# Low-Complexity Metaheuristic Design for STAR-RIS Assisted Secure NOMA-ISAC Networks


1st Hoang-Lai Pham
*Viettel High Technology Industries Corporation, Viettel Group*
Hanoi, Vietnam
laiph3@viettel.com.vn

2nd Trung Quang Pham
*Viettel High Technology Industries Corporation, Viettel Group*
Hanoi, Vietnam
trungpq12@viettel.com.vn

3rd Dang Y Hoang
*Viettel High Technology Industries Corporation, Viettel Group*
Hanoi, Vietnam
yhd10@viettel.com.vn

4th Viet Hai Dinh
*Viettel High Technology Industries Corporation, Viettel Group*
Hanoi, Vietnam
haidv29@viettel.com.vn

5th Khoa Hoang Thu Nguyen
*Viettel High Technology Industries Corporation, Viettel Group*
Hanoi, Vietnam
khoanht@viettel.com.vn

6th Tuan Anh Pham
*Viettel High Technology Industries Corporation, Viettel Group*
Hanoi, Vietnam
tuanpa44@viettel.com.vn



***Abstract*—In this paper, we study the integration of the non-orthogonal multiple access (NOMA) with simultaneously transmitting and reflecting reconfigurable intelligent surfaces (STAR-RIS) for secure integrated sensing and communication (ISAC) systems under multiple eavesdroppers. A multi-user scenario is considered where each sensing target can act as a potential eavesdropper, reflecting practical deployment challenges. To enhance physical layer security (PLS) while ensuring sensing performance, we jointly optimize the base station beamforming vectors, artificial noise, and STAR-RIS coefficients with the objective of maximizing the sum secrecy rate under the minimum beampattern gain constraints. The formulated problem is highly non-convex due to coupled NOMA decoding and STAR-RIS unit-modulus constraints. To efficiently tackle this challenge and enable a fast and practically implementable optimization, we adopt a low-complexity metaheuristic framework, where the whale optimization algorithm (WOA) is employed as a representative example. Simulation results validate the effectiveness of the proposed design, showing significant secrecy and sensing performance gains over benchmark schemes.**



***Index Terms*—Integrated sensing and communication (ISAC), Physical layer security (PLS), Simultaneously transmitting and reflecting reconfigurable intelligent surfaces (STAR-RIS), Non-orthogonal multiple access (NOMA), Whale optimization algorithm (WOA), Low-complexity.**


## I. Introduction

Integrated sensing and communication (ISAC) is regarded as a crucial technology for enabling sixth-generation (6G) networks, since it allows communication and sensing to share spectrum, hardware, and energy resources. By integrating these functionalities into a unified system, ISAC can improve spectrum efficiency, reduce deployment cost, and enable emerging applications such as unmanned aerial vehicles, smart cities, and the Internet of Things [1]. However, reusing signals for both communication and sensing introduces additional security challenges. In particular, sensing targets may function as potential eavesdroppers capable of intercepting confidential information. Consequently, physical layer security (PLS) emerges as an indispensable element in the design of ISAC systems [2], [3]. The key idea is to intentionally degrade the signal quality at potential eavesdroppers while ensuring that legitimate users maintain their required quality-of-service (QoS). To guarantee secure transmission, the studies in [2], [3] have employed artificial noise (AN) injection at the transmitter to obscure confidential signals from unauthorized receivers, while simultaneously optimizing beamforming vectors to satisfy the signal-to-interference-plus-noise ratio (SINR) constraints of legitimate users. Other approaches focus on optimizing the secrecy rate by balancing the power allocation between communication and sensing signals [4]. In addition, robust beamforming designs have been proposed to suppress information leakage toward sensing targets under imperfect channel state information [5].

Recent advances in secure ISAC have highlighted STAR-RIS as a key technology for jointly enhancing communication and sensing performance [6]. By enabling adaptive control of electromagnetic propagation in both transmission and reflection domains, STAR-RIS provides a powerful means to strengthen secrecy capacity [7]. Early contributions, such as [8], formulated secrecy rate maximization problems under eavesdropping scenarios, while ensuring minimum sensing SINR through joint optimization of system parameters. To address channel variability, [9] introduced a coupled phase-shift STAR-RIS architecture that integrates time-switching and energy-splitting protocols. Furthermore, robust secure ISAC under channel uncertainty is investigated in [10], where the optimization jointly involves BS beamforming, STAR-RIS coefficients, and AN. More recent work has further extended the applicability of STAR-RIS to multi-user and multi-eavesdropper environments, confirming its effectiveness in practical secure ISAC deployments [10], [11].

In parallel, multiple access techniques provide additional benefits for enhancing the performance of ISAC systems, among which are non-orthogonal multiple access (NOMA) [12], orthogonal multiple access (OMA) [13], rate-splitting

multiple access (RSMA) [14], etc. Notably, integrating NOMA into ISAC systems enables simultaneous support for a larger number of users by allowing multiple users to share the same time and frequency resources [12], [15]. Incorporating NOMA into ISAC systems has been shown to significantly improve spectral efficiency through successive interference cancellation (SIC). Moreover, incorporating PLS into NOMA-based ISAC systems is of great importance, as the power-domain nature of NOMA may expose users to additional security risks, particularly for users under weak channel conditions with increased susceptibility to eavesdropping due to the reliance on higher transmit power, necessitating joint design of secure transmission and resource allocation [4], [16], [17]. The authors in [17] model a PLS-enhanced NOMA-aided ISAC system, where a secure precoding scheme is developed to maximize the sum secrecy rate of multiple users via AN while simultaneously exploiting NOMA signals for target detection.

