Received: 9 March 2020 | Revised: 10 August 2020 | Accepted: 23 September 2020

DOI: 10.4218/etrij.2020-0084

ORIGINAL ARTICLE

ETRI Journal WILEY

# Power allocation-Assisted secrecy analysis for NOMA enabled cooperative network under multiple eavesdroppers

V. Narasimha Nayak | Kiran Kumar Gurrala

Department of Electronics and Communication Engineering, National Institute of Technology Andhra Pradesh, Andhra Pradesh, India

**Correspondence**
Narasimha Nayak Vankudoth, Department of Electronics and Communication Engineering, National Institute of Technology Andhra Pradesh, Andhra Pradesh, India.
Email: vnarasimhanayakphd@gmail.com

In this work, the secrecy of a typical wireless cooperative dual-hop non-orthogonal multiple access (NOMA)-enabled decode-and-forward (DF) relay network is investigated with the impact of collaborative and non-collaborative eavesdropping. The system model consists of a source that broadcasts the multiplexed signal to two NOMA users via a DF relay, and information security against the eavesdropper nodes is provided by a helpful jammer. The performance metric is secrecy rate and ergodic secrecy capacity is approximated analytically. In addition, a differential evolution algorithm-based power allocation scheme is proposed to find the optimal power allocation factors for relay, jammer, and NOMA users by employing different jamming schemes. Furthermore, the secrecy rate analysis is validated at the NOMA users by adopting different jamming schemes such as without jamming (WJ) or conventional relaying, jamming (J), and with control jamming (CJ). Simulation results demonstrate the superiority of CJ over the J and WJ schemes. Finally, the proposed power allocation outperforms the fixed power allocation under all conditions considered in this work.

**KEYWORDS**
Control jamming, DF, NOMA, physical layer security, secrecy rate

## 1 | INTRODUCTION

Because of its higher spectral efficiency, non-orthogonal multiple access (NOMA) has been considered one of the promising technologies for the present 5G and beyond wireless networks. NOMA technology multiplexes signals of different users at the source in the power domain, where all the user nodes are allowed to share the same resources with distinct power levels. In NOMA, super position coding is applied at the source to mix the signals and the multiplexed signal is forwarded to different users. In addition, successive interference cancelation (SIC) is applied at the destinations to extract the users' own information [1,2]. The authors in [3] investigated the performance of a NOMA wireless network under randomly deployed users with metrics like ergodic rate and outage probability, and they concluded that NOMA outperforms the conventional orthogonal multiple access (OMA) schemes. NOMA has the potential to be integrated with other available technologies (such as cooperative communications, physical layer security (PLS), and SWIPT). In cooperative NOMA, the information transmission at the relay node was carried out using basic amplify-forward (AF) and decode-forward (DF) protocols. The authors in [4] studied the performance analysis of the basic relaying protocols and derived the equation for outage probability. A cooperative NOMA system was studied with fixed power allocation (FPA) in which near user helps the far user in information transmission [5]. The outage probability analysis of the cooperative NOMA

This is an Open Access article distributed under the term of Korea Open Government License (KOGL) Type 4: Source Indication + Commercial Use Prohibition + Change Prohibition (http://www.kogl.or.kr/info/licenseTypeEn.do).
1225-6463/$ © 2021 ETRI

system was investigated in both full-duplex and half-duplex modes in [6]. Ding et al. [7] proposed a novel relay selection scheme for a cooperative NOMA network to enhance the outage probability performance. Recently, the demand for high speed and secured data transmission for next-generation wireless networks has attracted research interest. The recent related work regarding the PLS in NOMA-based wireless networks is highlighted in the following section.

## 1.1 | Related work

Because of the broadcast nature of the wireless channels, source information can be leaked to all unauthorized users in the wireless network [8]. For this system, the secrecy rate is determined by the link capacity difference between source-to-destination and source-to-eavesdropper wireless links. Robustness of the wireless network can be improved by enhancing the capacity of confidential links and simultaneously by minimizing the capacity of eavesdropper links. Optimal jammer and relay selection schemes were proposed in [9–11] to improve the secrecy performance of cooperative network in the presence of eavesdroppers. Two new relay selection schemes were introduced with power allocation, but jamming schemes were not considered [12]. In [13], a security-aware AF relaying scheme was proposed for a cooperative network in the presence of untrusted relays, and in addition, jamming and relay selection techniques were discussed to maximize the secrecy capacity. Additionally, Gurrala and Das [14] investigated the performance in terms of secrecy rate and intercept probability of hybrid decode amplify-forward cooperative network with fixed and optimal power allocation. In this work, the authors discussed different jamming schemes in a wireless cooperative network. The system secrecy performance depends on the location of NOMA users and eavesdroppers. In [15], outage probability is examined to analyze the impact of node location on the performance of the wireless NOMA network. A comprehensive study of cooperative relaying for securing the wireless information transmission against eavesdroppers was investigated in [16]. A two-way relay-based NOMA system with PLS was considered in [17], and the effect of an eavesdropper on the secrecy performance is validated in terms of secrecy outage probability and intercept probability. The secrecy outage probability of a DF relay-based NOMA network under a multi-relay scenario was examined in the presence of a single eavesdropper. Three different relay selection strategies were proposed and compared with traditional multi-relay forwarding under fixed and dynamic power allocation schemes [18]. Furthermore, the secrecy rate of a NOMA-based network was well investigated for both AF and DF relaying protocols but the jamming schemes were not incorporated in [19]. The work in [20] validated the secrecy outage behavior of a Nakagami fading channel-based cooperative NOMA network under three different cases, but jamming was not considered. The security performance of two different relay selection schemes for a cooperative NOMA network was illustrated and the expression for the secrecy outage probability was derived in [21]. Khan [22] examined the physical layer secrecy in the AF relay network with power allocation and evaluated the secure rate of the system by employing a single eavesdropper; here, a jammer was not considered. Therefore, different from existing work [17–22], a jamming-aided cooperative NOMA network in the presence of untrusted relay was considered to enhance the secrecy sum rate. The analytical expression for ergodic secrecy sum rate was derived and compared with the simulation results [23]. The performance of a SWIPT-enabled multi-input single-output NOMA cognitive radio network was investigated, where artificial noise-based cooperative jamming scheme was adopted to improve the secrecy performance. Simulation results of the considered network are compared with OMA schemes [24].

From the above literature survey, it can be noticed that the secrecy performance analysis of a cooperative NOMA network has not been addressed with collaborative and non-collaborative eavesdroppers, and in this scenario, jamming schemes have not yet been explored. The optimal power allocation schemes have also not been introduced for both jamming and control jamming conditions. Motivated by these observations in our analysis, a new control jamming (CJ) scheme is introduced for a cooperative NOMA DF relay network with multiple eavesdroppers (collaborative and non-collaborative). Here, we assume that eavesdroppers have a significant impact on both NOMA users. A differential evolution (DE) algorithm-based power allocation scheme is proposed to find the optimal power allocation factors of the relay, jammer, and both NOMA users.

The significant contributions of our work are summarized as follows.

(i) In this work, a system model of a DF relay-based cooperative NOMA network with multiple eavesdroppers (collaborative and non-collaborative) is introduced. The secrecy performance analysis is carried out in terms of secrecy rate, and the ergodic secrecy rate is obtained theoretically.

(ii) A new jamming scheme is proposed, called the CJ scheme, in which the NOMA users have the knowledge of jamming interference whereas the eavesdroppers do not have it. The secrecy rate of the CJ scheme is analyzed and its performance is compared with the jamming (J) and without jamming (WJ) schemes.

