Hybrid Resource Allocation Scheme in Secure Intelligent Reflecting Surface-Assisted IoT

Yumeng Su, Hongyuan Gao[*] and Shibo Zhang
College of Information and Communication Engineering, Harbin Engineering University
Harbin, 150001, China
[e-mail: suyumeng1994@126.com, gaohongyuan@hrbeu.edu.cn, liangziyanhua@126.com]
*Corresponding author: Hongyuan Gao

Received July 9, 2022; revised August 19, 2022; accepted August 25, 2022; published October 31, 2022

Abstract

With the rapid development of information and communications technology, the construction of efficient, reliable, and safe Internet of Things (IoT) is an inevitable trend in order to meet high-quality demands for the forthcoming 6G communications. In this paper, we study a secure intelligent reflecting surface (IRS)-assisted IoT system where malicious eavesdropper trying to sniff out the desired information from the transmission links between the IRS and legitimate IoT devices. We discuss the system overall performance and propose a hybrid resource allocation scheme for maximizing the secrecy capacity and secrecy energy efficiency. In order to achieve the trade-off between transmission reliability, communication security, and energy efficiency, we develop a quantum-inspired marine predator algorithm (QMPA) for realizing rational configuration of system resources and prevent from eavesdropping. Simulation results demonstrate the superiority of the QMPA over other strategies. It is also indicated that proper IRS deployment and power allocation are beneficial for the enhancement of system overall capacity.

Keywords: Internet of Things, secure communications, intelligent reflecting surface, hybrid resource allocation, QMPA

This work was supported by the Ph.D. Student Research and Innovation Fund of the Fundamental Research Funds for the Central Universities (3072021GIP0803), Heilongjiang Province Key Laboratory Fund of High Accuracy Satellite Navigation and Marine Application Laboratory (Grant No. HKL-2020-Y01), the National Natural Science Foundation of China (No. 61571149), the Initiation fund for postdoctoral research in Heilongjiang Province (Grant No.LBH-Q19098), and Key Laboratory of Advanced Marine Communication and InformationTechnology, Ministry of Industry and Information Technology.

http://doi.org/10.3837/tiis.2022.10.003 **ISSN : 1976-7277**

1. Introduction

Internet of Things (IoT) is a promising technology that can provide more information exchange opportunities for ubiquitous devices to realize intelligent identification, location, tracking, and supervision [1, 2]. However, with the influx of large number of smart devices in the age of information, the ever-increasing demand of data computing and remote information processing has resulted in the serious problems such as high operation cost, heavy burden, and uneven coverage of the existing IoT systems [3-5]. Especially for cell-edge devices, the quality of service is even worse [6]. As such, carrying out innovative researches on finding low hardware cost and efficient solutions is essential to promote the sustainable development of IoT.

Intelligent reflecting surface (IRS) is an emerging solution that can overcome the above limitations, which has attracted considerable attention from both the industry and academia [7-10]. IRS is a planar array composed of a large number of passive reflecting elements connected to a central controller through a specific control link [11]. The central controller can decide and adjust the phase shift of each elements of the IRS, and these decision results constitute the phase shift matrix [12]. On this basis, the propagation channel can be manipulated into a favorable shape, thus altering the reflected transmission gain and improving the experience of desired terminals [13]. As a means of cooperative communication, IRS can reflect the received signals as a passive array without additional energy supplement, which is regarded as an eco-friendly way to improve the data transmission capacity and energy efficiency.

The initial studies on IRS mainly focus on its implementation and performance analysis. The impact of centralized and distributed deployment of IRS on the system performance is first discussed in [14], and the capacity per reflecting element is expected to converage to a constant with an infinitely large IRS. In [15], the achievable rate of downlink IRS system is analyzed under the condition of limited IRS control links and the average symbol error rate is derived. Later, some effort has made on the IRS application of different communication scenarios. The ergodic capacity and approximate outage probability of the IRS-aided single-input single-output (SISO) system is analyzed in [16], and the performance of the general condition of multi-antenna transmitter and receiver is studied in [12]. As indicated in recent studies on IRS-aided systems, a proper phase shift matrix design is beneficial for improving the overall performance [17]. Discrete phase shift set is usually adopted by the IRS due to the hardware limitation. In [18] and [19], a quantization approach is presented for extracting discrete phase-shifts out of the optimized solution of the continuous ones. In order to alleviate the adverse impact of quantization error and reduce the implementation complexity, an alternate optimization mechanism for beamforming vector and phase-shift optimization is proposed in [20] to enhance the IRS gain and thus improve the system capacity.

Although existing researches have made certain improvements on the reliability of IRS-aided systems, there are still some limitations. Since the development of the emerging IRS technology is in its infancy, many aspects such as the corresponding communication network design, and system resources management need to be further explored. As for the resource management schemes mentioned in [9, 11, 12, 15-20], these methods, however, are only suitable for convex optimization problems, while the resource management of IRS is actually a typical non-convex optimization problem, which is NP-hard. When there exist large number of reflecting elements, these methods are difficult to find the best resource allocation solution. Moreover, most of them are only for a specific resource allocation, without comprehensively considering the joint impact of multiple resources on the system performance, which is prone to waste of resources. In addition, the network structure involved in the above studies most consider generalized communication scenarios, and it is hard to overcome the challenge of long-distance transmission, and wiretap attacks in practical systems. Due to the openness and sharing properties of wireless channels, wireless communication technology enables more and more devices connect to the Internet easily, but also provides convenience for malicious eavesdroppers [21-23]. Like reliability, security is also a critical concern for evaluating the quality of service (QoS) in future 6G communications [24]. Nowadays, though some effort has made on the IRS application of different communication scenarios, there is little research on the security issue of IRS networks, especiall for the energy efficiency and communication security performance.

In order to address the above limitations, we develop a secure IRS-assisted IoT network with the presence of passive eavesdropper and investigate secure and efficient transmisison issues to achieve a better overall performance of the IoT system. Since the information received at the IoT receiver are superposed from both the direct link (IoT transmitter) and reflected link (IRS) and the passive eavesdropper tries to extract the desired information from the IoT transmission process, we propose a hybrid resource allocation scheme including phase-shift matrix and transmit power management to optimize the transmission quality and security performance. A quantum-inspired marine predator algorithm (QMPA) is designed to adaptly adjust the management of system resources. Regarding on the problem of low energy efficiency for long-distance transmission in most current studies, our proposed QMPA-based solution can overcome this difficulty and save the hardware resources, which is capable to improve the QoS of IoT communication systems. The main contributions of our work are summarized as follows:

- A secure intelligent reflecting surface-assisted IoT framework is proposed under a practical situation that malicious eavesdropper may monitor the information transmission between IoT devices. The hybrid resource allocation scheme is developed to promote reliable, safe, and efficient transmission of IoT systems.
- Two important concerns of transmission efficiency and security are investigated in the secure IRS-assisted IoT network. Exact expressions of secrecy capacity and secrecy energy efficiency are formulated to evaluate the reliability and security performance of the secure IRS-assisted IoT system.
- A quantum-inspired marine predator algorithm is developed to achieve the rational hybrid resource allocation of the secure IRS-assisted IoT network. Theoretical analysis is conducted and simulation results highlight the efficiency and strong stability of QMPA over other benchmark strategies in different conditions.

