JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Optimization of different parameters of NOMA in Nakagami channel

[1] **JAMID MANZOOR**

**, [2] MR. SUMEER KHAJURIA, [3]DR. SAMERU SHARMA**

[1] *Research student of Govt.College of Engineering & Technology,Jammu ( 181122).*
[2] *Associate Professor of Govt.College of Engineering & Technology,Jammu ( 181122).*
[3] *Associate Professor of Govt.College of Engineering & Technology,Jammu ( 181122).*
Department of Electronics & Communication Engineering, Govt.College of Engineering & Technology,Jammu,India.

**Abstract:** NOMA is the multiple access scheme used in 5G technologies. This research investigated the secrecy outage probability (SOP) in Non-Orthogonal Multiple Access (NOMA) systems operating in a Nakagami fading channel. The study focused on the optimization of various factors to enhance the security performance of NOMA communication. The key factors explored include distance between communicating entities, threshold rate, path loss component, shape forming parameter of Nakagami channel, and the impact of shadowing. The methodology involves mathematical analysis and results generated through MATLAB to analyze the SOP under varying conditions. Different scenarios, including varying distances, threshold rates, and path loss components, are considered to understand their influence on security in NOMA. Moreover, the shape forming parameter of the Nakagami channel has been systematically studied to uncover its impact on secrecy. Furthermore, the research introduces the element of shadowing, investigating its effects on SOP in Nakagami channels. The analysis is being presented through both line and bar graphs, providing a comprehensive comparison of SOP trends under different scenarios. Notably, the graphs illustrate the dynamic relationship between SOP and Signal-to-Noise Ratio (SNR), showcasing the practical implications of the findings. The outcomes of this study contribute valuable insights into the design and optimization of NOMA systems for secure communication in Nakagami fading channels. The findings, generated through MATLAB are graphically depicted, aim to inform future developments in wireless communication systems, particularly those employing NOMA techniques.

**KEYWORDS: NOMA, OMA, MIMO, Secrecy outage probability, Nakagami channel, Rayleigh channel, Rician channel, physical layer security, shadowing, eavesdropper, Signal-to-Noise Ratio (SNR),**

**Introduction:** Wireless communication systems, a cornerstone of modern connectivity, face persistent challenges in ensuring secure and confidential information transmission. In this context, the adoption of Non-Orthogonal Multiple Access (NOMA) techniques has emerged as a promising avenue to enhance spectral efficiency. This research delves into the intricate dynamics of NOMA systems operating in Nakagami fading channels, aiming to optimize critical factors that influence the system's secrecy outage probability (SOP). As an innovative multiple access scheme, NOMA allows multiple users to share the same time-frequency resources, offering advantages such as increased throughput and improved fairness. However, the security implications of NOMA in fading channels, especially in Nakagami environments, necessitate a comprehensive exploration of various parameters. The primary focus of this study is to investigate the impact of key factors on the SOP of NOMA systems. These factors include the distance between communication entities, threshold rate for secure communication, path loss components, the shape-forming parameter inherent to Nakagami channels, and the influence of shadowing. Understanding the interplay of these elements is crucial for developing robust and secure NOMA-based wireless communication systems. To execute this investigation, MATLAB has been used to generate graphs and to analyze the SOP under diverse conditions. The graphs encompass scenarios with varying distances, threshold rates, and path loss components, offering insights into the trade-offs between these parameters and the security of NOMA communication. Furthermore, the shape-forming parameter of Nakagami channels has been systematically examined to discern its role in SOP. In addition, the research introduced the influence of shadowing on SOP within Nakagami channels. The outcomes are presented through detailed graphs, providing a visual representation of the SOP trends concerning Signal-to-Noise Ratio (SNR) variations. These graphs not only elucidate the intricate relationship between SOP and SNR but also serve as a practical reference for designing secure NOMA communication systems. In summary, this research endeavors to contribute significant insights into the secure implementation of NOMA techniques in Nakagami fading channels. By systematically optimizing critical parameters, the findings aim to advance the understanding of secure wireless communication, fostering the development of robust and efficient NOMA-based systems.

In the realm of wireless communication systems, Non-Orthogonal Multiple Access (NOMA) has emerged as a transformative concept. NOMA proved to be a groundbreaking paradigm for future cellular radio access, challenging existing LTE schemes. The focus is on downlink NOMA with successive interference cancellation (SIC), showcasing substantial capacity and throughput enhancements for cell edge users [1]. NOMA has got great potential to address challenges in 5G communication, emphasizing its non-orthogonal resource allocation by which arises different NOMA categories [2]. Turning to Multiple Input Multiple Output (MIMO) systems, NOMA implementation using shared pilots has been explored, demonstrating superior performance over traditional orthogonal access schemes [3]. In the uplink context, NOMA's impact has been assessed, revealing optimal retransmission probabilities for maximizing throughput [4]. The analysis extends to various fading channels [5], offering insights into outage probabilities and diversity orders for both uplink and downlink NOMA systems. Meanwhile, the capacity of MIMO NOMA has been examined, with a focus on cluster groups and power coefficient values [6]. Security considerations in the downlink phase are explored [7], presenting Power Allocation Factors and expressions for outage probabilities. Dynamic user grouping methods has been introduced for NOMA, showcasing good performance in Rayleigh fading environments [8]. Cooperative NOMA systems' security aspects are scrutinized [9], and Transmit Reference Signal/Orthogonal Reference Signal schemes are investigated for DF/AF-based NOMA systems [10]. The security of cooperative NOMA systems over Nakagami-m fading channels has been explored, providing insights into secrecy outage performance [11]. Finally, a proposed secure communication protocol for a MIMO NOMA network demonstrates the impact of antenna augmentation on secrecy performance [12]. In a downlink cooperative MISO NOMA network, analytical and asymptotic expressions for the secrecy outage probability had been derived, affirming the benefits of antenna enhancement [13]. This collective literature survey offers a diverse and comprehensive exploration of NOMA, covering various aspects and providing valuable insights for future research in this dynamic field.

