Wireless Personal Communications (2022) 124:2299–2312
https://doi.org/10.1007/s11277-022-09465-9

On Physical Layer Security of Double Shadowed Rician Fading Channels

Rupender Singh[1] · **Meenakshi Rawat**[1] · **Elias Yaacoub**[2]

Accepted: 4 January 2022 / Published online: 16 January 2022

Abstract
With the proliferation of fifth-generation (5G) mobile communication wireless networks, the investigation into the performance of physical layer secrecy is increasingly becoming the center of attention of recent studies. Physical layer security (PLS) is the pivotal notion of enhancing the secrecy of mobile communication wireless networks against eavesdropping by utilizing the intrinsic randomness of the wireless channel. In this study, we focus on the information-theoretic secrecy perspective in which authorized users convey their information to each other through a quasi-static channel and adversary users are obtaining this secret information through illegitimate wiretap quasi-static channel, where it is assumed that all the channels are represented as double shadowed Rician distributed. In this context, analytical solutions for the expressions of various physical layer secrecy metrics include the strictly positive secrecy capacity (SPSC) and the lower bound on secure outage probability (SOP^L) are procured in closed-form. In addition, another physical layer secrecy metric, i.e., average secrecy capacity (ASC) is also investigated and determined in analytical closed-form. The effect of double shadowing on the performance of PLS is investigated. It is found that severer shadowing improves the secrecy performance. Our results also show that the legitimate users can communicate secretly when the legitimate channel link is superior to illegitimate channel link.

Keywords Average secrecy capacity (ASC) · Double shadowed Rician fading · Mobile communication wireless networks · Secure outage probability (SOP) · Strictly positive secrecy capacity (SPSC)

✉ Rupender Singh
rupendersingh04cs39@gmail.com

Meenakshi Rawat
meenakshirawat_uofc@yahoo.ca

Elias Yaacoub
Elias@qu.edu.qa

[1] Department of Electronics and Communication Engineering, Indian Institute of Technology, Roorkee 247667, India

[2] Department of Computer Science and Engineering, Qatar University, Doha, Qatar

1 Introduction

Recently, physical layer security (PLS) of fifth-generation (5G) enabled mobile communication wireless networks have captivated considerable research attention since these approaches make wireless communication more invulnerable against eavesdropping without relying on different conventional encryption algorithms such as advanced encryption standard (AES), twofish encryption algorithm, blowfish encryption algorithm, and Rivest–Shamir–Adleman (RSA) [1–5]. Unlike these conventional algorithms, PLS is an information-theoretic based approach which exploits the intrinsic random behavior of wireless channels to provide secure communication in the strictest form. Numerous works exist that explore the secrecy performance of PLS in diverse small-scale fading scenarios such as Rayleigh, Nakagami-q, Rician, Weibull, α-μ and κ-μ, etc. in [6–11]. On the other hand, none of these traditional fading conditions characterize the new emerging mobile communication wireless networks scenarios such as Internet of Things (IoT), indoor-to-outdoor propagation, Ultra-dense networks, body area networks, and device-to-device (D2D) communication [12–14]. It is found in recent literature that these applications utilize long-term wireless medium that may be impacted by the shadowing. Hence, various works have been devoted to examining the behavioral performance of PLS over composite multipath/shadowed fading channels.

The repercussions of fading parameters on the performance of secure transmission through composite multipath/shadowed fading was studied in [15–20]. Lei et al. [15] anatomized the PLS performance of wireless systems in generalized-K (GK) fading channels. They derived closed-form solutions for the expressions of various PLS metrics, including average secrecy capacity (ASC), strictly positive secrecy capacity (SPSC), and secure outage probability (SOP) by using mixtures of gamma (MG) distribution. Further, this work was extended in [16]. The authors modelled the instantaneous signal-to-noise ratio (SNR) of legitimate users' channel and eavesdropper's channel as MG distributed. In [17], SOP, SPSC, and ASC were determined with help of Meijer-G function for correlated Nakagami-m/Gamma fading channels. This Meijer-G function is defined by using Mellins-Bernas' integral representation. A similar analysis for Fisher-Snedecor F fading conditions was presented in [18]. Ai et al. [19] analyzed the secure communication for PLS over double shadowed Rician fading channels. They derived SOP and SPSC expressions in closed-form using moment generating function (MGF) method. In [20], the authors studied secrecy characteristics for PLS over composite Weibull/lognormal fading channels with diversity analysis. They derived the PLS metrics for both the scenarios such as single eavesdropper and two eavesdroppers.

Recently, Simmons et al. [21] have developed a new comprehensive and unified fading distribution, called double shadowed Rician distribution. This unified fading distribution encompasses different fading models such as Rayleigh, Rician, Nakagami-q, shadowed Rician, and shadowed Rayleigh. This double shadowed Rician fading model comes from the scenarios where a Rician fading channel encounters double shadowing, which is resulted due to the combined effect of the line-of-sight (LOS) and the composite components. This fading distribution is very useful to model the scenario, where SNR of the channel link between transmitter and receiver follows varying shadowing levels, while the secondary round of shadowing is resulted because of moving obstacles. Moreover, this distribution is potentially suitable for modelling the channels in underwater acoustic communication, high-speed train communication and land mobile satellite systems.

Motivated by the recent advances in security issues in mobile communication wireless networks and aiming at investigating secure performance metrics include the SOP, SPSC, and ASC for analyzing PLS performance, we adopt a double shadowed Rician fading channel model for legitimate users' and eavesdropper's channels. In this paper, physical layer secrecy of double shadowed Rician fading environments is investigated and the expressions for different PLS performance metrics, including SOP, SPSC, and ASC are derived in closed-form using information-theoretic formulation based Wyner's wiretap model.

The remnant of this work is composed in the following manner. In Sect. 2, the channel and system model contemplated in this study is reviewed. In Sect. 3, the novel expressions for PLS metrics, including SOP, SPSC, and ASC are derived in closed-form. In Sect. 4, the obtained results are demonstrated with detailed discussion. Finally, Sect. 5 fruitions this work with concluding remarks.

