Secrecy Performance Analysis of IRS-assisted NLoS Wireless Systems Over Nakagami-m Fading Channel

Ravneet Kaur, and Bajrang Bansal, *Member, IEEE*

***Abstract*—Due to increasing security threats in next generation wireless networks and promising potential of intelligent reflecting surface (IRS) in enhancing the wireless system's performance, this paper focuses on secure transmission of passive and active IRS-assisted wireless communication system in the presence of single and multiple eavesdroppers. We propose optimized passive and active IRS based schemes with perfect phase estimation to mitigate the fading effects of legitimate link over Nakagami-m fading channel. The analytical expression for secrecy outage probability (SOP) is derived. We present the simulation results for secrecy capacity as well as SOP and compare them with different benchmark schemes like (a) random passive IRS, (b) passive IRS with phase error, and (c) without IRS. It is observed that the proposed optimized schemes outperform the different benchmark schemes. In addition, to get more insights, we also demonstrate the impact of varying the number of IRS reflecting elements, Nakagami shape parameter, and target secrecy rate on the secrecy performance of the system. Simulation results validate the derived analytical results.**

***Index Terms*—Physical layer security, intelligent reflecting surface, Nakagami-m fading, secrecy capacity, secrecy outage probability.**

I. Introduction

THE digital interconnection of numerous devices has been possible due to wireless communication [1]. In the envisioned future, there will be smart networked connection of devices which will be made possible due to the sixth generation (6G) technology that is expected to provide "service everywhere". Here, it becomes necessary to maintain the privacy and security of the large amount of information transmitted between these entities [2]. Since the wireless propagation environment is vulnerable to malicious attacks, it can be protected by applying physical layer security (PLS) techniques which are superior to traditional cryptographic strategies because they do not require complicated encoding/decoding methods [3]. Also, due to the decentralized and distributed structure of fifth generation (5G) and beyond networks, it becomes very hard to deal with cryptographic key management and distribution. So, by utilizing the inherent characteristics of channel propagation, such as fading, noise, and interference, security at physical layer can be realized [4].

To circumvent the adverse effects of such transmission medium and to enhance the PLS, it is required to intelligently gain control of it which can be achieved by utilizing reconfigurable devices referred to as intelligent reflecting surface (IRS). It is a planar surface having large number of reflecting elements that can intelligently control the phase, frequency, or amplitude of an incident signal. There are two main kinds of IRS: passive and active. It is crucial to study both types of IRS in order to clearly understand their applicability in real-life scenarios [5]. In passive IRS, the reflecting elements are able to intelligently modify the phase shifts of the incident signals without requiring any additional power supply, thus substantially reducing the hardware cost and energy consumption. The signals reflected from IRS are constructively added at the desired receiver to enhance the signal-to-noise ratio (SNR) and destructively combined at the eavesdropper to reduce the interference [6]. Due to its easy deployment and ability to smartly control the wireless propagation environment, IRS technology can be used to improve coverage, data rates, security, and energy efficiency of the wireless communication systems. Passive IRS is particularly useful in rural areas to enhance the signal coverage with limited infrastructure. Also, it is beneficial in designing low-power applications where energy savings are critical [7].

On the other hand, active IRS differs from passive IRS in the sense that it is equipped with active components also, that not only modify the phase shifts but can also change the amplitude of the incident signal at the cost of small additional power supply. This feature of active IRS helps in overcoming the multiplicative fading problem of passive IRS which occurs due to the total path loss of the base station (BS)-IRS-receiver link that is the product of the individual path losses (BS-IRS and IRS-receiver links), resulting in severe degradation of SNR. Active IRS is suitable for industrial or remote environments that require high quality signal in localized dead zones. It is also desirable in high-traffic urban areas such as airports, concerts, etc. to provide consistent, high-speed, and secured connectivity to users [8]. Both passive and active IRS have the ability to revolutionize the 6G networks by improving their coverage, security, energy efficiency, spectral efficiency, and adaptability [7], [9].

Due to many advantages of IRS, researchers have begun

Manuscript received January 27, 2025; revised February 21, 2025. Date of publication July 10, 2025. Date of current version July 10, 2025. The associate editor prof. Maja Braovic has been coordinating the review of this manuscript and approved it for publication.

Authors are with the Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Noida, India (e-mails: 20402005@mail.jiit.ac.in, bajrangbnsl@gmail.com).

Digital Object Identifier (DOI): 10.24138/jcomss-2025-0001

investigating its performance from different perspectives such as enhancing spectral efficiency, energy efficiency, PLS, and supporting wireless communications in simultaneous wireless information and power transfer (SWIPT), non-orthogonal multiple access (NOMA), and cognitive radio (CR) networks [10]. Owing to the passive nature of eavesdropping attack on the legitimate communication channel, it becomes very challenging to enhance the PLS of the system. In light of these challenges, research is being carried out worldwide to enhance the security of IRS-assisted wireless communication systems.

Taking into account the favourable characteristics of IRS, there are research works that cover the secrecy performance of passive IRS-assisted network topologies over Rayleigh and Rician fading channels. The authors in [11] and [12] considered a single eavesdropper wireless system where a single antenna receiver receives communicating signals from multi-antenna access point via IRS and maximized its secrecy rate by assuming Rician and Rayleigh fading respectively. In [13], considering Rician fading, the authors investigated the secrecy performance of a downlink wireless system consisting of multi-antenna transmitter that communicates with multiple receivers through IRS in the presence of multiple eavesdroppers. In [14], considering Rayleigh fading, the authors maximized the effective covert rate of an IRS-NOMA assisted covert communication system composed of a BS, users, monitor and an IRS that ensures low detection probability. These research works achieved enhanced secrecy performance by focusing more on complex optimization methods. On the other hand, in [15], assuming Rayleigh fading, the authors investigated the SOP of a single-antenna user system in the presence of an eavesdropper considering optimal IRS phase shifts.

Several studies in literature have investigated the secrecy performance of active IRS-assisted networks over Rayleigh and Rician fading channels. In [16], the authors analyzed the secrecy performance of a multi-antenna active IRS-assisted system over Rayleigh fading channels. An alternating optimization (AO) algorithm is developed for joint optimization of the beamforming vector at transmitter and reflecting matrix at IRS to enhance the secrecy rate of the proposed system. In another research [17], the authors enhanced the secrecy rate of an active IRS-assisted cognitive radio system by utilizing an iterative algorithm optimization. All the IRS-assisted links experienced Rician fading and the non-IRS links underwent Rayleigh fading. Inspired by the advanced capabilities of both passive and active IRS, the authors have considered hybrid active-passive IRS architecture in [18], [19] to maximize the secrecy rate of a millimeter wave multi-antenna system and a sophisticated downlink multi-antenna architecture by using joint optimization techniques.

In recent years, researchers have also analyzed the performance of passive and active IRS-assisted networks over Nakagami-m fading channels to study more realistic channel fading conditions. This distribution is generic as it can model signal fading conditions ranging from severe to moderate or even no fading at all. So, Nakagami-m model can be used to analyze the performance of communication systems that operate in environments with varying degree of multipath fading, including both line-of-sight (LoS) and non-LoS (NLoS) conditions [20]. It matches the empirical fading data more accurately as compared to Rayleigh, log-normal or Rician fading distributions due to its ability to adjust parameter m according to the varying fading conditions [21]. Considering passive IRS-assisted wireless networks, there are some research works in the literature that focus on different aspects of performance such as outage probability (OP), bit error rate (BER), and ergodic capacity (EC) over Nakagami fading channels [22]–[27]. Also, there are a handful of research works in which passive IRS is utilized to improve the secrecy performance, mitigate eavesdropping, and enhance the robustness of communication systems subject to Nakagami-m fading scenarios [1], [28]–[31]. Furthermore, in the context of active IRS-assisted wireless networks, there are few research studies in the literature that have focused on various aspects such as OP, EC, and spatial throughput (SP) over Nakagami-m fading channels [32]–[36]. But to the best of authors' knowledge, the secrecy analysis of active IRS-assisted wireless communication systems over Nakagami-m fading channel has not been done before.

From the aforementioned discussion, first, we have observed scarcity of work that performs a detailed investigation on the secrecy performance of passive IRS-assisted wireless networks over Nakagami-m fading channel. There is a lack of research dealing with impact of different system parameters on secrecy performance such as Nakagami shape parameter (m) and target secrecy rate. Second, we have also observed that role of active IRS in enhancing the secrecy performance of the communication system over Nakagami-m fading channel has not been reported before. By comprehensive secrecy analysis of passive and active IRS-assisted networks over Nakagami-m fading channel, we can contribute to the efficient design of next-generation secure communication systems that can operate in a wide range of real-world environments. A thorough secrecy analysis of both passive and active IRS-assisted systems over Nakagami-m fading is vital to achieve robust wireless communication in various important real world domains such as military and defense, banking, healthcare, and telemedicine.

Inspired by the above discussion, this work aims to fulfill the research gaps in the literature by performing comprehensive analysis of the secrecy performance of passive and active IRS-assisted systems over Nakagami-m fading channel. Specifically, the main contributions of our work are as follows:

- Considering Nakagami-m fading, we propose an optimized passive and active IRS-based scheme with perfect phase estimation in the presence of an eavesdropper to nullify the fading effects of legitimate link. This is done to enhance the secrecy performance of the considered system.
- We derive the analytical expression for SOP of the considered passive and active IRS-assisted system. It is a key performance metric that helps in assessing the level of security achieved by a communication system.
- The simulation results are presented for the secrecy capacity and SOP of the considered system. The accuracy of our theoretical analysis is also confirmed.

