{\alpha_D+\alpha_E,\alpha_E}\left(\frac{(\mathrm{I_E})^{\alpha_D}{\alpha_E}^{\alpha_E}}{\left(\mathrm{I_D}\Lambda^{\frac{\alpha_D}{2}}\right)^{\alpha_E}{\alpha_D}^{\alpha_D}} \right. \\
&\left.\middle|\, \begin{matrix} \Delta(\alpha_E, N), \Delta(\alpha_E, 1-\Theta) \\ \Delta(\alpha_D, 0), \Delta(\alpha_E, -\Theta) \end{matrix}\right),
\end{aligned} \tag{10}
$$

where Q^L and Z^L represent the deformations of Q and Z when $\gamma_E \to \infty$. Finally, substituting Equation (10) into Equation (6), Equation (5) can be obtained.

3.2. SPSC analysis

SPSC is the another key index for measuring the performance of communication models, it stands for the probability of instantaneous confidentiality ability is higher than zero [23,24]. The SPSC is defined as

$$
P_{SPSC} = \Pr(C_S > 0). \tag{11}
$$

According to the definition of instantaneous secrecy capacity, the condition $C_S > 0$ can be further transformed as

$$
\begin{aligned}
P_{SPSC} &= \Pr\left(C_S > 0\right) \\
&= \Pr\left(C_D - C_E > 0\right) \\
&= \Pr\left\{\frac{1+\gamma_D}{1+\gamma_E} > 1\right\} \\
&= \Pr\left(\gamma_D > \gamma_E\right) \\
&= 1 - \Pr\left(\gamma_D \leq \gamma_E\right).
\end{aligned} \tag{12}
$$

Then, using the PDF of the eavesdropper channel and the CDF of the main channel, P_{SPSC} can be written as

$$
\begin{aligned}
P_{SPSC} &= 1 - \int_0^{\infty}\int_0^{\gamma_E} f_D\left(\gamma_D\right)d\gamma_D f_E\left(\gamma_E\right)d\gamma_E \\
&= 1 - \int_0^{\infty} F_D\left(\gamma_E\right) f_E\left(\gamma_E\right)d\gamma_E.
\end{aligned} \tag{13}
$$

Substituting Equation (2) and Equation (3) into Equation (13), and then applying the corresponding Meijer's G-function integral identities, the exact SPSC expression can be obtained as follows.

Theorem 2: For the α-BX shadowed fading channels, the accurate analytical expression for the SPSC can be expressed by

$$
\begin{aligned}
P_{SPSC} = 1 &- \frac{\alpha_D(1-\xi_D)^{m_{DY}}\left(\Psi_D\right)^{-\frac{\alpha_D m_{DX}}{2}}}{2(\lambda_{\alpha_D})^{m_{DX}}\Gamma\left(m_{DX}\right)} \\
&\times \frac{\alpha_E(1-\xi_E)^{m_{EY}}\left(\Psi_E\right)^{-\frac{\alpha_E m_{EX}}{2}}}{2(\lambda_{\alpha_E})^{m_{EX}}\Gamma\left(m_{EX}\right)} e^{-\frac{1}{C\alpha_E}\left(\frac{1}{\Psi_E}\right)^{\frac{\alpha_E}{2}}} \\
&\times \sum_{p_D=0}^{\infty} \frac{\left(m_{DY}\right)_{p_D}\left(\frac{\xi_D}{\lambda_{\alpha_D}}\right)^{p_D}\left(\frac{1}{\Psi_D}\right)^{\frac{\alpha_D p_D}{2}}}{\left(m_{DX}\right)_{p_D} p_D!\frac{\alpha_D}{2}\left(\mathrm{I}_D\right)^{m_{DX}+p_D}} \\
&\times \sum_{p_E=0}^{\infty} \frac{\left(m_{EY}\right)_{p_E}\left(\frac{\xi_E}{\lambda_{\alpha_E}}\right)^{p_E}\left(\frac{\gamma_E}{\Psi_E}\right)^{\frac{\alpha_E p_E}{2}}}{\left(m_{EX}\right)_{p_E} p_E!} \\
&\times \frac{2{\alpha_E}^{m_{DX}+p_D+\Theta-\frac{3}{2}}\left(\mathrm{I}_D\right)^{-\Theta}}{\sqrt{\alpha_D}(2\pi)^{\frac{\alpha_D+\alpha_E}{2}-1}} \\
&\times G_{2\alpha_E,\alpha_D+\alpha_E}^{\alpha_D+\alpha_E,\alpha_E}\left(\frac{\left(\mathrm{I}_E\right)^{\alpha_D}{\alpha_E}^{\alpha_E}}{\left(\mathrm{I}_D\right)^{\alpha_E}{\alpha_D}^{\alpha_D}}\right. \\
&\left.\left|\begin{array}{l}\Delta\left(\alpha_E,N\right),\Delta\left(\alpha_E,1-\Theta\right) \\ \Delta\left(\alpha_D,0\right),\Delta\left(\alpha_E,-\Theta\right)\end{array}\right.\right).
\end{aligned} \tag{14}
$$

Proof: Similarly, the symbols have been given. By utilizing the integral equations (Equation (8.4.16.1) [26], Equation (2.24.1.1) [26] and Equation (11) [27]), we can obtain Equation (14).

4. Security prediction algorithm based on Self-LSTM

The Self-LSTM algorithm is proposed in this section. We focus on introduce the data set, network structure and specific details of the algorithm.

4.1. Data set

The dataset is defined as D_k, $D_k = (X_k, y_k)$. The input is $X_k = (x_{k1}, \ldots, x_{k11})$, where X_k consists of eleven input features, m_{DX},m_{DY}, Ω_{DX}, Ω_{DY}, α_D, m_{EX}, m_{EY},Ω_{EX}, Ω_{EY}, α_E and Ψ, respectively. The output is y_k.

We apply Min-Max normalization to preprocess the raw data, All data are scaled into the range [0, 1]. It can be formulated as

$$y_{mn} = \frac{x_{mn} - min\left(x_{mn}\right)}{max\left(x_{mn}\right) - min\left(x_{mn}\right)}, \tag{15}$$

where x_{mn} is original input data and y_{mn} is normalized data.

4.2. Self-LSTM architecture

Figure 1 illustrates the Self-LSTM architecture, which is composed of an input layer, an LSTM layer, a self-attention module, and an output layer. Figure 2 draws the specific internal structure of LSTM layer.

