# Exact Outage Analysis for Non-regenerative Secure Cooperation Against Double-tap Eavesdropping

Kotha Venugopalachary, *Student Member, IEEE*, Deepak Mishra, *Member, IEEE*, and Ravikant Saini *Member, IEEE*

***Abstract*—This paper presents the secrecy performance analysis of an amplify-and-forward relay-assisted cooperative communication system in the presence of a passive external eavesdropper. In contrast to existing works that assume high signal-to-noise ratio (SNR) approximations, we have investigated exact and secrecy outage probabilities. Furthermore, we consider a more challenging scenario where the source may not be reachable to the intended user directly. But the eavesdropper can tap both the source link and the relay link. First of all, the outage probability is analyzed at the intended user as well as the eavesdropper. Next, defining the secrecy rate for the amplify-and-forward (AF) relaying system, the expression of the secrecy outage probability (SOP) and the secrecy intercept probability (SIP) have been derived, respectively. Noticing the complexity involved in the integration of SOP and SIP expressions, the closed-form expressions have been derived for asymptotic cases. Finally, the exact and asymptotic analysis has been verified by performing Monte-Carlo simulations. It is observed that the relay position should be closer to the source compared to the eavesdropper to achieve improved SOP.**

***Index Terms*—amplify-and-forward, physical layer security, secrecy rate, cooperative systems, secrecy outage probability.**

## I. Introduction

Cooperative relaying in wireless communications has got extensive research interest as it helps in achieving fifth-generation (5G) objectives such as reliability, coverage area extension, and high data rate [1]–[6]. As the wireless channels are open in nature, the information transmission is prone to eavesdropping. With the enormous increase of online transactions and heterogeneity of connecting users, ensuring secrecy to the user's data is a challenging task. Securing information [7] from external eavesdroppers is a major concern for cooperative communication systems as well [1]. The physical layer security (PLS) has attracted the attention of researchers compared to the high-complex cryptography at higher levels (Application and Network) because it exploits the inherent characteristics of wireless channels [4], [8].

### A. Literature survey

Wireless PLS improvement using cooperative relaying schemes such as decode-and-forward (DF), amplify-and-forward (AF), randomize and forward (RF), and compress-and-forward (CF) have been investigated in [8]–[13]. Considering a jamming node, the PLS of cooperative NOMA in a severe scenario where there is no direct link from the source to far-destination while the direct link between the eavesdropper and source exists is investigated in [14]. Authors in [15] considered resource allocation in multi-carrier AF-relay systems under individual and sum power budget constraints to investigate the optimal secrecy rate. Authors in [16] have studied the analysis of secure beam forming and ergodic secrecy rate for AF relay networks and derived tight closed-form approximation for the ergodic secrecy rate for a large number of antennas. The secrecy outage probability (SOP) of relay and user (RU) selection in an AF system over Nakagami-m fading channels is discussed in [17], and provided the asymptotic SOP expressions for maximal ratio combining (MRC) and selection combining techniques.

### B. Motivation and Contributions

The DF relaying requires decoding capability at the relay node, which causes deployment costs. The cooperative jamming requires additional nodes and needs a generation of noise in the null space of the destination, causing more implementation and deployment costs. Whereas AF relaying simply amplifies the received signal using a power amplifier and retransmits, which is cost-effective and easy to deploy. Notifying the ease of deployment and the necessity of power-efficient low-cost implementation in the next-generation applications (like the internet of things (IoT) and their security), we are interested in studying the performance analysis of AF-relay assisted secure cooperative systems.

The secrecy performance analysis of AF systems with multiple relays and two hops under cochannel interference and correlated channels using optimal relay selection has been extensively investigated in [18], [19] without considering the dual-tapping of the eavesdropper. Considering full-duplex AF relaying, [20]–[22] have investigated the secrecy performance in terms of average secrecy rate and SOP. The PLS in AF relaying by considering direct links from the source to the destination and the eavesdropper has been investigated to a great extent [8], [23], [24]. Authors in [24] have considered the more general case of availability of direct links from source to both the destination and the eavesdropper and studied

K. Venugopalachary is with the Department of Electrical Engineering at the Shiv Nadar University, Uttar Pradesh 201314, India (E-mail: vk227@snu.edu.in).

D. Mishra is with the School of Electrical Engineering and Telecommunications (EET) at the University of New South Wales (UNSW) Sydney, NSW 2052, Australia (E-mail: d.mishra@unsw.edu.au).

R. Saini is with Department of Electrical Engineering at the IIT Jammu, Jammu (J&K) 181221, India (E-mail: ravikant.saini@iitjammu.ac.in).

This work was partially supported by the Faculty Funded Postdoctoral Research Fellowship support of EET School at UNSW Sydney.

Corresponding author: D. Mishra.

DOI: 10.36244/ICJ.2022.4.6

the PLS over mixed Rayleigh and double-Rayleigh fading channels. In this paper, they have considered the maximal ratio combining at both the destination and the eavesdropper to get the advantage of diversity. The assumption of a direct link only to the eavesdropper, not to the main user, gives a more practical situation to achieve secrecy where the eavesdropper can get diversity and maybe stronger than the intended user's channel. *To the best of our knowledge, a more challenging scenario of a two-hop AF secure cooperative system where the source may not be reachable to the intended user directly, but the eavesdropper can tap both the source link and the relay link has not been studied yet.* In this paper, we consider the aforementioned system model to investigate the performance in terms of exact outage probability, exact secrecy outage probability (SOP), and secrecy intercept probability (SIP). The contributions of the paper are briefly summarised as follows.

- Initially, the outage probability analysis is performed individually at the intended user and at the eavesdropper.
- Defining secrecy rate for AF-relaying system, the SOP and the SIP expressions are provided in the integral form.
- We provide the closed-form expressions for SOP and SIP for asymptotic analysis.
- Finally, we validate our analysis by performing Monte-carlo simulations.