## SYSTEM AND CHANNEL MODELS

Consider a NOMA system including a base station (B), two users (U1 which is a far user, and U2 which is near user), and an eavesdropper (E) in a wireless cellular network in Nakagami channel. In this case both users and E are very close to the cell bound. Therefore, it has been considered that there are no direct links between B and the users, as well as with E. Since Nakagami channel has been taken into consideration, shape forming parameter ‘m’ plays a great role in it. It has been further considered that all nodes in the network have single antennas and all the channels suffer from independent Nakagami fading. The superposed signal is sent to every user including eavesdropper

During the initial time slot, a superimposed mixture, [α1x1 + α2x2], is broadcasted from the base station (B) to the relay. Here, xi (i = 1, 2) represents the unit power signal received by user i, and αi is the power allocation coefficient. In order to fully satisfy the need of NOMA for user U1, it has been established that α1 ≥ α2 and power allocation factors has been defined in such a way that satisfy the equation α1^2 + α2^2 = 1. Subsequently, the received signal at the relay can be expressed as:

$$y = h_r(\alpha 1x1 + \alpha 2x2)\sqrt{p_s} + n$$

Where hr denotes the channel gain between the B and the relay and n is the additive white Gaussian noise with zero mean and variance N0

Consider two users near and far user and an eavesdropper in a communication system with channel gains $h_n$ $h_f$ and $h_e$ respectively. Since this research work has been done on Nakagami channel, it typically follows a Nakagami distribution .Accordingly, the links between the transmitter and users are modeled as correlated log-normal random variables (RVs). The distribution of correlated log-normal RVs are as hm ∼ ln N (µhm, σ2 hm), where m ∈ (sn, sf, se). Here, µhm and σ2 hm defines the mean and variance of ln (hm) [11]. The signal attenuation is modeled by αm = exp(−(α1 + α2f^κ) dm), here dm is the distance of link, f describes the transmit frequency in MHz, and α1 and α2 are attenuation constants obtained from experiments.

Let us consider the base station B transmits a source power equals Ps. Since near user requires less power and far user requires more power, the power allocation factors are being provided accordingly such that summation equals to 1. Let $\alpha_1$ is the power factor allocated to near user and $\alpha_2$ is the power factor allocated to the far user. The superposed signal will be equal to

$$x_s = \sqrt{\alpha_1 p_s} x_1 + \sqrt{\alpha_2 p_s} x_2$$

In the above equation x1 and x2 indicates the message signals from near user and far user respectively. This superposed signal is being received by all users including eavesdropper. Individually the received signals of near and far user is as follows

$$y_1 = \left(\sqrt{\alpha_1 p_s} x_1 + \sqrt{\alpha_2 p_s} x_2\right)\alpha_{sn} h_{sn} + n_n$$

$$y_2 = \left(\sqrt{\alpha_1 p_s} x_1 + \sqrt{\alpha_2 p_s} x_2\right)\alpha_{sf} h_{sf} + n_f$$

$h_{sn}$ and $h_{sf}$ represent the channel gain of near and far user respectively, $n_n$ and $n_f$ represent AWGN of near and far user with variances σn^2 and σf^2 [3].

After receiving the superposed signal from the base station, the near user applies SIC that is successive interference cancellation to the received signal. Since it contains the dominant power factor of far user, it decodes the strongest signal of far user first and then subtracts it from the superposed signal to get its desired signal. The far user after receiving the signal from base station treats signal of near user as noise and cancels it before getting its desired signal [6]. SNR at near user and far user can be calculated as

$$\gamma_1 = \frac{\alpha_1 \; p_s \alpha_{sn}^2 h_{sn}^2}{\sigma_1^2}$$

$$\gamma_2 = \frac{\alpha_2 \; p_s \alpha_{sn}^2 h_{sn}^2}{\alpha_1 p_s \alpha_{sf}^2 h_{sf}^2 + \sigma_2^2}$$

In the case of internal eavesdropping, means when far user intends to decode the message signal of near user. By considering this case it is assumed that x2 is perfectly decodable and SNR of far user to decode x1 is given by

$$\gamma_{2\to 1} = \frac{\alpha_1\ p_{sf} h_{sf}^2}{\sigma_2^2}$$

The signal received by this eavesdropper is as follows

$$y_e\ = (\sqrt{\alpha_1 p_s} x_1 + \sqrt{\alpha_2 p_s} x_2)\alpha_{se} h_{se} + n_e$$

