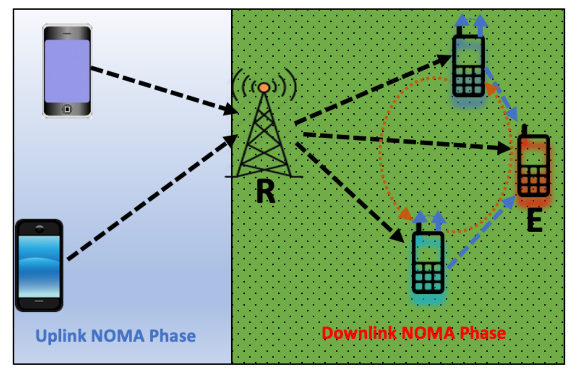
Secrecy Performance Analysis of Cooperative Non-Orthogonal Multiple Access in IoT Networks

Ashish Rauniyar, *Member, IEEE,* Olav N. Østerbø, *Senior Member, IEEE,* Jan Erik Håkegård *Senior Member, IEEE,* and Paal Engelstad, *Senior Member, IEEE*

***Abstract*— Different system models utilizing Non-orthogonal multiple access (NOMA) have been successfully studied to meet the growing capacity demands of the Internet of Things (IoT) devices for the next-generation networks. However, analyzing the anti-eavesdropping for NOMA systems under different scenarios and settings still needs further exploration before it can be practically deployed. Therefore, in this paper, we study the secrecy performance of a cooperative NOMA system in IoT networks where two source nodes communicate with their respective destination nodes via a common relay in the presence of an eavesdropper. Specifically, two source node sends their data in parallel over the same frequency band to the common relay node using uplink NOMA. Then, the relay node forwards the decoded symbols to the respective destination nodes using downlink NOMA in the presence of an eavesdropper. To enhance the security performance of the considered system, we study and propose an artificial noise (AN)-aided scheme in which the two destination nodes emit a jamming signal to confuse the eavesdropper while receiving the signal from the common relay node. We also study the effect of NOMA power allocation, perfect successive interference cancellation (pSIC), and imperfect SIC (ipSIC) on the considered system. Analytical expressions for the Ergodic capacity, Ergodic secrecy sum rate (ESSR), and secrecy outage probability (SOP) are mathematically derived and verified with the simulation results. Our results demonstrate that a significantly higher ESSR and lower SOP of the system can be attained compared to a conventional NOMA system without a destination-assisted jamming signal scheme.**



***Index Terms*— Capacity, Cooperative communications, Eavesdropper, Internet of Things, Jamming, NOMA, Secrecy, Sensors**

I. Introduction

The upcoming sixth-generation (6G) wireless communication network is aiming to revolutionize the connected world of the Internet of Things (IoT) with more autonomous and intelligent systems [1] [2]. According to estimates in [3], more than 80 billion IoT sensors/devices will be connected to the Internet by 2025, with global data flow reaching up to 175 trillion gigabytes. Therefore, the next-generation networks such as 6G networks are expected to fulfill the capacity demands of the future IoT networks [4] [5]. It is to be noted that sensors are the principal component that brings the idea of IoT into reality [6]. Wireless sensor networks (WSNs) and IoT have emerged as one of the most promising technologies, with widespread use in military, agricultural, and industrial applications. A detailed survey on different applications of WSN in IoT is outlined in [7] [8]. Specifically, the authors in [8] have reviewed sensors, smart data processing, communication protocols, and artificial intelligence to enable the deployment of AI-based sensors for next-generation IoT applications. Multiple access schemes have always been crucial in the development of large-scale wireless networks. Current orthogonal multiple access (OMA) schemes, such as frequency/time/code division multiple access (FDMA/TDMA/CDMA) techniques, allocate limited resources to each network user. Hence, such OMA schemes cannot meet the capacity demands of the future generation of 6G and IoT networks [9] [10]. In this regard, non-orthogonal multiple access (NOMA) has been proposed as a potential approach for meeting the capacity demands of future 6G and IoT networks [11]–[13].

In NOMA, several users share the same resource. NOMA is primarily divided into code domain NOMA and power domain NOMA. Each user in the code domain NOMA is given their own code-book, which is complex-valued, multidimensional, and sparse in nature. Sparse Code Multiple Access (SCMA), which uses the Message Passing Algorithm

A. Rauniyar and J. E. Håkegård are with Connectivity Technologies and Platforms Department, SINTEF Digital, Trondheim, 7034, Norway (e-mail: ashish.rauniyar@sintef.no; jan.e.hakegard@sintef.no).

O. N. Østerbø is with Telenor Research, Oslo, 1360, Norway (e-mail: olav.osterbo@getmail.no).

P. Engelstad is with Autonomous Systems and Sensor Technologies Research Group, Department of Technology Systems, University of Oslo, Oslo, 0316, Norway (e-mail: paal.engelstad@its.uio.no).

This research work was supported by the COPS (Comprehensive Privacy and Security for Resilient CPS/IoT) project funded by the Research Council of Norway under the project number:300102.

Accepted for Publication in IEEE Sensors Journal

This is the author accepted version of an article published in IEEE Sensors Journal
https://doi.org/10.1109/JSEN.2022.3199540

(MPA) for multi-user detection, is a popular code-domain NOMA approach [14]. The MPA's complexity, on the other hand, grows exponentially as the number of interfering users grows. Furthermore, we must increase the number of codebook patterns in order to increase the number of users supported by the code domain NOMA system. Adding additional codebook patterns increases the decoding complexity and lowers the system's reliability [15]. On the other hand, the third generation partnership project (3GPP)-Long Term Evolution (LTE) standard employs a power domain NOMA technique known as Multi-User Superposition Transmission (MUST) [16]. Therefore, in this paper, we limit ourselves to the power domain NOMA, which is used by the 3GPP LTE standard. More specifically, in the power domain NOMA, different users' signals are superimposed on each other based on its user channel conditions [17]. As shown in Fig. 1, in downlink NOMA, the user with poor channel conditions is allocated more power compared to the user with good channel conditions. Finally, at the receiver end, the signals of the users are separated using the signal-to-interference cancellation (SIC) approach [18] [19]. The working principle of uplink NOMA is shown in Fig. 2. The signals of users with good channel conditions are likely to be the strongest at the BS in uplink NOMA. As a result, the BS decodes these signals first. The BS then uses the SIC technique to decode weak user signals by removing the signals of users with strong channel conditions [20].

With the exponential growth of IoT devices and sensors, NOMA is regarded as a promising candidate for massive device-to-device (D2D) and machine-to-machine (M2M) communications since it can serve multiple users within a single resource block [21] [22]. However, the rapid expansion of wireless networks poses a huge challenge because it is fundamentally a broadcast medium, allowing easy access to transmitted data and making it extremely difficult to maintain secrecy and privacy in such networks [23] [24]. In addition, the data/information of mobile IoT sensors and devices, such as personal information, medical data, banking data, and so on, may be broadcasted through the wireless medium. Therefore, the security and privacy of these data pose a great challenge for the next-generation IoT networks [25] [26]. In this regard, physical layer security (PHY-security) is an attractive approach against wiretapping attacks as it inherently exploits the nature of the wireless broadcast medium to enhance information security [27]–[30]. There has recently been a growing interest in examining security issues with the NOMA enabled IoT networks [31]–[36].

Ren et al. studied the PHY-security of a wireless-powered relay aided NOMA system [31]. The authors studied a scenario where an eavesdropper wiretaps the source node's signal. With self-energy recycling, the full-duplex (FD) relay assisted the transmission from the source node to a near and a far NOMA user. Further, a PHY-security improvement method for a downlink NOMA in the presence of an active eavesdropper was studied in [32]. The authors suggested a minimum transmitter selection technique for an FD-enabled NOMA system to guarantee secure transmission in the presence of an active eavesdropper. A secrecy outage performance of a multiple-relay assisted NOMA network was analyzed in [33]. The closed-form expressions for outage probabilities were developed for two relay selection (RS) strategies: the optimal single relay selection scheme and the two-step single relay selection scheme. Similarly, for cooperative NOMA networks, closed-form expressions for secrecy outage probability for different relay selection schemes were investigated in [34]. In the presence of an eavesdropper, a secret transmission of uplink NOMA with a single antenna and multi-antenna users was examined in [35]. The authors studied the system's secrecy outage probability (SOP) and strictly positive secrecy capacity (SPSC) and derived the closed-form expressions. In [36], legitimate surveillance of a downlink NOMA network with multiple groups of suspicious users was investigated. Although all of these works have successfully studied the PHY-security of a NOMA system, analyzing the anti-eavesdropping for NOMA systems in IoT networks under different scenarios and settings still needs further exploration before it can be practically deployed. Therefore, this paper studies the secrecy performance analysis of a cooperative NOMA system in a relay sharing scenario from a PHY-security perspective. Here, two source nodes communicate with their respective destination nodes via a common relay in the presence of an eavesdropper. We examine and propose an artificial noise (AN)-aided strategy in which the two destination node emits a jamming signal to degrade the channel capacity of the eavesdropper while receiving the signal from the common relay node in order to improve the security performance of the considered cooperative NOMA enabled IoT system.

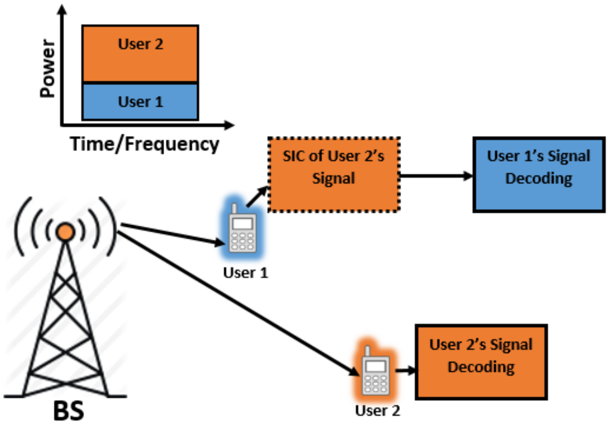


Fig. 1. Downlink NOMA

In summary, the major contributions of this paper are as follows:

- In a cooperative relay sharing situation where two source nodes communicate with their respective destination nodes in the presence of an eavesdropper, we propose and explore in detail the secrecy performance analysis of the cooperative NOMA in IoT networks.
- We further investigate and propose an artificial noise-aided strategy in which the two destination node emits a jamming signal to confuse the eavesdropper while

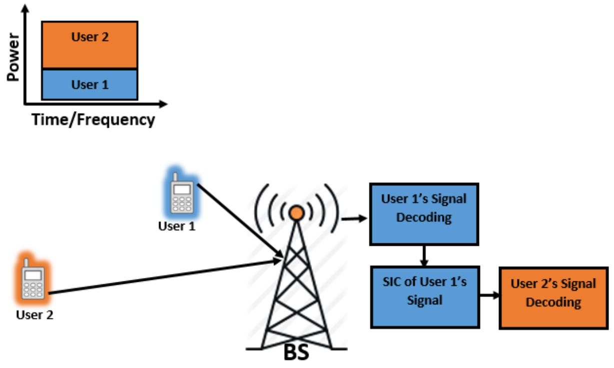


Fig. 2. Uplink NOMA

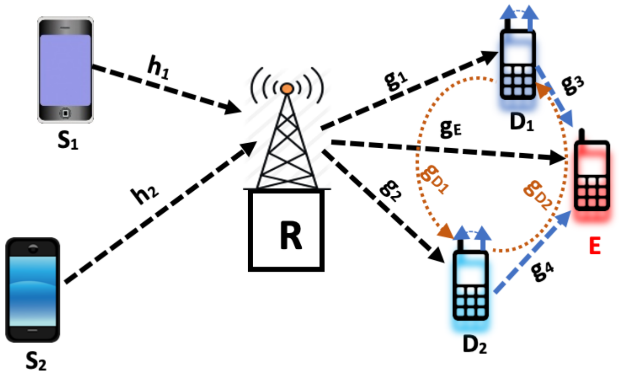


Fig. 3. System Model

receiving the signal from the common relay node in order to improve the security performance of the considered system.

- The Ergodic capacity (EC), Ergodic sum secrecy rate (ESSR), and the secrecy outage probability (SOP) of the system are analytically derived under both pSIC and ipSIC scenarios.
- Effect of NOMA power allocation coefficients, pSIC, and ipSIC on the considered system are thoroughly examined.
- Our results demonstrate that considerable ESSR and lower SOP can be achieved in comparison to a conventional NOMA system without a destination-assisted jamming signal scheme.

The rest of the paper is organized as follows. Our system model is presented in Section II. Section III reports the system's achievable data rate, Ergodic secrecy sum rate, and secrecy outage probability. This section also includes analytical derivations of the system's secrecy capacity, ESSR, and SOP. Section IV deals with numerical results and analysis. In Section V, conclusions are drawn, and future works are suggested.

II. System Model

Fig. 3 depicts the system model scenario under consideration. A practical scenario in the context of a smart city would be a group of IoT devices and sensors communicating with their destination IoT sensor nodes with the help of a cooperative relaying node. Due to the broadcast nature of the wireless medium, the data transmission between them is subjected to communication tapping due to the presence of an eavesdropper. The direct links between the source and destination nodes are absent because of the blockage from the tall buildings.

As shown in Fig. 3, our system model consists of two NOMA users in group $S = S_1, S_2$, two NOMA users in the group $D = D_1, D_2$, and an eavesdropper E. The IoT nodes S_1 and S_2 can only communicate and exchange information through the common relay node R. Due to deep shadowing or blockage, it is assumed that there is no direct communication between the groups S and D. As a result, R is used to communicate information between S_1, S_2, and D_1 and D_2 nodes. The eavesdropper attempts to overhear the received signal of the legitimate user nodes D_1 and D_2.