The remaining sections of our work are systemized as follows. Section 2 presents the system model and shows the analysis of secrecy capacity and secrecy energy efficiency. Section 3 introduces the principle of the proposed QMPA and its implementation process for hybrid resource allocation in the secure IRS-assisted IoT network. Section 4 and Section 5 show the simulation results and conclude this paper, respectively.

2. System Model and Analysis

2.1 System Model

We investigate a secure IRS-assisted IoT communication system where an IRS is employed to assist in the communication between the IoT transmitter and receiver, while reducing the information leakage by the passive eavesdropper as shown in **Fig. 1**. Considering most of the actual communication scenarios, the IoT transmitter, IoT receiver, and the eavesdropper are single-antenna devices. The IRS is composed of K passive reflecting elements and each element is capable to rescatter the received signal through an individual phase shift, which is adjusted by the central controller [12]. To be specific, the central controller is capable to modify the phase shifts of all reflecting elements in real-time, thus changing the wireless channel between the legitimate devices to be more favorable for their communications. With the help of IRS, the superposition of reflected signals and other path signals can boost the transmission gain at the IoT receiver and suppress the power received at unintended devices (i.e., the passive eavesdropper), which is beneficial for suppressing the cross-interference and improving the transmission quality and security.

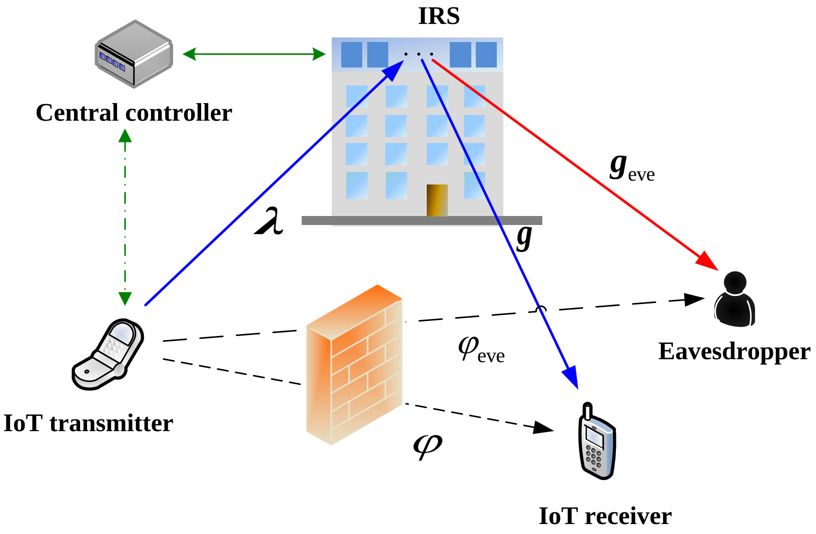

Fig. 1. A secure IRS-assisted IoT communication system

Regarding on the propagation, we adopt quasi-static flat-fading channels as in [25]. To characterize the theoretical performance of the secure IRS-assisted IoT, we assume that the channel state information (CSI) is available for all devices and the CSI remains approximately constant in one time slot [11, 12, 25]. $\boldsymbol{\lambda} \in \mathbb{C}^{K\times 1}$ and $\boldsymbol{g} \in \mathbb{C}^{1\times K}$ are CSI vectors from the IoT transmitter to the IRS and from the IRS to the IoT receiver, respectively. φ is the CSI from the IoT transmitter to its receiver. $\boldsymbol{g}_{\text{eve}} \in \mathbb{C}^{1\times K}$ is the CSI vector from the IRS to the eavesdropper and φ_{eve} is the CSI from the IoT transmitter to the eavesdropper. Since IRS is usually located in a position with line-of-sight (LoS) to all devices, $\boldsymbol{\lambda}$, $\boldsymbol{g}$, and $\boldsymbol{g}_{\text{eve}}$ are adopted by Rician fading model. For non-line-of-sight (NLoS) paths from the IoT transmitter to the IoT receiver and eavesdropper, φ and φ_{eve} are modeled by Rayleigh fading. For LoS link, the CSI from the

IoT transmitter to the IRS can be expressed as $\boldsymbol{\lambda}=\beta_{\mathrm{TI}}\left(\sqrt{\frac{L_{\mathrm{TI}}}{L_{\mathrm{TI}}+1}}\bar{\boldsymbol{\lambda}}+\sqrt{\frac{1}{L_{\mathrm{TI}}+1}}\hat{\boldsymbol{\lambda}}\right)$, where β_{TI} denotes the distance-dependent path loss from the IoT transmitter to the IRS, $L_{\mathrm{TI}}\in[0,\infty)$ is the Rician factor, $\bar{\boldsymbol{\lambda}}$ and $\hat{\boldsymbol{\lambda}}$ indicate the LoS component and the NLoS component. Accordingly, $\boldsymbol{g}$ and $\boldsymbol{g}_{\mathrm{eve}}$ can be modeled in a similar way with Rician factors L_{IR} and L_{IE}, respectively. For NLoS link, the CSI from the IoT transmitter to the IoT receiver is $\varphi=\beta_{\mathrm{TR}}\hat{\varphi}$, where β_{TR} denotes the distance-dependent path loss between the two devices, and $\hat{\varphi}\sim CN(0,1)$. φ_{eve} is also modeled in a similar way as φ.

Let x denote the transmitted signal of the IoT transmitter. We consider a normalized energy constraint as $\mathrm{E}\{\|x\|^2=1\}$. For downlink transmission, the signal received at the IRS is given by

$$\boldsymbol{y}_{\mathrm{IRS}}=\sqrt{P}\cdot\boldsymbol{\lambda}\cdot x+\boldsymbol{n} \tag{1}$$

where P is the power of the IoT transmitter, $\boldsymbol{n}$ is the complex white Gaussian noise vector at the IRS.

We define a $K\times K$ -dimensional matrix $\boldsymbol{\delta}=\sqrt{\eta}\mathrm{diag}\{\delta_1,\delta_2,...,\delta_K\}$ to determine the reflection matrix of the IRS, where η is the reflection efficiency, $\delta_k=e^{j\cdot\alpha_k}$, and $\alpha_k\in[0,2\pi)$ denotes the phase shift of the k-th reflecting element, $k=1,2,...,K$. The phase shift matrix of all reflecting elements at the IRS is $\boldsymbol{\alpha}=[\alpha_1,\alpha_2,...,\alpha_K]$. After phase shift adjustment and the reflection of IRS, the signal received by the IoT receiver can be expressed as

$$\bar{y}_{\mathrm{rec}}=\sqrt{P}\cdot(\boldsymbol{g}\cdot\boldsymbol{\delta}\cdot\boldsymbol{\lambda}+\varphi)\cdot x+(\boldsymbol{g}\cdot\boldsymbol{\delta})\cdot\boldsymbol{n}+w \tag{2}$$

where w is the white Gaussian noise at the receiver.

