Tsinghua Science and Technology
Doi:10.26599/TST.2026.9010007

Research/Review Article

Joint Beamforming and Intelligent Reflecting Surface Optimization for Enhanced Physical Layer Security

Shanwen Guan, Xintong Shen, Xinyun Zhang, Ji Li, Li Zhou (✉), Xiaonan Luo (✉)

Abstract Enhancing physical layer security through the deployment of intelligent reflecting surfaces (IRS) is an emerging and significant research direction in 6G wireless networks. Existing methods mainly focus on optimizing the transmit beamforming of the access point (AP) and the phase shift of the IRS to maximize the secrecy rate, while neglecting the optimization of the IRS amplitude. We propose a joint optimization framework that simultaneously optimizes the IRS amplitude, IRS phase shifts, and AP beamforming to enhance the secrecy rate. Due to the problem's non-convexity, existing alternating optimization methods face high challenges, particularly for large-scale IRS systems and high-power scenarios. To tackle these issues, we propose a competition mechanism-based multi-strategy swarm optimization algorithm, which aims to better balance global exploration and local exploitation capabilities, thereby achieving more optimal IRS configurations. Simulations demonstrate that jointly optimizing IRS amplitude, phase, and AP beamforming significantly improves secrecy rate over phase-only beamforming methods.

Keywords physical layer security; intelligent reflecting surface (IRS); secrecy rate; competitive swarm optimization

1 Introduction

The exponential proliferation of smart wearable devices has imposed unprecedented demands on wireless communication infrastructures, requiring robust connectivity for hundreds of billions of exponentially growing mobile terminals [1, 2]. Nevertheless, the inherent broadcast characteristics and open-medium nature of wireless networks make transmitted information highly vulnerable to both malicious interception and interference, significantly compromising data confidentiality and integrity [3]. This security challenge becomes particularly critical in mission-critical domains such as governmental communications, financial transactions, and military operations [4, 5]. Consequently, achieving information-theoretic security in mobile communications has become a central research frontier in modern telecommunications [6].

Current wireless security paradigms fall into two distinct architectural approaches: cryptographic-based application-layer security protocols [7] and physical-layer security mechanisms rooted in fundamental wireless communication principles [8]. Although cryptographic methods are still predominant, their dependence on upper-layer protocols requires complex key management infrastructures [9]. More critically, the advent of quantum computing and advanced cryptanalysis techniques has substantially exacerbated the vulnerability of cryptographic systems to brute-force attacks, thereby challenging their long-term sustainability [10]. In contrast, physical layer security techniques leverage wireless channel characteristics to improve the quality of the signal of legitimate users while reducing the reception of eavesdroppers [11–14]. The theoretical foundations of physical layer security were first established by Shannon through his pioneering work on information-theoretic security [15]. This was subsequently formalized by Wyner's wiretap channel model, which mathematically demonstrated that when the eavesdropper's channel is a degraded version of the legitimate channel, carefully designed channel coding schemes can guarantee secure communication even in adversarial environments [16]. This seminal work proved that legitimate receivers can achieve asymptotically perfect signal decoding while preventing eavesdroppers from extracting any meaningful information, provided specific channel conditions are satisfied.

Contemporary research in physical-layer security focuses primarily on three key technical dimensions: directional modulation, sidelobe manipulation and artificial noise injection. Zhao et al. developed an optimized precoding and beamforming framework that enhances mainlobe transmission efficiency while simultaneously suppressing sidelobe radiation through sophisticated angle coding techniques [17]. Yang's research team proposed an innovative switched array architecture that dynamically configures antenna subsets to optimize security

• Shanwen Guan, Xinyun Zhang, Ji Li, Li Zhou and Xiaonan Luo are with the Guangxi Key Laboratory of Image and Graphic Intelligent Processing, Guilin University of Electronic Technology, Guilin 541004, China. E-mail: sguan@guet.edu.cn; wxqys178@163.com; Liji@guet.edu.cn; lizhou2022@gmail.com; luoxn@guet.edu.cn
• Xintong Shen is with the College of Computing, Khon Kaen University, Khon Kaen, 40002 Thailand. E-mail: xintong.s@kkumail.com
• Shanwen Guan and Xintong Shen are co-first authors
Manuscript received: 2025-Jun-25; revised: 2025-Oct-12; accepted: 2025-Dec-31

performance in sidelobe regions [18]. Eltayeb et al. established a novel channel parameter conversion mechanism that transforms angular information into equivalent distance metrics, effectively mitigating main-beam eavesdropping threats through intelligent scattering paths [19].

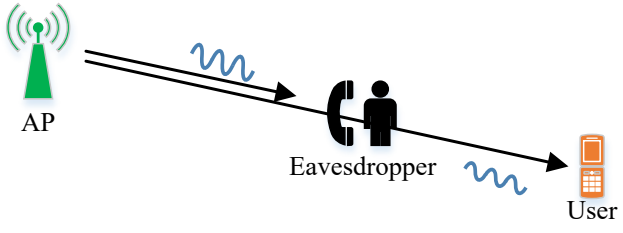

Fig. 1 Schematic model of a single-cell network system.

Chen [20] and Liu [21] introduced artificial noise at the transmitter and full-duplex receiver ends respectively to enhance physical-layer security. Through carefully designed artificial noise vectors, eavesdroppers' received signals are transformed into Gaussian white noise-like waveforms, significantly degrading the quality of intercepted signals and rendering unauthorized access to meaningful information infeasible. As shown in Fig. 1, this approach's effectiveness deteriorates significantly diminished when the legitimate communication channel exhibits a high spatial correlation with the eavesdropping channel, particularly in scenarios where the legitimate user's received signal power is lower than that of the eavesdropper.

In recent years, physical layer security mechanisms leveraging IRS-assisted communication have garnered substantial research interest. Being a key 6G enabler, the IRS comprises a software-controlled array of low-power reflective elements [22]. By dynamically adjusting the phase and amplitude of reflected signals, IRS technology can either amplify or attenuate signals along different propagation paths, thereby offering a novel paradigm for enhancing wireless communication quality and enabling intelligent channel reconfiguration [23, 24]. Due to its cost-effectiveness and compact form factor, IRS can be densely deployed across diverse environments, such as building facades and indoor spaces, to boost the overall performance of wireless networks. Thus, extensive research has focused on solving physical-layer security challenges in IRS-assisted systems [25].

Cui et al. investigated the scenario with known channel state information, using alternating optimization (AO) and semidefinite relaxation (SDR) techniques to jointly optimize the transmitter's beamforming and IRS's reflection coefficients, especially when legitimate and eavesdropping channels are highly spatially correlated [26]. Liu et al. [27] focused on secrecy rate maximization in multi-user multiple-input single-output (MISO) systems by jointly optimizing information and energy transmission. Their proposed two-stage optimization framework optimized the transmission beamforming vectors and power allocation strategy. Sun et al. extended this research by jointly optimizingactive IRS's transmission and reflection beams using a combination of SDR and AO techniques [28] . Meanwhile, Ge et al. addressed the challenge of unknown channel state information by employing an alternating optimization framework to jointly design the transmission beam and IRS reflection coefficients [29].