(iii) The secrecy rate maximization with the aid of control jamming is considered as an optimization problem subjected to total power constraint. The optimization problem is solved using the DE algorithm, which has low complexity and quick convergence, to find the optimal power allocation factors $\alpha_1$ and $\alpha_2$. Here, maximizing the secrecy rate is used as a cost function.

(iv) Finally, comparative analysis is carried out between the proposed power allocation (PPA) and FPA under the WJ, J, and CJ schemes in both collaborative and non-collaborative eavesdropping scenarios, and it is found that the PPA outperforms FPA.

This paper is organized into six sections. Section 2 describes the system model of a dual-hop cooperative NOMA network in DF mode. In Section 3, performance analysis of the system is presented and secrecy rate is further approximated analytically. In Section 4, the problem formulation and DE-based power allocation are reported. Simulation results are discussed in Section 5 followed by the conclusions in Section 6.

## 2 | SYSTEM MODEL

A wireless cooperative NOMA network that consists of a source (S) node that broadcasts the multiplexed signal to the two NOMA users ($D_1$ and $D_2$) with the cooperation of the DF relay (R) node in the presence of multiple eavesdroppers is considered as the system model. A jammer (J) node is introduced to forward an interference signal purposely to the eavesdroppers (E), as shown in Figure 1.

In our analysis, all the channel links are considered to be independent, exhibit Rayleigh flat fading, and operate in a half-duplex mode. In this network, there are no direct links present between source-to-eavesdropper and source-to-destination. The information transmission occurs in two phases (broadcast phase and cooperation phase). During the broadcast phase, the source employs super position principle to transmit the information signal $x_s = (a_1x_1 + a_2x_2)$ to the relay. Here, $a_1$ and $a_2$ represent the power allocation factors of the far user ($D_1$) and near user ($D_2$), respectively. In this phase, we assume that the source-to-relay information transmission is secured from the eavesdroppers.

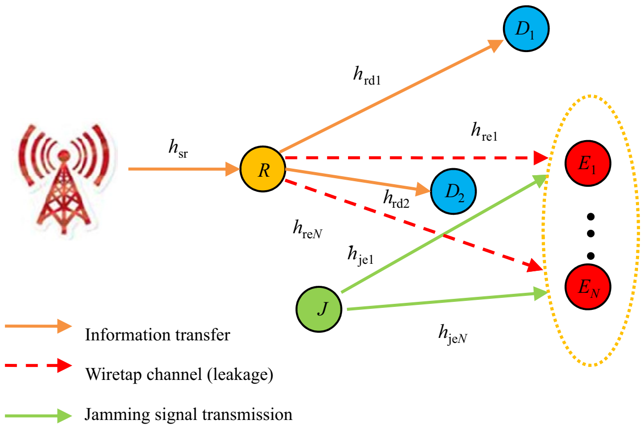

**FIGURE 1** Dual-hop cooperative NOMA network with PLS

During the first time slot, the received signal at the relay is given by

$$y_{sr} = h_{sr}\left(\sqrt{P_s a_1} x_1 + \sqrt{P_s a_2} x_2\right) + n_{sr}, \tag{1}$$

where $P_s$ represents the source transmit power. In the cooperation phase, the relay detects the received signal from the source and forwards it to the corresponding destinations. The signal received at the destinations can be expressed as

$$y_{rd_i} = \sqrt{P_r} h_{rd_i} \hat{y}_{sr} + n_{rd_i} \quad i = 1, 2, \tag{2}$$

where $\hat{y}_{sr}$ represents the decoded version of the signal that was received from the source. Meanwhile, the multiple eavesdroppers receive the leaky information from the relay-to-destination transmission and the jammer sends the interfering signal on to these eavesdroppers. The received signal at the eavesdroppers can be formulated as

$$y_{e_n} = y_{re_n} + y_{je_n} \; n = 1, \ldots, N, \tag{3}$$

where

$$y_{je_n} = \sqrt{P_j} h_{je_n} x + n_{je_n} \quad n = 1, \ldots, N; \tag{4}$$

$$y_{re_n} = \sqrt{P_r} h_{re_n} (\hat{y}_{sr}) + n_{re_n} \; n = 1, \ldots, N. \tag{5}$$

The received signal from the jammer to the NOMA users is given by

$$y_{jd_i} = \sqrt{P_j}\, h_{jd_i} x + n_{jd_i} \; i = 1, 2, \tag{6}$$

where $x$ is the interference signal created by the jammer. $P_r$ and $P_j$ represent powers at the relay node and jammer node, respectively. The channel gains $h_{sr}$, $h_{rd_i}$, $h_{re_n}$, $h_{je_n}$ $CN(0, \Omega_1)$ between all the nodes are considered to be zero-mean complex Gaussian random variables, and $n_{sr}, n_{rd_i}, n_{re_n}, n_{je_n} \sim CN(0, \sigma_A^2)$ represent complex additive white Gaussian noise at all the nodes with noise variance $N_0$.

Two jamming schemes are analyzed in this work, and their performance is compared with the performance of the conventional or WJ schemes to reveal the improvement in secrecy performance. In the WJ scheme, the relay and destinations (NOMA users) are able to decode the received signal properly and this scheme does not include any jamming process. In the J scheme, the jammer interference is not known at the destinations and eavesdroppers. Finally, a new special jamming scheme is introduced in a cooperative NOMA network in which information about the interference signal generated by jammer is known to NOMA users, whereas the eavesdroppers are unaware of it. The secrecy rate analysis for these three jamming schemes is given in Table 1.

# 3 | PERFORMANCE ANALYSIS

## 3.1 | Secrecy rate of a NOMA-based DF relay network with the CJ scheme

For a DF-operated relay network with control jamming, the secrecy rate is derived as follows. For user fairness and according to the basic principle of NOMA, high power is allocated to the far user ($D_1$), who is operating under poor channel conditions, and low power is allocated to near user ($D_2$), who is operating under strong channel conditions. The far user ($D_1$) decodes its own signal $x_1$ directly by considering the near user ($D_2$) signal $x_2$ as interference. It is assumed that perfect SIC is applied at the near user to decode its own signal $x_2$ by removing the far user signal $x_1$ from the combined NOMA signal. Based on the received signals at the relay and the corresponding destinations, the signal-to-noise ratio (SNR) calculations are obtained. From (1), the received SNRs at the relay to detect signals $x_1$ and $x_2$ respectively are given by

$$\gamma_{sr} = \frac{P_s a_1 |h_{sr}|^2}{P_s a_2 |h_{sr}|^2 + N_0} \quad \text{w.r.t. } D_1; \tag{7}$$

$$\gamma_{sr} = \frac{P_s a_2 |h_{sr}|^2}{N_0} \quad \text{w.r.t. } D_2. \tag{8}$$

In the cooperation phase, the signal received at the destination is given as

$$y_{rdi} = \sqrt{P_r} h_{rdi} \hat{y}_{sr} + n_{rdi} \quad i = 1, 2. \tag{9}$$

Using (9), the signal-to-interference-plus-noise ratio (SINR) received at the far user ($D_1$) can be expressed as

$$\gamma_{D1} = \frac{P_r a_1 \left|h_{rd_1}\right|^2}{P_r a_2 \left|h_{rd_1}\right|^2 + N_0}. \tag{10}$$

Similarly, the received SNR at the near user ($D_2$) is given by

$$\gamma_{D2} = \frac{P_r a_2 \left|h_{rd_2}\right|^2}{N_0}. \tag{11}$$

In cooperation phase, eavesdroppers are able to detect both information signals. The received SNRs at the eavesdroppers under collaborative and non-collaborative eavesdropping cases to detect signals $x_1$ and $x_2$ can be respectively obtained using (3).