We consider a worst case that the eavesdropper can overhear the signals from both the IoT transmitter and the IRS, that is to say, what the eavesdropper received is a mixed signal. Similarly, the signal received at the eavesdropper is given by

$$\bar{y}'_{\mathrm{eve}}=\sqrt{P}\cdot(\boldsymbol{g}_{\mathrm{eve}}\cdot\boldsymbol{\delta}\cdot\boldsymbol{\lambda}+\varphi_{\mathrm{eve}})\cdot x+(\boldsymbol{g}_{\mathrm{eve}}\cdot\boldsymbol{\delta})\cdot\boldsymbol{n}+w_{\mathrm{eve}} \tag{3}$$

For the convenience of calculation, we assume the power of white Gaussian noise at the IoT receiver and the eavesdropper is N_0, and the power of the complex white Gaussian noise vector at the IRS is $\bar{N}$. Hence, the signal-to-interference-plus-noise ratio (SINR) at the IoT receiver and the eavesdropper can be calculated by

$$\gamma=\frac{P\cdot(\boldsymbol{\lambda}^{\mathrm{H}}\cdot\boldsymbol{\delta}^{\mathrm{H}}\cdot\boldsymbol{g}^{\mathrm{H}}\cdot\boldsymbol{g}\cdot\boldsymbol{\delta}\cdot\boldsymbol{\lambda}+|\varphi|^2)}{\bar{N}\cdot(\boldsymbol{\delta}^{\mathrm{H}}\cdot\boldsymbol{g}^{\mathrm{H}}\cdot\boldsymbol{g}\cdot\boldsymbol{\delta})+N_0} \tag{4}$$

and

$$\gamma_{\mathrm{eve}}=\frac{P\cdot(\boldsymbol{\lambda}^{\mathrm{H}}\cdot\boldsymbol{\delta}^{\mathrm{H}}\cdot\boldsymbol{g}_{\mathrm{eve}}^{\mathrm{H}}\cdot\boldsymbol{g}_{\mathrm{eve}}\cdot\boldsymbol{\delta}\cdot\boldsymbol{\lambda}+|\varphi_{\mathrm{eve}}|^2)}{\bar{N}\cdot(\boldsymbol{\delta}^{\mathrm{H}}\cdot\boldsymbol{g}_{\mathrm{eve}}^{\mathrm{H}}\cdot\boldsymbol{g}_{\mathrm{eve}}\cdot\boldsymbol{\delta})+N_0} \tag{5}$$

where $(.)^{\mathrm{H}}$ indicates the conjugate transpose operation.

2.2 Security Analysis

We investigate two issues of the secure IRS-assisted IoT network, i.e, secrecy capacity and secrecy energy efficiency. The secrecy capacity indicates the difference between the transmission rate at the desired terminal (IoT receiver) and the information leakage rate by the malicious node (passive eavesdropper), which is calculated by

$$R^{\mathrm{S}} = (R - R_{\mathrm{eve}})^{+} \tag{6}$$

where $(a)^{+}$ represents $\max\{a, 0\}$, R and R_{eve} denote the transmission rate of the IoT receiver and information leakage rate by the eavesdropper, respectively. According to Shannon's theorem, we have

$$R = \log_2 \left|1 + \gamma\right| \tag{7}$$

and

$$R_{\mathrm{eve}} = \log_2 \left|1 + \gamma_{\mathrm{eve}}\right| \tag{8}$$

The secrecy energy efficiency is defined as the ratio of the secrecy capacity to the total power consumption [26-28], which is expressed as

$$\rho^{\mathrm{S}} = \frac{R^{\mathrm{S}}}{P_{\Sigma}} = \frac{\left(\log_2 \left|1+\gamma\right| - \log_2 \left|1+\gamma_{\mathrm{eve}}\right|\right)^{+}}{P + \overline{P}} \tag{9}$$

where $\overline{P}$ is the total operating power consumed by the IRS and the central controller.

2.3 Problem Formulation

In this paper, we aim to optimize the transmission quality and security performance of the secure IRS-assisted IoT system by jointly adjust the transmit power and phase-shift matrix through a hybrid resource allocation scheme. For the hybrid resource allocation of secrecy capacity maximization, the problem is formulated as

$$\begin{aligned} (\mathrm{P1}):\quad & \max R^{\mathrm{S}}(P, \boldsymbol{\alpha}) = \max (R - R_{\mathrm{eve}})^{+} \\ & \text{s.t.}\quad P \in (0,\ P_{\max}] \\ & \qquad\ \ \alpha_k \in [0, 2\pi), \quad k = 1, 2, \ldots, K \end{aligned} \tag{10}$$

where $P_{\max}$ is the maximum transmit power allowed by the IoT transmitter.

The problem of hybrid resource allocation for maximizing the secrecy energy efficiency of the secure IRS-assisted IoT system is given in the following formula:

$$\begin{aligned} (\mathrm{P2}):\quad & \max \rho^{\mathrm{S}}(P, \boldsymbol{\alpha}) = \max \frac{\left(\log_2 \left|1+\gamma\right| - \log_2 \left|1+\gamma_{\mathrm{eve}}\right|\right)^{+}}{P + \overline{P}} \\ & \text{s.t.}\quad P \in (0,\ P_{\max}] \\ & \qquad\ \ \alpha_k \in [0, 2\pi), \quad k = 1, 2, \ldots, K \end{aligned} \tag{11}$$

Note that (P1) and (P2) are non-convex multi-constraint optimization problems. The interaction between multiple resources coupled with information leakage by the eavesdropper, which makes the problems more difficult to solve. Therefore, both (P1) and (P2) are NP-hard problems and difficult for traditional algorithms to find appropriate solutions. The secrecy capacity and secrecy energy efficiency, however, are non-linear correlative. Therefore, it is essential to develop an effective solution for these difficulties.

3. Hybrid Resource Allocation Scheme Based on Quantum-inspired Marine Predator Algorithm

This section discusses the principle of QMPA as a simple and efficient swarm intelligence optimization solution and the process of solving the hybrid resource allocation problem.

3.1 Quantum-inspired Marine Predator Algorithm

QMPA is a population-based method. In QMPA, the population of quantum marine predators is denoted by $\boldsymbol{U}(t)$ in the t-th iteration, which is constituted by M quantum marine predators and all quantum marine predators searching in a D-dimensional speace to look for their prey (D represents the dimension of the optimization problem, i.e., transmit power of the IoT transmitter and phase-shift matrix of the IRS). The quantum position of each quantum marine predator is composed of D quantum bits. In the t-th iteration, the quantum position of the i-th quantum marine predator is expressed by

$$\boldsymbol{q}_i^t = [q_{i,1}^t, q_{i,2}^t, ..., q_{i,D}^t] \tag{12}$$

where $0 \le q_{i,d}^t \le 1$, $i = 1,2,...,M$, $d = 1,2,...,D$. Then, the position of the i-th quantum marine predator can be obtained through the mapping rule, which is given by

$$Q_{i,d}^t = Q_d^{\min} + q_{i,d}^t \cdot (Q_d^{\max} - Q_d^{\min}) \tag{13}$$

where $Q_{i,d}^t$ denotes the d-th position of the i-th quantum marine predator, $Q_d^{\min}$ and $Q_d^{\max}$ represent the lower bound and upper bound of the d-th dimensional searching space, respectively. The position of the i-th quantum marine predator is expressed by $\boldsymbol{Q}_i^t = [Q_{i,1}^t, Q_{i,2}^t, ..., Q_{i,D}^t]$, which corresponds to a hybrid resource allocation scheme of the secure IRS-assisted IoT system.