2 Channel and System Model

In this study, we are considering single-input-single-output (SISO) mobile communication wireless network model illustrated in Fig. 1, which includes legitimate mobile source (A), legitimate destination (B), and illegitimate mobile eavesdropper (E). A is trying to communicate secretly with B in the presence of E, which is trying to hear the secret information through eavesdropper's channel. In order to investigate the secrecy performance of the system under consideration, it is supposed that all communicating channels are subject to double shadowed Rician fading. The definitions of the parameters with their notations are provided in Table 1. If 1received signals at B and E are denoted by r_M and r_E, respectively, then, r_M and r_E can be written as

$$r_M(t) = h_M(t)s(t) + n_M(t) \tag{1}$$

$$r_E(t) = h_E(t)s(t) + n_E(t) \tag{2}$$

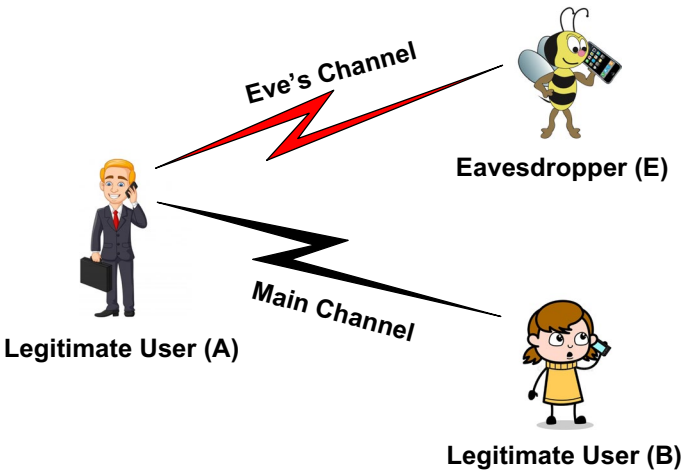


Fig. 1 Mobile communication single-hop wireless network model

Table 1 Notations for parameters

Parameters	Description
b	Representing subscript $b \in \{M, E\}$
$(a)_n$	Pochhamer symbol [23, Eq. (06.10.02.0001.01)]
m_s	Fading parameters of inverse Nakagami-m
m_d	Fading parameters of Nakagami-m
k	Rician parameter
$G_{p,q}^{m,n}(\cdot)$	Meijer's G-function [24, Eq. (8.2.1.1)]
$G_{p,q:t,u:y,z}^{m,n:r,s:w,x}[\cdot]$	Extended generalized bivariate Meijer-G function [EGBMGF] [25, Eq. (1)]

where $h_i(t)$ is representing the coefficients of quasi-static (i.e. $h_i(t) = h_i \ \forall i$) double shadowed Rician fading channel between A and B (or A and E), $i \in (M, E)$. $n_M(t)$ and $n_E(t)$ represent the complex Gaussian noise at B and E with $E[N_M] = E[N_E] = 0$, $E[N_M] = \sigma_M^2$, and $E[N_E] = \sigma_E^2$.

The corresponding SNR's at B and E are given by γ_M and γ_E, respectively. The probability density functions (PDFs) of γ_M and γ_E can be expressed as [22],

$$f_{\gamma_b}(\gamma_b) = \frac{\overline{\gamma}_b^{m_{s_b}} m_{s_b} (m_{s_b} - 1)^{m_{s_b}} (1 + k_b)}{\left(\gamma_b(1 + k_b) + (m_{s_b} - 1)\overline{\gamma}_b\right)^{m_{s_b}+1}} \left(\frac{m_{d_b}}{m_{d_b} + k_b}\right)^{m_{d_b}} \times {}_2F_1\left(m_{d_b}, m_{s_b} + 1; 1; \frac{k_b(1 + k_b)\gamma_b}{(m_{d_b} + k_b)\left(\gamma_b(1 + k_b) + (m_{s_b} - 1)\overline{\gamma}_b\right)}\right) \tag{3}$$

By using [23], (3) can also be expressed as

$$f_{\gamma_b}(\gamma_b) = \sum_{i=0}^{\infty} \frac{\overline{\gamma}^{m_{s_b}} m_{s_b} (m_{s_b} - 1)^{m_{s_b}} (1 + k_b)^{i+1} (m_{d_b})_i (m_{s_b} + 1)_i \gamma^i}{i!(1)_i \left(\gamma_b(1 + k_b) + (m_{s_b} - 1)\overline{\gamma}_b\right)^{m_{s_b}+i+1}} \left(\frac{m_{d_b}}{m_{d_b} + k_b}\right)^{m_{d_b}} \left(\frac{k_b}{m_{d_b} + k_b}\right)^i \tag{4}$$

which can be expressed in Meijer's G-function representation with the help of equations in [24, Eq. (8.4.2.5)] and [24, Eq. (8.2.2.15)] as

$$f_{\gamma_b}(\gamma_b) = \sum_{i=0}^{\infty} A_{b_i} G_{1,1}^{1,1}\left[\frac{(1 + k_b)\gamma_b}{(m_{s_b} - 1)\overline{\gamma}_b}\middle| \begin{matrix} -m_{s_b} \\ i \end{matrix}\right] \tag{5}$$

where

$$A_{b_i} = \frac{m_{s_b}(1 + k_b) k_b^i (m_{d_b})_i (m_{s_b} + 1)_i}{(m_{d_b} + k_b)^i (m_{s_b} - 1)\overline{\gamma}_b i!(1)_i \Gamma(m_{s_b} + 1 + i)} \left(\frac{m_{d_b}}{m_{d_b} + k_b}\right)^{m_{d_b}} \tag{6}$$

Also, the corresponding cumulative distribution functions (CDFs) can be obtained from (5) as

$$F_{\gamma_b}(\gamma_b) = \sum_{i=0}^{\infty} B_{b_i} G_{2,2}^{1,2}\left[\frac{(1 + k_b)\gamma_b}{(m_{s_b} - 1)\overline{\gamma}_b}\middle| \begin{matrix} 1 & 1 - m_{s_b} \\ i + 1 & 0 \end{matrix}\right] \tag{7}$$

where

$$B_{b_i} = \left(\frac{m_{d_b}}{m_{d_b}+k_b}\right)^{m_{d_b}} \left(\frac{k_b}{m_{d_b}+k_b}\right)^{i} \frac{\left(m_{d_b}\right)_i (i+1)_{m_{s_b}}}{\Gamma\left(m_{s_b}\right)\Gamma(i+1)\Gamma\left(i+m_{s_b}+1\right)} \tag{8}$$

