TẠP CHÍ KHOA HỌC VÀ GIÁO DỤC
ISSN: 1859-1612
Journal homepage: https://tckhgd.dhsphue.edu.vn

Exploiting adaptive particle swarm optimization and penalty function methods for secrecy rate maximization in secure IRS-aided SWIPT system

Nguyen Le Trung Thanh, Hoang Trong Duc, Le Phan Quoc Hung, Pham Viet Tuan

University of Education, Hue University

ARTICLE INFO

Article history:
Received: 22 December 2025
Received in revised form: 13 March 2026
Accepted: 16 March 2026
Published: 20 April 2026

Keywords:
Intelligent reflecting surface;
SWIPT;
Power-splitting;
Secrecy rate maximization;
Adaptive PSO.

ABSTRACT

In this work, the physical layer security of an intelligent reflecting surface (IRS)-assisted simultaneous wireless information and power transfer (SWIPT) system is investigated in the presence of an eavesdropper (Eve). The goal is to maximize the secrecy rate while satisfying the harvested energy threshold at the power-splitting (PS) receiver. By optimizing the phase shifts at the IRS, the signal is enhanced at the receiver while reduced at Eve. The solution approach via the penalty function technique and adaptive particle swarm optimization (PSO) is proposed and performed through numerical experiments. Eventually, the impacts of system factors such as transmission power and energy harvesting threshold on the convergent behavior and the secrecy rate are presented, and the future direction is discussed.

1. INTRODUCTION

Recently, the intelligent reflecting surface (IRS) has emerged as a highly promising technology to devise new cost-efficient wireless solutions that can support data/energy transmission in wireless networks such as Internet of Things (IoT), cellular, sensor systems (Wang et al., 2020; Mir et al., 2025; Liu et al., 2021). An IRS consists of numerous passive reflective elements, each controlled by a phase shift unit to manipulate the characteristics of incident signals (Mir et al., 2025). By carefully designing the phase shifts of these elements, an IRS can enhance signal reception at targeted destinations and/or suppress interference at unintended receivers, thereby creating more favorable propagation environments without the need for any radio-frequency (RF) chains. Due to their low-cost structure and ease of deployment, commonly installed on building surfaces, IRSs demonstrate strong potential for diverse applications, especially in dense urban environments where line-of-sight links between transmitters (Tx) and receivers (Rx) are often obstructed (Liu et al., 2021).

With the rapid growth of IoT devices, ensuring the sustainability of hardware and energy supplies has become a critical bottleneck obstructing the advancement of next-generation wireless networks. To tackle this challenge, simultaneous wireless information and power transfer (SWIPT) has been proposed as a promising solution. In a SWIPT framework, RF signals act as carriers of both information and energy, thereby enabling IoT devices to achieve data exchange and energy harvesting simultaneously. Consequently, maintaining an appropriate balance between communication performance and power delivery becomes a key design criterion in SWIPT systems (Psomas et al., 2024; Perera et al., 2017; Tang et al., 2023).

Because wireless high-power SWIPT signals are broadcast, they are easily affected by security risks such as jamming and information leakage. Recently, physical layer security (PLS) has gained much attention because it avoids complex key exchange methods and works well for low-latency B5G/6G applications. To improve secure communication rates, researchers have proposed using artificial noise and multiple-antenna technique. However, when the channels of legitimate users and eavesdroppers are correlated, or when eavesdroppers are closer to the base station, the secrecy rate is still limited. In (Niu et al., 2021), the authors

Corresponding author: Pham Viet Tuan;
E-mail address: phamviettuan@dhsphue.edu.vn
DOI: https://doi.org/10.26459/jse.044.2026

use passive IRSs for information security in SWIPT systems with a number of receivers and specific information receivers, considering the standard maximum power constraint. In (Hao et al., 2024; Fotock et al., 2024), the authors studied the maximization of secure energy efficiency for uplink and cell-free systems with the presence of multiple eavesdroppers. The authors in (Guo et al., 2024; Kaur et al., 2024) summarized the IRS research in information security and future research directions. In which, IRS applications combine with other techniques such as SWIPT, integrated sensing and communication (ISAC), and rate-splitting multiple access (RSMA) to improve the performance while ensuring the security of the system. In (Sarhan et al., 2025), the authors investigated the secrecy energy efficiency (SEE) maximization by optimizing IRS passive and BS active beamformers, and power constraints. The authors exploited deep reinforcement learning, an artificial intelligence technique by considering the PLS issue as a Markov decision process (MDP). However, we observe that most prior works applied non-convex approximations or machine learning methods in the security IRS-aided networks, especially in secure SWIPT networks. Therefore, in this work, the particle swarm optimization (PSO)-based approach is proposed to find a heuristic solution in security issue.

Introduced by Kennedy and Eberhart in 1995, PSO has become popular for its simplicity, flexibility, and effectiveness in solving various optimization problems. Originally, PSO is inspired by the social behavior of birds, fish, or insects, where each particle adjusts its movement based on its own experience and that of its neighbors to find the optimal solution within the search space (Abualigah, 2025). In this study, we focus on secure IRS-aided communication for a SWIPT system with a single power-splitting (PS) user and a single Eve. The maximization of the secrecy rate is investigated under the constraint of the required EH threshold. The meta-heuristic algorithm of PSO has proved the effectiveness in finding a heuristic global optimal solution. Thus, we exploit an animal-inspired PSO approach to solve the considered security IRS-aided issue. The key contributions are three-fold points:

(1) The IRS-aided SWIPT communication with a single PS-user and a single Eve is considered and the secrecy problem is formulated under the required EH threshold.

(2) The penalty method is initially applied to transform the problem into an unconstrained optimization problem and then the adaptive meta-heuristic PSO approach is applied to find the near-optimal phase shifts at the IRS for the security optimization problem.