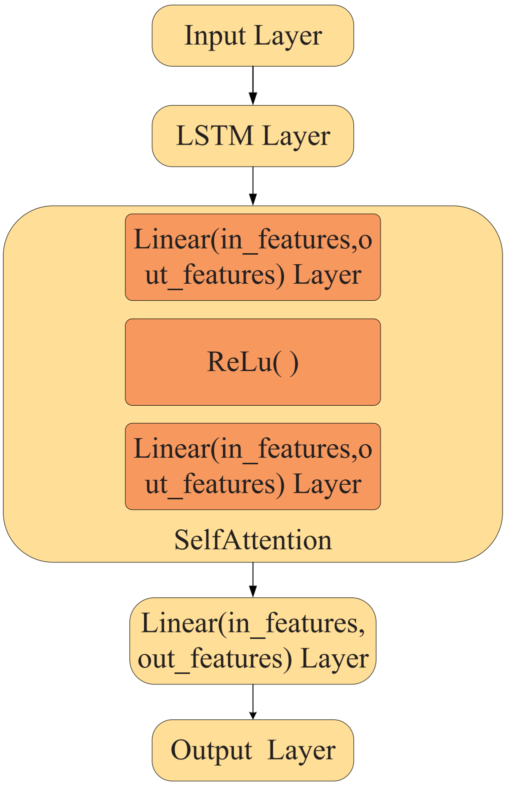

Figure 1. The structure of the Self-LSTM.

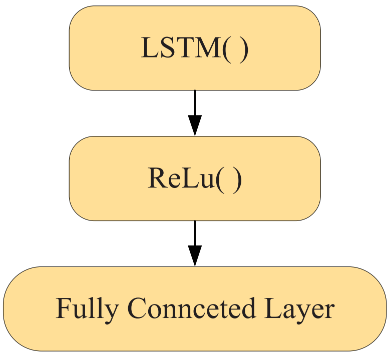

Figure 2. The components of the LSTM layer.

4.3. Self-LSTM prediction algorithm

Algorithm 1 presents the pseudo-code of the Self-LSTM algorithm. The concrete steps of the algorithm are as follows:

(1) Building the data set: According to Equation (5), we randomly select the values of each fading parameters to get the data set.The dataset is divided into three subsets: training, testing, and prediction. The parameters are shown in Table 2.

(2) Preprocessing data set: The data set is processed Max–Min normalization by utilizing Equation (15).

(3) Initializing the hyperparameters: We configure the network by specifying the initial hyperparameter values.

(4) Model training and testing: Iterative training is performed to update the network parameters, and the best-performing model on the validation set is retained for future testing.

(5) Predicting the Self-LSTM network: We load the saved checkpoint and apply it to the test samples to obtain predictions, which are then stored for further evaluation.

Algorithm 1 The Self-LSTM prediction algorithm

Input:
The ranges $l_1, l_2, l_3, l_4, l_5, l_6, l_7, l_8, l_9, l_{10}, l_{11}$ of the selected 11 variables, m_{DX}, m_{DY}, Ω_{DX}, Ω_{DY}, α_D, m_{EX}, m_{EY}, Ω_{EX}, Ω_{EY}, α_E;
Output:
The predictive values of SOP;
1: **for** k=1:11 **do**
2: $x_k = rand\,(l_k, g)$;
3: **end for**
4: $y = Equation\ (5)\,(x_1, x_2, x_3, \ldots, x_{11})$;
5: $Trainingset = [x_1, x_2, x_3, \ldots, x_{11}, y]$;
6: $Testingset = [x_1, x_2, x_3, \ldots, x_{11}, y]$;
7: $Predictingset = [x_1, x_2, x_3, \ldots, x_{11}, y]$;
8: Initialize network hyperparameters;
9: Train Self-LSTM using Training set and Testing set to obtain the trained network $Model$;
10: Obtain the predicting set output for the network $y = Model\,(Predictingset)$;
11: Calculate mean square error (MSE) and absolute error (AE).

Table 2. Dataset parameters.

Notation	**Meaning**
input	m_{DX}, m_{DY}, Ω_{DX}, Ω_{DY}, α_D, m_{EX}, m_{EY}, Ω_{EX}, Ω_{EY}, α_E
output	y_k
total	8050
training sets	6400
testing sets	1600
predicting data	50

4.4. Performance evaluation index

MSE and AE are used to evaluate the model performance. The MSE and AE are expressed by

$$\mathrm{MSE} = \frac{\sum_{g=1}^{V} (a_g - p_g)^2}{V}, \tag{16}$$

and

$$\mathrm{AE} = |a_g - p_g|, \tag{17}$$

where a is the actual value, p denotes the predicted value, and V stands for the quantity of the estimation sample.

5. Numerical results

This section finishes the theoretical simulation analysis and algorithm analysis. Specifically, we provides the simulation images and discusses the influences of fading parameters on the performance of PLS. Moreover, the prediction performance of the Self-LSTM algorithm is analyzed. The theoretical analysis and Monte Carlo simulations are implemented via MATLAB R2022b. The training and testing procedures are executed on an AMD R7 5800H processor.

5.1. Theoretical analysis

The theoretical results and Monte Carlo curves are displayed in this section. The analysis and simulation results are consistent. Moreover, we discussed the influences of fading parameters on the performance of model over α-BX shadowed distribution. The public parameters are $\Omega_{EX} = 10\,\text{dB}$, $\Omega_{DY} = \Omega_{EY} = -2\,\text{dB}$, $m_{EY} = 2$, $C_{th} = 1\,\text{dB}$ and $\Lambda = \exp(C_{th})$. In addition, $\Psi_D = \lambda\Psi_E$, λ is the ratio of the received SNR between the legal and the wiretap links, SOP simulation: $\Psi_E = 20\,\text{dB}$, whereas $\Psi_E = 1\,\text{dB}$ when SPSC simulation.

Figure 3 and Figure 4 compare the simulation results of SOP and SPSC *versus* λ for diverse (α_D, α_E). The simulation curves matched with the analysis results, which confirms the correctness of theoretical formulas. When $\alpha_E = 1$, a larger α_D causes a lower SOP and a higher SPSC. Therefore, we can get the conclusion that greater α_D can improve the secrecy performance.