In order to highlight the critical insights, the asymptotic CDF can be derived from (7) using [39, (07.34.06.0006.01)] as

$$F^{\infty}_{\gamma_b}\left(\gamma_b\right) = \sum_{i=0}^{\infty} B_{b_i} \frac{\Gamma(-i-1)\Gamma\left(i+1+m_{s_b}\right)}{\Gamma(i+2)} \left(\frac{\left(1+k_b\right)\gamma_b}{\left(m_{s_b}-1\right)\overline{\gamma_b}}\right)^{i+1} \tag{9}$$

3 Secrecy Capacity Analysis

Here, the exact analytical expressions of secrecy performance metrics for PLS, including lower bound of SOP (SOP^{L}), SPSC, and ASC are derived. For the sake of analysis, it is presumed that transmitter has full channel state information (CSI) of legitimate receiver and adversary receiver to ensure perfect secrecy. If the legitimate transmitter has full CSI of both the channel links, then the channel capacities can be estimated as $C_M = \log_2(1+\gamma_M)$ and $C_E = \log_2(1+\gamma_E)$ for the main channel and eavesdropper's channel, respectively. For one realization pair of SNRs $\left(\gamma_M, \gamma_E\right)$, the secrecy capacity,$C_S$, of quasi-static wiretap channel can be defined from [5] as

$$C_S = \begin{cases} \log_2(1+\gamma_M) - \log_2(1+\gamma_E) & \gamma_M > \gamma_E \\ 0 & \gamma_M \leq \gamma_E \end{cases} \tag{10}$$

3.1 SOP Analysis

The SOP is one of the useful PLS performance metrics and defined as a probability, which is defined for the event when instantaneous secrecy capacity fewer than the predetermined secrecy rate, $R_S \geq 0$. Therefore, SOP can be formulated mathematically as [6]

$$P_{out}(\gamma_{th}) = \text{P}(C_S \leq R_S) = \text{P}\left[\gamma_M \leq (1+\gamma_E)(1+\gamma_{th}) - 1\right] \tag{11}$$

where γ_{th} is denoting the threshold SNR. In terms of γ_{th}, R_S can be expressed as $R_S = \log_2(1+\gamma_{th})$.

Using basic probability theory, (11) can be formulated as

$$P_{out}(\gamma_{th}) = \int_0^{\infty} f_{\gamma_E}(\gamma_E) F_{\gamma_M}\left((1+\gamma_E)(1+\gamma_{th})\right) d\gamma_E \tag{12}$$

After substituting (5) and (7) into (12), we obtain

$$P_{out}(\gamma_{th}) = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} A_{E_j} B_{M_i} \int_0^{\infty} G_{1,1}^{1,1}\left[\frac{\left(1+k_E\right)\gamma_E}{\left(m_{s_E}-1\right)\overline{\gamma_E}}\middle| \begin{matrix} -m_{s_E} \\ j \end{matrix}\right] G_{2,2}^{1,2}\left[\frac{\left(1+k_M\right)\left((1+\gamma_E)(1+\gamma_{th})\right)}{\left(m_{s_M}-1\right)\overline{\gamma_M}}\middle| \begin{matrix} 1 & 1-m_{s_M} \\ i+1 & 0 \end{matrix}\right] d\gamma_E \tag{13}$$

The solution of integral in (13) seems not to be obtainable in closed-form due to the complexity. Therefore, we focus on deriving the lower bound of SOP in this paper. $\mathrm{SOP}^{\mathrm{L}}$ can be expressed from [6, Eq. (15)] as follows

$$P_{out}(\gamma_{th}) \geq SOP^{L}(\gamma_{th}) \equiv \mathrm{P}\left[\gamma_M \leq (1+\gamma_{th})\gamma_E\right] \tag{14}$$

Now, (12) can be rewritten for $\mathrm{SOP}^{\mathrm{L}}$ as

$$SOP^{L} = \int_0^{\infty} f_{\gamma_E}(\gamma_E) F_{\gamma_M}\left((1+\gamma_{th})\gamma_E\right) d\gamma_E \tag{15}$$

On substitution of (5) and (7) into (15), the expression of $\mathrm{SOP}^{\mathrm{L}}$ is given as

$$SOP^{L} = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} A_{E_j} B_{M_i} \int_0^{\infty} G_{1,1}^{1,1}\left[\frac{(1+k_E)\gamma_E}{\left(m_{s_E}-1\right)\overline{\gamma_E}}\middle| \begin{matrix} -m_{s_E} \\ j \end{matrix}\right] G_{2,2}^{1,2}\left[\frac{(1+k_M)(1+\gamma_{th})\gamma_E}{\left(m_{s_M}-1\right)\overline{\gamma_M}}\middle| \begin{matrix} 1 & 1-m_{s_M} \\ i+1 & 0 \end{matrix}\right] d\gamma_E \tag{16}$$

The solution of resultant integral in (16) can be procured with the help of [26, Eq. (7.811.5)] as

$$SOP^{L} = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} A_{E_j} B_{M_i} \left(\frac{\left(m_{s_E}-1\right)\overline{\gamma_E}}{(1+k_E)}\right) G_{3,3}^{2,3}\left[\frac{(1+k_M)(1+\gamma_{th})\left(m_{s_E}-1\right)\overline{\gamma_E}}{(1+k_E)\left(m_{s_M}-1\right)\overline{\gamma_M}}\middle| \begin{matrix} 1 & 1-m_{s_M} & -j \\ i+1 & m_{s_E} & 0 \end{matrix}\right] \tag{17}$$

Although the expression in (17) is obtained in terms of infinite series, the final results converge quickly for finite values of $\{m_s, m_d, k\}$. This can be justified from the numerical results in Fig. 1. In order to reveal the behavior of $\mathrm{SOP}^{\mathrm{L}}$, the asymptotic expression of $\mathrm{SOP}^{\mathrm{L}}$ at high SNR $\overline{\gamma_M} \to \infty$ is derived by substituting (5) and (9) into (15) and using the [23, Eq. (07.34.21.0009.01)] as

$$SOP_{\infty}^{L} = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} A_{E_j} B_{M_i} \left\{\frac{\Gamma(-i-1)\Gamma\left(i+m_{s_M}+1\right)\Gamma(i+j+2)\Gamma\left(m_{s_E}-i-1\right)}{\Gamma(i+2)} \times\left(\frac{(1+k_E)}{\left(m_{s_E}-1\right)\overline{\gamma_E}}\right)^{-i-1}\left(\frac{(1+k_M)(1+\gamma_{th})}{\left(m_{s_M}-1\right)\overline{\gamma_M}}\right)^{i+1}\right\} \tag{18}$$

Additionally, the secrecy diversity order (SDO) of the proposed system can be evaluated by utilizing $SOP_{\infty}^{L} = \left(G_c^s \overline{\gamma_M}\right)^{G_d^s}$ [27, Eq. (21)] as $G_d^s = i+1$.