- Secrecy performance of the proposed optimized passive and active IRS based schemes with perfect phase estimation are compared with three different benchmark schemes, i.e., (a) random passive IRS, (a) passive IRS with phase error, and (c) without IRS.
- Taking into account the single eavesdropper scenario, the impact of varying the number of IRS elements and the Nakagami shape parameter on the secrecy capacity and SOP of the proposed schemes is analyzed.
- The secrecy capacity of the proposed schemes is further analyzed in the presence of multiple eavesdroppers to gain a deeper understanding of more realistic and complex scenarios.
- Finally, we observe the impact of varying the target secrecy rate parameter on the SOP performance of the proposed schemes. This is crucial as it helps us to understand the effectiveness of our proposed schemes in realizing the robust and reliable communication systems.

Fig. 1 gives the structural representation of the paper. Section II presents a review of the related works. Section III presents the system and channel model and the proposed optimized passive and active IRS based schemes with perfect phase estimation. The concept of passive IRS with phase error is also presented. In Section IV, we discuss the secrecy capacity and derive the analytical expressions for SOP which provides the theoretical fundamentals for analyzing our proposed schemes. Simulation results and discussion are presented in Section V. Finally, the concluding remarks are made in Section VI.

II. Related Works

This section discusses recent works that are focused on passive and active IRS-based communication systems operating over Nakagami-m fading channel.

In the context of passive IRS-assisted networks over Nakagami-m fading channels, there are a few works in literature that demonstrated improvement in terms of OP, BER, and EC. In [22], considering two different IRS phase configurations and Nakagami-m fading, the authors investigated the performance of an IRS-assisted downlink communication system having single-antenna transmitter and receiver in terms of OP, BER, and EC. In [23], the authors proposed a new analytical framework that calculates the channel capacity for an IRS-assisted wireless network having single-antenna transmitter and receiver over Nakagami-m fading channels. The authors in [24] deduced the closed form expressions of OP and EC for full duplex Internet of Things (IoT) networks having a single-antenna transmitter and receiver over both realistic Rician and Nakagami fadings.

In [25], the authors analyzed the performance of passive IRS-assisted wireless system with single transmitter and receiver having spatially correlated Nakagami-m distributed IRS channel coefficients. Closed form expressions of symbol error probability (SEP), OP, and average channel capacity are obtained. The authors in [26] proposed an IRS-assisted bidirectional full-duplex (FD) wireless system having two source nodes equipped with dual antennas and derived the analytical expressions for OP and BER considering Nakagami-m fading. In another research [27], the authors investigated the performance of an IRS-assisted dual-hop wireless communication system having single transmitter and a receiver in terms of OP, average BER, and average capacity. The authors proposed a single link-switching threshold algorithm to get connectivity between end-user terminals and considered Rayleigh fading for LoS link and Nakagami fading for NLoS link respectively.

There are a handful of research works in which passive IRS is utilized to enhance the secrecy performance of wireless systems for Nakagami-m fading scenarios [1], [28]–[31]. In [1], the authors investigated the secrecy performance of Wyner's wiretap model where the access point is configured with passive IRS over Nakagami-m fading channels. The authors in [28] analyzed the SOP and bit error probability (BEP) of passive IRS-assisted wireless system consisting of a multi-antenna transmitter, a single antenna receiver, and an eavesdropper under Nakagami-m fading. In [29], considering the Nakagami-m fading, the authors investigated the PLS performance of simultaneously transmitting and receiving-IRS (STAR-IRS) NOMA network by deriving the analytical expressions of SOP. The authors in [30] considered a vehicle-to-infrastructure (V2I) communications system with IRS and analyzed its performance in terms of average secrecy capacity over Nakagami-m fading channels. In [31], considering Nakagami-m fading, the authors studied a passive IRS-assisted uplink NOMA communication system having a BS, multiple users, and an eavesdropper and evaluated its secrecy rate.

Considering active IRS-assisted communication systems over Nakagami-m fading channel, there are some notable research works that demonstrated improvement in performance metrics like OP, EC, and spatial throughput (SP) [32]–[36]. In [32], the authors investigated the performance of active IRS-assisted-NOMA with hardware impairments networks over cascaded Nakagami-m fading channel in terms of OP and EC. In another study [33], assuming Nakagami-m fading, the authors analyzed the approximate ergodic achievable rate of an active IRS-assisted communication system considering discrete phase shifters. The authors in [34] analyzed the performance of active IRS-assisted single-cell wireless network having a single antenna BS and multiple single antenna users over Nakagami-m fading channel in terms of spatial throughput. In another research [35], considering Nakagami-m fading channel, the authors analyzed the performance of active IRS-assisted NOMA networks composed of single antenna BS and multiple single antenna users. The impact of hardware impairment with imperfect and perfect successive interference cancellation is considered and the OP of the system is obtained. The authors in [36] investigated the performance of passive and active IRS-assisted systems having multiple antenna BS and single antenna user over Nakagami-m fading channel while considering discrete IRS phase shift designs. The maximum ratio transmission (MRT) based beamforming design is proposed to analyze the OP and EC of the system.

In view of the aforementioned research works on secrecy analysis of Nakagami-m fading scenarios, it is observed that passive IRS has been used in enhancing the secrecy performance of diverse communication systems but there is

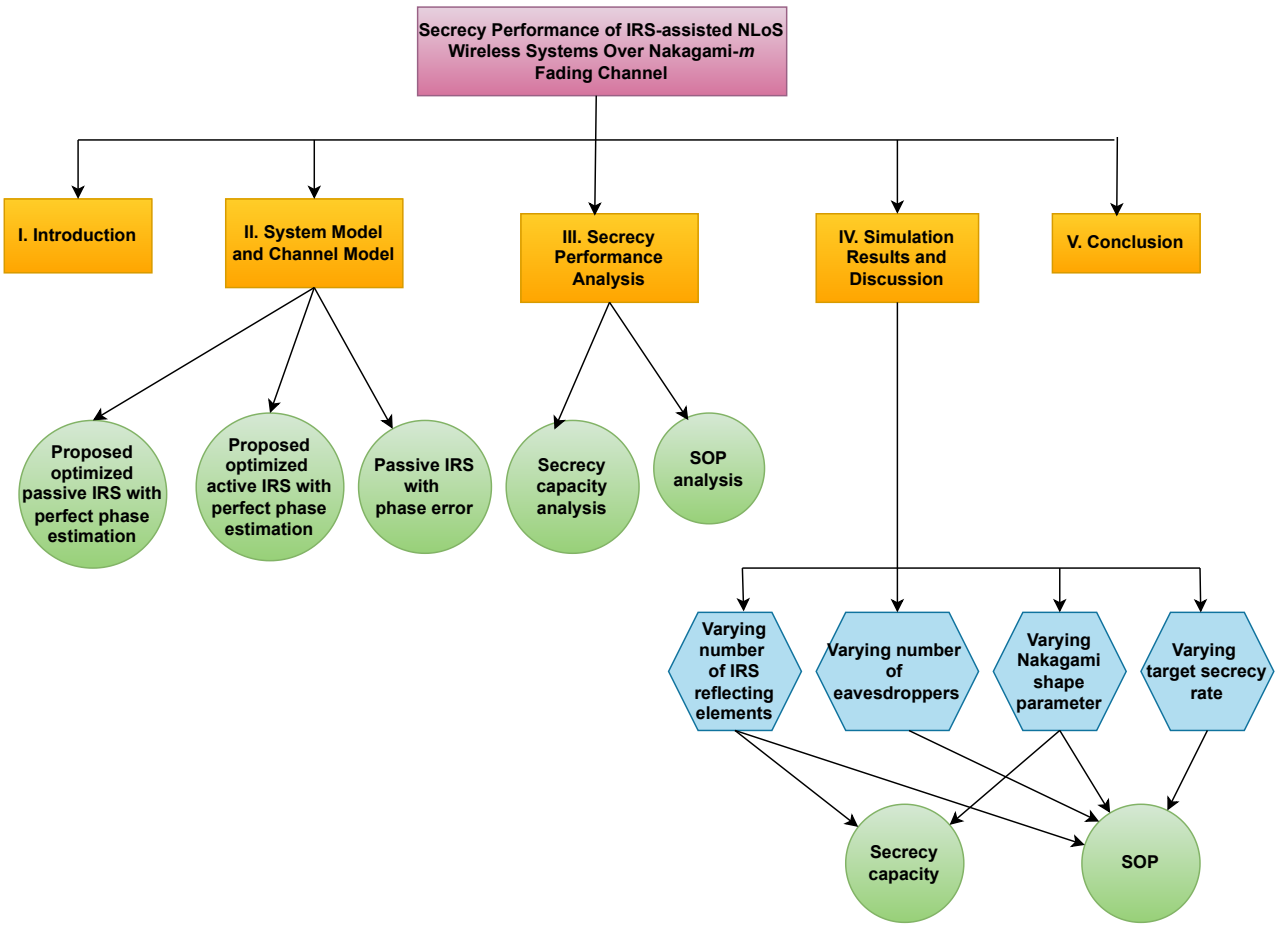


Fig. 1. Structural representation of the paper

a paucity of investigations while considering the impact of different parameters such as number of IRS elements, number of eavesdroppers, Nakagami shape parameter, and target secrecy rate on the secrecy performance. Also, in the context of active IRS, it can be inferred that active IRS has been widely studied for general communication enhancement, but its application specifically in secrecy analysis over Nakagami-m fading channels has not been explored. This motivates us to perform the comprehensive analysis of secrecy performance of passive and active IRS-assisted communication systems considering Nakagami-m fading.