Hua et al. proposed an IRS-assisted secure transmission scheme for millimeter-wave communications, where artificial noise is strategically designed to constrain the eavesdropper's channel capacity, effectively improving communication confidentiality [30]. Taneja et al. investigated reconfigurable intelligent surface-based "electromagnetic stealth" technology, which renders the legitimate communication undetectable to eavesdroppers, thereby enhancing communication covertness [31]. Peng et al. proposed a UAV-mounted mobile IRS system capable of dynamically adjusting both spatial positioning and reflection parameters to achieve time-varying wireless channel control for enhanced communication security [32]. Chen et al. proposed a dynamic IRS beamforming scheme that significantly improves the computational efficiency of mobile edge computing (MEC) systems by jointly optimizing computation mode selection, offloading time allocation, and IRS beamforming [33]. The index modulation and reflection-mode modulation approaches focus on information transmission through the activation of specific IRS element combinations, transforming continuous phase shift adjustments into discrete index feedback to modulate the reflected signals [34].

One of the principal challenges in IRS-assisted communication systems is the inherent nonconvexity of the joint optimization problem involving both the transmitter's beamforming design and the IRS reflection coefficient configuration. These optimization problems are notoriously difficult to solve directly due to the intricate non-convex nature of both the objective functions and the associated constraints [35]. Existing approaches predominantly rely on SDR and AO methodologies, which, while effective, entail substantial computational complexity. As the scale of the problem increases, the computational burden escalates significantly, leading to diminished algorithmic efficiency. Additionally, most existing studies primarily focus on optimizing the reflection phase of the IRS while constraining amplitude adjustments, thereby overlooking potential security enhancements achievable through amplitude optimization. This limitation curtails

the full security potential of IRS-assisted systems. Consequently, future research should prioritize the development of advanced optimization frameworks that not only address the intrinsic nonconvexity of these problems but also integrate both phase and amplitude optimization of IRS elements. Such advancements are essential to further enhance the security and efficiency of IRS-assisted wireless communication systems.

The fundamental challenge in physical-layer security for IRS-assisted systems lies in the joint optimization of transmitter beamforming and IRS reflection parameters, which exhibits strong nonconvexity that is inherently difficult to resolve directly. Conventional approaches suffer from exponentially growing computational complexity with system scaling, while the prevalent practice of optimizing only phase shifts while fixing amplitude coefficients severely limits the achievable security enhancement. This paper investigates the joint optimization of AP beamforming and IRS phase/amplitude configuration under strong channel correlation between legitimate and eavesdropping channels. We first formulate the average secrecy rate maximization problem incorporating IRS reflection amplitudes. To solve this large-scale nonconvex optimization, heuristic particle swarm optimization can provide effective approximate solutions [36, 37]. We propose a novel group-competitive swarm optimizer based on collective learning mechanisms. Experimental results demonstrate the superiority of our method over alternating optimization in large-scale IRS and high-power scenarios.

- We propose a novel optimization model incorporating IRS reflection amplitudes to maximize the average secrecy rate in IRS-assisted communications, overcoming the limitation of phase-only optimization in conventional approaches.
- Building on group learning theory, we propose a new Group-competitive Swarm Optimization (GSO) algorithm. The GSO algorithm forms learning groups through random selection of three particles per iteration and employs a competition mechanism to rank these particles. The algorithm applies distinct update strategies according to ranking results, effectively enhancing both particle diversity and exploratory capability. These mechanisms enable GSO to outperform conventional methods in handling large-scale optimization problems, demonstrating superior performance in complex scenarios.
- Experimental results demonstrate that IRS amplitude adjustment significantly enhances the secrecy rate in large-scale IRS systems operating under high-power conditions. When it comes to complex optimization problems that traditional alternating update methods cannot solve, the GSO algorithm shows excellent optimization performance and has more significant performance under high-power transmission conditions, achieving a higher average security rate and providing a feasible solution for strengthening the security of IRS-assisted communication systems.

The remainder of this paper is organized as follows. Section 2 presents the IRS-assisted secure communication system model and formulates a secrecy rate maximization problem through the joint optimization of beamforming and the amplitude and phase of the IRS. To address this complex and non-convexx optimization problem, Section 3 proposes a novel group competition optimization algorithm to obtain a suboptimal solutionto the optimization problem. Section 4 compares the proposed method with existing approaches to demonstrate its performance advantages. We draw conclusions in Section 5.

2 System Model And Problem Formulation

The IRS is composed of numerous low-cost programmable reflective elements, which can modulate the amplitude and phase of reflected signals by encoding of the IRS elements. The amplitude and phase adjustments range from [0,1] and [0,2π), respectively [38]. Consider the practical scenario depicted in Fig. 3, which involves an IRS-assisted downlink communication system. The system comprises an access point (AP) equipped with M half-wavelength-spaced antennas, a single-antenna legitimate user (User) and a single-antenna eavesdropper (Eve). The AP transmits information to the User, with Eve positioned between AP and User. Notably, the eavesdropper is closer to the AP than the legitimate user, giving Eve a more favorable communication channel.

To enhance the security of the communication system, an IRS with N reflective elements is deployed to assist in secure communication between the AP and the User. The IRS is equipped with a controller that regulates both the AP and the IRS. When the AP simultaneously transmits signals to both the IRS and the User, the beamforming at the AP and the encoding of the IRS reflective elements adjust the phase and amplitude of the reflected signals. This adjustment enables the IRS-reflected signal to constructively combine with the AP's direct signal at the User, enhancing the received signal strength. Simultaneously, the IRS-reflected signal destructively interferes with the AP's direct signal at Eve, weakening the received signal quality. This process reduces the eavesdropper's signal quality, improving system security and achieving secure physical layer communication.

All communication channels are assumed to be quasi-static flat-fading channels [39]. The channel coefficients from the AP to the user, from the AP to the IRS, from the AP to the eavesdropper (Eve), from the IRS to the Eve, and from the IRS to the user are denoted as $\mathbf{h}_{AU} \in \mathbb{C}^{M\times 1}$, $\mathbf{H}_{AI} \in \mathbb{C}^{M\times N}$, $\mathbf{h}_{AE} \in \mathbb{C}^{M\times 1}$, $\mathbf{h}_{IE} \in \mathbb{C}^{N\times 1}$, and $\mathbf{h}_{IU} \in \mathbb{C}^{N\times 1}$, respectively.

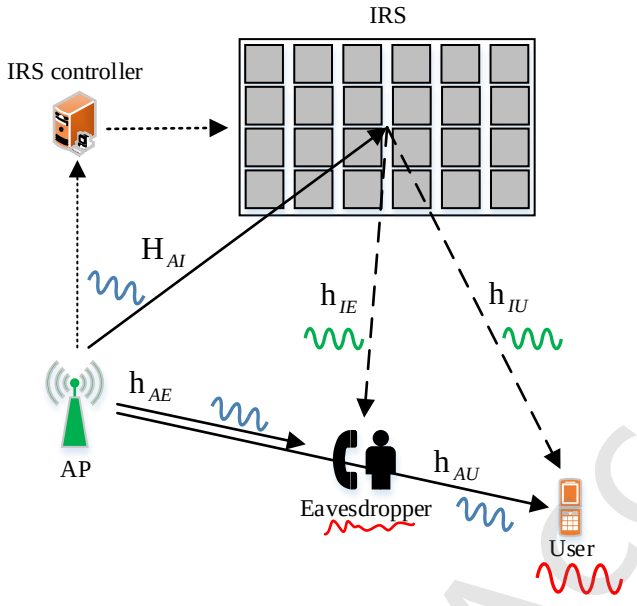

Fig. 2 IRS-assisted secure communication system.