(3) The numerical experiments are performed to evaluate the convergence and results of the proposed penalty-based adaptive PSO approach.

The outline of this paper is summarized as follows. The considered system and the secrecy rate maximization issue are presented in Section 2. The proposed penalty-based adaptive PSO algorithm for finding optimal solution is presented in Section 3. Lastly, the numerical experiments and concluding remarks are presented in Sections 4 and 5, respectively.

Notation: Throughout this paper, lowercase letters denote scalars, bold lowercase letters denote vectors, and bold uppercase letters denote matrices. In addition, $|x|$ is the absolute value of a complex scalar while $\|\mathbf{x}\|$ is the Euclidean norm of a complex vector $\mathbf{x}$. Furthermore, a diagonal matrix $\text{diag}(\mathbf{x})$ is generated from a diagonal vector $\mathbf{x}$. $\mathbb{C}^{m\times n}$ is indicated as the $m\times n$ complex matrix space. Lastly, $\mathcal{CN}\left(\mu,\sigma^2\right)$ denotes the distribution of a circularly symmetric complex Gaussian random variable with mean μ and variance σ^2.

2. NETWORK DESCRIPTION AND SECRECY PROBLEM FORMULATION

In this section, the system illustration is first presented for a secure SWIPT system with an external eavesdropper. After that, the channel and mathematical signal communication model are shown in detail. Secondly, the secrecy transmission problem is formulated under the constraints of the receiver's requirements.

2.1. Network description

In fig. 1, the considered SWIPT communication under the assistance of an IRS is shown. A single-antenna transmitter simultaneously sends confidential data and energy to the single-antenna PS receiver and prevents an external Eve from decoding information. The receiver equipped with a power-splitting architecture allocates a half for energy harvesting and the remaining part for information decoding. The single-antenna eavesdropper tries to eavesdrop on the communication between the transceiver. The channel state information (CSI) of every communication link is given perfectly at the transmitter and the IRS where they can be obtained by state-of-the-art estimation approaches (Abualigah, 2025). In an environment of signal blockage, there are no signals that

directly arrive from the transmitter to the receiver or the eavesdropper and the IRS with phase-shift reflection capability can support confidential data and energy transmission.

We denote the links from the transmitter to the IRS (Tx-IRS), from the IRS to the PS receiver (IRS-Rx), and from the IRS to the eavesdropper (IRS-Eve) as $\mathbf{G} \in \mathrm{C}^{N \times M}$, $\mathbf{h}_{\mathrm{R}} \in \mathrm{C}^{N \times 1}$, and $\mathbf{h}_{\mathrm{E}} \in \mathrm{C}^{N \times 1}$, respectively. The information symbol s with zero mean and unit variance $\mathrm{E}\left[|s|^2\right]=1$ is sent from the transmitter with power P_{T}, thus, the signal from the transmitter is expressed as $\sqrt{P_{\mathrm{T}}}s$.

Our proposed solution is based on the ideal assumption that perfect channel state information (CSI) is available at both the BS and the passive IRS as recent works (Wu & Zhang, 2020; Wei et al., 2024). In practice, acquiring accurate CSI is difficult because low-cost hardware is limited to signal reflection. In this work, the IRS is purely passive, without power amplifiers and lack of signal processing units. As a result, unlike conventional active transceivers, the IRS cannot transmit or process pilot symbols for channel estimation. In case of imperfect CSI, the proposed IRS design needs to be revisited and will be studied in future work. Note that the performance of this research can be behaved as an upper bound under imperfect CSI scenarios.

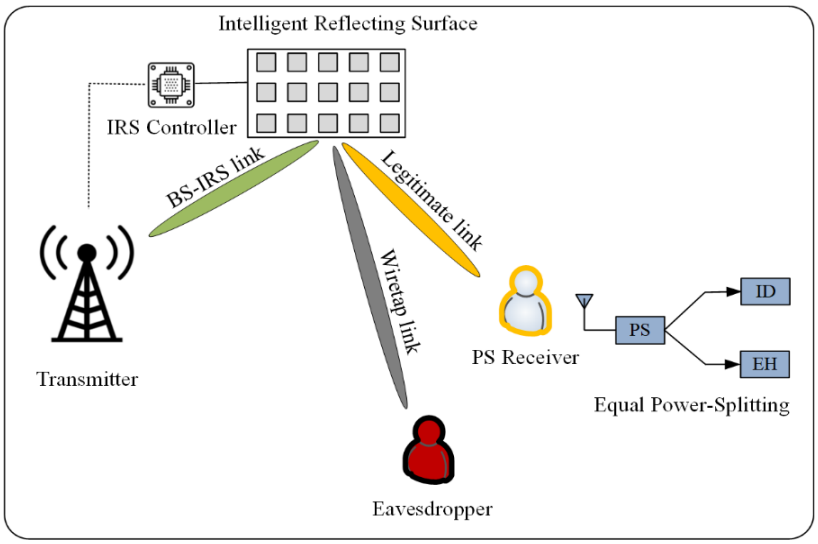

Figure 1. System model.

Each PS-based hybrid receiver employs a power-splitting structure to simultaneously perform information decoding and energy harvesting. To improve the quality of communication, a passive IRS intervention including *N* components is deployed. At the *n*th element of the active IRS, $\varphi_n \in [0, 2\pi)$ represents the phase-shift coefficient, $\forall n \in \mathrm{N} = \{1,...,N\}$. As a result, the phase-shift impact $\Phi = \mathrm{diag}\left(\left[e^{j\varphi_1}, \cdots, e^{j\varphi_N}\right]\right)$ expresses the reflection of the IRS.