Although NOMA and STAR-RIS have each shown considerable advantages in ISAC systems, their joint capability to enhance physical layer security remains largely underexplored. Most existing studies either overlook security aspects [18], [19], employ conventional RIS instead of STAR-RIS [4], [20] or confines the system model to single target cases [21]. Sinvestigates full-space STAR-RIS aided NOMA-ISAC systems with a focus on improving overall sensing and communication efficiency, whereas [18] addresses fairness optimization between users and sensing targets, both works omit secure transmission design. In [20], a NOMA-ISAC framework is studied with secure beamforming, where RIS is used to enhance legitimate communications under internal and external eavesdroppers. In [21], a STAR-RIS-enabled secure ISAC system with NOMA transmission was taken into account, where the base station (BS) jointly served multiple users and a sensing target. By jointly designing NOMA beamforming, artificial jamming, and STAR-RIS coefficients, the proposed in [21] model enhances PLS while simultaneously guaranteeing reliable target sensing. In addition, most of the aforementioned works in [18]–[21] rely on conventional optimization techniques to solve non-convex problems, which often lead to high computational complexity. Such approaches become less practical in large-scale STAR-RIS aided NOMA-ISAC systems with multiple users and eavesdroppers. In contrast, metaheuristic algorithms such as the whale optimization algorithm (WOA) in [22] offer a low-complexity yet effective alternative with strong global search capability, does not require gradient information or convex reformulation, and is straightforward to implement in practice. The joint design of STAR-RIS assisted secure NOMA-ISAC with low-complexity metaheuristics for secure communication and accurate sensing in multi-user, multi-target scenarios remains an open problem.

In this work, we study the integration of STAR-RIS into NOMA-assisted ISAC systems, aiming to optimize secure communication in multi-user and multi-target scenarios. The main contributions are summarized as follows:

- A STAR-RIS enabled NOMA-ISAC scheme designed to strengthen PLS under multi-user, multi-target conditions, where sensing targets are treated as potential eavesdroppers
- We formulate a joint optimization problem that maximizes the sum secrecy rate across communication users, under the constraints of SIC decoding, minimum beampattern gain, and BS power budget.
- To address the non-convexity of the formulated problem, we propose a low-complexity algorithm leveraging the Whale Optimization Algorithm (WOA).
- The obtained simulation results confirm the superiority of the proposed approach in realizing a desirable trade-off between communication security and sensing accuracy, outperforming conventional baseline schemes.

## II. System Model and Problem Formulation

### A. System Model

As illustrated in Fig. 1, we consider a STAR-RIS assisted secure NOMA-ISAC system. The system consists of a base station (BS), denoted as $B$, equipped with $M_B$ antennas in a uniform linear array (ULA), and a STAR-RIS, denoted as $S$, comprising $M_S$ elements arranged in a uniform planar array (UPA). Operating in energy-splitting mode, the STAR-RIS simultaneously reflects and transmits signals, with the corresponding diagonal matrices are represented by $\mathbf{\Gamma}_r$ and $\mathbf{\Gamma}_t$, respectively. The system serves $K_N$ NOMA communication users (CUs) located in the reflection region, and $K_T$ sensing targets (STs) situated in the transmission region. Each CU and ST is assumed to have a single receive antenna. Let $\mathcal{N} = \{1, 2, \ldots, K_N\}$ denote the set of all NOMA users, $\mathcal{T} = \{1, 2, \ldots, K_T\}$ denote the set of sensing targets. Furthermore, the direct BS-to-target links are blocked by environmental obstructions.

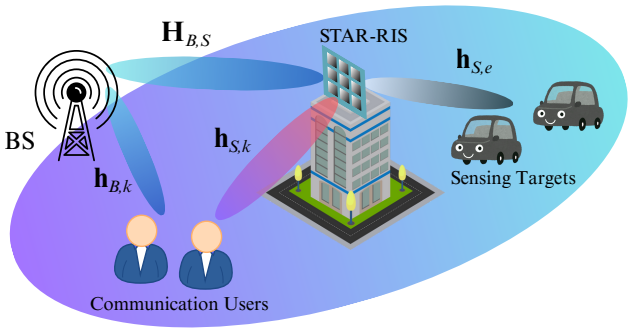



Fig. 1: Secure ISAC system model supported by STAR-RIS.

An NOMA signal $x_k \in \mathbb{C}$ is transmitted from BS to the $k$-th NOMA user $k \in \mathcal{N}$ via a dedicated beamforming vector $\mathbf{w}_k \in \mathbb{C}^{M_B}$. The set of all beamforming vectors is denoted as $\mathbf{W}_i = [\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_{K_N}]$. In addition, for simultaneous target sensing and secure communication, artificial noise $\mathbf{x}_a \in \mathbb{C}^{M_B}$ using a beamforming matrix $\mathbf{W}_a \in \mathbb{C}^{M_B \times M_B}$ is

superimposed with the information signal at the BS. Accordingly, the overall transmit signal $\mathbf{z}$ is given by

$$\mathbf{z} = \mathbf{W}_a \mathbf{x}_a + \sum_{k \in \mathcal{N}} \mathbf{w}_k x_k, \tag{1}$$

where $\mathbb{E}[|x_k|^2] = \mathbb{E}[\|\mathbf{x}_a\|^2] = 1$.