Let us consider the external eavesdropper which completely has the access to decode the signals and to eliminate inter user interference. Let the AWGN at E be ne and it has a variance of σ^2e. This case is actually worst case when eavesdropper has decodable ability of legitimate users and serves as extreme bound of SOP. For eavesdropper the SNR for decoding x1 and x2 is as

$$\gamma_{e\to 2} = \frac{\alpha_2\ \ p_{se} h_{se}^2}{\sigma_e^2}$$

$$\gamma_{e\to 1} = \frac{\alpha_1\ p_{se} h_{se}^2}{\sigma_e^2}$$

Now since the Nakagami channel has been taken into consideration, some of its characteristics needs to be explored. The Nakagami-m fading channel gain *h* follows a Gamma distribution with shape parameter *m* [11]. The probability density function (PDF) of the Nakagami-m distribution is as follows

$$f(h) = \frac{2m^m}{\Gamma(m)} h^{2m-1} e^{-mh^2}$$

The path loss component *PL* is modeled as a function of distance *d* and path loss exponent *α*:

$$PL(d) = \left(\frac{d}{do}\right)^{-\alpha}$$

Where $d_o$ is a reference distance.

In Nakagami-m fading channels within NOMA, the shape parameter (*m*) still characterizes the severity of fading. The Nakagami-m distribution is commonly used to model the fading in wireless communication channels.

$$m = \frac{1}{var(\ln(\gamma))}$$

The effect of shadowing has also been considered. Shadowing, also known as log-normal shadowing or path loss variation, is a phenomenon in wireless communication where the received signal strength experiences slow and random fluctuations due to obstacles, environmental conditions, or other factors. These fluctuations are often modeled as a log-normal distribution. It is given by

$$P_r\ = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2\ l\cancel{s}$$

Where:

- *Pr* is the received power.
- *Pt* is the transmitted power.
- *Gt* and *Gr* are the gains of the transmitting and receiving antennas.
- $\lambda$ is the wavelength of the signal.
- *d* is the distance between the transmitter and receiver.
- *Ls* is a shadowing (log-normal) random variable.

In this formula, *Ls* is often modeled as a log-normal random variable with a mean of 0 dB and a standard deviation denoted by $\sigma s$. The log-normal distribution is commonly used to represent the random nature of shadowing effects.

The power received *Pr* can be converted to the received signal strength in decibels (dB) using the formula:

Received Signal Strength (dB) =10·log10(*Pr*)

It's important to note that the specific formulation and parameters used in shadowing models may vary depending on the context and the wireless communication system being analyzed.

Since secrecy outage probability depends on distance between users and base station, power allocation factor, threshold rate, shape parameter, path loss exponent etc. These factors are being altered and respective change has been noticed in SOP vs SNR graph. SNR has been fixed to 30 db for reference. Rayleigh and Nakagami channels are also being compared by keeping all factors constant. Four scenerios has been considered i.e when both user and intruder are in Rayleigh channel, when both are in Nakagami channel, when user is in Nakagami and intruder is in Rayleigh and when user is in Rayleigh and intruder is in Nakagami. The effect of shadowing is also being considered and eavesdropper success rate has been generated. Nakagami is at last compared with Rayleigh and Rician and results show better results with Nakagami.