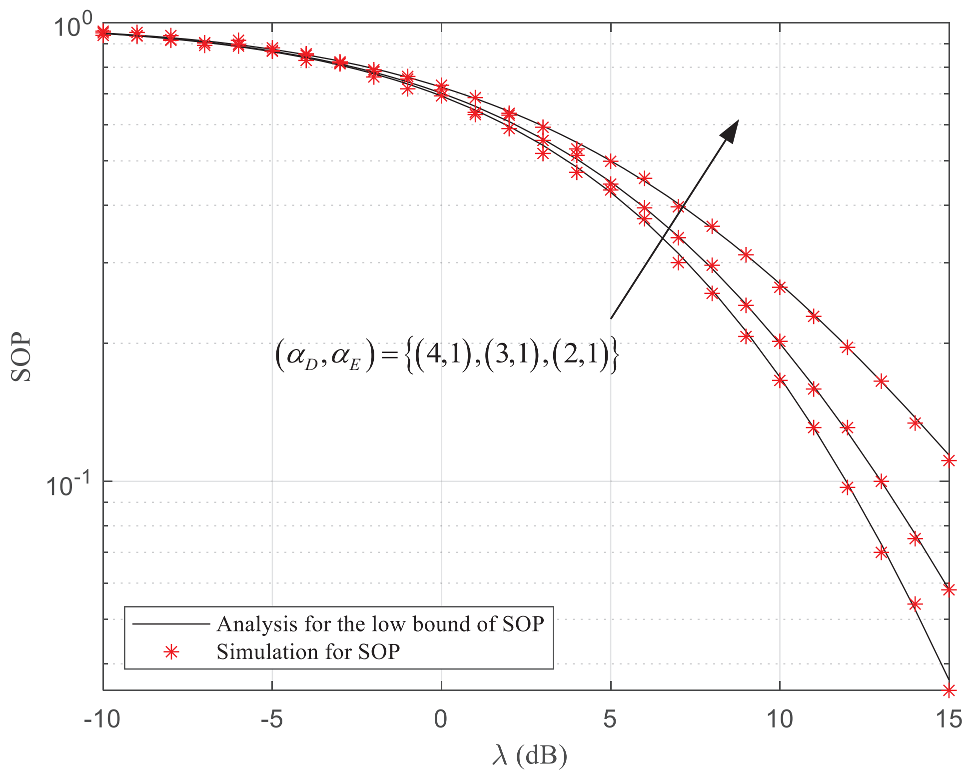

Figure 3. SOP *versus* λ with various (α_D, α_E), $m_{DX} = 1$, $m_{DY} = m_{EX} = 2$, $\Omega_{DX} = 10\,\text{dB}$.

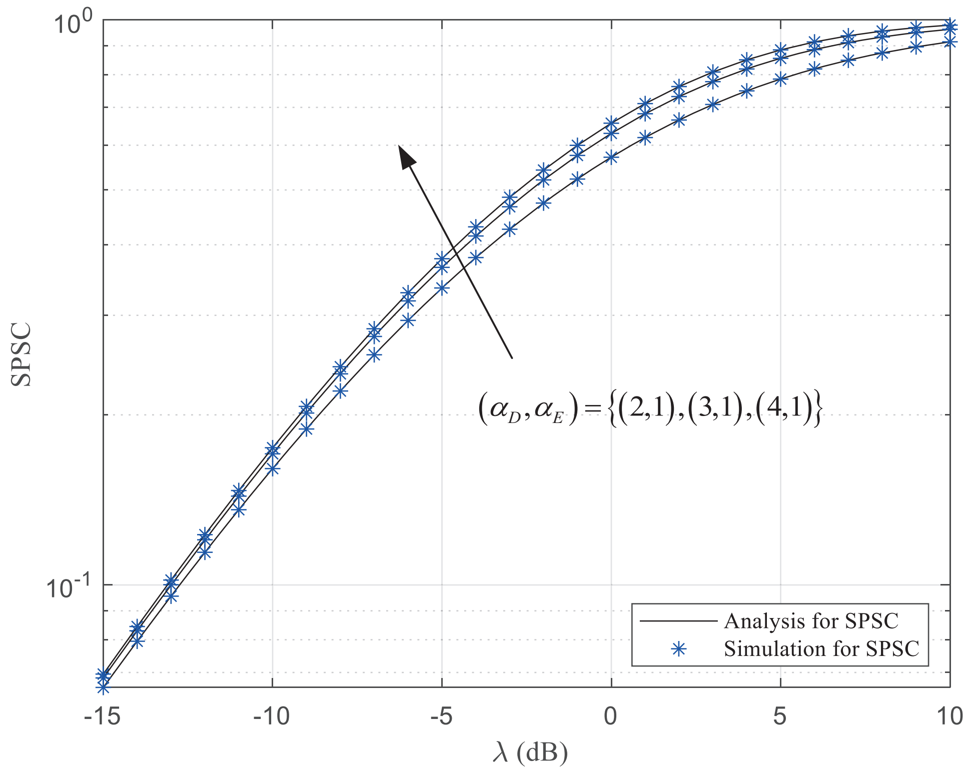

Figure 4. SPSC *versus* λ with various (α_D, α_E), $m_{DX} = 1$, $m_{DY} = m_{EX} = 2$, $\Omega_{DX} = 10$ dB.

Figure 5 and Figure 6 plot the SOP and SPSC *versus* λ for various parameters (m_{DX}, m_{DY}). The Monte Carlo curves and theoretical analysis images are matchable. The larger m_{DX} and m_{DY} decrease the SOP and increase the SPSC. We found the fact that greater m_{DX} and m_{DY} are conductive to enhancing the performance of considered model.