The remainder of the paper is divided into the following sections: Section II describes the system model and transmission protocol. The outage probability analysis of the intended user and the eavesdropper is analyzed individually in Section III. Section IV provides the SOP and the SIP analysis. The asymptotic analysis of SOP and SIP are detailed in Section V. Finally, Section VI shows the simulation results.

## II. System Model

### A. Topology

Consider a four-node wireless cooperative system consisting a source $\mathcal{S}$, a relay $\mathcal{R}$, a user $\mathcal{U}$ and an external eavesdropper $\mathcal{E}$ where all nodes are equipped with a single antenna. As shown in Fig. 1, $\mathcal{S}$ located at the origin, $(x_s, y_s) = (0, 0)$ of a two dimensional (2D) $x$-$y$ plain, communicates with $\mathcal{U}$ located at $(x_d, y_d) = (d, 0)$ via $\mathcal{R}$. $\mathcal{E}$ is assumed to be located at $(x_e, y_e)$ which tries to overhear the transmission from $\mathcal{S}$ to $\mathcal{R}$ and $\mathcal{R}$ to $\mathcal{U}$. As an essential scenario to examine in order to ensure security, it is assumed a direct link from $\mathcal{S}$ to $\mathcal{E}$ only and not to $\mathcal{U}$ while considering $\mathcal{R}$-to-$\mathcal{E}$ and $\mathcal{R}$-to-$\mathcal{U}$ links. We also assume the $\mathcal{S}$-to-$\mathcal{E}$ distance is greater than $\mathcal{S}$-to-$\mathcal{R}$. With path loss exponent $\alpha$, the channels undergo large-scale fading.

### B. Transmission Protocol and Channel Model

In the considered half-duplex relaying system, the transmission takes place in two phases [25]. In the first phase, the information is transmitted from $\mathcal{S}$ to $\mathcal{R}$, and in the second phase, $\mathcal{R}$ retransmits to $\mathcal{U}$ by amplifying the received signal with an amplification factor of $\beta$. Due to the broadcast nature of the transmission, $\mathcal{E}$ can overhear the information in both phases. Assuming $P_s$ and $P_r$ as transmit powers at $\mathcal{S}$ and $\mathcal{R}$ respectively, the received signals $y_{1R}$ at $\mathcal{R}$ and $y_{1E}$ at $\mathcal{E}$ from $\mathcal{S}$ in first phase, and the received signals $y_{2\mathcal{U}}$ at $\mathcal{U}$ and $y_{2\mathcal{E}}$ at $\mathcal{E}$ from $\mathcal{R}$ in the second phase are:

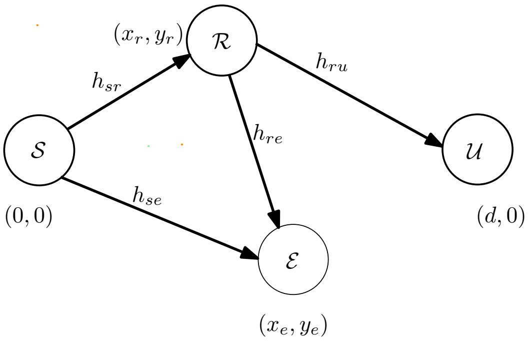


Fig. 1: Four-node AF secure cooperative system in 2D space.

$$y_{1\mathcal{R}} = h_{sr}\sqrt{P_s}x_1 + n_{1\mathcal{R}}, \quad y_{1\mathcal{E}} = h_{se}\sqrt{P_s}x_1 + n_{1\mathcal{E}}, \tag{1}$$

$$y_{2\mathcal{U}} = h_{ru}\sqrt{P_r}\beta x_1 + n_{2\mathcal{U}}, \; y_{2\mathcal{E}} = h_{re}\sqrt{P_r}\beta x_1 + n_{2\mathcal{E}}. \tag{2}$$

where $h_{sr}$, $h_{se}$, $h_{ru}$ and $h_{re}$ are the Rayleigh channel gain coefficients of $\mathcal{S}$-to-$\mathcal{R}$, $\mathcal{S}$-to-$\mathcal{E}$, $\mathcal{R}$-to-$\mathcal{U}$ and $\mathcal{R}$-to-$\mathcal{E}$ links respectively. $n_{1\mathcal{R}}$, $n_{1\mathcal{E}}$, $n_{2\mathcal{E}}$ $n_{2\mathcal{U}}$, represent mutually independent, Additive White Gaussian Noise (AWGN) with $N\left(0, \sigma^2\right)$ at $\mathcal{R}$, $\mathcal{E}$ in first and second phases and at $\mathcal{U}$ respectively. $x_1$ is unit power signal from $\mathcal{S}$ and $\beta = \frac{1}{\sqrt{P_s|h_{sr}|^2+\sigma^2}}$ is an amplification factor used at $\mathcal{R}$. At the eavesdropper, the signal received in two phases is combined using MRC.

## III. Individual Outage Probability Analysis

In this section, defining the rate, closed-form expressions for outage probability at the main user and eavesdropper are derived.