Accordingly, the signal arriving at the receiver from the IRS is represented as:

$$r_{\mathrm{R}} = \mathbf{h}_{\mathrm{R}}^{H} \mathbf{\Phi} \mathbf{G}\left(\sqrt{P_{\mathrm{T}}}s\right) + n_{\mathrm{R}} \tag{1}$$

Here, the receiver's antenna is subject to additive noise $n_{\mathrm{R}} \sim \mathrm{CN}\left(0, \sigma_{\mathrm{R}}^2\right)$. The PS-based hybrid receiver splits the received signal into two streams using a power-splitting coefficient ρ_{R}, where one stream, with a power ratio of $\rho_{\mathrm{R}} \in (0,1)$ is used for information decoding, and the other, with a power ratio of $(1-\rho_{\mathrm{R}})$ is used for energy harvesting. Consequently, the ID signal portion is represented as $r_{\mathrm{R}}^{\mathrm{ID}} = \sqrt{\rho_{\mathrm{R}}}\, r_{\mathrm{R}} + v_{\mathrm{R}}$ under processing noise $v_{\mathrm{R}} \sim \mathrm{CN}\left(0, \delta_{\mathrm{R}}^2\right)$. The EH signal portion is represented as $r_k^{\mathrm{EH}} = \sqrt{1-\rho_{\mathrm{R}}}\, r_{\mathrm{R}}$. For these reasons, the information rate of the PS receiver is formulated as

$$D_k = \log_2\left(1 + \frac{\rho_{\mathrm{R}} P_{\mathrm{T}} \left|\mathbf{h}_{\mathrm{R}}^{H} \mathbf{\Phi} \mathbf{g}\right|^2}{\rho_{\mathrm{R}} \sigma_{\mathrm{R}}^2 + \delta_{\mathrm{R}}^2}\right) \tag{2}$$

and the harvested energy with the presumption of perfect energy conversion efficiency is given by

$$E_k = (1-\rho_{\mathrm{R}})\left(P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{R}}^H\mathbf{\Phi}\mathbf{g}\right|^2\right) \tag{3}$$

For the eavesdropper, the received signal is expressed as:

$$r_{\mathrm{E}} = \mathbf{h}_{\mathrm{E}}^H\mathbf{\Phi}\mathbf{G}\left(\sqrt{P_{\mathrm{T}}}s\right) + n_{\mathrm{E}} \tag{4}$$

and the data rate is calculated as:

$$D_{\mathrm{E}} = \log_2\left(1+\frac{P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{E}}^H\mathbf{\Phi}\mathbf{g}\right|^2}{\sigma_{\mathrm{E}}^2}\right) \tag{5}$$

The secrecy rate is defined as:

$$R_{\mathrm{s}} = \left[\log_2\left(1+\frac{\rho_{\mathrm{R}}P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{R}}^H\mathbf{\Phi}\mathbf{g}\right|^2}{\rho_{\mathrm{R}}\sigma_{\mathrm{R}}^2+\delta_{\mathrm{R}}^2}\right) - \log_2\left(1+\frac{P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{E}}^H\mathbf{\Phi}\mathbf{g}\right|^2}{\sigma_{\mathrm{E}}^2}\right)\right]^+ \tag{6}$$

where $[a]^+$ is defined as $\max(a,0)$.

We also denote the signal-to-noise (SNR) of the receiver and the eavesdropper as $\gamma_{\mathrm{R}} = \frac{\rho_{\mathrm{R}}P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{R}}^H\mathbf{\Phi}\mathbf{g}\right|^2}{\rho_{\mathrm{R}}\sigma_{\mathrm{R}}^2+\delta_{\mathrm{R}}^2}$ and $\gamma_{\mathrm{E}} = \frac{P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{E}}^H\mathbf{\Phi}\mathbf{g}\right|^2}{\sigma_{\mathrm{E}}^2}$, respectively.

2.2. Secrecy rate maximization problem formulation

In our work, the objective is to maximize the secrecy rate by designing optimal phase shifts at the IRS under the required EH threshold, e_0, at the receiver. Then, the optimization problem **(P1)** is formulated as follows:

$$\underset{\{\varphi_n\}}{\text{maximize}} \left[\log_2\left(1+\frac{\rho_{\mathrm{R}}P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{R}}^H\mathbf{\Phi}\mathbf{g}\right|^2}{\rho_{\mathrm{R}}\sigma_{\mathrm{R}}^2+\delta_{\mathrm{R}}^2}\right) - \log_2\left(1+\frac{P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{E}}^H\mathbf{\Phi}\mathbf{g}\right|^2}{\sigma_{\mathrm{E}}^2}\right)\right]^+ \tag{7}$$

$$\text{subject to: } \mathbf{\Phi} = diag\left(\left[e^{j\varphi_1}, e^{j\varphi_2}, ..., e^{j\varphi_N}\right]^T\right),\ \varphi_n \in [0, 2\pi), \forall n \tag{8}$$

$$(1-\rho_{\mathrm{R}})\left(P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{R}}^H\mathbf{\Phi}\mathbf{g}\right|^2\right) \geq e_0 \tag{9}$$

In this problem, the PS receiver shares the balanced power of received signal for ID and EH executions, i.e., $\rho_{\mathrm{R}} = 0.5$. Then, we only focus on the optimization of IRS phase-shift parameters which are appropriate to apply PSO-based method. In the future, we will extend the proposed algorithm for finding the optimal PS factors and the transmitter parameters.