We have also assumed that channel state information (CSI) is perfectly known, and that each node in the group S is a half-duplex transceiver system and that each node in the group D, i.e., $D1$ and $D2$, is a full-duplex (FD) transceiver system. At D_1 and D_2, one antenna is used for signal reception from R, and another antenna is used for the artificial-noise (AN) transmission to the eavesdropper node E. Due to the full-duplex mode, the D_1 and D_2 nodes are subjected to self-interference. All wireless channels are subject to independent Rayleigh block fading plus additive white Gaussian noise with mean power N_0 in which the channel remains constant during block transmission and varies independently from one block to another. In addition, we assumed that each user in groups S and D is sorted by channel quality, i.e. $|h_1|^2 > |h_2|^2$ in group S and $|g_1|^2 < |g_2|^2$ in group D. Here, h_1, and h_2 are denoted as complex channel coefficients of the $S_1 \rightarrow R$, $S_2 \rightarrow R$ links, respectively, in group S where $h_i \sim CN\left(0, \lambda_{h_i} = 1/d_i^{-v}\right)$, d_i is the distance between R and i^{th} user in group S, λ_{h_i} is the variance, and v is the path loss exponent, $i = 1, 2$. Similarly, g_1, and g_2 are denoted as complex channel coefficients of the links, $R \rightarrow D_1$, $R \rightarrow D_2$ respectively, in group D where $g_i \sim CN\left(0, \lambda_{g_i} = 1/d_i^{-v}\right)$. g_E is the complex channel coefficients of the link, $R \rightarrow E$ and $g_E \sim CN\left(0, \lambda_{g_E} = 1/d_E^{-v}\right)$ where d_E is the distance between R and the eavesdropper E. Similarly, g_{D_1}, and g_{D_2} are the complex channel coefficients of the links, $D_1 \rightarrow D_2$ and $D_2 \rightarrow D_1$, respectively, and $g_{D_1} \sim CN\left(0, \lambda_{w_1} = 1/d^{-v}_{d_1 d_2}\right)$, $g_{D_2} \sim CN\left(0, \lambda_{w_2} = 1/d^{-v}_{d_1 d_2}\right)$, where $d_{d_1 d_2}$ is the distance between D_1 and D_2 node. The self-interference channels on the D_1 and D_2 node are assumed to be fading free [37].

The working of our system model can be divided into two stages as explained below.

A. First Stage

In this stage, each NOMA user, i.e. S_1 and S_2 in group S, uses the uplink NOMA protocol to non-orthogonally transfer information signals to the common relay node R. According to the uplink NOMA protocol, R decodes the signal of the strong channel user first, i.e. S_1, while treating the signal of the weak channel user, S_2, as noise. Then, using the signal-to-interference (SIC) cancellation approach, it cancels out the

S_1 signal to successfully decode the S_2 signal.

Accordingly, following the uplink NOMA protocol, both S_1 and S_2 simultaneously transmit symbols x_1 and x_2 with powers a_1P_T and a_2P_T, respectively. The total transmit power is P_T, and the NOMA power allocation coefficients for S_1 and S_2 are a_1 and a_2, respectively. Since, we have used uplink NOMA in this stage, the total transmit power constraint for the S_1 and S_2 users is $a_1 > a_2$, with $a_1 + a_2 = 1$.

During this stage, the information signal received at R is:

$$y_R = \sqrt{a_1P_T}h_1x_1 + \sqrt{a_2P_T}h_2x_2 + n_R, \tag{1}$$

where x_1, and x_2 are the information signals of the users S_1, and S_2, respectively. P_T is the total transmission power of the NOMA user nodes, and $n_R \sim CN(0, \sigma_R^2)$ is the Additive White Gaussian Noise (AWGN) at R with mean zero and variance σ_R^2.

Therefore, the received signal-to-interference-plus-noise ratios (SINR) at R for S_1 and S_2 user signals are respectively given by:

$$\gamma_{R\to x_1} = \frac{\rho a_1|h_1|^2}{\rho a_2|h_2|^2 + 1}, \tag{2}$$

$$\gamma_{R\to x_2} = \frac{\rho a_2|h_2|^2}{\rho a_1|\hat{h}_1|^2 + 1}, \tag{3}$$

where $\hat{h}_1 \sim CN(0, \xi\lambda_{h_1})$ and $\rho = \frac{P_T}{\sigma_R^2}$ represents the transmit signal-to-noise ratio (SNR). The parameter ξ, $0 \leq \xi \leq 1$, denotes the residual interference signal caused by the SIC imperfection at R. $\xi = 0$ denotes the perfect SIC (pSIC) and $\xi = 1$ denotes the imperfect SIC (ipSIC) at R.

B. Second Stage

In the second stage, in the presence of an eavesdropper, R broadcasts the decoded data using the downlink NOMA protocol. The strong channel NOMA user decodes and cancels the signals of the weak channel NOMA user before decoding its own signal. Accordingly, R broadcasts a superimposed composite signal ($\sqrt{a_3P_R}\hat{x_1} + \sqrt{a_4P_R}\hat{x_2}$) to D_1, D_2, and E using the downlink NOMA protocol. The total transmit power of the R is P_R, and the NOMA power allocation coefficients of the D_1 and D_2 signals at R are a_3 and a_4, respectively. $\hat{x_1}$ and $\hat{x_2}$ are the decoded symbols for S_1 and S_2 at R. Since we have used downlink NOMA in this stage, the total transmit power constraint of R for the users D_1 and D_2 implies that $a_3 > a_4$ with $a_3 + a_4 = 1$. Also, it should be noted that the destination nodes D_1 and D_2 are working in a full duplex mode. Therefore, they concurrently transmit the intended artificial noise signal to the eavesdropper E to degrade its channel while receiving the signal from R.

The received signal at D_2 in this stage can be expressed as:

$$\begin{aligned} y_{D_2} = {} & \underbrace{\sqrt{a_3P_R}g_2\hat{x_1} + \sqrt{a_4P_R}g_2\hat{x_2}}_{\textit{desired signal}} + \underbrace{\sqrt{P_{D_1}}x_{D_1}g_{D1}}_{\textit{interfering signal}} \\ & + \underbrace{\sqrt{P_{D_2}}x_{D_2}g_{2(nsi)}}_{\textit{self-interference}} + n_{D_2}, \end{aligned} \tag{4}$$

where P_{D_2} is the transmit power of the signal D_2 transmit to confuse the eavesdropper E, P_{D_1} is the transmit power of the signal D_1 transmit to confuse the eavesdropper E, $n_{D_2} \sim CN(0, \sigma_{D_2}^2)$, and $g_{2(nsi)} \sim CN(0, \sigma^2_{D_2(nsi)})$.

Now, the SINR at D_2 to decode $\hat{x_1}$ can be expressed as:

$$\gamma_{D_2\to R,\hat{x_1}} = \frac{a_3P_R|g_2|^2}{a_4P_R|g_2|^2 + \phi P_{D_1}|g_{D1}|^2 + \sigma^2_{D_2(nsi)} + \sigma^2_{D_2}} \tag{5}$$

where $\phi = 0$ denotes that D_2 can completely cancel the interference caused by D_1's transmitted signal and $\phi = 1$ denotes that D_2 cannot cancel the interference caused by D_1's transmitted signal.

After SIC, the SINR at D_2 to decode $\hat{x_2}$ can be expressed as:

$$\gamma_{D_2\to R,\hat{x_2}} = \frac{a_4P_R|g_2|^2}{a_3P_R|\hat{g_2}|^2 + \phi P_{D_1}|g_{D1}|^2 + \sigma^2_{D_2(nsi)} + \sigma^2_{D_2}} \tag{6}$$

where $\hat{g_2} \sim CN(0, \xi\lambda_{g_2})$.

Similarly, the received observation at the D_1 node in this stage can be expressed as:

$$\begin{aligned} y_{D_1} = {} & \underbrace{\sqrt{a_3P_R}g_1\hat{x_1} + \sqrt{a_4P_R}g_1\hat{x_2}}_{\textit{desired signal}} + \underbrace{\sqrt{P_{D_2}}x_{D_2}g_{D2}}_{\textit{interfering signal}} \\ & + \underbrace{\sqrt{P_{D_1}}x_{D_1}g_{1(nsi)}}_{\textit{self-interference}} + n_{D_1}, \end{aligned} \tag{7}$$

$n_{D_1} \sim CN(0, \sigma_{D_1}^2)$, and $g_{1(nsi)} \sim CN(0, \sigma^2_{D_1(nsi)})$.

Now, the SINR at D_1 to decode $\hat{x_1}$ can be expressed as:

$$\gamma_{D_1\to R,\hat{x_1}} = \frac{a_3P_R|g_1|^2}{a_4P_R|g_1|^2 + \phi P_{D_2}|g_{D_2}|^2 + \sigma^2_{D_1(nsi)} + \sigma^2_{D_1}} \tag{8}$$

where $\phi = 0$ denotes that D_1 can completely cancel the interference caused by the signal transmitted by D_2, and $\phi = 1$ denotes that D_1 cannot cancel the interference caused by the signal transmitted by D_2.

The eavesdropper E tries to overhear the received signals of the legitimate user nodes D_1 and D_2 signal. Furthermore, the D_1 and D_2 destination nodes emit a jamming signal to confuse the eavesdropper E while receiving the signal from the common relay node R to improve the system's secrecy performance. As a result, the eavesdropper's wiretapped signal E can be given as:

$$\begin{aligned} y_E = {} & (\sqrt{a_3P_R}\hat{x_1} + \sqrt{a_4P_R}\hat{x_2})g_E + \sqrt{P_{D_1}}x_{D_1}g_3 + \\ & \sqrt{P_{D_2}}x_{D_2}g_4 + n_E \end{aligned} \tag{9}$$

where $n_E \sim CN(0, \sigma_E^2)$.

In practice, the eavesdropper E cannot completely eliminate the artificial noise signal from the received signal. Here, we have assumed that the eavesdropper E has strong user detection capabilities in order to appropriately decode the users' messages from the wiretapped signal.

At the eavesdropper E, the SINR of the D_1 and D_2 users can be represented as:

$$\gamma_{E\rightarrow\hat{x}_1} = \frac{a_3 P_R |g_E|^2}{P_{D_1}|g_3|^2 + P_{D_2}|g_4|^2 + \sigma_E^2} \tag{10}$$

$$\gamma_{E\rightarrow\hat{x}_2} = \frac{a_4 P_R |g_E|^2}{P_{D_1}|g_3|^2 + P_{D_2}|g_4|^2 + \sigma_E^2} \tag{11}$$

III. Achievable Data Rate, Ergodic Secrecy Sum Rate, and Secrecy Outage Probability

A. Achievable Data Rate

The achievable data rate associated with the symbol x_1, according to our system model, is given by:

$$C_{x_1} = E\left[\frac{1}{2}\log_2\left(1+\min\left(\gamma_{R\rightarrow x_1}, \gamma_{D_2\rightarrow R,\hat{x}_1}, \gamma_{D_1\rightarrow R,\hat{x}_1}\right)\right)\right] \tag{12}$$

where E[·] denotes the statistical expectation operator.

Theorem 1: The analytical expression for the achievable data rate of x_1 can be expressed as:

$$\begin{aligned} C_{x_1}^{Ana} = \frac{a_3 e^{\frac{F-E}{a_4}}}{2\ln 2}\Bigg(& \frac{A^2 I\left(\frac{A}{a_4-A}, \frac{E}{a_4}, \frac{F}{a_4}\right)}{(A-B)(A-C)(A-D)} - \\ & \frac{B^2 I\left(\frac{B}{a_4-B}, \frac{E}{a_4}, \frac{F}{a_4}\right)}{(A-B)(B-C)(B-D)} + \frac{C^2 I\left(\frac{C}{a_4-C}, \frac{E}{a_4}, \frac{F}{a_4}\right)}{(A-C)(B-C)(C-D)} - \\ & \frac{D^2 I\left(\frac{D}{a_4-D}, \frac{E}{a_4}, \frac{F}{a_4}\right)}{(A-D)(B-D)(C-D)}\Bigg) \end{aligned} \tag{13}$$

where $I(a,b,c) = e^{\frac{c}{a}-ab}E_1\left(\frac{(1+a)c}{a}\right) + \sum_{i=1}^{\infty}(-1)^i \frac{E_i(c)}{a^{i-1}} S_i(ab)$, $S_i(x) = \sum_{k=i}^{\infty}(-1)^k \frac{(x)^k}{k!}$, $E(.)$ is an exponential integral, and $A = a_3 + a_4$, $B = a_4 + \frac{\lambda_{h_1} a_2 a_3}{\lambda_{h_2} a_1}$, $C = \frac{\phi \rho_{D_1} \lambda_{g_2}}{\rho_{P_R} \lambda_{w_1}}$, $D = \frac{\phi \rho_{D_2} \lambda_{g_1}}{\rho_{P_R} \lambda_{w_2}}$, $E = \frac{\lambda_{h_1} a_3}{\rho a_1}$, $F = \frac{2(\lambda_{g_1}+\lambda_{g_2})}{\rho_{P_R}}$

Proof: The proof is given in Appendix I.

Similarly, the achievable data rate associated with the symbol x_2 is given by:

$$C_{x_2} = E\left[\frac{1}{2}\log_2\left(1+\min\left(\gamma_{R\rightarrow x_2}, \gamma_{D_2\rightarrow R,\hat{x}_2}\right)\right)\right] \tag{14}$$

where E[·] denotes the statistical expectation operator.