By substituting the position into the fitness function, we can calculate the fitness value of the i-th quantum marine predators by $f(\boldsymbol{Q}_i^t)$. For the maximum optimization problem, a higher fitness value means a better performance. The quantum position of the i-th quantum marine predator with the highest fitness value until the t-th iteration is recorded as its historical optimal quantum position $\boldsymbol{u}_i^t = [u_{i,1}^t, u_{i,2}^t, ..., u_{i,D}^t]$; the quantum marine predator with the highest fitness value is defined as the elite predator of $\boldsymbol{U}(t)$, and its quantum position is recorded as global optimal quantum position $\boldsymbol{u}_{\text{best}}^t = [u_{\text{best},1}^t, u_{\text{best},2}^t, ..., u_{\text{best},D}^t]$.

The evolution process of quantum marine predators is the renewal process of quantum position. The quantum position of each quantum marine predator is updated through different quantum rotation angles in the stages of exploration, parallel predation and exploration, and predation. These stages are defined according to the rules governed by the movement of marine predators and prey. For simplicity, set $t_{\max}$ as the terminal number of iterations, τ_1 and τ_2 are thresholds for dividing different evolution stages, $\tau_1 < \tau_2$.

For the t-th iteration, if $t \le \tau_1 \cdot t_{\max}$, the quantum marine predator population conducts exploration to search for prey. The quantum rotation angle and quantum position of each quantum marine predator are generalized as

$$\theta_{i,d}^{t+1} = c_1 \cdot \omega_{i,d}^{t+1} \cdot (u_{\text{best},d}^t - q_{i,d}^t) \tag{14}$$

$$q_{i,d}^{t+1} = \text{abs}(q_{i,d}^t \cdot \cos\theta_{i,d}^{t+1} + \sqrt{1-(q_{i,d}^t)^2} \cdot \sin\theta_{i,d}^{t+1}) \tag{15}$$

where $\theta_{i,d}^{t+1}$ is the d-th quantum rotation angle of the i-th quantum marine predator, $d = 1,2,...,D$; c_1 is the impact factor that indicates the influence of elite predator on the quantum rotation angle during the exploration stage; $\omega_{i,d}^{t+1}$ is a random number that obeys standard normal distribution; and $\text{abs}(.)$ represents the absolute value function.

If $\tau_1 \cdot t_{\max} < t \le \tau_2 \cdot t_{\max}$, both predation and exploration occur in the quantum marine predator population, with the aim of searching for the area with more abundant preys while hunting. In this case, the quantum rotation angle and quantum position of each quantum marine predator are generated as

$$\theta_{i,d}^{t+1} = \begin{cases} c_2 \cdot \xi_{i,d}^{t+1} \cdot (q_{r_1,d}^t - u_{\text{best},d}^t + q_{r_2,d}^t - q_{i,d}^t), & i \in \{1,2,...,\varepsilon \cdot M\} \\ c_3 \cdot \varpi_{i,d}^{t+1} (u_{\text{best},d}^t - q_{i,d}^t) + c_4 \cdot \varsigma_{i,d}^{t+1} \cdot (u_{i,d}^t - q_{i,d}^t), & i \in \{\varepsilon \cdot M + 1, \varepsilon \cdot M + 2,...,M\} \end{cases} \tag{16}$$

$$q_{i,d}^{t+1} = \begin{cases} \text{abs}(u_{\text{best},d}^t \cdot \cos\theta_{i,d}^{t+1} + \sqrt{1-(u_{\text{best},d}^t)^2} \cdot \sin\theta_{i,d}^{t+1}), & i \in \{1,2,...,\varepsilon \cdot M\} \\ \text{abs}(q_{i,d}^t \cdot \cos\theta_{i,d}^{t+1} + \sqrt{1-(q_{i,d}^t)^2} \cdot \sin\theta_{i,d}^{t+1}), & i \in \{\varepsilon \cdot M + 1, \varepsilon \cdot M + 2,...,M\} \end{cases} \tag{17}$$

where c_2, c_3, and c_4 are impact factors, c_2 indicates the joint influence of elite predator and other quantum marine predators on the quantum rotation angle, c_3 and c_4 indicate the influence of elite predator and historical optimal quantum position on the quantum rotation angle; r_1 and r_2 are serial numbers of other quantum marine predators, $r_1 \in \{1,2,...,M\}$, $r_2 \in \{1,2,...,M\}$, $r_1 \ne i$, $r_2 \ne i$, $r_1 \ne r_2$; ε is control factor; $\xi_{i,d}^{t+1}$ and $\varsigma_{i,d}^{t+1}$ are random numbers that obey standard normal distribution; $\varpi_{i,d}^{t+1}$ is a random number that follows Levy distribution.

If $\tau_2 \cdot t_{\max} < t \le t_{\max}$, quantum marine predator population conducts predation based on the acquired prey information. The quantum rotation angle is generated as

$$\theta_{i,d}^{t+1} = c_5 \cdot \phi_{i,d}^{t+1} (u_{\text{best},d}^t - q_{i,d}^t) + c_6 \cdot \upsilon_{i,d}^{t+1} \cdot (u_{i,d}^t - q_{i,d}^t) \tag{18}$$

where c_5 and c_6 are impact factors that indicate the influence of elite predator and historical optimal quantum position on the quantum rotation angle during the predation stage, respectively; $\phi_{i,d}^{t+1}$ is a random number follows Levy distribution and $\upsilon_{i,d}^{t+1}$ is a random number that obeys standard normal distribution, respectively. The quantum position can be obtained by (15).

The updated position of each quantum marine predator can be obtained by (13). Then, the fitness value is calculated by the fitness function. Based on the memory saving rules in [29], we update the historical optimal quantum position of each quantum marine predator, the elite predator, and the corresponding global optimal quantum position of QMPA until the $(t+1)$-th iteration.

3.2 Computational complexity analysis

To evaluate the capability of the QMPA, in this part, we present the computational complexity analysis of the proposed algorithm. As shown in Section 3.1, the quantum position of each quantum marine predator is updated via the quantum rotation angles of exploration, parallel predation and exploration, and predation stages. For the t-th iteration, we first need to determine which behavior the quantum marine predator population conducts, and then update the quantum rotation angles and quantum position according to the quantum evolution rules. The computational complexity of these process is $O(2 \cdot M \cdot D + 1)$. Next, the updated quantum position of each quantum marine predator is mapped into the corresponding position, with the computational complexity of $O(M \cdot D)$. After mapping all the quantum marine predators, we calculate the fitness value by the fitness function and update the historical optimal quantum position and global optimal quantum position by the memory saving rules. The computational complexity is $O(2 \cdot M)$. Finally, we can conclude that the computational complexity of QMPA is $O(t(3 \cdot M \cdot D + 2 \cdot M + 1))$ after t iterations.