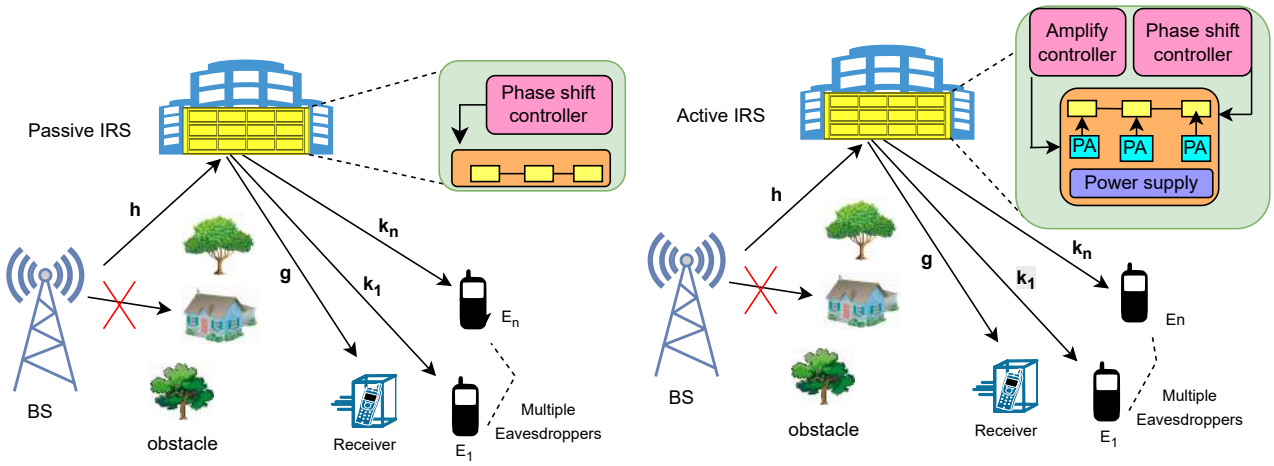
Table I shows the list of parameters used in the paper.

TABLE I
LIST OF PARAMETERS

Symbols	*Definition*
N	Number of IRS reflecting elements
y_i	Received signal at legitimate receiver and eavesdropper in passive/active IRS scenario where $i \in [Rp, Ep, Ra, Ea]$
s	Unit energy information bearing signal
h_l, g_l, k_l	Complex Gaussian RVs with zero mean and unit variance
P_t	Transmit power
ϕ_l	Phase shift at the l^{th} reflecting element of IRS
α	Amplification factor of active IRS element
ζ_i	Additive white Gaussian noise (AWGN) where $i \in [R, E]$
σ_i^2	Variance of AWGN where $i \in [R, E]$
ζ_I	Noise introduced by active IRS
σ_I^2	Variance of active IRS noise
$f_X(x)$	PDF of Nakagami-m distribution
m_d	Shape parameter of Nakagami-m distribution with $d \in [h_l, g_l, k_l]$
Ω_d	Spread parameter of Nakagami-m distribution with $d \in [h_l, g_l, k_l]$
γ_i	Received SNR where $i \in [Rp, Ep, Ra, Ea]$
ρ_d	Series of complex numbers
f_{γ_E}	PDF of Exponential RV
λ_E	Distribution parameter
C_s	Secrecy capacity
C_{tr}	Target secrecy rate

III. SYSTEM AND CHANNEL MODEL

We consider a wireless communication system in which a single-antenna BS transmits the information signal to single-antenna receiver (R) via IRS which has N passive/active reflecting elements in the presence of multiple non-colluding eavesdroppers E_i, $(i \in 1, 2, ..., n)$. Due to the presence of natural or man-made obstacles, the direct link between the BS and R and the BS and E_i, $(i \in 1, 2, ..., n)$ is completely blocked. We assume that all links undergo Nakagami-m fading and their channel state information (CSI) is known. The overall



(a) Passive IRS-assisted system model

(b) Active IRS-assisted system model

Fig. 2. Proposed passive and active IRS-based communication system model

system for passive and active IRS is depicted in Figs. 2a and 2b respectively. The corresponding received signals and the resulting SNR obtained at the legitimate receiver by exploiting the passive and the active IRS are detailed next.

First, considering passive IRS design, it has a phase shift circuit that can intelligently tune the phase shifts of each reflecting element to reflect the incident signal from the BS to the intended receiver but without any amplification. So, the received signals at the receiver (R) and the eavesdropper (E), i.e., y_{Rp} and y_{Ep} can be mathematically expressed as

$$y_{Rp} = \left(\sum_{l=1}^{N} h_l g_l e^{j\phi_l} \right) \sqrt{P_t} s + \zeta_R, \tag{1}$$

$$y_{Ep} = \left(\sum_{l=1}^{N} h_l k_l e^{j\phi_l} \right) \sqrt{P_t} s + \zeta_E, \tag{2}$$

where P_t denotes the transmit power, s is the unit energy information bearing signal, h_l, g_l, and k_l $(l \in 1, 2, ..., N)$ are the complex fading coefficients of the BS-IRS, IRS-R and IRS-E links respectively. These are the complex Gaussian random variables (RVs) with zero mean and unit variance. In addition, $\phi_l \in [0, 2\pi]$ is the phase shift at the l^{th} reflecting element of the IRS. The variables $\zeta_R \sim \mathcal{CN}(0, \sigma_R^2)$ and $\zeta_E \sim \mathcal{CN}(0, \sigma_E^2)$ are the additive white Gaussian noise (AWGN) having zero mean and variance σ_R^2 and σ_E^2 respectively. In (1) and (2), $h_l = |h_l| e^{j\theta_{h_l}}$, $g_l = |g_l| e^{j\theta_{g_l}}$, and $k_l = |k_l| e^{j\theta_{k_l}}$ where the envelopes $|h_l|$, $|g_l|$, and $|k_l|$ follow Nakagami-m distribution whose probability density function (PDF) is given as

$$f_X(x) = \frac{2 m_d^{m_d}}{\Gamma(m_d) \Omega_d^{m_d}} x^{2m_d - 1} e^{-\frac{m_d}{\Omega_d} x^2}. \tag{3}$$

The parameters m_d and Ω_d respectively denote the shape and spread parameters of Nakagami-m PDF with $d \in [h_l, g_l, k_l]$ and symbol Γ representing the Gamma function which is given as $\Gamma(n) = \int_0^\infty z^{n-1} e^{-z} dz$.

Next, in the active IRS-assisted scenario, besides phase shift circuit that can smartly tune the phase shifts of each reflecting element as in passive IRS, the architecture of active IRS consists of a power amplifier also to enhance the incident signal strength. However, it introduces additional noise similar to the conventional amplifiers. So, considering active IRS, the received signals at the receiver (R) and the eavesdropper (E), i.e., y_{Ra} and y_{Ea} can be mathematically expressed as

$$y_{Ra} = \left(\sum_{l=1}^{N} h_l g_l \alpha_l e^{j\phi_l} \right) \sqrt{P_t} s + (\mathbf{g}^T \mathbf{\Phi}) \zeta_I + \zeta_R, \tag{4}$$

$$y_{Ea} = \left(\sum_{l=1}^{N} h_l k_l \alpha_l e^{j\phi_l} \right) \sqrt{P_t} s + (\mathbf{k}^T \mathbf{\Phi}) \zeta_I + \zeta_E, \tag{5}$$

where ζ_I is the noise introduced by the active IRS that can be modeled as $\zeta_I \sim \mathcal{CN}(0, \sigma_I^2)$ and $\alpha_l \geq 1$ is the amplification factor at the l^{th} reflecting element of the IRS.

In the following subsections, we discuss the statistical analysis of our proposed schemes of optimized passive IRS with perfect phase estimation, optimized active IRS with perfect phase estimation, and the special case of passive IRS with phase error.

A. Proposed optimized passive IRS with perfect phase estimation

The received signal y_{Rp} in (1) can be written as

$$y_{Rp} = \left(\sum_{l=1}^{N} |h_l||g_l| e^{j(\theta_{h_l} + \theta_{g_l} + \phi_l)} \right) \sqrt{P_t} s + \zeta_R. \tag{6}$$

Taking into account the perfect phase estimation at passive IRS so as to nullify the overall phase shift induced by the fading channel and to maximize the received SNR at the

legitimate receiver, the optimized phase shift for the l^{th} element can be expressed as

$$\phi_l = -\theta_{h_l} - \theta_{g_l}. \tag{7}$$

From (7), it can be observed that the optimized IRS primarily targets constructive addition for the legitimate user, without explicitly targeting the eavesdropper's channel [15], [28], [37], [38]. Therefore, the optimal received SNR at the legitimate receiver is found as

$$\gamma_{Rp} = \left(\sum_{l=1}^{N} |h_l||g_l|\right)^2 \frac{P_t}{\sigma_R^2}. \tag{8}$$

Denoting $|h_l||g_l| = G_l$, (8) can be rewritten as

$$\gamma_{Rp} = \left(\sum_{l=1}^{N} G_l\right)^2 \frac{P_t}{\sigma_R^2} = \left(Y\frac{\sqrt{P_t}}{\sigma_R}\right)^2, \tag{9}$$

where $Y = \sum_{l=1}^{N} G_l$ represents the sum of N independent and identically distributed (i.i.d.) double Nakagami-m RVs.

B. Proposed Optimized active IRS with perfect phase estimation

The received signal y_{Ra} in (4) can be written as

$$y_{Ra} = \left(\sum_{l=1}^{N} |h_l||g_l|\alpha_l e^{j(\theta_{h_l}+\theta_{g_l}+\phi_l)}\right)\sqrt{P_t}s + (\mathbf{g}^T\mathbf{\Phi})\zeta_I + \zeta_R. \tag{10}$$

Considering perfect estimation of phase shifts induced by the fading channel at active IRS to maximize the SNR (as given in (7)) and assuming equal amplification factor α_l for all active IRS reflecting elements, i.e., $\alpha_1 = \alpha_2 = ... = \alpha_N = \alpha$ [39] to facilitate practical implementation, the received SNR at the intended receiver is expressed as

$$\gamma_{Ra} = \alpha^2 \left(\sum_{l=1}^{N} |h_l||g_l|\right)^2 \frac{P_t}{\sigma_R^2 + ||\mathbf{g}^T\mathbf{\Phi}||^2\sigma_I^2}, \tag{11}$$

which can be rewritten as

$$\gamma_{Ra} = \alpha^2 \left(\sum_{l=1}^{N} |h_l||g_l|\right)^2 \frac{P_t}{\sigma_2^2}, \tag{12}$$

where $\sigma_2^2 = \sigma_R^2 + ||\mathbf{g}^T\mathbf{\Phi}||^2\sigma_I^2$. Representing $|h_l||g_l| = G_l$, (12) can be rewritten as

$$\gamma_{Ra} = \left(\sum_{l=1}^{N} G_l\right)^2 \frac{P_t}{\sigma_2^2} = \left(Y\frac{\sqrt{P_t}}{\sigma_2}\right)^2, \tag{13}$$

which is similar to the SNR equation for passive IRS in (9).