Theorem 2: The analytical expression for the achievable data rate of x_2 can be expressed as:

$$\begin{aligned} C_{x_2}^{Ana} = \frac{a_4 e^{\frac{L-K}{\xi a_3}}}{2\ln 2}\Bigg(& \frac{G I\left(\frac{G}{\xi a_3 - G}, \frac{K}{\xi a_3}, \frac{L}{\xi a_3}\right)}{(G-H)(G-J)} - \\ & \frac{H I\left(\frac{H}{\xi a_3 - H}, \frac{K}{\xi a_3}, \frac{L}{\xi a_3}\right)}{(G-H)(H-J)} + \frac{J I\left(\frac{J}{\xi a_3 - J}, \frac{K}{\xi a_3}, \frac{L}{\xi a_3}\right)}{(G-J)(H-J)}\Bigg) \end{aligned} \tag{15}$$

where $I(a,b,c) = e^{\frac{c}{a}-ab}E_1\left(\frac{(1+a)c}{a}\right) + \sum_{i=1}^{\infty}(-1)^i \frac{E_i(c)}{a^{i-1}} S_i(ab)$, $S_i(x) = \sum_{k=i}^{\infty}(-1)^k \frac{(x)^k}{k!}$, $E(.)$ is an exponential integral, and $G = \xi a_3 + a_4$, $H = \xi a_3 + \frac{\lambda_{h_1} a_1 a_4}{\lambda_{h_2} a_2}$, $J = \frac{\phi \rho_{D_1} \lambda_{g_2}}{\rho_{P_R} \lambda_{w_1}}$, $K = \frac{\lambda_{h_2} a_4}{\rho a_2}$, $L = \frac{2\lambda_{g_2}}{\rho_{P_R}}$

Proof: The proof can be derived by following the similar steps as in Appendix I and hence it is omitted.

The achievable data rate of the system is given by:

$$C_{Sys} = C_{x_1} + C_{x_2} \tag{16}$$

Combining Equations (14) and (16) gives the analytical expression for the achievable data rate of the system.

Finally, the eavesdropper channel capacity for wiretapping x_1 and x_2 symbols at E can respectively be given as:

$$C_{E,x_1} = E\left[\frac{1}{2}\log_2\left(1+\gamma_{E\rightarrow\hat{x}_1}\right)\right] \tag{17}$$

$$C_{E,x_2} = E\left[\frac{1}{2}\log_2\left(1+\gamma_{E\rightarrow\hat{x}_2}\right)\right] \tag{18}$$

where E[·] denotes the statistical expectation operator.

Theorem 3: The analytical expression for EC for wiretapping the x_1 symbol at the eavesdropper E can be expressed as:

$$\begin{aligned} C_{E\rightarrow x_1}^{Ana} = \frac{1}{2\ln 2}\Bigg(& \frac{e^{C_1}E_1(C_1)}{(1-A_1)(1-B_1)} - \frac{A_1 e^{\frac{C_1}{A_1}} E_1\left(\frac{C_1}{A_1}\right)}{(1-A_1)(A_1-B_1)} + \\ & \frac{B_1 e^{\frac{C_1}{B_1}} E_1\left(\frac{C_1}{B_1}\right)}{(1-A_1)(A_1-B_1)}\Bigg) \end{aligned} \tag{19}$$

where $E_1(.)$ is an exponential integral of order 1, and $A_1 = \frac{\rho_{D_1}\lambda_E}{a_3 \rho_{P_R} \lambda_{g_3}}$, $B_1 = \frac{\rho_{D_2}\lambda_E}{a_3 \rho_{P_R} \lambda_{g_4}}$, and $C_1 = \frac{\lambda_E}{a_3 \rho_{P_R}}$

Proof: The proof is given in Appendix II.

Theorem 4: The analytical expression for EC for wiretapping the x_2 symbol at the eavesdropper E can be expressed as:

$$\begin{aligned} C_{E\rightarrow x_2}^{Ana} = \frac{1}{2\ln 2}\Bigg(& \frac{e^{C_2}E_1(C_2)}{(1-A_2)(1-B_2)} - \frac{A_2 e^{\frac{C_2}{A_2}} E_1\left(\frac{C_2}{A_2}\right)}{(1-A_2)(A_2-B_2)} + \\ & \frac{B_2 e^{\frac{C_2}{B_2}} E_1\left(\frac{C_2}{B_2}\right)}{(1-A_2)(A_2-B_2)}\Bigg) \end{aligned} \tag{20}$$

where $E_1(.)$ is an exponential integral of order 1, and $A_2 = \frac{\rho_{D_1}\lambda_E}{a_4 \rho_{P_R} \lambda_{g_3}}$, $B_2 = \frac{\rho_{D_2}\lambda_E}{a_4 \rho_{P_R} \lambda_{g_4}}$, and $C_2 = \frac{\lambda_E}{a_4 \rho_{P_R}}$

Proof: The proof can be derived by following the similar steps as in Appendix II, and hence it is omitted.

B. Ergodic Secrecy Sum Rate

The system's achievable secrecy capacity/Ergodic secrecy capacity should be determined to provide reliable communication between the source and the destination nodes in the presence of an eavesdropper. The achievable secrecy capacity is defined as the difference between the channel capacity of the data links and the eavesdropping link.

Therefore, the achievable secrecy capacity of x_1 and x_2 symbols can respectively be expressed as:

$$C_{Sec,x_1} = \left[C_{x_1} - C_{E,x_1}\right]^+ \tag{21}$$

$$C_{Sec,x_2} = \left[C_{x_2} - C_{E,x_2}\right]^+ \tag{22}$$

where $\left[x\right]^+ \triangleq \max\left[x, 0\right]$.

The achievable secrecy sum capacity of the system is given by:

$$C_{Sec-Sys} = \left[C_{x_1} - C_{E,x_1}\right]^+ + \left[C_{x_2} - C_{E,x_2}\right]^+ \tag{23}$$

Now, by using Jensen's inequality, the lower bound (lb) of the Ergodic secrecy sum rate (ESSR) for our system can be written as [31]:

$$\begin{aligned} E\left[C_{Sec-Sys}\right]^{Ana} &= C_{Sec-Sys,lb} \\ &\triangleq \left[E[C_{x_1}^{Ana}] - E[C_{E\to x_1}^{Ana}]\right]^+ + \\ &\quad \left[E[C_{x_2}^{Ana}] - E[C_{E\to x_2}^{Ana}]\right]^+ \end{aligned} \tag{24}$$

where E[·] denotes the statistical expectation operator.

Now, by substituting the Equations (13), (19), (15), and (20) respectively in Equation (24), gives the analytical expression for the ESSR of the considered system.

C. Secrecy Outage Probability Performance Analysis

In the physical layer security context, the secrecy outage probability (SOP) is utilized as one of the performance evaluation metrics. It is given by the probability that the difference between the main and the eavesdropper channels' capacities is below a predefined threshold, called secrecy target data rate (bps/Hz). In simple terms, a secrecy outage occurs in the system when the secrecy capacity falls below a predetermined threshold. For our considered system model, end-to-end SOP is given by:

$$\begin{aligned} P_{Out-Sec} &= \Pr(C_{Sec,x_1} < R_1 \;\cap\; C_{Sec,x_2} < R_2) \\ &= \underbrace{1 - \Pr(C_{Sec,x_1} > R_1)}_{SOP_{x_1}} \cap \underbrace{1 - \Pr(C_{Sec,x_2} > R_2)}_{SOP_{x_2}} \end{aligned} \tag{25}$$

where R_1 (bps/Hz) and R_2 (bps/Hz) are the secrecy target data rate for the $S_1 - D_1$ and $S_2 - D_2$ pair nodes respectively.

Theorem 5: The closed-form analytical expression for the secrecy outage probability of the considered system can be expressed as in Equation 26.

Proof: The detailed proof is given in Appendix III.

$$\begin{aligned} SOP_{Ana} = &\Bigg(1 - (1+t)(1-B_3t)^3 B_3^4 e^{D_3}\Bigg(B_4 \sum_{j=1}^{5} C_j I\Big(-\frac{\beta_j}{\alpha_j}, D_1, D_2\Big) + \delta_4 \sum_{j=1, j\neq 4}^{5} \frac{\alpha_j C_j}{-\alpha_4\beta_j + \alpha_j\beta_4}\Bigg[I\Big(-\frac{\beta_j}{\alpha_j}, D_1, D_2\Big) - \\ &I\Big(-\frac{\beta_4}{\alpha_4}, D_1, D_2\Big)\Bigg] + \frac{\delta_4 C_4}{\alpha_4} I_2\Big(-\frac{\beta_4}{\alpha_4}, D_1, D_2\Big) + \delta_5 \sum_{j=1, j\neq 5}^{5} \frac{\alpha_j C_j}{-\alpha_5\beta_j + \alpha_j\beta_5}\Bigg[I\Big(-\frac{\beta_j}{\alpha_j}, D_1, D_2\Big) - I\Big(-\frac{\beta_5}{\alpha_5}, D_1, D_2\Big)\Bigg] \\ &+ \frac{\delta_5 C_5}{\alpha_5} I_2\Big(-\frac{\beta_5}{\alpha_5}, D_1, D_2\Big)\Bigg)\Bigg)\Bigg(1 - (1+t)(1-\hat{B}_3t)^2 \hat{B}_3{}^3 e^{\hat{D}_3}\Bigg(\hat{B}_4 \sum_{j=1}^{4} \hat{C}_j I\Big(-\frac{\hat{\beta}_j}{\hat{\alpha}_j}, \hat{D}_1, \hat{D}_2\Big) + \hat{\delta}_3 \sum_{j=1, j\neq 3}^{4} \frac{\hat{\alpha}_j \hat{C}_j}{-\hat{\alpha}_3\hat{\beta}_j + \hat{\alpha}_j\hat{\beta}_3} \\ &\Bigg[I\Big(-\frac{\hat{\beta}_j}{\hat{\alpha}_j}, \hat{D}_1, \hat{D}_2\Big) - I\Big(-\frac{\hat{\beta}_3}{\hat{\alpha}_3}, \hat{D}_1, \hat{D}_2\Big)\Bigg] + \frac{\hat{\delta}_3 \hat{C}_3}{\hat{\alpha}_3} I_2\Big(-\frac{\hat{\beta}_3}{\hat{\alpha}_3}, \hat{D}_1, \hat{D}_2\Big) + \hat{\delta}_4 \sum_{j=1, j\neq 4}^{4} \frac{\hat{\alpha}_j \hat{C}_j}{-\hat{\alpha}_4\hat{\beta}_j + \hat{\alpha}_j\hat{\beta}_4}\Bigg[I\Big(-\frac{\hat{\beta}_j}{\hat{\alpha}_j}, \hat{D}_1, \hat{D}_2\Big) \\ &- I\Big(-\frac{\hat{\beta}_4}{\hat{\alpha}_4}, \hat{D}_1, \hat{D}_2\Big)\Bigg] + \frac{\hat{\delta}_4 \hat{C}_4}{\hat{\alpha}_4} I_2\Big(-\frac{\hat{\beta}_4}{\hat{\alpha}_4}, \hat{D}_1, \hat{D}_2\Big)\Bigg)\Bigg) \end{aligned} \tag{26}$$

where, $t = (2^{2R} - 1)$, $A_1 = \frac{\lambda_{h_1} a_2}{\lambda_{h_2} a_1}$, $A_2 = \frac{\phi\rho_{D_1}\lambda_{g_2}}{a_3\rho_{P_R}\lambda_{w_1}}$, $A_3 = \frac{\phi\rho_{D_2}\lambda_{g_1}}{a_3\rho_{P_R}\lambda_{w_2}}$, $A_4 = \frac{\rho_{D_1}\lambda_E}{a_3\rho_{P_R}\lambda_{g_3}}$, $A_5 = \frac{\rho_{D_2}\lambda_E}{a_3\rho_{P_R}\lambda_{g_4}}$, $B_1 = \frac{\lambda_{h_1}}{\rho a_1}$, $B_2 = \frac{2(\lambda_{g_1}+\lambda_{g_2})}{a_3\rho_{P_R}}$, $B_3 = \frac{a_4}{a_3}$, $B_4 = \frac{\lambda_E}{a_3\rho_{P_R}}$, $\alpha_1 = A_1(1 - B_3t)$, $\alpha_2 = (A_2 - B_3)(1 - B_3t)$, $\alpha_3 = (A_3 - B_3)(1 - B_3t)$, $\alpha_4 = A_4(1 - B_3t)$, $\alpha_5 = A_5(1 - B_3t)$, $\beta_1 = A_1 + B_3$, $\beta_2 = A_2$, $\beta_3 = A_3$, $\beta_4 = A_4(1 - tB_3) + (1+t)B_3$, $\beta_5 = A_5(1 - tB_3) + (1+t)B_3$, $\delta_4 = A_4B_3(1+t)$, $\delta_5 = A_5B_3(1+t)$, $D_1 = \frac{1-B_3t}{B_3}\left(B_1 + \frac{B_4}{t+1}\right)$, $D_2 = \frac{B_2}{B_3(1-B_3t)}$, $D_3 = B_4\frac{t}{t+1} - \frac{1}{B_3}\left(B_1 + \frac{B_4}{t+1}\right) + \frac{B_2}{B_3}$, $\hat{A}_1 = \frac{\lambda_{h_2} a_1 \xi}{\lambda_{h_1} a_2}$, $\hat{A}_2 = \frac{\phi\rho_{D_1}\lambda_{g_2}}{a_4\rho_{P_R}\lambda_{w_1}}$, $\hat{A}_3 = \frac{\rho_{D_1}\lambda_E}{a_4\rho_{P_R}\lambda_{g_3}}$, $\hat{A}_4 = \frac{\rho_{D_2}\lambda_E}{a_4\rho_{P_R}\lambda_{g_4}}$, $\hat{B}_1 = \frac{\lambda_{h_2}}{\rho a_2}$, $\hat{B}_2 = \frac{2\lambda_{g_2}}{a_4\rho_{P_R}}$, $\hat{B}_3 = \frac{\xi a_3}{a_4}$, $\hat{B}_4 = \frac{\lambda_E}{a_4\rho_{P_R}}$, $\hat{\alpha}_1 = \hat{A}_1(1 - \hat{B}_3t)$, $\hat{\alpha}_2 = (\hat{A}_2 - \hat{B}_3)(1 - \hat{B}_3t)$, $\hat{\alpha}_3 = \hat{A}_3(1 - \hat{B}_3t)$, $\hat{\alpha}_4 = \hat{A}_4(1 - \hat{B}_3t)$, $\hat{\beta}_1 = \hat{A}_1 + \hat{B}_3$, $\hat{\beta}_2 = \hat{A}_2$, $\hat{\beta}_3 = \hat{A}_3(1 - t\hat{B}_3) + (1+t)\hat{B}_3$, $\hat{\beta}_4 = \hat{A}_4(1 - t\hat{B}_3) + (1+t)\hat{B}_3$, $\hat{\delta}_3 = \hat{A}_3\hat{B}_3(1+t)$, $\hat{\delta}_4 = \hat{A}_4\hat{B}_3(1+t)$, $\hat{D}_1 = \frac{1-\hat{B}_3t}{\hat{B}_3}\left(\hat{B}_1 + \frac{\hat{B}_4}{t+1}\right)$, $\hat{D}_2 = \frac{\hat{B}_2}{\hat{B}_3(1-\hat{B}_3t)}$, $\hat{D}_3 = \hat{B}_4\frac{t}{t+1} - \frac{1}{\hat{B}_3}\left(\hat{B}_1 + \frac{\hat{B}_4}{t+1}\right) + \frac{\hat{B}_2}{\hat{B}_3}$, $C_j = \frac{\alpha_j\beta_j^2}{\prod_{i=1,i\neq j}^{5}(-\alpha_i\beta_j+\alpha_j\beta_i)}$,
$I(a,b,c) = e^{\frac{c}{a}-ab}E_1\big(\frac{(1+a)c}{a}\big) + \sum_{i=1}^{\infty}(-1)^i \frac{E_i(c)}{a^{i-1}} S_i(ab)$, $S_i(x) = \sum_{k=i}^{\infty}(-1)^k \frac{(x)^k}{k!}$,
$I_2(a,b,c) = \frac{1}{(1+a)a}e^{-(c+ab)} - \left(\frac{c}{a^2} + b\right)e^{\frac{c}{a}-ab}E_1\left(\frac{(1+a)c}{a}\right) + \sum_{i=1}^{\infty}(-1)^{i-1}\left(\frac{(i-1)}{a}S_i(ab) + bS_{i-1}(ab)\right)\frac{E_i(c)}{a^{i-1}}$, $\hat{C}_j = \frac{\hat{\alpha}_j\hat{\beta}_j}{\prod_{i=1,i\neq j}^{4}(-\hat{\alpha}_i\hat{\beta}_j+\hat{\alpha}_j\hat{\beta}_i)}$