The schematic system model [40] for the simulated single-cell network is shown in Fig. 3. The AP is centrally located within the cell, covering a radius of R. Both legitimate users and potential eavesdroppers are randomly and uniformly distributed throughout the cell. The channel matrix $\mathbf{H}_{AI}$, which describes the communication link between the AP and the IRS, is formulated as follows

$$\mathbf{H}_{AI} = m_{AI}\left(\sqrt{\frac{K_{AI}}{1+K_{AI}}}\mathbf{H}_{AI}^{L} + \sqrt{\frac{1}{1+K_{AI}}}\mathbf{H}_{AI}^{N}\right), \tag{1}$$

where $m_{AI} = \sqrt{l_0\left(\frac{d_0}{d_{AI}}\right)^{\alpha_{AI}}}$ and $l_0 = (\frac{\lambda_c}{4\pi})^2$ is a constant where λ_c is the wavelength of the carrier's center frequency. d_0 is the reference distance. d_{AI} denotes the distance between the AP and IRS, and α_{AI} is the corresponding path loss exponent. The small-scale fading is modeled as Rician fading with the Rician factor K_{AI}. The Line-of-Sight (LoS) and non-Line-of-Sight (NLoS) components are denoted by $\mathbf{H}_{AI}^{L}$ and $\mathbf{H}_{AI}^{N}$, respectively, and are expressed as products of array response vectors.

$$\begin{aligned}
\mathbf{H}_{AI}^{L} &= \mathbf{a}_I(\theta_x,\theta_y)\mathbf{a}_A^H(\phi),\\
\mathbf{a}_I(\theta_x,\theta_y) &= \mathbf{a}_{Ix}(\theta_x)\otimes\mathbf{a}_{Iy}(\theta_y),\\
\mathbf{a}_A(\phi) &= \left[1, e^{j\pi\phi},\ldots,e^{j\pi\phi(M-1)}\right]^T,\\
\mathbf{a}_x(\theta) &= \left[1, e^{j\pi\theta},\ldots,e^{j\pi\theta(n_x-1)}\right]^T, \quad \text{for } x\in\{Ix,Iy\},
\end{aligned} \tag{2}$$

where θ_x and θ_y are the directional cosines of the angles of arrival at the IRS along the horizontal axes and ϕ is the directional cosine of the angle of departure at the AP. n_{I_x} and n_{I_y} denote the number of IRS elements along the horizontal and vertical dimensions respectively. The remaining channels in the system are modeled similarly. For the passive IRS, the received signals by the user and eavesdropper can be expressed as

$$y_j = (\mathbf{h}_{Ij}^H\mathbf{Q}\mathbf{H}_{AI} + \mathbf{h}_{Aj}^H)\mathbf{x} + w_j \quad j\in\{U,E\}, \tag{3}$$

where $\mathbf{x} = \sqrt{P_{AP}}\mathbf{f}s$ represents the precoded transmit signal from the AP. $\mathbf{f} = \sqrt{\frac{1}{M}}[1, e^{j\pi\alpha},\ldots,e^{j\pi(M-1)\alpha}]^T$ denotes the beamforming vector and s denotes the confidential information symbol with zero mean and unit variance. P_{AP} is the transmit power of s. $w_j \sim \mathcal{CN}(0,\delta_U^2)$ represents the additive white Gaussian noise at receiver $j\in\{U,E\}$, where δ_U^2 and δ_E^2 denote the noise variances at the user and eavesdropper, respectively. $\mathbf{Q} = \mathrm{diag}(\mathbf{q})$ denotes the IRS reflection coefficient matrix [24], where $\mathbf{q} = [\eta_1 e^{j\beta_1}, \eta_2 e^{j\beta_2},\ldots,\eta_N e^{j\beta_N}] \triangleq [q_1, q_2,\ldots,q_N]$. η_n and β_n denote the amplitude reflection coefficient and phase shift of the n-th IRS element, respectively.

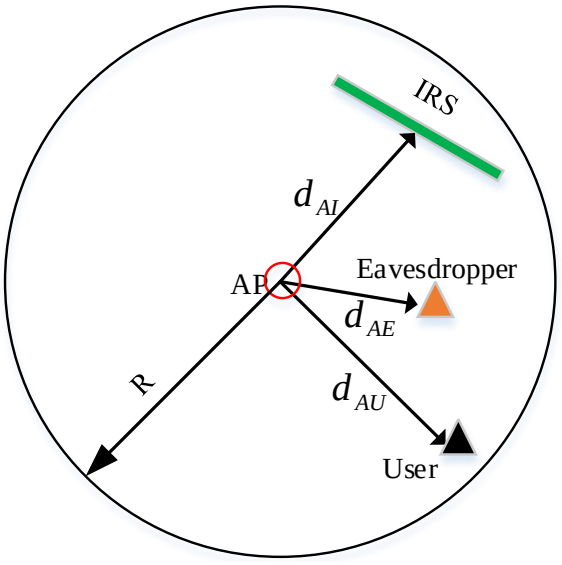

Fig. 3 Schematic model of a single-cell network system.

In physical layer security research, the security perfor-

mance of communication systems is frequently quantified using intuitive numerical metrics, where the secrecy rate serves as a key metric for assessing instantaneous security performance. The secrecy rate is derived from the signal-to-interference-plus-noise ratio (SINR) and is influenced by the reflection coefficient adjustments of an intelligent reflecting surface. While conventional IRS-assisted security schemes primarily optimize phase shifts, the additional ability to adjust reflection amplitudes introduces extra degrees of freedom, significantly enhancing secrecy performance. Therefore, a deeper investigation into how IRS amplitude tuning affects SINR and secrecy rate is essential for optimizing secure communication systems.

To derive the secrecy rate, we first define the SINRs for the legitimate user and the eavesdropper. Let R_{U} and R_{E} denote the SINRs at the legitimate user and eavesdropper, respectively

$$R_{\mathrm{U}} = \frac{\left|\left(\mathbf{h}_{AU}^{H} + \mathbf{h}_{IU}^{H}\boldsymbol{Q}\mathbf{H}_{AI}\right)\mathbf{x}\right|^{2}}{\sigma_{U}^{2}}, \tag{4}$$

$$R_{\mathrm{E}} = \frac{\left|\left(\mathbf{h}_{AE}^{H} + \mathbf{h}_{IE}^{H}\boldsymbol{Q}\mathbf{H}_{AI}\right)\mathbf{x}\right|^{2}}{\sigma_{E}^{2}}. \tag{5}$$

Based on Shannon's theorem, the channel capacities for the legitimate user and eavesdropper are given by

$$C_{\mathrm{U}} = \log_2\left(1 + R_{\mathrm{U}}\right), C_{\mathrm{E}} = \log_2\left(1 + R_{\mathrm{E}}\right), \tag{6}$$

The secrecy rate is defined as the difference between the channel capacity of the legitimate receiver and the channel capacity of the eavesdropper [41]. Thus, the maximum achievable secrecy rate R_{sec} between the AP and the user (in bits/second/Hz) can be expressed as:

$$R_{\mathrm{sec}} = \left[C_{\mathrm{U}} - C_{\mathrm{E}}\right]^{+} \tag{7}$$

In IRS-assisted secure communication systems, while phase adjustment improves signal quality for legitimate users and degrades reception for eavesdroppers, the IRS's amplitude adjustment capability also critically influences SINR and secrecy rate performance. When the IRS-assisted channel is strong, increasing reflection amplitude boosts the legitimate user's received signal power, elevating R_{U} and directly improving the secrecy rate. By tuning the amplitude of IRS elements, the signal gain at the eavesdropper can be suppressed, lowering R_{E} and consequently maximizing R_{sec}. Although phase-only optimization improves performance, joint amplitude-phase optimization further enhances legitimate users' signal quality and simultaneously suppresses eavesdroppers' received power, achieving superior security performance.

Theoretically, each IRS element can adjust both phase and amplitude of its reflection coefficient. However, practical joint optimization of amplitude and phase remains challenging, even with alternating optimization methods. Typically, IRS elements are constrained to unit modulus ($|q_n| = 1$), focusing solely on phase adjustment while ignoring amplitude modulation.

