CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Secrecy performance of a keyhole-based multi-user system with multiple eavesdroppers
Authors	Alam, Parwez;Dubey, Ankit;Moualeu, Jules M.;Ngatched, Telex M. N.;Kundu, Chinmoy
Publication date	2025-09-30
Original Citation	Alam, P., Dubey, A., Moualeu, J. M., Ngatched, T. M. N. and Kundu, C. (2025) 'Secrecy performance of a keyhole-based multi-user system with multiple eavesdroppers', 2025 IEEE 101st Vehicular Technology Conference (VTC2025-Spring), Oslo, Norway, 17-20 June 2025, pp. 1-5. https://doi.org/10.1109/VTC2025-Spring65109.2025.11174874
Type of publication	Conference item;proceedings-article
Link to publisher's version	10.1109/vtc2025-spring65109.2025.11174874
Rights	© 2024, IEEE. For the purpose of Open Access, the author has applied a CC BY public copyright license to any Author Accepted Manuscript version arising from this submission.
Download date	2026-11-05 20:41:53
Item downloaded from	https://hdl.handle.net/10468/18282

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Secrecy Performance of a Keyhole-based Multi-user System with Multiple Eavesdroppers

Parwez Alam*, Ankit Dubey†, Jules M. Moualeu‡, Telex M. N. Ngatched§, and Chinmoy Kundu¶,
*†Department of EE, Indian Institute of Technology Jammu, Jammu & Kashmir, India
‡School of Electrical and Information Engineering, University of the Witwatersrand, Johannesburg, South Africa
§Department of Electrical and Computer Engineering, McMaster University, Hamilton ON, Canada
¶Wireless Communications Laboratory, Tyndall National Institute, University College Cork, Cork, Ireland
{*2022ree0013,†ankit.dubey}@iitjammu.ac.in, ‡jules.moualeu@wits.ac.za, §ngatchet@mcmaster.ca, ¶chinmoy.kundu@tyndall.ie

***Abstract*—This paper investigates the secrecy performance of a keyhole-aided multi-user communication network in the presence of multiple eavesdroppers. The communication happens through the same keyhole for legitimate users and eavesdroppers. In this context, the secrecy performance is evaluated for a user scheduling technique by obtaining the exact closed-form expression of secrecy outage probability (SOP). Further, a simplified asymptotic SOP expression is derived assuming high signal-to-noise ratio (SNR) scenario for a better understanding of the impact of system parameters. The effect of the keyhole parameters, number of users, number of eavesdroppers, and threshold secrecy rate on the SOP performance are also investigated for the considered system model. In the high-SNR regime, the asymptotic SOP saturates to a constant value and does not depend on the keyhole parameter and the channel parameter of the source-to-keyhole channel.**

***Index Terms*—Asymptotic analysis, keyhole, physical layer security, secrecy outage probability.**

I. Introduction

In a highly scattered environment, single-user communication with multiple transmit and receive antennas can achieve high spectral efficiency [1]. Moreover, such an environment makes the signal from each transmit antenna appear highly uncorrelated at each receive antenna. If the signals arriving at the receive antennas are correlated, then the spectral efficiency is reduced. However, a low signal correlation at each of the receive antennas is not a guarantee to achieve high capacity. A degenerative propagation scenario called "*keyhole*" may reduce capacity even though the system has uncorrelated transmit and receive signals [2]–[4].

Realistically, a keyhole effect may arise during the propagation of electromagnetic radiation through a hallway, tunnel, or corridor where the signal from the transmitter can propagate to the receiver only through the keyhole. A portion of the incident electric field is transmitted through the keyhole. The ratio of the transmitted field through the keyhole to the incident field on the keyhole is called the scattering cross-section of the keyhole [1]. The dimensions of the keyhole should be much smaller than the corresponding wavelength [5]. Although the signals at the antennas are not correlated, the keyhole effect reduces the multiple-input multiple-output (MIMO) channel capacity comparable to the single-input single-output (SISO) channel capacity [6], [7]. As the keyhole channel reduces the channel rank to one regardless of the number of antennas at the transmitter and receiver, the spatial diversity is more beneficial than the multiplexing gain of the MIMO channel [5]. Motivated by this, the authors in [8] studied a transmit and receive antenna selection in the presence of keyhole condition wherein it was shown that the antenna selection did not decrease the diversity of the keyhole channel.

