IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 May 2024, accepted 18 June 2024, date of publication 21 June 2024, date of current version 28 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3417619

RESEARCH ARTICLE

Multi-Objective Optimization-Based GA in PLS of IRS-Assisted PDNOMA Communication

THUC KIEU-XUAN[1], HONG NGUYEN-THI[2], AND ANH LE-THI[1]
[1]Faculty of Information Technology, Hanoi University of Industry, Hanoi, Vietnam
[2]Posts and Telecommunications Institute of Technology, Hanoi, Vietnam

Corresponding author: Anh Le-Thi (leanh@haui.edu.vn)

This work was supported by Hanoi University of Industry under Grant 19-2023-RD/HD-DHCN.

ABSTRACT The intelligent reflecting surface (IRS) supports communication systems well, especially in physical layer security for the cooperative power domain non-orthogonal multiple access (PDNOMA). In this work, we investigate the secrecy performance of PDNOMA with the assistance of the IRS and a multiple-relaying network in the presence of an eavesdropper. Three selection strategies are considered at the relaying network to boost the system's performance: the first method is based on the best relay selection, the second on the max-min concept, and the third on harmonious characteristics. Moreover, the phase shift of IRS element and power allocation for each NOMA user can be controlled to improve the secrecy quality and reduce the influence of an eavesdropper (E). Besides, applying the technique of transmitting artificial noise (AN) from the source is also considered in this paper to interfere with the signal at E. Furthermore, in this paper, we determine two primary metrics to evaluate the secrecy performance of our proposed system: the worst secrecy capacity and secrecy energy efficiency. The balance of these two metrics needs to be assured to improve the secrecy performance. Thus, in this paper, we consider the multi-object problem and propose the genetic algorithm-based approach, a non-dominated sorting genetic algorithm with three procedures (NSGA-II), to solve this problem. Then, to highlight the proposed algorithm's outstanding performance, we compare it with other algorithms, Reference point based NSGA-II (R-NSGA-II) and the exhaustive search (ES). Additionally, the impacts of critical system parameters are investigated for both cases as IRS and none-IRS assistance comprises three relaying selection techniques, the number of IRS elements, the strength of AN signal, the distances of source-relay link, relay-IRS link, and IRS-Eavesdropper link. Finally, the summaries of these archived results show the benefits of our proposed model in different cases of the deployment of the IRS and without the IRS.

INDEX TERMS IRS-assisted PDNOMA, non-dominated sorting genetic algorithm, multi-objective optimization, worst secrecy capacity, secrecy energy efficiency.

I. INTRODUCTION

With the rapid development of wireless techniques, the 5G (fifth generation) network generation has been widely launched worldwide. Technology constantly evolves, and the world's research community is moving towards the new generation of networks - the sixth generation (6G). The core technologies that will be applied in future networks, such as Beyond-5G (B5G) and 6G, including artificial intelligence, massive MIMO network technology, THz communication, quantum communication, intelligent reflecting surfaces (IRS), non-orthogonal multiple access (NOMA) technologies, etc have been pointed out. References [1], [2], and [3] show that NOMA and IRS are potential applications to B5G and 6G networks for improving the high efficiency in resource use, serving many users and devices simultaneously, expanding coverage, and declaring savings in development costs. However, as the number of users in the IRS/NOMA application network increases, the threat of security attacks will also increase [4], [5]. Thus, the problem is how to maintain the security performance of wireless systems against the risk of attacks is necessary. The challenging

The associate editor coordinating the review of this manuscript and approving it for publication was Adnan M. Abu-Mahfouz.

question posed is how to simultaneously achieve the security effectiveness of the system across various performance metrics of a communication system. The multi-objective algorithms can solve this problem. Moreover, optimization problems using conventional mathematical algorithms will be challenging to apply to complex networks with massive users, such as NOMA-aided IRS. Therefore, improving the quality of the NOMA network with the support of the IRS in general and enhancing the quality of security in particular has been a hot topic recently. In information and communication technology, evolutionary computation, such as Genetic algorithm (GA) or algorithms-based GA, is part of Artificial Intelligence (AI) that is applied as an optimal technique to achieve high efficiency and low operating costs [6], [7]. Low dynamic response calculation time can be performed in real-time, especially for the algorithms applied for the multi-objective, which is also a benefit of these evolutionary algorithms.

A. BACKGROUND

As one of the key technologies that will be widely applied to future generation B5G and 6G networks, Artificial Intelligence will help improve and automate the services of these future network systems. Evolutionary computing is one of the critical techniques of AI, and research achievements in evolutionary computing are widely applied in life, science, and engineering, especially in telecommunication systems. References [6], [7], and [8] have shown the possibility of evolutionary computing for improving the quality of telecommunications networks with different problems. The most typical representative of evolutionary computing is the genetic algorithm that simulates the adaptive evolutionary process of biological populations based on Darwin's theory. GA is a random optimal search method that simulates evolution, inheritance, and the struggle for survival [9]. The critical difference between GA and other search methods is that GA maintains and processes a set of solutions called a population. In [10], [11], and [12], the essential benefits of GA in improving the performance of wireless sensor networks and Internet of Things (IoT) wireless networks are presented. Moreover, numerous factors demand consideration to ensure the efficient operation of wireless communication systems. Assessing the system's quality necessitates a balanced evaluation of performance metrics, particularly concerning the domain of physical layer security. Hence, it becomes imperative to encompass the system's security aspects alongside diverse metrics. While mathematical methodologies are commonly employed for single-objective optimization concerning convex functions, addressing intricate, non-convex, and multi-objective problems poses significant challenges. Consequently, meta-heuristic optimization algorithms, notably evolutionary-based approaches derived from Genetic Algorithms, emerge as pivotal tools. These algorithms have demonstrated efficacy in tackling complex multi-objective problems, particularly within the domain of telecommunication systems [13], [14], [15].

The IRS technique is considered one of the essential and breakthrough technological solutions that can be applied to 6G [2], [16]. The application of IRS in wireless systems will reduce the cost of deployment and still achieve spectrum efficiency and energy efficiency for future wireless networks thanks to many elements with low-cost operation [17], [18]. Specifically, the IRS is a meta-surface consisting of many configurable passive elements attached to an intelligent controller that allows dynamic adjustment of signal reflection for different purposes, such as enhancing signal power and eliminating interference. Reference [19] have provided a comprehensive overview of the benefits of IRS technology compared to other technological solutions. It presents empirical evidence showcasing the efficacy of IRS-facilitated wireless communication within novel contexts, integrating it with relevant technologies. Notably, within the context of relay scenarios augmented by the IRS, the plausibility of enhancing the system's physical layer security through this scheme is extensively deliberated upon. Furthermore, [20], [21], and [22] have recently shown the critical roles of the IRS in improving the performance of unmanned aerial vehicle (UAV) communications, vehicle-to-vehicle communication, cognitive radio networks, smart cities, etc.

Meanwhile, the NOMA technique in the power domain is considered a potential multiple access candidate for next-generation mobile networks [23], [24], especially since the application of NOMA can meet the massive connectivity requirement of the new 6G networks. An investigation into advanced multiple access methodologies centering on NOMA has been presented in [25]. The methodology aims to mitigate various challenges anticipated in the 6G landscape. These challenges encompass heterogeneous data traffic, accommodating extensive connectivity, achieving ultrahigh bandwidth efficiency, and meeting the stringent demands for ultra-low latency. Typically, extant NOMA schemes can be categorized broadly into two classifications: power-domain NOMA (PDNOMA) and code-domain NOMA [26]. PDNOMA focuses on uneven power distribution among users, helping to make the most of the communication capacity within the same physical resource. This technique does not require additional bandwidth to improve spectrum efficiency, so it does not require significant changes in the infrastructure aspect [27]. Thus, this technique effectively enhances system performance and optimizes network resource utilization in current communication systems. Additionally, it also enables the system to serve a massive number of users while ensuring stable and quality communications in environments with limited radio resources.

Therefore, combining the PDNOMA technique with IRS is a potential solution to increase network capacity, optimize resource allocation, reduce deployment, and save costs [4], [28], [29]. The energy efficiency of IRS-supported NOMA for 6G wireless communication has been presented in [30] by optimizing the active beam-forming and power allocation factors of users. Moreover, [31] considered a joint optimization of the time allocation factor and phase shift matrices in

the IRS wireless-powered NOMA IoT network. This study showed the sum throughput enhancement and critical benefits by IRS compared with no IRS. At the same time, [29] and [32] have investigated the sum rate optimization of IRS with NOMA and highlighted the critical advantages of IRS. In other cases, [33], [34], [35], [36], [37], and [38] have investigated the NOMA communication with the assistance of the IRS and demonstrated the outstanding results that the IRS delivers compared to not applying to the IRS. In there, [35] has considered both IRS with NOMA system and IRS with orthogonal multiple access system (OMA) in which a big IRS surface has divided into sub-surfaces to reduce the implementation complexity.

In addition, network security concerns are always a hot topic for future networks, B5G, and 6G [39]. Developing solutions to enhance secure transmission capabilities in wireless environments is a complex problem that requires focused research. Due to how signals are transmitted in radio communications, the information transmitted from the transceiver to the receiver may be eavesdropped. One of the security studies in wireless communications is to exploit jamming signals, including artificial jamming signals, to improve secrecy performance and protect against dangerous risks from attackers [40]. However, research results on enhancing security for B5G and 6G with non-orthogonal multiple access techniques and the assistance of the IRS still need to be improved. The secrecy performance of the NOMA network with IRS and no IRS cases and application of the jamming technique has been studied in [41], [42], [43], and [44]. These have presented the advantage of jamming technical methods in improving the system's security.

B. MOTIVATION AND CONTRIBUTIONS

From the analysis above, we can see that many research works have studied NOMA with the assistance of the IRS and have provided different methods to improve the security quality of these systems. However, these studies still need to comprehensively analyze an optimal solution using evolutionary computation, such as genetic algorithm and variants of GA for both single-objective and multi-objective problems. Currently, we especially realized that no publications consider the application of evolutionary algorithms to enhance the secrecy performance of the NOMA system, specifically bolstered by the IRS, encompassing various relay node selection strategies in scenarios involving the presence of an eavesdropping node. Moreover, the multi-objective optimization-based GA is the most popular method and can solve non-convex problems with constraint conditions [45], [49]. Therefore, in this study, we exploit the advantages of an evolutionary algorithm, such as NSGA-II, and compare them with other techniques, like R-NSGA-II and Exhaustive Search (ES), to address the problem of improving the secrecy performance in the NOMA cooperative relay network with the IRS. Our main contributions are listed as follows:

- (1) To our current understanding, this study represents the inaugural endeavor aimed at scrutinizing and refining the IRS-assisted relaying NOMA network in the presence of an Eavesdropper. Additionally, the investigation evaluates the impact of various relay selection approaches on the overall secrecy performance.
- (2) We are the first to have designed an NSGA-II algorithm with three procedures - a fast non-dominated sorting (FNDS), a fast crowding distance calculator (CDC), and a simple CCO (Crowded Comparison operator) tailored to address the multi-objective optimization challenge within our proposed system model. This algorithm optimizes power allocation coefficients to enhance the secrecy performance across two key metrics: the secrecy capacity-worst (SCW) and secrecy energy efficiency (SEE).
- (3) The assessment involves an evaluation of the security efficacy exhibited by the pertinent system, considering scenarios with and without the assistance of the IRS. Furthermore, it entails a comparative analysis between the outcomes generated by the proposed NSGA-II algorithm and alternative algorithms like R-NSGA-II and the ES algorithm. This comparative study aims to ascertain the efficacy and comparative performance of NSGA-II in relation to the aforementioned algorithms.
- (4) Finally, we performed simulation evaluations under different scenarios to examine the system's secrecy performance on both SCW and SEE metrics, precisely convergence behavior and computation time, the decision-making alterations, the number of IRS elements, relaying selection methods, location of IRS and Eavesdropper, the strength of artificial noise, and signal-to-noise ratio (SINR) at Eavesdropper.

The rest of this manuscript's structure is as follows: Section II encompasses the System model, which is further subdivided into three distinct subsections labeled A, B, and C. Section III pertains to Performance analysis and comprises four subsections denoted A, B, C, and D. Subsequently, Section IV encompasses seven subsections dedicated to experiment conduction and result analysis. The paper culminates with the conclusions drawn in Section V.

II. SYSTEM MODEL

We consider a NOMA cooperative transmission downlink system with the IRS planar. We assume an eavesdropping device, E, is used to evaluate the system's security. In the model illustrated in Figure 1, the system includes two wireless propagation phases: the first phase is the S-Relay cluster wireless connection, and the second phase, which uses the IRS to improve the transmission environment, is the radio link from the selected relay to the users. Specifically, the source node S implements NOMA multi-user superposition encode [26], while K relays in the same cluster use a cooperative forwarding protocol to forward signals to the users. In a cooperative transmission network, the amplify-and-forward protocol (AF) or the decoder-to-forward protocol (DF) is adopted [27]. In this study, we consider the relaying network

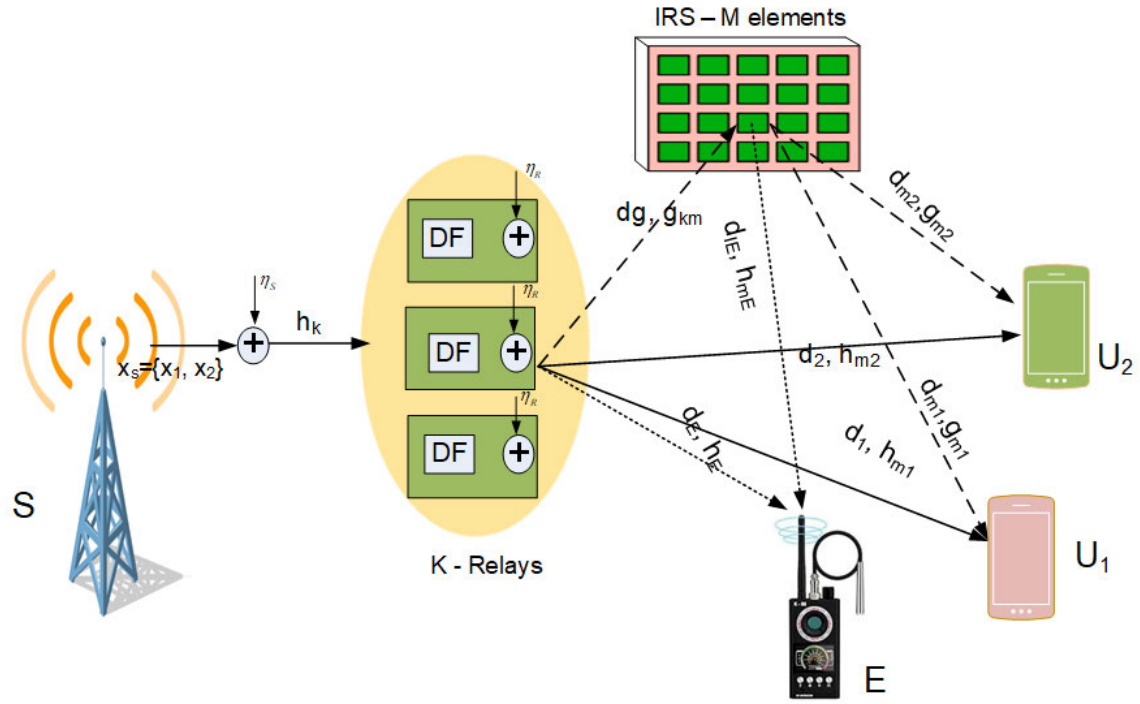


FIGURE 1. IRS-aid NOMA for EH relaying networks.

that uses the DF approach to forward the relay's received signal to destination users.