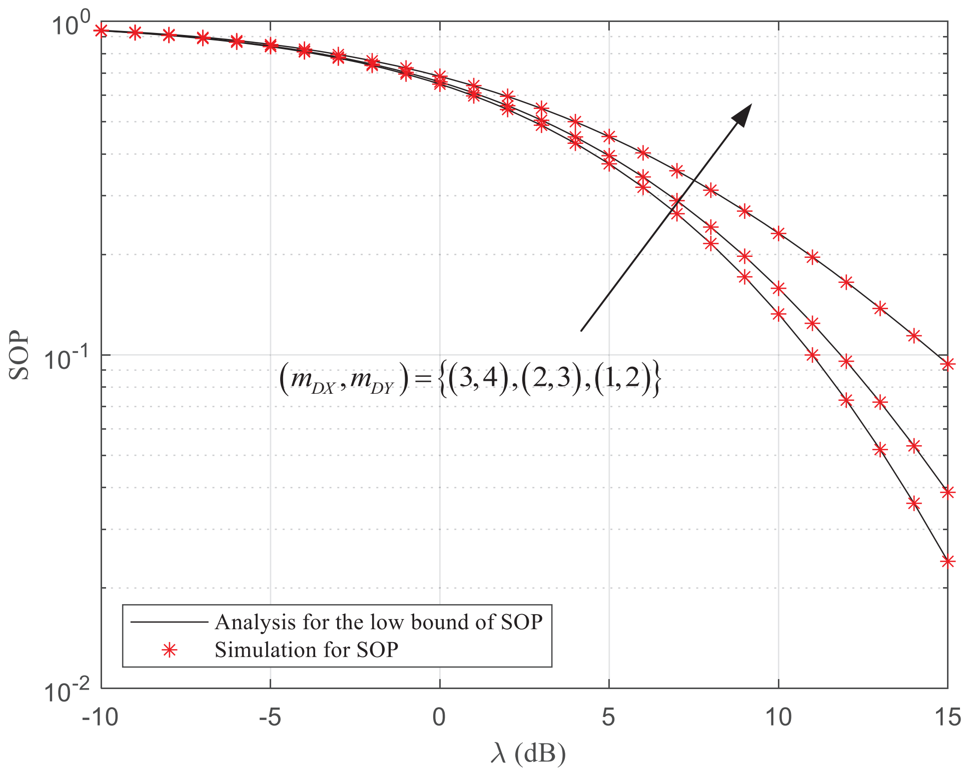

Figure 5. SOP *versus* λ with various (m_{DX}, m_{DY}), $m_{EX} = 2$, $\Omega_{DX} = 10\,$dB, $\alpha_D = 2$, $\alpha_E = 1$.

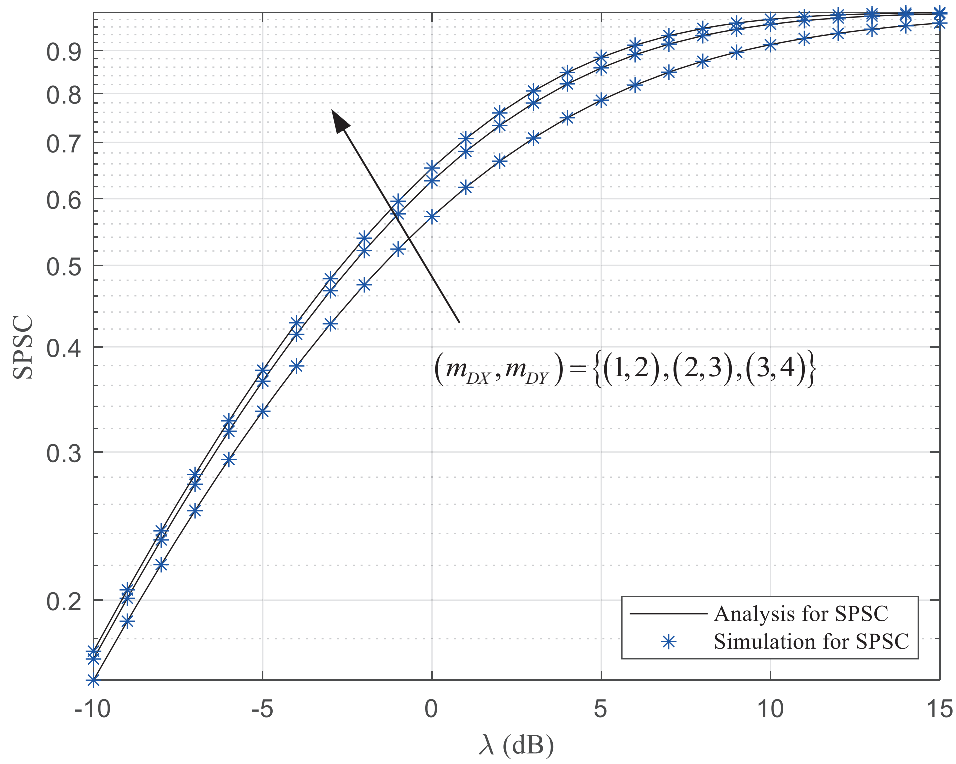

Figure 6. SPSC *versus* λ with various (m_{DX}, m_{DY}), $m_{EX} = 2$, $\Omega_{DX} = 10\,\text{dB}$, $\alpha_D = 2$, $\alpha_E = 1$.

Figure 7 and Figure 8 depict the SOP and SPSC *versus* λ for different $(\Omega_{DX}, \Omega_{EX})$. The theoretical results and simulation analysis are coincident. When $\Omega_{EX} = 10\,\text{dB}$, the lower Ω_{DX} causes smaller SOP and larger SPSC, which means that smaller Ω_{DX} can reinforce the security of Wyner's model over α-BX shadowed fading channels.