3. PROPOSED ADAPTIVE PSO-BASED SOLUTION ALGORITHM WITH PENALTY FUNCTION

Firstly, based on the penalty method, we move the energy constraint into secrecy rate objective function with a penalty factor $\mu > 0$ and obtain problem **(P2)** as follows:

$$\underset{\{\varphi_n\in[0,2\pi)\}}{\text{maximize}} \left(\left[\log_2\left(1+\frac{\rho_{\mathrm{R}}P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{R}}^H\mathbf{\Phi}\mathbf{g}\right|^2}{\rho_{\mathrm{R}}\sigma_{\mathrm{R}}^2+\delta_{\mathrm{R}}^2}\right) - \log_2\left(1+\frac{P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{E}}^H\mathbf{\Phi}\mathbf{g}\right|^2}{\sigma_{\mathrm{E}}^2}\right)\right]^+ - \mu\left[e_0 - (1-\rho_{\mathrm{R}})\left(P_{\mathrm{T}}\left|\mathbf{h}_{\mathrm{R}}^H\mathbf{\Phi}\mathbf{g}\right|^2\right)\right]^+\right) \tag{10}$$

The penalized objective function serves as the fitness function, defined as:

$$R_{\mathrm{s\_pen}}(\varphi_n) = R_{\mathrm{s}}(\varphi_n) - \mu\left[\max\left(0, e_0 - E(\varphi_n)\right)\right] \tag{11}$$

where $R_s(\varphi_n)$ is the secrecy rate function given in (6), and $E(\varphi_n)$ is the harvested energy function given in (3). Hence, the problem formulated in (10) is rewritten as follows:

$$\underset{\{\varphi_n \in [0,2\pi)\}}{\text{maximize}} \quad \left(R_s(\varphi_n) - \mu\left[\max\left(0,\, e_0 - E(\varphi_n)\right)\right]\right) \tag{12}$$

Using the large penalty factor μ, the maximization procedure of penalized fitness function allows finding the optimal phase shifts in the secrecy rate optimization problem without the EH constraint. After that, we solve problem (**P2)** by the adaptive meta-heuristic PSO method. An adaptive PSO algorithm is employed to solve the secrecy rate maximization problem. The proposed algorithm comprises two main steps, presented as follows.

The first step is initialization. A swarm of N_p particles is initialized, where each particle represents a candidate IRS phase vector $\{\varphi_n\}$. The phase components (positions) are randomly drawn from a uniform distribution over $[0,2\pi)$. Initial velocities v_n are set to zero. An initial penalty factor μ_0 is assigned. For each particle, the secrecy rate $R_s(\varphi_n)$, harvested energy $E(\varphi_n)$, and fitness function value $R_{s\_pen}(\varphi_n)$ are computed. Each particle's personal best position $pbest_n$ is initialized as φ_n accordingly. At initialization, the global best $gbest$ is selected using a feasibility-aware rule: if feasible particles exist, i.e., particles satisfying the EH constraint $E(\varphi_n) \geq e_0$, the one with the highest secrecy rate is chosen; otherwise, the particle with the smallest energy constraint violation is selected. This guarantees an initial search direction toward the feasible region.

The second step is iterative optimization. At each iteration, the swarm evolves through adaptive penalty adjustment, particle state update, and feasibility-aware best-solution selection. First, the penalty factor is updated adaptively. If at least one particle violates the energy EH constraint, i.e., $E(\varphi_n) < e_0$, the penalty factor is increased as $\mu = \alpha\mu$, where $\alpha > 1$. Otherwise, if all particles remain feasible for k consecutive iterations, the penalty factor is reduced as $\mu = \mu / \alpha$. Next, each particle updates its velocity and position according to the standard PSO update rules. The velocity of particle n at iteration $t+1$ is updated as:

$$v_n^{(t+1)} = \omega v_n^{(t)} + c_1 r_1 (pbest_n - \varphi_n^{(t)}) + c_2 r_2 (gbest - \varphi_n^{(t)}) \tag{13}$$

where ω is the inertia weight, c_1 and c_2 are the cognitive and social acceleration coefficients, respectively. Moreover, r_1 and r_2 are independently generated random scalars uniformly distributed in the interval $(0,1)$ at each iteration and for each particle, which introduce stochasticity into the particle movement and balance exploration and exploitation. The particle position is then updated as:

$$\varphi_n^{(t+1)} = \varphi_n^{(t)} + v_n^{(t+1)} \tag{14}$$

followed by a modulo operation to enforce the phase constraint $\varphi_n^{(t+1)} \in [0,2\pi)$.

For each updated particle, the secrecy rate $R_s(\varphi_n)$, the harvested energy $E(\varphi_n)$, and the corresponding penalized fitness value $R_{s\_pen}(\varphi_n)$ are recomputed. The individual best solution of each particle is updated whenever an improvement in the penalized fitness is observed.

Finally, the global best solution $gbest$ is selected using a feasibility-aware rule. Let F denote the set of feasible particles satisfying $E(\varphi_n) \geq e_0$, and I the set of infeasible ones. If $F \neq \varnothing$, the global best is chosen as the feasible particle achieving the maximum secrecy rate:

$$gbest = \arg\left(\max_{\varphi_n \in F} R_s(\varphi_n)\right). \tag{15}$$

Otherwise, when all particles are infeasible, the global best is chosen as the particle with the minimum energy constraint violation, defined by $e_0 - E(\varphi_n)$:

$$gbest = \arg\left(\min_{\varphi_n \in I}(e_0 - E(\varphi_n))\right). \tag{16}$$

This iterative process is repeated until the maximum number of iterations is reached or a stopping criterion is satisfied. The algorithm is illustrated by the flowchart (fig. 2) and summarized in table 1 below.