*1) Outage Analysis at the Intended User:* As per the transmission protocol, the amplified signal is transmitted to the main user. Then, the achievable rate at $\mathcal{U}$ is given as [26]

$$R_{\mathcal{U}} = \frac{1}{2}\log\left(1 + \frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr} + \gamma_{ru} + 1}\right), \tag{3}$$

where $\gamma_{sr}{=}\frac{P_s|h_{sr}|^2}{d_{sr}^{\alpha}}$, $\gamma_{ru}{=}\frac{P_r|h_{rd}|^2}{d_{ru}^{\alpha}}$ are the signal to noise ratios (SNRs) over $\mathcal{S}$-to-$\mathcal{R}$ and $\mathcal{R}$-to-$\mathcal{U}$ links, and are exponentially distributed with means $\mu_1 = \frac{p_s}{d_{sr}^{\alpha}}$ and $\mu_2 = \frac{p_r}{d_{ru}^{\alpha}}$, respectively. The ratio, $\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1} = \gamma_{sru}$ is the effective SNR at the $\mathcal{U}$ under the AF relaying and its distribution is used to investigate the outage probability. The outage occurs when the $R_{\mathcal{U}}$ at $\mathcal{U}$ is less than a threshold rate $r_u$ and its probability is called outage probability. The outage probability at the $\mathcal{U}$, $P_{out}^{\mathcal{U}}$ is

$$\begin{aligned}
P_{out}^{\mathcal{U}} &= \Pr\left(\frac{1}{2}\log_2\left(1 + \frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr} + \gamma_{ru} + 1}\right) \le r_u\right) \\
&\overset{\rho_u = 2^{2r_u}}{=} \Pr\left(1 + \frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr} + \gamma_{ru} + 1} \le \rho_u\right) \\
&= \Pr\left(\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr} + \gamma_{ru} + 1} \le \rho_u - 1\right) \\
&= F_{\gamma_{sru}}(\rho_u - 1),
\end{aligned} \tag{4}$$

where $F_{\gamma_{sru}}$ is the cumulative distribution function (CDF) of the random variable (RV) $\gamma_{sru} = \frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}$ which is a ratio of product of RVs ($\gamma_{sr}\gamma_{ru}$) and sum of RVs ($\gamma_{sr}+\gamma_{ru}$). The CDF of the RV $\gamma_{sru}$ is given as

$$F_{\gamma_{sru}}(\gamma) = 1 - 2\mathrm{e}^{-a_1\gamma}a_2\sqrt{\gamma(\gamma+1)}K_1(2a_2\sqrt{\gamma(\gamma+1)}),$$

where $a_1 = \mu_1 + \mu_2$ and $a_2 = \sqrt{\mu_1\mu_2}$.

*2) Outage Analysis at the Eavesdropper:* When it comes to the transmission protocol, the $\mathcal{E}$ gets the signal two times, and then it uses MRC to merge the two versions of the signal. The rate that can be achieved at $\mathcal{E}$ is represented as

$$R_{\mathcal{E}} = \frac{1}{2}\log\left(1+\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}\right), \tag{5}$$

where $\gamma_{se} = \frac{P_s|h_{se}|^2}{d_{se}^{\alpha}}$ and $\gamma_{re} = \frac{P_r|h_{re}|^2}{d_{re}^{\alpha}}$ are the SNRs over the links $\mathcal{S}$-to-$\mathcal{E}$ and $\mathcal{R}$-to-$\mathcal{E}$, and are exponentially distributed with means $\lambda_1 = \frac{p_s}{d_{se}^{\alpha}}$ and $\lambda_2 = \frac{p_r}{d_{ru}^{\alpha}}$ respectively. Due to two copies of the received signal at $\mathcal{E}$: one from the $\mathcal{R}$ and another (2) from the $\mathcal{S}$, the effective SNR at the $\mathcal{E}$ by employing the MRC is given as $W = \gamma_{se} + \frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}$. The outage occurs at $\mathcal{E}$ if the $R_{\mathcal{E}}$ is less than a threshold rate $r_e$. The outage probability at the $\mathcal{E}$, $P_{out}^{\mathcal{E}}$ is given as

$$\begin{aligned}
P_{out}^{\mathcal{E}} &= \Pr\left(\frac{1}{2}\log\left(1+\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}\right)\le r_e\right)\\
&\overset{\rho_e=2^{2r_e}}{=} \Pr\left(\left(\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}\right)\le \rho_e-1\right)\\
&= \Pr(X+Z\le\rho_e-1) = \Pr(W\le\rho_e-1)\\
&= F_W(\rho_e-1),
\end{aligned} \tag{6}$$

where $W = X+Z$, $X = \gamma_{se}$ and $Z = \frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}$ with its CDF $F_W(w)$. The CDF of $W$ is given as

$$\begin{aligned}
F_W(w) &= \int_{z=0}^{\infty}\int_{x=0}^{w-z} f_X(x)f_Z(z)d_xd_z\\
&= \int_{z=0}^{\infty} f_Z(z)F_X(w-z)d_z\\
&= \int_{z=0}^{\infty}[2\mathrm{e}^{-b_1z}[b_1b_2\sqrt{z(z+1)}K_1(2b_2\sqrt{z(z+1)})\\
&+ b_2^2(2z+1)K_0(2b_2\sqrt{z(z+1)})]](1-\mathrm{e}^{-\lambda_1(w-z)})dz\\
&= 1-2\mathrm{e}^{-\lambda_1 w}\int_{z=0}^{\infty}\mathrm{e}^{-(b_1-\lambda_1)z}\\
&\qquad \Big[b_1b_2\sqrt{z(z+1)}K_1(2b_2\sqrt{z(z+1)})\\
&\qquad + b_2^2(2z+1)K_0(2b_2\sqrt{z(z+1)})\Big]dz,
\end{aligned} \tag{7}$$

where $b_1 = \mu_1+\lambda_2$ and $b_2 = \sqrt{\mu_1\lambda_2}$.

Using the CDF of $W$, the $P_{out}^{\mathcal{E}}$ is given as

$$\begin{aligned}
P_{out}^{\mathcal{E}} &= 1-2\mathrm{e}^{-\lambda_1(\rho_e-1)}\int_{z=0}^{\infty}\mathrm{e}^{-(b_1-\lambda_1)z}\\
&\qquad \Big[b_1b_2\sqrt{z(z+1)}K_1(2b_2\sqrt{z(z+1)})\\
&\qquad + b_2^2(2z+1)K_0(2b_2\sqrt{z(z+1)})\Big]dz.
\end{aligned} \tag{8}$$

In the next section, by defining the secrecy rate for the considered AF relaying system where there is no direct link to the intended user while having a direct link along with the relay link to the eavesdropper, i.e., double tapping of an eavesdropper, we provide the detailed SOP analysis.