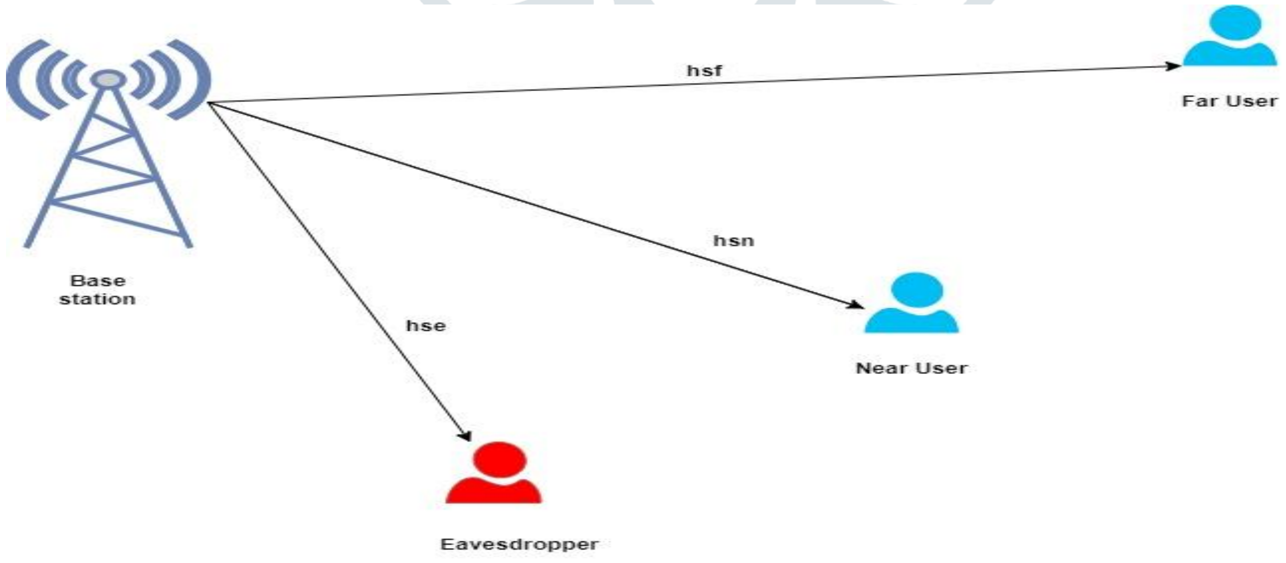


**Fig 1** NOMA with two users and eavesdropper

## RESULTS

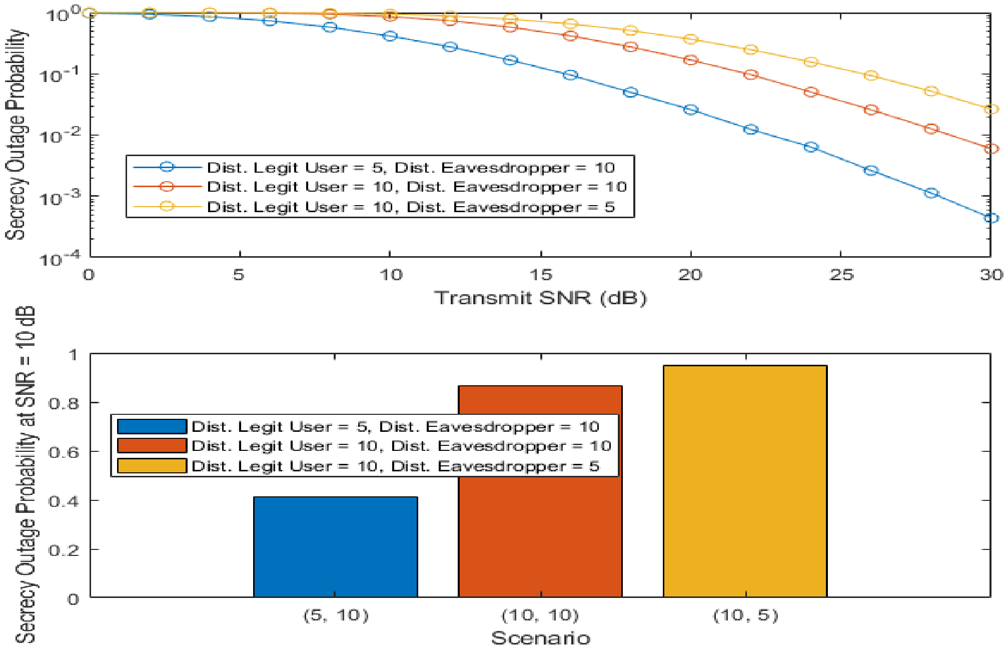


**Fig 1 SOP vs SNR by varying distance**

**Fig 1** shows how SOP changes when the distance has been changed by keeping SNR fixed at 30 db, in both line and bar graph. Distance of user and eavesdropper from base station has been changed to three different values and the case when user is close to base station while eavesdropper is far shows better results in terms of sop than other two cases. In addition to that the worst case scenario is when eavesdropper is close and legitimate user is far from base station.