3.3 Process of QMPA-based Hybrid Resource Allocation

In this section, we present the detailed implementation process of hybrid resource allocation based on QMPA (HRA-QMPA) in a secure IRS-assisted IoT network. Based on what we have discussed in Section 2, we aim to find appropriate transmit power of IoT transmitter and phase shift of each reflecting elements to achieve the best secrecy performance. Hence, for the proposed QMPA, the dimention of searching space of the quantum marine predator is $D = K + 1$, and $Q_d^{\min} = 0 \quad \forall d$, $Q_d^{\max} = \begin{cases} P_{\max}, d = 1 \\ 2\pi, \ d = 2,3,...,K+1 \end{cases}$. As indicated in Section 3.1, the position of a quantum marine predator is corresponding to a feasible hybrid resource allocation scheme, that is, $\boldsymbol{Q}_i^t = [Q_{i,1}^t, Q_{i,2}^t, ..., Q_{i,D}^t] = [P_i^t, \alpha_{i,1}^t, \alpha_{i,2}^t, ..., \alpha_{i,K}^t]$. The central controller sends the phase shift information to the reflecting elements and the power information to the IoT transmitter. For the HRA-QMPA, (10) and (11) are considered as fitness functions for the maximization problems of secrecy capacity and secrecy energy efficiency, respectively.

The implementation steps of HRA-QMPA are summarized as follows:

Hybrid resource allocation based on QMPA

```
Input system parameters of the secure IRS-assisted IoT network;
Determine optimization problem; // select (10) or (11) for secrecy capacity or secrecy energy
    efficiency maximization, respectively;
Initialize parameter settings of QMPA and the population of quantum marine predators that
    including quantum position, the corresponding position, and historical optimal quantum position;
$t = 1$ // the first iteration;
Calculate the fitness value according to the specific optimization problem;
Obtain the elite predator and global optimal quantum position;
while $t \le t_{\max}$
if $t \le \tau_1 \cdot t_{\max}$
    Update quantum rotation angles and quantum position through exploration by (14) and (15)
else if $\tau_1 \cdot t_{\max} < t \le \tau_2 \cdot t_{\max}$
    Update quantum rotation angles and quantum position through parallel predation and
    exploration by (16) and (17)
else
    Update quantum rotation angles and quantum position through predation by (18) and (15)
end if
Obtain the position of the updated quantum marine predator by (13);
Calculate the fitness value of the updated quantum marine predators;
Accomplish memory saving and update the historical optimal quantum position, elite predator
    and global optimal quantum position;
Set $t = t + 1$ ;
end while
Obtain the hybrid resource allocation scheme according to the global optimal quantum position;
Output: The hybrid resource allocation result based on QMPA.
```

4. Simulation Results

This section investigates the capability of the proposed hybrid resource allocation scheme based on QMPA in improving the secrecy capacity and secrecy energy efficiency performance of the secure IRS-assisted IoT network. Consider a sub-6G scenario as in [16], the noise power spectrum density is -174 dBm/Hz, and the system bandwidth is 10 MHz. We assume that the IoT is located at (0, 0), and the IoT receiver, the IRS, and the eavesdropper are located at (240, 0), (120, 90), and (220, -50), respectively. As a result, we can obtain the distance between any two devices. The LoS component and the NLoS component are modeled by [12]. The path loss exponent of LoS link is set to 2.5 and the path loss exponent of NLoS link is set to 3.7. The operating power of the IRS is 0.5W. Unless specified otherwise, we set $L_{\mathrm{TI}} = L_{\mathrm{IR}} = L_{\mathrm{IE}} = L$. All results are the average of 200 Monte-Carlo simulations.

4.1 Performance Comparison of QMPA

Since there is no solution especially designed for the NP-hard problems (P1) and (P2), we adopt several benchmark schemes for comparison to verify the effectiveness of the proposed QMPA. Some classical methods including marine predator algorithm (MPA) [29], backtracking search algorithm (BSA) [30], differential evolution (DE) algorithm [31], particle swarm optimization (PSO) algorithm [32], artificial bee colony (ABC) algorithm [33], Dinkelbach algorithm [34], and half power-random resource allocation (HPRRA) scheme in [35] are applied for the hybrid resource allocation problem in the secure IRS-assisted IoT network. For the HPRRA scheme, the IoT transmitter broadcasts its signal with half the maximum allowed transmission power and the central controller randomly assigns the phase shift of each reflecting element of the IRS. For the proposed QMPA, we set $M = 10$, $t_{\max} = 500$, $\tau_1 = 0.1$, $\tau_2 = 2/3$, $c_1 = 0.2$, $c_2 = 0.25$, $c_3 = 0.3$, $c_4 = 0.1$, $c_5 = 0.3$, $c_6 = 0.1$. For each quantum marine predator, all elements of the quantum position are randomly initialized between 0 and 1. Without loss of generality and fairness, the population size and the terminal iteration number of the above strategies are set to the same value of QMPA. The other parameter settings of MPA, BSA, DE, PSO, and ABC can refer to [29], [30], [31], [32], and [33], respectively.

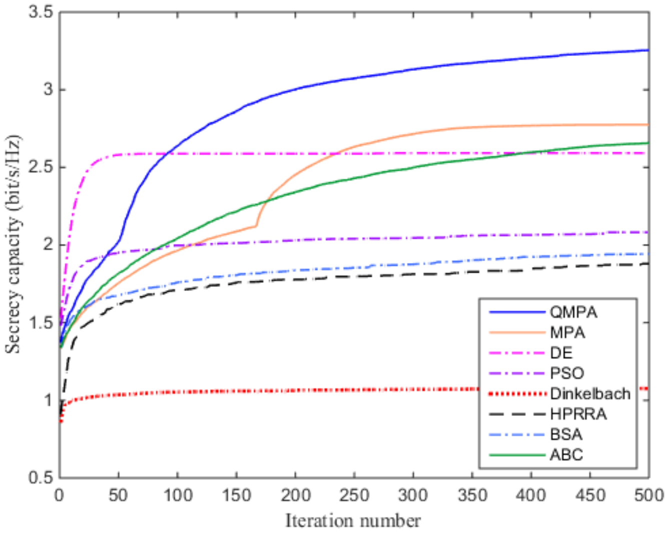

Fig. 2. Secrecy capacity versus iteration number ($K = 50$, $P_{\max} = 40\mathrm{dBm}$, $\eta = 1$, $L = 1$)

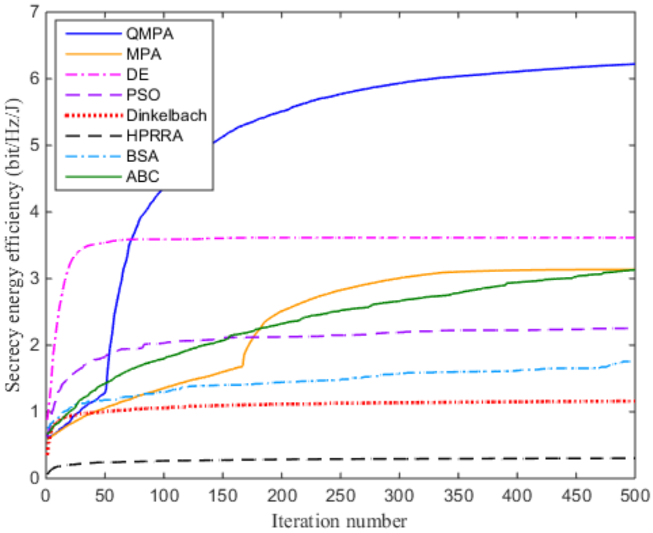

Fig. 3. Secrecy energy efficiency versus iteration number ($K = 50$, $P_{\max} = 40\text{dBm}$, $\eta = 1$, $L = 1$)