Collaborative case:

$$\text{w.r.t. } x_1 : \gamma_{E1}^{C} = \sum_{n=1}^{N} \frac{P_r a_1 \left|h_{re_n}\right|^2}{P_j \left|h_{je_n}\right|^2 + 2N_0}; \tag{12}$$

$$\text{w.r.t. } x_2 : \gamma_{E2}^{C} = \sum_{n=1}^{N} \frac{P_r a_2 \left|h_{re_n}\right|^2}{P_j \left|h_{je_n}\right|^2 + 2N_0}. \tag{13}$$

Non-collaborative case:

$$\text{w.r.t. } x_1 : \gamma_{E1}^{NC} = \max_{e_n \varepsilon S_{\text{eaves}}} \frac{P_r a_1 \left|h_{re_n}\right|^2}{P_j \left|h_{je_n}\right|^2 + 2N_0} \; n = 1, \ldots, N; \tag{14}$$

$$\text{w.r.t. } x_2 : \gamma_{E2}^{NC} = \max_{e_n \, \varepsilon \, S_{\text{eaves}}} \frac{P_r a_2 \left|h_{re_n}\right|^2}{P_j \left|h_{je_n}\right|^2 + 2N_0} \; n = 1, \ldots, N. \tag{15}$$

Here, $S_{\text{eaves}}$ represents the set of all non-collaborative eavesdroppers. In the non-collaborative eavesdropping case, the impact of the eavesdropper with the highest SNR is considered. Finally, the secrecy rate [25] for collaborative and non-collaborative conditions with control jamming at $D_1$ and $D_2$ is expressed respectively as

$$C_{Di}^{cj} = 0.5 * \log_2 \left[ \frac{1 + \min(\gamma_{sr}, \gamma_{Di})}{1 + (\gamma_{Ei}^{C})} \right] \quad i = 1, 2; \tag{16}$$

$$C_{Di}^{cj} = 0.5 * \log_2 \left[ \frac{1 + \min(\gamma_{sr}, \gamma_{Di})}{1 + (\gamma_{Ei}^{NC})} \right] \quad i = 1, 2. \tag{17}$$

## 3.2 | Theoretical approximation of the ergodic secrecy rate with the CJ scheme

The ergodic secrecy rate for DF relaying [26] is given as

$$\begin{aligned} C_{Di}^{cj} = {} & \frac{W}{2} \int_{0}^{\infty} \log_2(1+\gamma) f_{\gamma_{Di}}(\gamma) \mathrm{d}\gamma \\ & - \frac{W}{2} \int_{0}^{\infty} \log_2(1+\gamma) f_{\gamma_{Ei}}(\gamma) \mathrm{d}\gamma \; i = 1, 2. \end{aligned} \tag{18}$$

Here, the probability distribution functions $f_{\gamma_{Di}}(\gamma)$ and $f_{\gamma_{Ei}}(\gamma)$ are respectively given by.

**TABLE 1** Secrecy rate of a DF relaying-based NOMA network for different jamming schemes

| Jamming type | Secrecy rate expressions at the far user ($D_1$) and near user ($D_2$) under collaborative and non-collaborative eavesdropping conditions |
|---|---|
| WJ scheme | At $D_1$:<br>$C^{wj}_{D1} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_1 \lvert h_{sr}\rvert^2}{P_s a_2 \lvert h_{sr}\rvert^2 + N_0}, \frac{P_r a_1 \lvert h_{rd_1}\rvert^2}{P_r a_2 \lvert h_{rd_1}\rvert^2 + N_0}\right)}{1+\left(\sum_{n=1}^{N} \frac{P_r a_1 \lvert h_{re_n}\rvert^2}{N_0}\right)}\right)$; $C^{wj}_{D1} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_1 \lvert h_{sr}\rvert^2}{P_s a_2 \lvert h_{sr}\rvert^2 + N_0}, \frac{P_r a_1 \lvert h_{rd_1}\rvert^2}{P_r a_2 \lvert h_{rd_1}\rvert^2 + N_0}\right)}{1+\left(\max_{e_n \varepsilon S_{\text{eaves}}} \left(\frac{P_r a_1 \lvert h_{re_n}\rvert^2}{N_0}\right)\right)}\right)$ |
|  | At $D_2$:<br>$C^{wj}_{D2} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_2 \lvert h_{sr}\rvert^2}{N_0}, \frac{P_r a_2 \lvert h_{rd_2}\rvert^2}{N_0}\right)}{1+\left(\sum_{n=1}^{N} \frac{P_r a_2 \lvert h_{re_n}\rvert^2}{N_0}\right)}\right)$; $C^{wj}_{D2} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_2 \lvert h_{sr}\rvert^2}{N_0}, \frac{P_r a_2 \lvert h_{rd_2}\rvert^2}{N_0}\right)}{1+\left(\max_{e_n \varepsilon \mathrm{S}_{\text{eaves}}} \left(\frac{P_r a_2 \lvert h_{re_n}\rvert^2}{N_0}\right)\right)}\right)$ |
| J scheme | At $D_1$:<br>$C^{j}_{D1} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_1 \lvert h_{sr}\rvert^2}{P_s a_2 \lvert h_{sr}\rvert^2 + N_0}, \frac{P_r a_1 \lvert h_{rd_1}\rvert^2}{P_r a_2 \lvert h_{rd_1}\rvert^2 + 2N_0 + P_j \lvert h_{jd_1}\rvert^2}\right)}{1+\left(\sum_{n=1}^{N} \frac{P_r a_1 \lvert h_{re_n}\rvert^2}{P_j \lvert h_{je_n}\rvert^2 + 2N_0}\right)}\right)$; $C^{j}_{D1} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_1 \lvert h_{sr}\rvert^2}{P_s a_2 \lvert h_{sr}\rvert^2 + N_0}, \frac{P_r a_1 \lvert h_{rd_1}\rvert^2}{P_r a_2 \lvert h_{rd_1}\rvert^2 + 2N_0 + P_j \lvert h_{jd_1}\rvert^2}\right)}{1+\left(\max_{e_n \varepsilon S_{\text{eaves}}} \left(\frac{P_r a_1 \lvert h_{re_n}\rvert^2}{P_j \lvert h_{je_n}\rvert^2 + 2N_0}\right)\right)}\right)$ |
|  | At $D_2$:<br>$C^{j}_{D2} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_2 \lvert h_{sr}\rvert^2}{N_0}, \frac{P_r a_2 \lvert h_{rd_2}\rvert^2}{2N_0 + P_j \lvert h_{jd_2}\rvert^2}\right)}{1+\left(\sum_{n=1}^{N} \frac{P_r a_2 \lvert h_{re_n}\rvert^2}{P_j \lvert h_{je_n}\rvert^2 + 2N_0}\right)}\right)$; $C^{j}_{D2} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_2 \lvert h_{sr}\rvert^2}{N_0}, \frac{P_r a_2 \lvert h_{rd_2}\rvert^2}{2N_0 + P_j \lvert h_{jd_2}\rvert^2}\right)}{1+\left(\max_{e_n \varepsilon \mathrm{S}_{\text{eaves}}} \left(\frac{P_r a_2 \lvert h_{re_n}\rvert^2}{P_j \lvert h_{je_n}\rvert^2 + 2N_0}\right)\right)}\right)$ |
| CJ scheme | At $D_1$:<br>$C^{cj}_{D1} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_1 \lvert h_{sr}\rvert^2}{P_s a_2 \lvert h_{sr}\rvert^2 + N_0}, \frac{P_r a_1 \lvert h_{rd_1}\rvert^2}{P_r a_2 \lvert h_{rd_1}\rvert^2 + N_0}\right)}{1+\left(\sum_{n=1}^{N} \frac{P_r a_1 \lvert h_{re_n}\rvert^2}{P_j \lvert h_{je_n}\rvert^2 + 2N_0}\right)}\right)$; $C^{cj}_{D1} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_1 \lvert h_{sr}\rvert^2}{P_s a_2 \lvert h_{sr}\rvert^2 + N_0}, \frac{P_r a_1 \lvert h_{rd_1}\rvert^2}{P_r a_2 \lvert h_{rd_1}\rvert^2 + N_0}\right)}{1+\left(\max_{e_n \varepsilon S_{\text{eaves}}} \left(\frac{P_r a_1 \lvert h_{re_n}\rvert^2}{P_j \lvert h_{je_n}\rvert^2 + 2N_0}\right)\right)}\right)$ |
|  | At $D_2$:<br>$C^{cj}_{D2} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_2 \lvert h_{sr}\rvert^2}{N_0}, \frac{P_r a_2 \lvert h_{rd_2}\rvert^2}{N_0}\right)}{1+\left(\sum_{n=1}^{N} \frac{P_r a_2 \lvert h_{re_n}\rvert^2}{P_j \lvert h_{je_n}\rvert^2 + 2N_0}\right)}\right)$; $C^{cj}_{D2} = 0.5 * \log_2\left(\frac{1+\min\left(\frac{P_s a_2 \lvert h_{sr}\rvert^2}{N_0}, \frac{P_r a_2 \lvert h_{rd_2}\rvert^2}{N_0}\right)}{1+\left(\max_{e_n \varepsilon S_{\text{eaves}}} \left(\frac{P_r a_2 \lvert h_{re_n}\rvert^2}{P_j \lvert h_{je_n}\rvert^2 + 2N_0}\right)\right)}\right)$ |