The number of relay nodes in a cluster includes K nodes. In particular, relay selection strategies rely on channel state information (CSI) to select the most reasonable relay node. We also investigated several relay node selection strategies listed by formula (2)(3)(4).

Currently, two popular techniques in physical layer security are applied to reduce the influence of eavesdroppers, which are artificial noise (AN) and jamming [40]. In this research, we consider the case of exploiting AN, meaning that the selected relay will transmit additional AN with different transmitting power levels. In this study, we assume that the AN technique is applied at the selected relay using pre-coding technology, and the AN signal is embedded in the transmitted signal to improve the system's secrecy performance.

In the second phase, the intelligence reflective surface is deployed to improve the transmission environment by reflecting the incident signal from the selected relay (R_b) to the IRS elements. The IRS planar comprises M separate elements that are re-configurable passive units. Each element can induce a change in amplitude and phase for the incident signal. Adjusting the phase-shift variable and amplitude-reflection coefficient to each element independently can enhance the link quality and boost the coverage considerably [47].

In this study, we focus on improving the secrecy performance of the NOMA system in total, including the secrecy data rate sum of both U_1 and U_2, by applying the proposed multi-objective optimization approach and controlling the phase shift of IRS elements. Thus, we don't consider the control of phase shift for separate users. As a result, the users' received signal is the vector sum of the connections, including the R_b-users connection and the IRS-users reflected signal. The terminal users include the legal users and one illegal node. Terminal legal devices use successive interference cancellation (SIC) technology to decode their signals, while the eavesdropper, we consider both cases using SIC and not. The SIC technique is an effective candidate to decode the superposed information at each NOMA receiver. The SIC receiver first decodes the stronger signal, subtracts it from the combined signal, and isolates the weaker one from the residue.

In the following subsections, we present our proposed system's mathematical model, signal transmission model, and signal-to-noise ratio model.

A. CHANNEL MODEL

Consider every part of the system to be in the same cell. There are two wireless propagation stages in the system. First, the link between the BS and the relay cluster, with the distance denoted by d_0. Assume there are obstructions and no line of sight (LoS) links in the transmission space connecting the BS to the relay. The channel is a Rayleigh block fading that is identical and independent. Let's denote h_k as the channel coefficient of the link between the BS and the *kth* relay in the K-Relays cluster $h_k \sim CN(0, \delta^2_{R_k})$, with $k = 1, 2, \ldots, K$. $CN(0, \delta^2_{R_k})$ is the complex Gaussian distribution and $\delta_{R_k} = d_0^{-\nu/2}$ where ν is the path loss exponent

The second radio propagation stage is between the selected Relay (R_b) and the users. Here, we investigate the cases of systems with IRS (including $M > 0$ elements in the IRS planar) and systems without IRS. In the case of a system without IRS, it is considered a specific case of using IRS with the number of elements $M = 0$. Signals transmitted from R_b to users via two wireless connections, including the transmission channel from the relay selected to the users, denoted by R_b-Users, is described as the Rayleigh fading distribution.

Denote $h_{bj} \sim CN(0, \delta_j^2)$ with $j = \{1, 2, E\}$ as the channel coefficient from R_b to users U_1, U_2, and E in the absence of IRS support in the proposed system, respectively. Where $\delta_j = d_j^{-\nu/2}$ and ν are the path loss, d_j is the distance between R_b to U_1, U_2, and E, respectively.

When an IRS-using system is present, the Rb-IRS-Users and Rb-Users connection signals are added to form the received signal at the users. The R_b-IRS-Users link consists of incident signals from R_b to IRS elements (R_b-IRS) and reflected signals from IRS elements to users (IRS-Users). Both R_b-IRS and IRS-Users connections have LoS components and Rice fading distribution as

$$g = \delta_{m_i}\left(\sqrt{\frac{K_g}{K_g+1}}g^{LoS} + \sqrt{\frac{1}{K_g+1}}g^{NLoS}\right).$$

Here $g \in \mathbb{G} = \{g_{km}, g_{mj}\}, j = \{1,2,\mathrm{E}\}, m = \{1, 2, .., M\}$ and $\delta_{mj} = d_{mj}^{-\nu/2}$, where ν stands for large-scale fading brought on by path loss, and d_{mj} is the distance between the IRS and the users. The R_b-IRS channel coefficient, with distance d_{km}, is denoted by g_{km}. K_g, g^{LoS}, and g^{NLoS} are the Rician factor, LoS, and Non-LoS components of channel g, respectively. The g^{LoS} and g^{NLoS} components are i.i.d. complex Gaussian distributed with zero mean and unit variance. Let η_m represent the reflection amplitude coefficient and θ_m stand for the phase shift of the m^{th} IRS element, where $0 \leqslant \eta_m \leqslant 1$ and $\theta_m \in (-\pi, \pi]$.

In this model, we assume that U_1 is farther away than U_2 from the source S and that users do not have any direct links. The location of unlawful user E could be near the relay cluster, between users, or close to the IRS. Another factor we'll look at to determine the ideal IRS placement is where E is located. The constraints on the channel coefficients are as follows, presuming the locations of authorized users are as stated above: $\left\|\sum_{m=1}^{M} g_{km}\eta_m e^{i\theta_m} g_{m1}\right\|^2 \leq \left\|\sum_{m=1}^{M} g_{km}\eta_m e^{i\theta_m} g_{m2}\right\|^2$ and $\|h_{k1}\|^2 \leq \|h_{k2}\|^2$, where h_{kj} with $j = \{1, 2, E\}$ are channel coefficient of k^{th}-relay and U_j links.

B. SIGNAL TRANSMISSION

Equation (1) states that the superimposed signal of two users, with the NOMA power allocation factors α_1 and α_2, is broadcast in space to the relay nodes from source node S. In conventional PD-NOMA, power allocation (PA) is inversely proportional to the CSI value. Therefore, the higher fraction of the transmitted power S will be allocated to the farther user U_1. In contrast, the smaller portion of the transmitted power will be fed to the closer user U_2.

$$x_S = \sqrt{\alpha_1 P}x_1 + \sqrt{\alpha_2 P}x_2, \tag{1}$$

where $x_j, j = 1, 2$, is the signal of U_j, α_j is the power allocated to x_j satisfying $\alpha_1 + \alpha_2 \leq 1$ and $\alpha_1 \geq \alpha_2$ with P is the transmitted power of S.

At the relay nodes, use relay node selection strategies in the cooperative network such as best relay strategy, max-min strategy, and harmonic mean function as the formulas below. Here, we denote R_b as the selected relay.

- The best relay selection strategy:

$$\{R_b\} = k^{th} \arg\max_{1\leq k\leq K} \|h_k\|^2. \tag{2}$$

- Max-min relay rule:

$$\{R_b\} = \max_{1\leq k\leq K}\left\{\min\left(\|h_k\|^2, \|h_{k1}\|^2, \|h_{k2}\|^2\right)\right\}. \tag{3}$$

- Harmonic mean function:

$$h_i = \left\{\frac{3}{\frac{1}{\|h_k\|^2} + \frac{1}{\|h_{k1}\|^2} + \frac{1}{\|h_{k2}\|^2}}\right\}, i = 1, 2\ldots, K$$
$$h_b = \max\{hi\}, i = 1, 2\ldots, K, \tag{4}$$

where $\|\cdot\|^2$ is the Euclidean norm for a complex number h_i and h_b is the channel coefficients in the i^{th} relay and the selected relay (R_b).

The following equation gives the superposition signal x_S at R_b:

$$y_{R_b} = \sqrt{P\alpha_1}x_1 h_b + \sqrt{P\alpha_2}x_2 h_b + n_{R_b}^{[a]}, \tag{5}$$

where P is transmitted power from BS, h_b is the channel coefficient of the BS - R_b link, and $n_{R_b}^{[a]} \sim CN\left(0, \sigma_{aR}^2\right)$ is additive white Gaussian noise (AWGN).

We apply a decode-and-forward approach in this proposed system model at relaying nodes. This indicates that the chosen relay will interpret the received signal and carry out the signal relay. Because of the DF protocol, the R_b can transmit the superimposed signal to destination users with the same power allocation ratio in the next propagation stage. In this stage, we assume that the power allocation coefficients for each user from the selected relay are the same values in the first stage. P_r is the transmitting power level of the selected relay R_b, and we have the signal broadcast from the chosen relay as

$$x_{R_b} = \sum_{j=1}^{2}\sqrt{P_r\alpha_j}x_j. \tag{6}$$

Moreover, to increase the security performance in PLS, we employ the AN technique at R_b. As a result, the signal transmitted by the R_b antenna includes the superimposed signal following the DF process and the artificial noise signal with the transmit power P_{AN}, which can be expressed as follows:

$$x^a{}_{R_b} = \sum_{j=1}^{2}\sqrt{P_r\alpha_j}x_j + \sqrt{P_{AN}}x_{AN} + n_{R_b}^a, \tag{7}$$

where $n^a_{R_b}$ is AWGN of the relay antenna, x_{AN} is AN signal with the power level P_{AN}.

The chosen relay transmits the superposed signals to destination users via two paths: IRS reflection links and direct links. As a result, the signal received at U_j with $j = 1, 2, E$ is made up of a signal reflected by the IRS and directed to the R_b-U_j link. The scenario of no IRS is distinguished by the number of IRS elements $M = 0$. Let denote $\Theta = diag(\theta) \in \mathbb{C}^{M\times M}$ with $\theta = [\theta_1,\theta_2,\cdots,\theta_M]^T$.

The received signals at the legal destination users are given as

$$\begin{aligned} y_{U_1} &= \left(g^H_{km}\Theta g_{m1} + h_{k1}\right) x_{R_b} + n_{U_1} \\ &= \left(g^H_{km}\Theta g_{m1} + h_{k1}\right) \sum_{j=1}^{L} \sqrt{P_r\alpha_j} x_j + n_{U_1}, \end{aligned} \tag{8}$$

and

$$\begin{aligned} y_{U_2} &= \left(g^H_{km}\Theta g_{m2} + h_{k2}\right) x_{R_b} + n_{U_2} \\ &= \left(g^H_{km}\Theta g_{m2} + h_{k2}\right) \sum_{j=1}^{L} \sqrt{P_r\alpha_j} x_j + n_{U_2}. \end{aligned} \tag{9}$$

Additionally, the Eavesdropper node overhears the transmitted signal from the designated relay. The received signal at location E can be formally expressed as follows:

$$\begin{aligned} y_E &= \left(g^H_{km}\Theta g_{mE} + h_{kE}\right) x_{R_b} + n_E \\ &= \left(g^H_{km}\Theta g_{mE} + h_{kE}\right) \sum_{j=1}^{L} \sqrt{P_r\alpha_j} x_j + n_E. \end{aligned} \tag{10}$$

C. FORMULATIONS OF SINR

This subsection delineates the methodology for formulating the Signal Interference Noise Rate (SINR) of the designated relay (R_b) and the user entities encompassing the legal destination users and the eavesdropper node.

To begin with, at the intermediate node selected R_b, the users' SINR having signals x_1 and x_2 respectively as the following

$$\gamma^{x_1}_{R_b} = \frac{P\alpha_1\|h_b\|^2}{P\sum\limits_{j=2}^{L}\alpha_j\|h_b\|^2 + N_0}, \tag{11}$$

$$\gamma^{x_2}_{R_b} = \frac{P\alpha_2\|h_b\|^2}{N_0}. \tag{12}$$

where, $\gamma^{x_1}_{R_b}$ and $\gamma^{x_2}_{R_b}$ is the SINR of the signals x_1 and x_2 of the destination equipment U_1 and U_2, respectively.α_j is a rate of power allocation for signal x_j, with $j = 1, 2$. h_b is the channel coefficient of the $BS - R_b$ link, and N_0 is the AWGNs at R_b.

As R_b applied the DF protocol, before forwarding the signals in the next phase, R_b had to decode its received signal successfully, and the SINRs must be greater than a given threshold.

Subsequently, the NOMA receiver of each user applied the SIC technique so SINRs of U_j with $j = 1, 2$ for information signal of x_1 and x_2 can be expressed respectively as

- At $U1$:

$$\gamma^{x_1}_{U_1} = \frac{\alpha_1 P_r\left(\left|\left(g^H_{km}\Theta g_{m1} + h_{k1}\right)\right|\right)^2}{\alpha_2 P_r\left(\left|\left(g^H_{km}\Theta g_{m1} + h_{k1}\right)\right|\right)^2 + N_0}, \tag{13}$$

$$\gamma^{x_2}_{U_1} = \frac{\alpha_1 P_r\left(\left|\left(g^H_{km}\Theta g_{m1} + h_{k1}\right)\right|\right)^2}{\alpha_2 P_r\left(\left|\left(g^H_{km}\Theta g_{m2} + h_{k2}\right)\right|\right)^2 + N_0}. \tag{14}$$

- At U_2:

$$\gamma^{x_1}_{U_2} = \frac{\alpha_1 P_r\left(\left|\left(g^H_{km}\Theta g_{m2} + h_{k2}\right)\right|\right)^2}{\alpha_2 P_r\left(\left|\left(g^H_{km}\Theta g_{m2} + h_{k2}\right)\right|\right)^2 + N_0}, \tag{15}$$

$$\gamma^{x_2}_{U_2} = \frac{\alpha_2 P_r\left(\left|\left(g^H_{km}\Theta g_{m2} + h_{k2}\right)\right|\right)^2}{N_0}, \tag{16}$$

where $h_{(k)j}, j \in \{1, 2\}$, is the channel coefficient of the $R_b - U_j$ link, and n_{U_j} is the AWGNs at U_j. Since SIC is employed at NOMA receivers, U_2 needs to successfully decode the information x_1 of U_1, and following this, U_2 abstract the detected signal x_1 and has its own signal x_2 while U_1 just decode self-signal.