## IV. Secrecy Outage Probability Analysis

### A. Secrecy Rate Definition for Amplify-and-forward Relaying

The secrecy rate is the non-negative difference of the main and eavesdropper channels' rates, i.e. $R_s = [R_{\mathcal{U}} - R_{\mathcal{E}}]^+$. Hence, the secrecy rate for AF relaying is given as

$$R_s^{AF} = \left[\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}}{1+\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}}\right)\right]^+. \tag{9}$$

The secrecy rate equation in (9) is simplified by giving a proposition as (9) is more complicated to study the analyze.

*Proposition 1:* The upper bound of the secrecy rate (9) is

$$R_s^{AF} = \left[\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}}{1+\gamma_{se}+\gamma_{re}}\right)\right]^+. \tag{10}$$

*Proof:* For any positive values of $\gamma_{sr}$ and $\gamma_{re}$

$$\begin{aligned}
\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1} &\le \gamma_{sr}\\
\gamma_{sr}\gamma_{re} &\le (\gamma_{sr}+\gamma_{re}+1)\gamma_{sr}\\
0 &\le \gamma_{sr}(\gamma_{sr}+1).
\end{aligned} \tag{11}$$

Similarly, it can be observed that

$$\begin{aligned}
\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1} &\le \gamma_{re}\\
\gamma_{sr}\gamma_{re} &\le (\gamma_{sr}+\gamma_{re}+1)\gamma_{re}\\
0 &\le \gamma_{re}(\gamma_{re}+1).
\end{aligned} \tag{12}$$

Hence, $\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1} \le \min\{\gamma_{sr},\gamma_{re}\}$. As the relay location is assumed such that $d_{sr} < d_{re}$, $\gamma_{sr} > \gamma_{re}$. Hence, the maximum value of $\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}$ is equal to $\gamma_{re}$. ■

### B. Secrecy Outage Probability

The secrecy outage occurs when the $R_s^{AF}$ is less than a threshold rate $R_{th}$ and the corresponding probability is called secrecy outage probability (SOP). The SOP in AF relaying system is given as:

$$\begin{aligned}
P_{sop}^{AF} &= \Pr\left(R_s^{AF} < R_{th}\right)\\
&= \Pr\left(\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}}{1+\gamma_{se}+\gamma_{re}}\right) < R_{th}\right)\\
&\overset{\rho=2^{2R_{th}}}{=} \Pr\left(\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1} < \rho(\gamma_{se}+\gamma_{re})+(\rho-1)\right)\\
&= \Pr(W_1 - W_2 < \rho-1)\\
&= \Pr(W<\rho-1) = F_W(\rho-1)\\
&= \int_{-\infty}^{\infty}\left[\int_{-\infty}^{w_2+\rho-1} f_{W_1}(w_1)f_{\rho W_2}(w_2)dw_1\right]dw_2\\
&= \int_0^{\infty} f_{W_2}(w_2)F_{W_1}(w_2+\rho-1)dw_2,
\end{aligned} \tag{13}$$

where $W$ is the difference of two RVs $W_1 = \frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}$ and $W_2 = \rho(\gamma_{se}+\gamma_{re})$. $f_{W_2}$ is the PDF of $W_2$ and $F_{W_1}$, $F_W$ are the CDFs of $W_1$, $W$ respectively. The PDF $f_{W_2}$ and the CDF $F_{W_1}$ are obtained by using transformation of RVs [27], [28] :

$$f_{W_2} = \frac{\lambda_1\lambda_2}{|\rho|(\lambda_1-\lambda_2)}\left(\mathrm{e}^{-(\lambda_2 w_2/\rho)} - \mathrm{e}^{-(\lambda_1 w_2/\rho)}\right), \tag{14}$$

$$\begin{aligned} F_{W_1} &= 1 - 2\mathrm{e}^{-(\mu_1+\mu_2)w_1}\sqrt{\mu_1\mu_2 w_1(w_1+1)} \\ &\quad K_1\left(2\sqrt{\mu_1\mu_2 w_1(w_1+1)}\right). \end{aligned} \tag{15}$$

Hence, by substituting (15) in (13), we obtain $P_{sop}^{AF}$ as:

$$\begin{aligned} P_{sop}^{AF} = \int_0^\infty & \frac{\lambda_1\lambda_2}{|\rho|(\lambda_1-\lambda_2)}\left(\mathrm{e}^{-(\lambda_2 w_2/\rho)} - \mathrm{e}^{-(\lambda_1 w_2/\rho)}\right) \\ & \Big[1 - 2\mathrm{e}^{-(\mu_1+\mu_2)(w_2+\rho-1)} \\ & \sqrt{\mu_1\mu_2(w_2+\rho-1)(w_2+\rho)} \\ & K_1\left(2\sqrt{\mu_1\mu_2(w_2+\rho-1)(w_2+\rho)}\right)\Big] dw_2. \end{aligned} \tag{16}$$

### C. Secrecy Intercept Probability

The secrecy intercept probability (SIP) is defined as the probability at which the secrecy rate is less than zero. The corresponding mathematical expression of the SIP is given as

$$\begin{aligned} P_{sip}^{AF} &= \Pr\left(\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}}{1+\gamma_{se}+\gamma_{re}}\right) \le 0\right) \\ &= \Pr\left(\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1} \le (\gamma_{se}+\gamma_{re})\right) \\ &= \int_0^\infty \frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_2)}\left(\mathrm{e}^{-\lambda_2 w_2} - \mathrm{e}^{-\lambda_1 w_2}\right) \\ &\quad \Big[1 - 2\mathrm{e}^{-(\mu_1+\mu_2)w_2}\sqrt{\mu_1\mu_2 w_2(w_2+1)} \\ &\quad K_1\left(2\sqrt{\mu_1\mu_2 w_2(w_2+1)}\right)\Big] dw_2 \\ &= 1 - \frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_2)}\int_0^\infty 2\sqrt{\mu_1\mu_2 w_2(w_2+1)} \\ &\quad \left(\mathrm{e}^{-(\mu_1+\mu_2+\lambda_2)w_2} - \mathrm{e}^{-(\mu_1+\mu_2+\lambda_1)w_2}\right) \\ &\quad K_1\left(2\sqrt{\mu_1\mu_2 w_2(w_2+1)}\right) dw_2. \end{aligned} \tag{17}$$

Since the modified Bessel function contains complex parameters, the integration in (16) and (17) are intractable. The next section presents the SOP and SIP for asymptotic regimes.