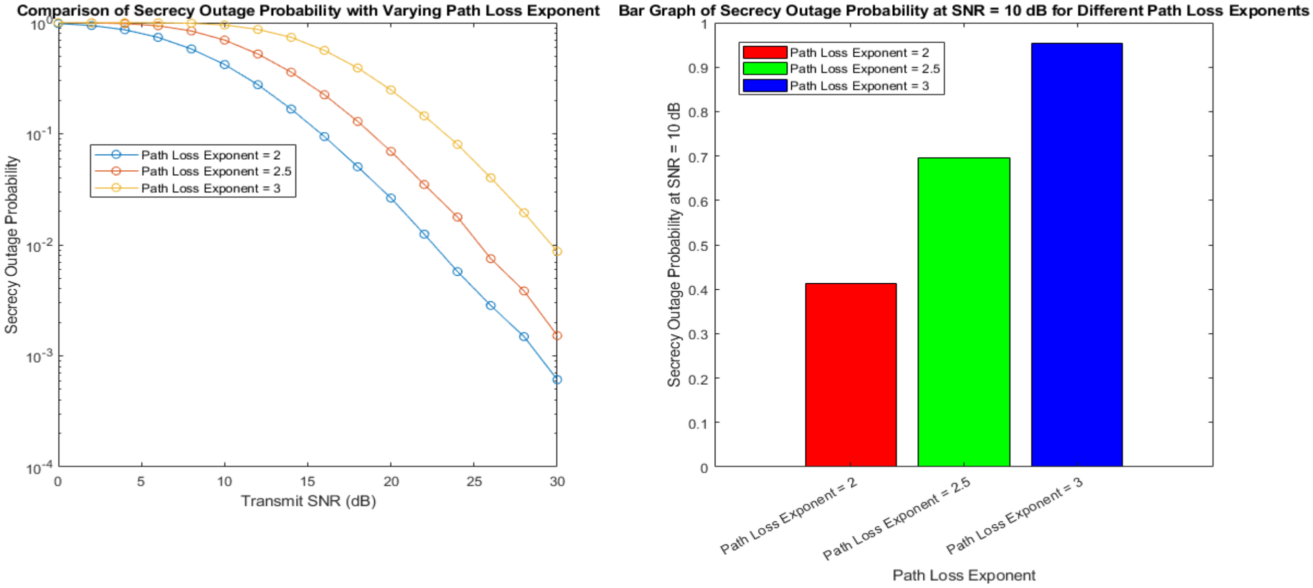
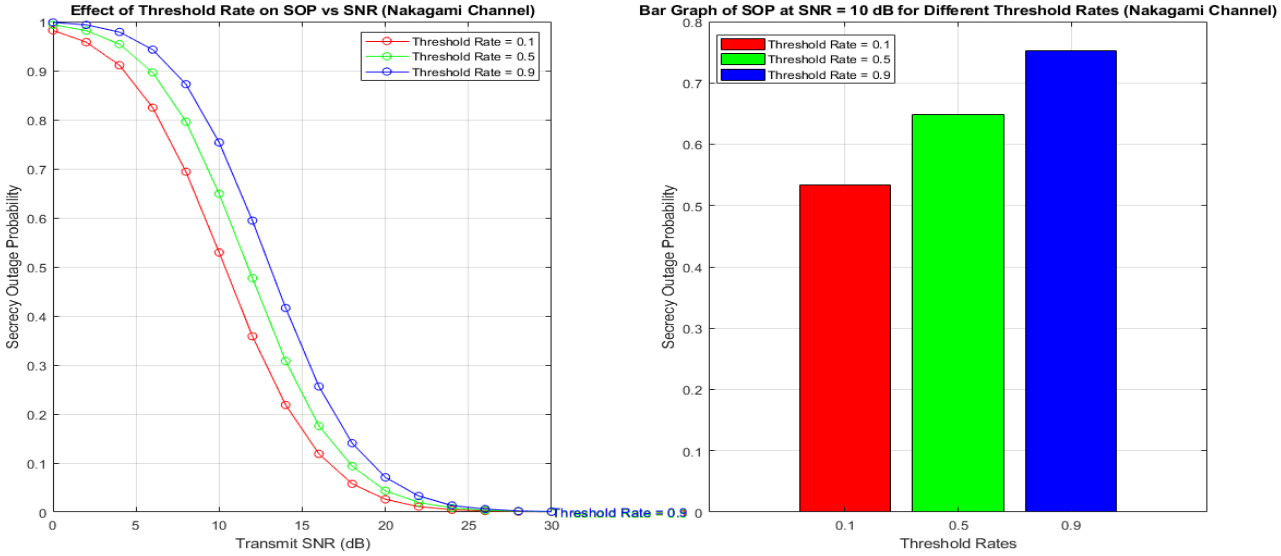


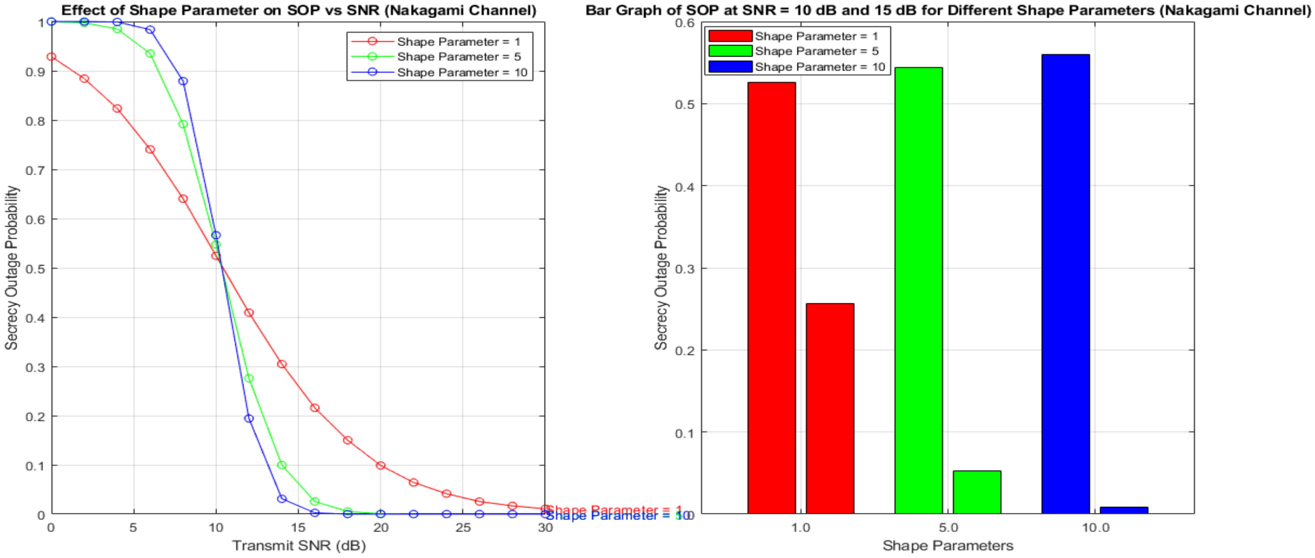
**Fig 2 SOP vs SNR by varying path loss exponent**

**Fig 2** describes the effect of path loss exponent on SOP in both line and bar graph. Path loss exponent has been considered to three different values and results show that less path loss exponent leads to better sop.