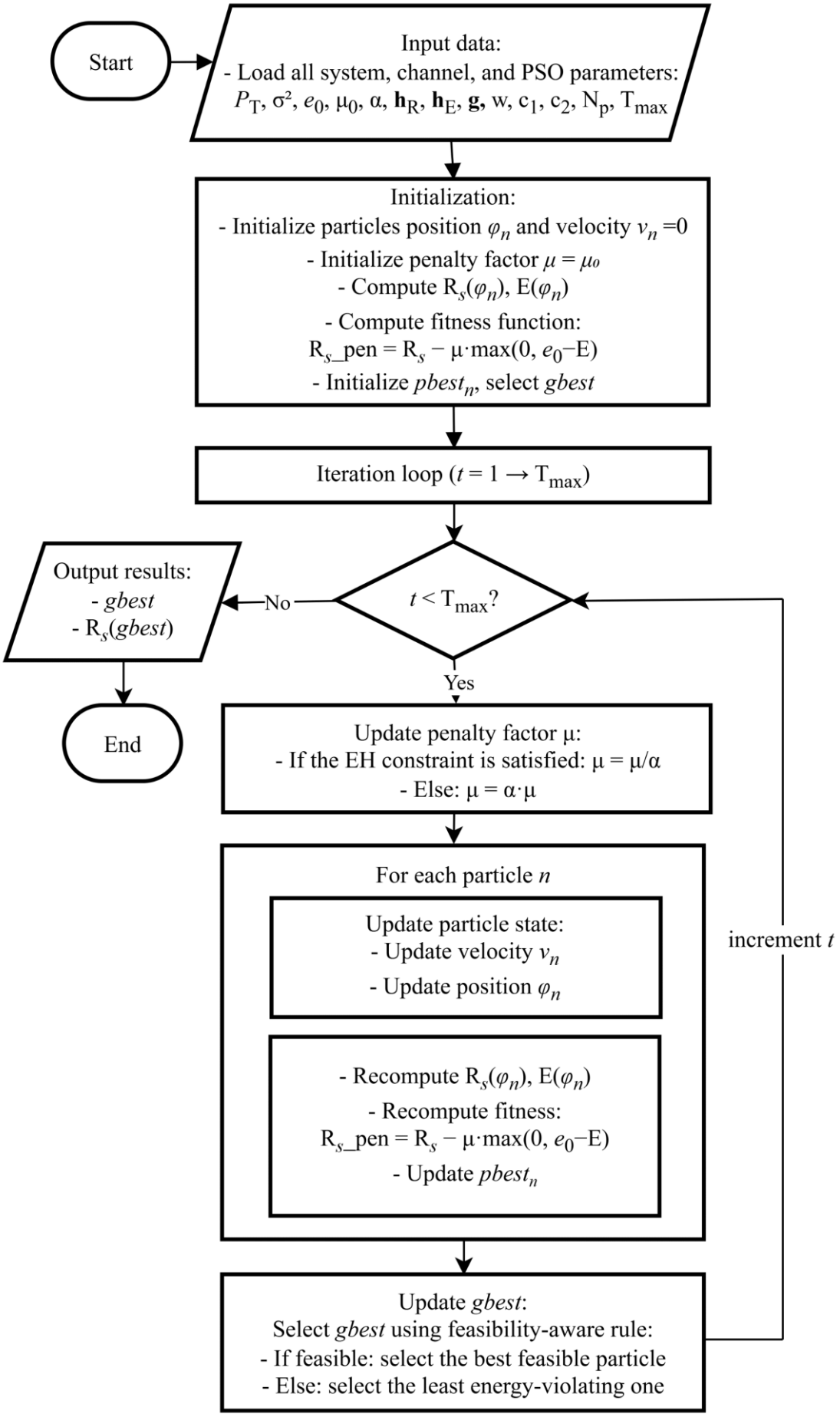

Figure 2. Flowchart of adaptive PSO with penalty function for SWIPT secrecy rate optimization.

Table 1. Proposed algorithm description

Step 1:	**Input data**
	Load all system, channel, and PSO parameters: P_T, σ_E^2, σ_R^2, δ_R^2, e_0, $\mathbf{h}_R$, $\mathbf{h}_E$, $\mathbf{g}$, w, c_1, c_2, N_p, T_{max}, μ_0, α.
Step 2:	**Initialization**
	For each particle n:
	Initialize random particle phase (position) $\varphi_n \in [0, 2\pi)$ and velocity $v_n = 0$
	Set penalty factor: $\mu = \mu_0$
	Compute secrecy rate: $R_s(\varphi_n)$
	Compute harvested energy: $E(\varphi_n)$
	Compute penalty violation: $\Delta(\varphi_n) = \max(0, e_0 - E(\varphi_n))$
	Compute penalized objective function (fitness function): $R_{s\_pen}(\varphi_n) = R_s(\varphi_n) - \mu\Delta(\varphi_n)$
	Initialize personal best: Set $pbest_n = \varphi_n$
	Select the global best $gbest$:
	If any feasible particle exists, choose one with highest R_s
	Else, choose particle with smallest violation $(e_0 - E)$
Step 3:	**Iterative optimization** ($t = 1, ..., T_{max}$)
	Update penalty factor:
	If any particle violates EH constraint: $\mu = \alpha\mu$
	Else if all particles feasible for k consecutive iterations: $\mu = \mu / \alpha$
	Update particle: for each particle n:
	Update velocity: $v_n^{(t+1)} = \omega v_n^{(t)} + c_1 r_1 (pbest_n - \varphi_n^{(t)}) + c_2 r_2 (gbest - \varphi_n^{(t)})$
	Update position: $\varphi_n^{(t+1)} = \varphi_n^{(t)} + v_n^{(t+1)}$
	Recompute: $R_s(\varphi_n)$, $E(\varphi_n)$, $\Delta(\varphi_n)$
	Recompute fitness: $R_{s\_pen}(\varphi_n)$
	Update personal best $pbest_n$:
	If $R_{s\_pen}(\varphi_n) > R_{s\_pen}(pbest_n)$ then update $pbest_n$
	Update global best $gbest$**:**
	Let F be the set of feasible particles $(E \geq e_0)$, I be the infeasible ones.
	If $F \neq \varnothing$: $gbest = \arg\left(\max_{\varphi_n \in F} R_s(\varphi_n) \right)$
	Else (all particles are infeasible): $gbest = \arg\left(\min_{\varphi_n \in I} (e_0 - E(\varphi_n)) \right)$.
Step 4:	**Output**
	Return optimal phase vector, $gbest$, and maximum secrecy rate achieved, $R_s(gbest)$.