TABLE I
SIMULATION PARAMETERS

Parameter	Symbol	Values
Distance between R and S_1	d_{S_1}	0.25 m
Distance between R and S_2	d_{S_2}	0.50 m
Distance between R and D_1	d_{D_1}	0.50 m
Distance between R and D_2	d_{D_2}	0.25 m
Distance between D_1 and D_2	$d_{D_1-D_2}$	1 m
Distance between R, D_1, D_2 and E	d_E	1 m
Path Loss Factor	v	4
Transmit SNR	$\frac{P_T}{\sigma^2}$, $\frac{P_R}{\sigma^2}$,	0-30 dB
Transmit SNR	$\frac{P_{D_1}}{\sigma^2}$, $\frac{P_{D_2}}{\sigma^2}$	0-30 dB
Residual Self-interference	$\sigma^2_{D_1(nsi)}$	1
Residual Self-interference	$\sigma^2_{D_2(nsi)}$	1
Secrecy Target Data Rate for S_1	R_1	0.2 bps/Hz
Secrecy Target Data Rate for S_2	R_2	0.2 bps/Hz
Residual Interfering Signal	ξ	10^{-4}
Fixed Power Factor for NOMA	a_1	0.6
Fixed Power Factor for NOMA	a_2	0.4
Fixed Power Factor for NOMA	a_3	0.9
Fixed Power Factor for NOMA	a_4	0.1

IV. NUMERICAL RESULTS AND DISCUSSIONS

This section verifies our derived mathematical analysis for the ESSR and SOP of the considered system with the Monte-Carlo simulation results. Unless otherwise stated, the simulation parameters used for the experiments are listed in Table I. For the Monte-Carlo experiments, we have used MATLAB to average over 10^6 random realizations of Rayleigh fading channels, i.e., h_1, h_2, g_1, g_2 g_3, g_4, g_E, g_{D_1} and g_{D_2}.

In Fig. 4, we plot the ESSR for the considered system for both pSIC and ipSIC cases under the presence of eavesdropper E. For comparison, we also plot the system's effective Ergodic capacity. We can clearly observe that the presence of an eavesdropper in the system results in a decrease in ESSR. Also, the imperfect SIC in the system tends to lower the ESSR. The difference in ESSR and the Ergodic sum capacity of the system for both pSIC and ipSIC cases is less at lower transmit SNR, i.e. less than 10 dB. However, the difference is clearly visible at higher transmit SNR. Moreover, the analytical results completely match the simulation results. This indicates that our derived mathematical analysis is correct. For our considered system model, when the destination D_1 and D_2 nodes transmit jamming signal to the eavesdropper E while receiving the information signal from the common relay node R, they tend to create interference on each other as well. This will also affect the ESSR achieved by the system. In the next-generation wireless architecture, the destination nodes will often adopt advanced interference cancellation techniques so that they can completely cancel the interference caused by each other [38]. When the destination node D_1 and D_2 can completely cancel the interference while transmitting the jamming signal to the eavesdropper E, a higher ESSR can be achieved for both pSIC and ipSIC cases as depicted in Fig. 5. For this scenario, we refer to them as No-Int case. From Fig. 5, we can observe that, in the No-Int case, ESSR is almost double for the pSIC case compared to the ESSR where destination nodes cannot cancel the effect of the jamming signal on each other.

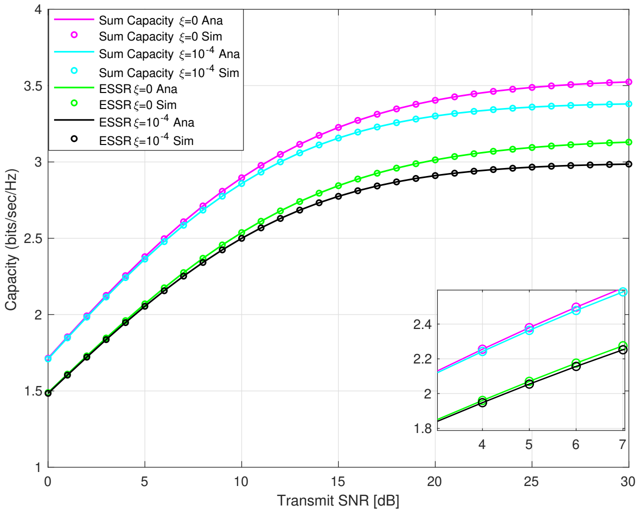


Fig. 4. Sum Capacity and ESSR of the System

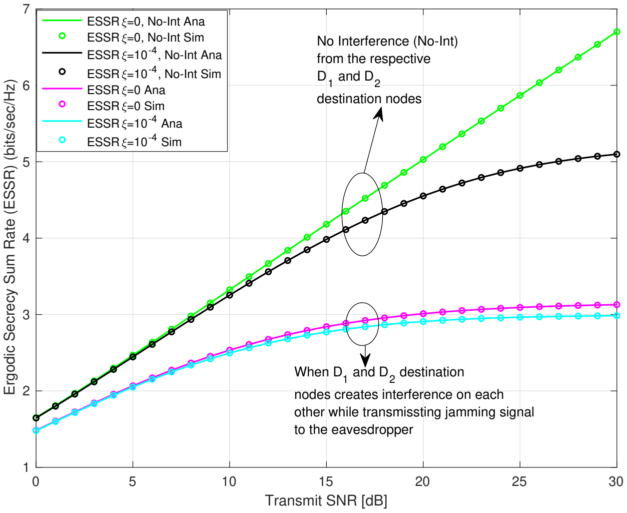


Fig. 5. Comparison of ESSR with or without Interfering Signal

We have used uplink NOMA in the first stage for the transmission of S_1 and S_2 data symbols to the common relay node R. Then we used downlink NOMA in the second stage for the transmission of decoded symbols at R to the respective destination nodes D_1 and D_2. The users S_1, S_2, D_1, and D_2 are placed at a certain distance from the relay node R in a way that uplink NOMA can be utilized in the first stage and downlink NOMA can be used in the second stage. Hence, following the principle of uplink and downlink NOMA, their power allocation coefficients also play an important role in the ESSR performance of the system, as shown in Fig. 6 and Fig. 7, respectively. Fig. 6 and Fig. 7 are plotted at a transmit SNR of 15 dB. From Fig. 6, we can see that the ESSR for both the

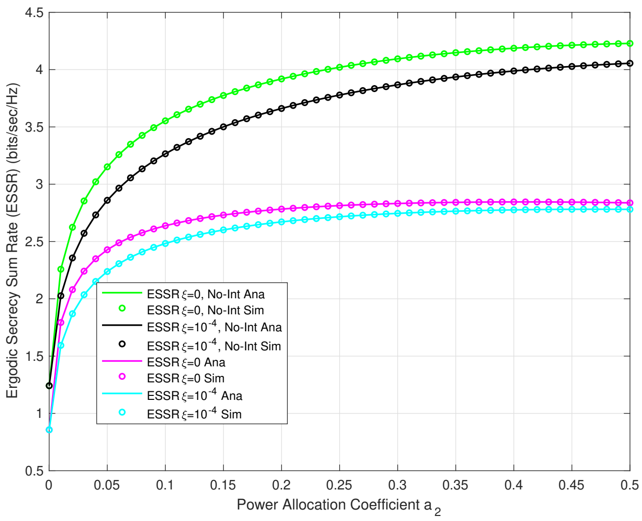


Fig. 6. ESSR vs NOMA Power Allocation Co-efficient a_2

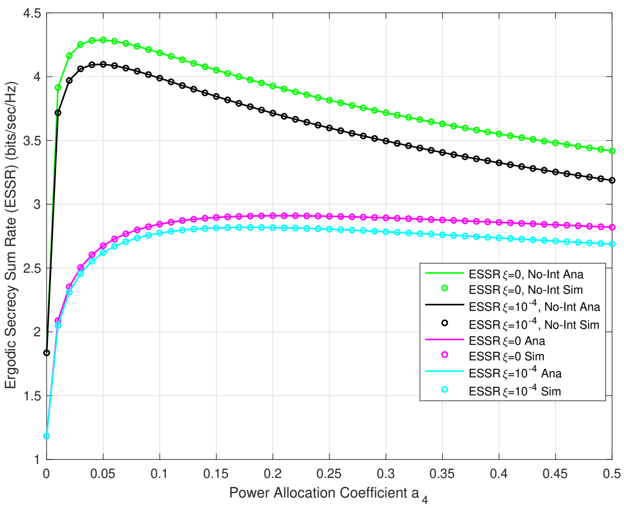


Fig. 7. ESSR vs NOMA Power Allocation Co-efficient a_4

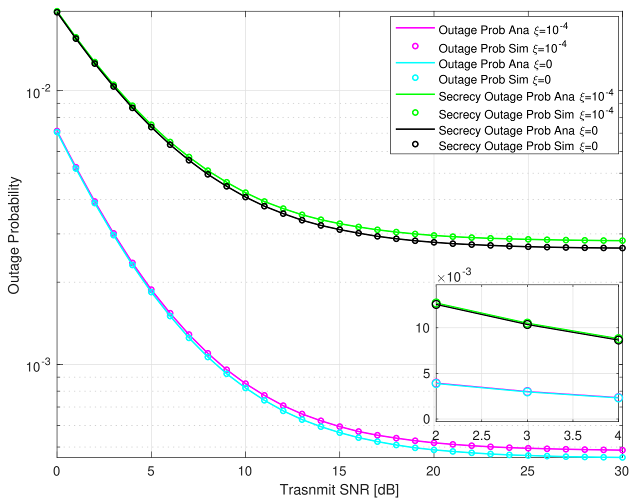


Fig. 8. Outage Probability and SOP of the System

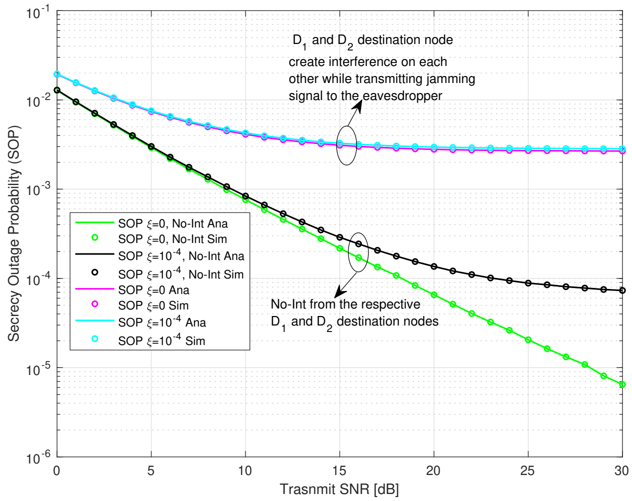


Fig. 9. Comparison of SOP with or without Interfering Signal

No-Int case and interfering case increases with the increase in NOMA power allocation coefficient a_2. However, as shown in Fig. 7, the ESSR of the system first increases with the increase in NOMA power allocation coefficient a_4, and then it starts decreasing. Therefore, it depicts that a suitable choice of NOMA power allocation coefficients can further increase the ESSR of the system. This also indicates that a dynamic power allocation for NOMA can increase the ESSR of the system instead of having a fixed power allocation.

In Fig. 8, we plot the secrecy outage probability of the system for both pSIC, and ipSIC cases against different transmit SNR values. For comparison, we also plot the system's effective outage probability. We can clearly observe that the presence of an eavesdropper in the system tends to increase the SOP of the considered system. In Fig. 8, we also see that the outage probability is much lower when there is no eavesdropper in the system. Also, ipSIC increases the SOP and outage probability as expected. The difference between pSIC and ipSIC is higher at transmitting SNR greater than 10 dB. In addition, the analytical results completely match the simulation results indicating that our derived mathematical analysis is correct.