Due to the broadcast nature of wireless media, a wireless transmission is susceptible to eavesdropping. Physical layer security (PLS) is emerging as an efficient solution to provide security in wireless networks due to its low-complexity techniques which use physical characteristics of the wireless channel to provide security [9]. In [10] and [11], a keyhole-aided MIMO-vehicle-to-vehicle (MIMO-V2V) in the presence of an eavesdropper is investigated, assuming that both the main and eavesdropper channels are modeled as two mutually independent MIMO keyhole channels. Specifically, the closed-form expressions of the non-zero secrecy capacity, secrecy outage probability (SOP), and average secrecy capacity (ASC) are derived. In [12], a secure communication scenario through multi-keyhole MIMO channels is considered where the effect of the number of keyholes on the ergodic secrecy capacity is investigated.

A keyhole channel resembles a cascade of two fading channels where local scatterers in the vicinity produce more than one multiplicative small-scale fading processes, i.e., cascaded fading [5], [13]. In [14], the PLS of a system consisting of a transmitter and receiver in a cascaded κ-μ channel is investigated in the presence of multiple colluding and non-colluding eavesdroppers. In [15], the securecy performance of a cognitive radio networks (CRNs) in a cascaded Rayleigh fading channel is investigated. A user scheduling approach is considered to secure the keyhole-based power line communication (PLC) in the presence of an eavesdropper in [16].

MIMO transceivers employ multiple radio frequency (RF) chains and low-noise amplifiers (LNA), which is expensive. Furthermore, MIMO systems are also computationally expensive due to high-dimensional signaling and complex decoding algorithms [8]. in the presence of a keyhole condition, spatial diversity is more beneficial than the multiplexing gain, which negates the application of MIMO processing. On the

other hand, a single-input single-output (SISO) system, which leverages a single antenna for transmission and reception of the RF signal, offers a cost-effective and power-efficient solution, particularly in scenarios where hardware complexity and power consumption pose significant challenges, such as in Internet of Things (IoT) networks deployed in smart cities, smart home, and smart industries [17]. Thus, the security of future IoT-based multi-user systems in keyhole channels would require inexpensive technology. However, the PLS techniques for multiple distributed low-complexity users in keyhole channels are not adequately studied. Moreover, most studies on the security of keyhole channel employ MIMO transceivers which is expensive [10]–[12]. Assuming cascaded fading channels, no work in the literature has considered the detrimental effect of multiple eavesdroppers (see [14]–[16] and the references therein). Moreover, the works in [14] and [15] do not consider user scheduling techniques for security enhancement. Though the work in [16] adopts a user scheduling technique in the presence of a single eavesdropper, a PLC channel is assumed, which is quite different from the wireless channel.

Motivated by the above discussion, the present work considers a system where a source is communicating with multiple users via a keyhole channel in the presence of multiple eavesdroppers. The communication occurs through the same keyhole for all the users and eavesdroppers. In addition, a user scheduling technique is proposed for security enhancement, which inherently has less complexity and can be deployed in future low-cost low-complexity networks. Our key contributions are as follows.

- We derive the closed-form expression for the SOP of the keyhole channel in the presence of multiple eavesdroppers where a user is selected for scheduling among multiple users.
- We derive a simplified asymptotic SOP for the high SNR approximation to gain deeper insights.
- We evaluate the impact of scattering cross-section of keyhole, number of users and eavesdroppers, and the secrecy rate threshold on the system secrecy performance.

The rest of the paper is organized as follows. Section II introduces the system model of the proposed keyhole-based multi-user multi-eavesdropper system. Section III presents the theoretical framework of the SOP for the underlying system, while Section IV highlights the high-SNR asymptotic analysis of the SOP. In Section V, numerical results are presented. Finally, concluding remarks are provided in Section VI.

Notation: $\mathbb{P}[\cdot]$ represents the probability of the occurrence of an event, $\mathbb{E}[\cdot]$ is the expectation operator, $K_1(\cdot)$ denotes the modified Bessel function of the second kind of order 1. The probability density function (PDF) and the cumulative distribution function (CDF) of a random variable X are denoted by $f_X(\cdot)$ and $F_X(\cdot)$, respectively.