4. NUMERICAL EXPERIMENTS

This section presents the numerical simulations of penalty-based adaptive PSO iterative method for maximizing the secrecy rate. As in (Wu & Zhang, 2020; Wei et al., 2024), a considered network communicates on a carrier with frequency 750 MHz and the bandwidth of 1 MHz. In addition, the BS and IRS are located at (0, 0) and (4, 3) meters, respectively. The legitimate receiver and the eavesdropper are placed at (7.5, 0) and (8.5, 0) meters, respectively. The transmission channels include small-scale multipath fading modeled by a Rayleigh distribution and log-normal path attenuation. The distance-dependent pathloss for every channels is expressed as $PL(d) = (-30 - 10\xi \log_{10}(d))$ dB where the pathloss with reference distance 1m is -30dB, d indicates a channel distance, and ξ indicates a pathloss exponent. The pathloss exponents for both Tx–IRS and IRS–Rx links are set to 2.2.

In experiments, the PS ratio is fixed to $\rho_R = 0.5$, i.e., half of the received power is used for information decoding and the remaining part is allocated to energy harvesting. The transmit power is set to $P_T = 37\,\text{dBW}$. The noise powers of the Eve and the PS receiver are $\sigma_E^2 = -60.22\,\text{dBm}$, $\sigma_R^2 = -60.22\,\text{dBm}$, and $\delta_R^2 = -40\,\text{dBm}$, respectively, while the required harvested-energy threshold is $e_0 = -20\,\text{dBm}$. For the proposed penalty-based adaptive PSO, the inertia weight is chosen as $w = 0.7$ to balance exploration and exploitation, and the cognitive and social acceleration coefficients are set symmetrically to $c_1 = c_2 = 1.6$. The swarm size is $N_p = 30$ particles and the maximum number of iterations is $T_{\max} = 200$, which is sufficient to observe convergence in the considered scenarios. The penalty mechanism is initialized with $\mu_0 = 5$ and adaptively adjusted using the multiplicative factor $\alpha = 1.01$ according to the constraint satisfaction status during the search process.

Fig. 3 illustrates the behavior of the proposed penalty-based adaptive PSO algorithm for optimizing the secrecy rate in a secure IRS-aided system with SWIPT, single user, and single external eavesdropper in several random channel cases. As observed in fig. 3, the values of secrecy rate in the considered cases increase sharply in a few tens of iterations, and then gradually increase until around the 100th iteration and converge after the 120th iteration. After that, fig. 3 presents the secrecy rate results until the 200th iteration without change. Therefore, these results show the fast convergence and achieve the near-optimal points effectively.

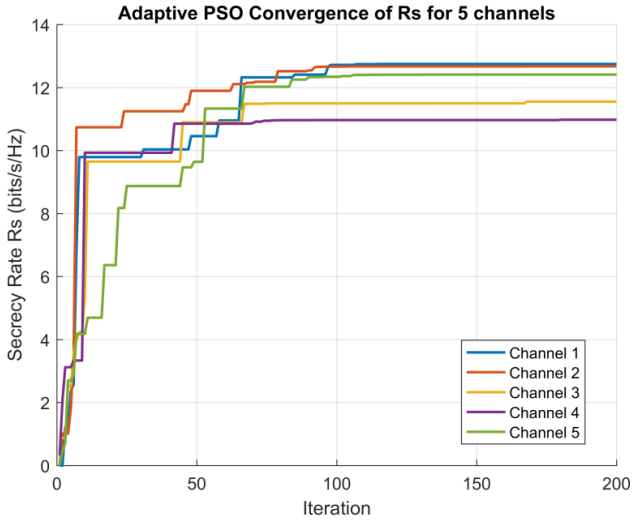

Figure 3. Adaptive PSO convergence.

Fig. 4 illustrates the average secrecy rate versus the EH threshold of the receiver over 200 iterations under 100 channel realizations, $P_T = 37\,\text{dBW}$, and $N = 20$. We observe that the secrecy rate values increase rapidly and converge to 11.576, 11.511, and 11.240 bits/s/Hz according to the three EH cases of -25 dBm, -21 dBm, and -20 dBm, respectively. We obtain a lower secrecy rate value with a higher EH value since the IRS phase shift is optimized with priority given to satisfying a high EH constraint and then maximizing the secrecy rate value.

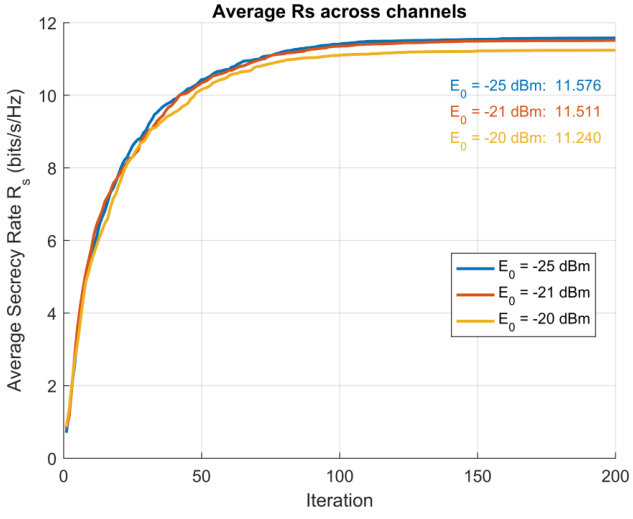

Figure 4. Secrecy rate versus EH threshold, e_0.