Similar to Fig. 5, in Fig. 9, we tested the SOP of the considered system when destination nodes D_1 and D_2 can completely cancel the effect of the interference on each other while transmitting the jamming signal to the eavesdropper. From Fig. 9, we can observe that, in the No-Int case, a significant decrease in the SOP can be achieved compared to the SOP where destination nodes cannot cancel the effect of the jamming signal on each other. This means that when the interference caused by destination nodes on each other is considered, the secrecy outage performance is the worst. Thus, the destination node should be placed far from each other to create less interference on each other while transmitting the jamming signal to the eavesdropper.

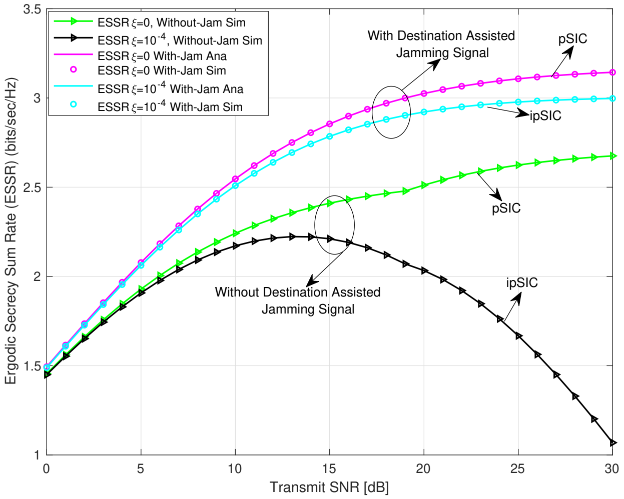


Fig. 10. Comparison of ESSR with or without Destination Assisted Jamming Signals

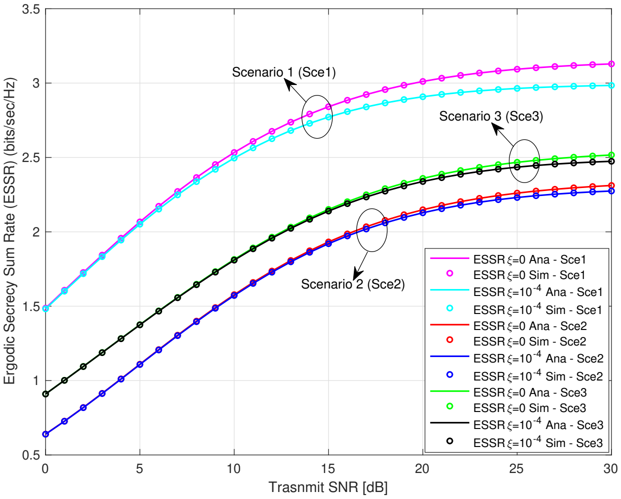


Fig. 12. Effect of Distances on ESSR Performance

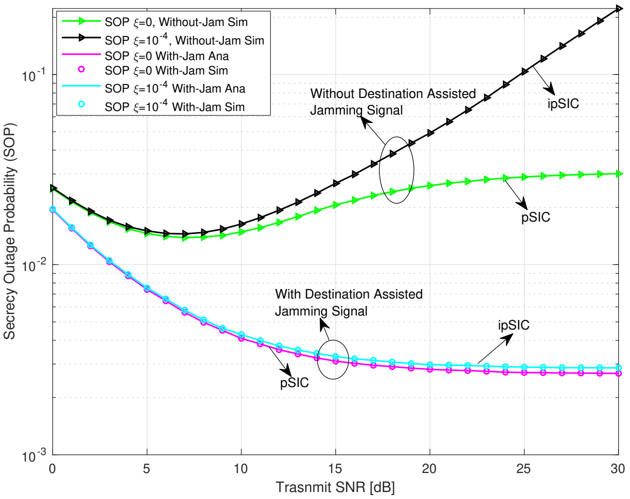


Fig. 11. Comparison of SOP with or without Destination Assisted Jamming Signals

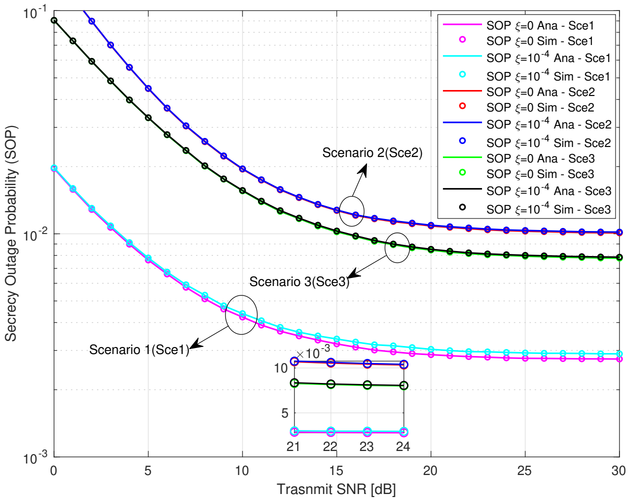


Fig. 13. Effect of Distances on SOP Performance

In Fig. 10 and Fig. 11, we compare the ESSR and SOP of the considered system without destination-assisted jamming signals. We can clearly observe in Fig. 10 that a higher ESSR can be achieved with destination-assisted jamming signals for both pSIC and ipSIC cases compared to those without destination-assisted jamming signals. Similarly, in Fig. 11, we notice that the destination-assisted jamming signal can decrease the SOP of the considered system. Also, without destination-assisted jamming signals, the SOP tends to increase even at higher transmit SNR, i.e, greater than 10 dB. Therefore, it can be assured that the destination-assisted jamming signals can improve the system security and thus ensure reliable communication.

In Fig. 12 and Fig. 13, we measure the impact of distances on the ESSR and SOP performance of the system, respectively. Specifically, we created three scenarios, namely, Scenario 1 (Sce1), Scenario 2 (Sce2), and Scenario 3 (Sce3). Sce1 is a reference scenario for our system model where the distance parameters are taken as outlined in Table 1. In Sce2, the relay is placed closer to S_1 and S_2 nodes and far away from D_1 and D_2 nodes. Also, the distances between D_1 and D_2 nodes and eavesdropper distance from D_1, D_2, and the relay node is increased. The parameters in Sec2 are: $d_{S_1} = 0.15m$, $d_{S_2} = 0.25m$, $d_{D_1} = 0.75m$, $d_{D_2} = 0.50m$, $d_E = 1.5m$ and $d_{D_1-D_2} = 1.5m$. Similarly, in Sce3, the relay is placed closer to D_1 and D_2 nodes and far away from S_1 and S_2 nodes. Also, the distances between D_1 and D_2 nodes and eavesdropper distance from D_1, D_2, and the relay node are reduced. The parameters in Sec3 are: $d_{S_1} = 0.50m$, $d_{S_2} = 0.75m$, $d_{D_1} = 0.25m$, $d_{D_2} = 0.15m$, $d_E = 0.5m$ and $d_{D_1-D_2} = 0.5m$. From Fig. 12 and 13, we observe that out of all these three scenarios, Sce1 gives the higher ESSR and lower SOP performance for our system model compared to Sce2 and Sce3. It is due to the fact that the relay, source, and destination nodes are placed in a way that will get the benefit of both uplink and downlink NOMA during transmission, and the destination nodes can effectively transmit jamming signals to the eavesdropper while decoding their own signals from the relay node with reduced interference on each other. However, Sce2 gives the worst ESSR and SOP performance compared to Sec1 and Sce3, as shown in Fig. 12 and Fig. 13, respectively. Although in Sce2, the distance between D_1 and D_2 is increased, which decreases the inference between them, these destination nodes require more power to emit a jamming signal to confuse the eavesdropper that is located far away from them. However, in Sce3, the destination nodes D_1 and D_2 require less power to emit a jamming signal to confuse the eavesdropper located near them. Therefore, as pointed out in Fig. 12 and Fig. 13, the relay, source, and destination nodes should be placed efficiently for reduced interference and to benefit both uplink and downlink NOMA, thereby enhancing its ESSR and lowering its SOP performance.

V. Conclusions and Future Work

In this paper, we studied the secrecy performance analysis of a NOMA system in a cooperative relay sharing scenario using uplink and downlink NOMA. We have proposed a destination-assisted jamming scheme where the two destination node emits a jamming signal to the eavesdropper to improve the system's secrecy performance. We derived the analytical expressions for the Ergodic secrecy sum rate and secrecy outage probability of the considered system under the pSIC and ipSIC scenarios. Our results indicated that a positive ESSR and a lower SOP could be attained with a destination-assisted jamming signal. Therefore, a reliable secrecy performance of the system can be assured. Our results also demonstrate that the NOMA power allocation coefficients and ipSIC affect the target secrecy rate performance of the system. Therefore, a perfect SIC technique and a dynamic power allocation scheme can further enhance the secrecy performance of the system. Finally, our results also showed that a significantly higher ESSR and lower SOP could be achieved with destination-assisted jamming signals for both pSIC and ipSIC cases compared to conventional NOMA without destination-assisted jamming signals.

For future work, we would like to study the dynamic power allocation scheme that will further enhance the security performance of the considered system. The application of artificial intelligence methods to physical-layer security to make future communications more intelligent is also an interesting research direction for our future work.

Appendix I
Proof of Theorem 1

Let $\gamma = \min\left(\gamma_{R\to x_1}, \gamma_{D_2\to R,\hat{x_1}}, \gamma_{D_1\to R,\hat{x_1}}\right)$

$$F_\gamma(\gamma) = \Pr\left(\min\left(\gamma_{R\to x_1}, \gamma_{D_2\to R,\hat{x_1}}, \gamma_{D_1\to R,\hat{x_1}}\right) < \gamma\right)$$

$$F_\gamma(\gamma) = \Pr\left(\min\left(\frac{\rho a_1 X_1}{\rho a_2 X_2 + 1}, \frac{a_3\rho_{P_R} Y_2}{a_4\rho_{P_R} Y_2 + \phi\rho_{D_1} W_1 + 1 + 1}, \right.\right.$$
$$\left.\left.\frac{a_3\rho_{P_R} Y_1}{a_4\rho_{P_R} Y_1 + \phi\rho_{D_2} W_2 + 1 + 1}\right) < \gamma\right)$$

where, $|h_1|^2 \sim X_1, |h_2|^2 \sim X_2, |g_1|^2 \sim Y_1, |g_2|^2 \sim Y_2$, $|g_{D_1}|^2 \sim W_1, |g_{D_2}|^2 \sim W_2, \frac{P_R}{\sigma_R^2} = \rho_{P_R}, \sigma^2_{D_2(nsi)} = 1$, $\sigma^2_{D_2} = 1, \sigma^2_{D_1(nsi)} = 1, \sigma^2_{D_1} = 1$

$$= 1 - \underbrace{\Pr\left(\frac{\rho a_1 X_1}{\rho a_2 X_2 + 1} \geq \gamma\right)}_{I_1} \underbrace{\Pr\left(\frac{a_3\rho_{P_R} Y_2}{a_4\rho_{P_R} Y_2 + \phi\rho_{D_1} W_1 + 2}\right.}_{I_2}$$
$$\underbrace{\left.\geq \gamma\right)} \underbrace{\Pr\left(\frac{a_3\rho_{P_R} Y_1}{a_4\rho_{P_R} Y_1 + \phi\rho_{D_2} W_2 + 2} \geq \gamma\right)}_{I_3}$$

Now, $I_1 = \Pr\left(\frac{\rho a_1 X_1}{\rho a_2 X_2 + 1} \geq \gamma\right)$

Conditioning I_1 on X_2,

$$I_1 = \int_{x_2=0}^{\infty} \Pr\left(X_1 \geq \frac{a_2\gamma x_2}{a_1} + \frac{\gamma}{\rho a_1}\right) f_{X_2}(x_2)dx_2$$

$$I_1 = \int_{x_2=0}^{\infty} e^{-\left(\frac{\gamma a_2 \lambda_{h_1} x_2}{a_1} + \frac{\lambda_{h_1}\gamma}{\rho a_1}\right)} \lambda_{h_2} e^{-\lambda_{h_2} x_2} dx_2$$

After some algebraic calculations, we get:

$$I_1 = \frac{\lambda_{h_2} e^{-\frac{\lambda_{h_1}\gamma}{\rho a_1}}}{\left(\frac{\gamma a_2 \lambda_{h_1}}{a_1} + \lambda_{h_2}\right)}$$

$$I_2 = \Pr\left(\frac{a_3\rho_{P_R} Y_2}{a_4\rho_{P_R} Y_2 + \phi\rho_{D_1} W_1 + 1 + 1} \geq \gamma\right)$$

$$I_2 = \Pr\left(Y_2 \geq \frac{\phi\rho_{D_1} W_1\gamma + 2\gamma}{\rho_{P_R}(a_3 - \gamma a_4)}\right)$$

Conditioning I_2 on W_1, we get:

$$I_2 = \int_{w_1=0}^{\infty} \Pr\left(Y_2 \geq \frac{\phi\rho_{D_1} w_1\gamma + 2\gamma}{\rho_{P_R}(a_3 - \gamma a_4)}\right) f_{W_1}(w_1)dw_1$$

$$I_2 = \int_{w_1=0}^{\infty} e^{-\frac{(\phi\rho_{D_1} w_1\gamma + 2\gamma)\lambda_{g_2}}{\rho_{P_R}(a_3-\gamma a_4)}} \lambda_{w_1} e^{-\lambda_{w_1} w_1} dw_1$$

After some algebraic calculations, we get:

$$I_2 = \frac{\lambda_{w_1} e^{-\frac{2\gamma\lambda_{g_2}}{\rho_{P_R}(a_3-\gamma a_4)}}}{\left(\frac{\phi\rho_{D_1}\gamma\lambda_{g_2}}{\rho_{P_R}(a_3-\gamma a_4)} + \lambda_{w_1}\right)}$$