As discussed in Sect. 1, the double shadowed Rician distribution includes other well-known fading distributions. The values of the fading parameters i.e., $\{m_s, m_d, k\}$ for the special cases of double shadowed Rician distribution are provided in Table 2. Thus, the $\mathrm{SOP}^{\mathrm{L}}$ in (17) can be reduced to the special case of Rayleigh fading condition as

$$SOP_{Ray}^{L} = 1 - \frac{\overline{\gamma_M}}{\overline{\gamma_M} + (1+\gamma_{th})\overline{\gamma_E}} \tag{19}$$

with the help of [24, Eqs. (8.2.2.8) and (8.2.2.9)] and [23, Eqs. (07.34.25.0005.01) and (07.34.25.0007.01)] by setting $\{m_s \to \infty, m_d \to \infty, k \to 0\}$ in (17). It is noteworthy that the derived expression in (19) is similar to the $\mathrm{SOP}^{\mathrm{L}}$ in [28, Eq. (9)].

Table 2 Fading parameters for special cases of double shadowed Rician distribution

Fading parameters			Fading models
$m_s \to \infty$	m_d	k	Shadowed Rician
$m_s \to \infty$	$m_d \to 0$	k	Shadowed Rayleigh
$m_s \to \infty$	$m_d \to 0.5$	k	Nakagami-q
$m_s \to \infty$	$m_d \to \infty$	k	Rician
$m_s \to \infty$	$m_d \to \infty$	$k \to 0$	Rayleigh

3.2 SPSC Analysis

The SPSC is an indispensable paradigm on the PLS secrecy performance, which can be defined using (14) as $1 - P_{out}(0)$. The SPSC refers to the probability which can be calculated for the scenario when positive secrecy capacity, i.e.,$C_S > 0$ is achieved. The expression of SPSC can be evaluated by substituting $\gamma_{th} = 0$ into (17) as

$$SPSC = 1 - \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} A_{E_j} B_{M_i} \left(\frac{(m_{s_E}-1)\overline{\gamma_E}}{(1+k_E)}\right) G_{3,3}^{2,3}\left[\frac{(1+k_M)(m_{s_E}-1)\overline{\gamma_E}}{(1+k_E)(m_{s_M}-1)\overline{\gamma_M}}\middle| \begin{matrix} 1 & 1-m_{s_M} & -j \\ i+1 & m_{s_E} & 0 \end{matrix}\right] \tag{20}$$

3.3 ASC Analysis

According to [20], the ASC can be written from (9) as $\overline{C_S} = I_1 + I_2 - I_3$, where

$$I_1 = \int_0^{\infty} \log\left(1+\gamma_M\right) f_{\gamma_M}(\gamma_M) F_{\gamma_E}(\gamma_M) d\gamma_M \tag{21}$$

$$I_2 = \int_0^{\infty} \log\left(1+\gamma_E\right) f_{\gamma_E}(\gamma_E) F_{\gamma_M}(\gamma_E) d\gamma_E \tag{22}$$

$$I_3 = \int_0^{\infty} \log\left(1+\gamma_E\right) f_{\gamma_E}(\gamma_E) d\gamma_E \tag{23}$$

On substituting (5) and (7) into (21), we obtain

$$I_1 = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} A_{M_i} B_{E_j} \int_0^{\infty} \log\left(1+\gamma_M\right) G_{1,1}^{1,1}\left[\frac{(1+k_M)\gamma_M}{(m_{s_M}-1)\overline{\gamma_M}}\middle| \begin{matrix} -m_{s_M} \\ i \end{matrix}\right] G_{2,2}^{1,2}\left[\frac{(1+k_E)\gamma_M}{(m_{s_E}-1)\overline{\gamma_E}}\middle| \begin{matrix} 1 & 1-m_{s_E} \\ j+1 & 0 \end{matrix}\right] d\gamma_M \tag{24}$$

To obtain the solution of (24), we express $\log_2(\cdot)$ in Meijer-G representation using [24, Eq. (8.4.6.5)], then using the following integral from [23]

$$\int_0^\infty G_{p,q}^{m,n}\left[t\middle|\begin{matrix}a_1,...,a_p\\ b_1,...,b_q\end{matrix}\right] G_{p_1,q_1}^{m_1,n_1}\left[xt\middle|\begin{matrix}a_{11},...,a_{1p_1}\\ b_{11},...,b_{1q_1}\end{matrix}\right] G_{p_2,q_2}^{m_2,n_2}\left[yt\middle|\begin{matrix}a_{21},...,a_{2p_2}\\ b_{21},...,b_{2q_2}\end{matrix}\right] dt = G_{q,p:p_1,q_1:p_2,q_2}^{n,m:m_1,n_1:m_2,n_2}\left[\begin{matrix}-b_1,...,-b_q\\ -a_1,...,-a_p\end{matrix}\middle|\begin{matrix}a_{11},...,a_{1p_1}\\ b_{11},...,b_{1q_1}\end{matrix}\middle|\begin{matrix}a_{21},...,a_{2p_2}\\ b_{21},...,b_{2q_2}\end{matrix}\middle|\frac{x}{z},\frac{y}{z}\right] \tag{25}$$

we have integral I_1 in closed-form as

$$I_1 = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} A_{M_i} B_{E_j} G_{2,2:1,1:1,2}^{2,1:1,1:1,2}\left[\frac{(1+k_M)}{(m_{s_M}-1)\overline{\gamma_M}}, \frac{(1+k_E)}{(m_{s_E}-1)\overline{\gamma_E}}\middle|\begin{matrix}-1 & 0\\ -1 & -1\end{matrix}\middle|\begin{matrix}-m_{s_M}\\ i\end{matrix}\middle|\begin{matrix}1 & 1-m_{s_E}\\ j+1 & 0\end{matrix}\right] \tag{26}$$