II. SYSTEM MODEL

We consider a multi-user communication system with multiple eavesdroppers where a source S is communicating with M legitimate users $\mathrm{D}^{(m)}$ for $m \in \mathcal{M} = \{1, 2, \ldots, M\}$ in the presence of N passive eavesdroppers $\mathrm{E}^{(n)}$ for $n \in \mathcal{N} = \{1, 2, \ldots, N\}$ as shown in Fig. 1. The communication takes place through a keyhole with scattering cross-section δ, separating the regions containing the users and the source. The eavesdroppers reside in the same region containing the users. It is assumed that the direct links from S to $\mathrm{D}^{(m)}$ or $\mathrm{E}^{(n)}$ for any $m \in \mathcal{M}$ and $n \in \mathcal{N}$, respectively, does not exist. The fading channels between the source-to-keyhole, keyhole-to-m-th destination, and keyhole-to-n-th eavesdropper are denoted by g, $h_d^{(m)}$, and $h_e^{(n)}$, respectively. We consider g, $h_d^{(m)}$ for all $m \in \mathcal{M}$, and $h_e^{(n)}$ for all $n \in \mathcal{N}$ to be mutually independent, complex Gaussian random variables (RV). We also assume that $h_d^{(m)}$ for all $m \in \mathcal{M}$ and $h_e^{(n)}$ for all $n \in \mathcal{N}$ are identically distributed. However, g, $h_d^{(m)}$ any m, and $h_e^{(n)}$ for any n are not identically distributed. The magnitude of the links follows the Rayleigh distribution. Hence, the channel powers $|g|^2$, $|h_d^{(m)}|^2$ for any $m \in \mathcal{M}$, and $|h_e^{(n)}|^2$ for any $n \in \mathcal{N}$, follow an exponential distribution with parameters ζ_g, ζ_{h_d} and ζ_{h_e}, respectively. The CDF and PDF of an exponentially distributed RV Z with parameter ζ_Z can be expressed respectively as

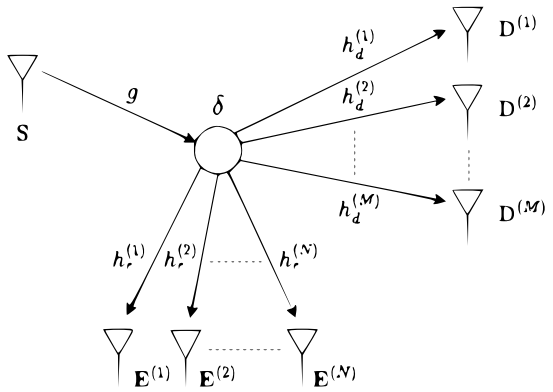


Fig. 1: A keyhole-based system model with a source, multiple users, and multiple eavesdroppers.

$$F_Z(z) = 1 - \exp\left(-\frac{z}{\zeta_Z}\right), \tag{1}$$

$$f_Z(z) = \frac{1}{\zeta_Z} \exp\left(-\frac{z}{\zeta_Z}\right). \tag{2}$$

The signal received at $\mathrm{D}^{(m)}$ through the keyhole is given by

$$y_d^{(m)} = g\delta h_d^{(m)} x + n_d^{(m)}, \tag{3}$$

where x is the transmitted signal with average transmitted power $\mathbb{E}\left(|x|^2\right) = P$ and $n_d^{(m)} \sim \mathcal{CN}\left(0, \sigma_d^2\right)$ for each m, is the additive white Gaussian noise (AWGN) at $\mathrm{D}^{(m)}$ with mean zero and variance σ_d^2. Similarly, the received signal at $\mathrm{E}^{(n)}$ can be written as

$$y_e^{(n)} = g\delta h_e^{(n)} x + n_e^{(n)}, \tag{4}$$

where $n_e^{(n)} \sim \mathcal{CN}\left(0, \sigma_e^2\right)$ for each n, is the AWGN at $\mathrm{E}^{(n)}$ with mean zero and variance σ_e^2.