Now, according to the central limit theorem (CLT), Y can be approximated as a Gaussian distributed RV. Here, it should be noted that to get the mean, (μ_Y) and variance, (σ_Y^2) of Y, we need to find the mean and variance of $G_l = |h_l||g_l|$ which is double Nakagami-m distributed. The statistical parameters of G_l denoted by μ_G and σ_G^2 can be found by using the c^{th} moment of G_l given as [40]

$$E[G_l^c] = \prod_{k=1}^{2} \frac{\Gamma(m_k + \frac{c}{2})}{\Gamma(m_k)} \left(\frac{\Omega_k}{m_k}\right)^{c/2}. \tag{14}$$

For calculating the mean, we consider $c = 1$ in (14), which gives

$$\mu_G = E[G_l] = \frac{\Gamma(m_1 + \frac{1}{2})}{\Gamma(m_1)} \left(\frac{\Omega_1}{m_1}\right)^{1/2} \frac{\Gamma(m_2 + \frac{1}{2})}{\Gamma(m_2)} \left(\frac{\Omega_2}{m_2}\right)^{1/2}. \tag{15}$$

For variance, we use the relation $\sigma_G^2 = E[G_l^2] - E[G_l]^2$. So, the parameters $\mu_Y = N\mu_G$ and $\sigma_Y^2 = N\sigma_G^2$ can be found accordingly.

The results of our proposed optimized passive and active IRS-assisted schemes are compared with different benchmark schemes, i.e., random passive IRS, passive IRS with phase error, and without IRS. In the case of random passive IRS, the IRS phase shifts are randomly initialized irrespective of the phase shifts induced by the fading channel. The scheme of passive IRS with phase error is discussed in the following subsection.

C. Passive IRS with phase error

In this case, due to the complete lack of knowledge about the phases of h_l and g_l, they cannot be perfectly estimated. So, the deviation of ϕ_l from the ideal case can be modeled by the phase noise Θ_l, which is uniformly distributed from $[-\pi, \pi)$. Considering passive IRS, the received signal y_{Rp} in (1) is thus given as

$$y_{Rp} = \left(\sum_{l=1}^{N} |h_l||g_l|e^{j\Theta_l}\right)\sqrt{P_t}s + \zeta_R, \tag{16}$$

where $\Theta_l = \theta_{h_l} + \theta_{g_l} + \phi_l \neq 0$ but is uniformly distributed on $[-\pi,\pi)$. It is assumed that different Θ_l ($l = 1, 2, ..., N$) are i.i.d. with common characteristic function stated as a sequence of complex numbers $\{\rho_D\}_{D\in Z}$ [41]

$$\rho_D = E[e^{jD\Theta_l}]. \tag{17}$$

Here, considering $b = E[|h_l|] = E[|g_l|]$, the N RVs $|h_l||g_l|e^{j\Theta_l}$, $l = 1, 2, ..., N$ are i.i.d. with common mean $\mu = b^2\rho_1$ and variance, $v = 1 - b^4\rho_1^2$ [42].

Now, for Θ_l as uniformly distributed, $\rho_1 = 0$ which implies $\mu = 0$ and $v = 1$. Thus, the channel coefficient $Y = \sum_{l=1}^{N} |h_l||g_l|e^{j\Theta_l}$ has complex normal distribution with $\mu_Y = 0$ and $v_Y = N$. This consequently means that the equivalent channel resembles the Rayleigh fading.

IV. Secrecy Performance Analysis

In this Section, we derive the secrecy capacity and SOP of the proposed passive and active IRS based schemes.

A. Secrecy Capacity

The secrecy capacity is defined as the difference between the channel capacity of the legitimate link and that of the eavesdropper link. It implies that with this capacity, the transmitter can send messages over the legitimate channel to the intended receiver without any interference from the eavesdroppers. For

multiple eavesdroppers' scenario with passive and active IRS (as considered in Figs. 2a and 2b), it is expressed as

$$C_s = log_2(1+\gamma_R) - max\Big(log_2(1+\gamma_{E_1}), log_2(1+\gamma_{E_2}), ..., log_2(1+\gamma_{E_n})\Big), \tag{18}$$

where n is the number of eavesdroppers. Based on existing literature [43]–[45] and to ensure guaranteed secure communication, we have analyzed the secrecy capacity in the worst-case scenario where the strongest (best) eavesdropper is considered. Here it should be noted that $\gamma_R = \gamma_{Rp}$, $\gamma_E = \gamma_{Ep}$ for the passive IRS and $\gamma_R = \gamma_{Ra}$, $\gamma_E = \gamma_{Ea}$ for the active IRS-assisted scenarios.

For the considered system in Fig. 2a with passive and using (2), the received SNR at the eavesdropper is given as

$$\gamma_{Ep} = \left|\sum_{l=1}^{N} h_l k_l e^{j\phi_l}\right|^2 \frac{P_t}{\sigma_E^2}. \tag{19}$$

For the considered system in Fig. 2b with active IRS, using (5) and keeping in mind equal amplification factor, i.e., $\alpha_l = \alpha$ for all active IRS elements (as discussed before), the received SNR at the eavesdropper is given as

$$\begin{aligned}\gamma_{Ea} &= \alpha^2 \left|\sum_{l=1}^{N} h_l k_l e^{j\phi_l}\right|^2 \frac{P_t}{\sigma_E^2 + ||\mathbf{k}^T\mathbf{\Phi}||^2\sigma_I^2}, \\ &= \alpha^2 \left|\sum_{l=1}^{N} h_l k_l e^{j\phi_l}\right|^2 \frac{P_t}{\sigma_3^2},\end{aligned} \tag{20}$$

where $\sigma_3^2 = \sigma_E^2 + ||\mathbf{k}^T\mathbf{\Phi}||^2\sigma_I^2$.

Now, for our proposed optimized passive and active IRS-assisted schemes with perfect phase estimation and following CLT, the RV $Z = \sum_{l=1}^{N} h_l k_l e^{j\phi_l}$ in (19) and (20) can be approximated as a complex Gaussian distributed RV. Further, it is a well-known fact that for a complex Gaussian RV Z, its squared magnitude $|Z|^2$ follows an exponential distribution. Consequently, γ_E (γ_{Ep} for passive IRS and γ_{Ea} for active IRS) becomes an exponential RV with PDF given as

$$f_{\gamma_E(x)} = \frac{1}{\lambda_E} e^{-x/\lambda_E}, \tag{21}$$

where λ_E is the distribution parameter. Here, for passive IRS-assisted case, $\lambda_E = \lambda_{E_p} = \frac{NP_t}{\sigma_E^2}$ and for active IRS-assisted case, $\lambda_E = \lambda_{E_a} = \frac{NP_t}{\sigma_3^2}$.

B. SOP

It quantifies the probability when a communication link fails to achieve the target secrecy rate, i.e., $C_S < C_{tr}$ where $C_{tr} > 0$ is the target secrecy rate. It can be expressed as [15]

$$\begin{aligned}SOP &= P(log_2(1+\gamma_R) - log_2(1+\gamma_E) < C_{tr}) \\ &= \int_0^{\infty} F_{\gamma_R}(\gamma_E\phi + \phi - 1) f_{\gamma_E}(\gamma_E) d\gamma_E,\end{aligned} \tag{22}$$

where $\phi = 2^{C_{tr}}$. Here, for passive IRS-assisted scenario, $\gamma_R = \gamma_{Rp}$ and $\gamma_E = \gamma_{Ep}$. For active IRS-assisted scenario, $\gamma_R = \gamma_{R_p}$ and $\gamma_E = \gamma_{Ep}$.

Denoting $\beta = \frac{\sqrt{P_t}}{\sigma_R}$ for passive IRS and $\beta = \frac{\sqrt{P_t}}{\sigma_2}$ for active IRS in (9) and (13) respectively and by knowing the fact that Y is a Gaussian distributed RV with mean $a = \mu_Y$ and variance $\sigma^2 = \sigma_Y^2$, the CDF of $Z = Y\beta$ can be expressed as

$$F_Z(z) = \int_0^{z/\beta} \frac{1}{\sqrt{2\pi\sigma^2}} e^{\frac{-(y-a)^2}{2\sigma^2}} dy. \tag{23}$$

Using the relation $erf(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-w^2} dw$ and performing some straightforward manipulations, i.e., $F_{\gamma_R}(z) = F_{Z^2}(z) = F_Z(\sqrt{z})$, the CDF of γ_R is given as

$$F_{\gamma_R}(z) = \frac{1}{2}\left[erf\left(\frac{a}{\sqrt{2\sigma^2}}\right) + erf\left(\frac{\frac{\sqrt{z}}{\beta} - a}{\sqrt{2\sigma^2}}\right)\right]. \tag{24}$$

This expression can be simplified by using the approximation [15]

$$erf(u) = 1 - erfc(u) \approx 1 - \sum_{\psi=1}^{3} p_\psi e^{-q_\psi u^2}, \tag{25}$$

where $p_\psi = [1/6 \quad 1/3 \quad 1/3]$ and $q_\psi = [1 \quad 4 \quad 4/3]$.