In practical systems, legitimate users often face more severe channel limitations than eavesdroppers. To fully exploit IRS capabilities, we jointly optimize the reflection phase and amplitude across all elements to maximize the secrecy rate. Unlike conventional unit-modulus constraints ($|q_n| = 1, \forall n$), we relax this to $|q_n| \leqslant 1, \forall n$ to unlock the IRS's full potential through joint amplitude-phase optimization.

Our aim is to maximize the secrecy rate. The joint design of the transmit beamformers at the AP and the $\mathbf{Q}$ at the IRS can be formulated as follows

$$\begin{aligned} &\max_{\mathbf{Q},\boldsymbol{x}} R_{\mathrm{sec}} \\ &\text{s.t. } \|\mathbf{x}\|^2 \leqslant P_{max},\ |q_n| \leqslant 1, \forall n \end{aligned} \tag{8}$$

with P_{max} symbolizes the maximum transmit power of AP.

In this system, the eavesdropper is assumed to be active, indicating it can interact with the communication system. Meanwhile, since the legitimate user distrusts the eavesdropper, the system prioritizes acquiring the eavesdropper's CSI to mitigate security threats. Thus, for evaluating the IRS-assisted system's performance limits, we reasonably assume the AP can obtain perfect CSI of both user and eavesdropper [42]. The goal is to jointly design the AP beamforming and IRS reflection coefficients to maximize secrecy rate by strengthening the combined signal at the user while suppressing it at the eavesdropper. The optimization problem (8) becomes highly challenging due to its non-convexity and IRS reflection amplitude variables.

To address this, a novel multi-strategy swarm optimization algorithm based on the competition mechanism is employed to optimize Eq.(8). Unlike convex optimization theory, which requires complex analytical computations, the proposed algorithm simply iterates and updates particles based on appropriate encoding of the optimization problem. Furthermore, to improve the secrecy rate, this paper proposes a novel competitive swarm optimization algorithm based on group learning.

3 A Novel Group-based Competitive Swarm Optimizer

3.1 Proposed GSO Algorithm

The competitive swarm optimization (CSO) algorithm improves population diversity through competition mechanisms,

demonstrating strong performance in optimization problems. However, CSO may converge to local optima when handling highly complex functions. We propose a novel GSO algorithm featuring intra-group competition and multiple update strategies , where particles dynamically select learning strategies based on competition results to significantly improve algorithmic diversity and optimization performance.

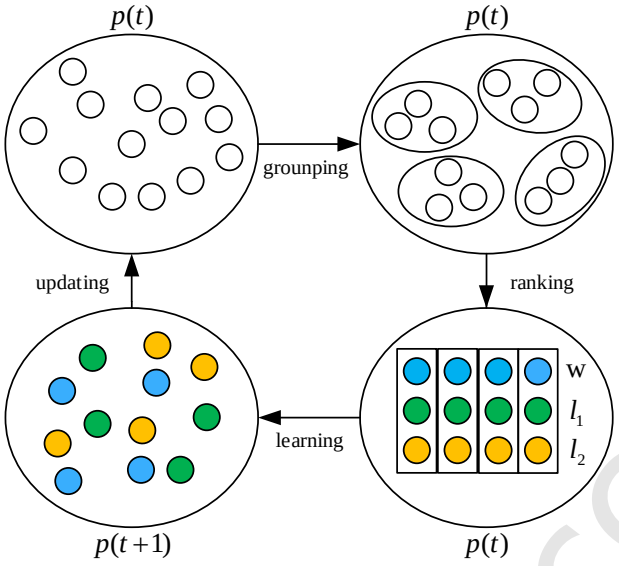

Fig. 4 Schematic diagram of the GSO framework.

As shown in Fig. 4, GSO organizes particles into triplets, ranked by secrecy rate as w (winner), l_1 (first loser) , and l_2 (second loser). Two superior particles, w and l_1, guide the update and learning process of the loser l_2. The velocity V_{l_2} and position X_{l_2} of loser l_2 are updated by

$$\begin{aligned} V_{l_2}(t) = r_1 V_{l_2}(t) + r_2 \left(X_w(t) - X_{l_2}(t)\right) \\ +\varphi r_3 \left(X_{l_1}(t) - X_{l_2}(t)\right), \\ X_{l_2}(t+1) = X_{l_2}(t) + V_{l_2}(t), \end{aligned} \tag{9}$$

where $X_i(t)$ and $V_i(t), i = \{w, l_1, l_2\}$ denote the position and velocity of particle i at generation t, respectively. Additionally, φ, r_1, r_2, and r_3 are uniformly distributed random variables [0, 1].

To maintain population diversity, the suboptimal particle l_1 undergoes mutation. The l_1 position update rule is

$$C_{l_1} = \begin{cases} rand(l_1), & rand(0,1) \leqslant Cr \\ X_{l_1}(t), & otherwise \end{cases} \tag{10}$$

$$X_{l_1}(t+1) = \begin{cases} C_{l_1}, & f(X_{l_1}(t)) \leqslant f(C_{l_1}) \\ X_{l_1}(t), & otherwise \end{cases} \tag{11}$$

where C_{l_1} is the mutated candidate solution and $Cr \in [0, 1]$ is the mutation probability controlling how often l_1 is replaced by C_{l_1}. The fitness function $f(X)$, corresponding to the optimization objective defined in Eq. 7. In particular, the elite particle w preserves its optimal state through direct propagation to the subsequent generation, maintaining the convergence properties of the algorithm.

According to the non-convex optimization problem (8), the encoding for the k-th particle $\mathbf{p}_k \in \mathcal{R}^{L\times 1}$ is as follows

$$\mathbf{p}_k = [P_{AP}, \alpha, \eta_1, ..., \eta_N, \beta_1, ..., \beta_N,] \tag{12}$$

where $L = 2 + 2 \cdot N$.

The optimization problem-solving process for IRS-assisted secure communication systems based on the GSO algorithm is illustrated in the Algorithm 1.

Algorithm 1 GSO

Require: K is the size of swarm P.
1: Initialize t_{max} and $t = 0$.
2: **while** $t \leqslant t_{max}$ **do**
3: Calculate the fitness of all particles in $P(t)$.
4: Divide all particles into $K/3$ groups.
5: **for** each group **do**
6: Identify winner w, l_1 and losers l_2 based on competitive mechanisms and $f(X_w) > f(X_{l_1}) > f(X_{l_2})$.
7: Update X_{l_2} using Eq.9
8: Update X_{l_1} using Eq.10 and Eq. 11
9: **end for**
10: $t = t + 1$.
11: **end while**

3.2 Theoretical Analysis

An effective optimizer must achieve an optimal balance between exploration and exploitation as particles navigate the search space. Through a unified parametric framework characterized by the mixing coefficient λ and target point T [43], the update schemes of GSO, CSO, and PSO are systematically expressed in the canonical form. The Eq.9 is rewritten as follows

$$\begin{cases} V_{l_2} = r_1 V_{l_1} + \lambda_1 (T_1 - X_{l_2}), & \text{(13a)} \\ \lambda_1 = r_2 + \varphi r_3, & \text{(13b)} \\ T_1 = \dfrac{r_2}{r_2 + \varphi r_3} X_w + \dfrac{\varphi r_3}{r_2 + \varphi r_3} X_{l_1} & \text{(13c)} \end{cases}$$

In the CSO algorithm, the global mean of the particles is utilized to guide their learning, and its update equation can

be reformulated as:

$$\begin{cases} V_l = r_1 V_l + \lambda_2 (T_2 - X_l), & \text{(14a)} \\ \lambda_2 = r_2 + \varphi r_3, & \text{(14b)} \\ T_2 = \dfrac{r_2}{r_2 + \varphi r_3} X_w + \dfrac{\varphi r_3}{r_2 + \varphi r_3} \bar{X} & \text{(14c)} \end{cases}$$

Similarly, the PSO algorithm updates particles based on both the global best and individual best solutions, with its update equation rewritten as follows

$$\begin{cases} V_i = \omega V_i + \lambda_3 (T_3 - X_i), & \text{(15a)} \\ \lambda_3 = c_1 r_1 + c_2 r_2, & \text{(15b)} \\ T_3 = \dfrac{c_1 r_1 pbest_i}{c_1 r_1 + c_2 r_2} + \dfrac{c_2 r_2 gbest}{c_1 r_1 + c_2 r_2} & \text{(15c)} \end{cases}$$

where c_1 and c_2 denote acceleration coefficients. $pbest_i$ denotes the personal best position found so far by particle i, while $gbest$ represents the global best position among all particles.