$$f_{\gamma_{Di}}(\gamma) = \frac{1}{\gamma_{Di}} \exp\left(\frac{-\gamma}{\gamma_{Di}}\right); \tag{19}$$

$$f_{\gamma_E}(\gamma) = \frac{1}{\gamma^C_{Ei}} \exp\left(\frac{-\gamma}{\gamma^C_{Ei}}\right) (\text{or}) f_{\gamma_E}(\gamma) = \frac{1}{\gamma^{NC}_{Ei}} \exp\left(\frac{-\gamma}{\gamma^{NC}_{Ei}}\right). \tag{20}$$

By substituting (19) and (20) into (18), the ergodic secrecy capacity can be written as follows.

For the collaborative eavesdropping case:

$$C^{cj}_{Di} = \frac{W}{2\ln 2}\left[\left(\exp(\gamma_{Di}^{-1}).\, E_1(\gamma_{Di}^{-1})\right) - \left(\exp((\gamma^C_{Ei})^{-1}).\, E_1((\gamma^C_{Ei})^{-1})\right)\right]. \tag{21}$$

For the non-collaborative eavesdropping case:

$$C^{cj}_{Di} = \frac{W}{2\ln 2}\left[\left(\exp(\gamma_{Di}^{-1}).\, E_1(\gamma_{Di}^{-1})\right) - \left(\exp((\gamma^{NC}_{Ei})^{-1}).\, E_1((\gamma^{NC}_{Ei})^{-1})\right)\right]. \tag{22}$$

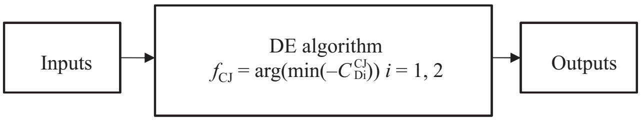
Inputs
DE algorithm
$f_{\mathrm{CJ}} = \arg(\min(-C_{\mathrm{Di}}^{\mathrm{CJ}}))\ i = 1, 2$
Outputs

**FIGURE 2** Block diagram of the proposed DE-based algorithm

Here, $E_1(.)$ is the exponential integral, and it can be expressed as $E_1(x) = \int_x^\infty \frac{\exp(-t)}{t}\mathrm{d}t$.

## 4 | PROBLEM STATEMENT AND PROPOSED SOLUTION

### 4.1 | Problem formulation

The prime objective of this paper is to enhance the secrecy performance of the considered network in the existence of multiple collaborative and non-collaborative eavesdroppers. Under the collaborative eavesdropping condition, the optimization problem is defined as

$$Maximize \left\{C_{Di}^{cj}\right\} = Maximize \left\{0.5 * \log_2 \left[\frac{1+\min(\gamma_{sr}, \gamma_{Di})}{1+(\gamma_{Ei}^{C})}\right]\right\} i = 1, 2, \tag{23}$$

subject to

$$a_1 > a_2; a_1 + a_2 = 1; 0 < \alpha_1 < 1; P_s + P_r + P_j = P; P_s = P/3; P_r = \alpha_1(P - P_s); P_j = (1 - \alpha_1)(P - P_s) \tag{24}$$

For the non-collaborative eavesdropping condition, the problem can be formulated as.

$$Maximize \left\{C_{Di}^{cj}\right\} = Maximize \left\{0.5 * \log_2 \left[\frac{1+\min(\gamma_{sr}, \gamma_{Di})}{1+(\gamma_{Ei}^{NC})}\right]\right\} i = 1, 2 \tag{25}$$

subject to

$$a_1 > a_2; a_1 + a_2 = 1; 0 < \alpha_1 < 1; P_s + P_r + P_j = P; P_s = P/3; P_r = \alpha_1(P - P_s); P_j = (1 - \alpha_1)(P - P_s).$$

### 4.2 | Proposed DE algorithm-based power allocation

The defined optimization problem is solved to provide the optimal power allocation factors: $\alpha_1$ and $\alpha_2$. These optimal factors will determine the optimal powers of the relay, jammer, and NOMA users in such a way that the secrecy rate will be improved further. Even though we have convex optimization techniques, evolutionary algorithms are preferred for the solution of the defined optimization problem because of their low computational burden and quick convergence. In this case, the DE algorithm [27] is applied to maximize the secrecy rate as the cost function. The DE algorithm is one of the simplest and most efficient evolutionary search optimization algorithms, which has several advantages. For instance, it can find the global minimum using few control parameters, it has quick convergence, and it can define variables in decimal format. It has operations such as crossover, mutation, and selection. A block diagram and flowchart of the proposed DE algorithm for obtaining optimal power allocation factors are shown in Figures 2 and 3, respectively. The parameters used in the flow chart are described as follows: $G_\mathrm{d}$ indicates total number of generations, $NP$ is the total number of population members, $g$ indicates individual generation, and $d$ represents the parameters of the objective function.

Cost function: $f_{CJ} = arg(\min(-C_{Di}^{cj}))$ i = 1,2

subject to

$$0 < \alpha_1 < 1;\ P_s + P_r + P_j = P;\ P_s = P/3;\ P_r = \alpha_1(P - P_s); P_j = (1 - \alpha_1)(P - P_s);\ 0 < \alpha_2 < 1;\ a_1 = \alpha_2;\ a_2 = (1 - \alpha_2);\ a_1 > a_2;\ a_1 + a_2 = 1$$

Inputs → $P_s, P_r, P_j, N_0, h_{sr}, h_{rd_i}, h_{re_n}, h_{je_n}, d_{sr}, d_{rd_i}, d_{re_n}, d_{je_n}, R, m$

Outputs → $\alpha_1, \alpha_2$

Initialization: In the $g$th generation, the $j$th individual of the population can be computed as

$$\alpha^{g,j} = [\alpha_1^{g,j}, \alpha_2^{g,j}]^T \quad j = 1, 2, \ldots, NP. \tag{26}$$

Fitness evolution: The cost functions for the optimization of the power allocation factors are given by.

$$\text{w.r.t. } D_1 : E_1 = f_{CJ}^{g,j}(u^{g,j}) = C_{\mathrm{D1}}^{\mathrm{cj}}(u^{g,j}).$$

$$\text{w.r.t. } D_2 : E_1 = f_{CJ}^{g,j}(u^{g,j}) = C_{D2}^{cj}(u^{g,j}).$$

Further, $E_2$ is the cost function value of the $j$th individual in the $g$th generation of $(v^{g,j})$, which is given by

$$\text{w.r.t. } D_1 : E_2 = f_{CJ}^{g,j}(v^{g,j}) = C_{D1}^{cj}(v^{g,j}).$$

$$\text{w.r.t. } D_2 : E_2 = f_{CJ}^{g,j}(v^{g,j}) = C_{\mathrm{D2}}^{\mathrm{cj}}(v^{g,j}).$$

Here, the $(u^{g,j})$ is defined as target vectors and $(v^{g,j})$ is trail vectors generated after the mutation and crossover operations.