Similarly, I_2 can be obtained by replacing m_{s_M},m_{d_M},k_M and $\overline{\gamma_M}$ in (26) with m_{s_E},m_{d_E},k_E and $\overline{\gamma_E}$ and vice-versa, as

$$I_2 = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} A_{E_j} B_{M_i} G_{2,2:1,1:1,2}^{2,1:1,1:1,2}\left[\frac{(1+k_E)}{(m_{s_E}-1)\overline{\gamma_E}}, \frac{(1+k_M)}{(m_{s_M}-1)\overline{\gamma_M}}\middle|\begin{matrix}-1 & 0\\ -1 & -1\end{matrix}\middle|\begin{matrix}-m_{s_E}\\ j\end{matrix}\middle|\begin{matrix}1 & 1-m_{s_M}\\ i+1 & 0\end{matrix}\right] \tag{27}$$

Furthermore, the integral I_3 can be rewritten by substituting (5) into (23) as

$$I_3 = \sum_{i=0}^{\infty} A_{E_i} \int_0^\infty \log\left(1+\gamma_E\right) G_{1,1}^{1,1}\left[\frac{(1+k_E)\gamma_E}{(m_{s_E}-1)\overline{\gamma_E}}\middle|\begin{matrix}-m_{s_E}\\ i\end{matrix}\right] d\gamma_E \tag{28}$$

which can be simplified by expressing $\log_2(\cdot)$ in Meijer-G representation from [24, Eq. (8.4.6.5)] and using following integral from [23]

$$\int_0^\infty G_{u,v}^{s,t}\left[t\middle|\begin{matrix}c_1,...,c_u\\ d_1,...,d_v\end{matrix}\right] G_{p,q}^{m,n}\left[zt\middle|\begin{matrix}a_1,...,a_p\\ b_1,...,b_q\end{matrix}\right] dt = G_{v+p,u+q}^{m+t,n+s}\left[\begin{matrix}a_1,...,a_n,-d_1,...,-d_v,a_{n+1},...,a_p\\ b_1,...,b_m,-c_1,...,-c_u,b_{m+1},...,b_q\end{matrix}\right] \tag{29}$$

we obtain I_3 in a closed-form as

$$I_3 = \sum_{i=0}^{\infty} A_{E_i} G_{3,3}^{3,2}\left[\frac{(1+k_E)}{(m_{s_E}-1)\overline{\gamma_E}}\middle|\begin{matrix}-m_{s_E} & -1 & 0\\ i & -1 & -1\end{matrix}\right] \tag{30}$$

Finally, by substituting I_1, I_2 and I_3 into the expression of $\overline{C_S}$, ASC can be evaluated straightforward.

4 Numerical Results

This section presents the analytical results to study the effects of double shadowing fading parameters and average SNRs on the PLS secrecy performance. The figures have been obtained by setting $\{m_{s_M} = m_{s_E} = m_s\}$, $\{m_{d_M} = m_{d_E} = m_d\}$ and $\{k_M = k_E = k\}$. First, we discuss the effect of predetermined secrecy rate on the performance of SOP^{L}. In Fig. 2, the SOP^{L} is demonstrated as a function of $\overline{\gamma_M}$ for different values of $R_S = \{1.17, 2.05, 3.45\}$ nat/s/Hz. One can observe that secrecy performance degrades as R_S increases. This observation shows that for a high target secrecy rate, it is challenging to increase the secrecy

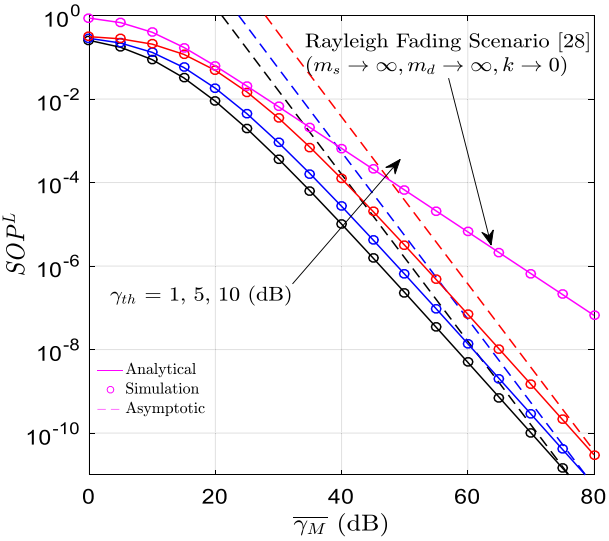


Fig. 2 SOP^{L} versus $\overline{\gamma_M}$ when $m_s = 1.7$, $m_d = 1.3k = 1.2$, and $\overline{\gamma_E} = 2dB$

capacity of the system even by increasing the average SNR of the main channel. It is also noted that the increasing $\overline{\gamma_M}$ provides sufficient improvement in the secrecy performance for a fixed value of R_S. This is because increasing $\overline{\gamma_M}$ improves the quality of the main channel and result in a higher secrecy capacity. In addition, the tightness of the derived results can be observed by the perfect match between asymptotic results with the analytical results at the high SNR regime. Moreover, the SOP^{L} is also compared with the result in [28] to show the consistency of the derived results.

Figure 3 illustrates the consequences of $\{m_s, m_d\}$ on the lower bound on SOP for different scenarios. It is pronounced from the analytical results shown in Fig. 3 that superior main channel $(\overline{\gamma_M} > \overline{\gamma_E})$ provides better secrecy with compared to superior eavesdropper's channel $(\overline{\gamma_M} < \overline{\gamma_E})$. The reason for this behavior is that a higher value of $\overline{\gamma_M}$ improves the