Substituting (21) and (24) in (22), we get

$$SOP = \frac{1}{2\lambda_E}\int_0^{\infty} e^{\frac{-\gamma_E}{\lambda_E}} \left[erf\left(\frac{\frac{\sqrt{\gamma_E\phi+\phi-1}}{\beta} - a}{\sqrt{2\sigma^2}}\right) + erf\left(\frac{a}{\sqrt{2\sigma^2}}\right)\right] d\gamma_E. \tag{26}$$

By assuming $w = \sqrt{\gamma_E\phi + \phi - 1}$, it can be rewritten as

$$\begin{aligned}SOP &= \\ &\frac{e^{\frac{\theta-1}{\lambda_E\theta}}}{\lambda_E\theta}\int_{\sqrt{\theta-1}}^{\infty} e^{\frac{-w^2}{\lambda_E\theta}}\left[erf\left(\frac{w-\beta a}{\beta\sqrt{2\sigma^2}}\right) + erf\left(\frac{a}{\sqrt{2\sigma^2}}\right)\right] w dw \\ &= \frac{e^{\frac{\theta-1}{\lambda_E\theta}}}{\lambda_E\theta} I.\end{aligned} \tag{27}$$

Using (25), I can be simplified as

$$\begin{aligned}I = &\left[\int_{\sqrt{\theta-1}}^{\beta a} e^{\frac{-w^2}{\lambda_E\theta}}\left(-1 + erf\left(\frac{a}{\sqrt{2\sigma^2}}\right)\right) w dw + \right. \\ &\int_{\beta a}^{\infty} e^{\frac{-w^2}{\lambda_E\theta}}\left(erf\left(\frac{a}{\sqrt{2\sigma^2}}\right) + 1\right) w dw + \\ &\int_{\sqrt{\theta-1}}^{\beta a} e^{\frac{-w^2}{\lambda_E\theta}} \sum_{\psi=1}^{3} p_\psi e^{-q_\psi\left(\frac{a-\frac{w}{\beta}}{\sqrt{2\sigma^2}}\right)^2} w dw - \\ &\left.\int_{\beta a}^{\infty} e^{\frac{-w^2}{\lambda_E\theta}} \sum_{\psi=1}^{3} p_\psi e^{-q_\psi\left(\frac{\frac{w}{\beta}-a}{\sqrt{2\sigma^2}}\right)^2} w dw\right] \\ &= Q_1 + Q_2 + Q_3 - Q_4.\end{aligned} \tag{28}$$

Now, further doing some simplifications, Q_i , $i \in (1,2,3,4)$ in (28) can be written as

$$\begin{aligned}Q_1 = \frac{\lambda_E\theta}{2}\Big[&e^{\frac{-(\theta-1)}{\lambda_E\theta}} erf\left(\frac{a}{\sqrt{2\sigma^2}}\right) - e^{\frac{-(\theta-1)}{\lambda_E\theta}} - \\ &e^{\frac{-(\beta^2a^2)}{\lambda_E\theta}} erf\left(\frac{a}{\sqrt{2\sigma^2}}\right) + e^{\frac{-(\beta^2a^2)}{\lambda_E\theta}}\Big],\end{aligned} \tag{29}$$

TABLE II
COMPARISON OF PROPOSED WORK WITH EXISTING WORK IN LITERATURE

	System Model		Secrecy Parameters		Different performance parameters			
Ref.	LoS	NLoS	Secrecy capacity	SOP	Number of eavesdroppers	Number of IRS reflecting elements (N)	Shape parameter (m)	Target secrecy rate (C_{tr})
[1]	×	✓	×	✓	×	✓	✓	×
[28]	✓	✓	×	✓	×	✓	✓	×
[29]	×	✓	×	✓	×	✓	✓	×
[30]	×	✓	✓	×	×	✓	×	×
[31]	×	✓	✓	✓	×	✓	×	×
Proposed work	×	✓	✓	✓	✓	✓	✓	✓

$$Q_2 = \frac{\lambda_E \theta}{2}\left[e^{\frac{-\beta^2 a^2}{\lambda_E \theta}} erf\left(\frac{a}{\sqrt{2\sigma^2}}\right) + e^{\frac{-\beta^2 a^2}{\lambda_E \theta}}\right], \quad (30)$$

$$Q_3 = \sum_{\psi=1}^{3} p_\psi \left[\frac{e^{-r_w} e^{-2o_w\sqrt{\theta-1}} e^{-t_w(\theta-1)}}{2m_w} - \frac{e^{-r_w} e^{-2o_w\beta a} e^{-t_w\beta^2 a^2}}{2m_w} + \frac{o_w\sqrt{\pi} e^{\left(\frac{o_w^2 - t_w r_w}{t_w}\right)}}{2t_w\sqrt{t_w}} erf\left(\frac{o_w + t_w\sqrt{\theta-1}}{\sqrt{t_w}}\right) - \frac{o_w\sqrt{\pi} e^{\left(\frac{o_w^2 - t_w r_w}{t_w}\right)}}{2t_w\sqrt{t_w}} erf\left(\frac{o_w + t_w\beta a}{\sqrt{t_w}}\right)\right], \quad (31)$$

where $t_w = \frac{1}{\lambda_E \theta} + \frac{q_n}{2\beta^2\sigma^2}$, $o_w = \frac{-q_n a}{2\beta\sigma^2}$ and $r_w = \frac{q_n a^2}{2\sigma^2}$.

$$Q_4 = \sum_{\psi=1}^{3} p_\psi \left[\frac{e^{-r_w} e^{-2\beta a o_w} e^{-t_w\beta^2 a^2}}{2t_w} - \frac{o_w\sqrt{\pi} e^{\frac{o_w^2 - t_w r_w}{t_w}}}{2t_w\sqrt{t_w}} + \frac{o_w\sqrt{\pi} e^{\frac{o_w^2 - t_w r_w}{t_w}}}{2t_w\sqrt{t_w}} erf\left(\frac{o_w + t_w\beta a}{\sqrt{t_w}}\right)\right], \quad (32)$$

where t_w, o_w and r_w are same as above for Q_3. In the next section, we present the numerical results and confirm the accuracy of the presented analytical derivation of SOP by comparison of the simulation results with the analytical results.

V. SIMULATION RESULTS AND DISCUSSION

In this Section, numerical simulation results are presented to demonstrate the secrecy performance of the proposed optimized passive and active IRS-assisted schemes with perfect phase estimation. Table II shows the comparison of proposed work with the existing work based on the Nakagami-*m* fading to demonstrate the comprehensive analysis performed in the proposed solution. The comparison is done in terms of system model, different secrecy parameters like secrecy capacity and SOP, and different performance parameters like number of IRS reflecting elements (N), number of eavesdroppers, Nakagami shape parameter (m), and target secrecy rate (C_{tr}). It can be clearly seen from this table that the proposed work gives a more comprehensive analysis as compared to the existing work by considering the detailed impact of different performance parameters on the secrecy performance. Considering active IRS-assisted system over Nakagami-m fading channel, no work has been reported so far in terms of its secrecy analysis.

The simulation results are presented for different secrecy parameters like secrecy capacity and SOP. The accuracy of the analytical expressions for SOP is confirmed by comparison of the analytical and simulation results. The performance of the proposed optimized passive and active IRS schemes with perfect phase estimation are compared with three different benchmark schemes: (a) random passive IRS, where the IRS elements have random phases irrespective of the channel coefficients, (b) passive IRS with phase error, where the phase values of IRS reflecting elements are not perfectly tuned with the phases of channel fading coefficients, and (c) no IRS, which is the case without IRS. The simulation parameters considered in results are shown in Table III.

TABLE III
SIMULATION PARAMETERS

Parameters	Value
N	6
No. of eavesdroppers	3
Amplification factor (α)	20 dB
SNR	-30 to 30 dB
m_d ($d \in [h_l, g_l, k_l]$)	2
Ω_d ($d \in [h_l, g_l, k_l]$)	1
Target secrecy rate (C_{tr})	0.3
Fading distribution	Nakagami-m

Considering single eavesdropper scenario and the different simulation parameters mentioned in Table III, Fig. 3 shows the secrecy capacity versus SNR for the proposed schemes and the results are compared with different benchmark schemes. Secrecy capacity signifies the security rate at which the legitimate user can transmit the data without any information leakage to the eavesdropper. It can be observed from Fig. 3 that both proposed optimized schemes based on passive and active IRS with perfect phase estimation outperform the different considered benchmark schemes. This is because IRS with perfect phase estimation combats the effects of channel fading coefficients for the legitimate link. This results into constructive addition at the desired receiver and destructive addition at the eavesdropper. Further a significant difference

can be observed in between the secrecy performance of the proposed schemes with perfect phase estimation and that of the IRS (passive) having uniform error in phase estimation.

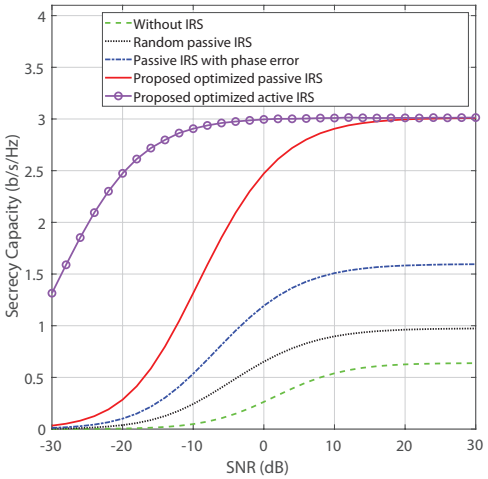


Fig. 3. Secrecy capacity versus SNR for different schemes with single eavesdropper and $N = 6$

On comparing proposed optimized passive and active IRS based solutions, it is observed that the solution based on active IRS provides better secrecy performance than that of the passive IRS based solution. This is because active IRS not only reflects but also amplifies the received signal from the BS before forwarding it to the end user. Specially, active IRS based solution is observed to provide a significant performance improvement at low SNR values while showing saturation effect at higher SNR. This saturation behavior at higher SNR values can be attributed to the asymptotic behavior of secrecy rate where secrecy capacity approaches a limit on increasing the SNR and any further increase in SNR shows negligible gain. This consequently leads to similar secrecy capacity for both passive and active IRS based solutions.