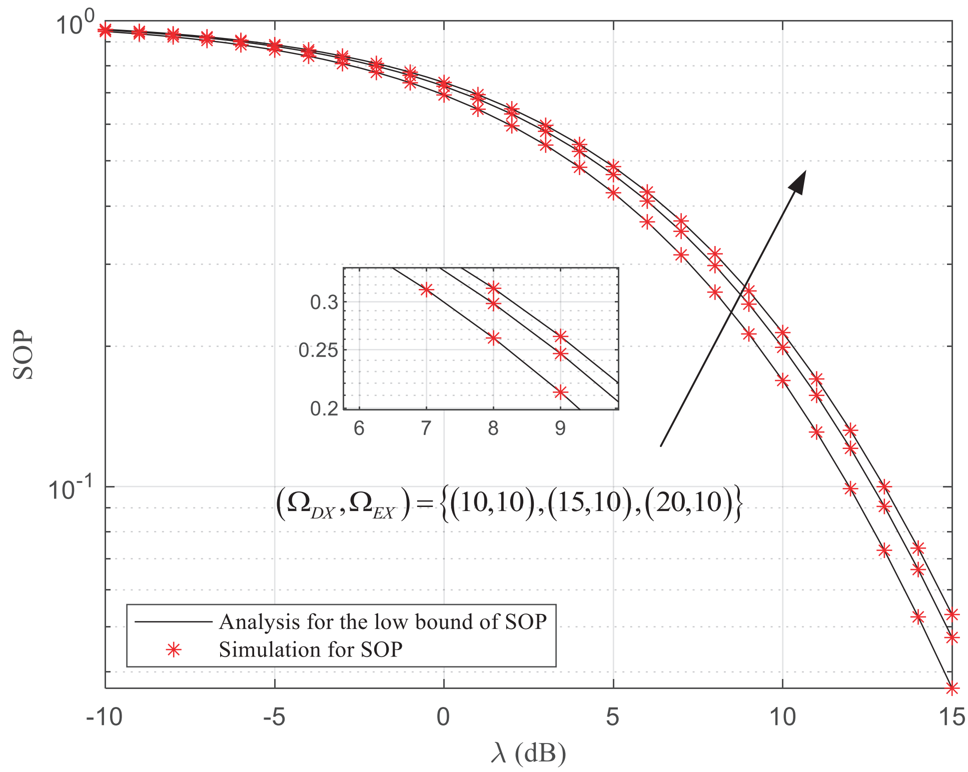

Figure 7. SOP *versus* λ with various $(\Omega_{DX}, \Omega_{EX})$, $m_{DX} = 1$, $m_{DY} = m_{EX} = 2$, $\alpha_D = 4$, $\alpha_E = 1$.

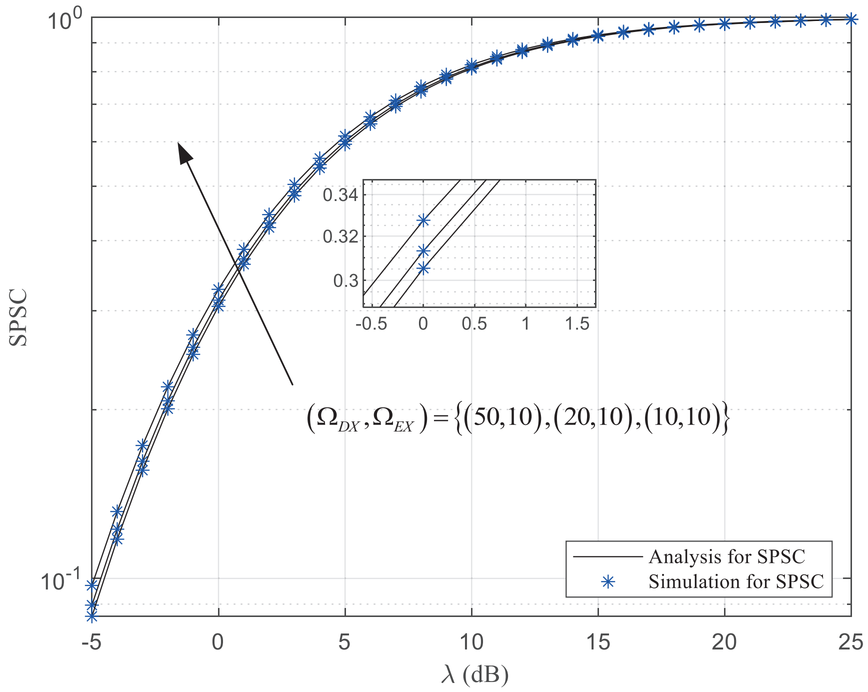

Figure 8. SPSC *versus* λ with various $(\Omega_{DX}, \Omega_{EX})$, $m_{DX} = m_{DY} = 2$, $m_{EX} = 1.5$, $\alpha_D = 1$, $\alpha_E = 4$.

5.2. Evaluation of prediction accuracy

According to the evaluation indicators of algorithm performance, we provides the prediction results of four algorithms.

The dataset consists of 8050 samples, of which 6400 are used for training and 1600 for testing. We update weights and biases constantly to avoid occurring the over-fitting phenomenon. Finally, 50 pieces of data are used to predict the ultimate results.

Figures 9–12 plot the MSE and AE images of the four networks. Figure 13 and Figure 14 describe the MSE value and runtime for the four networks. The Self-LSTM exhibits higher prediction accuracy and lower time consumption, as illustrated in Figure 13 and Figure 14.

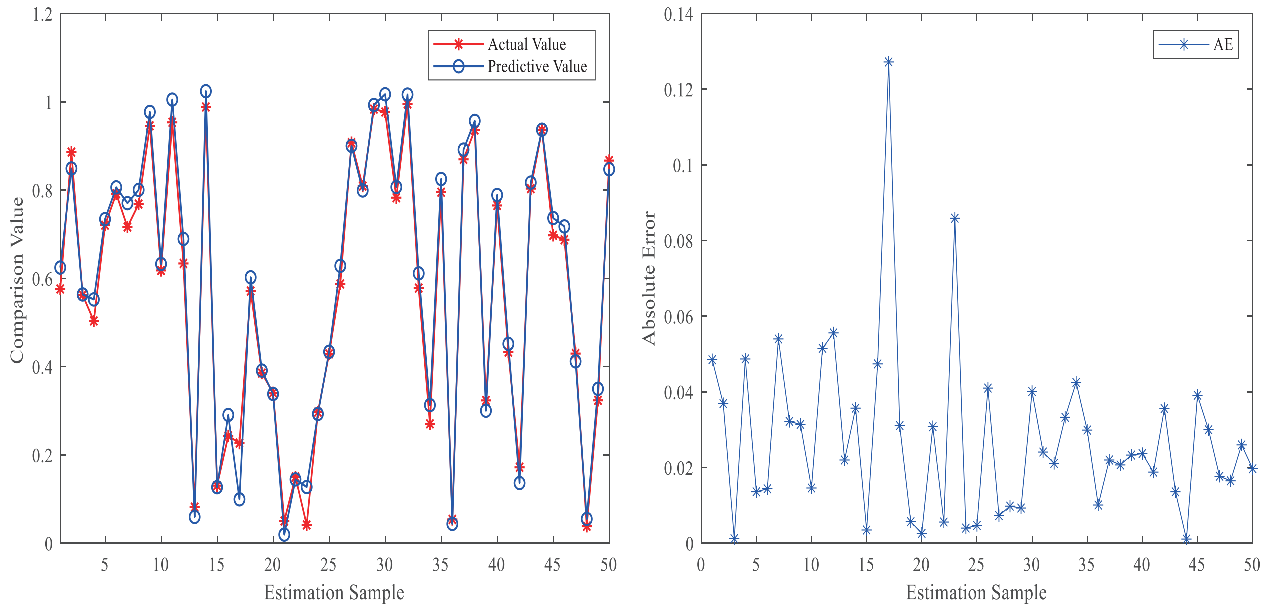

Figure 9. Self-LSTM.