Finally, we suppose that Eve has a multi-user detection capability. In particular, parallel interference cancellation (PIC) is employed at eavesdropping equipment to decode the superposed signal of legal users. Because Eve doesn't know information about AN, the received SINRs at Eve to detect U_j's message can be written as follows

$$\gamma^{x_1}_{E} = \frac{\alpha_1 P_r\left(\left|\left(g^H_{km}\Theta g_{mE} + h^H_{kE}\right)\right|\right)^2}{\left(\alpha_2 P_r + P_{AN}\right)\left(\left|\left(g^H_{km}\Theta g_{mE} + h^H_{kE}\right)\right|\right)^2 + N_0}, \tag{17}$$

$$\gamma^{x_2}_{E} = \frac{\alpha_2 P_r\left(\left|\left(g^H_{km}\Theta g_{mE} + h^H_{kE}\right)\right|\right)^2}{P_{AN}\left(\left|\left(g^H_{km}\Theta g_{mE} + h^H_{kE}\right)\right|\right)^2 + N_0}. \tag{18}$$

Based on the assumption that the DF protocol would be applied at the selected relay node, thus the achievable information capacity of users can be expressed as:

$$C_{U_1} = \frac{1}{2}\log\left\{1 + \min\left(\gamma^{x_1}_R, \gamma^{x_1}_{U_1}\right)\right\}, \tag{19}$$

and

$$C_{U_2} = \frac{1}{2}\log\left\{1 + \min\left(\gamma^{x_2}_R, \gamma^{x_2}_{U_2}\right)\right\}, \tag{20}$$

and

$$C^{x_1}_E = \frac{1}{2}\log\left(1 + \gamma^{x_1}_E\right), \tag{21}$$

and

$$C^{x_2}_E = \frac{1}{2}\log\left(1 + \gamma^{x_2}_E\right). \tag{22}$$

III. PERFORMANCE ANALYSIS

In this subsection, we perform the performance analysis of the proposed system. Here, the parameters to evaluate the system performance are the security capacity-worst and the secrecy energy efficiency. SCW means that we based on the secrecy capacity parameter estimated at each legal user and optimized the smallest value of this parameter. For a system like the proposed PD-NOMA that requires secrecy, setting up system parameters such as user power allocation, IRS deployment location, and AN interference power allocation to ensure a given SCW threshold will have practical significance. Moreover, we also investigate the SEE performance parameter to assess how energy efficient the system is to ensure minimum secrecy SCW performance. To determine the trade-off, we have built a program based on the NSGA-II algorithm.

To begin with, we present the formula for calculating the secrecy capacity of legal destination users. Afterward, based on those users' formulas, we offer the problem of maximizing both SCW and SEE functions with some constraints. Finally, the basic NSGA-II algorithm and the program based on NSGA-II are figured out to solve the multi-objective function optimization problem with the same constraints.

A. THE SECRECY CAPACITY/RATE OF THE LEGITIMATES

Firstly, based on the assumption that the DF protocol would be applied at the selected relay node, the achievable capacity of x_j at each user can be expressed as

$$C_{U_1} = \frac{1}{2}\log\left\{1+\min\left(\gamma_R^{x_1}, \gamma_{U_1}^{x_1}\right)\right\}, \tag{23}$$

and

$$C_{U_2} = \frac{1}{2}\log\left\{1+\min\left(\gamma_R^{x_2}, \gamma_{U_2}^{x_2}\right)\right\}, \tag{24}$$

and

$$C_E^{x_1} = \frac{1}{2}\log\left(1+\gamma_E^{x_1}\right), \tag{25}$$

and

$$C_E^{x_2} = \frac{1}{2}\log\left(1+\gamma_E^{x_2}\right). \tag{26}$$

where C_{U_j}, $C_E^{x_j}$ are symbols of the information capacity of U_j and E, respectively.

Next, considering the presence of an eavesdropper, the PD-NOMA proposed system, which includes the legitimate link capacity, is the capacity between the legitimate transmitter and the legal user. In contrast, the capacity of the illegal link is the capacity between the confident transmitter and the eavesdropper. In addition, [25] showed that the definition of secrecy capacity (SC) presents the capacious difference between the legal and eavesdropping links. The secrecy capacity of LUs denoted by SC_{U_j} is given as the following formulas

$$SC_{U_1} = \left[C_{U_1} - C_E^{x_1}\right]^+, \tag{27}$$

and

$$SC_{U_2} = \left[C_{U_2} - C_E^{x_2}\right]^+. \tag{28}$$

where $[x]^+ = \max\{x, 0\}$ means that if $C_{U_j} \le C_E^{x_j}$ then $SC_{U_j} = 0$.

The physical meaning of secrecy capacity is that the upper bound of the transmission rate that satisfies the criteria of reliability and secrecy may be determined.

B. THE WORST SECRECY CAPACITY OF THE SYSTEM

First, we will find the worst secrecy rate, which means the minimum secrecy capacities at the destination users.

$$\begin{aligned} SCW &= \min\left\{SC_{U_1}, SC_{U_2}\right\} \\ &= \min\left\{\left[C_{U_1} - C_E^{x_1}\right]^+, \left[C_{U_2} - C_E^{x_2}\right]^+\right\} \\ &= \frac{1}{2}\min \\ &\quad \left\{\begin{vmatrix} \log\left\{1+\min\left(\gamma_R^{x_1}, \gamma_{U_1}^{x_1}\right)\right\} - \log\left(1+\gamma_E^{x_1}\right) \\ \log\left\{1+\min\left(\gamma_R^{x_2}, \gamma_{U_2}^{x_2}\right)\right\} - \log\left(1+\gamma_E^{x_2}\right) \end{vmatrix}, \right\} \\ &= \frac{1}{2}\min\left\{\begin{vmatrix} \log\left\{\frac{1+\min\left(\gamma_R^{x_1}, \gamma_{U_1}^{x_1}\right)}{1+\gamma_E^{x_1}}\right\} \\ \log\left\{\frac{1+\min\left(\gamma_R^{x_2}, \gamma_{U_2}^{x_2}\right)}{1+\gamma_E^{x_2}}\right\} \end{vmatrix}, \right\}. \end{aligned} \tag{29}$$

Afterward, using equation (29), we have the maximization problem of SCW under multiple constraints for both cases without IRS and IRS-aided transmission, which can be formulated as below. Here Q denotes to the none-IRS and IRS-aided cases.

$$Maximization \underbrace{SCW}_{\substack{\alpha_1,\alpha_2 \\ \theta_m\in(-\pi,\pi]}} = Max \underbrace{\left\{\min\left\{SC_{U_1}^Q, SC_{U_2}^Q\right\}\right\}}_{\substack{\alpha_1,\alpha_2 \\ \theta_m\in(-\pi,\pi]}}, \tag{30a}$$

$$subject \quad to: \tag{30b}$$

$$\min\left(\gamma_R^{x_1}, \gamma_{U_1}^{x_1}\right) \ge \gamma_{01}{}', \tag{30c}$$

$$\min\left(\gamma_R^{x_2}, \gamma_{U_2}^{x_2}\right) \ge \gamma_{02}, \tag{30c}$$

$$\alpha_1 + \alpha_2 \le 1, \tag{30d}$$

$$\alpha_1 > \alpha_2. \tag{30e}$$

Here, γ_{0j} is the threshold at which signal information can be decoded successfully. And then, we figure out the boundaries of the variables α_j, $j = 1,2$ based on the constraint (30b and 30c) of the problem (30a). Considering multi-constraint conditions (30b)-(30c) in which the first constraint (30b) is non-convex. The two both case of α_1 and α_2 are presented by **Lemma 1** and **Lemma 2** as follows:

Lemma 1. The boundaries of the α_1, α_2 in the without IRS case can be expressed as follows:

$$\frac{\gamma_{02}\gamma_{01}}{\min\left(\frac{1}{\psi_1}, \frac{\|h_{k2}\|^2}{\psi_2}\right)} + \gamma_{01}\max\left\{\psi_1, \frac{\psi_2}{\|h_{k1}\|^2}\right\} \leq \alpha_1 < 1,$$

and

$$\frac{\gamma_{02}}{\min\left(\frac{1}{\psi_1}, \frac{\|h_{k2}\|^2}{\psi_2}\right)} \leq \alpha_2 < 1, \tag{31}$$

here $\psi_1 = \left(\frac{P\|h_{k*}\|^2}{N_0}\right)^{-1}$ and $\psi_2 = \frac{N_0}{P_r}$.

Proof. See in Appendix A

Lemma 2: The boundaries of the α_1, α_2 in the IRS-aided case can be calculated as

$$\left[\begin{array}{l}\frac{\gamma_{02}\gamma_{01}}{\min\left(\frac{1}{\psi_1}, \frac{\left(\left|\left(g_{km}^H \Theta g_{m2} + h_{k2}^H\right)\right|\right)^2}{\psi_2}\right)} + \\ \gamma_{01}\max\left\{\psi_1, \frac{\psi_2}{\left(\left|\left(g_{km}^H \Theta g_{m1} + h_{k1}^H\right)\right|\right)^2}\right\}\end{array}\right] \leq \alpha_1 < 1,$$

and

$$\frac{\gamma_{02}}{\min\left(\frac{1}{\psi_1}, \frac{\left(\left|\left(g_{km}^H \Theta g_{m2} + h_{k2}^H\right)\right|\right)^2}{\psi_2}\right)} \leq \alpha_2 < 1, \tag{32}$$

here $\psi_1 = \left(\frac{P\|h_{k*}\|^2}{N_0}\right)^{-1}$ and $\psi_2 = \frac{N_0}{P_r}$.

Proof. See in Appendix B

C. THE SECRECY ENERGY EFFICIENCY OF THE SYSTEM

The *SEE* is defined as the ratio between the achievable secrecy sum rate to the total consumed power of the NOMA system [44], and it can be expressed as

$$SEE = SSR/P_{total} \tag{33}$$

Here, *SSR* is the sum secrecy rate, and P_{total} is the total power consumption. Sum secrecy rate of U_1 and U_2 as

$$SSR^Q = SC_1^Q + SC_2^Q \tag{34}$$

here Q={none-IRS, IRS-aided}. Next, we consider the power assumption of the proposed system model in two cases, including without IRS and IRS-supported cases.

In the case without IRS, the consumption of power is calculated as

$$\begin{aligned} P_{total}^{[\overline{IRS}]} &= \left(P_1 + P_2 + P_{cU_1} + P_{cU_2}\right) + P_{cBS} + (P_{cR} + P_r) \\ &= \left(\alpha_1 P + \alpha_2 P + P_{cU_1} + P_{cU_2}\right) + P_{cBS} + (P_{cR} + P_r) \end{aligned} \tag{35}$$

P_{c_x} with $x = [U_1, U_2, BS, R]$ as circuit power at each node In the case of IRS-supported transmission, the consumption of power is formulated as

$$\begin{aligned} P_{total}^{[IRS]} &= \left[\begin{array}{l}\left(P_1 + P_2 + P_{cU_1} + P_{cU_2}\right) + \\ P_{cBS} + (P_{cR} + P_R) + M \times P_{cIRS}\end{array}\right] \\ &= \left[\begin{array}{l}\left(\alpha_1 P + \alpha_2 P + P_{cU_1} + P_{cU_2}\right) \\ + P_{cBS} + (P_{cR} + P_R) + M \times P_{cIRS}\end{array}\right]. \end{aligned} \tag{36}$$

Then, the secrecy energy efficiency of the proposed system can be expressed as

$$SEE = \frac{SSR^{[Q]}}{P_{total}^{[Q]}}, \tag{37}$$

$$Maximization \quad \underbrace{SEE}_{\substack{\alpha_1,\alpha_2 \\ \theta_m \in (-\pi,\pi]}} = Max \frac{SSR^{[Q]}}{P_{total}^{[Q]}}, \tag{38a}$$

$$subject\ to: \begin{array}{l}\min\left(\gamma_R^{x_1}, \gamma_{U_1}^{x_1,q}\right) \geq \gamma_{01}, \\ \min\left(\gamma_R^{x_2}, \gamma_{U_2}^{x_2,q}\right) \geq \gamma_{02},\end{array} \tag{38b}$$

$$\alpha_1 + \alpha_2 \leq 1, \tag{38c}$$

$$\alpha_1 > \alpha_2. \tag{38d}$$

These constraint conditions (38b)-(38d) are similar in maximizing the secrecy data rate.

D. NSGA-II BASED PROGRAM FOR ALLOCATION POWER POLICY IN THE PDNOMA-IRS DOWNLINK SYSTEM WITH AN EAVESDROPPER

1) NSGA-II STANDARD

Multi-objective optimization problems (MOPs) in the domain of science and engineering [45] are the approaches to handle multiple objectives simultaneously, where the objectives are usually inharmonious, resulting to an intractable task in obtaining a well-balanced agreement for each objective.

NSGA-II is one of the well-known effective techniques for handling MOPs. Its non-dominated solutions are said to be Pareto optimal solutions. Figure 2 illustrates the basic flowchart of that algorithm.

The main idea behind the Pareto NSGA-II is to find the Pareto front, also called the Pareto set or non-dominated solutions, that corresponds to a set of optimal solutions. All objectives are appropriately balanced while remaining unaffected by a non-dominated solution. In other words, Pareto dominance compares each answer x with all the other solutions in the population until one of them takes the lead. If no solution dominates x, the NSGA-II designates x as non-dominated and selects it as one of the Pareto fronts.

Assume that we maximize a set of objectives f_i, $i = 1, \ldots, m$ a solution x dominates xi if $\forall\ i\ f_i(xi) \leq f_i(x)$ and $\exists\ j|f_j(xi) < f_j(x)$.

The first step in NSGA-II is randomly creating the initial population P_0 of individuals encoded using a specific representation. Then, genetic operations such as crossover and mutation form a child population Q_0 from the parent population P_0. Both populations are merged to form the next generation, and a subset of individuals is chosen based on the dominance principle. This process will be repeated until the last iteration meets the stop criterion.

For each solution, a crowding distance is also computed by determining the distance to the nearest solutions along each objective function. The crowding distance is then utilized to modify each solution's fitness.

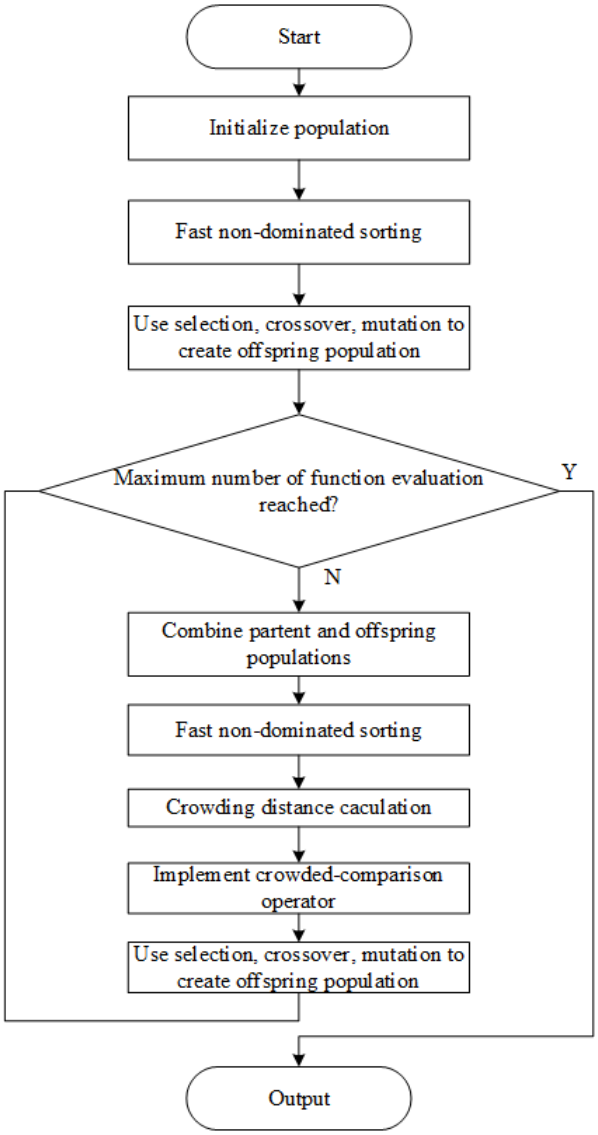


FIGURE 2. The flow chart of NSGA -II algorithm.