Considering scenario of single eavesdropper with same simulation parameters as used in Fig. 3, Fig. 4 shows the effect of varying the number of IRS reflecting elements (N) on the secrecy performance of the proposed optimized schemes. It can be seen that for both schemes, the secrecy capacity improves on increasing the number of reflecting elements. This performance enhancement is attributed to the fact that a larger N increases the received SNR at the desired receiver and that consequently results into increased secrecy capacity. In addition, the active IRS based solution is shown to perform better than the passive IRS based solution because of the signal amplification capability of active IRS. Moreover, the same secrecy capacity at higher SNR for any value of N is again due to the asymptotic behavior of secrecy rate.

Fig. 5 shows the dependency of secrecy capacity on the number of eavesdroppers with other simulation parameters as mentioned in Table III. It is observed that the secrecy capacity for both proposed optimized passive and active IRS based schemes reduces on increasing the number of eavesdroppers. This is because of the larger information leakage with increase in the number of eavesdroppers. This means that the information intended for the legitimate user is now received by

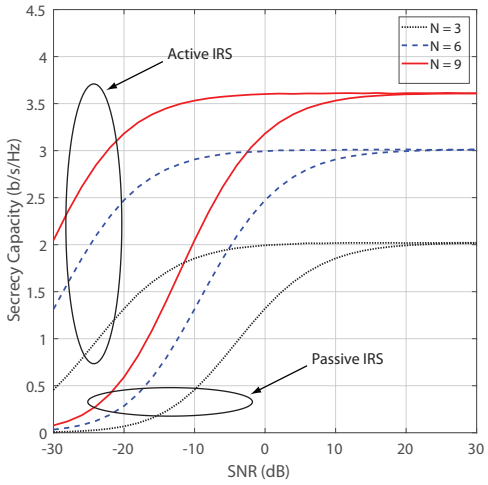


Fig. 4. Secrecy capacity versus SNR for proposed optimized passive and active IRS for different values of N

more eavesdroppers and that results into reduction in secrecy capacity. Here, considering the information leakage threat by multiple eavesdroppers, it is remarkable to note the higher performance gain achieved by active IRS because of the signal amplification.

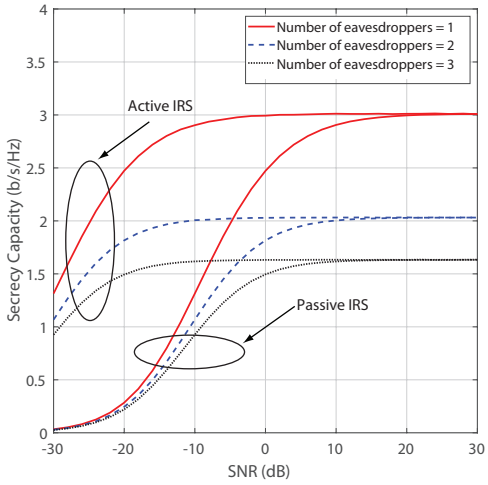


Fig. 5. Secrecy capacity versus SNR for proposed optimized passive and active IRS for different number of eavesdroppers with $N = 6$

With same simulation parameters, Fig. 6 shows the effect of varying the Nakagami shape parameter m on the secrecy capacity for single eavesdropper scenario. Furthermore, keeping the significance of shape parameter in mind, Fig. 7 plots the secrecy capacity versus shape parameter for a particular value of SNR ($0\ dB$). It can be observed from these two Figs. that the secrecy capacity increases with the increase in value of m. This is due to the fact that with higher values of m, the severity of fading conditions reduces and that results into improved signal strength at the legitimate user. It should be noted that this shape parameter m relates the amplitudes of strong and weak components in the wireless medium, and depending on its value, Nakagami distribution can reduce to different fading distributions. As a special case, for the considered

values $m = 0.5$ and $m = 1$, Nakagami-m distribution reduces to unilateral Gauss distribution and familiar Rayleigh fading distribution respectively. Moreover, from both Figs., it can be observed that the proposed active IRS based solution provides better secrecy performance than that of using the passive IRS. This is due to the amplification capability of active IRS.

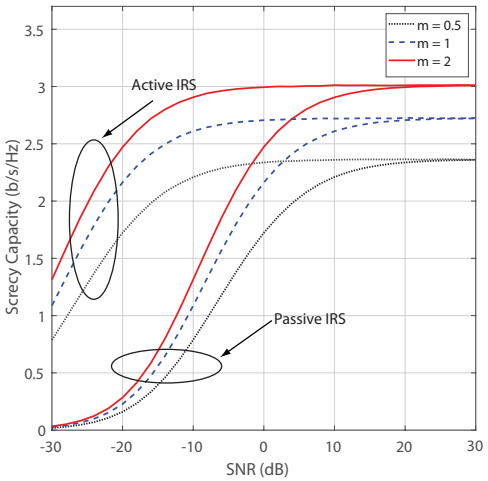


Fig. 6. Secrecy capacity versus SNR for proposed optimized passive and active IRS for different values of Nakagami shape parameter m with $N = 6$

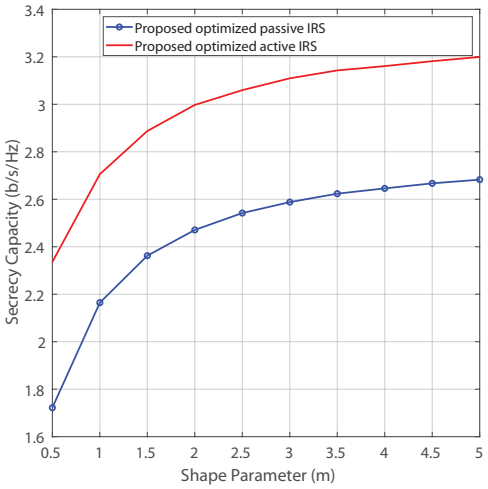


Fig. 7. Secrecy capacity versus Nakagami shape parameter m for proposed optimized passive and active IRS with $N = 6$

Now in the context of SOP performance, Fig. 8 shows the SOP for the proposed schemes and compares the result with different benchmark schemes. First, the exact match between the simulation and analytical results confirms the accuracy of the proposed analytical expression for SOP. Second, it can be observed that the proposed methods outperform the different benchmark schemes and shows the best SOP performance. This is because both proposed optimized passive and active IRS-assisted schemes with perfect phase estimation mitigate the effects of channel fading coefficients and thus result into constructive addition at the desired receiver. This increases the received SNR at the legitimate user and consequently improves the SOP of the system.

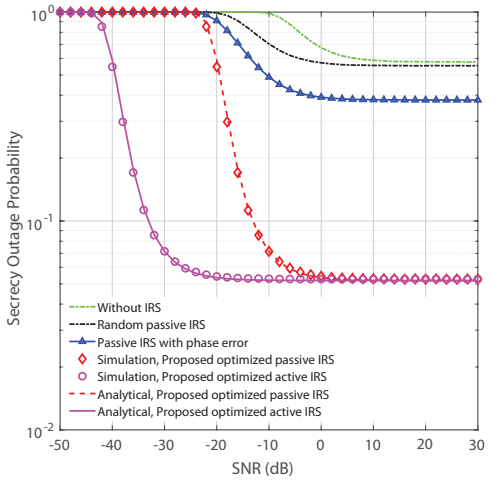


Fig. 8. SOP versus SNR for different schemes with single eavesdropper and $N = 6$

TABLE IV
PERFORMANCE COMPARISON OF PROPOSED WORK WITH BENCHMARK SCHEMES

Secrecy Parameters	Without IRS	Random passive IRS	Passive IRS with phase error	Proposed optimized passive IRS	Proposed optimized active IRS
Secrecy capacity $(b/s/Hz)$	0.048	0.242	0.536	1.315	2.906
SOP	0.987	0.704	0.488	0.071	0.053

Further, while comparing the proposed passive and active IRS based solutions, it is observed that the solution based on active IRS provides better SOP performance than that of the passive IRS based solution. This is due to the same reason as mentioned before for secrecy capacity where active IRS can not only reflect but also amplify the received signal from the BS before transmitting it towards the end user.

Considering secrecy performance at a particular value of SNR (-10 dB), Table IV compares the proposed approach with considered benchmark schemes in terms of secrecy capacity and SOP. It can be clearly seen from this table that the proposed schemes outperform the considered benchmark schemes and provides the best secrecy performance.

Next, to analyze the impact of IRS reflecting elements (N) on SOP, Figs. 9 and 10 show the dependency of SOP on varying the value of N for both proposed passive and active IRS based solutions. Here also, the exact match between the analytical and simulation results confirms the accuracy of the derived expression for SOP. Further, it is observed that the SOP performance for both schemes improves with increase in value of N since with higher value of N, more transmitter information, which is blocked by obstacles, can be efficiently reflected towards the desired receiver. This results in an increase in the received SNR at the legitimate user, thus improving the SOP.

Figs. 11 and 12 show the SOP variation with changing the Nakagami shape parameter m for both proposed schemes.