When comparing the first components of T_i (i =1, 2, 3), both GSO and CSO employ the winner X_w to update the loser's position. However, in PSO, the best position $pbest_i$ of the particle X_i is updated only when X_i finds a better solution, which indicates that $pbest_i$ may not change in many successive generations. Consequently, both GSO and CSO maintain greater competitive diversity compared to PSO. Regarding the second components of T_1 and T_2, CSO updates the mean position of the swarm $\bar{X}$ in every generation. However, GSO, however, randomly selects distinct secondary exemplars X_{l_1} for individual particles rather than using a shared reference. GSO demonstrates superior diversity preservation compared to CSO through its randomized individual guidance mechanism rather than relying on fixed population means, thus exhibiting enhanced capability to escape local optima and accelerate convergence toward promising solution regions.

Exploitation ability and exploration ability are equally important. This is because a good exploitation ability can quickly locate better areas so that the optimization time can be reduced. It's important to some problems with limited computational resources and unimodal problems. To analyze the exploitation ability of GSO, three representative particles are selected from the same group: the best particle X_w and two ordinary particles X_{l_1} and X_{l_2}, satisfying the fitness relationship

$$f(X_w) \geqslant f(X_{l_1}) \geqslant f(X_{l_2}) \tag{16}$$

Combining the definitions of personal best $pbest_i$ of i and global best $gbest$ defined in classical PSO, we have the following relationship:

$$\begin{cases} f(gbest) \geqslant f(pbest_w) \geqslant f(X_w), \\ f(gbest) \geqslant f(pbest_{l_1}) \geqslant f(X_{l_1}), \\ f(gbest) \geqslant f(pbest_{l_2}) \geqslant f(X_{l_2}). \end{cases} \tag{17}$$

Let

$$\Delta F_{GSO} = |f(X_{l_1}) - f(X_{l_2})|, \tag{18}$$

$$\Delta F_{CSO} = |f(X_w) - f(X_2)|, \tag{19}$$

$$\Delta F_{PSO} = |f(gbestW) - f(X_{l_2})|, \tag{20}$$

Here, ΔF_{GSO} represents the fitness difference between ordinary particles within the same group in GSO, ΔF_{CSO} reflects the update difference dominated by the winning particle X_w in CSO, and ΔF_{PSO} measures the difference between the global best particle $gbest$ and an ordinary particle in PSO. Combining the above formula together, the following relationship can be obtained:

$$\Delta F_{GSO} \leqslant \Delta F_{CSO} \leqslant \Delta F_{PSO}, \tag{21}$$

The formula shows that GSO, comparing with CSO and PSO, has a better exploitation ability to exploit the small gaps between two positions whose fitness values are very similar.

In short, GSO can preserve good exploitation and exploration abilities. However, it's not enough for a good EA because the two abilities usually conflict with each other during evolution. Thus, there should be a balance between these two abilities.

This approach enhances interaction and learning among particles, reducing the overall dependency of the entire population on a single winning particle. It helps prevent falling into local optima.

3.3 Time Complexity Study

In the proposed GSO algorithm, three particles are randomly grouped and ranked based on their fitness values. The best performing particle is retained, while the second best particle undergoes a mutation to update, resulting in a computational complexity of $\mathcal{O}(K \cdot L)$. The worst performing particle updates its position based on velocity calculations, a process executed dimension-wise, leading to an overall complexity of $\mathcal{O}(K \cdot L)$. The primary computational complexity of the optimization problem arises from the numerator calculations of R_{U} and R_{E}. Since the IRS reflection matrix Q is a diagonal matrix, the associated computational complexity can be expressed as $\mathcal{O}(N^2 \cdot K)$. Taking into account all components, the total computational complexity of the proposed algorithm is given by $\mathcal{O}(t_{max} \cdot L \cdot K \cdot N^2)$. The computational complexity of the beamforming-only approach is primarily determined

by the eigenvalue decomposition operations, resulting in an approximate complexity of $\mathcal{O}(M^3)$, where M represents the number of AP antennas. In contrast, the IRS-assisted AO algorithm with a complexity of $\mathcal{O}(N^2M^2)$, in addition to solving a semi-definitee programming problem that incurs computational overhead $\mathcal{O}(N^4)$. Taking into account the maximum iteration number T and the practical scenario where N is significantly larger than M , the overall complexity of these benchmark algorithms can be approximated as $\mathcal{O}(t_{max}N^4M)$.

By comparison, the proposed GSO algorithm significantly reduces computational complexity, but requires a larger number of iterations t_{max} to achieve convergence, which may lead to increased computational time in practical applications. However, the method exhibits greater versatility and effectively avoids the common solution difficulties encountered in traditional complex optimization problems. Therefore, despite potentially requiring more computation time, it substantially enhances the practicality and adaptability of the algorithm while maintaining performance. This method is particularly well-suited for large-scale IRS-assisted wireless communication systems, where the number of reflecting elements far exceeds the number of AP antennas ($N >> M$). This approach thus provides an efficient solution for practical beamforming design.

4 Simulation

In this section, we conducted numerical experiments to validate the efficacy of the proposed method. We benchmarked its performance against established schemes:

- **GSO with IRS:** Utilizes GSO for joint beamforming design towards the IRS at the AP.
- **CSO with IRS:** Applies CSO for joint beamforming design towards the IRS at the AP [44].
- **PSO with IRS:** Applies PSO for joint beamforming design towards the IRS at the AP [45].
- **AP MRT with IRS:** Implements maximum ratio transmission (MRT)-based beamforming towards the IRS at the AP [26].
- **Optimal AP without IRS:** Does not involve IRS and designs $\mathbf{x}$ [41].
- **Upper bound:** Represents a secrecy rate upper bound of the SDR algorithm [27].

Table 1 outlines the key simulation parameters used to evaluate the performance of the IRS-assisted secure communication system. The access point (AP) is equipped with $M = 4$ antennas. The base station, user, and eavesdropper are aligned along the horizontal axis at $\boldsymbol{p}_{\mathrm{b}} = [0, 0]$, $\boldsymbol{p}_{\mathrm{u}} = [150, 0]$ and $\boldsymbol{p}_{\mathrm{e}} = [145, 0]$ respectively. The IRS is strategically placed at $\boldsymbol{p}_{\mathrm{r}} = [145, 5]$, forming a triangle with the user and eavesdropper to facilitate effective reflection paths. We can calculate d_{AE} and d_{AU} with the points $\boldsymbol{p}_{\mathrm{b}}$, $\boldsymbol{p}_{\mathrm{u}}$, $\boldsymbol{p}_{\mathrm{e}}$ and $\boldsymbol{p}_{\mathrm{r}}$.