Under the assumption that the transmitted signals are independent and have unit power normalization, the overall transmit power at the BS can be obtained as

$$P_B = \mathbb{E}\left\{\|\mathbf{z}\|^2\right\} = \mathrm{tr}(\mathbf{R}_a) + \sum_{k \in \mathcal{N}} \|\mathbf{w}_k\|^2, \tag{2}$$

where $\mathbf{R}_a = \mathbf{W}_a \mathbf{W}_a^H$.

The BS-to-STAR-RIS channel is represented by the MIMO channel matrix $\mathbf{H}_{B,S} \in \mathbb{C}^{M_B \times M_S}$. The direct channel from BS to $k$-th NOMA user is denoted by $\mathbf{h}_{B,k} \in \mathbb{C}^{M_B}$, while the channel between the STAR-RIS and NOMA user is denoted by $\mathbf{h}_{S,k} \in \mathbb{C}^{M_S}$. For the STs, the channel from the STAR-RIS to the target is denoted by $\mathbf{h}_{S,e} \in \mathbb{C}^{M_S}$. Accordingly, the received signal at NOMA user $k \in \mathcal{N}$ can be expressed as

$$y_k = \left(\mathbf{h}_{B,k}^H + \mathbf{h}_{S,k}^H \mathbf{\Gamma}_r \mathbf{H}_{B,S}\right) \mathbf{z} + n_k, \tag{3}$$

where $n_k \sim \mathcal{CN}(0, \sigma^2)$ is the additive white Gaussian noise (AWGN) at the NOMA users.

In the considered model, NOMA is applied to support terrestrial communications. Based on NOMA, the first user, having the weakest channel gain, decodes its own message under the interference of all others. Each user $k = 2, \ldots, K_N$ executes SIC by sequentially decoding and subtracting the signals of users $i < k$, and then demodulates its desired message. The STAR-RIS–user channel gains can be represented as

$$\|\mathbf{h}_{B,1}\|^2 \leq \cdots \leq \|\mathbf{h}_{B,K_N}\|^2, \tag{4}$$

For notational simplicity, the phase-shift vector of the STAR-RIS is defined as

$$\mathbf{u}_d^H = [u_{d,1}, \ldots, u_{d,M_S}],$$

In particular, $u_{d,m}$ corresponds to the transmission component for $d = t$ and the reflection component for $d = r$. Hence, we have

$$\mathbf{h}_{S,k}^H \mathbf{\Gamma}_r \mathbf{H}_{B,S} = \mathbf{u}_r^H \mathbf{H}_k, \tag{5a}$$

$$\mathbf{h}_{S,e}^H \mathbf{\Gamma}_t \mathbf{H}_{B,S} = \mathbf{u}_t^H \mathbf{H}_e, \tag{5b}$$

where $\mathbf{H}_k = \mathrm{diag}(\mathbf{h}_{S,k}^H)\mathbf{H}_{B,S}, \mathbf{H}_e = \mathrm{diag}(\mathbf{h}_{S,e}^H)\mathbf{H}_{B,S}$.

In line with conventional NOMA operation, SIC demodulation order constraints is specified as

$$\begin{aligned} |\mathbf{u}_r^H \mathbf{H}_k \mathbf{w}_1|^2 &\geq |\mathbf{u}_r^H \mathbf{H}_k \mathbf{w}_2|^2 \geq \cdots \geq |\mathbf{u}_r^H \mathbf{H}_k \mathbf{w}_k|^2 \\ &\geq \max_{j \in \mathcal{N}, j > k} |\mathbf{u}_r^H \mathbf{H}_k \mathbf{w}_j|^2, \quad \forall k \in \mathcal{N} \end{aligned} \tag{6}$$

For implementing NOMA SIC, the $k$-th user is required to successively demodulate the signals of users with weaker channel conditions. Accordingly, the SINR for the $k$-th user to decode the $i$-th user's signal ($i \leq k$) can be formulated as

$$\gamma_{k,i} = \frac{|\mathbf{u}_r^H \mathbf{H}_k \mathbf{w}_i|^2}{\sum_{l=i+1}^{K_N} |\mathbf{u}_r^H \mathbf{H}_k \mathbf{w}_l|^2 + \|\mathbf{u}_r^H \mathbf{H}_k \mathbf{W}_a\|^2 + \sigma^2}. \tag{7}$$

Hence, the transmission rate for the $k$-th user to decode the $i$-th user's signal ($i \leq k$) can be formulated as

$$R_{k,i} = \log_2\left(1 + \gamma_{k,i}\right). \tag{8}$$

We consider the target as an eavesdropper aiming to capture the confidential information intended for the legitimate users. Noting that sensing targets typically cannot perform SIC, the $j$-th eavesdropping SINR associated with the $i$-th user is $R_{j,i}^e = \log_2(1 + \gamma_{j,i}^e)$, where $\gamma_{j,i}^e$ can be expressed as

$$\gamma_{j,i}^e = \frac{|\mathbf{u}_t^H \mathbf{H}_j \mathbf{w}_i|^2}{\sum_{\substack{l=1 \\ l \neq i}}^{K} |\mathbf{u}_t^H \mathbf{H}_j \mathbf{w}_l|^2 + \|\mathbf{u}_t^H \mathbf{H}_j \mathbf{W}_a\|^2 + \sigma^2}. \tag{9}$$

Accordingly, the secrecy rate achieved for the $k$-th user to decode the $i$-th user's signal ($i < k$) is given by

$$R_{k,i}^{sec} = \left[R_{k,i} - \max_{j \in \mathcal{T}} R_{j,i}^e\right]^+, \quad \forall k, i \in \mathcal{N}, \tag{10}$$

where $[x]^+ \triangleq \max\{x, 0\}$. If $\exists R_{j,i}^e \geq R_{k,i}$, the value of $R_{k,i}^{sec}$ becomes zero. Therefore, $[x]^+$ can be disregarded and is not further discussed throughout this paper.