To maximize the signal-to-noise ratio (SNR) at the users,

we select the best user m^* among M users for scheduling, which has the maximum source-to-user channel power gain. In this case, the instantaneous SNR at the best user $\mathrm{D}^{(m^*)}$ can be expressed as

$$\gamma_d = \bar{\gamma}_d |g|^2 \delta^2 \max_{m \in \mathcal{M}} \{|h_d^{(m)}|^2\}, \tag{5}$$

where $\bar{\gamma}_d = \frac{P}{\sigma_d^2}$. To measure the worst case secrecy, we measure the secrecy against the eavesdropper n^* which has the best source-to-eavesdropper channel power gain. In this case, the instantaneous SNR at $\mathrm{E}^{(n^*)}$ can be expressed as

$$\gamma_e = \bar{\gamma}_e |g|^2 \delta^2 \max_{n \in \mathcal{N}} \{(|h_e^{(n)}|^2)\}, \tag{6}$$

where $\bar{\gamma}_e = \frac{P}{\sigma_e^2}$.

Using the order statistics, the CDF of $\bar{\gamma}_d \max_{\forall m}\{|h_d^{(m)}|^2\}$ can be expressed as

$$\begin{aligned} F_X(x) &= \mathbb{P}\left[\max_{\forall m}\{|h_d^{(m)}|^2\} \leq \frac{x}{\bar{\gamma}_d}\right] = \left[1 - \exp\left(-\frac{x}{\zeta_{h_d}\bar{\gamma}_d}\right)\right]^M \\ &= 1 + \sum_{m=1}^{M} (-1)^m \binom{M}{m} \exp\left(-\frac{mx}{\zeta_{h_d}\bar{\gamma}_d}\right), \end{aligned} \tag{7}$$

where $X = \bar{\gamma}_d \max_{\forall m}\{|h_d^{(m)}|^2\}$. By differentiating (7), the corresponding PDF is obtained as

$$f_X(x) = \sum_{m=1}^{M} (-1)^{m+1} \binom{M}{m} \frac{m}{\zeta_{h_d}\bar{\gamma}_d} \exp\left(-\frac{mx}{\zeta_{h_d}\bar{\gamma}_d}\right). \tag{8}$$

Similarly, the CDF of $\bar{\gamma}_e \max_{\forall n}\{|h_e^{(n)}|^2\}$ can be expressed as

$$F_Y(y) = 1 + \sum_{n=1}^{N} (-1)^n \binom{N}{n} \exp\left(-\frac{ny}{\zeta_{h_e}\bar{\gamma}_e}\right), \tag{9}$$

where $Y = \bar{\gamma}_e \max_{\forall n}\{|h_e^{(n)}|^2\}$. The corresponding PDF is obtained as

$$f_Y(y) = \sum_{n=1}^{N} (-1)^{n+1} \binom{N}{n} \frac{n}{\zeta_{h_e}\bar{\gamma}_e} \exp\left(-\frac{ny}{\zeta_{h_e}\bar{\gamma}_e}\right). \tag{10}$$

The normalized capacity per Hertz of bandwidth of the user channel and the eavesdropper channel are given by $C_{\mathrm{B}} = \log_2(1+\gamma_d)$ and $C_{\mathrm{E}} = \log_2(1+\gamma_e)$, respectively. The achievable secrecy rate (C_{S}) is then defined as [18]

$$C_{\mathrm{S}} = [C_{\mathrm{B}} - C_{\mathrm{E}}]^+ = \max\left[\log_2\left(\frac{1+\gamma_d}{1+\gamma_e}\right), 0\right], \tag{11}$$

where $[x]^+ = \max\{x, 0\}$.

III. Secrecy Outage Probability (SOP)

A secrecy outage happens when the instantaneous secrecy rate is less than the desired threshold secrecy rate R_{th} for the system. The SOP can then be expressed mathematically as [19]

$$\begin{aligned} \mathcal{P}_{\text{out}} &= \mathbb{P}\left[\log_2\left(\frac{1+\gamma_d}{1+\gamma_e}\right) < R_{\mathrm{th}}\right], \\ &= \mathbb{P}\left[\max_{\forall m}\{|h_d^{(m)}|^2\}\bar{\gamma}_d - \rho \max_{\forall n}\{|h_e^{(n)}|^2\}\bar{\gamma}_e < \frac{(\rho-1)}{\delta^2|g|^2}\right], \\ &= \mathbb{P}\left[\max_{\forall m}\{|h_d^{(m)}|^2\}\bar{\gamma}_d < \frac{(\rho-1)}{\delta^2|g|^2} + \rho \max_{\forall n}\{|h_e^{(n)}|^2\}\bar{\gamma}_e\right], \end{aligned} \tag{12}$$