Optimal solution: The optimal values of $(\alpha_1^{g,j})$ and $(\alpha_2^{g,j})$ are estimated once the termination criteria have been met.

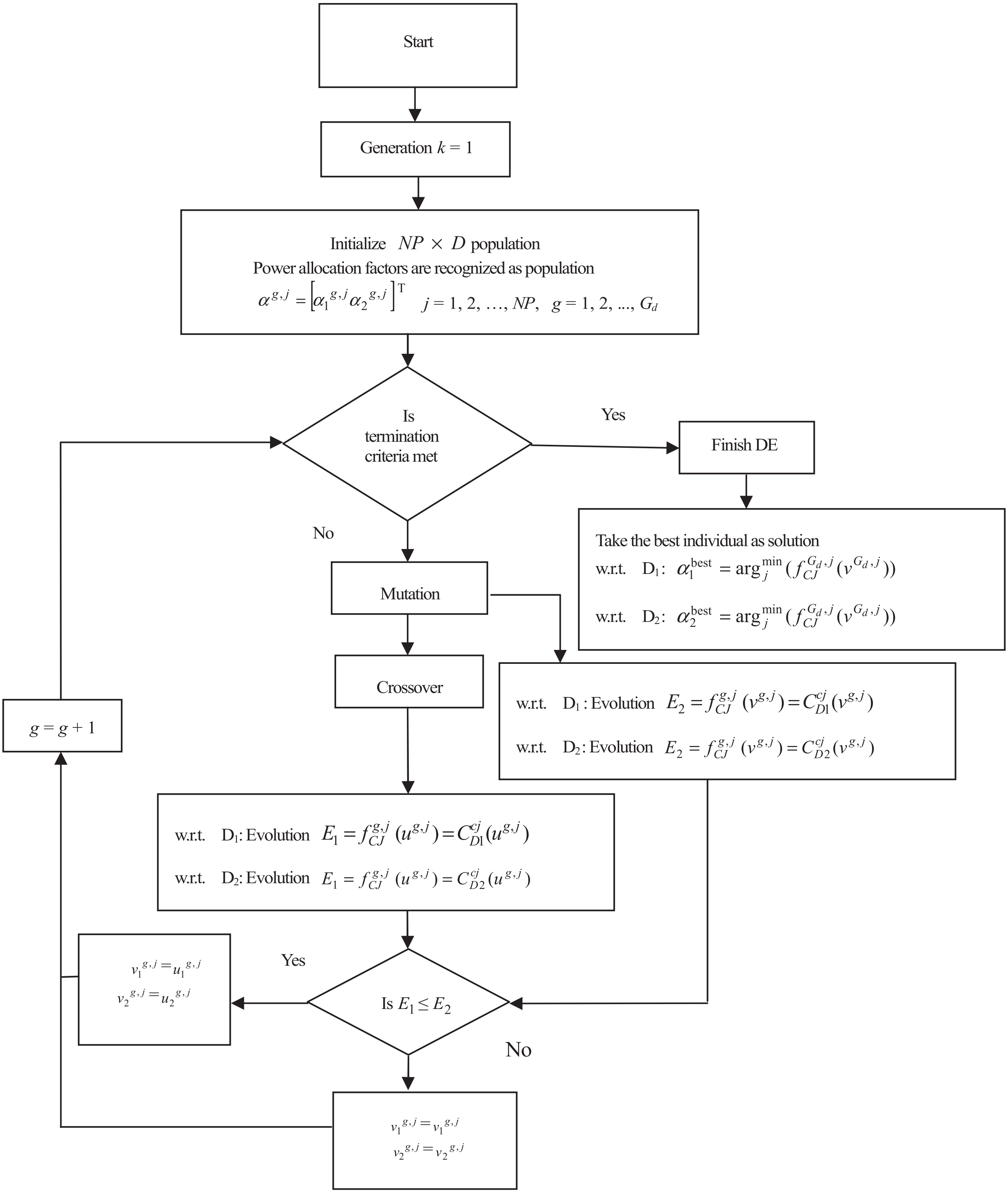
Start
Generation $k = 1$
Initialize $NP \times D$ population
Power allocation factors are recognized as population
$\alpha^{g,j} = [\alpha_1^{g,j}\alpha_2^{g,j}]^T \quad j = 1, 2, \dots, NP, \quad g = 1, 2, \dots, G_d$
Is termination criteria met
Yes
Finish DE
Take the best individual as solution
w.r.t. $D_1$: $\alpha_1^{best} = \arg_j^{\min}(f_{CJ}^{G_d,j}(v^{G_d,j}))$
w.r.t. $D_2$: $\alpha_2^{best} = \arg_j^{\min}(f_{CJ}^{G_d,j}(v^{G_d,j}))$
No
Mutation
Crossover
w.r.t. $D_1$: Evolution $E_2 = f_{CJ}^{g,j}(v^{g,j}) = C_{D1}^{cj}(v^{g,j})$
w.r.t. $D_2$: Evolution $E_2 = f_{CJ}^{g,j}(v^{g,j}) = C_{D2}^{cj}(v^{g,j})$
$g = g + 1$
w.r.t. $D_1$: Evolution $E_1 = f_{CJ}^{g,j}(u^{g,j}) = C_{D1}^{cj}(u^{g,j})$
w.r.t. $D_2$: Evolution $E_1 = f_{CJ}^{g,j}(u^{g,j}) = C_{D2}^{cj}(u^{g,j})$
Yes
$v_1^{g,j} = u_1^{g,j}$
$v_2^{g,j} = u_2^{g,j}$
Is $E_1 \le E_2$
No
$v_1^{g,j} = v_1^{g,j}$
$v_2^{g,j} = v_2^{g,j}$

**FIGURE 3** DE algorithm for attaining optimal power allocation factors

The best individual who has a low cost function value is taken as the optimal solution. For optimal power allocation, the optimal solution can be expressed as

$$\alpha_1^{best}, \alpha_2^{best} = arg_n^{\min}(f_{CJ}^{G_d,j}(v^{G_d,j})) \quad j = 1, 2, \dots, NP. \tag{27}$$

## 5 | SIMULATION RESULTS

In this section, the secrecy performance analysis of DF relaying-based cooperative NOMA network with collaborative and non-collaborative eavesdroppers under different J

**TABLE 2** Simulation specifications

| Parameter | Specifications |
|---|---|
| Total number of bits | $10^4$ |
| Modulation | QPSK |
| Channel | Rayleigh flat fading |
| Path Loss Exponent (m) | 3 |
| Number of relays (R) | 1 |
| Number of jammers (J) | 1 |
| Number of eavesdroppers (N) | 4 |
| Noise variance (*No*) | 1 |
| DE parameters | DE step size F = 0.8, Crossover probability (CR) = 0.5, NP (total number of population members) = 50*D, D = N (the number of parameters of the objective function), Iterations = 200 |
| Relay network topology | Linear topology |

and WJ schemes is examined by Monte Carlo simulations. Table 2 presents the simulation parameters. It can be noticed that the DE-based power allocation algorithm gives optimal values $\alpha_1$ (relay, jammer power allocation factor) and $\alpha_2$ (the power allocation factor of the NOMA users), which are given in Table 3. For the simulation, the MATLAB platform was used, and for each result, a total of $10^4$ independent simulations were run. For the analysis, an SNR range 0 to 30 dB was considered.