In addition, the achievable secrecy rate for the $i$-th user is computed based on the minimum rate over all users $k \geq i$. It is assumed that the SINR observed at the $i$-th user is smaller than the SINR observed at subsequent users decoding the $i$-th user's signal. Consequently, we have

$$R_i^{sec} = \min_{k \in \mathcal{N}, k > i} R_{k,i}^{sec}, \quad \forall i \in \mathcal{N}. \tag{11}$$

For system evaluation, the beampattern gain from the STAR-RIS to the $e$-th target is used as the sensing performance indicator, given by

$$\begin{aligned} \mathcal{B}_e &= \mathbb{E}\left(\left|\mathbf{h}_{S,e}^H \mathbf{\Gamma}_t \mathbf{H}_{B,S} \mathbf{z}\right|^2\right) \\ &= \mathbf{h}_{S,e}^H \mathbf{\Gamma}_t \mathbf{H}_{B,S} \left(\mathbf{R}_a + \sum_{k \in \mathcal{N}} \mathbf{w}_k \mathbf{w}_k^H\right) \mathbf{H}_{B,S}^H \mathbf{\Gamma}_t^H \mathbf{h}_{S,e}. \end{aligned} \tag{12}$$

### *B. Problem Formulation*

For secure communication of NOMA users, the transmit beamforming $\mathbf{w}_k$, artificial noise $\mathbf{W}_a$, and the phase-shift vector of the STAR-RIS $\mathbf{u}_d$ ($d \in \{t, r\}$) are jointly optimized to maximize the sum secrecy rate. Accordingly, the joint optimization problem can be expressed as

$$\max_{\mathbf{W}_a,\mathbf{W}_i,\mathbf{u}} \quad \sum_{i=1}^{K_N} R_i^{sec} \tag{13a}$$

$$\text{s.t.} \quad R_{k,k} \geq \epsilon_k, \quad \forall k \in \mathcal{N}, \tag{13b}$$

$$\mathcal{B}_e \geq \kappa_e, \quad \forall e \in \mathcal{T}, \tag{13c}$$

$$|\mathbf{u}_r^H \mathbf{H}_k \mathbf{w}_1|^2 \geq \cdots \geq |\mathbf{u}_r^H \mathbf{H}_k \mathbf{w}_k|^2$$
$$\cdots \geq \max_{j=k+1,\ldots,K_N} |\mathbf{u}_r^H \mathbf{H}_k \mathbf{w}_j|^2, \tag{13d}$$

$$\|\mathbf{W}_a\|^2 + \sum_{k\in\mathcal{N}} \|\mathbf{w}_k\|^2 \leq P, \tag{13e}$$

$$|\mathbf{u}_{t,n}|^2 + |\mathbf{u}_{r,n}|^2 = 1, \quad \forall n, \tag{13f}$$

where $\epsilon_k$ denotes the required rate threshold at each legitimate user. To guarantee satisfactory target detection, constraint (13c) ensures that the beampattern gain from the STAR-RIS towards the target is no lower than the threshold $\kappa_e$. In (13e), $P$ represents the maximum transmit power at the BS. Finally, constraint (13f) specifies the passive beamforming condition at the STAR-RIS.

Due to the strong coupling among the optimization variables, problem (13a)–(13d) is challenging to solve directly. To overcome this difficulty, we develop a proposed iterative algorithm based on metaheuristics in the next section.

## III. Proposed Iterative Algorithm Based on Metaheuristic

### A. Solution Encoding

The formulated secrecy rate maximization problem in (13) is highly non-convex due to the joint optimization of BS beamforming, artificial noise, and STAR-RIS coefficients. To overcome these challenges, we adopt a metaheuristic approach based on the whale optimization algorithm, which is known for its strong global search capability and low complexity in solving non-convex optimization problems.

To apply WOA, the optimization variables are encoded into a search agent (solution vector) as

$$\mathbf{x} = \big[\Re\{\mathrm{vec}(\mathbf{W}_a)\}, \Im\{\mathrm{vec}(\mathbf{W}_a)\}, \ \Re\{\mathrm{vec}(\mathbf{W}_i)\},$$
$$\Im\{\mathrm{vec}(\mathbf{W}_i)\}, \ \Re\{\mathbf{u}_t\}, \Im\{\mathbf{u}_t\}, \ \Re\{\mathbf{u}_r\}, \Im\{\mathbf{u}_r\}\big], \tag{14}$$

where each agent $\mathbf{x}$ represents a candidate solution consisting of the BS beamforming vectors, the artificial noise matrix, and the transmission/reflection coefficients of the STAR-RIS. The dimension of $\mathbf{x}$ depends on the number of users, antennas, and STAR-RIS elements.

### B. Fitness Function

The fitness function for each agent is defined as the negative sum secrecy rate:

$$f(\mathbf{x}) = -\sum_{k=1}^{K_N} R_k^{\mathrm{sec}}(\mathbf{x}), \tag{15}$$

where $R_k^{\mathrm{sec}}(\mathbf{x})$ is the secrecy rate of the $k$-th user. Infeasible solutions violating the constraints in (13) are penalized with a large positive value to ensure feasibility.

### C. Whale Optimization Algorithm

The whale optimization algorithm is a nature-inspired metaheuristic that imitates the bubble-net hunting strategy of humpback whales [22]. It consists of three main operators: encircling prey, bubble-net attacking, and random search.