where $\rho = 2^{R_{\mathrm{th}}}$. To obtain the solution of the above expression, we first rewrite (12) as

$$\mathcal{P}_{\text{out}} = \mathbb{P}\left[X < \frac{(\rho-1)}{\delta^2 Z} + \rho Y\right], \tag{13}$$

where Z represents the RV $|g|^2$, and RVs X and Y are already defined in (7) and (9), respectively. The expression of (13) in the integral form can be written as

$$\mathcal{P}_{\text{out}} = \int_{z=0}^{\infty}\int_{y=0}^{\infty}\left[F_X\left(\frac{(\rho-1)}{\delta^2 z} + \rho y\right)\right] f_Y(y) f_Z(z) dy dz. \tag{14}$$

By substituting the analytical expression of $F_X(x)$, $f_X(x)$, and $f_Y(y)$ already derived in (7), (8), and (10), respectively, the SOP is written as

$$\begin{aligned} \mathcal{P}_{\text{out}} = \int_{z=0}^{\infty} \Bigg[1 + \sum_{m=1}^{M}\sum_{n=1}^{N} \binom{M}{m}\binom{N}{n} \frac{n(-1)^{m+n+1}}{\zeta_{h_e}\bar{\gamma}_e} \\ \times \int_{y=0}^{\infty} \exp\left(-\frac{m\left(\frac{(\rho-1)}{\delta^2 Z} + \rho Y\right)}{\zeta_{h_d}\bar{\gamma}_d} - \frac{ny}{\zeta_{h_e}\bar{\gamma}_e}\right) dy\Bigg] f_Z(z) dz. \end{aligned} \tag{15}$$

After evaluating the inner integral and substituting the PDF $f_Z(z)$ from (2) in (15), we get

$$\begin{aligned} \mathcal{P}_{\text{out}} = 1 - \sum_{m=1}^{M}\sum_{n=1}^{N} \binom{M}{m}\binom{N}{n} \frac{(-1)^{m+n} n \zeta_{h_d}\bar{\gamma}_d}{m\rho\zeta_{h_e}\bar{\gamma}_e + n\zeta_{h_d}\bar{\gamma}_d} \\ \times \underbrace{\int_{z=0}^{\infty} \frac{1}{\zeta_g} \exp\left(-\frac{m(\rho-1)}{\delta^2 z \zeta_{h_d}\bar{\gamma}_d}\right) \exp\left(-\frac{z}{\zeta_g}\right) dz}_{I}. \end{aligned} \tag{16}$$

After some mathematical manipulations and with the aid of [20, eq. (3.324.1)], which enables us to use the modified Bessel function for the solution of I, we get the closed-form solution for the SOP in (16) as

$$\begin{aligned} \mathcal{P}_{\text{out}} = 1 - \sum_{m=1}^{M}\sum_{n=1}^{N} \binom{M}{m}\binom{N}{n} \frac{(-1)^{m+n} n \zeta_{h_d}\bar{\gamma}_d}{m\rho\zeta_{h_e}\bar{\gamma}_e + n\zeta_{h_d}\bar{\gamma}_d} \\ \times \sqrt{\frac{4m(\rho-1)}{\delta^2\zeta_g\zeta_{h_d}\bar{\gamma}_d}} K_1\left(\sqrt{\frac{4m(\rho-1)}{\delta^2\zeta_g\zeta_{h_d}\bar{\gamma}_d}}\right). \end{aligned} \tag{17}$$

IV. Asymptotic Analysis

The closed-form expression of the SOP derived in (17) does not provide useful insights into the system design. To address this issue, we derive a simple and explicit expression that approximates the SOP in the high-SNR regime. To this end, we assume that the transmit power P increases asymptotically, i.e. $P \to \infty$, leading to $\bar{\gamma}_d = \frac{P}{\sigma_d^2} \to \infty$. Herewith we can use

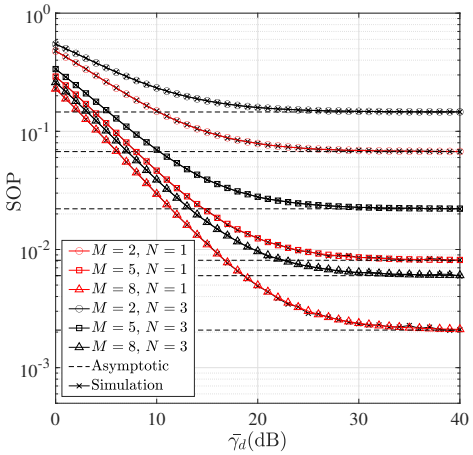


Fig. 2: The SOP versus $\bar{\gamma}_d$ for different M and N.