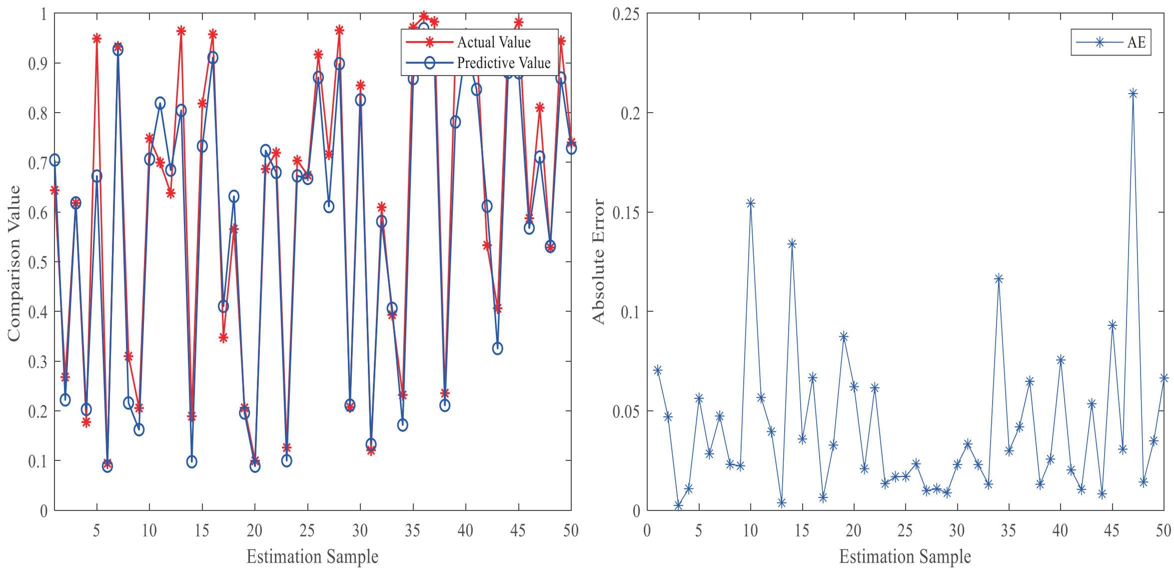

Figure 10. LSTM.

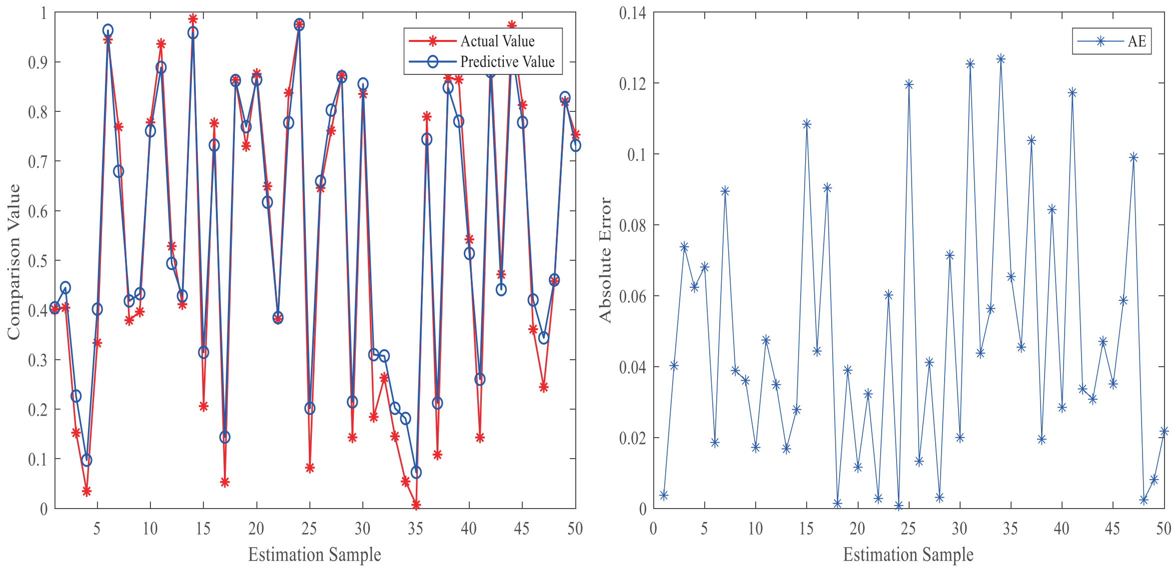

Figure 11. DenseNet.

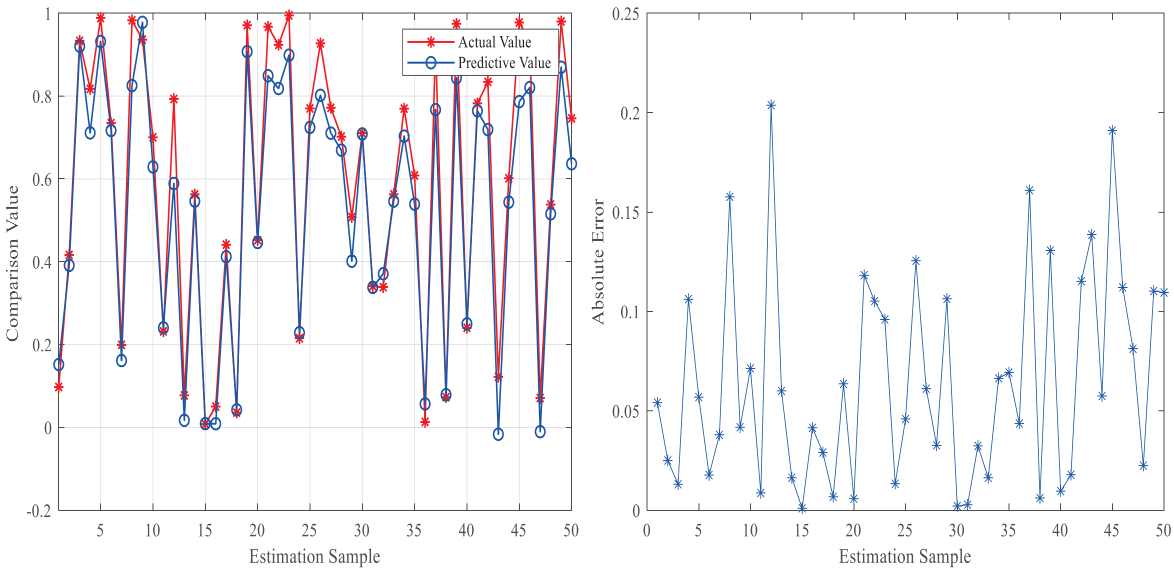

Figure 12. CNN.