Fig. 5a depicts the convergence behavior of the average secrecy rate R_s in an IRS-aided secure communication system for different numbers of IRS reflecting elements N. As the iterations progress, the secrecy rate increases and eventually converges, demonstrating the effectiveness and stability of the proposed adaptive penalty-based PSO algorithm. It is observed that a larger number of IRS elements leads to a higher achievable average secrecy rate. Specifically, the secrecy performance improves monotonically as N increases from 10 to 40. This gain stems from the enhanced passive beamforming capability provided by more IRS elements, which strengthens the legitimate link while suppressing information leakage to the eavesdropper. For all considered values of N, the secrecy rate rises rapidly during the initial iterations and then gradually saturates.

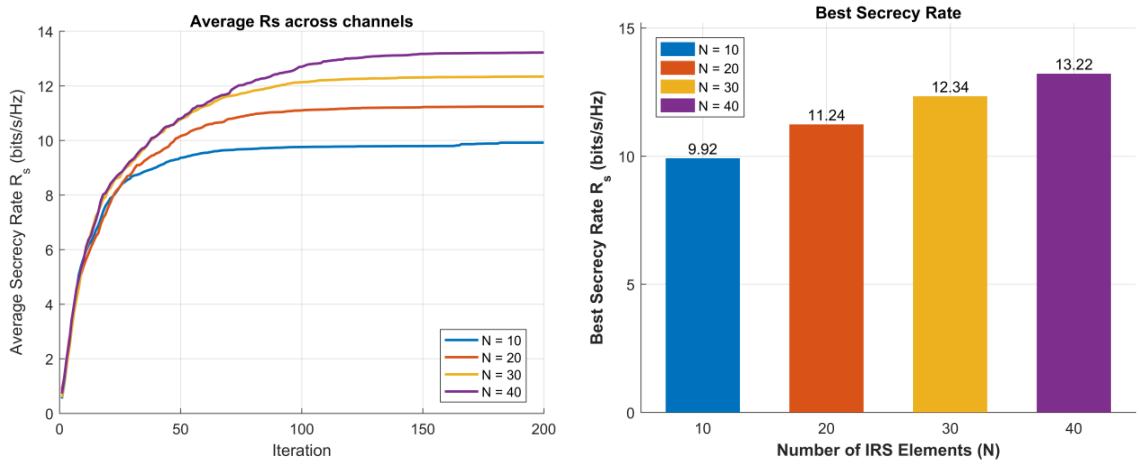

Figure 5. **(a)** Secrecy rate versus IRS element number, N. **(b)** Convergent values, R_s.

Fig. 5b shows the converged values of the secrecy rate versus the IRS element number in a bar plot. At convergence, the system with $N = 40$ achieves the highest secrecy rate, followed by $N = 30, 20$ and $N = 10$. The increasing performance gap at higher N highlights the critical role of IRS size in achieving substantial secrecy enhancements. The results confirm that deploying a larger IRS significantly improves physical-layer security by providing additional degrees of freedom to intelligently reflect signals, thereby improving signal quality at the legitimate receiver while mitigating eavesdropping threats.

Fig. 6 illustrates the convergence behavior of the average secrecy rate versus the number of iterations for two optimization schemes: the conventional PSO and the proposed adaptive PSO with a penalty function. The system parameters are $P_T = 37\,\text{dBW}$ and $N = 40$. As the iterations increase, the secrecy rate achieved by both algorithms improves rapidly in the early stages and then gradually saturates, indicating convergence. The proposed adaptive PSO consistently outperforms the conventional PSO across almost all iterations, achieving a higher secrecy rate, $R_s = 13.18\,\text{bits/s/Hz}$ compared to $R_s = 12.41\,\text{bits/s/Hz}$ that of the conventional scheme. In particular, while both methods exhibit similar initial trends, the adaptive PSO attains a larger steady-state secrecy rate, demonstrating its enhanced capability in exploring and exploiting the search space. This result confirms the effectiveness of the adaptive mechanism and penalty function in improving the optimization performance compared to the conventional PSO approach.

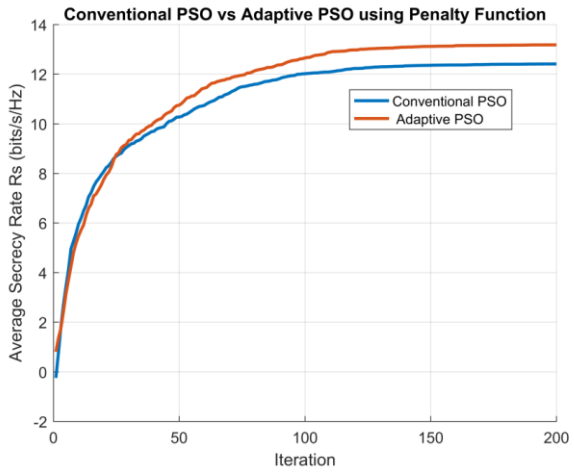

Figure 6. Conventional PSO versus adaptive PSO.

5. CONCLUSION

This work investigated the secure SWIPT system with IRS support and the presence of an eavesdropper. The legitimate power-splitting receiver performs a balanced power split for data decoding and energy harvesting. The objective of secrecy rate optimization is achieved by the proposed iterative algorithm, which is combined with the penalty technique and the adaptive PSO method. The computational evaluations show that the proposed solution procedure exhibits rapid convergence behavior under several channel realizations. Moreover, the secrecy rate is improved with the increase of transmission power or the decrease of EH threshold. Lastly, the multiple receivers and multiple eavesdroppers along with multiple antennas at the transmitter will be considered for future research directions.

Acknowledgments

This research is funded by University of Education, Hue University under grant number NCTB-T.24-TN.103.02.

REFERENCES

Abualigah, L. (2025). Particle swarm optimization: Advances, applications, and experimental insights. *Computers, Materials & Continua*, *82*(2), 1539.