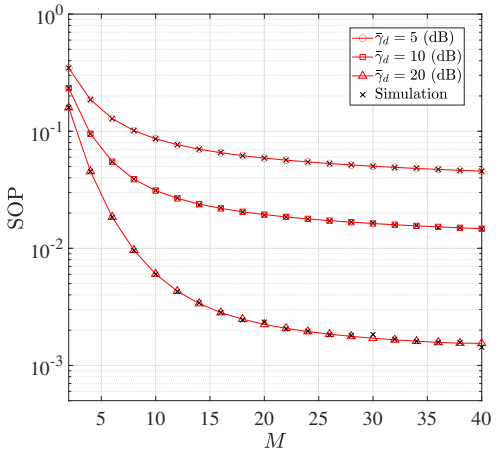


Fig. 3: The SOP versus M for different values of $\bar{\gamma}_d \in \{5, 10, 20\}$.

the following approximation in (17) [21, eq. (9.6.9)]

$$z \lim_{z \to 0} K_1(z) = 1, \tag{18}$$

which yields

$$\lim_{\bar{\gamma}_d \to \infty} \sqrt{\frac{4m\left(\rho - 1\right)}{\delta^2 \zeta_g \zeta_{h_d} \bar{\gamma}_d}} K_1\left(\sqrt{\frac{4m\left(\rho - 1\right)}{\delta^2 \zeta_g \zeta_{h_d} \bar{\gamma}_d}}\right) = 1. \tag{19}$$

After substituting (19) in (17), the asymptotic SOP can be expressed as

$$\mathcal{P}_{\text{out}}^{\infty} = 1 - \sum_{m=1}^{M} \sum_{n=1}^{N} \binom{M}{m} \binom{N}{m} \frac{(-1)^{m+n} n \zeta_{h_d} \sigma_e^2}{m \rho \zeta_{h_e} \sigma_d^2 + n \zeta_{h_d} \sigma_e^2}. \tag{20}$$

From (20), it can be inferred that the asymptotic SOP saturates in the high-SNR depending on the number of users, the number of eavesdroppers, the channel parameters of the keyhole-to-users and the keyhole-to-eavesdroppers, the noise power at the users and the eavesdroppers, and the desired threshold secrecy rate. Furthermore, the asymptotic SOP does not depend on the scattering cross-section and the channel parameter of the source-to-keyhole channel.

V. Numerical Results

In this section, we evaluate the SOP and asymptotic SOP performance of the keyhole-aided multi-user communication system in the presence of multiple eavesdroppers. Unless otherwise specified, the system parameters are taken as $\zeta_g = 3$ dB, $\zeta_{h_d} = 6$ dB, $\zeta_{h_e} = -3$ dB, $R_{\text{th}} = 1$ bits per channel use (bpcu), and $\delta = 0.5$.

In Fig. 2, the SOP is plotted against $\bar{\gamma}_d$ for the different combinations of $M \in \{2, 5, 8\}$ and $N \in \{1, 3\}$. From the plots, it is observed that the theoretical SOP obtained in (17) perfectly matches with the corresponding Monte Carlo simulations, which validates the correctness of our analysis. In general, we observe that the SOP improves with the increase in $\bar{\gamma}_d$ and M and with the decrease in N. For example, among the considered parameter combinations, the best performance is observed when the highest value of M and the lowest value of N are considered, i.e., when $M = 8$ and $N = 1$.

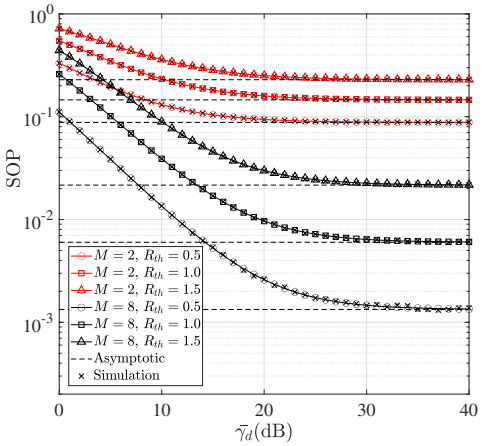


Fig. 4: The SOP versus $\bar{\gamma}_d$ for $M \in \{2, 8\}$ and $R_{\text{th}} \in \{0.5, 1, 1.5\}$.