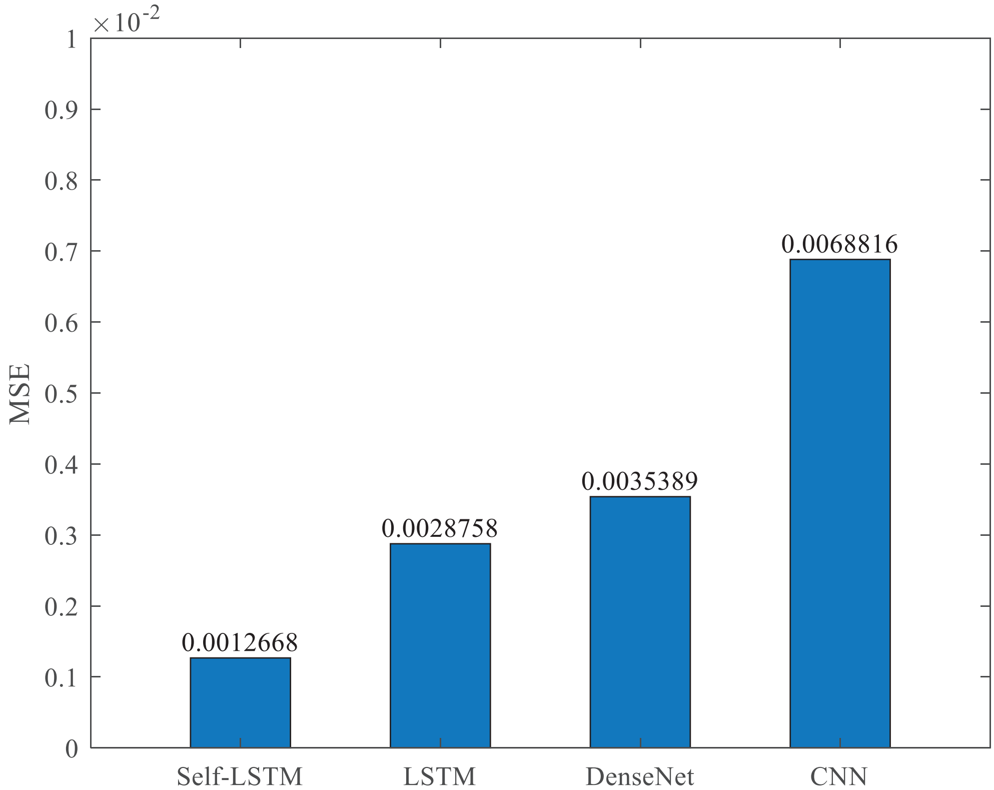

Figure 13. The MSE of four prediction algorithms.

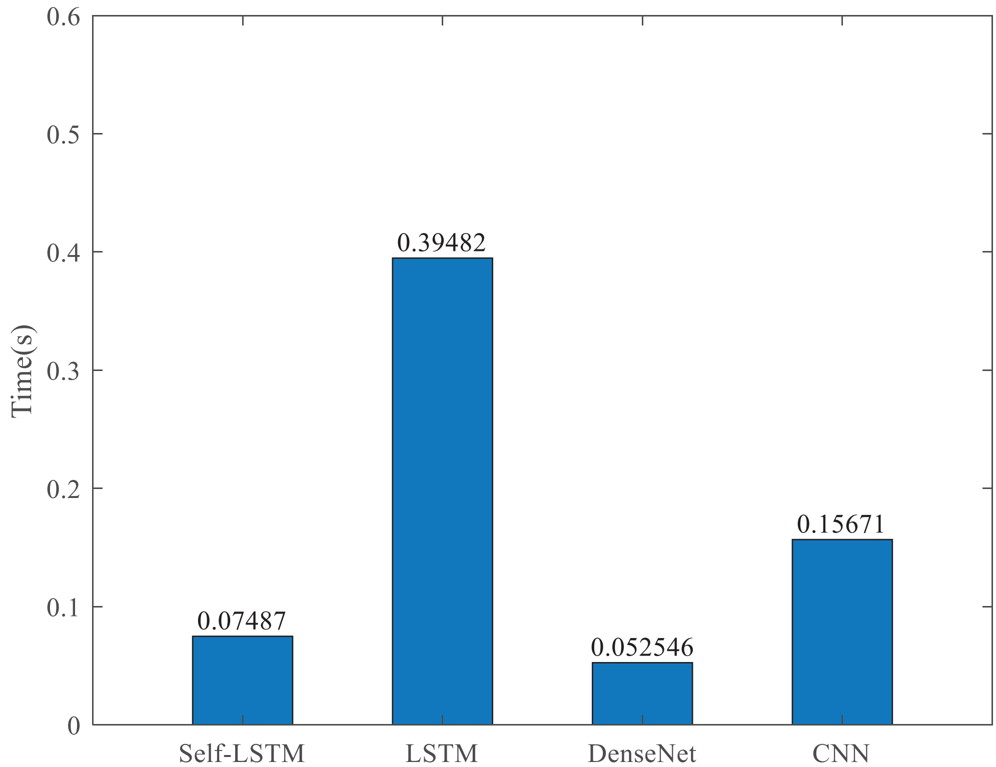

Figure 14. The running time (s) of four prediction algorithms.

6. Conclusion

In this paper, we investigate the secrecy performance based on Wyner's wiretap model over α-BX shadowed fading channels and predict the security performance by using the proposed Self-LSTM. The analytic expressions of SOP and SPSC are derived. Through massive simulation, the validity of the analysis results is verified. More specifically, the impacts of fading parameters on the performance of wiretap model are analyzed. The research results demonstrate that a higher α_D, m_{DX} and m_{DY} or a lower Ω_{DX} are helpful in enhancing the secrecy performance of PLS. Meanwhile, the results demonstrate that the Self-LSTM achieves higher accuracy and shorter runtime than the standard LSTM, DenseNet and CNN algorithms. In the future, we will combine the more complex algorithm to evaluate the security of considered system.