The secrecy rate analysis of far user ($D_1$) with PPA and FPA is shown in Figure 4 for the CJ and other jamming schemes. Here, both the collaborative (C) and non-collaborative (NC) eavesdropping conditions are considered. The secrecy rate of the C eavesdropping condition is less than the NC condition because all the eavesdroppers significantly affect the relay-to-destination information transmission and there is a strong link between the relay and eavesdroppers. In all cases, it can be noticed that the CJ scheme outperforms all other jamming schemes because in this condition, the destination is aware of the interference generated by the jammer. Furthermore, it can also be noticed that PPA performs better in terms of secrecy rate than the FPA scheme in both the C and NC eavesdropping conditions. For the NC eavesdropping condition at ρ = 20 dB, a secrecy rate of 0.78 bits/s/Hz and 0.56 bits/s/Hz is respectively observed with PPA and FPA under the CJ condition. Because $D_1$ is a weak user with worse channel conditions, the observed secrecy rate is low, but it is enhanced in the high SNR region when the proportionate signal power is allocated by PPA.

**TABLE 3** Optimal transmit powers of the nodes in Watts at ρ = 15 dB when the relay is located close to the eavesdroppers

| Power allocation method | Relay power ($P_r$) | Jammer power ($P_j$) | Near user power | Far user power |
|---|---|---|---|---|
| FPA | 0.4706 | 0.4706 | 0.1883 | 0.2823 |
| DEPA (PPA) | 0.6146 | 0.3268 | 0.1315 | 0.3391 |

The impact of the jammer location with respect to the eavesdropper location on the performance metric secrecy rate is presented for collaborative eavesdropping in Figure 5 with PPA and FPA at far user $D_1$. In this scenario, control jamming is an efficient solution to combat the strong relay-to-eavesdropper links to avoid the interference at the destination and maximize the secrecy rate. This figure shows that an increase in the jammer-to-eavesdropper distance will degrade the secrecy performance because jamming becomes weak whenever the eavesdroppers are located far away from the jammers. In this case, PPA also outperforms the FPA.

Figure 6 demonstrates the impact of relay-to-eavesdropper distance on the secrecy rate. This result shows that secrecy performance enhances with increases in relay-to-eavesdropper distance because the link between the relay and eavesdropper becomes weak. In this case also, the CJ scheme, which has the ability to decode the jammer signal at the far user ($D_1$), is a promising technique for improving the secrecy capacity. The maximized secrecy rate is observed for PPA but not FPA.

In Figure 7, the secrecy rate versus transmit SNR is presented for the near user ($D_2$) with CJ and other jamming schemes under C and NC eavesdropping conditions. In this case, the secrecy rate is higher because of the strong link present between the jammer and the near user ($D_2$). Because $D_2$ is the near user with SIC ability, it obtains a higher secrecy rate than the far user ($D_1$). The WJ scheme is inefficient because the relay is placed near the eavesdroppers. This figure shows that the NC eavesdropping condition yields better performance than the C eavesdropping condition. The CJ scheme obtains a higher gain than the J and WJ schemes in terms of secrecy rate.

Figure 8 illustrates the influence of jammer-to-eavesdropper distance on secrecy rate at $D_2$ with PPA. Both jamming schemes CJ and J confound the eavesdroppers and improve the secrecy rate of the considered wireless network. The secrecy performance will degrade whenever the jammer-to-eavesdropper link is weak. The plot shows that the CJ scheme provides a higher secrecy rate than all other jamming schemes. Figure 9 depicts the secrecy rate performance of near user ($D_2$) at different SNR conditions with different jamming schemes under the C eavesdropping condition. In this scenario, the CJ scheme also obtains a better secrecy rate than the J and WJ schemes. This figure validates the secrecy rate improvement of near user ($D_2$) compared to far user ($D_1$). In Figure 10, the secrecy performance enhancement of NOMA over conventional OMA is examined at near user ($D_2$) by adopting different jamming schemes with FPA under the NC eavesdropping condition. For the comparison, the transmit power of the signal of each user in

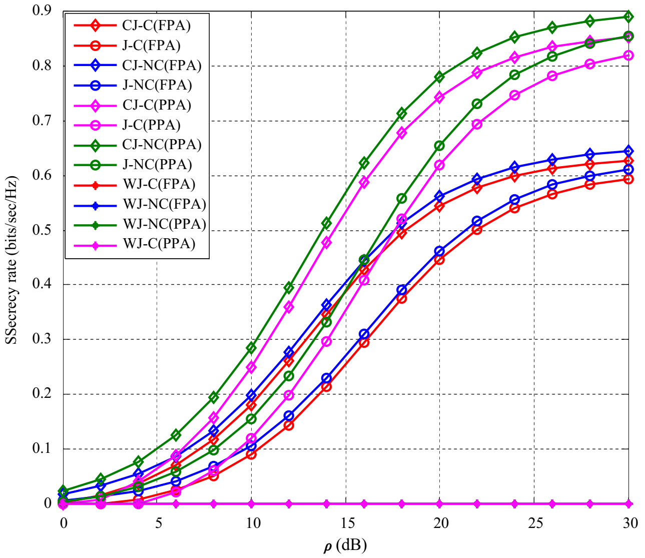

**FIGURE 4** Secrecy rate versus SNR at $D_1$ with FPA and PPA for C and NC eavesdropping conditions

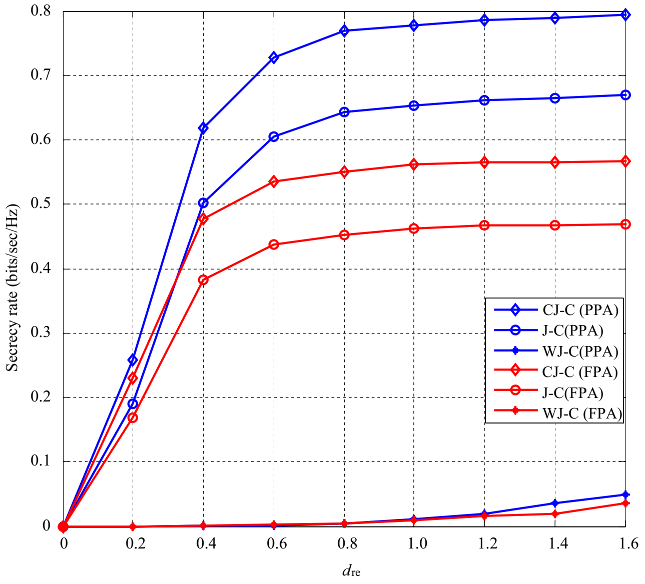

**FIGURE 6** Secrecy rate versus relay-to-eavesdropper distance in the presence of collaborative eavesdroppers at $D_1$

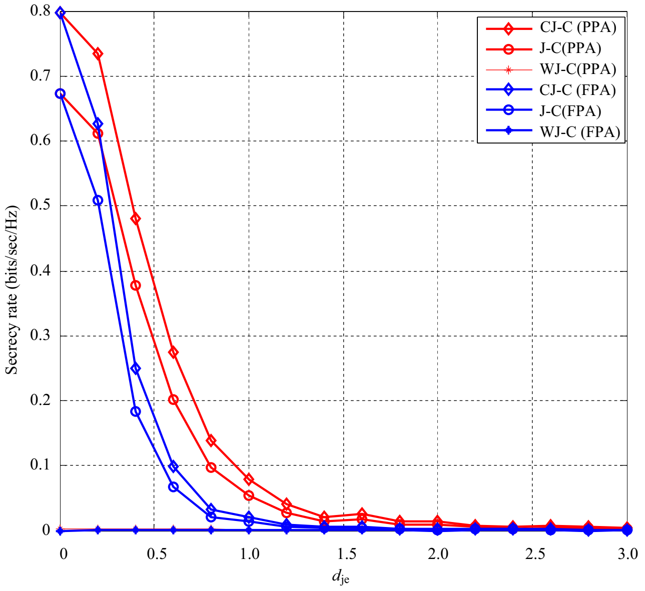

**FIGURE 5** Impact of jammer-to-eavesdropper distance on secrecy rate comparison of PPA and FPA in the C eavesdropping condition at $D_1$