## V. Asymptotic Secrecy Analysis Analysis

### A. The Approximated Secrecy Outage Probability

By assuming that the end-to-end SNR of main channel is very stronger than the effective SNR over the eavesdropper channel, i.e., $\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}} >> (\gamma_{se}+\gamma_{re})$, the SOP is given as

$$\begin{aligned} \tilde{P}_{sop}^{AF} &= \Pr\left(\frac{1}{2}\log\left(\frac{\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}}}{\gamma_{se}+\gamma_{re}}\right) < R_{th}\right) \\ &\overset{\rho=2^{2R_{th}}}{=} \Pr\left(\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}} < \rho(\gamma_{se}+\gamma_{re})\right) \\ &= \Pr\left(Z_1 - Z_2 < 0\right) = F_Z(0) \\ &= 1 - \frac{2\lambda_1\lambda_2\sqrt{\mu_1\mu_2}}{\rho(\lambda_1-\lambda_2)}\int_0^\infty z_2 K_1\left(z_2\, 2\sqrt{\mu_1\mu_2}\right) \\ &\quad \left(\mathrm{e}^{-(\mu_1+\mu_2+\frac{\lambda_2}{\rho})z_2} - \mathrm{e}^{-(\mu_1+\mu_2+\frac{\lambda_1}{\rho})z_2}\right) dz_2. \end{aligned} \tag{18}$$

The closed form expression for $\tilde{P}_{sop}^{AF}$ in (18) can be obtained as (19), where $F\left(.,.;.;.\right)$ is the Gauss hypergeometric function (Table of integrals series and products [29]). In (19), $A_1 = \frac{\mu_1+\mu_2}{2} + \frac{\lambda_2}{\rho}$, $A_2 = \frac{\mu_1+\mu_2}{2} + \frac{\lambda_1}{\rho}$, and $B = \sqrt{\mu_1\mu_2}$.

### B. Intercept probability for High SNR Regime

As the equation (17) involves the integration of a modified Bessel function of the second kind with difficult functional parameters, it is very difficult to obtain the closed-form expression for it. To relax the intractability of integration in (17), it is assumed that $\gamma_{sr} + \gamma_{ru} >> 1$. Hence, the secrecy rate equation in (10) reduces to the following equation

$$R_s^{AF} = \left[\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}}}{1+\gamma_{se}+\gamma_{re}}\right)\right]^+. \tag{20}$$

Now, the intercept probability is given as

$$\begin{aligned} \tilde{P}_{sip}^{AF} &= \Pr\left(\frac{1}{2}\log\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}}}{1+\gamma_{se}+\gamma_{re}}\right) < 0\right) \\ &= \Pr\left(\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}} < (\gamma_{se}+\gamma_{re})\right) \\ &= \Pr\left(Z_1 - Z_2 < 0\right) = F_Z(0) \\ &= 1 - \frac{\lambda_1\lambda_2\sqrt{\mu_1\mu_2}}{(\lambda_1-\lambda_2)}\int_0^\infty z_2 K_1\left(z_2\sqrt{\mu_1\mu_2}\right) \\ &\quad \left(\mathrm{e}^{-(\frac{\mu_1+\mu_2}{2}+\lambda_2)z_2} - \mathrm{e}^{-(\frac{\mu_1+\mu_2}{2}+\lambda_1)z_2}\right) dz_2. \end{aligned} \tag{21}$$

The closed form expression is same as that of (19), where $A_1 = \frac{\mu_1+\mu_2}{2} + \lambda_2$, $A_2 = \frac{\mu_1+\mu_2}{2} + \lambda_1$, and $B = \sqrt{\mu_1\mu_2}$.

## VI. Numerical results

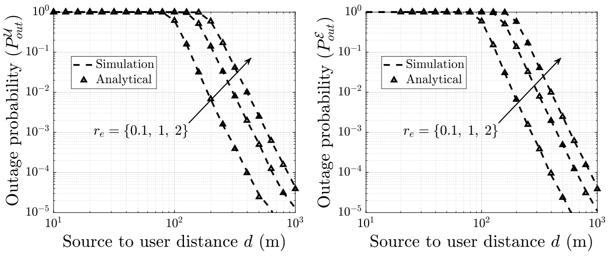
In this section, we validate the analytical expressions derived in Section III, Section IV and Section V. ***Default simulation parameters:*** Unless otherwise specified explicitly in figures, we set the default parameters that follow, the distance from source to the destination $d = 100$m, the total power $P_t = 40$dBm, the noise variance $\sigma^2 = -90$dBm and the path loss exponent $\alpha = 3$. The relay is located close to the source node with coordinates $(x_r,\ y_r) = (\frac{d}{10},\ \frac{d}{100})$ and the eavesdropper is located at $(x_e, y_e) = (\frac{d}{2},\ -2d)$ such that it is far from the source compared to the relay node. We perform $10^6$ channel realizations to show the simulation results.