Encircling prey: Whales recognize the location of prey and encircle it. In the algorithm, the current best solution, referred to as the leader, is assumed to be the prey. The position of a search agent is updated as

$$\mathbf{X}(t+1) = \mathbf{X}^*(t) - V.\mathbf{\Delta}, \tag{16}$$

where $\mathbf{X}^*(t)$ is the current leader position, $V$ is the random value. The vector $\mathbf{\Delta}$, having the same dimension as $\mathbf{X}$, specifies the direction of movement from the current position, which is given by

$$\mathbf{\Delta} = |L \cdot \mathbf{X}^*(t) - \mathbf{X}(t)|, \tag{17}$$

where $L$ is the random value. Here, the value $V$ and $L$ are computed using the following equations:

$$V = 2vr_1 - v, \quad L = 2r_2, \tag{18}$$

with the random value $r_1, r_2 \sim U(0,1)$, and $v$ decreases linearly from 2 to 0 over iterations.

Bubble-net attacking mechanism (exploitation phase): The bubble-net strategy is modeled by two approaches applied with equal probability. The first is shrinking encircling, where reducing the value of $|V|$ gradually drives the agents closer to the leader. The second is spiral updating, in which the position is updated along a logarithmic spiral. Specifically, a spiral trajectory is constructed between the whale and the prey to imitate the humpback's twisting motion, expressed as

$$\mathbf{X}(t+1) = \mathbf{X}^*(t) + \mathbf{\Delta}' \cdot e^{cq} \cos(2\pi q), \tag{19}$$

where $\mathbf{\Delta}' = |\mathbf{X}^*(t) - \mathbf{X}(t)|$ denotes the distance between the whale at position $\mathbf{X}$ and the prey at $\mathbf{X}^*$, $c$ is a constant parameter that defines the shape of the logarithmic spiral, and $q \sim U(-1,1)$. Humpback whales improve their ability to capture prey by swimming in a contracting circle while simultaneously following a spiral trajectory, rather than moving directly toward the current prey location. To model this combined behavior, a probabilistic rule is applied: with probability $\rho < 0.5$ the shrinking-encircling mechanism is selected, and with probability $\rho \geq 0.5$ the spiral model is used to update the whale's position, where $\rho \sim U(0,1)$.

Random search (exploration phase): During the exploration phase, the whale's behavior is regulated by the parameter $V$, in a manner analogous to the encirclement stage. Specifically, when $|V| > 1$, the foraging whale is directed away from another member. To avoid premature convergence, WOA allows agents to search around randomly selected whales as:

$$\mathbf{X}(t+1) = \mathbf{X}_{rand}(t) - V \cdot \mathbf{\Delta}_{rand}, \tag{20}$$

where $\mathbf{X}_{rand}$ is a randomly chosen agent and $\mathbf{\Delta}_{rand} = |L \cdot \mathbf{X}_{rand} - \mathbf{X}(t)|$ is the whale's movement in the search phase.

Algorithm Steps: At each iteration $t$, each whale updates its position based on the above rules:

$$\mathbf{X}(t+1) = \begin{cases} \mathbf{X}^*(t) - V \cdot \mathbf{\Delta}, & \rho < 0.5,\ |V| \le 1, \\ \mathbf{X}_{rand}(t) - V \cdot \mathbf{\Delta}_{rand}, & \rho < 0.5,\ |V| > 1, \\ \mathbf{X}^*(t) + \mathbf{\Delta}' \cdot e^{cq} \cos(2\pi q), & \rho \ge 0.5, \end{cases} \tag{21}$$

where $\rho \sim U(0,1)$. This mechanism balances exploitation and exploration.

The proposed method employs WOA to jointly optimize beamforming, AN, and STAR-RIS coefficients. The pseudocode is given in Algorithm 1.

**Algorithm 1** WOA-Based Iterative Algorithm for Maximizing the Sum Secrecy Rate

**Initialization**:
Set the population size $N$, max iterations $T_{\max}$.
Randomly initialize $N$ agents $\{\mathbf{x}_i\}$ within feasible region.
Evaluate fitness $f(\mathbf{x}_i)$ for all agents.
Set leader as the agent with the lowest fitness.
**for** $t = 1$ to $T_{\max}$ **do**
  **for** each agent $\mathbf{x}_i$ **do**
    Generate random numbers $V$, $L$, $\rho$, $q$.
    **if** $\rho < 0.5$ **then**
      **if** $|V| < 1$ **then**
        Update towards leader (exploitation).
      **else**
        Update towards random agent (exploration).
      **end if**
    **else**
      Update by spiral motion around leader.
    **end if**
    Apply boundary control and constraint handling.
    Evaluate new fitness $f(\mathbf{x}_i)$.
  **end for**
  Update leader if a better solution is found.
**end for**
Output best solution $\mathbf{x}^*$ and secrecy rate.

### D. Complexity Analysis

Let $N$ be the population size, $T_{\max}$ the maximum iterations, and $d$ the problem dimension. Each iteration requires $O(Nd)$ updates and $O(N)$ fitness evaluations, where the main computational load is secrecy rate and SINR calculation. Therefore, the overall complexity is approximately $O(NT_{\max}d)$, which is more efficient than conventional AO-based optimization approaches.