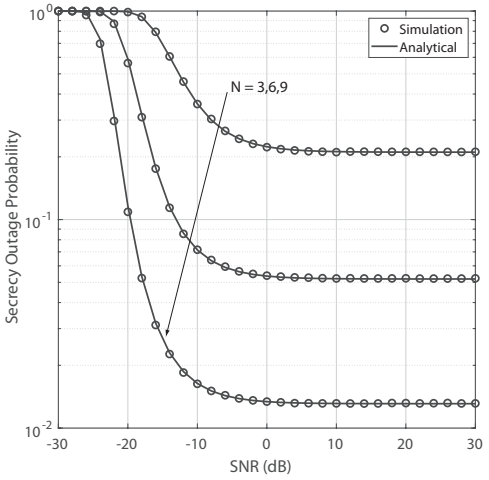


Fig. 9. SOP versus SNR for different values of N for the proposed optimized passive IRS-assisted system

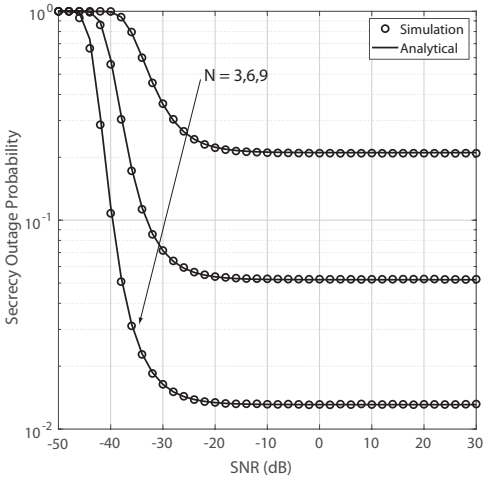


Fig. 10. SOP versus SNR for different values of N for the proposed optimized active IRS based system

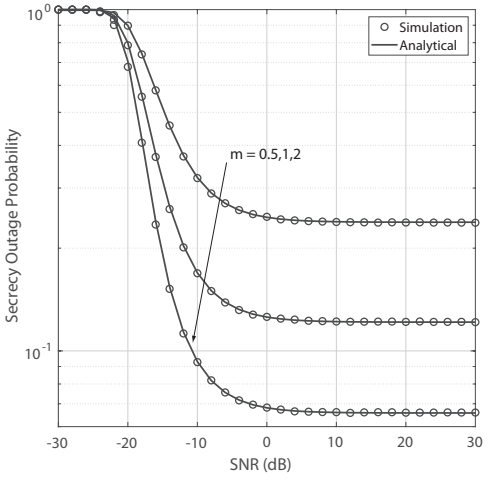


Fig. 11. SOP versus SNR for different values of m for the proposed optimized passive IRS based system

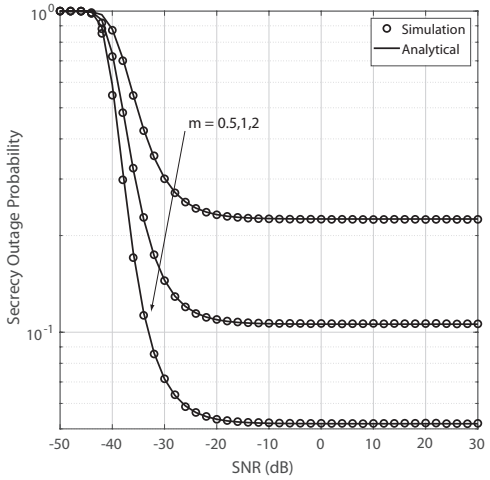


Fig. 12. SOP versus SNR for different values of m for the proposed optimized active IRS-based system

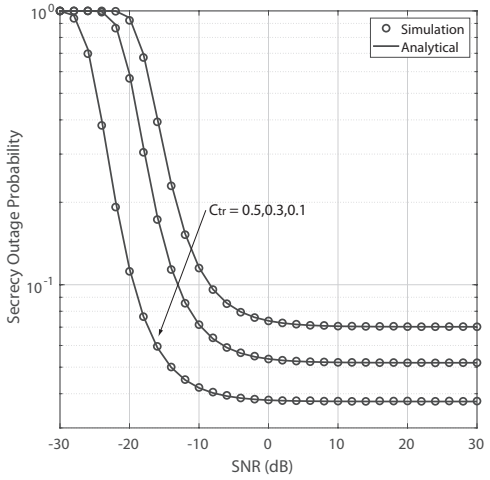


Fig. 13. SOP versus SNR for different values of C_{tr} for passive IRS based system

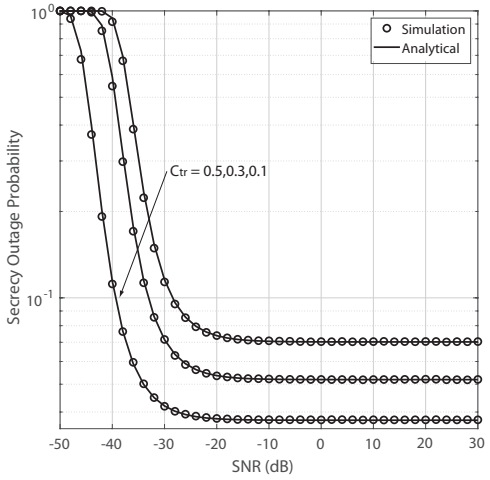


Fig. 14. SOP versus SNR for different values of C_{tr} for active IRS based system

It can be observed that the SOP performance improves on increasing the value of this parameter. This is attributed to the fact that higher value of m reduces the fading effect

and consequently improves the legitimate signal strength. This further results into improved SOP performance.

Figs. 13 and 14 show the effect of changing the target secrecy rate C_{tr} on the SOP performance for the proposed solutions. It should be noted that this parameter measures the maximum rate at which information can be transmitted successfully over the legitimate link without any leakage towards the eavesdropper. It can be seen from these figures that the SOP performance of the system improves on decreasing the target secrecy rate.

Summarizing, the proposed solution is observed to outperform the different benchmark schemes for analyzing the secrecy performance of wireless communication in Nakagami fading scenario with single and multiple eavesdroppers.

VI. Conclusion

In this paper, passive and active IRS-assisted novel schemes with perfect phase estimation have been proposed for analyzing the secrecy performance of wireless communication system in Nakagami fading scenario. The secrecy performance of the passive and active IRS-assisted schemes is evaluated in terms of different parameters like secrecy capacity and SOP. The numerical results for the proposed schemes are compared with different benchmarks schemes like random passive IRS, passive IRS with phase error, and without IRS. Considering single and multiple eavesdropper scenarios, it has been observed that the proposed schemes provide the best secrecy capacity in comparison to that provided by other benchmark schemes. In the context of SOP performance, analytical expression is provided for SOP and the accuracy of that is confirmed by comparison of the analytical results with the simulation results. Further, the SOP performance of the proposed schemes is observed to be better than that of the different benchmark schemes. In addition, the effect of different performance parameters such as the number of IRS reflecting elements, number of eavesdroppers, Nakagami shape parameter, and target secrecy rate on secrecy performance is analyzed in a comprehensive way.

References

[1] A. K. Yadav, S. Yadav, A. Pandey, and A. Silva, "On the secrecy performance of RIS-enabled wireless communications over Nakagami-m fading channels," *ICT Exp.*, vol. 9, no. 3, pp. 452–458, 2023, https://doi.org/10.1016/j.icte.2022.04.003.

[2] D. T. Uysal, P. D. Yoo, and K. Taha, "Data-driven malware detection for 6G networks: A survey from the perspective of continuous learning and explainability via visualisation," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 61–71, 2023, https://doi.org/10.1109/OJVT.2022.3219898.

[3] R. Kaur, B. Bansal, S. Majhi, S. Jain, C. Huang, and C. Yuen, "A survey on reconfigurable intelligent surface for physical layer security of next-generation wireless communications," *IEEE Open J. Veh. Technol.*, vol. 5, pp. 172–199, 2024, https://doi.org/10.1109/OJVT.2023.3348658.

[4] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, 2018, https://doi.org/10.1109/JSAC.2018.2825560.

[5] A. Khan, S. A. H. Mohsan, A. Elfikky, A. I. Boghdady, S. Ahmad, and N. Innab, "A survey of intelligent reflecting surfaces: Performance analysis, extensions, potential challenges, and open research issues," *Veh. Commun.*, p. 100859, 2024, https://doi.org/10.1016/j.vehcom.2024.100859.

[6] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2283–2314, 2020, https://doi.org/10.1109/COMST.2020.3004197.

[7] Z. Zhang, L. Dai, X. Chen, C. Liu, F. Yang, R. Schober, and H. V. Poor, "Active RIS vs. passive RIS: Which will prevail in 6G?" *IEEE Trans. Commun.*, vol. 71, no. 3, pp. 1707–1725, 2023, https://doi.org/10.1109/TCOMM.2022.3231893.

[8] A. Khan, S. A. H. Mohsan, A. Elfikky, A. I. Boghdady, S. Ahmad, and N. Innab, "A survey of intelligent reflecting surfaces: Performance analysis, extensions, potential challenges, and open research issues," *Veh. Commun.*, vol. 51, p. 100859, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209624001347

[9] I. Hameed and I. Koo, "Enhancing throughput in IoT networks: The impact of active RIS on wireless powered communication systems," *Electronics*, vol. 13, no. 7, p. 1402, 2024, https://doi.org/10.3390/electronics13071402.

[10] D. Selimis, K. P. Peppas, G. C. Alexandropoulos, and F. I. Lazarakis, "On the performance analysis of RIS-empowered communications over Nakagami-m fading," *IEEE Commun. Lett.*, vol. 25, no. 7, pp. 2191–2195, 2021, https://doi.org/10.1109/LCOMM.2021.3073981.

[11] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, 2019, https://doi.org/10.1109/LWC.2019.2919685.

[12] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *2019 IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6, https://doi.org/10.1109/GLOBECOM38437.2019.9014322.