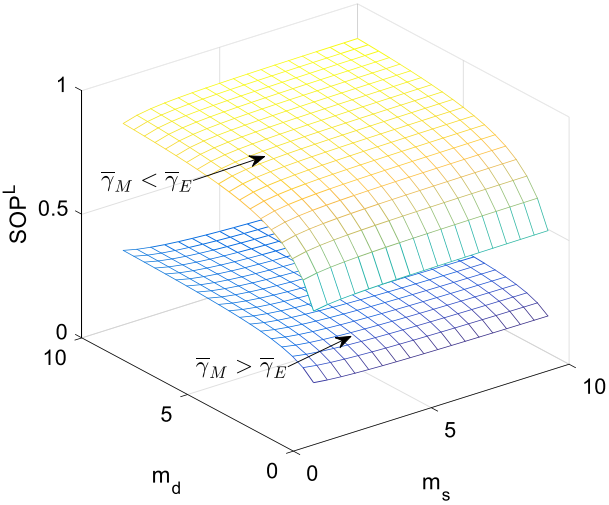


Fig. 3 SOP^{L} versus $\{m_s, m_d\}$ when $k = 3.2$ and $\gamma_{th} = 2dB$

Table 3 Lower bound on SOP

$\{m_s, m_d\} = \{2.5, 1.5\}$ $(\overline{\gamma_M} > \overline{\gamma_E})$	$\{m_s, m_d\} = \{2.5, 1.5\}$ $(\overline{\gamma_M} < \overline{\gamma_E})$
0.2023	0.5877
$\{m_s, m_d\} = \{1.5, 2.5\}$ $(\overline{\gamma_M} > \overline{\gamma_E})$	$\{m_s, m_d\} = \{1.5, 2.5\}$ $(\overline{\gamma_M} < \overline{\gamma_E})$
0.2542	0.6759

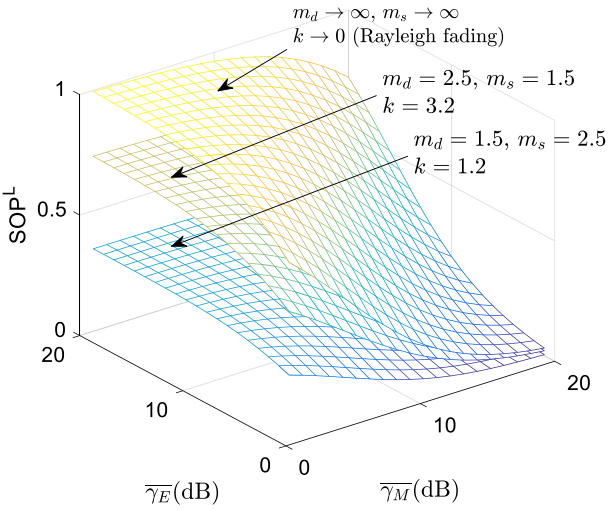


Fig. 4 SOP$^{\mathrm{L}}$ versus $\{\overline{\gamma_M}, \overline{\gamma_E}\}$ when $\gamma_{th} = 2dB$

quality of the main channel, which results in an enhanced capacity of the main channel, while the higher value of $\overline{\gamma_E}$ improve the quality of the wiretap channel and results in a higher capacity of eavesdropper's link. It can also be noticed that low values of multiplicative shadowing parameter m_s can enhance secrecy. This is because, in severe shadowing, the legitimate users can communicate secretly in comparison to the low fading regime. This observation is summarized in Table 3.

Figure 4 shows the lower bound on SOP against $\{\overline{\gamma_M}, \overline{\gamma_E}\}$ under different double shadowing Rician fading conditions. As anticipated, an increasing average SNR $\overline{\gamma_M}$ leads to deterioration in the security performance in context of the SOP$^{\mathrm{L}}$, whereas increasing average SNR $\overline{\gamma_E}$ is incremental to the security performance. It is also observed that the greatest SOP$^{\mathrm{L}}$ occurs for low values of multiplicative shadowing parameter m_s, when compared to the LOS shadowing parameter m_d. For example, the SOP$^{\mathrm{L}}$ observed when $\{m_s, m_d, k\} = \{2.5, 1.5, 3.2\}$ is 0.1569, while the SOP$^{\mathrm{L}}$ observed when $\{m_s, m_d, k\} = \{1.5, 2.5, 1.2\}$ is 0.0625. This result is presented in Table 4. To obtain further intuitions, Fig. 4 includes the SOP$^{\mathrm{L}}$ for Rayleigh fading channels as a special case of double shadowed Rician fading channels. It is obvious to note that the profile of SOP$^{\mathrm{L}}$ for Rayleigh fading channels is similar to SOP$^{\mathrm{L}}$ for double shadowed Rician fading channels.

Figure 5 demonstrates the behavior of SPSC for various scenarios versus shadowing parameters $\{m_s, m_d\}$. As expected, it can be noticed that superior main channel $(\overline{\gamma_M} > \overline{\gamma_E})$ provides an improvement in the SPSC, whereas deterioration in the SPSC can be observed for superior eavesdropper's channel $(\overline{\gamma_M} < \overline{\gamma_E})$. The reason for this behavior is similar, as

Table 4 Lower bound on SOP

$\{m_s, m_d, k\} = \{2.5, 1.5, 3.2\}$ $\{\overline{\gamma_M}, \overline{\gamma_E}\} = \{15dB, 5dB\}$	$\{m_s, m_d, k\} = \{2.5, 1.5, 3.2\}$ $\{\overline{\gamma_M}, \overline{\gamma_E}\} = \{5dB, 15dB\}$
0.1559	0.7036
$\{m_s, m_d, k\} = \{1.5, 2.5, 1.2\}$ $\{\overline{\gamma_M}, \overline{\gamma_E}\} = \{15dB, 5dB\}$	$\{m_s, m_d, k\} = \{1.5, 2.5, 1.2\}$ $\{\overline{\gamma_M}, \overline{\gamma_E}\} = \{5dB, 15dB\}$
0.0625	0.3368