## IV. Numerical Results

To validate the proposed scheme, we present simulation results and conduct a comparative study to evaluate its performance in enhancing the PLS on STAR-RIS-assisted NOMA-ISAC system. The network topology is established on a two-dimensional plane, with the BS positioned at (0, 0) and the STAR-RIS deployed at (50m, 50m). Two STs are located at the angle of $45^\circ$ and $-45^\circ$ from the STAR-RIS in the transmission, whereas two CUs are randomly placed at the maximum distance of 50m from STAR-RIS in the reflection region. The channel links are assumed to follow a Rician fading model with a K-factor of 3 dB. The large-scale fading is characterized by a reference path loss of $10^{-3}$ at 1m and a path loss exponent of 2.2 for all links, except for the BS-Users link, where an exponent of 3.6 is applied. Unless otherwise specified, the main simulation parameters are configured as follows. The noise power is set to -90 dBm, and the transmit power budget at the BS is limited to 30 dBm. The minimum secrecy rate requirements are specified as 1.0 bps/Hz. The maximum number of iterations is capped at 1000. Furthermore, all performance results are averaged over 100 independent Monte Carlo channel realizations.

The performance of the proposed scheme with optimally configured STAR-RIS is extensively compared against several baseline strategies. Specifically, three representative benchmarks are considered: (i) NOMA-ISAC with randomly configured STAR-RIS, which does not fully exploit the reconfigurable capability of STAR-RIS, and conventional RIS, where only reflection is supported; (ii) STAR-RIS-assisted ISAC with OMA. The evaluation is carried out under diverse scenarios by varying the BS power budget, the number of BS antennas, communication users, sensing targets, and STAR-RIS elements, as well as different beampattern gain requirements to capture sensing constraints.

Firstly, Fig. 2 illustrates the convergence behavior of the proposed algorithm in terms of the sum secrecy rate. As observed, the objective value increases rapidly during the initial iterations and gradually stabilizes as the number of iterations grows. Specifically, the algorithm reaches about 95% convergence by the 15-th iteration and achieves full convergence around the 300-th iteration, demonstrating its fast and stable convergence as well as practical implementability for secure STAR-RIS aided NOMA-ISAC networks. Moreover, the proposed NOMA scheme with optimally configured STAR-RIS achieves a higher minimum secrecy rate compared to all benchmarks. Taken together, these findings confirm the effectiveness of the proposed design, particularly in terms of faster convergence and enhanced secrecy performance.

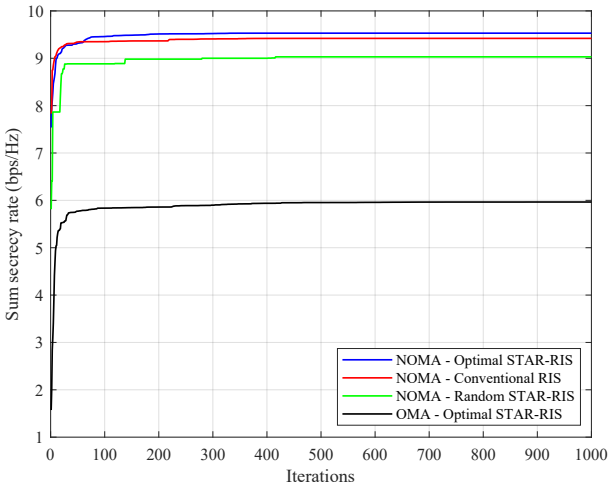



Fig. 2: Convergence of the iterative optimizing algorithm.

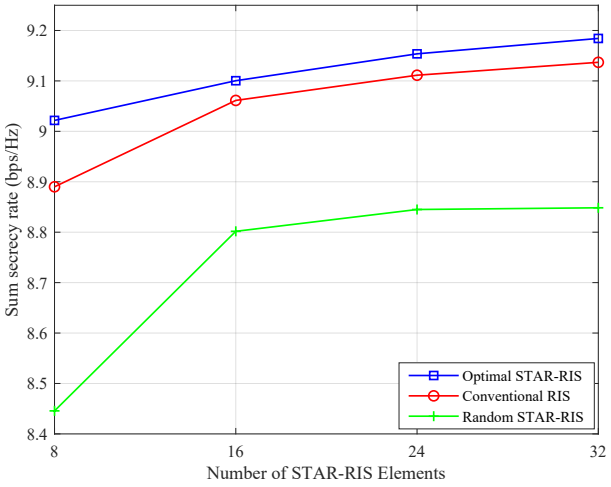



Fig. 3: Impact of number of STAR-RIS elements on sum secrecy rate.

Fig. 3 depicts the sum secrecy rate as a function of the number of STAR-RIS elements under different RIS configurations. It can be seen that increasing the number of elements consistently improves the secrecy performance, since a larger STAR-RIS provides more degrees of freedom for enhancing desired signals and suppressing eavesdroppers. Among the considered schemes, the optimal STAR-RIS design achieves the highest secrecy rate, followed by the conventional RIS, while the random STAR-RIS offers the lowest performance, highlighting the importance of joint optimization in exploiting the full potential of STAR-RIS for secure ISAC systems. For instance, the difference between the optimal and random configurations reaches about 0.34 bps/Hz when the number of elements is 32. This observation highlights the strong capability of the proposed algorithm in exploiting the benefits of the STAR-RIS. While simply increasing the STAR-RIS size naturally improves sensing performance even without optimization, coupling it with a carefully designed algorithm yields substantially greater gains. These findings emphasize that the STAR-RIS scale plays a pivotal role in maximizing overall system efficiency.