Similarly,

$$I_3 = \Pr\left(\frac{a_3\rho_{P_R} Y_1}{a_4\rho_{P_R} Y_1 + \phi\rho_{D_2} W_2 + 2} \geq \gamma\right)$$

$$I_3 = \frac{\lambda_{w_2} e^{-\frac{2\gamma\lambda_{g_1}}{\rho_{P_R}(a_3-\gamma a_4)}}}{\left(\frac{\phi\rho_{D_2}\gamma\lambda_{g_1}}{\rho_{P_R}(a_3-\gamma a_4)} + \lambda_{w_2}\right)}$$

Therefore,

$F_\gamma(\gamma) = 1 - I_1 I_2 I_3$

The EC in terms of CDF $F_\gamma(\gamma)$ can be written as:

$$C_{x_1}^{Ana} = \frac{1}{2\ln 2}\int_{\gamma=0}^{\infty} \frac{1}{1+\gamma}[1 - F_\gamma(\gamma)]d\gamma$$

$$C_{x_1}^{Ana} = \frac{1}{2\ln 2}\int_{\gamma=0}^{\frac{a_3}{a_4}} \frac{1}{1+\gamma} \frac{\lambda_{h_2} e^{-\frac{\lambda_{h_1}\gamma}{\rho a_1}}}{\left(\frac{\gamma a_2\lambda_{h_1}}{a_1} + \lambda_{h_2}\right)} \times$$

$$\frac{\lambda_{w_1}\lambda_{w_2}e^{-\frac{2\gamma(\lambda_{g_1}+\lambda_{g_2})}{\rho_{P_R}(a_3-\gamma a_4)}}}{\left(\frac{\phi\rho_{D_1}\gamma\lambda_{g_2}}{\rho_{P_R}(a_3-\gamma a_4)}+\lambda_{w_1}\right)\left(\frac{\phi\rho_{D_2}\gamma\lambda_{g_1}}{\rho_{P_R}(a_3-\gamma a_4)}+\lambda_{w_2}\right)}d\gamma$$

Let, $x = \frac{\gamma}{a_3 - \gamma a_4} \rightarrow \gamma = \frac{a_3 x}{1 + a_4 x}$, then

$$C_{x_1}^{Ana} = \frac{a_3}{2\ln 2}\int_{x=0}^{\infty}\frac{1}{(1+Ax)}\frac{1}{(1+Bx)}\frac{1}{(1+Cx)}\frac{e^{-\frac{Ex}{1+a_4x}-Fx}}{(1+Dx)}dx$$

where, $A = a_3 + a_4, B = a_4 + \frac{\lambda_{h_1}a_2a_3}{\lambda_{h_2}a_1}, C = \frac{\phi\rho_{D_1}\lambda_{g_2}}{\rho_{P_R}\lambda_{w_1}}$, $D = \frac{\phi\rho_{D_2}\lambda_{g_1}}{\rho_{P_R}\lambda_{w_2}}, E = \frac{\lambda_{h_1}a_3}{\rho a_1}$ and $F = \frac{2(\lambda_{g_1}+\lambda_{g_2})}{\rho_{P_R}}$

Now, by partial fraction method, we get,

$$C_{x_1}^{Ana} = \frac{a_3}{2\ln 2}\left(\frac{A^3}{(A-B)(A-C)(A-D)}\int_{x=0}^{\infty}\frac{e^{-\frac{Ex}{1+a_4x}-Fx}}{(1+Ax)}dx - \frac{B^3}{(A-B)(B-C)(B-D)}\int_{x=0}^{\infty}\frac{e^{-\frac{Ex}{1+a_4x}-Fx}}{(1+Bx)}dx + \frac{C^3}{(A-B)(B-C)(C-D)}\int_{x=0}^{\infty}\frac{e^{-\frac{Ex}{1+a_4x}-Fx}}{(1+Cx)}dx - \frac{D^3}{(A-D)(B-D)(C-D)}\int_{x=0}^{\infty}\frac{e^{-\frac{Ex}{1+a_4x}-Fx}}{(1+Dx)}dx\right)$$

Now, in order to solve the integral, we introduce $y = 1 + a_4x$ as new integration variable. We then find,

$$\int_{x=0}^{\infty}\frac{e^{-\frac{Ex}{1+a_4x}-Fx}}{(1+Ax)}dx = \frac{e^{\frac{F-E}{a_4}}}{a_4 - A}\int_{y=1}^{\infty}\frac{e^{\frac{E}{a_4}\frac{1}{y}-\frac{F}{a_4}y}}{(1+\frac{A}{a_4-A}y)}dy$$

$$= \frac{e^{\frac{F-E}{a_4}}}{A}I\left(\frac{A}{a_4-A}, \frac{E}{a_4}, \frac{F}{a_4}\right)$$

where, $I(a,b,c) = a\int_{y=1}^{\infty}\frac{e^{\frac{b}{y}-cy}}{1+ay}dy$ and $I(a,b,c)$ can be expressed in summation series as:

$$I(a,b,c) = e^{\frac{c}{a}-ab}E_1\left(\frac{(1+a)c}{a}\right) + \sum_{i=1}^{\infty}(-1)^i\frac{E_i(c)}{a^{i-1}}S_i(ab)$$

where, $S_i(x) = \sum_{k=i}^{\infty}(-1)^k\frac{(x)^k}{k!}$

Hence, we have,

$$C_{x_1}^{Ana} = \frac{a_3e^{\frac{F-E}{a_4}}}{2\ln 2}\left(\frac{A^2I(\frac{A}{a_4-A},\frac{E}{a_4},\frac{F}{a_4})}{(A-B)(A-C)(A-D)} - \frac{B^2I(\frac{B}{a_4-B},\frac{E}{a_4},\frac{F}{a_4})}{(A-B)(B-C)(B-D)} + \frac{C^2I(\frac{C}{a_4-C},\frac{E}{a_4},\frac{F}{a_4})}{(A-C)(B-C)(C-D)} - \frac{D^2I(\frac{D}{a_4-D},\frac{E}{a_4},\frac{F}{a_4})}{(A-D)(B-D)(C-D)}\right)$$

This ends the proof of Theorem 1.

Appendix II
Proof of Theorem 3

The CDF of $\gamma_{E\rightarrow x_1}$ can be expressed as:

$$F_\gamma(\gamma) = \Pr\left(\frac{a_3\rho_{P_R}E}{\rho_{D_1}Y_3 + \rho_{D_2}Y_4 + 1} < \gamma\right)$$

$$F_\gamma(\gamma) = 1 - \underbrace{\Pr\left(\frac{a_3\rho_{P_R}E}{\rho_{D_1}Y_3 + \rho_{D_2}Y_4 + 1} \geq \gamma\right)}_{I_4}$$

where, $|g_E|^2 \sim E, |g_3|^2 \sim Y_3, |g_4|^2 \sim Y_4, \sigma_E^2 = 1$

Now,

$$I_4 = \Pr\left(E \geq \frac{\rho_{D_1}\gamma Y_3}{a_3\rho_{P_R}} + \frac{\rho_{D_2}\gamma Y_4}{a_3\rho_{P_R}} + \frac{\gamma}{a_3\rho_{P_R}}\right)$$

Conditioning I_4 on Y_3 and Y_4, we get,

$$I_4 = \int_{y_3=0}^{\infty}\int_{y_4=0}^{\infty}\Pr\left(E \geq \frac{\rho_{D_1}\gamma y_3}{a_3\rho_{P_R}} + \frac{\rho_{D_2}\gamma y_4}{a_3\rho_{P_R}} + \frac{\gamma}{a_3\rho_{P_R}}\right)\times f_{Y_3}(y_3)f_{Y_4}(y_4)dy_3dy_4$$

$$I_4 = \int_{y_3=0}^{\infty}\int_{y_4=0}^{\infty}e^{-\left(\frac{\rho_{D_1}\gamma y_3\lambda_E}{a_3\rho_{P_R}}+\frac{\rho_{D_2}\gamma y_4\lambda_E}{a_3\rho_{P_R}}+\frac{\gamma\lambda_E}{a_3\rho_{P_R}}\right)}\times \lambda_{g_3}e^{-\lambda_{g_3}y_3}\lambda_{g_4}e^{-\lambda_{g_4}y_4}dy_3dy_4$$

$$I_4 = \int_{y_3=0}^{\infty}\int_{y_4=0}^{\infty}\lambda_{g_3}\lambda_{g_4}e^{-\frac{\gamma\lambda_E}{a_3\rho_{P_R}}}e^{-\left(\frac{\rho_{D_1}\gamma\lambda_E}{a_3\rho_{P_R}}+\lambda_{g_3}\right)y_3}\times e^{-\left(\frac{\rho_{D_2}\gamma\lambda_E}{a_3\rho_{P_R}}+\lambda_{g_4}\right)y_4}dy_3dy_4$$

After some algebraic calculations, we get:

$$I_4 = \frac{\lambda_{g_3}\lambda_{g_4}e^{-\frac{\gamma\lambda_E}{a_3\rho_{P_R}}}}{\left(\frac{\rho_{D_1}\gamma\lambda_E}{a_3\rho_{P_R}}+\lambda_{g_3}\right)\left(\frac{\rho_{D_2}\gamma\lambda_E}{a_3\rho_{P_R}}+\lambda_{g_4}\right)}$$

Therefore,

$F_\gamma(\gamma) = 1 - I_4$

The EC in terms of CDF $F_\gamma(\gamma)$ can be expressed as:

$$C_{E\rightarrow x_1}^{Ana} = \frac{1}{2\ln 2}\int_{\gamma=0}^{\infty}\frac{1}{1+\gamma}[1 - F_\gamma(\gamma)]d\gamma$$

$$C_{E\rightarrow x_1}^{Ana} = \frac{1}{2\ln 2}\int_{\gamma=0}^{\infty}\frac{1}{1+\gamma}\frac{\lambda_{g_3}\lambda_{g_4}e^{-\frac{\gamma\lambda_E}{a_3\rho_{P_R}}}}{\left(\frac{\rho_{D_1}\gamma\lambda_E}{a_3\rho_{P_R}}+\lambda_{g_3}\right)\left(\frac{\rho_{D_2}\gamma\lambda_E}{a_3\rho_{P_R}}+\lambda_{g_4}\right)}$$

Now, we take, $A_1 = \frac{\rho_{D_1}\lambda_E}{a_3\rho_{P_R}\lambda_{g_3}}, B_1 = \frac{\rho_{D_2}\lambda_E}{a_3\rho_{P_R}\lambda_{g_4}}$, and $C_1 = \frac{\lambda_E}{a_3\rho_{P_R}}$

$$C_{E\rightarrow x_1}^{Ana} = \frac{1}{2\ln 2}\int_{\gamma=0}^{\infty}\frac{1}{1+\gamma}\frac{e^{-C_1\gamma}}{(1+A_1\gamma)(1+B_1\gamma)}d\gamma$$

By partial fraction method, we get,

$$C_{E\rightarrow x_1}^{Ana} = \frac{1}{2\ln 2}\left(\frac{1}{(1-A_1)(1-B_1)}\int_{\gamma=0}^{\infty}\frac{e^{-C\gamma}}{(1+\gamma)}d\gamma - \frac{A_1^2}{(1-A_1)(A_1-B_1)}\int_{\gamma=0}^{\infty}\frac{e^{-C_1\gamma}}{(1+A\gamma)}d\gamma + \frac{B_1^2}{(1-A_1)(A_1-B_1)}\times \int_{\gamma=0}^{\infty}\frac{e^{-C_1\gamma}}{(1+B_1\gamma)}d\gamma\right.$$

We now consider the integral, $\int_{\gamma=0}^{\infty}\frac{e^{-C_1\gamma}}{(1+A_1\gamma)}d\gamma$

Taking $z = 1 + A_1\gamma$ as new integration variable, we get,

$$\int_{\gamma=0}^{\infty} \frac{e^{-C_1\gamma}}{(1+A_1\gamma)} d\gamma = \frac{e^{\frac{C_1}{A_1}} E_1\left(\frac{C_1}{A_1}\right)}{A_1}$$

where $E_1(.)$ is an exponential integral of order 1.

Therefore,

$$C_{E\to x_1}^{Ana} = \frac{1}{2\ln 2}\left(\frac{e^{C_1}E_1(C_1)}{(1-A_1)(1-B_1)} - \frac{A_1 e^{\frac{C_1}{A_1}} E_1\left(\frac{C_1}{A_1}\right)}{(1-A_1)(A_1-B_1)} + \right.$$

$$\left. \frac{B_1 e^{\frac{C_1}{B_1}} E_1\left(\frac{C_1}{B_1}\right)}{(1-A_1)(A_1-B_1)}\right)$$

This ends the proof of Theorem 3.