Fig. 2 and **Fig. 3** are convergence performance comparisons of the proposed QMPA and other strategies with set the number of reflecting elements $K = 50$, the maximum transmit power $P_{\max} = 40\text{dBm}$, and the reflection efficiency $\eta = 1$. We consider both LoS and NLoS components with Rician factor $L = 1$. Though some classical solutions such as PSO, DE, and Dinkelbach algorithms are widely accepted for solving engineering problems, these algorithms are easy to fall into local optimum especially for the complicated optimization problems of (P1) and (P2). From the simulation results, we can find that Dinkelbach algorithm performs the worst among all solutions for the secrecy capacity maximizaiton. The reason is that Dinkelbach algorithm is one of the methods for solving convex optimization problems, for the non-convex, NP-hard optimization problems, it is difficult to find an appropriate solution for such method. For the HPRRA scheme, though it can achieve 1.82 bit/s/Hz for the secrecy capacity performance, it performs the worst on the secrecy energy efficiency. In order to improve the convergence speed and enhance the optimization ability, our proposed QMPA combines the merits of of quantum computing. Under different quantum rotation angles, the diversity of QMPA population is increased and quantum marine predators can quickly converge to the best solution through global information sharing. Hence, QMPA can achieve the best secrecy capacity and secrecy energy efficiency performance for the hybrid resource allocation in the secure IRS-assisted IoT network. When the number of iterations reaches 500, the secrecy capacity of the QMPA-based HRA is 3.26 bit/s/Hz, which is 0.48 bit/s/Hz, 0.6 bit/s/Hz, 0.67 bit/s/Hz, 1.18 bit/s/Hz, 1.32 bit/s/Hz, 1.38 bit/s/Hz, and 2.18 bit/s/Hz higher than that of MPA, ABC, DE, PSO, BSA, HPRRA, and Dinkelbach schemes.

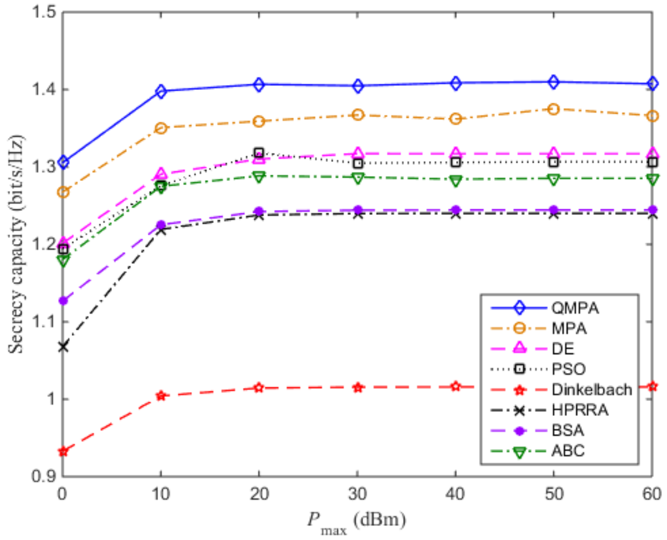

Fig. 4. Secrecy capacity versus $P_{\max}$ with $K = 20$, $\eta = 1$, $L = 1$

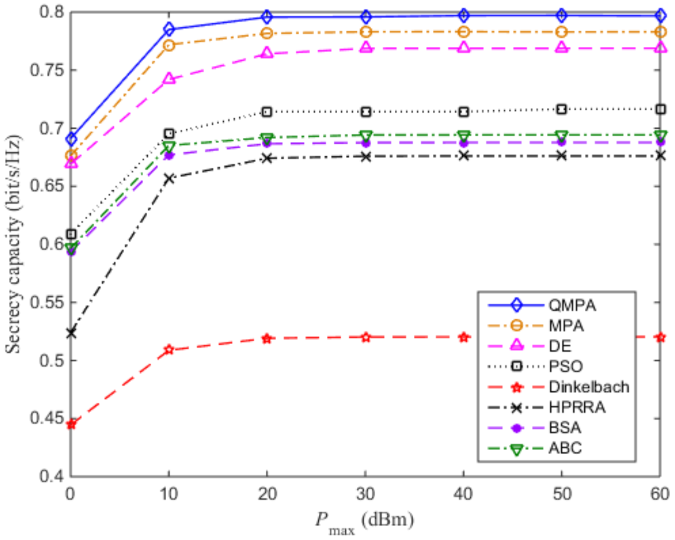

Fig. 5. Secrecy capacity versus $P_{\max}$ with $K = 20$, $\eta = 1$, $L = 0$

Fig. 4 and **Fig. 5** investigate the secrecy capacity performance with $P_{\max}$ varying from 0dBm to 60dBm in two different conditions, i.e., both LoS and NLoS components ($L = 1$), and without LoS component (only NLoS, $L = 0$). In the simulation, we assume the number of reflecting elements $K = 50$ and the reflection efficiency $\eta = 1$. The results show that the secrecy gradually increases with $P_{\max}$ at first. When $P_{\max}$ is over 20dBm, the secrecy tends to a constant value with the increase of $P_{\max}$. By comparing the results of these two figures, we can find that the presence of LoS component can boost the secrecy capacity performance of the secure IRS-assisted IoT network. For QMPA, there is a 0.61 bit/s/Hz increase on secrecy capacity with $L = 1$ compared with that of $L = 0$. The results also indicate that QMPA can achieve the best performance compared with other schemes.

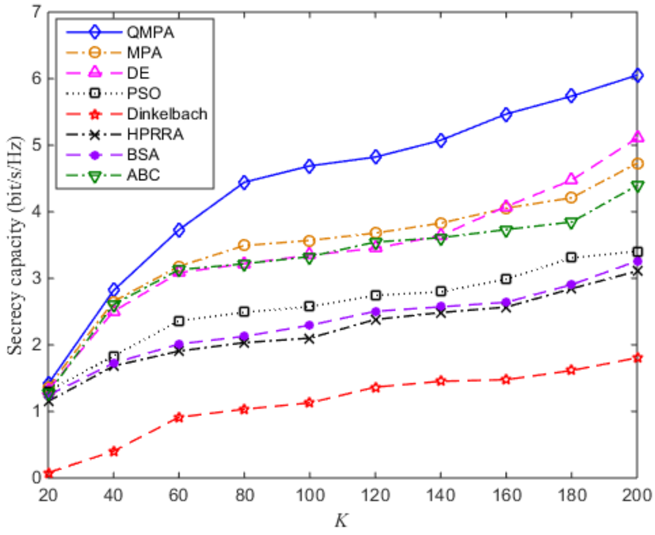

Fig. 6. Secrecy capacity versus K with $P_{\max} = 40\text{dBm}$, $\eta = 1$, $L = 1$