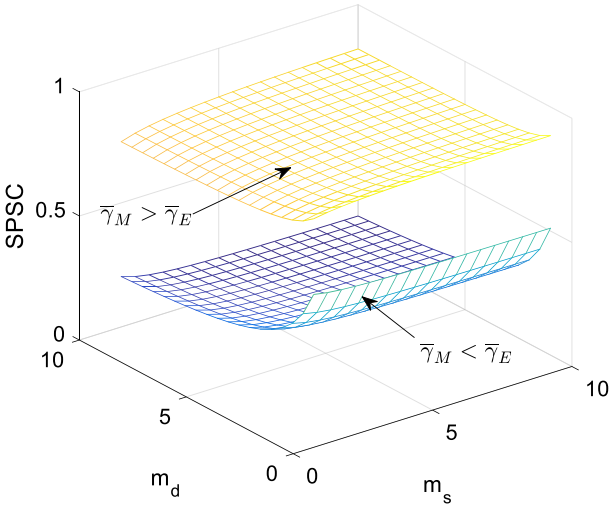
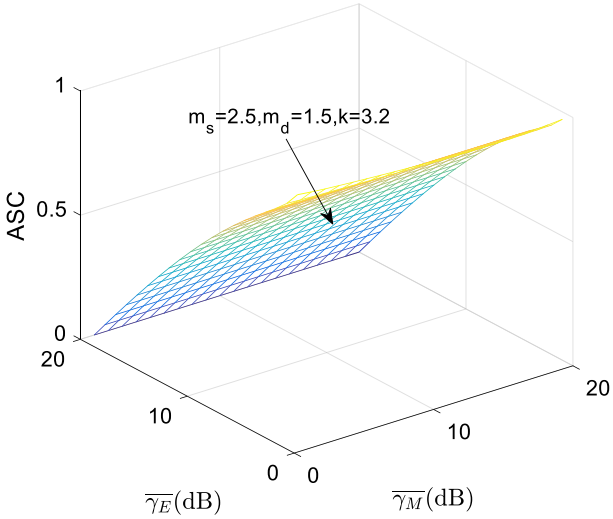


Fig. 5 SPSC versus $\{m_s, m_d\}$ when $k = 3.2$ and $\gamma_{th} = 0dB$

discussed in Fig. 3. The result also shows that decreasing multiplicative shadowing parameter m_s improves the SPSC. This is because a lower m_s represents severe shadowing conditions resulting from the obstacles moving in the vicinity of either transmitter or receiver. Under the severe shadowing conditions, it becomes difficult for the eavesdropper to overhear secure communication between the intended users. This observation is consistent with the results in [20]. Similarly, one can also find the greatest SPSC for severe shadowing of LOS components (low values of m_d).

Figure 6 depicts the ASC versus for various values of $\{\overline{\gamma_M}, \overline{\gamma_E}\}$. It is demonstrated from the result that the behavioral performance of ASC improves as the average SNR $\overline{\gamma_M}$ increases, whereas the behavioral performance of ASC deteriorates as the average SNR $\overline{\gamma_E}$ increases. This is because the secrecy capacity depends on the channel capacities of the main channel and the eavesdropper's link. The channel capacities of the main channel and eavesdropper's link is higher and lower, respectively, for the higher $\overline{\gamma_M}$ and lower $\overline{\gamma_E}$, respectively. This means that the difference between the two capacities (i.e., main channel and eavesdropper's link) is enhanced and hence the secrecy capacity is improved. This observation can be justified from (10).

Fig. 6 ASC versus $\{\overline{\gamma_M}, \overline{\gamma_E}\}$



5 Conclusion

In this study, we have analyzed the secure transmission for PLS of a single-hop mobile communication wireless network over double shadowed Rician fading channels in the presence of an eavesdropper for the first time. In particular, we have derived novel solutions for the expressions of different PLS metrics, including SOP^{L}, SPSC, and ASC. It was shown that double shadowing has a significant impact on secrecy performance. Specifically, the results demonstrated that a superior main channel improves the PLS secrecy performance. Furthermore, it was found that severe shadowing conditions enhance PLS secrecy performance.

Acknowledgements This publication was supported, in part by the "Visvesvaraya Ph.D. Scheme," Ministry of Electronics and Information Technology, Government of India, under Grant MIT-1100-CSE and in part by Qatar University and IS-Wireless—International Research Collaboration Co-Fund Grant No. IRCC-2021-003. The findings achieved herein are solely the responsibility of the authors.

Funding This publication was supported, in part by the "Visvesvaraya Ph.D. Scheme," Ministry of Electronics and Information Technology, Government of India, under Grant MIT-1100-CSE and in part by Qatar University and IS-Wireless—International Research Collaboration Co-Fund Grant no. IRCC-2021–003. The findings achieved herein are solely the responsibility of the authors.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

References

1. Yang, N., Wang, L., Geraci, G., Elkashlan, M., Yuan, J., & Renzo, M. D. (2015). Safeguarding 5G wireless communication networks using physical layer security. *IEEE Communications Magazine, 53*(4), 20–27.
2. Kapetanovic, D., Zheng, G., & Rusek, F. (2015). Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Communications Magazine, 53*(6), 21–27.