This is because the diversity in the keyhole-to-user channel improves as M increases, leading to improved user channel SNR. On the contrary, diversity reduces in the keyhole-to-eavesdropping channel as N decreases. We also observe that the SOP improves with $\bar{\gamma}_d$ in the low-SNR regime; however, it saturates in the high-SNR regime. The saturation value exactly matches the asymptotic SOP derived in (19) in the high-SNR regime.

In Fig. 3, the SOP is plotted against M to see the effect of M on the SOP for the different values of $\bar{\gamma}_d \in \{5, 10, 20\}$ dB when $N = 3$. The SOP performance improves sharply with the increase in M initially, however, a diminishing return can be seen as M increases. As M increases, the rate of performance improvement gradually decreases and at higher values of M, the performance gradually saturates depending on other system parameters.

Fig. 4 shows the impact of the threshold secrecy rate R_{th} on the SOP for the different combinations of $M \in \{2, 8\}$ and $N = 3$. As the required threshold R_{th} increases, the SOP performance decreases for a given M, which is intuitive. At a higher value of M, changes in R_{th} impact the SOP

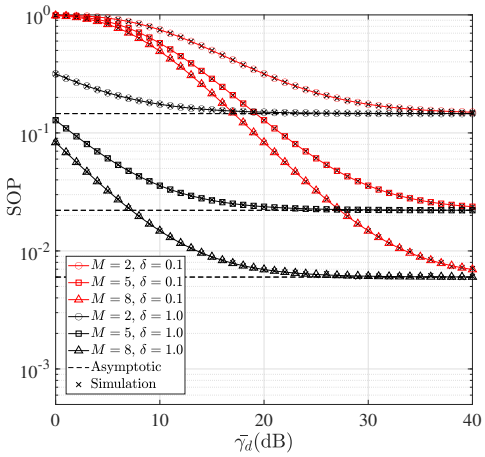


Fig. 5: The SOP versus $\bar{\gamma}_d$ for $M \in \{2, 5, 8\}$ and $\delta \in \{0.1, 1.0\}$.

performance more as the performance gaps corresponding to different R_{th} are more when $M = 8$ than when $M = 2$.

Fig. 5 shows the impact of the keyhole parameter δ on the SOP for the different combinations of $M \in \{2, 5, 8\}$ and $N = 3$. We observe that the SOP improves for the higher values of δ for any M. The higher value of δ represents a large keyhole size, which leads to better transmission with stronger multi-path propagation. For example, we see that the SOPs when $\delta = 1$ for any M is far better than that of $\delta = 0.1$ because the small δ results in severe signal attenuation and deep fades. In addition, we observe no influence of δ on the SOP performance in the high-SNR regime, i.e., the SOPs for $\delta = 0.1$ and $\delta = 1$ provide the same asymptotic results for a particular M in the high-SNR regime. This corroborates the remark made after obtaining the asymptotic SOP in (20), the asymptotic expression is independent of δ in the high-SNR regime.

VI. Conclusions

In this paper, we have presented the secrecy performance analysis of a single keyhole-aided multi-user communication network in the presence of multiple eavesdroppers. Wherein the wireless link experiences an independent Rayleigh fading. The keyhole supports the transmission of both legitimate and unauthorized links. We have derived the exact closed-form expression of the SOP and asymptotic SOP of a user scheduling technique for the keyhole-aided network. Numerical results have shown that the asymptotic SOP in the high-SNR regime saturates to a constant value depending on the system parameters. As such, it can be inferred that there is no influence of the scattering cross-section parameter of the keyhole and the channel parameter of the source-to-keyhole channel on the SOP performance.

Acknowledgment

This work was supported in part by the Ministry of Electronics and Information Technology (MeitY), Govt. of India through its project SwaYaan-Capacity Building in Drone/UAS with Ref. No. L14011/29/2021-HRD and in part by Taighde Éireann – Research Ireland under Grant number 22/PATH-S/10788.