Appendix III Proof of Theorem 5

Let us first evaluate,

$$SOP_{x_1} = 1 - \Pr(C_{Sec,x_1} > R_1)$$

$$SOP_{x_1} = 1 - \Pr\left(\frac{1}{2}\log_2\left(1+\min\left(\gamma_{R\to x_1}, \gamma_{D_2\to R,\hat{x}_1}, \gamma_{D_1\to R,\hat{x}_1}\right)\right)\right.$$

$$\left. -\frac{1}{2}\log_2\left(1+\gamma_{E\to x_1}\right) > R_1\right)$$

$$SOP_{x_1} = 1 - \Pr\left(\frac{1}{2}\log_2\left(\frac{1+\min\left(\gamma_{R\to x_1}, \gamma_{D_2\to R,\hat{x}_1}, \gamma_{D_1\to R,\hat{x}_1}\right)}{(1+\gamma_{E\to x_1})}\right)\right.$$

$$\left. > R_1\right)$$

$$SOP_{x_1} = 1 - \Pr\left(\log_2\left(\frac{1+\min\left(\gamma_{R\to x_1}, \gamma_{D_2\to R,\hat{x}_1}, \gamma_{D_1\to R,\hat{x}_1}\right)}{(1+\gamma_{E\to x_1})}\right)\right.$$

$$\left. > 2R_1\right)$$

Applying Log on both sides,

$$SOP_{x_1} = 1 - \Pr\left(\left(\frac{1+\min\left(\gamma_{R\to x_1}, \gamma_{D_2\to R,\hat{x}_1}, \gamma_{D_1\to R,\hat{x}_1}\right)}{(1+\gamma_{E\to x_1})}\right)\right.$$

$$\left. > 2^{2R_1}\right)$$

$$SOP_{x_1} = 1 - \Pr\left(\left(1+\min\left(\gamma_{R\to x_1}, \gamma_{D_2\to R,\hat{x}_1}, \gamma_{D_1\to R,\hat{x}_1}\right)\right)\right.$$

$$\left. > 2^{2R_1}(1+\gamma_{E\to x_1})\right)$$

$$SOP_{x_1} = 1 - \Pr\left(\left(\min\left(\gamma_{R\to x_1}, \gamma_{D_2\to R,\hat{x}_1}, \gamma_{D_1\to R,\hat{x}_1}\right)\right)\right.$$

$$\left. > (2^{2R_1}-1) + 2^{2R_1}\gamma_{E\to x_1}\right)$$

Let, $(2^{2R_1}-1) = t$

$$SOP_{x_1} = 1 - \Pr\left(\left(\min\left(\gamma_{R\to x_1}, \gamma_{D_2\to R,\hat{x}_1}, \gamma_{D_1\to R,\hat{x}_1}\right)\right)\right.$$

$$\left. > t + (t+1)\gamma_{E\to x_1}\right)$$

$$SOP_{x_1} = 1 - \Pr\left(Z_1 > t + (t+1)Z_2\right)$$

where Z_1 and Z_2 are independent random variables and,

$Z_1 = \min\left(\gamma_{R\to x_1}, \gamma_{D_2\to R,\hat{x}_1}, \gamma_{D_1\to R,\hat{x}_1}\right)$ and $Z_2 = \gamma_{E\to x_1}$

From Theorem 1 and Theorem 3, the distribution functions for these two random variables are already found to be:

$$1 - F_{Z_1}(\gamma) = \frac{\lambda_{h_2} e^{-\frac{\lambda_{h_1}\gamma}{\rho a_1}}}{\left(\frac{\gamma a_2 \lambda_{h_1}}{a_1} + \lambda_{h_2}\right)}$$

$$\frac{\lambda_{w_1}\lambda_{w_2} e^{-\frac{2\gamma(\lambda_{g_1}+\lambda_{g_2})}{\rho_{P_R}(a_3-\gamma a_4)}}}{\left(\frac{\phi\rho_{D_1}\gamma\lambda_{g_2}}{\rho_{P_R}(a_3-\gamma a_4)} + \lambda_{w_1}\right)\left(\frac{\phi\rho_{D_2}\gamma\lambda_{g_1}}{\rho_{P_R}(a_3-\gamma a_4)} + \lambda_{w_2}\right)} d\gamma$$

$$1 - F_{Z_2}(\gamma) = \frac{\lambda_{g_3}\lambda_{g_4} e^{-\frac{\gamma\lambda_E}{a_3\rho_{P_R}}}}{\left(\frac{\rho_{D_1}\gamma\lambda_E}{a_3\rho_{P_R}} + \lambda_{g_3}\right)\left(\frac{\rho_{D_2}\gamma\lambda_E}{a_3\rho_{P_R}} + \lambda_{g_4}\right)}$$

Now, conditioning SOP_{x_1} on $Z_2 = z$, we get,

$$SOP_{x_1} = 1 - \int_{z=0}^{\infty} \Pr\left(Z_1 > t + (t+1)z\right) f_{Z_2}(z) dz$$

$SOP_{x_1} = 1 - \int_{z=0}^{\infty} \left(1 - F_{Z_1}(t+(t+1)z)\right) f_{Z_2}(z) dz$ where the PDF of Z_2 is the derivative of $F_{Z_2}(z)$ which is found to be:

$$f_{Z_2}(z) = F'_{Z_2}(z) = \frac{e^{-\frac{\lambda_E}{a_3\rho_{P_R}}z}}{\left(1+\frac{\rho_{D_1}\lambda_E}{a_3\rho_{P_R}\lambda_{g_3}}z\right)\left(1+\frac{\rho_{D_2}\lambda_E}{a_3\rho_{P_R}\lambda_{g_4}}z\right)} \times$$

$$\left(\frac{\lambda_E}{a_3\rho_{P_R}} + \frac{\frac{\rho_{D_1}\lambda_E}{a_3\rho_{P_R}\lambda_{g_3}}}{1+\frac{\rho_{D_1}\lambda_E}{a_3\rho_{P_R}\lambda_{g_3}}z} + \frac{\frac{\rho_{D_2}\lambda_E}{a_3\rho_{P_R}\lambda_{g_4}}}{1+\frac{\rho_{D_2}\lambda_E}{a_4\rho_{P_R}\lambda_{g_4}}z}\right)$$

Now, we can express SOP_{x_1} as:

$$SOP_{x_1} = 1 - \int_{z=0}^{\frac{a_3-ta_4}{a_4(t+1)}} \frac{e^{-\frac{\lambda_{h_1}(t+(t+1)z)}{\rho a_1}}}{\left(1+\frac{\lambda_{h_1}a_2(t+(t+1)z)}{\lambda_{h_2}a_1}\right)} \times$$

$$\frac{e^{-\frac{2(\lambda_{g_1}+\lambda_{g_2})}{\rho_{P_R}}\frac{(t+(t+1)z)}{a_3-(t+(t+1)z)a_4}}}{\left(1+\frac{\phi\rho_{D_1}\lambda_{g_2}}{\rho_{P_R}\lambda_{w_1}}\frac{(t+(t+1)z)}{a_3-(t+(t+1)z)a_4}\right)\left(1+\frac{\phi\rho_{D_2}\lambda_{g_1}}{\rho_{P_R}\lambda_{w_2}}\frac{(t+(t+1)z)}{a_3-(t+(t+1)z)a_4}\right)} \times$$

$$\frac{e^{-\frac{\lambda_E}{a_3\rho_{P_R}}z}}{\left(1+\frac{\rho_{D_1}\lambda_E}{a_3\rho_{P_R}\lambda_{g_3}}z\right)\left(1+\frac{\rho_{D_2}\lambda_E}{a_3\rho_{P_R}\lambda_{g_4}}z\right)}\left(\frac{\lambda_E}{a_3\rho_{P_R}} + \frac{\frac{\rho_{D_1}\lambda_E}{a_3\rho_{P_R}\lambda_{g_3}}}{1+\frac{\rho_{D_1}\lambda_E}{a_3\rho_{P_R}\lambda_{g_3}}z} + \right.$$

$$\left. \frac{\frac{\rho_{D_2}\lambda_E}{a_3\rho_{P_R}\lambda_{g_4}}}{1+\frac{\rho_{D_2}\lambda_E}{a_4\rho_{P_R}\lambda_{g_4}}z}\right) dz$$

To simplify the notation, we introduce the following constants:

$$A_1 = \frac{\lambda_{h_1}a_2}{\lambda_{h_2}a_1}, A_2 = \frac{\phi\rho_{D_1}\lambda_{g_2}}{a_3\rho_{P_R}\lambda_{w_1}}, A_3 = \frac{\phi\rho_{D_2}\lambda_{g_1}}{a_3\rho_{P_R}\lambda_{w_2}},$$

$$A_4 = \frac{\rho_{D_1}\lambda_E}{a_3\rho_{P_R}\lambda_{g_3}}, A_5 = \frac{\rho_{D_2}\lambda_E}{a_3\rho_{P_R}\lambda_{g_4}}, B_1 = \frac{\lambda_{h_1}}{\rho a_1},$$

$$B_2 = \frac{2(\lambda_{g_1} + \lambda_{g_2})}{a_3\rho_{P_R}}, B_3 = \frac{a_4}{a_3}, B_4 = \frac{\lambda_E}{a_3\rho_{P_R}}$$

Hence,

$$SOP_{x_1} = 1 - \int_{z=0}^{\frac{1-tB_3}{B_3(t+1)}} \frac{e^{-B_1(t+(t+1)z)}}{(1 + A_1(t + (t+1)z))}\times$$
$$\frac{e^{-B_2\frac{(t+(t+1)z)}{1-(t+(t+1)z)B_3}}}{\left(1 + A_2\frac{(t+(t+1)z}{1-(t+(t+1)z)B_3}\right)\left(1 + A_3\frac{(t+(t+1)z}{1-(t+(t+1)z)B_3}\right)}$$
$$\frac{e^{-B_4z}}{(1 + A_4z)(1 + A_5z)}\left(B_4 + \frac{A_4}{1 + A_4z} + \frac{A_5}{1 + A_5z}\right)dz$$

Taking $y = t + (t+1)z$, $x = \frac{y}{1 - B_3y}$, $w = 1 + B_3x$ and finally $w = \frac{v}{1 - B_3t}$ as new integration variables and after some algebraic calculations, we get,

$$SOP_{x_1} = 1 - (1+t)(1 - B_3t)^3B_3^4e^{D_3}\int_{v=1}^{\infty}\frac{ve^{\frac{D_1}{v}}e^{-D_2v}}{\prod_{i=1}^{5}(-\alpha_i + \beta_iv)}\times$$
$$\left(B_4 + \frac{\delta_4v}{-\alpha_4 + \beta_4v} + \frac{\delta_5v}{-\alpha_5 + \beta_5v}\right)dv$$

where, $\alpha_1 = A_1(1 - B_3t), \alpha_2 = (A_2 - B_3)(1 - B_3t)$, $\alpha_3 = (A_3 - B_3)(1 - B_3t), \alpha_4 = A_4(1 - B_3t), \alpha_5 = A_5(1 - B_3t)$, $\beta_1 = A_1 + B_3, \beta_2 = A_2, \beta_3 = A_3, \beta_4 = A_4(1 - tB_3) + (1+t)B_3$, $\beta_5 = A_5(1 - tB_3) + (1+t)B_3, \delta_4 = A_4B_3(1+t)$, $\delta_5 = A_5B_3(1+t)$,

$D_1 = \frac{1 - B_3t}{B_3}\left(B_1 + \frac{B_4}{t+1}\right), D_2 = \frac{B_2}{B_3(1 - B_3t)}$, and

$$D_3 = B_4\frac{t}{t+1} - \frac{1}{B_3}\left(B_1 + \frac{B_4}{t+1}\right) + \frac{B_2}{B_3}$$

By partial fraction method, we get,

$$SOP_{x_1} = 1 - (1+t)(1 - B_3t)^3B_3^4e^{D_3}\times$$
$$\left(B_4\sum_{j=1}^{5}C_jI\left(-\frac{\beta_j}{\alpha_j}, D_1, D_2\right)\right.$$
$$+\delta_4\sum_{j=1,j\neq4}^{5}\frac{\alpha_jC_j}{-\alpha_4\beta_j + \alpha_j\beta_4}\left[I\left(-\frac{\beta_j}{\alpha_j}, D_1, D_2\right)-\right.$$
$$\left.I\left(-\frac{\beta_4}{\alpha_4}, D_1, D_2\right)\right] + \frac{\delta_4C_4}{\alpha_4}I_2\left(-\frac{\beta_4}{\alpha_4}, D_1, D_2\right)+$$
$$\delta_5\sum_{j=1,j\neq5}^{5}\frac{\alpha_jC_j}{-\alpha_5\beta_j + \alpha_j\beta_5}\left[I\left(-\frac{\beta_j}{\alpha_j}, D_1, D_2\right)-\right.$$
$$\left.\left.I\left(-\frac{\beta_5}{\alpha_5}, D_1, D_2\right)\right] + \frac{\delta_5C_5}{\alpha_5}I_2\left(-\frac{\beta_5}{\alpha_5}, D_1, D_2\right)\right)$$

where C_j is the product defined by:

$$C_j = \frac{\alpha_j\beta_j^2}{\prod_{i=1,i\neq j}^{5}(-\alpha_i\beta_j + \alpha_j\beta_i)} \text{ and}$$

$$I(a,b,c) = a\int_{y=1}^{\infty}\frac{e^{\frac{b}{y}-cy}}{1 + ay}dy$$

$I(a,b,c)$ can be expressed in summation series as:

$$I(a,b,c) = e^{\frac{c}{a}-ab}E_1\left(\frac{(1+a)c}{a}\right) + \sum_{i=1}^{\infty}(-1)^i\frac{E_i(c)}{a^{i-1}}S_i(ab)$$

where, $S_i(x) = \sum_{k=i}^{\infty}(-1)^k\frac{(x)^k}{k!}$ and,

$$I_2(a,b,c) = \int_{y=1}^{\infty}\frac{e^{\frac{b}{y}-cy}}{(1 + ay)^2}dy,$$

$I_2(a,b,c)$ can also be expressed in summation series as:

$$I_2(a,b,c) = \frac{1}{(1+a)a}e^{-(c+ab)} - \left(\frac{c}{a^2} + b\right)e^{\frac{c}{a}-ab}E_1\left(\frac{(1+a)c}{a}\right)+$$
$$\sum_{i=1}^{\infty}(-1)^{i-1}\left(\frac{(i-1)}{a}S_i(ab) + bS_{i-1}(ab)\right)\frac{E_i(c)}{a^{i-1}}$$