## Fig 3 SOP vs SNR by varying threshold rates

**Fig 3** depicts change in SOP by considering different threshold values. Three different threshold rates has been considered and the one with lower value has considerably lower secrecy outage probability.



## Fig 4 SOP vs SNR by varying shape parameter

**Fig 4** depicts how SOP changes by changing shape parameter ‘m’. Shape parameter ‘m’ has been changed to three different values. The results show that before snr=10db the sop increases as we increase shape parameter ‘m’ but after snr is greater than 10db for instance snr=15db has been taken and the result concludes that sop decreases on increasing ‘m’.

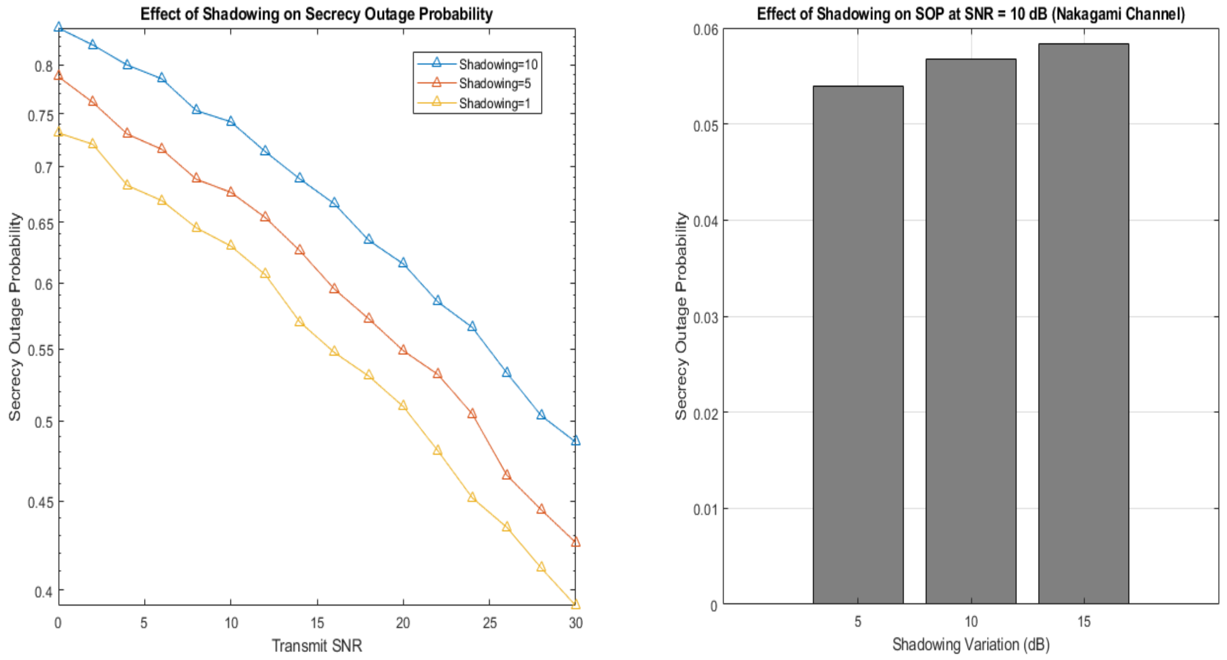


Fig 5 SOP vs SNR by considering shadowing effect

**Fig 5** shows the effect of shadowing on SOP. The shadowing effect has been considered to three different values and the result indicates that lower shadowing lead to lower sop and better performance.

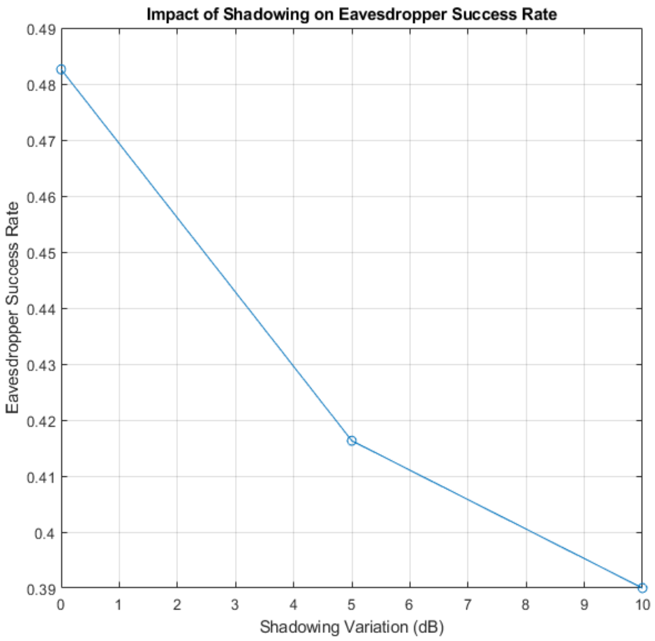


Fig 6 impact of shadowing on eavesdropper success rate

**Fig 6** shows the Impact of shadowing on eavesdropper success rate and result shows eavesdropper success rate decreases on increasing shadowing effect.