2) NSGA-II BASED PROGRAM FOR ALLOCATION POWER POLICY IN THE PDNOMA-IRS DOWNLINK SYSTEM

We designed a dynamic power allocation program for our proposed model, employing the NSGA-II standard algorithm [46]. The objective is to maximize both the secrecy energy efficiency and the secrecy capacity of legal users within the PDNOMA-IRS downlink system. In this context, the eavesdropper simulates infiltration, utilizing a jammer to transmit a jamming signal. Our assumptions include constant circuit usage for the system's components, as well as a constant power dissipation for each IRS element. Consequently, power consumption is directly proportional to the number of IRS elements in our system, contrasting with the scenario lacking IRS. Algorithm 1 describes the program in further depth.

Overall, the program includes steps based on the steps of the NSGA-II algorithm to find solutions so that both the SEE and SCW objective functions reach the maximum value with several given constraints according to problems (30a)-(30d) and (38a)-(38b), respectively.

Algorithm 1 The Program of SCW and SEE Maximization Based on NSGA-II (SCENSGA-II)

Input: SCW, SEE, $pop-size$, $iter$
Output: PF
Initialize: population P_0 including α_1 and α_2 according to the constraint formula (30b)-(30d) or (38b)-(38d), and in the range [0, 1]. The phase shift θ_m of each IRS element is assumed to follow a linear algorithm [43] and in the range of $[-\pi, \pi]$.
Call FNDS
Create offspring populations by GA
While $(t < iter)$
  $t = t + 1$
  Combine parent and offspring populations
  Call FNDS
  Call CDC
  Updating $P(t)$
  Storing PF
  CCO follows formula (40)
  Create offspring populations by GA
End While
Return PF

In the initialization step, the proposed system's parameters are assigned and the population is randomly initialized. In particular, system parameters are set for macro-cell indoor/outdoor systems, and the population is randomly generated in the range of variable power allocations for each legal user.

Following this, to sort the FNDS, it is necessary to calculate objective functions SCW and SEE based on formula functions (30a) and (38a) and the procedure FNDS is called. In Algorithm 2 presents FNDS in more detail. Next, selection, crossover, and mutation are performed to create an offspring population.

In the subsequent stage, the loop whose termination condition is the given iterations to find solutions, including SEE and SCW. If the termination is not satisfied, the process of finding SEE and SCW is repeated based on the NSGA-II algorithm, including combining parent and offspring populations, FNDS procedure and CDC procedure, implementing CCO, and using genetic techniques to create the next generation. While FNDS is presented in Algorithm 2, we also present about CDC in Algorithm 3 and CCO in formula (40). Regarding to CDC, this procedure is intended to determine the sum of Euclidean distances from each individual to two neighboring solutions in each front to assess the density of solutions surrounding the solution under consideration in the following manner:

$$CD_{P_i} = \sum_{\Psi \in \{SCW, SEE\}} \frac{\Psi(P_{i+1}) - \Psi(P_{i-1})}{\Psi_{\max} - \Psi_{\min}}, \quad (39)$$

Algorithm 2 Fast Non-Dominated Sorting Procedure (FNDS)

Input: $P(x)$
Output: $f(k)$
  for $p \in P(x)$:
    Init $D_p = \emptyset$ is the set containing all the individuals that are dominated by p
    Init $n_p = 0$ is the number of individuals that dominated p
    for $q \in P(x)$:
      if p dominates q:
        $D_p = D_p \cup q$ Add q to the set of solutions dominated by p
      else
        n_p=$n_p + 1$ Increment the domination counter of p
      end
    if $n_p == 0$: p belongs to the first front
      $f(1) = f(1) \cup p$
      $p_{rank} = 1$
    end
  $k = 1$ Initialize the front counter
  while $f(k) \neq \emptyset$
    $H = \emptyset$
    for $p \in f(k)$
      for $q \in D_p$
        $n_q = n_q - 1$
        if $n_q = 0$: q belongs to the next front
          $q_{rank} = k + 1$
          $H = H \cup q$
    $k = k + 1$
    $f(k) = H$
Return $f(k)$

where CD_{P_i} is the crowding distance of individual P_i, Ψ_{max} and Ψ_{min} are the maximum and minimum of the fitness values, respectively, when using the objective function Ψ, $\Psi \in \{SCW, SEE\}$. CDC is shown in further detail in Algorithm 3. With CCO, this is an operator that is applied in the selection process of the algorithm to obtain a uniformly spread-out Pareto optimal front. The CCO is defined in a partial order as follows:

$$\begin{aligned} &p \, dominates \, q \; if \; q_{rank} < p_{rank} \\ &\text{or}((p_{rank} == q_{rank}) \\ &\text{and}(CD_p > CDq)), \end{aligned} \tag{40}$$

where every individual p in the population has two attributes, those are non-domination rank p_{rank} and crowding distance (CD_p). In the context of differing non-domination ranks between two solutions, a preference is accorded to the solution possessing the lower (superior) rank. Alternatively, when both solutions pertain to the same front, preference is given to the solution in a less crowded region.

Finally, when the termination condition is met, the output, including the two Pareto-optimal fronts of the SEE and SCW functions, is printed.

Algorithm 3 Crowding Distance Calculator Procedure (CDC)

Input: $f(k)$
Output: CD_{P_i}
  Assign j is the number of individuals in $f(k)$
  for i in range (j):
    Init $CD_{P_i} = 0$
    Init $CD_{P_1} = CD_{P_j} = \infty$
    Caculate CD_{P_i} using (39)
  end
  Return CD_{P_i}

Upon securing a collection of non-dominated solutions, an inquiry arises regarding how a decision-maker can refine the set to encompass only a limited number or a singular solution. This deliberative process pertaining to multi-objective problems is commonly recognized as Multi-Criteria Decision Making (MCDM). In the present investigation, we have utilized the decomposition technique denominated Augmented Scalarization Function (ASF), as introduced in the scholarly work referenced as [48]. ASF is widely recognized within the multi-objective optimization domain. Its application necessitates the specification of weights, serving as indicators of the user's preferences. These weights are represented by a vector comprising solely positive floating-point values, whose summation equals one, and the vector's length corresponds to the number of objectives under consideration.

We conduct an assessment of the computational complexity associated with SCENSGA-II. Specifically, our focus lies on the examination of one iteration within the entirety of the algorithm [45]. In this regard, we delineate the fundamental operations, elucidating their respective worst-case complexities as follows:

- FNDS procedure is $g1 = O(n_f(2n_p)^2)$
- CD procedure is $g2 = O(n_f(2n_p)log(2n_p))$
- sorting on CCO is $g3 = O(2n_p log(2n_p))$

where n_f is the number of objective functions, n_p is the size of population. The overall complexity of the algorithm is $n_{iter} * (g1 + g2 + g3)$ with n_{iter} denotes the iteration of the algorithm.

The convergence of SCENSGA-II is assessed through a hypothesis-testing approach. Statistical tests are employed to scrutinize the presence of a significant difference between consecutive iterations. Should the observed difference prove non-significant, the algorithm is deemed to have achieved convergence. The results obtained from our simulations provide compelling evidence to assert the convergence of SCENSGA-II.

IV. EXPERIMENT AND RESULT ANALYSIS

In this section, we conduct simulations to scrutinize the attained outcomes by tackling the aforementioned optimization challenges concerning the performance metrics of our proposed system. The primary constituents of this section encompass the configuration of environmental parameters, simulation methodologies, analytical scenarios, and an exposition of the experimental findings.

A. DEPLOYMENT OF ENVIRONMENTAL SETTINGS AND EXPERIMENTAL SCENARIOS

In this manuscript, the simulation outcomes are conducted using the Matlab and Pycharm software environments, leveraging a computer configuration boasting 16GB of RAM and a CPU processing speed of 2.8GHz. To assess the system's security robustness, the algorithmic analysis outlined earlier encompasses two pivotal facets: the system's security strength evaluated through its security capacity and energy efficiency. Specifically, when appraising the security capacity, the focus lies on the SCW, aimed at enhancing the system's security even under the most adverse operating conditions. To comprehensively scrutinize the proposed system's quality, this section delineates various scenarios outlined in the tabulated format below, alongside the system's constants and unchanging parameters.

B. ANALYSIS OF CONVERGENCE, TIME COMPUTATION

In this subsection, we scrutinize the convergence patterns and computational prowess inherent in our proposed NSGA-II methodology and alternative approaches, aiming to determine the most suitable technique for our specific problem domain. In Figure 3, we analyze the convergence traits of our proposed NSGA-II algorithm alongside R-NSGA-II. Fundamentally, R-NSGA-II is derived from NSGA-II; however, its convergence rate demonstrates a slower trajectory than NSGA-II within our problem domain. Specifically, concerning the simulation results pertaining to worst-case security capacity, NSGA-II attains a convergence goal of approximately 100 iterations across three particle size (PAS) variations (30, 40, 50), while R-NSGA-II achieves a convergence point of around 200 iterations. Similarly, in the context of the experimental results for energy efficiency SEE analysis, NSGA-II exhibits a swifter convergence in contrast to R-NSGA-II.

Additionally, Table 2 elucidates the computational time aspects, highlighting NSGA-II as the most efficient, followed by R-NSGA-II, while exhaustive search (ES) exhibits the lengthiest computational duration. Specifically, Table 2 showcases convergence times: R-NSGA-II at 3.0929 seconds reaching convergence by iteration 200, NSGA-II at 0.24957 seconds achieving convergence by iteration 80, and ES at 40000 seconds. Computational efficiency is paramount in wireless communication paradigms, particularly in real-time communication scenarios. Consequently, to satisfy the stringent transmission time requisites, NSGA-II emerges as the most fitting solution for our proposed system dealing with multi-objective optimization challenges.

Furthermore, insights from Figure 3 reveal that NSGA-II exhibits superior convergence outcomes across both metrics, namely SCW and SEE, compared to R-NSGA-II. In Figure 3, NSGA-II attains convergence values of approximately 1.5 for SCW and 0.95 for SEE, whereas R-NSGA-II reaches 1.3 for SCW and 0.92 for SEE. This comparative analysis underscores NSGA-II's superior performance across both SCW and SEE metrics, indicating its efficacy in delivering enhanced results in these performance criteria.

In conclusion, based on the foregoing analysis, our proposed NGSA-II algorithm for addressing the SCW and SEE challenges within the NOMA/IRS model exhibits significantly improved computational efficiency compared to both R-NSGA-II and ES algorithms while concurrently upholding the system's security integrity. Consequently, in the ensuing experimental scenarios, our primary focus lies in meticulously examining the security integrity of our proposed system. These examinations will specifically investigate the impact of critical system parameters by employing the NGSA-II algorithm.

From the above analysis, we realize that NSGA-II is a potential candidate for addressing the multi-optimization problem for our proposed system model compared to RNSGA and ES methods. Thus, in the following experimental scenarios, we focus on results that apply NSGA-II.

C. THE PARETO FRONT OF SEE VERSUS SCW

This section explores the variability in confidentiality performance concerning decision-making alterations for two fundamental functions within our proposed model, SCW and SEE. Employing NSGA-II, a multi-objective optimization algorithm, we aim to derive solutions for both functions concurrently, denoted as SCW and SEE, respectively. In the realm of multi-objective optimization problems, there exists no assurance that a singular solution will optimize each objective simultaneously, leading to what is termed as conflicting objective functions. Various terms, such as non-dominated, Pareto optimal, and Pareto efficient, characterize solutions wherein none of the objective functions can be enhanced without compromising the values of other objectives.

In this section, we present graphical representations delineating solution sets encompassing the SCW and SEE functions, forming what is known as the Pareto front, in scenarios involving IRS (with a quantity of IRS elements $M = 10$) and without IRS ($M = 0$) and in both the cases $PAN = Pr$, as depicted in Figures 4a and 4b, respectively. To begin with, we can see that the two figures have the same trend, wherein SCW attains its maximum value while SEE reaches its minimum and vice versa. To get more clarity, we only analyze Figure 4a, and Figure 4b is similar. We consider three solutions S1, S2, and S3 in Pareto front (PF), taken in the feasible solution space. At solution S1, SEE grows to around 7.328, then SCW will decrease and

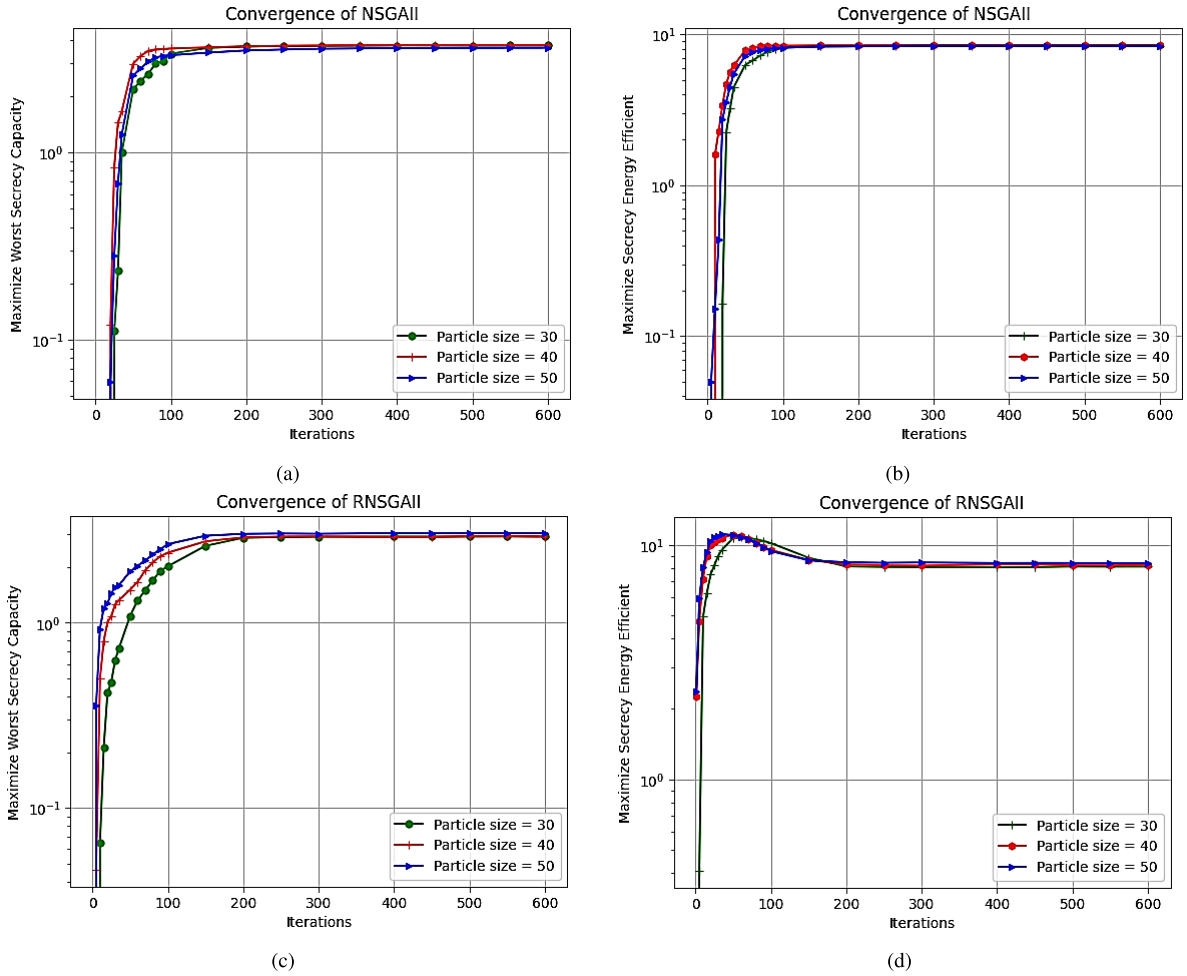


FIGURE 3. Convergence behavior of NSGA-II and R-NSGA-II on SCW and SEE.