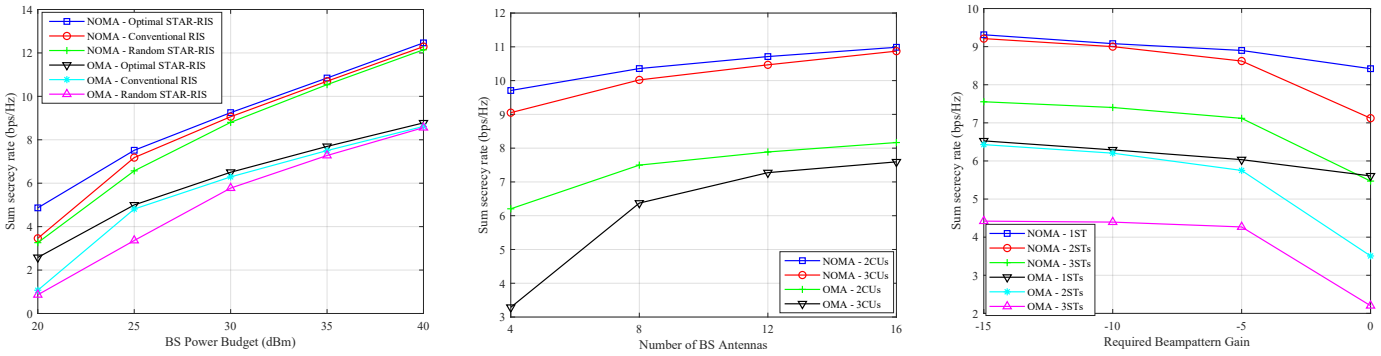
A comparable yet more evident trend is observed in various RIS cases. Fig. 4a shows the sum secrecy rate performance versus the BS transmit power budget for different multiple access schemes and RIS configurations. As expected, the secrecy rate increases monotonically with higher transmit power. It is observed that NOMA consistently outperforms OMA across all RIS settings, confirming the efficiency of NOMA in handling multi-user interference and improving spectral utilization. Moreover, the optimal STAR-RIS design achieves the best performance, while conventional RIS provides moderate gains and random STAR-RIS yields the lowest secrecy rate, highlighting the significant benefit of jointly optimizing STAR-RIS coefficients. Furthermore, the performance gap between the optimal STAR-RIS and the random STAR-RIS configurations becomes more evident across all transmit power levels, which indicates the critical role of optimized STAR-RIS design in fully exploiting its reconfigurable capability. Overall, these results verify the advantage of integrating NOMA and STAR-RIS for enhancing secrecy in ISAC systems.

Regarding the results of the sum secrecy rate performance versus the number of BS antennas under different multiple access schemes and user settings, Fig. 4b show that the secrecy rate increases with more BS antennas, since additional antennas provide higher spatial degrees of freedom for enhancing the desired signals and mitigating eavesdropping. It is also evident that NOMA significantly outperforms OMA for both two-user and three-user cases, validating its efficiency in exploiting the BS antenna array. Moreover, when the number of communication users increases to three, the system achieves slightly lower secrecy rate compared to the two-user case, due to stronger inter-user interference and more stringent decoding constraints. However, with an increasing number of antennas, the performance gap difference between NOMA and OMA diminishes, indicating that both schemes converge in the large-antenna regime. Nevertheless, the proposed NOMA scheme still maintains robust performance and clear advantages over OMA in multi-user secure ISAC scenarios.

Finally, Fig. 4c illustrates the trade-off between secure communication and sensing performance by plotting the sum secrecy rate versus the required beampattern gain under different multiple access and target settings. As expected, increasing the required beampattern gain strengthens the sensing capability, but simultaneously reduces the achievable secrecy rate, since more transmit power and spatial resources are allocated to sensing rather than suppressing eavesdroppers. It is also revealed that NOMA consistently outperforms OMA across all cases, highlighting its ability to more efficiently balance communication and sensing. Furthermore, the secrecy rate degradation becomes more pronounced as the number of sensing targets increases, due to the stricter beampattern constraints. In particular, increasing the number of sensing users from two to three further reduces the secrecy rate by about 0.28 bps/Hz at a beampattern gain of –5 dB, revealing the resource competition between sensing and communication. These results clearly demonstrate the inherent trade-off in ISAC systems and the necessity of advanced optimization methods to achieve a favorable balance between secure communication and reliable sensing.

## V. Conclusions

In this paper, we investigated a secure NOMA-ISAC system empowered by STAR-RIS under a multi-user and multi-sensing-target scenario. To jointly enhance the secrecy rate and sensing performance, we formulated a challenging non-convex optimization problem that incorporates base station beamforming, STAR-RIS coefficients, and communication–sensing trade-offs. To efficiently solve this problem with reduced computational burden, we proposed a low-complexity meta-heuristic approach based on the whale optimization algorithm (WOA). Simulation results demonstrated that the proposed scheme achieves fast and stable convergence and significant secrecy performance gains compared with conventional RIS




(a) (b) (c)

Fig. 4: Sum secrecy rate versus BS power budget, number of BS antennas, and required beampattern gain under various system scenarios.

and random STAR-RIS benchmarks. In particular, NOMA consistently outperformed OMA in terms of secrecy rate, and the advantages of the optimal STAR-RIS design became more pronounced with larger array sizes and higher BS power budgets. Moreover, the results revealed a fundamental trade-off between secure communication and sensing performance, underscoring the necessity of carefully designed optimization strategies. Overall, this work highlights the effectiveness of STAR-RIS and NOMA integration for secure ISAC networks, and showcases the potential of metaheuristic optimization for achieving a favorable balance between security, efficiency, and practicality, while remaining easy to implement on simple hardware platforms.

## ACKNOWLEDGMENT

We would like thank Viettel High Technology Industries Corporation, Viettel Group for providing essential resources enabling the completion of this work.