[13] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent reflecting surface: A programmable wireless environment for physical layer security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019, https://doi.org/10.1109/ACCESS.2019.2924034.

[14] T. Zhifa, Z. Jianhua *et al.*, "Performance analysis of covert communication in IRS-assisted NOMA networks," *Scientia Sinica Informationis*, vol. 54, no. 6, pp. 1502–1515, 2024, https://doi.org/10.1360/SSI-2023-0174.

[15] L. Yang, J. Yang, W. Xie, M. O. Hasna, T. Tsiftsis, and M. D. Renzo, "Secrecy performance analysis of RIS-aided wireless communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 12 296–12 300, 2020, https://doi.org/10.1109/TVT.2020.3007521.

[16] L. Dong, H.-M. Wang, and J. Bai, "Active reconfigurable intelligent surface aided secure transmission," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 2181–2186, 2022, https://doi.org/10.1109/TVT.2021.3135498.

[17] Z. Liu, J. Wang, H. Jiang, J. Wang, X. Li, and W. Xie, "Physical layer security performance analysis of IRS-aided cognitive radio networks," *Electronics*, vol. 12, no. 12, p. 2615, 2023, https://doi.org/10.3390/electronics12122615.

[18] E. N. Egashira, D. P. M. Osorio, N. T. Nguyen, and M. Juntti, "Secure mmwave MIMO networks employing hybrid active-passive RIS," *IEEE Trans. Commun.*, pp. 1–1, 2024, https://doi.org/10.1109/TCOMM.2024.3490495.

[19] A. Nutchanat, K. Woradit, and P. Champrasert, "Secured wireless communications using multiple active and passive intelligent reflecting surfaces," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 1763–1779, 2025, https://doi.org/10.1109/OJCOMS.2025.3544870.

[20] N. Beaulieu and C. Cheng, "Efficient Nakagami-m fading channel simulation," *IEEE Trans. Veh. Technol.*, vol. 54, no. 2, pp. 413–424, 2005, https://doi.org/10.1109/TVT.2004.841555.

[21] K. Peppas, H. Nistazakis, and G. Tombras, "An overview of the physical insight and the various performance metrics of fading channels in wireless communication systems," *Adv. trends wireless commun.*, vol. 13, pp. 1–22, 2011, https://doi.org/10.5772/15028.

[22] D. Selimis, K. P. Peppas, G. C. Alexandropoulos, and F. I. Lazarakis, "On the performance analysis of RIS-empowered communications over Nakagami-m fading," *IEEE Commun. Lett.*, vol. 25, no. 7, pp. 2191–2195, 2021, https://doi.org/10.1109/LCOMM.2021.3073981.

[23] A. Al-Rimawi, A. Al-Dweik, and A. A. Siddig, "Capacity analysis of adaptive IRS-aided transmission with direct link in Nakagami-m fading channels," *IEEE Trans. Cogn. Commun. Netw.*, vol. 10, no. 3, pp. 920–937, 2024, https://doi.org/10.1109/TCCN.2023.3342417.

[24] S. Li, S. Yan, L. Bariah, S. Muhaidat, and A. Wang, "IRS-assisted full duplex systems over rician and Nakagami fading channels," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 217–229, 2023, https://doi.org/10.1109/OJVT.2022.3233857.

[25] A. P. Ajayan, S. P. Dash, and B. Ramkumar, "Approximate composite channel statistics and performance analysis of IRS-aided wireless system under Nakagami-m fading," *IEEE Access*, vol. 11, pp. 102 290–102 300, 2023, https://doi.org/10.1109/ACCESS.2023.3317277.

[26] R. Rajesh and A. Bagubali, "Performance analysis of reflective intelligent surface assisted bidirectional full-duplex communication systems over Nakagami-m fading channels," *Int. J. Commun. Syst.*, p. e6058, 2024, https://doi.org/10.1002/dac.6058.

[27] M. Jana and S. Kumar, "Performance analysis of IRS-assist dual-hop wireless communication system," *Physical Commun.*, vol. 68, p. 102550, 2025, https://doi.org/10.1016/j.phycom.2024.102550.

[28] R. C. Ferreira, M. S. Facina, F. A. de Figueiredo, G. Fraidenraich, and E. R. de Lima, "Secrecy analysis and error probability of LIS-aided communication systems under Nakagami-m fading," *Entropy*, vol. 23, no. 10, p. 1284, 2021, https://doi.org/10.3390/e23101284.

[29] X. Li, Y. Zheng, M. Zeng, Y. Liu, and O. A. Dobre, "Enhancing secrecy performance for STAR-RIS NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 2684–2688, 2023, https://doi.org/10.1109/TVT.2022.3213334.

[30] N. Mensi, D. B. Rawat, and E. Balti, "Physical layer security for V2I communications: Reflecting surfaces vs. relaying," in *2021 IEEE Global Commun. Conf. (GLOBECOM)*, 2021, pp. 01–06, https://doi.org/10.1109/GLOBECOM46510.2021.9685258.

[31] K. M. Hamza, S. Basharat, H. Jung, M. Gidlund, and S. A. Hassan, "Secrecy analysis of RIS-assisted uplink NOMA systems under Nakagami-m fading," in *2024 IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2024, pp. 1511–1516, https://doi.org/10.1109/ICCWorkshops59551.2024.10615519.

[32] X. Yue, M. Song, C. Ouyang, Y. Liu, T. Li, and T. Hou, "Exploiting active RIS in NOMA networks with hardware impairments," *IEEE Trans. Veh. Technol.*, vol. 73, no. 6, pp. 8207–8221, 2024, https://doi.org/10.1109/TVT.2024.3352813.

[33] C. Gong, H. Li, S. Hao, K. Long, and X. Dai, "Active RIS enabled secure NOMA communications with discrete phase shifting," *IEEE Trans. Wireless Commun.*, vol. 23, no. 4, pp. 3493–3506, 2024, https://doi.org/10.1109/TWC.2023.3309006.

[34] Y. Li, C. You, and Y. J. Chun, "Active-IRS aided wireless network: System modeling and performance analysis," *IEEE Commun. Lett.*, vol. 27, no. 2, pp. 487–491, 2023, https://doi.org/10.1109/LCOMM.2022.3221116.

[35] M. Song, X. Yue, C. Ouyang, Y. Liu, T. Li, and T. Hou, "Outage performance of active RIS in NOMA networks over nakagami-m fading channels," in *2023 IEEE 98th Veh. Technol. Conf. (VTC2023-Fall)*, 2023, pp. 1–6, https://doi.org/10.1109/VTC2023-Fall60731.2023.10333805.

[36] K.-T. Nguyen, T.-H. Vu, H. Shin, and S. Kim, "Performance analysis of active RIS and passive RIS-aided MISO systems over nakagami-m fading channel with imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 74, no. 3, pp. 4334–4348, 2025, https://doi.org/10.1109/TVT.2024.3491501.

[37] E. Basar, "Transmission through large intelligent surfaces: A new frontier in wireless communications," in *2019 European Conf. Netw. Commun. (EuCNC)*, 2019, pp. 112–117, https://doi.org//10.1109/EuCNC.2019.8801961.

[38] D. L. Galappaththige, A. Devkota, and G. Amarasuriya, "On the performance of IRS-assisted relay systems," in *2021 IEEE Global Commun. Conf. (GLOBECOM)*, 2021, pp. 01–06, https://doi.org/10.1109/GLOBECOM46510.2021.9685500.

[39] Z. Kang, C. You, and R. Zhang, "Active-passive IRS aided wireless communication: New hybrid architecture and elements allocation optimization," *IEEE Trans. Wireless Commun.*, vol. 23, no. 4, pp. 3450–3464, 2024, https://doi.org/10.1109/TWC.2023.3308373.

[40] G. K. Karagiannidis, N. C. Sagias, and P. T. Mathiopoulos, "$n*$Nakagami: A novel stochastic model for cascaded fading channels," *IEEE Trans. Commun.*, vol. 55, no. 8, pp. 1453–1458, 2007, https://doi.org/10.1109/TCOMM.2007.902497.

[41] K. V. Mardia and P. E. Jupp, *Directional statistics*. John Wiley & Sons, 2009, https://doi.org/10.1002/9780470316979.

[42] B. Picinbono, "Second-order complex random vectors and normal distributions," *IEEE Trans. Signal Process.*, vol. 44, no. 10, pp. 2637–2640, 1996, https://doi.org/10.1109/78.539051.

[43] N. Nandan, S. Majhi, and H.-C. Wu, "Secure beamforming for MIMO-NOMA-based cognitive radio network," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1708–1711, 2018, https://doi.org/10.1109/LCOMM.2018.2841378.

[44] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *2009 Conf. Record Forty-Third Asilomar Conf. Signals, Syst. Comput.*, 2009, pp. 829–833, https://doi.org/10.1109/ACSSC.2009.5469979.

[45] W. Wang, K. C. Teh, and K. H. Li, "Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 505–515, 2017, https://doi.org/10.1109/TIFS.2016.2620279.

Ravneet Kaur received the M.Tech. degree in Digital Communication from the Department of Electronics and Communication Engineering, GGSIP University, New Delhi, in 2014. Her research interests include passive optical networks, wireless communication, physical layer security, RIS-assisted communication.

Bajrang Bansal (Member, IEEE) received the B.E. Degree in Electronics and Communication Engineering from Institute of Technology and Management, Gurugram, India in 2005, M.Tech. Degree in VLSI Design and CAD from the Thapar University, Punjab, India in 2008, and Ph.D. in Wireless Communication from Delhi Technological University, Delhi, India in 2017. Currently, he is an Assistant Professor at Jaypee Institute of Information Technology, Noida, India. His research interests include wireless channel modeling for UWB propagation, performance analysis of fading channels, physical layer security, RIS-assisted communication, and analysis of mm-wave propagation for 5G cellular networks.