TABLE 1. Time computation (in seconds).

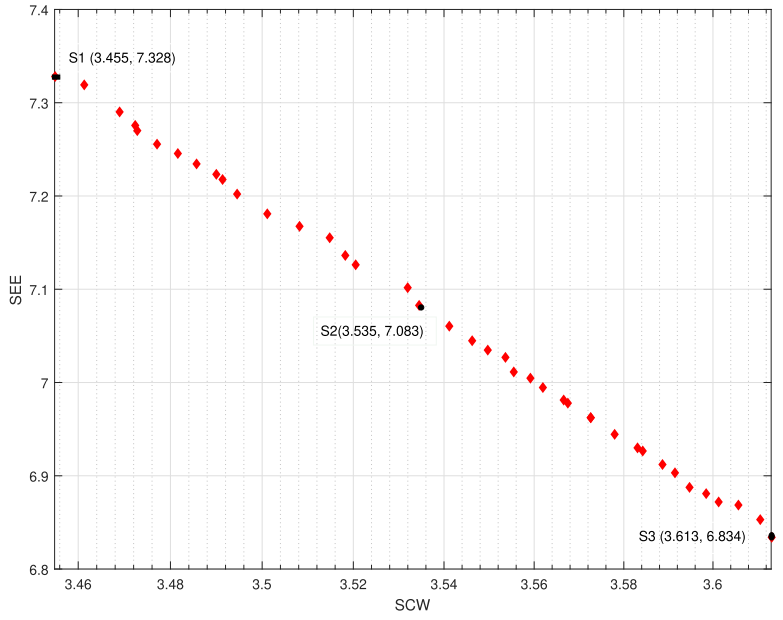
Methods	PAS =30, step-size=0.01	PAS =40, step-size=0.01	PAS = 50, step-size=0.01	PAS = 30, step-size=0.001	PAS =40, step-size=0.001	PAS = 50, step-size=0.001
NGSA-II	Iterations=100	Iterations =80	Iterations =80	Iterations=100	Iterations =80	Iterations =80
	0.4559	**0.24957**	**0.2809**	**0.4070**	**0.2589**	**0.2661**
R-NSGA-II	Iteration =200	iterations=200	iterations=150	Iteration =200	iterations=200	iterations=150
	2.3506	3.0929	4.392	2.992	3.1365	4.433
ES	M=3, Step=0.1	M=3, Step=0.06	M=3, Step=0.03	M=4, Step=0.1	M=4, Step=0.06	M=4, Step=0.03
	6314,36	11138.93	16683.71	7869.35	13868.48	18566.31

reach a limit with a value of around 3.455 and can not be declined further. Meanwhile, when the SEE value reduces to 6.834, the SCW value will increase to around 3.613 solution S3. The results depict that if the design option favors SEE optimization then solution S1 should be chosen. Conversely, if the option priors to SCW optimality, the appropriate candidate should be the S3 solution, or if the balance is between SEE and SCW, solution S2 (3.535 and 7.083) is the best candidate. Generally speaking, this delineation encapsulates the trade-off between the security cost per user and the system's energy efficiency.

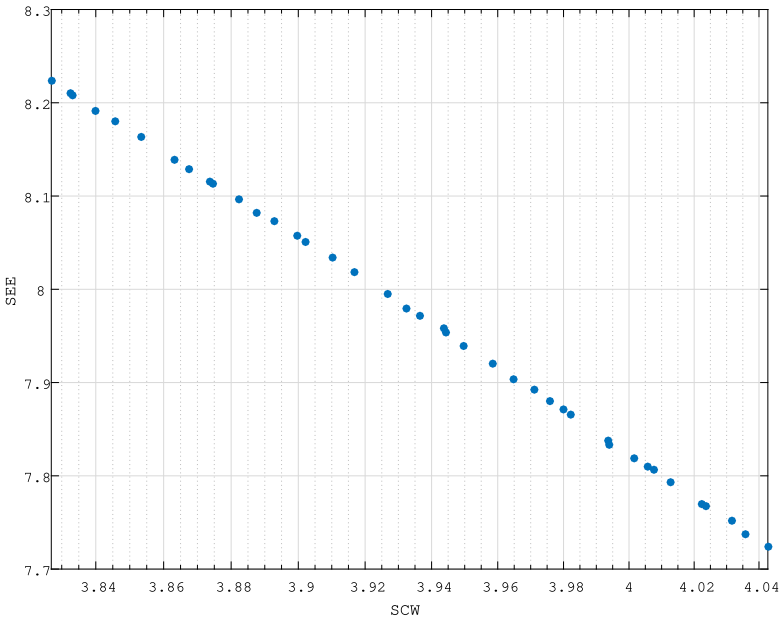
Furthermore, using IRS yields superior *SCW* and *SEE* values, figure 4b, for the system compared to scenarios where IRS is not employed, Figure 4b. The SEE and SCW values in the IRS-aided cases get around 8.224 and 3.824, while the values in the no IRS model are, in turn, about 7.328 and 3.455.

D. IMPACTS OF THE NUMBER OF IRS ELEMENTS ON SCW AND SEE WITH RELAYING SELECTION METHODS

In this subsection, we explore the impact of varying the quantity of IRS elements on the performance metrics—specifically SCW and SEE—within our proposed system in considering different relay selection methods. These experimental investigations involve configuring key system parameters, as outlined in Table 1, including the distance of the Relay-Eavesdropper link set at $d_{RE} = 20$ meters. Before



(a) PAN=Pr M=0, N=7

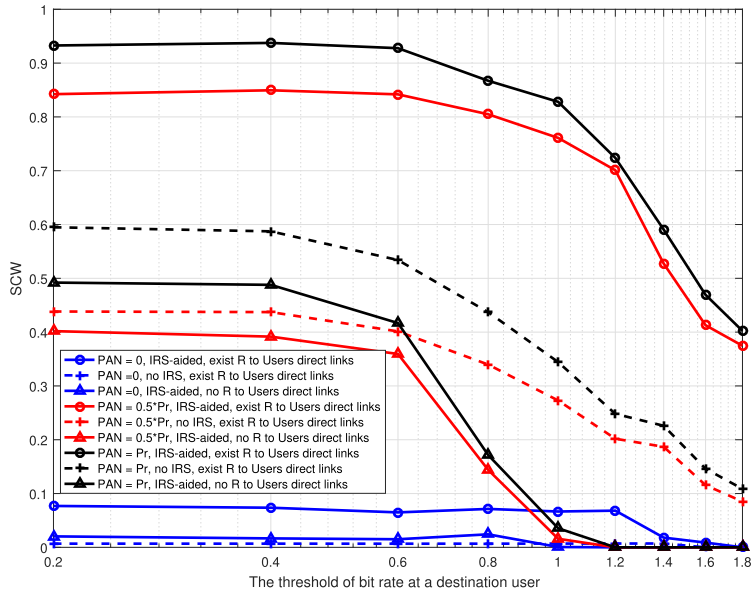


(b) PAN=Pr M=10, N=7

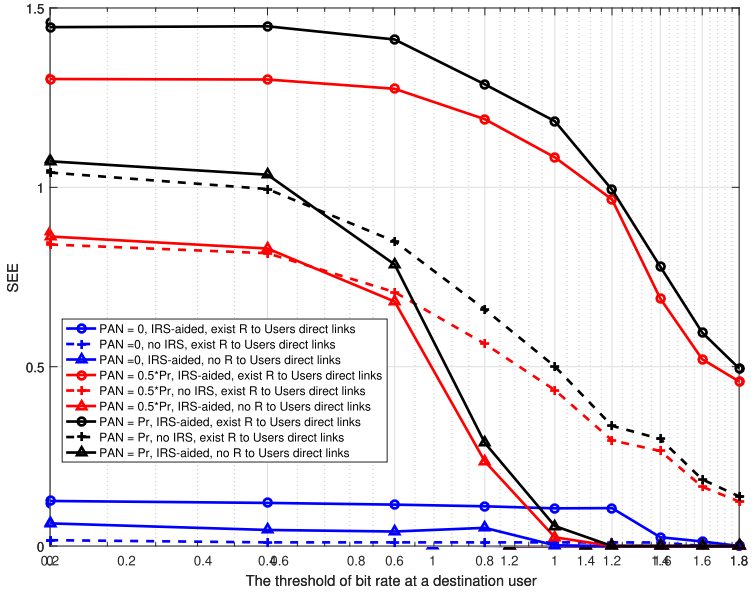
FIGURE 4. **The Pareto front of SEE vs SCW with non-IRS (a) and IRS-aided (b) models.**

considering the effects of the number of IRS elements on SCW and SEE, we investigate the system model's efficiency with the IRS's assistance. This experiment result is presented in Figures 5a and 5b. It can be seen from Figure 5 three kinds of models are examined: the first model includes the assistance of the IRS in the presence of a direct link of Relay-Users; the second model includes the IRS in the absence of a direct link of Relay-Users because of obstacles; the final model with the direct link of Relay-users without the assistance of IRS. Figure 5 shows that the first model offers the best performance in SCW and SEE compared to other models, and the third model provides the worst secrecy performance. Clearly, our proposed algorithm for the multi-objective optimization problem for the system model with IRS can improve the secrecy performance on both SCW and SEE. Thus, our proposed system model in Figure 1 gets better secrecy performance and energy efficiency when deployed.

Figure 6 shows the effects of the number of IRS elements on our proposed system's SCW (a) and SEE (b).



(a)

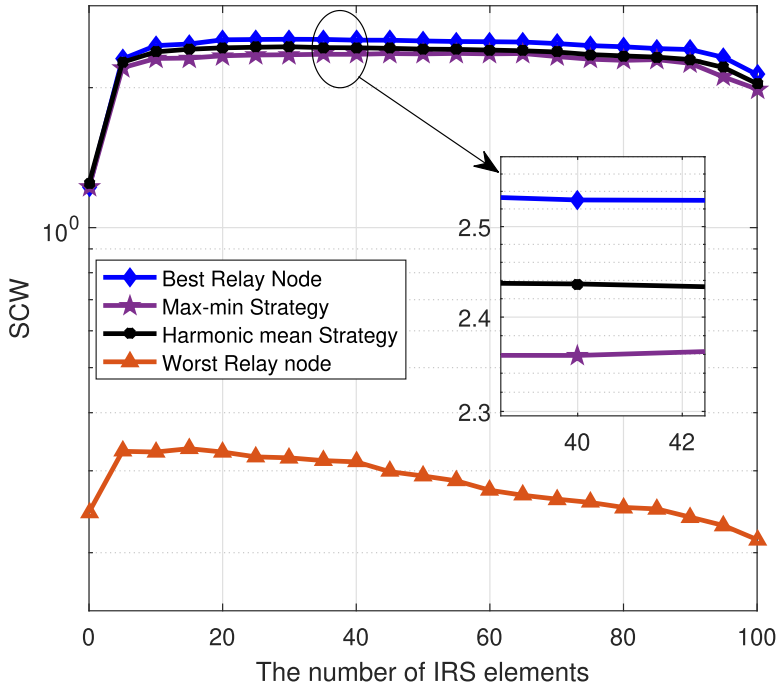


(b)

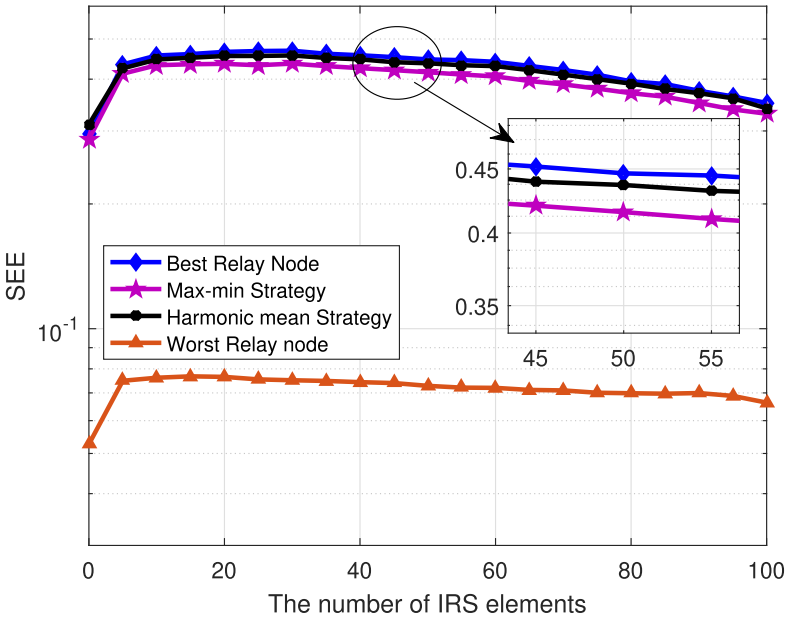
FIGURE 5. **The effects of kinds of system models on SCW (a) and SEE (b) versus the threshold of bit rate.**

From Figure 6, selecting the number of IRS elements for deployment within a network emerges as a pivotal consideration, exerting significant influence on system performance. Notably, low and high quantities of IRS elements significantly affect the SEE metric of the proposed system. Optimal SEE is achieved with a judicious number of IRS elements. Figure 5a illustrates that within a range of 10 to 90 IRS elements, both SEE and SCW metrics demonstrate higher values. However, with the number of IRS elements beyond approximately 100, SEE experiences a decline toward smaller values. Hence, identifying an appropriate quantity of IRS elements becomes imperative to enhance system performance and mitigate deployment expenses. Moreover, selecting the IRS element quantity for system deployment warrants careful evaluation, considering both implementation costs and the resultant system quality. In the context of our proposed security system, it becomes evident that maintaining a specific range of IRS elements leads to heightened security quality.