Data availability statement

The data or datasets that support the findings of this study are available from the author upon reasonable request.

Declaration of generative AI and AI-assisted technologies

During the preparation of this manuscript, the authors used generative AI tools only to improve language and readability. Specifically, the authors used DeepSeek and ChatGPT for language polishing and readability enhancement in limited sections of the manuscript. The authors take full responsibility for the content of the manuscript.

Acknowledgments

We would like to thank the anonymous reviewers for their constructive comments and suggestions, which helped improve the quality of this paper.

Authors' contribution

Jiangfeng Sun: conceptualization, methodology, supervision, project administration, funding acquisition, writing—review and editing; Shuiwang Niu: software, validation, formal analysis, investigation, data curation, visualization, writing—original draft preparation. All authors have read and agreed to the published version of the manuscript.

Conflicts of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Lei H, Gao C, Guo Y, Pan G. On physical layer security over generalized gamma fading channels. *IEEE Commun. Lett.* 2015, 19(7):1257–1260.

[2] Sun J, Li X, Huang M, Ding Y, Jin J, *et al.* Performance analysis of physical layer security over κ-μ shadowed fading channels. *IET Commun.* 2018, 12(8):970–975.

[3] Lyu Q, Han G, Fu X. Physical layer security in multi-hop AF relay network based on compressed sensing. *IEEE Commun. Lett.* 2018, 22(9):1882–1885.

[4] Li X, Jiang J, Wang H, Han C, Chen G, *et al.* Physical layer security for wireless-powered ambient backscatter cooperative communication networks. *IEEE Trans. Cogn. Commun. Netw.* 2023, 9(4):927–939.

[5] Yadav S, Gurjar DS. Secrecy performance of SIMO underlay cognitive radio networks over α-μ fading channels. *IEEE Access* 2021, 9:62616–62629.

[6] Sun J, Bie H, Li X, Zhang J, Pan G, *et al.* Secrecy performance analysis of SIMO systems over correlated κ-μ shadowed fading channels. *IEEE Access* 2019, 7:86090–86101.

[7] Lou Y, Zheng Y, Cheng J, Zhao H. Performance of SWIPT-based differential AF relaying over Nakagami-*m* fading channels with direct link. *IEEE Wirel. Commun. Lett.* 2017, 7(1):106–109.

[8] Sun J, Wang X, Tian X, Wu Y, Li X. Security analysis of relaying NOMA systems over Beaulieu–Xie fading channels with I/Q imbalance. *Phys. Commun.* 2022, 55:101881.

[9] Li M, Selim B, Muhaidat S, Sofotasios PC, Dianati M, *et al.* Effects of residual hardware impairments on secure NOMA-based cooperative systems. *IEEE Access* 2019, 8:2524–2536.

[10] Hawaibam S, Singh AD. Error rate analysis of different modulation schemes over shadowed Beaulieu–Xie fading channels. *IETE J. Res.* 2023, 69(12):8538–8544.

[11] Gvozdarev AS, Artemova TK. On the physical layer security peculiarities of wireless communications in the presence of the Beaulieu–Xie shadowed fading. *Mathematics* 2022, 10(20):3724.

[12] Silva HS, Almeida DB, Queiroz WJ, Silva HT, Fonseca IE, *et al.* Capacity analysis of shadowed Beaulieu–Xie fading channels. *Digit. Signal Process.* 2022, 122:103367.

[13] Cheng W, Hu Z, Ma T, Nie G. On the statistics of the α-Beaulieu–Xie and its extreme distributions with their applications. *IEEE Commun. Lett.* 2023, 27(3):817–821.

[14] Liang L, Ye H, Yu G, Li GY. Deep-learning-based wireless resource allocation with application to vehicular networks. *Proc. IEEE* 2019, 108(2):341–356.

[15] Hu Q, Gao F, Zhang H, Jin S, Li GY. Deep learning for channel estimation: interpretation, performance, and comparison. *IEEE Trans. Wirel. Commun.* 2020, 20(4):2398–2412.

[16] Chen X, Zhang J, Lin B, Chen Z, Wolter K, *et al.* Energy-efficient offloading for DNN-based smart IoT systems in cloud-edge environments. *IEEE Trans. Parallel Distrib. Syst.* 2021, 33(3):683–697.

[17] Raj V, Kalyani S. Backpropagating through the air: deep learning at physical layer without channel models. *IEEE Commun. Lett.* 2018, 22(11):2278–2281.

[18] Mattu SR, Theagarajan LN, Chockalingam A. Deep channel prediction: a DNN framework for receiver design in time-varying fading channels. *IEEE Trans. Veh. Technol.* 2022, 71(6):6439–6453.

[19] Zappone A, Di Renzo M, Debbah M. Wireless networks design in the era of deep learning: model-based, AI-based, or both? *IEEE Trans. Commun.* 2019, 67(10):7331–7376.

[20] Gvozdarev AS. Closed-form analysis of the α-Beaulieu–Xie shadowed fading channel. *IEEE Wirel. Commun. Lett.* 2023, 12(9):1623–1627.

[21] Gradshteyn IS, Ryzhik IM. Table of integrals, series, and products. *Math. Comput.* 2007, 20(96):1157–1160.

[22] Arti MK. Beamforming and combining based scheme over κ-μ shadowed fading satellite channels. *IET Commun.* 2016, 10(15):2001–2009.

[23] Barros J, Rodrigues MR. Secrecy capacity of wireless channels. In *Proceedings of the 2006 IEEE International Symposium on Information Theory*, Seattle, USA, July 9–14, 2006, pp. 356–360.

[24] Bloch M, Barros J, Rodrigues MR, McLaughlin SW. Wireless information-theoretic security. *IEEE Trans. Inf. Theory* 2008, 54(6):2515–2534.

[25] Liu X. Probability of strictly positive secrecy capacity of the Weibull fading channel. In *Proceedings of the 2013 IEEE Global Communications Conference*, Atlanta, USA, December 9–13, 2013, pp. 659–664.

[26] Prudnikov AP, Brychkov YA, Marichev OI. *Integrals and Series, Volume 3: More Special Functions*, 1st ed. New York: Gordon and Breach Science Publishers, 1990.

[27] Adamchik VS, Marichev O. The algorithm for calculating integrals of hypergeometric-type functions and its realization in the REDUCE system. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, Tokyo, Japan, August 20–24, 1990, pp. 212–224.