### A. Validation of the Outage and Intercept Probability Analysis

In Fig. 2 (a) and Fig. 2 (b), we validate the outage analysis at the intended user and the eavesdropper respectively. Fig. 2 (a) shows the outage probability at the intended user derived in (4) and Fig. 2 (b) shows the outage probability at the intended user derived in (8), for different values of threshold rates $r_u = r_e = \{0.1,\ 1,\ 2\}$. It is observed from Fig. 2 that the outage probability improves with the reduction in threshold rates since the random nature of fading channel does not allow the channel to achieve significant rates.

Fig. 3 is plotted to show the validation of secrecy intercept probability. The intercept probability variation is drawn by changing the relay transmit power for different locations of eavesdropper such as $x_e = \frac{d}{2}$ and $y_e = \{\frac{x_e}{10}, x_e, 5x_e\}$. It is noted from the figure that the intercept probability increases as the distance between the eavesdropper and the source increase due to the leakage of information being more when the eavesdropper is closer to the source.

$$P_{so}^{AF} = 1 - \frac{64\lambda_1\lambda_2\mu_1\mu_2}{3(\lambda_1-\lambda_2)}\left[(A_1+B)^{-3} F\left(3, \frac{3}{2}; \frac{5}{2}; \frac{A_1-B}{A_1+B}\right) - (A_2+B)^{-3} F\left(3, \frac{3}{2}; \frac{5}{2}; \frac{A_2-B}{A_2+B}\right)\right]. \quad (19)$$



(a)

(b)

Fig. 2: The outage probability analysis with the variation of relay position.

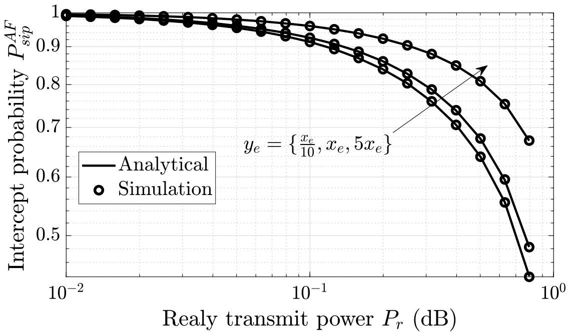


Fig. 3: Intercept performance with the variation of relay power

### B. Verification of the Asymptotic and the Exact SOP

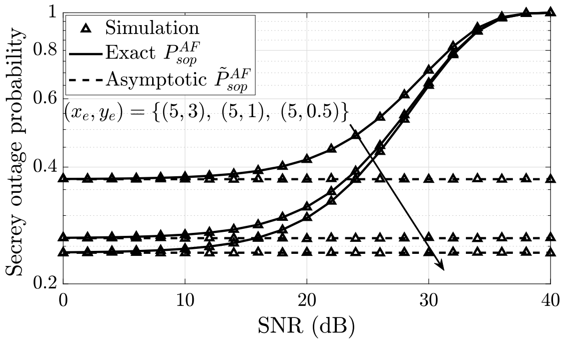


Fig. 4: Validation of exact SOP and the approximated SOP.

In Fig. 4, the performance variation of SOP in the exact and approximate regime of AF relaying has been analyzed and also verified the analysis by performing simulations. In the figure the exact SOP derived in (16) and the asymptotic SOP in (19) derived from (18) are shown by varying the SNR for various locations of eavesdropper $(x_e, y_e) = \{(5,\ 3), (5,\ 1), (5,\ 0.5)\}d$. In the figure, the eavesdropper coordinated are normalized w.r.t. the distance between $\mathcal{S}$ and $\mathcal{U}$. Fig. 4, also, validates the secrecy outage performance of the exact SOP in (16) and the approximated SOP in (19). It is noted that the SOP decreases as the eavesdropper moves away from the source. And also, it is verified that the exact and the approximated SOPs are the same at low SNRs.

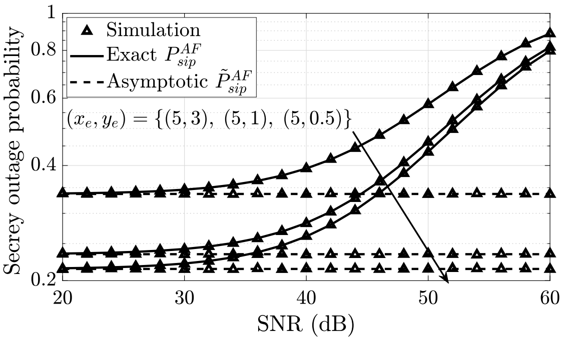
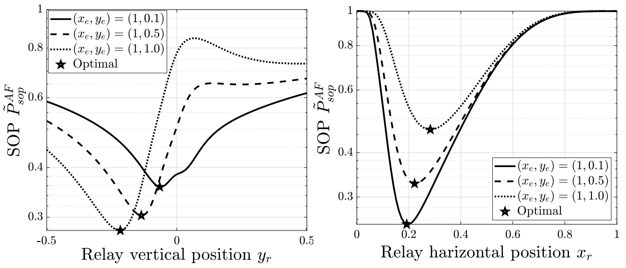


Fig. 5: Validation of intercept probability

In Fig. 5, the secrecy intercept probability is analyzed with the variation of SNR for different locations of the eavesdropper. The figure shows the validation of the exact secrecy intercept probability in (17) and the approximated SIP in (19) obtained from (21). It is noted that the analytical and the simulations exactly match each other. It is observed that the SIP is less as the eavesdropper is located farther from the source compared to the user relay node. And also, the asymptotic SIP is the same as the exact SIP at low SNRs.

### C. Insights on Optimal Relay Location



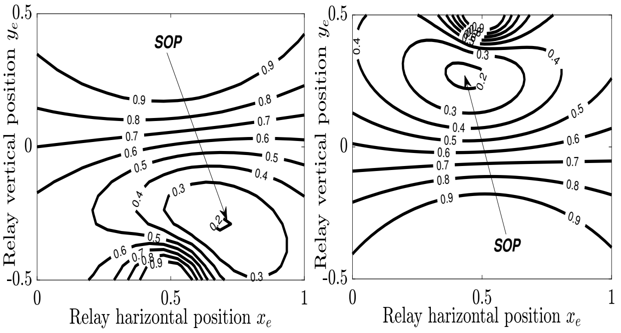
(a)

(b)

Fig. 6: The SOP performance with the variation of *R* position.