Moreover, Figure 6 illustrates the efficacy of the implemented transition node selection methodologies within our proposed model. Under the system parameters delineated in



(a) PAN=Pr, M=10, N=7



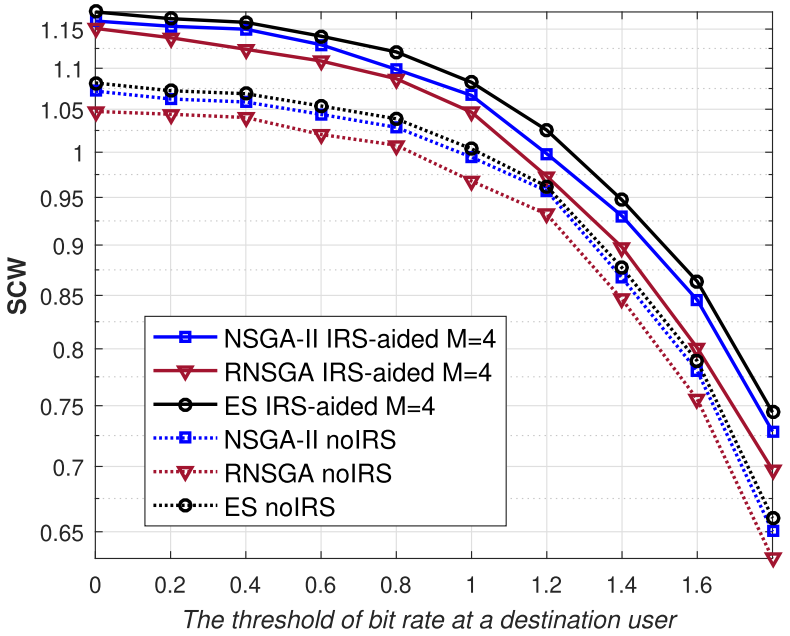
(b) PAN=0 M=10, N=7

FIGURE 6. Effects of IRS elements' number and the strategies of relay selection on SCW (a) and SEE (b).

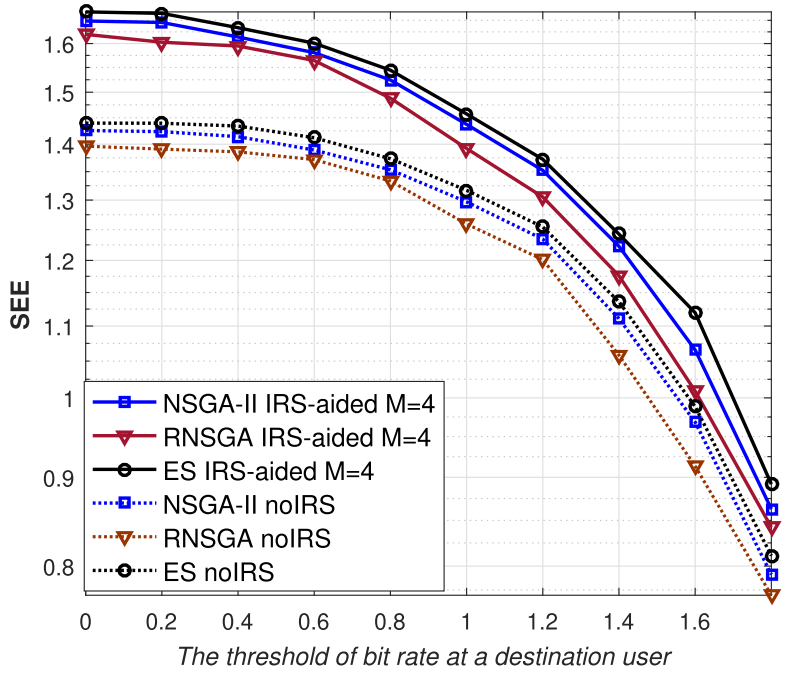
Table 1, it becomes apparent that the best relay node selection and the harmonic mean function techniques yield superior results. Notably, instances where the relay node experiences the worst transmission channel result in diminished security quality across SEE and SCW metrics. These findings allow for assessing security quality thresholds on both indicators within this system, highlighting the average lowest and highest thresholds within the range of 0.3 to 1.5.

E. IMPACTS OF LOCATIONS OF EAVESDROPPER AND IRS ON SCW AND SEE

Figures 8 and 9 illustrate the impact of the eavesdropper node's positioning and the placement of the IRS within our proposed system. The foundational parameters governing the system configuration are detailed in Table 1 within Section IV-A. Analysis of the figure reveals that the proximity of the eavesdropping node to the relay network directly



(a)



(b)

FIGURE 7. The number of IRS elements and three relay selecting strategies affect SCW (a) and SEE (b).

influences the security efficacy of the system, leading to reduced measurements in both SCW and SEE. This outcome is attributed to the eavesdropping node's closer proximity to the relay network, resulting in heightened signal strength interception. Conversely, as the eavesdropping node moves farther away, there is an observable increase in both SCW and SEE values. Because of the NSGA-II application, when the E is positioned at a specified farthest distance, SCW and SEE reach a threshold value.

Regarding the position of the IRS concerning the relaying network, it is observed that when the IRS is distant from the relaying network, both SCW and SEE values decrease. However, the system's quality improves within 10-15 meters of IRS-Relay distance. These results, achieved through the

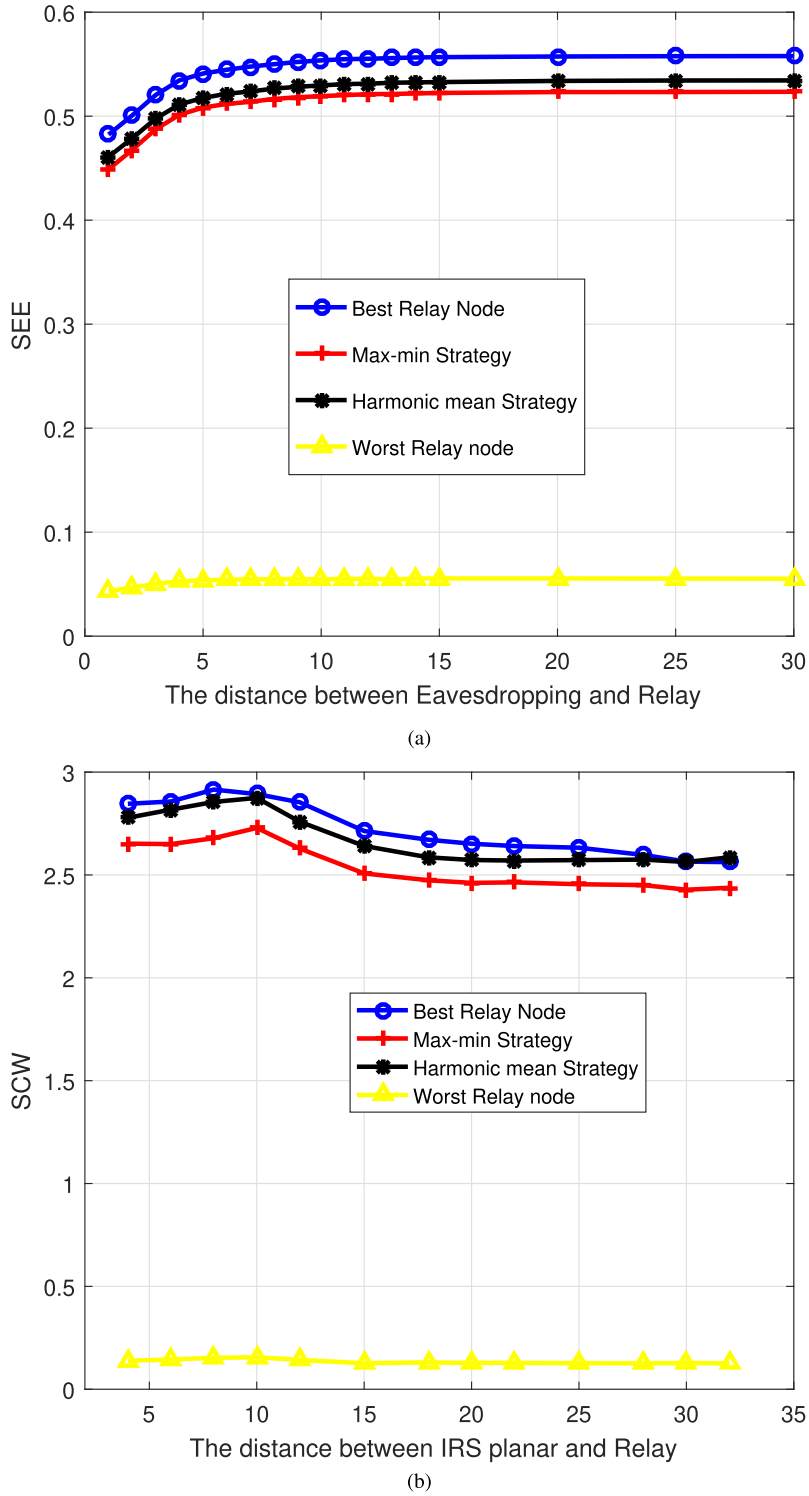


FIGURE 8. The location of the Eavesdropper and the IRS on SCW (a) and SEE (b).

application of NSGA-II, optimize the security quality of the system in terms of both SCW and SEE. In practical system deployment, carefully considering the IRS placement is crucial to attaining optimal security quality.

Both Figures 8 and 9 consistently demonstrate, given the established channel values detailed in Table 1 of Section IV-A and varying distances, that the method of selecting relay nodes achieves varying degrees of effectiveness. Specifically, the best relay selection method proves most efficient, followed by the max-min and harmonic approaches, and finally, the lowest secrecy performance in selecting the worst relay method. The descriptions provided in Figures 4

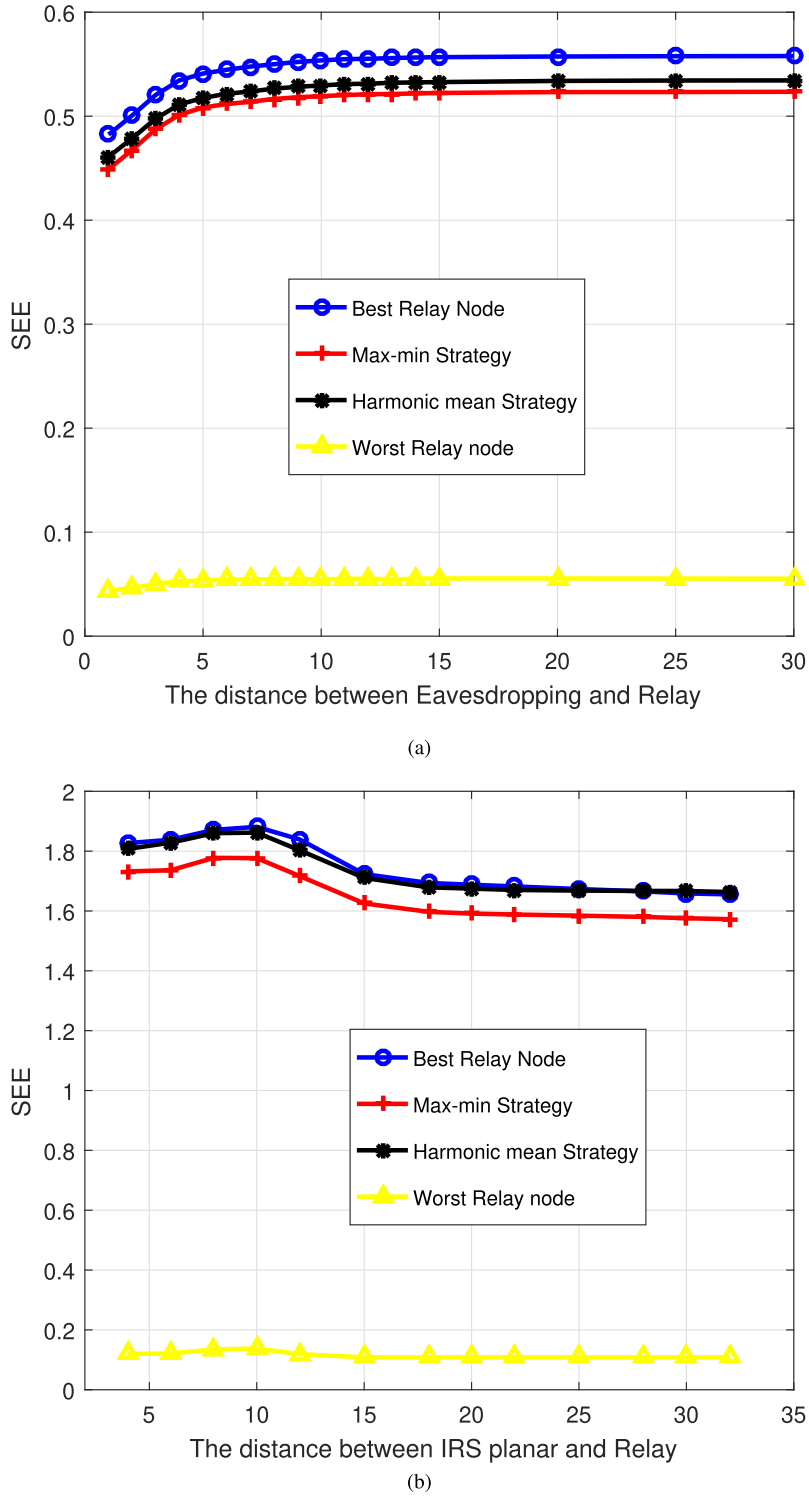
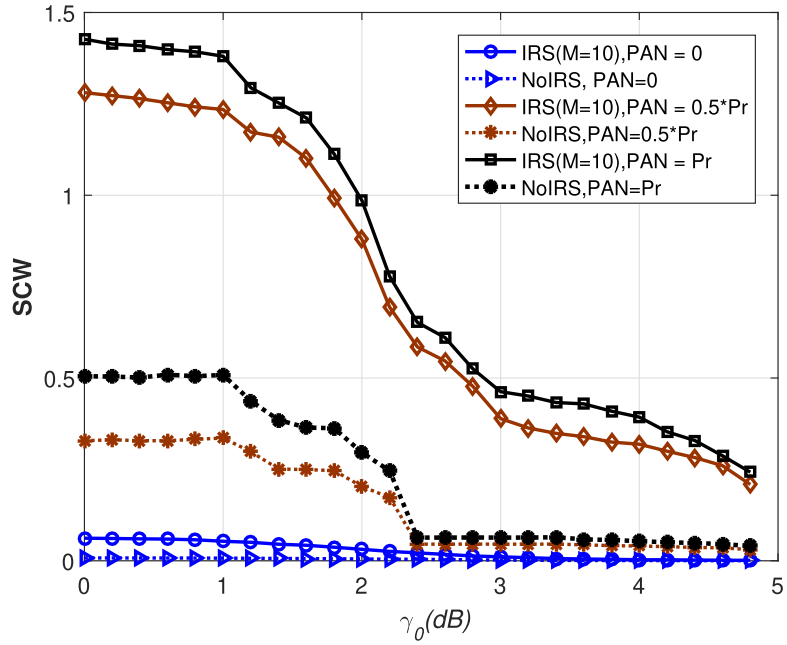


FIGURE 9. The location of the Eavesdropper and the IRS on SCW (a) and SEE (b).