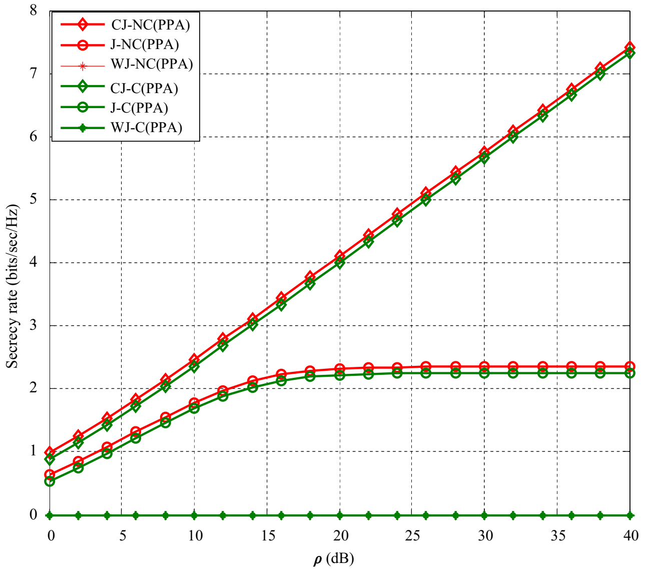

**FIGURE 7** Secrecy rate versus SNR at $D_2$ for the C and NC conditions

the OMA network is considered to be the same. It can be seen that the NOMA achieves superior secrecy performance in both CJ and J conditions.

## 5.1 | Convergence analysis

The convergence analysis of the proposed DE-based PPA scheme is validated in terms of maximizing secrecy rate and shown in Figure 11. At a particular SNR of ρ = 15 dB, the PPA converges quickly (< 20 iterations).

Some of the important insights of the total simulation analysis are as follows:

(i) The secrecy performance of the network is better in the case of non-collaborative eavesdropping than in the case of collaborative eavesdropping under all jamming schemes.

(ii) Among the three jamming schemes, the CJ scheme attains a higher secrecy rate than the J and WJ schemes in the presence of both collaborative and non-collaborative eavesdroppers.

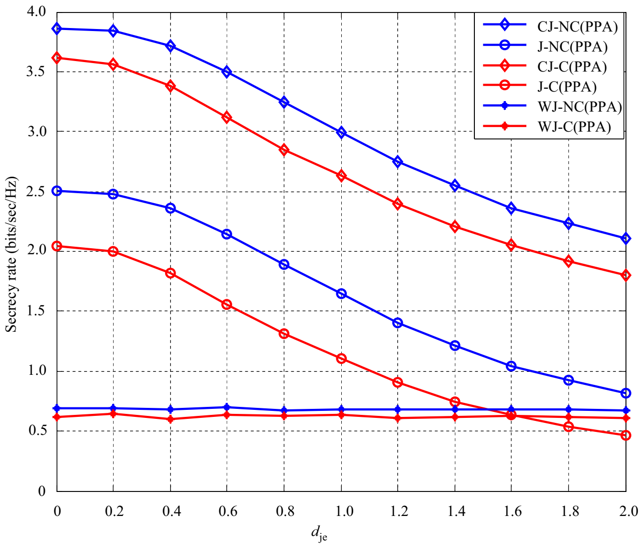

**FIGURE 8** Impact of jammer-to-eavesdropper distance on secrecy rate for the C eavesdropping condition at $D_2$

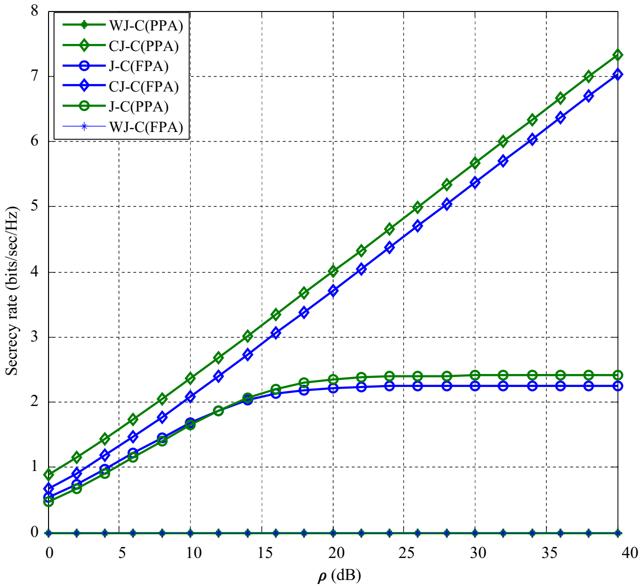

**FIGURE 9** Secrecy rate versus SNR at $D_2$ with FPA and PPA for the C condition

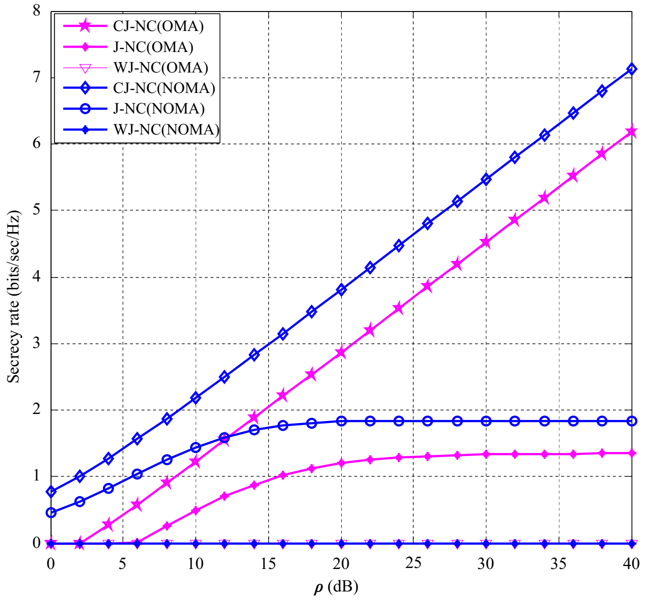

**FIGURE 10** Secrecy rate versus SNR at $D_2$ with the NOMA and OMA schemes

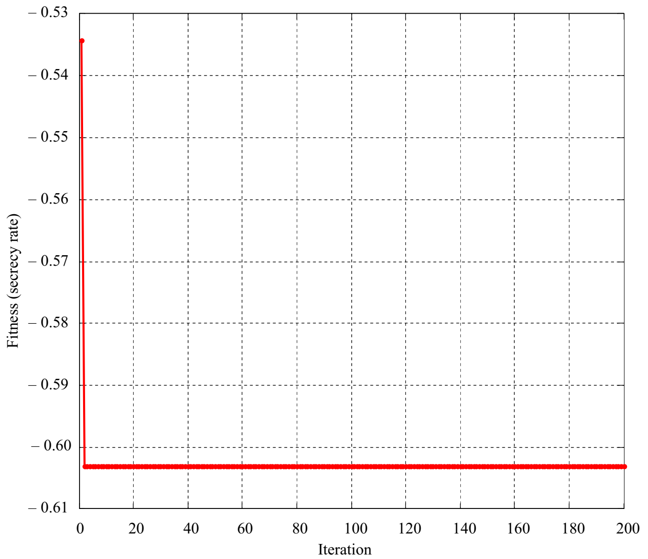

**FIGURE 11** Convergence analysis of the proposed differential evolution based PPA scheme

(iii) As the distance between jammer-to-eavesdropper increases, the secrecy rate degrades.