Table 1 Simulation Parameters

Parameter	Symbol	Value
AP dimensions	M	4
BS position	$\boldsymbol{p}_{\mathrm{b}}$	$[0, 0]$
User position	$\boldsymbol{p}_{\mathrm{u}}$	$[150, 0]$
Eavesdropper position	$\boldsymbol{p}_{\mathrm{e}}$	$[145, 0]$
IRS position	$\boldsymbol{p}_{\mathrm{r}}$	$[145, 5]$
Reference distance loss	ζ_0	-30 dB
Reference distance	d_0	1 m
Path loss	$\alpha_{\mathrm{AU}}, \alpha_{\mathrm{AE}}$	3
Path loss	α_{AI}	2.2
Rician factor	$K_{\mathrm{AI}}, K_{\mathrm{IU}}, K_{\mathrm{IE}}$	1
Noise variance	σ_U^2, σ_E^2	-80dBm

The reference path loss is set to $\zeta_0 = -30\,\mathrm{dB}$ at distance $d_0 = 1\,\mathrm{m}$. The path loss exponents are selected based on the typical urban propagation scenario is assumed with $\alpha_{\mathrm{AU}} = \alpha_{\mathrm{AE}} = 3$ for the direct links, while the AP-IRS link has a smaller exponent $\alpha_{\mathrm{AI}} = 2.2$, reflecting favorable line-of-sight (LoS) conditions. All IRS-related links are modeled as Rician fading channels with a Rician factor $K_{\mathrm{AI}} = K_{\mathrm{IU}} = K_{\mathrm{IE}} = 1$, indicating moderate LoS components. The noise power at both the user and the eavesdropper is set to $\sigma_U^2 = \sigma_E^2 = -80\,\mathrm{dB}$, consistent with thermal noise levels under typical receiver noise figures. These parameters collectively provide a realistic foundation for assessing the proposed secure transmission strategies.

Fig. 5 illustrates the average secrecy rates of various schemes against the transmit power P_{AP}, for $N = 64$. It is evident that IRS-based methods significantly enhance the average secrecy rate compared to configurations without IRS. Moreover, as the transmission power increases, the secrecy performance of IRS-based schemes improves notably. This indicates that IRS can effectively leverage signal reflections to enhance the communication system's secrecy, thereby countering eavesdropping attacks.

The Alternating Optimization (AO) method performs well when the power is below 25 dB. As the power exceeds 25 dB, while the conventional PSO algorithm shows comparable performance to AO due to its limited optimization capability, both the CSO algorithm and our proposed GSO algorithm for optimizing IRS reflection coefficients exhibit significant advantages in achieving higher secrecy rates. The GSO algorithm incorporates an innovative diversified particle update mechanism that preserves advantageous particle

characteristics while enhancing population diversity, ultimately outperforming both CSO and PSO algorithms with performance advantages that scale with increasing transmit power.

From the experiments, it can be observed that when the transmission power is below 25 dB, the performance of the proposed algorithm is inferior to that of the Alternating Optimization (AO) algorithm. However, when the transmission power exceeds 25 dB, the performance of the proposed GSO algorithm surpasses that of the AO algorithm, with the performance gap widening as the power increases. Therefore, under transmission powers of 15 dB and 30 dB, we investigated the impact of the number of IRS reflection units on the average secrecy rate.

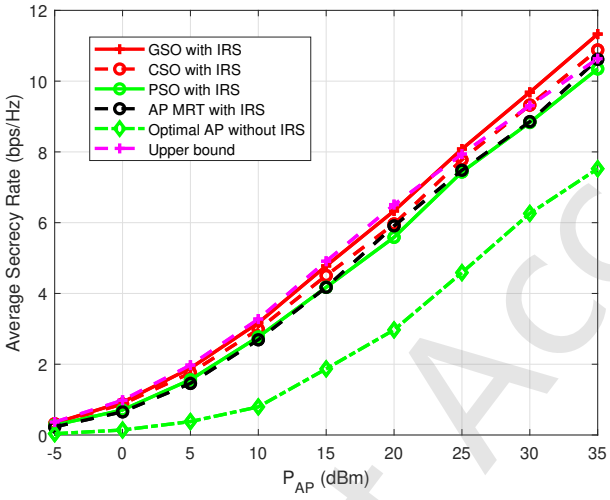

Fig. 5 Secrecy rate versus P_{AP}.

Fig. 6 illustrates the average secrecy rates of different schemes against the numbe of IRS reflection units with $P_{AP} = 15dB$. We observe that with the number of IRS reflection units increases, the average secrecy rate of IRS-assisted communication systems improves significantly, greatly surpassing that of systems without IRS assistance. This indicates the crucial role of IRS in enhancing the secrecy performance of communication systems, with its advantages becoming more pronounced as the number of reflection units grows. It also suggests that IRS effectiveness is more prominent in large-scale deployments.

Compared to CSO and PSO, the GSO algorithm performs better in terms of the average secrecy rate, indicating that GSO is more effective in optimizing IRS reflection coefficients. GSO leverages its internal diversity to better handle larger-scale optimization problems, thus improving the system's secrecy performance. As the scale of the optimization problem increases, its complexity also increases. The diversity of particles in the GSO algorithm allows it to excel in handling large-scale problems compared to CSO and PSO.

At low power levels, the impact of adjusting IRS reflection coefficients on system performance is relatively small. In such cases, both GSO and CSO perform below the upper performance bound of the alternating optimization algorithm, which may be due to the limited impact of IRS amplitude adjustments on system performance under low power conditions. Therefore, we further investigated the impact of the number of IRS reflection units on the average secrecy rate when the maximum transmission power is 30 dB and examined the effect of IRS amplitude optimization on the average secrecy rate.

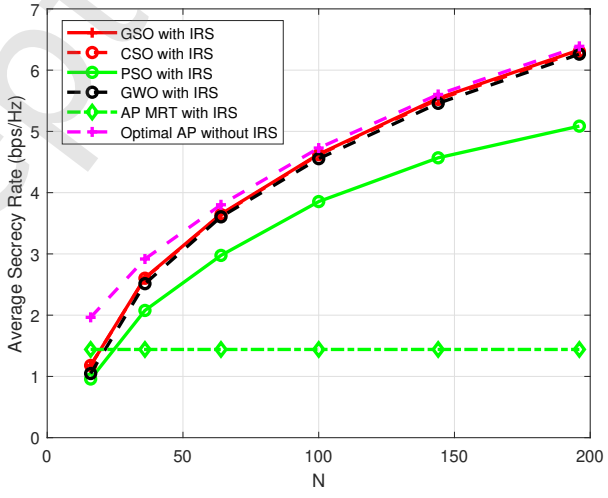

Fig. 6 Secrecy rate versus N, $P_{AP} = 15dB$.

This study examined the influence of IRS amplitude by varying the number of reflection units, presenting the results of the average secrecy rate at $P_{AP} = 30$dB in Fig. 7. The results indicate that when the number of IRS reflection units increases, the average secrecy rate also increases, further demonstrating the significant potential of IRS in enhancing the security of wireless communication systems. When the number of IRS reflection units is relatively small, the performance of optimization algorithms is below the performance limit of the alternating optimization algorithm. However, when the number of reflecting elements exceeds 64, the performance of these algorithms improves significantly, with both GSO and CSO surpassing the performance limit of the alternating optimization method. As the number of reflecting elements continues to increase, the gap between the average secrecy rate achieved by the optimization algorithms and the performance upper bound of the alternating optimization

method further widens. Notably, the performance differences between the proposed GSO algorithm and the CSO and PSO algorithms become increasingly pronounced in large-scale scenarios.