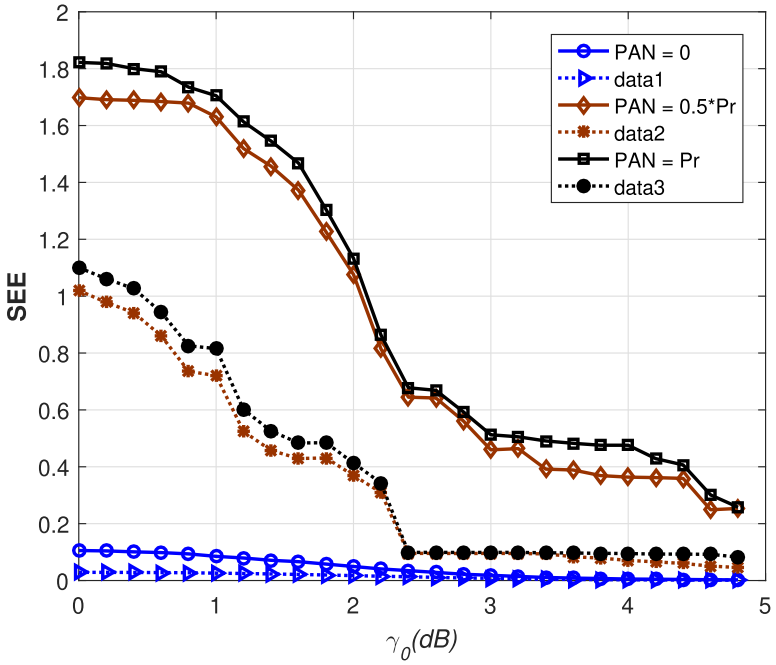
and 5 afford insight into the operational thresholds of the system based on two security quality indices: SCW and SEE. Concretely, for SCW, the average threshold in this experiment ranges from 0.5 to 3.75, while for SEE, it falls within the range of (1.2 to 4.2).

F. EFFECTS OF THE STRENGTH OF ARTIFICIAL NOISE ON SCW AND SEE

In this section, we analyze the impact of artificial noise AN on both metrics of secrecy performance as SCW and SEE in scenarios with and without the IRS's assistance. Three



(a)

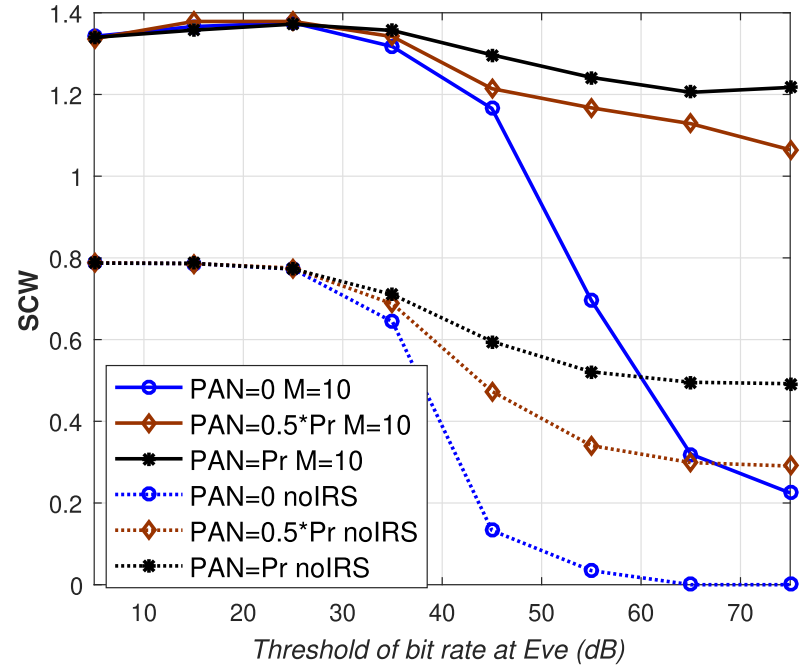


(b)

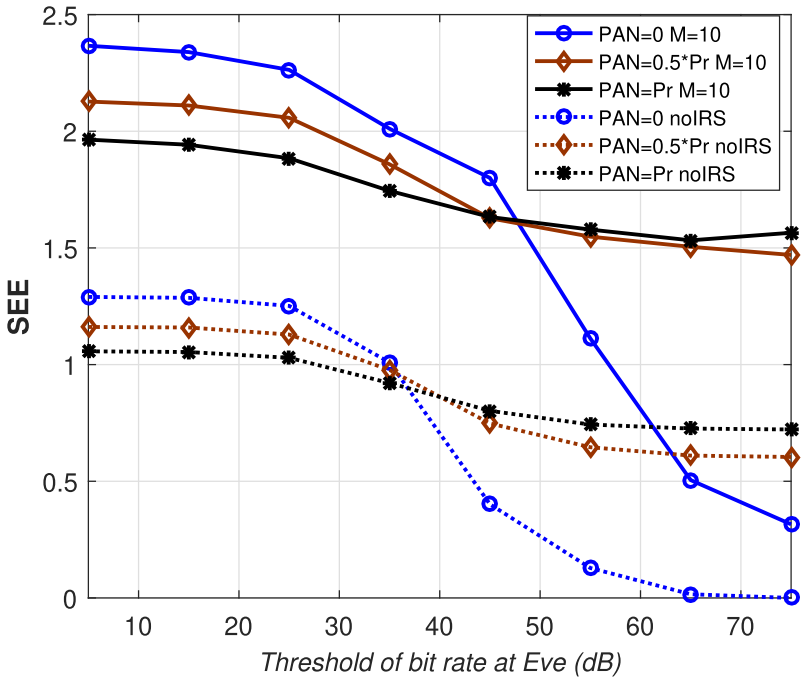
FIGURE 10. Effects of the strength of artificial noise on SCW (a) and SEE (b).

power levels of artificial noise are investigated: the absence of artificial noise ($P_{AN} = 0$), $P_{AN} = 0.5\,Pr$, and $P_{AN} = Pr$. Figures 7a and 7b show that the system employing an IRS exhibits significantly higher SCW and SEE than the system without IRS support. The solid lines represent the IRS-aided scenario, while the dashed lines depict the non-IRS scenario.

Furthermore, both SCW and SEE demonstrate higher values when employing artificial noise AN with increased levels. Particularly, when the system operates without artificial noise, despite utilizing an IRS, the system's security quality is lower than the scenario without an IRS but with the transmission of artificial noise. This implies that



(a)



(b)

FIGURE 11. Impacts of SNR at Eavesdropper on SCW (a) and SEE (b).

a combination of IRS and artificial noise is necessary to enhance the system's security capacity.

G. EFFECTS OF SNR AT EAVESDROPPER ON SCW AND SEE

Figures 9a and 9b investigate the influence of SINR at the eavesdropping node on SCW and SEE. This examination scrutinizes the impact of this parameter on scenarios with and without IRS support, distinguished by clear, direct lines, and clean lines on the graph, respectively.

In a broader context, the system applying the IRS consistently demonstrates improved SCW and SEE metrics. Specifically, focusing on SCW values, an increase in SNR at node Eave leads to a decrement in SCW. Notably, in instances without transmitting AN ($PAN = 0$), SCW experiences a

sharp decline, reaching values lower than when the system operates without IRS.

Conversely, SEE at low SNR values at node E (less than 50 dB) diminishes as PAN power escalates. As the SNR at E exceeds 50 dB, SEE exhibits variable values with different *PAN* settings. However, in scenarios without AN, there is a notable reduction in SEE, dipping below the values observed when the system operates without IRS. Given the distinct trends observed in SCW and SEE, ensuring reasonable security capacity for each user requires a trade-off: diminishing the system's SEE. The system's amalgamation of IRS and AN enhances overall security while balancing these metrics.

V. CONCLUSION

In this paper, we have investigated and analyzed the secrecy performance of the proposed system in the presence of eavesdroppers through two metrics: secrecy capacity and energy utilization. Specifically, the system's architecture included a cooperative NOMA framework in a multi-relaying network coupled with the IRS support implementation. The application of the IRS enhances the strength of the received signal for the destination users and mitigates the impact of eavesdropping nodes. To improve security quality across both evaluated metrics of the proposed system, we proposed the NSGA-II and R-NSGA-II algorithms to effectively address the multi-objective problem: optimizing the system's security quality while ensuring security capacity and enhancing the system's energy efficiency. Moreover, this paper investigated the impact of four relaying selection approaches to find the most suitable method for the proposed system. Furthermore, the effectiveness of the proposed algorithms and the influence of crucial system parameters have been examined in experimental scenarios. The findings underscore the computational efficiency and confidentiality efficacy of NSGA-II in comparison with R-NSGA-II and the ES method, both in scenarios involving IRS assistance and those without IRS. Finally, simulated outcomes ascertain the superior performance of the NOMA-relaying network integrated with IRS compared to IRS-absent system configurations.

APPENDIX A
PROOF OF LEMMA 1

Find the boundaries of α_1 and α_2 in the case of non-IRS system

This appendix provides the detailed proof for Lemma 1. To simply the presentation, we denote

$$X = \|h_k\|^2, Y = \left\{ \|h_{kj}\|^2, \left(\left\| \sum_{m=1}^{M} g_{km}\eta_m e^{i\theta_m} g_{mj} + h_{kj} \right\| \right)^2 \right\}.$$

By substituting equations (16)-(20) SINR in constraint (29.1) as $\min\left(\gamma_R^{x_1}, \gamma_{U_1}^{x_1,noIRS}\right) \geq \gamma_{01}$ and $\min\left(\gamma_R^{x_2}, \gamma_{U_2}^{x_2,noIRS}\right) \geq \gamma_{02}$.

We will consider the first constraint as

$$\begin{aligned}
&\min\left(\frac{P\alpha_1\|h_{k*}\|^2}{P\alpha_2\|h_{k*}\|^2+N_0}, \frac{P_r\alpha_1\|h_{k1}\|^2}{P_r\alpha_2\|h_{k1}\|^2+N_0}\right) \geq \gamma_{01}, \\
&\Leftrightarrow \begin{cases} \dfrac{P\alpha_1\|h_{k*}\|^2}{P\alpha_2\|h_{k*}\|^2+N_0} \geq \gamma_{01} \\ \dfrac{P_r\alpha_1\|h_{k1}\|^2}{P_r\alpha_2\|h_{k1}\|^2+N_0} \geq \gamma_{01} \end{cases} \\
&\Leftrightarrow \begin{cases} \dfrac{\frac{P\alpha_1}{N_0}\|h_{k*}\|^2}{\frac{P\alpha_2}{N_0}\|h_{k*}\|^2+1} \geq \gamma_{01} \\ \dfrac{\frac{P_r\alpha_1}{N_0}\|h_{k1}\|^2}{\frac{P_r\alpha_2}{N_0}\|h_{k1}\|^2+1} \geq \gamma_{01} \end{cases} \\
&\Leftrightarrow \begin{cases} \dfrac{P\alpha_1}{N_0}\|h_{k*}\|^2 \geq \gamma_{01}\dfrac{P\alpha_2}{N_0}\|h_{k*}\|^2 + \gamma_{01} \\ \dfrac{P_r\alpha_1}{N_0}\|h_{k1}\|^2 \geq \gamma_{01}\dfrac{P_r\alpha_2}{N_0}\|h_{k1}\|^2 + \gamma_{01} \end{cases} \\
&\Leftrightarrow \begin{cases} \alpha_1 \geq \gamma_{01}\alpha_2 + \gamma_{01}\dfrac{N_0}{P\|h_{k*}\|^2} \\ \alpha_1 \geq \gamma_{01}\alpha_2 + \gamma_{01}\dfrac{N_0}{P_r\|h_{k1}\|^2} \end{cases} \\
&\Leftrightarrow \begin{cases} \alpha_1 \geq \gamma_{01}\alpha_2 + \gamma_{01}\max\left\{\dfrac{N_0\|h_{k*}\|^2}{P}, \dfrac{N_0\|h_{k1}\|^2}{P_r}\right\} \\ \alpha_2 \leq \dfrac{\alpha_1}{\gamma_{01}} - \max\left\{\dfrac{N_0}{P\|h_{k*}\|^2}, \dfrac{N_0}{P_r\|h_{k1}\|^2}\right\}. \end{cases}
\end{aligned}$$

For the second constraint, we have:

$$\begin{aligned}
&\min\left(\frac{P\alpha_2\|h_{k*}\|^2}{N_0}, \frac{P_r\alpha_2\|h_{k2}\|^2}{N_0}\right) \geq \gamma_{02} \\
&\Leftrightarrow \alpha_2 \min\left(\frac{P\|h_{k*}\|^2}{N_0}, \frac{P_r\|h_{k2}\|^2}{N_0}\right) \geq \gamma_{02} \\
&\Leftrightarrow \alpha_2 \geq \frac{\gamma_{02}}{\min\left(\frac{P\|h_{k*}\|^2}{N_0}, \frac{P_r\|h_{k2}\|^2}{N_0}\right)} \\
&\frac{\gamma_{02}\gamma_{01}}{\min\left(\frac{P\|h_{k*}\|^2}{N_0}, \frac{P_r\|h_{k2}\|^2}{N_0}\right)} \\
&\quad + \gamma_{01}\max\left\{\frac{N_0}{P\|h_{k*}\|^2}, \frac{N_0}{P_r\|h_{k1}\|^2}\right\} \leq \alpha_1.
\end{aligned}$$

And then,

$$\begin{aligned}
\alpha_1 \in &\left[\frac{\gamma_{02}\gamma_{01}}{\min\left(\frac{P\|h_{k*}\|^2}{N_0}, \frac{P_r\|h_{k2}\|^2}{N_0}\right)} \right. \\
&\left. + \gamma_{01}\max\left\{\frac{N_0}{P\|h_{k*}\|^2}, \frac{N_0}{P_r\|h_{k1}\|^2}\right\}, 1 \right) \\
\alpha_2 \in &\left[\frac{\gamma_{02}}{\min\left(\frac{P\|h_{k*}\|^2}{N_0}, \frac{P_r\|h_{k2}\|^2}{N_0}\right)}, 1 \right).
\end{aligned} \tag{41}$$

From Eq.41, we can get the boundaries of α_1 and α_2 in the case of a non-IRS-aided system, as in Lemma 1.