# COMPARISON

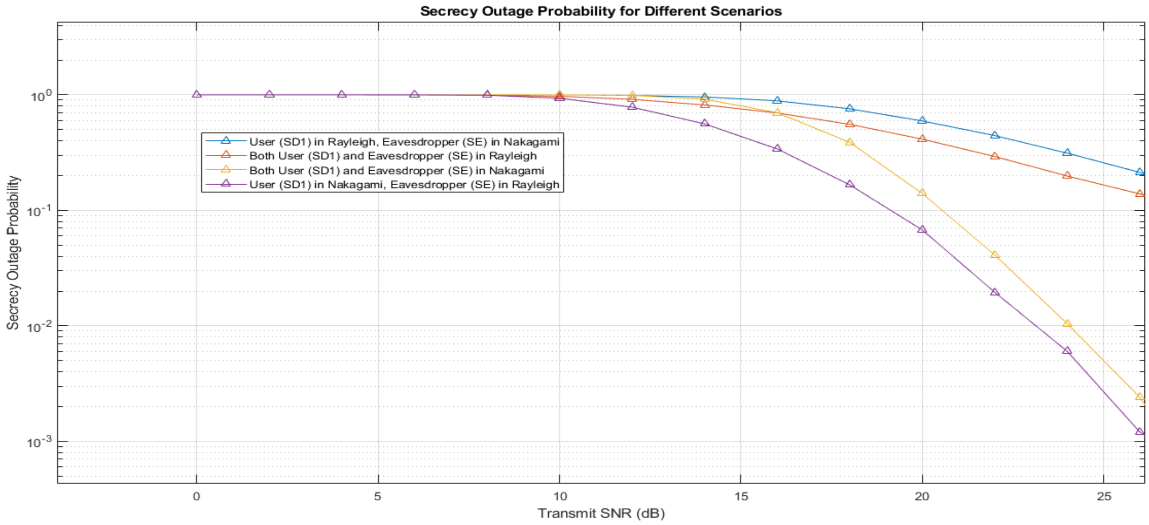


Fig 7 comparison of Rayleigh and Nakagami channels

**Fig 7** shows the comparison of two channels Rayleigh and Nakagami and this creates four cases. First when user is in Nakagami and eavesdropper in Rayleigh, second when both are in Nakagami, third when both are in Rayleigh and fourth when user is in Rayleigh and eavesdropper is in Nakagami. Result shows that first case has lower sop than other cases while fourth is the worst case scenario.

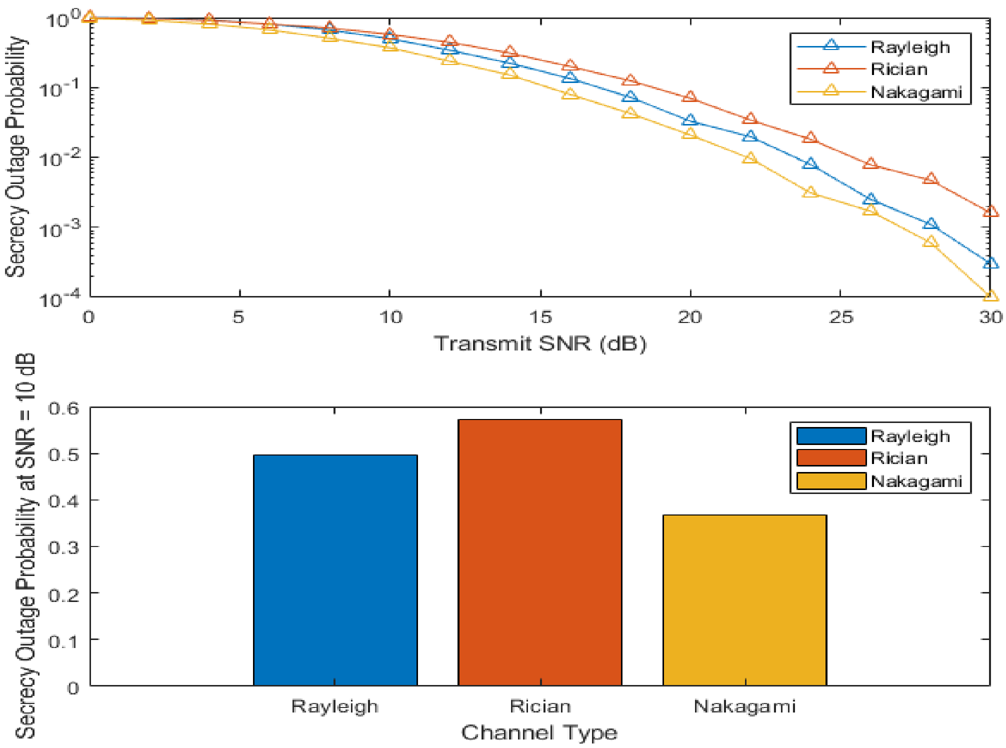


Fig 8 comparison of Rayleigh Rician and Nakagami channels

**Fig 8** compares Rayleigh, Rician and Nakagami fading channels by keeping all factors constant. The result shows that Nakagami performs well and sop is lower than other two channels.