These observations indicate that as the number of IRS reflecting elements increases, the complexity of the optimization problem rises accordingly. The proposed GSO algorithm demonstrates more significant advantages in solving such complex problems compared to the CSO and PSO algorithms.

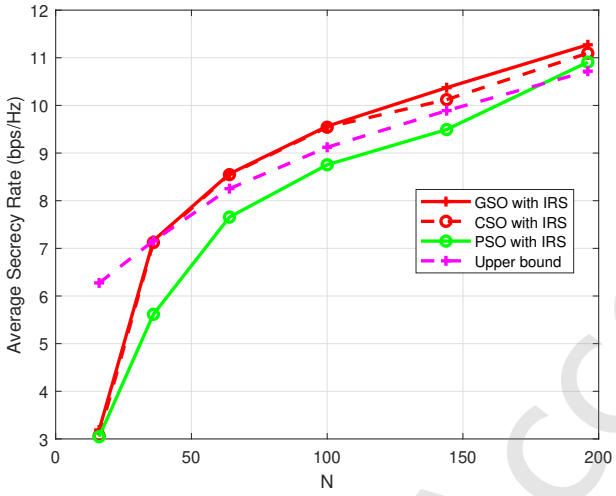

Fig. 7 Secrecy rate versus N, $P_{AP} = 30dB$.

In summary, the problem of maximizing the secrecy rate through joint optimization of IRS reflection coefficients proposed in this paper effectively leverages the potential of IRS in channel control, significantly enhancing the security of wireless communication systems. Additionally, the GSO algorithm introduced in this paper demonstrates superior exploration and exploitation capabilities compared to existing algorithms, effectively avoiding local optima. The GSO algorithm provides better optimization results when addressing large-scale optimization problems.

5 Conclusions

This paper investigates the impact of IRS reflection amplitude on the security of IRS-assisted communication systems and proposes a problem of joint optimization of transmitter beamforming and IRS reflection phase and amplitude to maximize user secrecy rate. Due to the difficulties faced by traditional alternating optimization algorithms in solving this problem, inspired by the concept of swarm learning, a novel Group Competitive Swarm Optimization (GSO) algorithm is proposed. This algorithm forms learning groups by randomly selecting three particles, ranks the particles using a competition mechanism, and updates their positions based on the ranking results with different strategies. Experimental results validate that the GSO algorithm can more effectively optimize transmitter beamforming and IRS reflection amplitude and phase under large-scale IRS systems and high-power transmission conditions, achieving higher secrecy rates and providing a new solution for secure communication in IRS-assisted communication systems.

This work thoroughly incorporates the dynamic configuration of IRS into the modeling process to achieve optimal reflection control. Nevertheless, in practical implementations, frequent adjustments of IRS phase and amplitude may incur substantial feedback overhead. Recent literature in the domains of physical layer security and 6G communications has increasingly emphasized system architectures that rely on a limited set of discrete reflection states or quantized control schemes. Such low-complexity, feedback-efficient designs have garnered significant scholarly attention and are considered pivotal to enabling large-scale practical deployments. Accordingly, future research should aim to extend the proposed optimization framework to scenarios that are more amenable to practical engineering constraints, with particular emphasis on evaluating the adaptability and scalability of the approach under constrained control conditions. This represents a critical direction for ongoing and future research.

Acknowledgment

This work was supported by the National Natural Science Foundation of China under Grant 62495081 and Grant 62502111, is supported by the Joint International Research Laboratory of Spatio-temporal Information and Intelligent Location Services under Grant Number C25GAH13, is supported by the project for Enhancing Young and Middle-aged Teacher's Research Basis Ability in Colleges of Guangxi under Grant Number 2025KY0237.

Declaration of competing interest

The authors have no competing interests to declare that are relevant to the content of this article.

Reference

[1] J. C. Mesa, M. D. MacLean, M. MS, A. Nguyen, R. Patel, T. Diemer, J. Lim, C. H. Lee, and H. Lee, A wearable device towards automatic detection and treatment of opioid overdose, *IEEE Trans. Biomed. Circuits Syst.*, vol. 18, no. 2, pp. 396–407, Nov. 2024.

[2] T. Wei, W. Feng, Y. Chen, C.-X. Wang, N. Ge, and J. Lu, Hybrid satellite-terrestrial communication networks for the maritime internet of things: Key technologies, opportunities, and challenges, *IEEE Internet of Things J.*, vol. 8, no. 11, pp. 8910–8934, Feb. 2021.

[3] W. Li, L. Zhang, Y. Wu, Z. Hong, S. Laflèche, S.-I. Park, S. Kown, S. Ahn, N. Hur, E. Iradier, I. Bilbao, J. Montalban, and P. Angueira, Integrated inter-tower wireless communications network for terrestrial broadcasting and multicasting systems, *IEEE Trans. Broadcast*, vol. 67, no. 3, pp. 570–581, May 2021.

[4] M. Wang, J. Wu, T. Zhang, J. Wu, and G. Li, Effective identity authentication based on multiattribute centers for secure government data sharing, *Tsinghua Sci. Technol.*, vol. 29, no. 3, pp. 736–752, Jun. 2024. [Online]. Available: https://www.sciopen.com/article/10.26599/TST.2023.9010049

[5] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, Safeguarding 5g wireless communication networks using physical layer security, *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

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

[7] K. L. Narayanan and R. Naresh, A effective encryption and different integrity schemes to improve the performance of cloud services, in *ICONAT*, Jan. 2022, pp. 1–5.

[8] A. Yener and S. Ulukus, Wireless physical-layer security: Lessons learned from information theory, *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Sep. 2015.

[9] Z. Xu, J. Cui, K. Hu, and M. Wang, Integral attack on the full future block cipher, *Tsinghua Sci. Technol.*, vol. 30, no. 1, pp. 161–170, Jan. 2025. [Online]. Available: https://www.sciopen.com/article/10.26599/TST.2024.9010007

[10] J. M. Hamamreh, H. M. Furqan, and H. Arslan, Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey, *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, Oct. 2019.

[11] T. Xia, M. M. Wang, J. Zhang, and L. Wang, Maritime internet of things: Challenges and solutions, *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 188–196, Mar. 2020.

[12] J. Du, A partially coupled ldpc coded scheme for the gaussian wiretap channel, *IEEE Commun. Lett.*, vol. 24, no. 1, pp. 7–10, Oct. 2020.

[13] A. K. Yerrapragada, T. Eisman, and B. Kelley, Physical layer security for beyond 5g: Ultra secure low latency communications, *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2232–2242, Aug. 2021.

[14] M. Li, P. Xue, H. Yuan, and Y. Han, Physical layer security for cr-noma network with cooperative jamming, *Tsinghua Sci. Technol.*, vol. 30, no. 2, pp. 708–720, Apr. 2025.

[15] C. E. Shannon, Communication theory of secrecy systems, *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[16] A. D. Wyner, The wire-tap channel, *The Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[17] W. Zhao, S.-H. Lee, and A. Khisti, Phase-only zero forcing for secure communication with multiple antennas, *IEEE J. Sel. Top. Signal Process.*, vol. 10, no. 8, pp. 1334–1345, Sep. 2016.

[18] W. Yang, L. Tao, X. Sun, R. Ma, Y. Cai, and T. Zhang, Secure on-off transmission in mmwave systems with randomly distributed eavesdroppers, *IEEE Access*, vol. 7, pp. 32 681–32 692, Mar. 2019.