Fotock, R. K., Zappone, A., & Di Renzo, M. (2024). Secrecy energy efficiency maximization in RIS-aided wireless networks. In *ICC 2024 – IEEE International Conference on Communications* (pp. 3065–3070).

Guo, M., Lin, Z., Ma, R., An, K., Li, D., Al-Dhahir, N., & Wang, J. (2024). Inspiring physical layer security with RIS: Principles, applications, and challenges. *IEEE Open Journal of the Communications Society, 5*, 2903–2925.

Hao, W., Li, J., Sun, G., Huang, C., Zeng, M., Dobre, O. A., & Yuen, C. (2024). Robust security energy efficiency optimization for RIS-aided cell-free networks with multiple eavesdroppers. *IEEE Transactions on Communications, 72*(12), 7401–7416.

Kaur, R., Bansal, B., Majhi, S., Jain, S., Huang, C., & Yuen, C. (2024). A survey on reconfigurable intelligent surface for physical layer security of next-generation wireless communications. *IEEE Open Journal of Vehicular Technology, 5*, 172–199.

Kennedy, J., & Eberhart, R. C. (1995). Particle swarm optimization. In *Proceedings of ICNN'95 – International Conference on Neural Networks* (Vol. 4, pp. 1942–1948).

Liu, Y., Liu, X., Mu, X., Hou, T., Xu, J., Di Renzo, M., & Al-Dhahir, N. (2021). Reconfigurable intelligent surfaces: Principles and opportunities. *IEEE Communications Surveys & Tutorials, 23*(3), 1546–1577.

Mir, U., Abbasi, U., Mir, T., & Pullisani, S. (2025). Intelligent reflecting surface-assisted cognitive radio networks: Recent trends, usages, challenges, and future directions. *IEEE Open Journal of the Communications Society*, *6*, 5030–5049.

Niu, H., Chu, Z., Zhou, F., Zhu, Z., Zhen, L., & Wong, K. K. (2021). Robust design for intelligent reflecting surface-assisted secrecy SWIPT network. *IEEE Transactions on Wireless Communications, 21*(6), 4133–4149.

Perera, T. D. P., Jayakody, D. N. K., Sharma, S. K., Chatzinotas, S., & Li, J. (2018). Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges. *IEEE Communications Surveys & Tutorials, 20*(1), 264–302.

Psomas, C., Ntougias, K., Shanin, N., Xu, D., Mayer, K., Tran, N. M., ... & Krikidis, I. (2024). Wireless information and energy transfer in the era of 6G communications. *Proceedings of the IEEE, 112*(7), 764–804.

Sarhan, A. Y., Abdullah, O. A., Al-Hraishawi, H., & Alsubaei, F. S. (2025). Reinforcement learning-driven secrecy energy efficiency maximization in RIS-enabled communication systems. *IEEE Access, 13*, 128048–128059.

Tang, J., Peng, Z., So, D. K. C., Zhang, X., Wong, K. K., & Chambers, J. A. (2023). Energy efficiency optimization for a multiuser IRS-aided MISO system with SWIPT. *IEEE Transactions on Communications, 71*(10), 5950–5962.

Wang, Z., Liu, L., & Cui, S. (2020). Channel estimation for intelligent reflecting surface assisted multiuser communications: Framework, algorithms, and analysis. *IEEE Transactions on Wireless Communications*, *19*(10), 6607–6620.

Wei, Y., Peng, Z., Tang, J., Zhang, X., Wong, K. K., & Chambers, J. A. (2024). Max-min fair beamforming design for a RIS-assisted system with SWIPT. *IEEE Transactions on Vehicular Technology, 73*(8), 12148–12153.

Wu, Q., & Zhang, R. (2020). Joint active and passive beamforming optimization for intelligent reflecting surface assisted SWIPT under QoS constraints. *IEEE Journal on Selected Areas in Communications, 38*(8), 1735–1748.

Khai thác các phương pháp hàm phạt và tối ưu bầy đàn thích nghi cho tối đa hóa tốc độ bảo mật trong hệ thống SWIPT được hỗ trợ bởi IRS

Nguyễn Lê Trung Thành, Hoàng Trọng Đức, Lê Phan Quốc Hưng, Phạm Việt Tuấn

Trường Đại học Sư phạm, Đại học Huế

THÔNG TIN BÀI BÁO

Quá trình xử lý:
Ngày nhận bài: 22/12/2025
Ngày nhận bản chỉnh sửa: 13/3/2026
Ngày nhận đăng: 16/3/2026
Ngày xuất bản: 20/4/2026

Từ khóa:
Bề mặt phản xạ thông minh;
Truyền đồng thời thông tin và năng lượng;
Chia công suất;
Tối đa tốc độ bảo mật;
Tối ưu bầy đàn thích nghi.

Tác giả liên hệ:
Phạm Việt Tuấn
Địa chỉ e-mail:
phamviettuan@dhsphue.edu.vn

TÓM TẮT

Trong bài báo này, bảo mật lớp vật lý của hệ thống truyền đồng thời thông tin và năng lượng (SWIPT) với sự hỗ trợ của bề mặt phản xạ thông minh (IRS) được nghiên cứu với sự hiện diện của một máy nghe lén (Eve). Mục tiêu là tối đa tốc độ bảo mật đồng thời đạt được ngưỡng thu hoạch năng lượng tại máy thu chia công suất. Nhờ tối ưu độ dịch pha tại IRS, tín hiệu được nâng cao tại máy thu trong khi giảm xuống tại Eve. Phương pháp giải theo kỹ thuật hàm phạt và tối ưu bầy đàn (PSO) thích nghi được đề xuất và thực hiện qua các mô phỏng số. Cuối cùng, chúng tôi trình bày các tác động của các thông số hệ thống như công suất phát và ngưỡng thu hoạch năng lượng và hướng nghiên cứu tiếp theo.