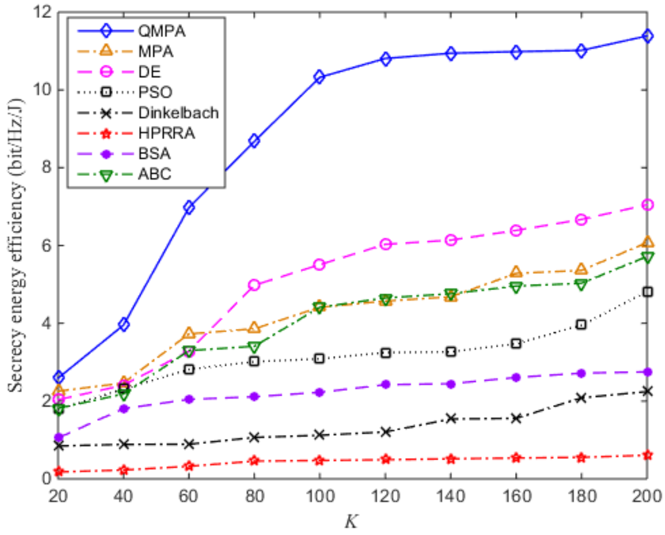

Fig. 7. Secrecy energy efficiency versus K with $P_{\max} = 40\text{dBm}$, $\eta = 1$, $L = 1$

Fig. 6 and **Fig. 7** investigate the security performance with the variation of the number of reflecting elements of the secure IRS-assisted IoT network. In the simulation, we set $P_{\max} = 40\text{dBm}$, $\eta = 1$, and $L = 1$. For both secrecy capacity and secrecy energy effiency, we observe that the performance of all scheme increases with K. It is clear that a larger number of reflecting elements is beneficial to improve the channel gain between the IRS and the destination node. Moreover, the performance of the hybrid resource allocation based on QMPA outperforms that of other schemes in any K.

4.2 Impact of Different Parameters

In this section, we discuss the impact of different system parameters on the performance of the proposed HRA-QMPA scheme.

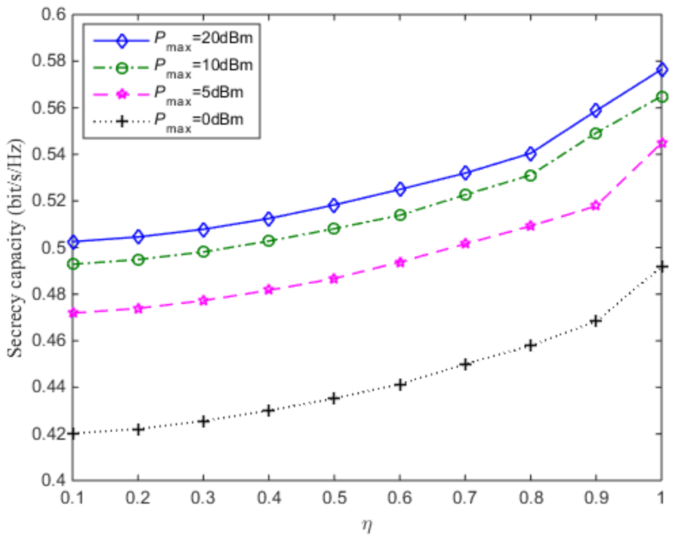

Fig. 8. Secrecy capacity comparisons under different η with $P_{\max} \in \{0,5,10,20\}$ dBm and $K=10$ ($L=1$)

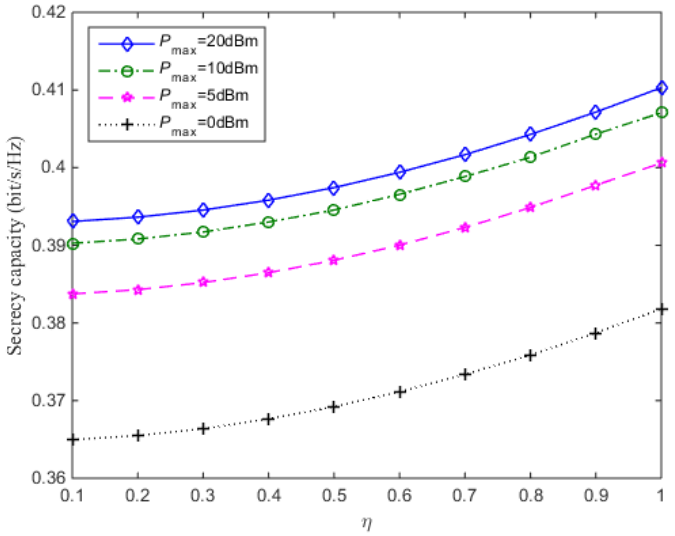

Fig. 9. Secrecy capacity comparisons under different η with $P_{\max} \in \{0,5,10,20\}$ dBm and $K=10$ ($L=0$)

Fig. 8 and **Fig. 9** investigate the impact of maximum transmit power $P_{\max}$ and reflection efficiency η on the secrecy capacity performance under two circumstances where $L=1$ and $L=0$, respectively. It is observed that both secrecy capacity and secrecy energy efficiency can be improved with a higher reflection efficiency at the IRS. Since a larger $P_{\max}$ will permit the IoT transmitter to broadcast its signal with a higher power, it is clear that the performance of the proposed HRA-QMPA increases with $P_{\max}$. The results also indicate the effect of LoS component. Take $P_{\max} = 20\text{dBm}$ as an example, when $\eta = 1$, the secrecy capacity under the condition of both LoS and NLoS components ($L = 1$) is 41.4% higher than that of only NLoS component ($L = 0$).

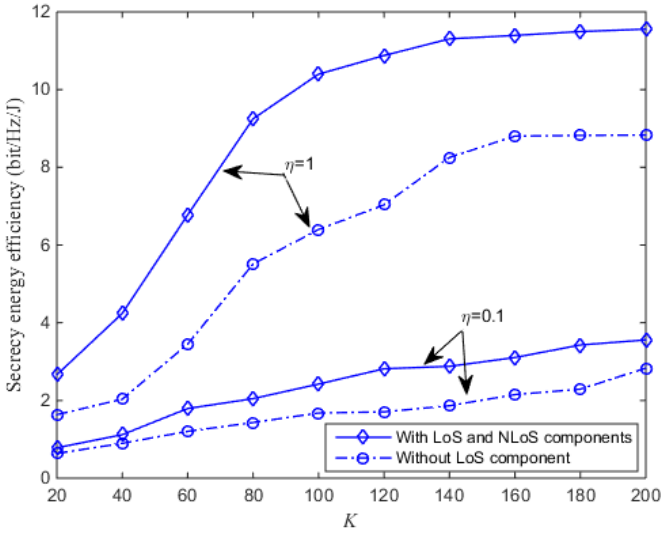

Fig. 10. Secrecy energy efficiency comparisons under different K with $P_{\max} = 20\text{dBm}$, $\eta \in \{0.1,1\}$, and $L \in \{0,1\}$

Fig. 10 investigates the secrecy energy efficiency performance under different η and channel conditions with $P_{\max} = 20\text{dBm}$ and K varying from 20 to 200. The simulation result indicates that the secrecy energy efficiency is a monotonic increasing function of K in all cases. It is clear that the transmission gain of a channel contains LoS component is superior to that only contains NLoS component. From the simulation, we also observe that a higher reflection efficiency contributes to a better performance of the secure IRS-assisted IoT network, which is consistent with **Fig. 8** and **Fig. 9**. However, in most cases, the reflection efficiency is difficult to reach 1 due to hardware limitations. Moreover, too many reflecting elements may cause a waste of system resources. Hence, a proper IRS deployment is essential to achieve the communication reliability while promoting energy conservation in practial communicatin scenarios.