**Conclusion:** Secrecy Outage Probability (SOP) in a Non-Orthogonal Multiple Access (NOMA) system operating over Nakagami fading channels have been analyzed. Various key factors, including distance optimization, threshold rate, path loss components, shape-forming parameters, and the impact of shadowing effects have been explored. The findings highlight the significance of optimizing these parameters to enhance the security and spectral efficiency of NOMA systems in Nakagami channels. The achieved results demonstrate the critical role of each factor in influencing the SOP. In addition, this research work provides valuable insights into the intricate trade-offs and opportunities for securing wireless communication systems in the context of NOMA over Nakagami fading channels. The optimization strategies proposed in this research contribute to advancing the understanding of secure communication in wireless networks. As wireless systems continue to evolve, the outcomes of this study offer practical implications for designing robust and secure NOMA-based communication systems. Additional parameters and scenarios can be altered to further refine the proposed optimization strategies and adapt them to emerging wireless technologies in future. In summary, this research contributes to the ongoing discourse on enhancing the security of wireless communication systems, particularly in the context of NOMA. The comprehensive analysis and optimization strategies presented herein pave the way for future developments in wireless security, offering a valuable foundation for researchers and practitioners alike.

## REFERENCES

[1] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li and K. Higuchi, "Non-Orthogonal Multiple Access (NOMA) for Cellular Future Radio Access," 2013 IEEE 77th Vehicular Technology Conference (VTC Spring), Dresden, Germany, 2013.

[2] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-lin and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," in IEEE Communications Magazine, vol. 53, no. 9, pp. 74-81, September 2015, doi: 10.1109/MCOM.2015.7263349.

[3] H. V. Cheng, E. Björnson and E. G. Larsson, "Performance Analysis of NOMA in Training-Based Multiuser MIMO Systems," in IEEE Transactions on Wireless Communications, vol. 17, no. 1, pp. 372-385, Jan. 2018, doi: 10.1109/TWC.2017.2767030.

[4] J.B. Seo, B. C. Jung and H. Jin, "Nonorthogonal Random Access for 5G Mobile Communication Systems," in IEEE Transactions on Vehicular Technology, vol. 67, no. 8, pp. 7867-7871, Aug. 2018, doi: 10.1109/TVT.2018.2825462.

[5] A. Agarwal, R. Chaurasiya, S. Rai and A. K. Jagannatham, "Outage Probability Analysis for NOMA Downlink and Uplink Communication Systems With Generalized Fading Channels," in IEEE Access, vol. 8, pp. 220461-220481, 2020.

[6] M. Zeng, A. Yadav, O. A. Dobre, G. I. Tsiropoulos and H. V. Poor, "On the Sum Rate of MIMO-NOMA and MIMO-OMA Systems," in IEEE Wireless Communications Letters, vol. 6, no. 4, pp. 534-537, Aug. 2017, doi: 10.1109/LWC.2017.2712149.

[7] Mohammad A Ahmad, M. A. Raza and O. A. Dobre, "Signature-Based Nonorthogonal Massive Multiple Access for Future Wireless Networks: Uplink Massive Connectivity for Machine-Type Communications," in IEEE Vehicular Technology Magazine, vol. 13, no. 4, pp. 40-50, Dec. 2018, doi: 10.1109/MVT.2018.2869425.

[8] Y. Yin, Y. Peng, M. Liu, J. Yang and G. Gui, "Dynamic User Grouping-Based NOMA Over Rayleigh Fading Channels," in IEEE Access, vol. 7, pp. 110964-110971, 2019.

[9] J. Chen, L. Yang and M. -S. Alouini, "Physical Layer Security for Cooperative NOMA Systems," in IEEE Transactions on Vehicular Technology, vol. 67, no. 5, pp. 4645-4649, May 2018.

[10] Z. Wang and Z. Peng, "Secrecy Performance Analysis of Relay Selection in Cooperative NOMA Systems," in IEEE Access, vol. 7, pp. 86274-86287, 2019.

[11] C. Yu, H. -L. Ko, X. Peng and W. Xie, "Secrecy Outage Performance Analysis for Cooperative NOMA Over Nakagami- m Channel," in IEEE Access, vol. 7, pp. 79866-79876, 2019, doi: 10.1109/ACCESS.2019.2923450.

[12] D. -D. Tran, H. -V. Tran, D. -B. Ha and G. Kaddoum, "Secure Transmit Antenna Selection Protocol for MIMO NOMA Networks Over Nakagami-m Channels," in IEEE Systems Journal, vol. 14, no. 1, pp. 253-264, March 2020, doi: 10.1109/JSYST.2019.2900090.

[13] T.N Kieu, Duc-Dung Tran, Dac-Binh Ha & Miroslav Voznak (2022) Secrecy Performance Analysis of Cooperative MISO NOMA Networks Over Nakagami-m Fading, IETE Journal of Research, 68:2, 1183-1194, DOI: 10.1080/03772063.2019.1643267.