(iv) In all the considered cases, PPA provides a higher secrecy rate than FPA scheme in both collaborative and non-collaborative eavesdropping cases under all jamming schemes.

## 6 | CONCLUSIONS

In this work, the secrecy performance analysis of the NOMA enabled DF relay network was investigated in the presence of multiple eavesdroppers in collaborative and non-collaborative cases, and for the further improvement in secrecy rate, a novel power allocation scheme was proposed. A DE algorithm-based power allocation was proposed to find the optimal power allocation factors of relay, jammer, and NOMA users by employing different jamming schemes. In addition, a performance comparison was carried out over the proposed CJ scheme as well as the J and WJ schemes for the considered wireless network by changing both the locations of the relay and jammer with respect to the eavesdroppers. From the simulation result analysis, it can be observed that CJ attains a better secrecy performance. Moreover, the DF relaying protocol with PPA outperforms that of FPA under both C and NC eavesdropping conditions.

## ORCID

*Narasimha Nayak Vankudoth* https://orcid.org/0000-0001-8230-8030

## REFERENCES

1. L. Dai et al., *Nonorthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends*, IEEE Commun. Mag. **53** (2015), 74–81.
2. Z. Wei et al., *A survey of downlink non–orthogonal multiple access for 5G wireless communication networks*, ZTE Commun. **14** (2016), 17–26.
3. Z. Ding et al., *On the performance of nonorthogonal multiple access in 5G systems with randomly deployed users*, IEEE Signal Process. Lett. **21** (2014), 1501–1505.
4. Y. Xiao et al., *Forwarding strategy selection in dual-hop NOMA relaying systems*, IEEE Commun. Lett. **22** (2018), 1644–1647.
5. Z. Ding, M. Peng, and H. V. Poor, *Cooperative non-orthogonal multiple access in 5G systems*, IEEE Commun. Lett. **19** (2015), 1462–1465.
6. C. Zhong and Z. Zhang, *Non-orthogonal multiple access with cooperative full-duplex relaying*, IEEE Commun. Lett. **20** (2016), 2478–2481.
7. Z. Ding, H. Dai, and H. V. Poor, *Relay selection for cooperative NOMA*, IEEE Wirel. Commun. Lett. **5** (2016), 416–419.
8. L. Lai and H. El Gamal, *The relay-eavesdropper channel: Cooperation for secrecy*, IEEE Trans. Inf. Theory. **54** (2008), 4005–4019.
9. Y. Feng, et al., *Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access*, IEEE Trans. Inf. Forensics Security. **14** (2019), 1670–1683.
10. I. Krikidis, J. Thompson, and S. Mclaughlin, *Relay selection for secure cooperative networks with jamming*, IEEE Trans. Wirel. Commun. **8** (2009), 5003–5011.
11. D. H. Ibrahim and E. S. Hassan, *E1-Dolil, a new relay and jammer selection schemes for secure one-way cooperative networks*, Wirel. Pers. Commun. **75** (2014), 665–685.
12. L. Tang et al., *Secure wireless communications via cooperative relaying and jamming*, in Proc. GLOBECOM Workshops (GC Wkshps) (Houston, TX, USA), Dec. 2012, pp. 849–853.
13. L. Sun et al., *Security-aware relaying scheme for cooperative networks with untrusted relay nodes*, IEEE Commun. Lett. **19** (2015), 463–466.
14. K. K. Gurrala and S. Das, *Performance study of hybrid decode-amplify-forward (HDAF) relaying scheme for physical layer security in wireless cooperative network*, Int. J. Commun. Syst. **30** (2017), no. 8, e3182.
15. Y. Liu et al., *Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks*, IEEE Trans. Wirel. Commun. **16** (2017), 1656–1672.
16. F. Jameel et al., *A comprehensive survey on cooperative relaying and jamming strategies for physical layer security*, IEEE Commun. Surveys. **21** (2019), 2734–2771.
17. M. K. Shukla, H. H. Nguyen, and O. J. Pandey, *Secrecy performance analysis of two-way relay non-orthogonal multiple access systems*, IEEE Access **8** (2020), 39502–39512.
18. H. Lei et al., *Secrecy outage analysis for cooperative NOMA systems with relay selection schemes*, IEEE Trans. Commun. **67** (2018), 6282–6298.
19. J. Chen, L. Yang, and M.-S. Alouini, *Physical layer security for cooperative NOMA systems*, IEEE Trans. Veh. Technol. **67** (2018), 4645–4649.
20. C. Yu et al., *Secrecy outage performance analysis for cooperative NOMA over Nakagami-m Channel*, IEEE Access **7** (2019), 79866–79876.
21. Z. Wang and Z. Peng, *Secrecy performance analysis of relay selection in cooperative NOMA systems*, IEEE Access **7** (2019), 86274–86287.
22. W. U. Khan, *Maximizing physical layer security in relay-assisted multicarrier non orthogonal multiple access transmission*, Internet Technol. Lett. **2** (2019), e76.
23. L. Lv et al., *Secure cooperative communications with an untrusted relay: A NOMA-inspired jamming and relaying approach*, IEEE Trans. Inf. Forensics Secur. **14** (2019), 3191–3205.
24. F. Zhou et al., *Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT*, IEEE J. Sel. Areas Commun. **36** (2018), 918–931.
25. S. Leung-Yan-Cheong and M. Hellman, *The gaussian wire-tap channel*, IEEE Trans. Inf. Theory. **24** (1978), 451–456.
26. K. K. Gurrala and S. Das, *Maximized channel capacity based power allocation technique for multi relay hybrid decode-amplifyforward cooperative network*, Wirel. Personal Commun. **87** (2015), 663–678.
27. A. K. Qin and P. N. Suganthan, *Self-adaptive differential evolution algorithm for numerical optimization*, in Proc. IEEE Congr. Evolut. Comput. (Edinburgh, UK), Sept. 2005, pp. 1785–1791.

## AUTHOR BIOGRAPHIES

**V. Narasimha Nayak** received his B-Tech degree from SBIT, Khammam, Telangana, India, in 2007 and his M-Tech degree from the National Institute of Technology, Rourkela, India, with specialization in VLSI design and embedded systems in 2010. He is currently pursuing his PhD in the Department of Electronics and Communication Engineering with specialization in wireless communication at the National Institute of Technology Andhra Pradesh, India. His research areas include NOMA and physical layer security.

**Kiran Kumar Gurrala** has been working as an assistant professor at the Department of Electronics and Communication Engineering at the National Institute of Technology Andhra Pradesh, India, since May 2018. He received his B-Tech degree from GEC, Gudlavalleru, Andhra Pradesh, India, in 2006 and his M-Tech from the National Institute of Technology, Rourkela, India, with specialization in telematics and signal processing in 2011. He received his PhD in the Department of Electrical Engineering with specialization in wireless communication from the National Institute of Technology, Rourkela, India. His research areas include cooperative communications in next-generation wireless networks.