We analyze the secrecy outage probability performance in Fig. 6 and provide the optimal secrecy outage probability. Fig. 6(a) gives the performance the SOP in (16) with the variation of horizontal relay position $x_r$ and Fig. 6(b) gives the SOP with the variation of vertical relay position $y_r$ for various locations of eavesdropper. It is observed that the optimal SOP improved as the $\mathcal{E}$ is away from the line of sight path from $\mathcal{S}$ to $\mathcal{U}$ while the relay is closer to the $\mathcal{S}$.

Fig.7 represents the optimal relay location to obtain the optimal. It shows the SOP variation with the relay position for various locations of eavesdropper $(x_e, y_e) = \{(\frac{D}{10}, \frac{3}{4}x_e), (\frac{D}{10}, \frac{1}{4}x_e)\}$. It is observed that the optimal relay placement is closer to the destination if the eavesdropper is located at $(\frac{D}{10}, \frac{3D}{40})$ and it should be placed near the midpoint of $\mathcal{S}$ and $\mathcal{U}$ when $\mathcal{E}$ is at $(\frac{D}{10}, \frac{D}{40})$ to get the best SOP performance.



(a) $x_e = \frac{d}{10}, y_e = \frac{3}{4}x_e$ (b) $x_e = \frac{d}{10}, y_e = \frac{1}{4}x_e$

Fig. 7: The optimal relay position for better SOP

## VII. Conclusion

Outage analysis and secrecy outage analysis have been performed at the intended user as well as the eavesdropper in an AF relay-assisted cooperative system. To gain more analysis, an asymptotic scenario has been considered, and closed-form expressions for SOP and SIP have been derived. Numerical results validated the analytical formulation and showed the performance variation with the variation of SNR. Finally, key insights on relay location to obtain optimal SOP are given, which leads to an optimization problem.

## References

[1] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts*, vol. 21, no. 3, pp. 2734–2771, 2019, **DOI**: 10.1109/COMST.2018.2865607.

[2] C. Cebrail, A.-O. Musaab, F. Mohammed, and A.-O. Wael, "Cooperative OSIC system to exploit the leakage power of MU-MIMO beamforming based on maximum SLR for 5G," *Infocommun. J.*, vol. 11, no. 3, pp. 13–20, 2019, **DOI**: 10.36244/ICJ.2019.3.3.

[3] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015,**DOI**: 10.1109/MCOM.2015.7355563.

[4] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, Firstquarter 2017, **DOI**: 10.1109/COMST.2016.2598968.

[5] A. Fayad and T. Cinkler, "Cost-effective delay-constrained optical fron- thaul design for 5G and beyond," *Infocommun. J.,* vol. 14, no. 2, pp. 19–27, 2022, **DOI**: 10.36244/ICJ.2022.2.2.

[6] R. Saini and D. Mishra, "Chapter 4 - Privacy-aware physical layer security techniques for smart cities," in *Smart Cities Cybersecurity and Privacy*, D. B. Rawat and K. Z. Ghafoor, Eds. Elsevier, 2019, pp. 39–56, **DOI**: 10.1016/B978-0-12-815032-0.00004-4.

[7] H. Garmani, D. Ait Omar, M. El Amrani, M. Baslam, and M. Jourhmane, "Joint beacon power and beacon rate control based on game theoretic approach in vehicular Ad Hoc networks," *Infocommun. J.*, vol. 13, no. 1, pp. 58–67, 2021, **DOI**: 10.36244/ICJ.2021.1.7.

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010, **DOI**: 10.1109/TSP.2009.2038412.

[9] R. Saini, D. Mishra, and V. Kotha, "Power allocation and relay placement for secrecy outage minimization over DF relayed system," in *2021 IEEE 18th Annual Consumer Commun. Networking Conf. (CCNC)*, 2021, pp. 1–4, **DOI**: 10.1109/CCNC49032.2021.9369642.

[10] K. Venugopalachary, D. Mishra, R. Saini, and V. Chakka, "Optimizing secrecy performance of trusted RF relay against external eavesdropping," in *2019 IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6, **DOI**: 10.1109/GLOBECOM38437.2019.9013579.

[11] S. Thapar, D. Mishra, and R. Saini, "Novel outage-aware NOMA protocol for secrecy fairness maximization among untrusted users," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13259–13272, 2020, **DOI**: 10.1109/TVT.2020.3022560.

[12] I. Amin, D. Mishra, R. Saini, and S. Aïssa, "QoS-aware secrecy rate maximization in untrusted NOMA with trusted relay," *IEEE Commun. Lett.*, vol. 26, no. 1, pp. 31–34, 2022, **DOI**: 10.1109/LCOMM.2021.3124902.

[13] P. K. Hota, S. Thapar, D. Mishra, R. Saini, and A. Dubey, "Ergodic performance of downlink untrusted NOMA system with imperfect SIC," *IEEE Commun.* Lett., vol. 26, no. 1, pp. 23–26, 2022, **DOI**: 10.1109/LCOMM.2021.3126746.

[14] K. Cao, B. Wang, H. Ding, F. Gong, H. Hu, J. Tian, and T. Cheng, "Energy harvesting jammer enabled secure communication for cooperative NOMA systems," in *2020 Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2020, pp. 801–806, **DOI**: 10.1109/WCSP49889.2020.9299881.

[15] A. Jindal and R. Bose, "Resource allocation in secure multicarrier AF relay system under individual power constraints," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5070–5085, June 2017, **DOI**: 10.1109/TVT.2016.2623747.