Now, by following the similar steps as for the derivation of SOP_{x_1}, SOP_{x_2} can be expressed as:

$$SOP_{x_2} = 1 - (1+t)(1 - \hat{B}_3t)^2\hat{B_3}^3e^{\hat{D}_3}\left(\hat{B}_4\sum_{j=1}^{4}\hat{C}_jI\left(-\frac{\hat{\beta}_j}{\hat{\alpha}_j}, \hat{D}_1, \hat{D}_2\right)\right.$$
$$+\hat{\delta}_3\sum_{j=1,j\neq3}^{4}\frac{\hat{\alpha}_j\hat{C}_j}{-\hat{\alpha}_3\hat{\beta}_j + \hat{\alpha}_j\hat{\beta}_3}\left[I\left(-\frac{\hat{\beta}_j}{\hat{\alpha}_j}, \hat{D}_1, \hat{D}_2\right)-\right.$$
$$\left.I\left(-\frac{\hat{\beta}_3}{\hat{\alpha}_3}, \hat{D}_1, \hat{D}_2\right)\right] + \frac{\hat{\delta}_3\hat{C}_3}{\hat{\alpha}_3}I_2\left(-\frac{\hat{\beta}_3}{\hat{\alpha}_3}, \hat{D}_1, \hat{D}_2\right)+$$
$$\hat{\delta}_4\sum_{j=1,j\neq4}^{4}\frac{\hat{\alpha}_j\hat{C}_j}{-\hat{\alpha}_4\hat{\beta}_j + \hat{\alpha}_j\hat{\beta}_4}\left[I\left(-\frac{\hat{\beta}_j}{\hat{\alpha}_j}, \hat{D}_1, \hat{D}_2\right)-\right.$$
$$\left.\left.I\left(-\frac{\hat{\beta}_4}{\hat{\alpha}_4}, \hat{D}_1, \hat{D}_2\right)\right] + \frac{\hat{\delta}_4\hat{C}_4}{\hat{\alpha}_4}I_2\left(-\frac{\hat{\beta}_4}{\hat{\alpha}_4}, \hat{D}_1, \hat{D}_2\right)\right)$$

where, $\hat{A}_1 = \frac{\lambda_{h_2}a_1\xi}{\lambda_{h_1}a_2}, \hat{A}_2 = \frac{\phi\rho_{D_1}\lambda_{g_2}}{a_4\rho_{P_R}\lambda_{w_1}}, \hat{A}_3 = \frac{\rho_{D_1}\lambda_E}{a_4\rho_{P_R}\lambda_{g_3}}$, $\hat{A}_4 = \frac{\rho_{D_2}\lambda_E}{a_4\rho_{P_R}\lambda_{g_4}}, \hat{B}_1 = \frac{\lambda_{h_2}}{\rho a_2}, \hat{B}_2 = \frac{2\lambda_{g_2}}{a_4\rho_{P_R}}$, $\hat{B}_3 = \frac{\xi a_3}{a_4}, \hat{B}_4 = \frac{\lambda_E}{a_4\rho_{P_R}}$, $\hat{\alpha}_1 = \hat{A}_1(1 - \hat{B}_3t), \hat{\alpha}_2 = (\hat{A}_2 - \hat{B}_3)(1 - \hat{B}_3t), \hat{\alpha}_3 = \hat{A}_3(1 - \hat{B}_3t)$, $\hat{\alpha}_4 = \hat{A}_4(1 - \hat{B}_3t), \hat{\beta}_1 = \hat{A}_1 + \hat{B}_3, \hat{\beta}_2 = \hat{A}_2, \hat{\beta}_3 = \hat{A}_3(1 - t\hat{B}_3)+$ $(1+t)\hat{B}_3, \hat{\beta}_4 = \hat{A}_4(1 - t\hat{B}_3) + (1+t)\hat{B}_3, \hat{\delta}_3 = \hat{A}_3\hat{B}_3(1+t)$, $\hat{\delta}_4 = \hat{A}_4\hat{B}_3(1+t), \hat{D}_1 = \frac{1 - \hat{B}_3t}{\hat{B}_3}\left(\hat{B}_1 + \frac{\hat{B}_4}{t+1}\right)$,

$$\hat{D}_2 = \frac{\hat{B}_2}{\hat{B}_3(1 - \hat{B}_3t)}, \hat{D}_3 = \hat{B}_4\frac{t}{t+1} - \frac{1}{\hat{B}_3}\left(\hat{B}_1 + \frac{\hat{B}_4}{t+1}\right) + \frac{\hat{B}_2}{\hat{B}_3}$$

and $\hat{C}_j$ is the product defined by:

$$\hat{C}_j = \frac{\hat{\alpha}_j\hat{\beta}_j}{\prod_{i=1,i\neq j}^{4}(-\hat{\alpha}_i\hat{\beta}_j + \hat{\alpha}_j\hat{\beta}_i)}$$

Now, by substituting the derived expression for SOP_{x_1}, and SOP_{x_2}, we finally get the SOP of considered system as in Equation 26.

This completes the proof of Theorem 5.

References

[1] S. Wang, T. Sun, H. Yang, X. Duan, and L. Lu, "6g network: Towards a distributed and autonomous system," in *2020 2nd 6G wireless summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[2] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6g wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 28–41, 2019.

[3] D. Reinsel, J. Gantz, and J. Rydning, "Data age 2025: The digitization of the world from edge to core," *Seagate https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf*, 2018.

[4] A. H. Sodhro, S. Pirbhulal, Z. Luo, K. Muhammad, and N. Z. Zahid, "Toward 6g architecture for energy-efficient communication in iot-enabled smart automation systems," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5141–5148, 2020.

[5] U. Gustavsson, P. Frenger, C. Fager, T. Eriksson, H. Zirath, F. Dielacher, C. Studer, A. Pärssinen, R. Correia, J. N. Matos *et al.*, "Implementation challenges and opportunities in beyond-5g and 6g communication," *IEEE Journal of Microwaves*, vol. 1, no. 1, pp. 86–100, 2021.

[6] A. Rauniyar, P. Engelstad, and J. Moen, "A new distributed localization algorithm using social learning based particle swarm optimization for internet of things," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*. IEEE, 2018, pp. 1–7.

[7] M. A. Jamshed, K. Ali, Q. H. Abbasi, M. A. Imran, and M. Ur-Rehman, "Challenges, applications and future of wireless sensors in internet of things: a review," *IEEE Sensors Journal*, 2022.

[8] S. C. Mukhopadhyay, S. K. S. Tyagi, N. K. Suryadevara, V. Piuri, F. Scotti, and S. Zeadally, "Artificial intelligence-based sensors for next generation iot applications: a review," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 24 920–24 932, 2021.

[9] A. Rauniyar, P. Engelstad, and O. N. Østerbø, "Capacity enhancement of noma-swipt iot relay system with direct links over rayleigh fading channels," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, p. e3913, 2020.

[10] A. Rauniyar, A. Yazidi, P. Engelstad, and O. N. Østerbo, "A reinforcement learning based game theoretic approach for distributed power control in downlink noma," in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*. IEEE, 2020, pp. 1–10.

[11] Y. Ma, Z. Yuan, W. Li, and Z. Li, "Novel solutions to noma based modern random access for 6g enabled iot," *IEEE Internet of Things Journal*, 2021.

[12] Z. Wu, K. Lu, C. Jiang, and X. Shao, "Comprehensive study and comparison on 5g noma schemes," *IEEE Access*, vol. 6, pp. 18 511–18 519, 2018.

[13] W. U. Khan, F. Jameel, M. A. Jamshed, H. Pervaiz, S. Khan, and J. Liu, "Efficient power allocation for noma-enabled iot networks in 6g era," *Physical Communication*, vol. 39, p. 101043, 2020.

[14] H. Nikopour and H. Baligh, "Sparse code multiple access," in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2013, pp. 332–336.

[15] N. M. Balasubramanya, A. Gupta, and M. Sellathurai, "Combining code-domain and power-domain noma for supporting higher number of users," in *2018 IEEE global communications conference (GLOBECOM)*. IEEE, 2018, pp. 1–6.

[16] 3rd Generation Partnership Project (3GPP), "Study on downlink multi-user superposition transmission for LTE, TSG RAN Meeting 67," *Tech. Rep. RP-150496*, Mar 2015.

[17] O. Maraqa, A. S. Rajasekaran, S. Al-Ahmadi, H. Yanikomeroglu, and S. M. Sait, "A survey of rate-optimal power domain noma with enabling technologies of future wireless networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2192–2235, 2020.

[18] M. F. Kader, M. B. Shahab, and S. Y. Shin, "Exploiting non-orthogonal multiple access in cooperative relay sharing," *IEEE Communications Letters*, vol. 21, no. 5, pp. 1159–1162, 2017.

[19] A. Rauniyar, P. E. Engelstad, and O. N. Østerbø, "On the performance of bidirectional noma-swipt enabled iot relay networks," *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2299–2315, 2020.

[20] A. Rauniyar, P. Engelstad, and O. N. Østerbø, "An adaptive user pairing strategy for uplink non-orthogonal multiple access," in *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*. IEEE, 2020, pp. 1–7.

[21] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive non-orthogonal multiple access for cellular iot: Potentials and limitations," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 55–61, 2017.

[22] M. B. Shahab, R. Abbas, M. Shirvanimoghaddam, and S. J. Johnson, "Grant-free non-orthogonal multiple access for iot: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1805–1838, 2020.

[23] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[24] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.

[25] Y. Ai, M. Cheffena, T. Ohtsuki, and H. Zhuang, "Secrecy performance analysis of wireless sensor networks," *IEEE Sensors letters*, vol. 3, no. 5, pp. 1–4, 2019.

[26] T. D. Hieu, T. T. Duy, and B.-S. Kim, "Performance enhancement for multihop harvest-to-transmit wsns with path-selection methods in presence of eavesdroppers and hardware noises," *IEEE Sensors Journal*, vol. 18, no. 12, pp. 5173–5186, 2018.

[27] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[28] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2016.

[29] 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 Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[30] B. Wang, G. Feng, W. Guo, Y. Sun, and Y. Liu, "Achievable rate of beamforming dual-hop relay network with a jammer and eh constraint," *IEEE Sensors Journal*, vol. 20, no. 17, pp. 10 123–10 129, 2020.

[31] Y. Ren, Y. Tan, M. Makhanbet, and X. Zhang, "Improving physical layer security of cooperative noma system with wireless-powered full-duplex relaying," *Information*, vol. 12, no. 7, p. 279, 2021.

[32] K. Shim, T. N. Do, T.-V. Nguyen, D. B. da Costa, and B. An, "Enhancing phy-security of fd-enabled noma systems using jamming and user selection: Performance analysis and dnn evaluation," *IEEE Internet of Things Journal*, 2021.

[33] H. Lei, Z. Yang, K.-H. Park, I. S. Ansari, G. Pan, and M.-S. Alouini, "On physical layer security of multiple-relay assisted noma systems," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2019, pp. 1–6.

[34] H. Li, Y. Chen, M. Zhu, J. Sun, D.-T. Do, V. G. Menon, and P. Shynu, "Secrecy outage probability of relay selection based cooperative noma for iot networks," *IEEE Access*, vol. 9, pp. 1655–1665, 2020.

[35] M.-S. Van Nguyen, D.-T. Do, F. Afghah, S. R. Islam, and A.-T. Le, "Exploiting secrecy performance of uplink noma in cellular networks," *IEEE Access*, vol. 9, pp. 95 135–95 154, 2021.

[36] D. Xu, "Proactive eavesdropping of suspicious non-orthogonal multiple access networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13 958–13 963, 2020.

[37] Z. Zhang, Z. Ma, M. Xiao, Z. Ding, and P. Fan, "Full-duplex device-to-device-aided cooperative nonorthogonal multiple access," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 5, pp. 4467–4471, 2016.

[38] C. D. Nwankwo, L. Zhang, A. Quddus, M. A. Imran, and R. Tafazolli, "A survey of self-interference management techniques for single frequency full duplex systems," *IEEE Access*, vol. 6, pp. 30 242–30 268, 2017.

ASHISH RAUNIYAR is currently working as a Research Scientist at SINTEF Digital, Norway. He received his Ph.D. Degree in Computer Science from the University of Oslo, Norway in 2021. He was a graduate research assistant at Wireless Emerging Networking System (WENS) Lab, where he completed his Master's degree in IT Convergence Engineering at Kumoh National Institute of Technology, South Korea. He was a recipient of Best Paper Awards at 2020 IEEE 43rd International Conference on Telecommunications and Signal Processing (TSP), Milan, Italy, 28th IEEE International Telecommunication Networks and Applications Conference (ITNAC), 2018, Sydney, Australia, and AI-DLDA 2018 International Summer School on Artificial Intelligence, Udine-Italy, 2018. He was a winner of the European Satellite Navigation Competition (ESNC) in 2017. He was also selected as "Top 200 Young Researchers in Computer Science & Mathematics" and invited to attend Heidelberg Laureate Forum, Heidelberg, Germany in 2017, and Global Young Scientist Summit, Singapore in 2020. His main research area includes 5G/6G Signal Processing, Autonomous Systems and Networks, Internet of Things, Machine Learning, Wireless Communications, and Computer Networking.

OLAV N. ØSTERBØ received his M.Sc. in Applied Mathematics from the University of Bergen in 1980 and his Ph.D. from NTNU in 2004. He joined Telenor in 1980 and has more than 30 years of experience in telecom research. Activities in recent years have been related to QoS and performance analysis. Current research topics include Traffic Modeling, Analysis of Interference in Radio Networks, Scheduling, Traffic Differentiation, and M2M.

JAN ERIK HÅKEGÅRD received the degree Sivilingeniør (M.Sc.) in 1990 from the Department of Electronical Engineering and Informatics, The Norwegian Institute of Technology (NTH), Trondheim, Norway. In 1997 he received a Docteur (Ph.D.) degree in Electronics and Communications at ENST, site de Toulouse, France. Since 1997, he has been with SINTEF Digital, working on research and development projects related to various types of wireless communication systems. He is currently leading SINTEF activities within the Satellite and Terrestrial Communication Systems.

PAAL E. ENGELSTAD received a Bachelor's Degree in Physics from the Norwegian University of Science and Technology (NTNU) in 1993, a Master's Degree (Hons.) in Physics from NTNU/Kyoto University, Japan, in 1994, the Ph.D. Degree in Computer Science from the University of Oslo in 2005. He is currently a Full Professor with the Autonomous Systems and Sensor Technologies Research Group, Department of Technology Systems, University of Oslo. He is also a Research Scientist at the Norwegian Defence Research Establishment and a Professor II at Oslo Metropolitan University. He holds a number of patents and has been publishing a number of papers over the past years. His current research interests include Fixed, Wireless, and Adhoc Networking, Cybersecurity, Machine Learning, and Distributed and Autonomous Systems.