## REFERENCES

[1] N. González-Prelcic, M. F. Keskin, O. Kaltiokallio, M. Valkama, D. Dardari, X. Shen, Y. Shen, M. Bayraktar, and H. Wymeersch, "The integrated sensing and communication revolution for 6g: Vision, techniques, and applications," *Proceedings of the IEEE*, 2024.

[2] Z. Ren, L. Qiu, J. Xu, and D. W. K. Ng, "Robust transmit beamforming for secure integrated sensing and communication," *IEEE Transactions on Communications*, vol. 71, no. 9, pp. 5549–5564, 2023.

[3] N. Su, F. Liu, and C. Masouros, "Secure radar-communication systems with malicious targets: Integrating radar, communications and jamming functionalities," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 83–95, 2020.

[4] C. Jiang, C. Zhang, C. Huang, J. Ge, M. Debbah, and C. Yuen, "Exploiting RIS in Secure Beamforming Design for NOMA-Assisted Integrated Sensing and Communication," *IEEE Internet of Things Journal*, 2024.

[5] R. Ranjan, M. V. Katwe, A. Bhattacharya, H. B. Mishra, K. Singh, and D. W. K. Ng, "A robust star-ris-assisted mu-mimo system for integrated sensing and communications," *IEEE Transactions on Cognitive Communications and Networking*, 2025.

[6] J. Xu, Y. Liu, X. Mu, and O. A. Dobre, "STAR-RISs: Simultaneous transmitting and reflecting reconfigurable intelligent surfaces," *IEEE Communications Letters*, vol. 25, no. 9, pp. 3134–3138, 2021.

[7] M. M. Kamal, S. Z. U. Abideen, M. Al-Khasawneh, A. Alabrah, R. S. A. Larik, and M. I. Marwat, "Optimizing secure multi-user isac systems with star-ris: A deep reinforcement learning approach for 6g networks," *IEEE Access*, 2025.

[8] Z. Liu, X. Li, H. Ji, and H. Zhang, "Exploiting STAR-RIS for physical layer security in integrated sensing and communication networks," in *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. IEEE, 2023, pp. 1–6.

[9] Z. Zhu, M. Gong, G. Sun, P. Liu, and D. Mi, "Ai-enabled star-ris aided miso isac secure communications," *Tsinghua Science and Technology*, vol. 30, no. 3, pp. 998–1011, 2024.

[10] T. Zhou, K. Xu, G. Hu, X. Xia, C. Li, C. Wei, and C. Liao, "Robust and Secure Beamforming Design for STAR-RIS-Enabled IoE ISAC Systems," *IEEE Internet of Things Journal*, 2024.

[11] Z. Liu, X. Li, H. Ji, and H. Zhang, "Active star-ris enabled isac networks against simultaneous eavesdropping and detection attacks," *IEEE Internet of Things Journal*, 2025.

[12] C. Dou, N. Huang, Y. Wu, L. Qian, and T. Q. Quek, "Sensing-efficient noma-aided integrated sensing and communication: A joint sensing scheduling and beamforming optimization," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 10, pp. 13 591–13 603, 2023.

[13] Z. Wei, J. Piao, X. Yuan, H. Wu, J. A. Zhang, Z. Feng, L. Wang, and P. Zhang, "Waveform design for mimo-ofdm integrated sensing and communication system: An information theoretical approach," *IEEE Transactions on Communications*, vol. 72, no. 1, pp. 496–509, 2023.

[14] C. Zhang, S. Qu, L. Zhao, Z. Wei, Q. Shi, and Y. Liu, "Robust secure beamforming design for downlink ris-isac systems enhanced by rsma," *IEEE Wireless Communications Letters*, 2024.

[15] Z. Wang, Y. Liu, X. Mu, Z. Ding, and O. A. Dobre, "Noma empowered integrated sensing and communication," *IEEE Communications Letters*, vol. 26, no. 3, pp. 677–681, 2022.

[16] L. Zhang, Y. Wang, H. Chen, and Y. Cao, "Physical layer security of the noma-assisted isac systems under near-field scenario," *IEEE Internet of Things Journal*, 2025.

[17] Z. Yang, D. Li, N. Zhao, Z. Wu, Y. Li, and D. Niyato, "Secure precoding optimization for noma-aided integrated sensing and communication," *IEEE Transactions on Communications*, vol. 70, no. 12, pp. 8370–8382, 2022.

[18] N. Xue, X. Mu, Y. Liu, and Y. Chen, "Noma-assisted full space star-ris-isac," *IEEE Transactions on Wireless Communications*, vol. 23, no. 8, pp. 8954–8968, 2024.

[19] Y. Wang, Z. Yang, J. Cui, P. Xu, G. Chen, T. Q. Quek, and R. Tafazolli, "Optimizing the fairness of star-ris and noma assisted integrated sensing and communication systems," *IEEE Transactions on Wireless Communications*, vol. 23, no. 6, pp. 5895–5907, 2023.

[20] Y. Li, M. Jin, Q. Guo, J. Yao, T. Jiang, and J. Liu, "Secure beamforming and power allocation for ris-assisted noma-isac systems with internal and external eavesdroppers," *IEEE Transactions on Cognitive Communications and Networking*, 2025.

[21] W. Wei, X. Pang, C. Xing, N. Zhao, and D. Niyato, "STAR-RIS aided secure NOMA integrated sensing and communication," *IEEE Transactions on Wireless Communications*, 2024.

[22] S. Mirjalili and A. Lewis, "The whale optimization algorithm," *Advances in engineering software*, vol. 95, pp. 51–67, 2016.