3. Zou, Y., Zhu, J., Yang, L., Liang, Y. C., & Yao, Y. D. (2015). Securing physical-layer communications for cognitive radio networks. *IEEE Communications Magazine, 53*(9), 48–54.
4. Chen, X., Zhong, C., Yuen, C., & Chen, H. (2015). Multi-antenna relay aided wireless physical layer security. *IEEE Communications Magazine, 53*(12), 40–46.
5. Ai, Y., Cheffena, M., Ohtsuki, T., & Zhuang, H. (2019). Secrecy performance analysis of wireless sensor networks. *IEEE Sensors Letters, 3*(5), 1–4.
6. Bhargav, N., Cotton, S. L., & Simmons, D. E. (2016). Secrecy capacity analysis over κ-μ fading channels: Theory and applications. *IEEE Transactions on Communications, 64*(7), 3011–3024.
7. Romero-Jerez, J. M., & Lopez-Martinez, F. J. (2107). A new framework for the performance analysis of wireless communications under Hoyt (Nakagami-*q*) fading. *IEEE Transactions on Information Theory*, 63(3), 1693–1702.
8. Jameel, F., Wyne, S., & Krikidis, I. (2017). Secrecy outage for wireless sensor networks. *IEEE Communications Letters, 21*(7), 1565–1568.
9. Lei, H., Ansari, I. S., Pan, G., Alomair, B., & Alouini, M. S. (2017). Secrecy capacity analysis over α−μ fading channels. *IEEE Communications Letters, 21*(6), 1445–1448.
10. Gao, Y., Ge, H., & Gao, H. (2016). Physical layer security with maximal ratio combining over heterogeneous κ-μ and η-μ fading channels. *Wireless Personal Communications, 86*, 1387–1400.
11. Tuan, V. P., & Kong, H. Y. (2019). Secrecy outage analysis of an untrusted relaying energy harvesting system with multiple eavesdroppers. *Wireless Personal Communications, 107*, 797–812.
12. Ibdah, Y., & Ding, Y. (2015). Mobile-to-mobile channel measurements at 1.85 GHz in suburban environments. *IEEE Transactions on Communications, 63*(2), 466–475.
13. Hamid, S., Al-Dweik, A.J., Mirahmadi, M., Mubarak, K., & Shami, A. (2105). Inside-out propagation: Developing a unified model for the interference in 5G networks. *IEEE Vehicular Technology Magazine*, 10(2), 47–54.
14. Yacoub, M. D. (2016). The *α-η-κ-μ* fading model. *IEEE Transactions on Antennas and Propagation, 64*(8), 3597–3610.
15. Lei, H., Zhang, H., Ansari, I. S., Gao, C., Guo, Y., Pan, G., & Qaraqe, K. A. (2016). Performance analysis of physical layer security over Generalized-K fading channels using a mixture Gamma distribution. *IEEE Communications Letters, 20*(2), 408–411.
16. Kong, L., & Kaddoum, G. (2019). Secrecy characteristics with assistance of mixture gamma distribution. *IEEE Wireless Communications Letters, 8*(4), 1086–1089.
17. Alexandropoulos, G. C., & Peppas, K. P. (2018). Secrecy outage analysis over correlated composite Nakagami- m/Gamma fading channels. *IEEE Wireless Communications Letters, 22*(1), 77–80.
18. Kong, L., & Kaddoum, G. (2018). On physical layer security over the fisher-snedecor F wiretap fading channels. *IEEE Access, 6*, 39466–39472.
19. Ai, Y., Kong, L., & Cheffena, M. (2019). Secrecy outage analysis of double shadowed Rician channels. *Electronics Letters, 55*(13), 765–767.
20. Singh, R., & Rawat, M. (2019). Performance analysis of physical layer security over Weibull/lognormal composite fading channel with MRC reception. *International Journal of Electronics and Communications, 110*, 1–13.
21. Simmons, N., Silva, C. R. N. D., Cotton, S. L., Sofotasios, P. C., & Yacoub, M. D. (2019). Double shadowing the Rician fading model. *IEEE Wireless Communications Letters, 8*(2), 344–347.
22. Singh, R., Rawat, M., & Pradhan, P. M. (2020). Effective capacity of wireless networks over double shadowed Rician fading channels. *Wireless Networks, 26*(2), 1347–1355.
23. Wolfram Research, Inc. [Online]. Available: http://functions.wolfram.com/id. Accessed: Nov., 2019.
24. Prudnikov, A. P., Brychkov, Y. A., & Marichev, O. I. (1990). *Integrals, and series: More special functions* (Vol. 3). Gordon and Breach Science Publishers.
25. Sharma, B. L., & Abiodun, R. F. A. (1974). Generating function for generalized function of two variables. *American Mathematical Society, 46*(1), 69–72.
26. Gradshteyn, I. S., & Ryzhik, M. (2007). *Table of Integrals, Series, and Product*. Academic.
27. Arezumand, H., Zamiri-Jafarian, H., & Soleimani-Nasab, E. (2017). Outage and diversity analysis of underlay cognitive mixed RF-FSO cooperative systems. *Journal of Optical Communications and Networking, 9*(10), 909–920.
28. Bloch, M., Barros, J., Rodrigues, M. R. D., & McLaughlin, S. W. (2008). Wireless information-theoretic security. *IEEE Transactions on Information Theory, 54*(6), 2515–2534.

Rupender Singh received the B.Tech. degree in electronics and communication engineering from MJP Rohilkhand University, Bareilly, India in 2008 and the M.Tech. degree in microwave and optical communication engineering from Delhi Technological University, Delhi, India in 2015 and Ph.D. degree in Wireless Communication from the Indian Institute of Technology, Roorkee, India in 2021. From 2009 to 2014, he worked as an Assistant Professor with World Institute of Technology, Gurgaon, India. He has published one book and presented 25 papers in national and international journals/conferences. His current research interest is focused on wireless communication, physical layer security, and optical wireless communication.

Meenakshi Rawat received the Ph.D. degree in electrical and computer engineering from the University of Calgary, Calgary, AB, Canada, in 2012. From 2012 to 2013, she was a Post-Doctoral Research Fellow with the University of Calgary. From 2013 to 2014, she was a Post-Doctoral Project Researcher and a Scientist with The Ohio State University, Columbus, OH, USA. She is currently an Associate Professor with IIT Roorkee, India, and the Founding Director at Linearized Amplifier Services Private Ltd. Dr. Rawat was a part of Calgary Group that won the Overall Championship and the Best Design Prize of the 3rd Annual Smart Radio Challenge, Wireless Innovation Forum. She was a three-time recipient of the Research Production Award of the University of Calgary and the Best Paper Award of the 82nd ARFTG Conference, Columbus, in 2013, and 83rd ARFTG Conference, Tampa, FL, USA, in 2014. She was the Workshop Co-Chair for ARFTG-82, the Session Chair for iMARC 2014, Bengaluru, India, and the Chair of the Session "Women in Microwave" in iMARC 2019. She is a Frequent Workshop Presenter in IMS Conference.

Elias Yaacoub received the B.E. degree in electrical engineering from Lebanese University, in 2002, and the M.E. degree in computer and communications engineering and Ph.D. degree in electrical and computer engineering from the American University of Beirut (AUB), in 2005 and 2010, respectively. He worked as a Research Assistant with the American University of Beirut, from 2004 to 2005, and Munich University of Technology, in Spring 2005. From 2005 to 2007, he worked as a Telecommunications Engineer with Dar Al-Handasah, Shair, and Partners. From November 2010 to December 2014, he worked as a Research Scientist/Research and Development Expert with Qatar Mobility Innovations Center (QMIC), where he led the Broadband Wireless Access Technology Team. Afterward, he joined the Strategic Decisions Group (SDG), where he worked as a Consultant, till February 2016. Then, he joined Arab Open University (AOU) as an Associate Professor and a Coordinator of the M.Sc. Program in information security and forensics. From February 2018 to August 2019, he worked as an Independent Researcher/a Consultant and he was also affiliated with AUB as a part-time Faculty Member. He has been an Associate Professor with the Computer Science and Engineering Department, Qatar University, since August 2019. His research interests include wireless communications, resource allocation in wireless networks, intercell interference mitigation techniques, antenna theory, sensor networks, and physical layer security.