References

[1] D. Chizhik, G. J. Foschini, M. J. Gans, and R. A. Valenzuela, "Keyholes, correlations, and capacities of multielement transmit and receive antennas," *IEEE Trans. Wireless Commun.*, vol. 1, no. 2, pp. 361–368, Apr. 2002.

[2] D. Chizhik, G. J. Foschini, and R. A. Valenzuela, "Capacities of multi-element transmit and receive antennas: Correlations and keyholes," *Electron. Lett.*, vol. 36, no. 13, pp. 1099–1100, Jun. 2000.

[3] D. Gesbert, H. Bolcskei, D. A. Gore, and A. J. Paulraj, "Outdoor MIMO wireless channels: Models and performance prediction," *IEEE Trans. Commun.*, vol. 50, no. 12, pp. 1926–1934, Dec. 2002.

[4] S. Loyka and A. Kouki, "On MIMO channel capacity, correlations, and keyholes: analysis of degenerate channels," *IEEE Trans. Commun.*, vol. 50, no. 12, pp. 1886–1888, Dec. 2002.

[5] G. Levin and S. Loyka, "From multi-keyholes to measure of correlation and power imbalance in MIMO channels: Outage capacity analysis," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3515–3529, Jun. 2011.

[6] P. Almers, F. Tufvesson, and A. F. Molisch,, "Keyhole effect in MIMO wireless channels: Measurements and theory," *IEEE Trans. Wireless Commun.*, vol. 5, no. 12, pp. 3596–3604, Dec. 2006.

[7] S. Loyka, "Multiantenna capacities of waveguide and cavity channels," *IEEE Trans. Veh. Technol.*, vol. 54, no. 3, pp. 863–872, May. 2005.

[8] S. Sanayei and A. Nosratinia, "Antenna selection in keyhole channels," *IEEE Trans. Commun.*, vol. 55, no. 3, pp. 404–408, Mar. 2007.

[9] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[10] X. Zang, C. Ouyang, and H. Yang, "Secrecy performance analysis of MIMO-V2V communications with keyhole effect," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Rio de Janeiro, Brazil, 04-08 Dec. 2022, pp. 1200–1205.

[11] X. Zang, H. Xu, C. Ouyang, and H. Yang, "PHY security in MIMOME keyhole channels," in *Proc. IEEE International Symposium on Broad band Multimedia Systems and Broadcasting (BMSB)*, Beijing, China, 14-16 Jun. 2023, pp. 1–6.

[12] R. Sultana, M. Z. I. Sarkar, and M. S. Hossain, "Security in multiple keyhole MIMO channels," in *Proc. 9th Int. Conf. Elect. Comput. Eng. (ICECE)*, Dhaka, Bangladesh, Dec. 2016, pp. 230–233.

[13] H. Zhang, Z. Liao, Z. Shi, G. Yang, Q. Dou, and S. Ma, "Performance analysis of MIMO-HARQ assisted V2V communications with keyhole effect," *IEEE Trans. Commun.*, vol. 70, no. 5, pp. 3034–3046, May. 2022.

[14] D. Tashman and W. Hamouda, "Cascaded κ-μ fading channels with colluding and non-colluding eavesdroppers: Physical-layer security analysis," *Future Internet*, vol. 13, no. 8, p. 205, Aug. 2021.

[15] D. H. Tashman and W. Hamouda, "Physical-layer security for cognitive radio networks over cascaded rayleigh fading channels," in *Proc. IEEE Global Commun. Conf.*, Taipei, Taiwan, Dec. 2020, pp. 1–6.

[16] C. Kundu, A. Dubey, A. M. Tonello, A. Nallanathan, and M. F. Flanagan, "Destination scheduling for secure pinhole-based power-line communication," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 2245–2260, Sep. 2023.

[17] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, Jun. 2015.

[18] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 356–360.

[19] J. M. Moualeu, P. C. Sofotasios, D. B. da Costa, S. Muhaidat, W. Hamouda, and U. S. Dias, "Physical-layer security of SIMO communication systems over multipath fading conditions," *IEEE Trans. Sustain. Comput.*, vol. 6, no. 1, pp. 105–118, Jan-Mar. 2021.

[20] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 8th ed. Academic Press, 2015.

[21] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, 10th ed., New York, USA, 1968, vol. 55.