[16] O. Waqar, H. Tabassum, and R. Adve, "Secure beamforming and ergodic secrecy rate analysis for amplify-and-forward relay networks with wireless powered jammer," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3908–3913, 2021, **DOI**: 10.1109/TVT.2021.3063341.

[17] D. Lee,"Secrecy analysis of relay-users election in AS-AF systems over nakagami fading channels," *IEEE Trans. Veh. Technol.,* vol. 70, no. 3, pp. 2378–2388, 2021, **DOI**: 10.1109/TVT.2021.3058262.

[18] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, 2016, **DOI**: 10.1109/JSTSP.2016.2607692.

[19] L. Fan, R. Zhao, F. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, 2017, **DOI**: 10.1109/TCOMM.2017.2691712.

[20] S. Han, J. Li, W. Meng, M. Guizani, and S. Sun, "Challenges of physical layer security in a satellite-terrestrial network," *IEEE Network*, pp. 1–7, 2022, **DOI**: 10.1109/MNET.103.2000636.

[21] L. Qing, H. Guangyao, and F. Xiaomei, "Physical layer security in multi-hop AF relay network based on compressed sensing," *IEEE Commun. Lett.*, vol. 22, no. 9, pp. 1882–1885, 2018, **DOI**: 10.1109/LCOMM.2018.2853101.

[22] M. Marzban, A. El Shafie, A. Sultan, and N. Al-Dhahir, "Securing full-duplex amplify-and-forward relay-aided communications through processing-time optimization," *IEEE Trans. Veh. Technol.*, pp. 1–1, 2022, https://doi.org/10.1109/TVT.2022.3163376.

[23] A. H. A. El-Malek and S. A. Zummo, "Cooperative cognitive radio model for enhancing physical layer security in two-path amplify-and-forward relaying networks," in *Proc. IEEE GLOBECOM*, 2015, pp. 1–6, **DOI**: 10.1109/GLOCOM.2015.7417778.

[24] A. Pandey and S. Yadav, "Physical layer security in cooperative AF relaying networks with direct links over mixed rayleigh and double-rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10 615–10 630, 2018, **DOI**: 10.1109/TVT.2018.2866590.

[25] K. Venugopalachary, D. Mishra, R. Saini, and V. Chakka, "Secrecy-aware jointly optimal transmit power budget sharing and trusted DF relay placement," in *2019 IEEE Wireless Commun. Networking Conf. Workshop (WCNCW)*, 2019, pp. 1–6, **DOI**: 10.1109/WCNCW.2019.8902623.

[26] K. R. Liu, A. K. Sadek, W. Su, and A. Kwasinski, Cooperative communications and networking. Cambridge university press, 2009.

[27] A. Papoulis and S. U. Pillai, Probability, Random Variables, and Stochastic Processes, 4th ed. Boston: McGraw Hill, 2002.

[28] B. Barua, H. Q. Ngo, and H. Shin, "On the SEP of cooperative diversity with opportunistic relaying," *IEEE Commun. Lett.*, vol. 12, no. 10, pp. 727–729, Oct. 2008, **DOI**: 10.1109/LCOMM.2008.080915.

[29] I. S. Gradshteyn and I. M. Ryzhik, Table of integrals, series, and products, 7th ed. Academic Press, Amsterdam, 2007.

**Kotha Venugopalachary** (Student Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Nalla Malla Reddy Engineering College, affiliated with Jawaharlal Nehru Technological University (JNTU), Hyderabad, India, in 2013, the M.Tech. degree in Computational Engineering from the Rajiv Gandi University of Knowledge and Technologies, Andrapradesh, India in 2016, and currently doing Ph.D. on the topic of physical layer security in wireless cooperative systems in the department of electrical engineering, Shiv Nadar University, Uttar Pradesh, India, since 2017. His research interests include wireless communication (cooperative systems), resource allocation, physical layer security, and Graph signal processing.

**Deepak Mishra** (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Guru Gobind Singh Indraprastha University, New Delhi, India, in 2012, and the Ph.D. degree in electrical engineering from the Indian Institutes of Technology Delhi, New Delhi, in 2017. He has been a Senior Research Associate with the School of Electrical Engineering and Telecommunications, University of New South Wales Sydney, Australia, since August 2019. Before that, he was a Postdoctoral Researcher with the Department of Electrical Engineering (ISY), Linköping University, Linköping, Sweden, from August 2017 to July 2019. He has also been a Visiting Researcher with the Northeastern University, Boston, MA, USA, University of Rochester, Rochester, NY, USA, Huawei Technologies, Paris, France, and Southwest Jiaotong University, Chengdu, China.

His current research interests include energy harvesting cooperative communication networks, massive MIMO, backscattering, physical layer security, as well as signal processing and energy optimization schemes for the uninterrupted operation of wireless networks. He was a recipient of the IBM Ph.D. Fellowship Award in 2016, the Raman Charpak Fellowship Award in 2017, and the Endeavour Research Fellowship Award in 2018. He was selected as an Exemplary Reviewer of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS in 2017 and 2018, IEEE WIRELESS COMMUNICATIONS LETTERS in 2019, and IEEE TRANSACTIONS ON COMMUNICATIONS in 2019 and 2020.

**Ravikant Saini** (Member, IEEE) received the B.Tech. degree in Electronics and Communication Engineering and M.Tech. degree in Communication Systems from the Indian Institute of Technology Roorkee, India, in 2001 and 2005, respectively. He has received the Ph.D. degree from the Indian Institute of Technology Delhi, India, in 2017. From 2005 to 2009 he worked as a Senior Software Engineer with Aricent Technology, Gurgaon, India. From 2009 to 2011 he worked as an Assistant Professor in Shobhit University, Meerut, India. He is currently an Assistant Professor in the Department of Electrical Engineering, IIT Jammu, Jammu, India. His research interests include wireless communication, resource allocation, and physical layer security.