APPENDIX B
PROOF OF LEMMA 2

Find the boundaries of α_1 and α_2 in the case of IRS-aided system

$$\min\left(\frac{P\alpha_1\|h_{k*}\|^2}{P\alpha_2\|h_{k*}\|^2+N_0},\frac{\alpha_1 P_r\left(\left|\left(g_{km}^H\Theta g_{m1}+h_{k1}^H\right)\right|\right)^2}{\alpha_2 P_r\left(\left|\left(g_{km}^H\Theta g_{m1}+h_{k1}^H\right)\right|\right)^2+N_0}\right)$$
$$\geq \gamma_{01}\alpha_1 \in \left[\frac{\gamma_{02}\gamma_{01}}{\min\left(\frac{P\|h_{k*}\|^2}{N_0},\frac{P_r\left(\left|\left(g_{km}^H\Theta g_{m2}+h_{k2}^H\right)\right|\right)^2}{N_0}\right)}\right.$$
$$\left.+\gamma_{01}\max\left\{\frac{N_0}{P\|h_{k*}\|^2},\frac{N_0}{P_r\left(\left|\left(g_{km}^H\Theta g_{m1}+h_{k1}^H\right)\right|\right)^2}\right\},1\right)$$

And,

$$\min\left(\frac{P\alpha_2\|h_{k*}\|^2}{N_0},\frac{\alpha_2 P_r\left(\left|\left(g_{km}^H\Theta g_{m2}+h_{k2}^H\right)\right|\right)^2}{N_0}\right)\geq\gamma_{02}$$

We have the boundaries of α_1 and α_2:

$$\alpha_1 \in \left[\frac{\gamma_{02}\gamma_{01}}{\min\left(\frac{P\|h_{k*}\|^2}{N_0},\frac{P_r\left(\left|\left(g_{km}^H\Theta g_{m2}+h_{k2}^H\right)\right|\right)^2}{N_0}\right)}\right.$$
$$\left.+\gamma_{01}\max\left\{\frac{N_0}{P\|h_{k*}\|^2},\frac{N_0}{P_r\left(\left|\left(g_{km}^H\Theta g_{m1}+h_{k1}^H\right)\right|\right)^2}\right\},1\right), \tag{42}$$

and

$$\alpha_2 \in \left[\frac{\gamma_{02}}{\min\left(\frac{P\|h_{k*}\|^2}{N_0},\frac{P_r\left(\left|\left(g_{km}^H\Theta g_{m2}+h_{k2}^H\right)\right|\right)^2}{N_0}\right)},1\right). \tag{43}$$

Finally, from Eq.42-43, we can get the boundaries of α_1 and α_2 in the case of an IRS-aided system, as in Lemma .

REFERENCES

[1] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y. A. Zhang, "The roadmap to 6G: AI empowered wireless networks," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 84–90, Aug. 2019.
[2] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May 2020.
[3] M. Mahbub and R. M. Shubair, "Analysis of IRS-assisted NOMA for 6G wireless communications," 2022, *arXiv:2211.13045*.
[4] S. Kumar, P. Yadav, M. Kaur, and R. Kumar, "A survey on IRS NOMA integrated communication networks," *Telecommun. Syst.*, vol. 80, no. 2, pp. 277–302, Jun. 2022.
[5] Z. Tang, T. Hou, Y. Liu, J. Zhang, and C. Zhong, "A novel design of RIS for enhancing the physical layer security for RIS-aided NOMA networks," *IEEE Wireless Commun. Lett.*, vol. 10, no. 11, pp. 2398–2401, Nov. 2021.
[6] B. Ji, Y. Wang, K. Song, C. Li, H. Wen, V. G. Menon, and S. Mumtaz, "A survey of computational intelligence for 6G: Key technologies, applications and trends," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7145–7154, Oct. 2021.
[7] A. Fayad, T. Cinkler, J. Rak, and M. Jha, "Design of cost-efficient optical fronthaul for 5G/6G networks: An optimization perspective," *Sensors*, vol. 22, no. 23, p. 9394, Dec. 2022.
[8] T. Mezair, Y. Djenouri, A. Belhadi, G. Srivastava, and J. C.-W. Lin, "A sustainable deep learning framework for fault detection in 6G Industry 4.0 heterogeneous data environments," *Comput. Commun.*, vol. 187, pp. 164–171, Apr. 2022.
[9] E. G. Johnson, A. D. Kathman, D. H. Hochmuth, A. L. Cook, D. R. Brown, and W. F. Delaney, "Advantages of genetic algorithm optimization methods in diffractive optic design," *Proc. SPIE*, vol. 10271, pp. 56–76, Dec. 1993.
[10] A. B. Alnajjar, A. M. Kadim, R. A. Jaber, N. A. Hasan, E. Q. Ahmed, M. S. M. Altaei, and A. L. Khalaf, "Wireless sensor network optimization using genetic algorithm," *J. Robot. Control*, vol. 3, no. 6, pp. 827–835, 2022.
[11] A. Davahli, M. Shamsi, and G. Abaei, "Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 11, pp. 5581–5609, Nov. 2020.
[12] D. J. Bahadur and L. Lakshmanan, "A novel method for optimizing energy consumption in wireless sensor network using genetic algorithm," *Microprocess. Microsyst.*, vol. 96, Feb. 2023, Art. no. 104749.
[13] D. Vidyarthi and L. Khanbary, "Multi-objective optimization for channel allocation in mobile computing using NSGA-II," *Int. J. Netw. Manag.*, vol. 21, no. 3, pp. 247–266, 2011.
[14] X. Dong, L. Cheng, G. Zheng, and T. Wang, "Multi-objective optimization method for spectrum allocation in cognitive heterogeneous wireless networks," *AIP Adv.*, vol. 9, no. 4, Apr. 2019.
[15] Z. Fei, B. Li, S. Yang, C. Xing, H. Chen, and L. Hanzo, "A survey of multi-objective optimization in wireless sensor networks: Metrics, algorithms, and open problems," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 550–586, 1st Quart., 2017.
[16] M. Noor-A-Rahim, F. Firyaguna, J. John, M. O. Khyam, D. Pesch, E. Armstrong, H. Claussen, and H. V. Poor, "Toward Industry 5.0: Intelligent reflecting surface in smart manufacturing," *IEEE Commun. Mag.*, vol. 60, no. 10, pp. 72–78, Oct. 2022.
[17] W. Mei, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless networks: From single-reflection to multireflection design and optimization," *Proc. IEEE*, vol. 110, no. 9, pp. 1380–1400, Sep. 2022.
[18] W. Jiang and F.-L. Luo, "Intelligent reflecting surface-aided communications for 6G," in *6G Key Technologies: A Comprehensive Guide*. Hoboken, NJ, USA: Wiley, 2023, pp. 295–362.
[19] Y. Wang, B. Ji, and D. Li, "IRS assist wireless communication: Scenarios, advantages, convergence," *J. Comput. Electron. Inf. Manage.*, vol. 10, no. 3, pp. 40–45, May 2023.
[20] M. Mahbub and R. M. Shubair, "Intelligent reflecting surfaces in UAV-assisted 6G networks: An approach for enhanced propagation and spectral characteristics," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Jun. 2022, pp. 1–6.
[21] D. Tagliaferri, M. Mizmizi, R. A. Ayoubi, G. G. Gentili, and U. Spagnolini, "Conformal intelligent reflecting surfaces for 6G V2V communications," in *Proc. 1st Int. Conf. 6G Netw. (6GNet)*, Jul. 2022, pp. 1–8.
[22] A. Shakeel, A. Iqbal, A. Nauman, R. Hussain, X. Li, and K. Rabie, "6G driven vehicular tracking in smart cities using intelligent reflecting surfaces," in *Proc. IEEE 97th Veh. Technol. Conf. (VTC-Spring)*, Jun. 2023, pp. 1–7.
[23] M. Mounir, M. B. El_Mashade, and A. M. Aboshosha, "On the selection of power allocation strategy in power domain non-orthogonal multiple access (PD-NOMA) for 6G and beyond," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, p. e4289, Jun. 2022.
[24] Aws. Z. Yonis and A. Nawaf, "Investigation of evolving multiple access technologies for 5G wireless system," in *Proc. 8th Int. Eng. Conf. Sustain. Technol. Develop. (IEC)*, Erbil, Iraq, Feb. 2022, pp. 118–122.
[25] Y. Liu, W. Yi, Z. Ding, X. Liu, O. Dobre, and N. Al-Dhahir, "Application of NOMA in 6G networks: Future vision and research opportunities for next-generation multiple access," 2021, *arXiv:2103.02334*.
[26] Y. Liu, S. Zhang, X. Mu, Z. Ding, R. Schober, N. Al-Dhahir, E. Hossain, and X. Shen, "Evolution of NOMA toward next generation multiple access (NGMA) for 6G," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 4, pp. 1037–1071, Apr. 2022.
[27] M. Ghous, A. K. Hassan, Z. H. Abbas, G. Abbas, A. Hussien, and T. Baker, "Cooperative power-domain NOMA systems: An overview," *Sensors*, vol. 22, no. 24, p. 9652, Dec. 2022.
[28] M. Zeng, W. Hao, O. A. Dobre, and Z. Ding, "Cooperative NOMA: State of the art, key techniques, and open challenges," *IEEE Netw.*, vol. 34, no. 5, pp. 205–211, Sep. 2020.

[29] X. Li, Z. Xie, Z. Chu, V. G. Menon, S. Mumtaz, and J. Zhang, "Exploiting benefits of IRS in wireless powered NOMA networks," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 175–186, Mar. 2022.
[30] W. Jiang and H. D. Schotten, "Orthogonal and non-orthogonal multiple access for intelligent reflection surface in 6G systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Glasgow, U.K., Mar. 2023, pp. 1–6.
[31] A. Ihsan, W. Chen, M. Asif, W. U. Khan, and J. Li, "Energy-efficient IRS-aided NOMA beamforming for 6G wireless communications," 2022, *arXiv:2203.16099*.
[32] J. Choi, L. Cantos, J. Choi, and Y. H. Kim, "Sum rate optimization of IRS-aided uplink muliantenna NOMA with practical reflection," *Sensors*, vol. 22, no. 12, p. 4449, Jun. 2022.
[33] A. L. Thi, H. N. Thi, T. P. Viet, and V. N. Q. Bao, "Performance evaluation of cooperative NOMA-IRS network using particle swarm optimization," in *Proc. 8th NAFOSTED Conf. Inf. Comput. Sci. (NICS)*, Hanoi, Vietnam, Dec. 2021, pp. 296–301.
[34] F. Fang, Y. Xu, Q.-V. Pham, and Z. Ding, "Energy-efficient design of IRS-NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 14088–14092, Nov. 2020.
[35] M. Fu, Y. Zhou, and Y. Shi, "Intelligent reflecting surface for downlink non-orthogonal multiple access networks," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2019, pp. 1–6.
[36] B. Zheng, Q. Wu, and R. Zhang, "Intelligent reflecting surface-assisted multiple access with user pairing: NOMA or OMA?" *IEEE Commun. Lett.*, vol. 24, no. 4, pp. 753–757, Apr. 2020.
[37] G. Yang, X. Xu, and Y.-C. Liang, "Intelligent reflecting surface assisted non-orthogonal multiple access," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, May 2020, pp. 1–6.
[38] Z. Ding, R. Schober, and H. V. Poor, "On the impact of phase shifting designs on IRS-NOMA," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1596–1600, Oct. 2020.
[39] M. Mitev, A. Chorti, H. V. Poor, and G. P. Fettweis, "What physical layer security can do for 6G security," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 375–388, 2023.
[40] J. D. V. Sánchez, L. Urquiza-Aguiar, M. C. P. Paredes, and D. P. M. Osorio, "Survey on physical layer security for 5G wireless networks," *Ann. Telecommun.*, vol. 76, pp. 155–174, Sep. 2021.
[41] T. A. Le and H. Y. Kong, "Evaluating the performance of cooperative NOMA with energy harvesting under physical layer security," *Wireless Pers. Commun.*, vol. 108, no. 2, pp. 1037–1054, Sep. 2019.
[42] A. Souzani, M. A. Pourmina, P. Azmi, and M. Naser-Moghadasi, "Physical layer security enhancement via IRS based on PD-NOMA and cooperative jamming," *IEEE Access*, vol. 11, pp. 65956–65967, 2023.
[43] M. Ji, J. Chen, L. Lv, Q. Wu, Z. Ding, and L. Yang, "Simultaneous information relaying and jamming via IRS to secure NOMA networks," in *Proc. 14th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nov. 2022, pp. 1119–1124.
[44] Y. Pei, X. Yue, Y. Yao, X. Li, H. Wang, and D.-T. Do, "Secrecy communications of intelligent reflecting surfaces aided NOMA networks," *Phys. Commun.*, vol. 52, Jun. 2022, Art. no. 101691.
[45] H. Ma, Y. Zhang, S. Sun, T. Liu, and Y. Shan, "A comprehensive survey on NSGA-II for multi-objective optimization and applications," *Artif. Intell. Rev.*, vol. 56, no. 12, pp. 15217–15270, Dec. 2023, doi: 10.1007/s10462-023-10526-z.
[46] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: NSGA-II," *IEEE Trans. Evol. Comput.*, vol. 6, no. 2, pp. 182–197, Apr. 2002.
[47] Y. Cheng, K. H. Li, Y. Liu, and K. C. Teh, "Outage performance of downlink IRS-assisted NOMA systems," in *Proc. IEEE Global Commun. Conf.*, Taipei, Taiwan, Dec. 2020, pp. 1–6.
[48] M. Abouhawwash and M. A. Jameel, "KKT proximity measure versus augmented achievement scalarization function," *Int. J. Comput. Appl.*, vol. 182, no. 24, pp. 1–7, Oct. 2018.
[49] A. Konak, D. W. Coit, and A. E. Smith, "Multi-objective optimization using genetic algorithms: A tutorial," *Rel. Eng. Syst. Saf.*, vol. 91, no. 9, pp. 992–1007, Sep. 2006.

THUC KIEU-XUAN received the Engineering degree in electronics and telecommunication and the master's degree in information processing and communication from Hanoi University of Science and Technology, Hanoi, Vietnam, in 1999 and 2004, respectively, and the Ph.D. degree in electrical engineering from the University of Ulsan, South Korea, in 2012. He is currently a Lecturer with Hanoi University of Industry, Hanoi. His research interests include signal processing, embedded systems, wireless sensor networks, and wireless communication systems.

HONG NGUYEN-THI received the B.E. degree in electrical engineering from Le Quy Don Technical University, Vietnam, in 2012, and the master's degree in information engineering from the Posts and Telecommunication Institute of Technology, in 2023. From 2012 to 2017, she was an Information Technology Assistant with NOC, Vietnam. Since 2017, she has been a Teacher with the Faculty of Telecommunications Engineering, Technical College of Communications, Vietnam. Her major research interests include cooperative NOMA communications systems, MIMO communication, physical-layer security, energy harvesting, intelligent reflecting systems, and artificial intelligence.

ANH LE-THI received the B.E. degree in electrical engineering and the M.E. degree in information systems from Le Quy Don Technical University, Vietnam, in 2011 and 2015, respectively, and the Ph.D. degree from the Department of Electrical Engineering, University of Ulsan, South Korea, in 2020. She is currently a Lecturer with Hanoi University of Industry, Hanoi, Vietnam. Her major research interests include cooperative NOMA communications systems, MIMO communication, physical layer security, IRS, and cyber security.