[19] M. E. Eltayeb and R. W. Heath, Securing mmwave vehicular communication links with multiple transmit antennas, in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2018, pp. 1–6.

[20] P. Chen, J. Ouyang, W.-P. Zhu, M. Lin, A. E. Shafie, and N. Al-Dhahir, Artificial-noise-aided energy-efficient secure beamforming for multi-eavesdroppers in cognitive radio networks, *IEEE Syst. J.*, vol. 14, no. 3, pp. 3801–3812, Feb. 2020.

[21] C. Liu, L.-L. Yang, and W. Wang, Secure spatial modulation with a full-duplex receiver, *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 838–841, Sep. 2017.

[22] X. Zhu, Y. Yang, z. liu, Z. Ding, x. tao, S. Li, Z. Chen, X. Ma, C.-L. I., S. Han, K. Li, c. pan, x. shen, z. zheng, Y. Guo, Z. Ding, H. Haas, w. tong, p. zhu, and L. Hanzo, Towards 6g wireless communication networks: Vision, enabling technologies, and new paradigm shifts, *Sci. China Inf. Sci.*, vol. 64, pp. 1–74, Jan. 2020.

[23] G. Zhou, C. Pan, H. Ren, K. Wang, K. K. Chai, and K.-K. Wong, User cooperation for irs-aided secure mimo systems, *Intelligent and Converged Networks*, vol. 3, no. 1, pp. 86–102, Mar. 2022.

[24] Q. Wu and R. Zhang, Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming, *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Aug. 2019.

[25] M. D. Marco Di Renzo and et al., Smart radio environments empowered by reconfigurable ai meta-surfaces: An idea whose time has come, *EURASIP J. Wireless Commun. Netw*, vol. 2019, no. 1, pp. 1–20, May 2019.

[26] M. Cui, G. Zhang, and R. Zhang, Secure wireless communication via intelligent reflecting surface, *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, May 2019.

[27] L. Liu, R. Zhang, and K.-C. Chua, Secrecy wireless information and power transfer with miso beamforming, *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Apr. 2014.

[28] J. Sun, J. Li, W. Hao, X. Mu, Z. Chu, and P. Xiao, Secure transmission design with strong channel correlation for passive/active ris communications, *IEEE Wireless Commun. Lett.*, vol. 12, no. 8, pp. 1394–1398, May 2023.

[29] Y. Ge and J. Fan, Robust secure beamforming for intelligent reflecting surface assisted full-duplex miso systems, *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 253–264, Dec. 2022.

[30] M. Hua, L. Yang, Q. Wu, C. Pan, C. Li, and A. L. Swindlehurst, Uav-assisted intelligent reflecting surface symbiotic radio system, *IEEE Trans. Wireless Commun.*, vol. 20, no. 9, pp. 5769–5785, Sep. 2021.

[31] A. Taneja, S. Rani, A. Alhudhaif, D. Koundal, and E. S. Gündüz, An optimized scheme for energy efficient wireless communication via intelligent reflecting surfaces, *Expert Sys. App.*, vol. 190, p. 116106, Mar. 2022.

[32] Z. Peng, Z. Zhang, L. Kong, C. Pan, L. Li, and J. Wang, Deep reinforcement learning for ris-aided multiuser full-duplex secure communications with hardware impairments, *IEEE Internet of Things J.*, vol. 9, no. 21, pp. 21 121–21 135, May 2022.

[33] G. Chen, Q. Wu, R. Liu, J. Wu, and C. Fang, Irs aided mec systems with binary offloading: A unified framework for dynamic irs beamforming, *IEEE J. Sel. Areas Commun.*, vol. 41, no. 2, pp. 349–365, Dec. 2022.

[34] Q. Wu, B. Zheng, C. You, L. Zhu, K. Shen, X. Shao, W. Mei, B. Di, H. Zhang, E. Basar *et al.*, Intelligent surfaces empowered wireless network: Recent advances and the road to 6g, *Proc. IEEE*, vol. 112, no. 7, pp. 724–763, Jun. 2024.

[35] X. Yu, D. Xu, and R. Schober, Enabling secure wireless communications via intelligent reflecting surfaces, in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6.

[36] H. Luo, L. Han, T. Shuai, and F. Wang, Approximation and heuristic algorithms for the priority facility location problem with outliers, *Tsinghua Sci. Technol.*, vol. 29, no. 6, pp. 1694–1702, Jun. 2024.

[37] S. Luo, X. Zhu, and J. Ran, Key technology innovation mode of new energy industry ecological integration system based on particle swarm optimization algorithm, *Tsinghua Sci. Technol.*,, vol. 29, no. 6, pp. 1752–1762, Feb. 2024.

[38] Q. Wu and R. Zhang, Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network, *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Nov. 2020.

[39] L. Dai, B. Wang, M. Peng, and S. Chen, Hybrid precoding-based millimeter-wave massive mimo-noma with simultaneous wireless information and power transfer, *IEEE J. Sel. Areas in Commun.*, vol. 37, no. 1, pp. 131–141, Oct. 2019.

[40] X. Yu, D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, Robust and secure wireless communications via intelligent reflecting surfaces, *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2637–2652, Jul. 2020.

[41] A. Khisti and G. W. Wornell, Secure transmission with multiple antennas i: The misome wiretap channel, *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jun. 2010.

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

[43] R. Lan, Y. Zhu, H. Lu, Z. Liu, and X. Luo, A two-phase learning-based swarm optimizer for large-scale optimization, *IEEE Trans. Cybern.*, vol. 51, no. 12, pp. 6284–6293, Dec. 2021.

[44] R. Cheng and Y. Jin, A competitive swarm optimizer for large scale optimization, *IEEE Trans. Cybern.*, vol. 45, no. 2, pp. 191–204, May 2015.

[45] Y. del Valle, G. K. Venayagamoorthy, S. Mohagheghi, J.-C. Hernandez, and R. G. Harley, Particle swarm optimization: Basic concepts, variants and applications in power systems, *IEEE Trans. Evol. Comput.*, vol. 12, no. 2, pp. 171–195, Apr. 2008.

Author biography

Shanwen Guan received the B.E. degree in electronic information engineering from Wuhan Institute of Technology, Wuhan, China, in 2016, and the Ph.D. degree in cyberspace security from Guilin University of Electronic Technology in 2024. He is currently affiliated with the Postdoctoral Research Station in Information and Communication Engineering, and the Joint International Research Laboratory of Spatio-Temporal Information and Intelligent Location Services at Guilin University of Electronic Technology, China. His research interests include variational inference, direction-of-arrival (DOA) estimation, and heuristic optimization algorithms.

Xintong Shen received his Bachelor's degree in Software Engineering from Liaoning University of Technology in 2020. He is currently studying Artificial Intelligence at the School of Computer Science, Khon Kaen University in Thailand, with research interests including nature-inspired optimization algorithms and image processing.

Xinyun Zhang is currently a research assistant in the School of Computer Science and Information Security, Guilin University of Electronic Science and Technology. Her current research areas include image processing and speech signal processing.

Ji Li received the Ph.D. degree from Université de Montréal, Montreal city of Quebec Province, Canada, in 2007. Since 2020, he entered the School of Computer Science and Information Security of Guilin University of Electronic Technology as a professor. His main research fields include: indoor positioning, wireless communication, artificial intelligence, palm vein recognition and multi-source data fusion.

Li Zhou received the Ph.D. degree from Lanzhou University, Lanzhou, China, in 2024. His current research interests include affective computing, video and image processing, and automatic depression detection.

Xiaonan Luo is currently a Professor with the School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China. His current research interests include computer vision, image processing, and computer graphics and CAD.