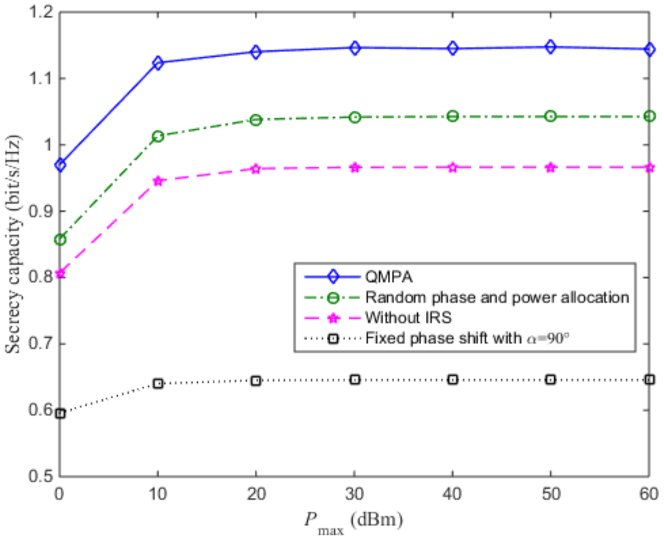

Fig. 11. Secrecy capacity comparisons under different $P_{\max}$ with $K=10$, $\eta=1$, and $L=1$

Fig. 11 studies the secrecy capacity performance under different conditions with $K=10$, $\eta=1$, and $L=1$. From the simulations, we can see that the secrecy capacity of QMPA is the highest among the different conditions, which is 0.1 bit/s/Hz, 0.17 bit/s/Hz, and 0.50 bit/s/Hz higher than that of the conditions with random phase and power allocation, without IRS, and fixed phase shift with $\alpha=\pi/2$. From the **Figs. 2** to **11**, we can conclude that our proposed QMPA can achieve the best performance in all conditions.

5. Conclusion

This paper has developed a secure IRS-assisted IoT framework and investigated transmission efficiency and security issues to achieve a better overall system performance. The expressions of secrecy capacity and secrecy energy efficiency are derived, which provide means for evaluating the security performance. A hybrid resource allocation scheme is proposed for promoting reliable, safe, and efficient transmission of the IoT system. To this end, QMPA is designed to achieve the rational allocation of system resources while lessen the information leakage by the passive eavesdropper. Simulation results indicate the high-efficiency and stability of the QMPA over benchmark solutions in different situations. In the future, it would be beneficial to incorporate the efforts of this work into massive IoT, smart grids, ultra-dense, and heterogeneous communication scenarios for further exploration.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2347-2376, 4th Quart. 2015. Article(CrossRefLink)

[2] Y. Huo, C. Meng, R. N. Li, and T. Jing, “An overview of privacy preserving schemes for industrial Internet of Things,” *China Communications*, vol. 17, no. 10, pp. 1-18, Oct. 2020. Article(CrossRefLink)

[3] S. Verma, S. Kaur, M. A. Khan, and P. S. Sehdev, “Toward green communication in 6G-enabled massive Internet of Things,” *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5408-5415, Apr. 2021. Article(CrossRefLink)

[4] N.-N. Dao, Q.-V. Pham, N. H. Tu, T. T. Thanh, V. N. Q. Bao, D. S. Lakew, and S. Cho, “Survey on aerial radio access networks: Toward a comprehensive 6G access infrastructure,” *IEEE Communications Surveys and Tutorials*, vol. 23, no. 2, pp. 1193-1225, 2nd Quart. 2021. Article(CrossRefLink)

[5] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, “A survey on access control in the age of Internet of Things,” *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4682-4696, Jun. 2020. Article(CrossRefLink)

[6] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, “A survey on security and privacy issues in edge-computing-assisted Internet of Things,” *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4004-4022, Mar. 2021. Article(CrossRefLink)

[7] Q. Wu, and R. Zhang, “Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network,” *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106-112, Jan. 2020. Article(CrossRefLink)

[8] B. Matthiesen, E. Bjornson, E. De Carvalho, and P. Popovski, “Intelligent reflecting surface operation under predictable receiver mobility: A continuous time propagation model,” *IEEE Wireless Communications Letters*, vol. 10, no. 2, pp. 216-220, Feb. 2021. Article(CrossRefLink)

[9] G. H. Yu, X. M. Chen, C. J. Zhong, D. W. K. Ng, and Z. Y. Zhang, “Design, analysis, and optimization of a large intelligent reflecting surface-aided B5G cellular Internet of Things,” *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8902-8916, Sept. 2020. Article(CrossRefLink)

[10] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M. S. Alouini, and R. Zhang, “Wireless communications through reconfigurable intelligent surfaces,” *IEEE Access*, vol. 7, pp. 116753-116773, 2019. Article(CrossRefLink)

[11] Y. H. Jia, C. C. Ye, and Y. Cui, “Analysis and optimization of an intelligent reflecting surface-assisted system with interference,” *IEEE Transactions on Wireless Communications*, vol. 19, no. 12, pp. 8068-8082, Dec. 2020. Article(CrossRefLink)

[12] S. W. Zhang, and R. Zhang, “Capacity characterization for intelligent reflecting surface aided MIMO communication,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 8, pp. 1823-1838, Aug. 2020. Article(CrossRefLink)

[13] O. Ozdogan, E. Bjornson, and E. G. Larsson, “Intelligent reflecting surfaces: Physics, propagation, and pathloss modeling,” *IEEE Wireless Communications Letters*, vol. 9, no. 5, pp. 581-585, May 2020. Article(CrossRefLink)

[14] S. Hu, F. Rusek, and O. Edfors, “Beyond massive MIMO: The potential of data transmission with large intelligent surfaces,” *IEEE Transactions on Signal Processing*, vol. 66, no. 10, pp. 2746-2758, May 2018. Article(CrossRefLink)

[15] M. Jung, W. Saad, M. Debbah, and C. S. Hong, “On the optimality of reconfigurable intelligent surfaces (RISs): Passive beamforming, modulation, and resource allocation,” *IEEE Transactions on Wireless Communications*, vol. 20, no. 7, pp. 4347-4363, 2021. Article(CrossRefLink)

[16] Q. Tao, J. Wang, and C. Zhong, “Performance analysis of intelligent reflecting surface aided communication systems,” *IEEE Communications Letters*, vol. 24, no. 11, pp. 2464-2468, Nov. 2020. Article(CrossRefLink)

[17] J. K. Zuo, Y. W. Liu, Z. J. Qin, and N. Al-Dhahir, “Resource allocation in intelligent reflecting surface assisted NOMA systems,” *IEEE Transactions on Communications*, vol. 68, no. 11, pp. 7170-7183, Nov. 2020. Article(CrossRefLink)

[18] C. W. Huang, G. C. Alexandropoulos, A. Zappone, M. Debbah, and C. Yuen, “Energy Efficient Multi-User MISO Communication using Low Resolution Large Intelligent Surfaces,” in *Proc. of IEEE Globecom Workshops (GC Wkshps)*, pp. 1-6, 2018. Article(CrossRefLink)

[19] J. Chen, Y. C. Liang, Y. Y. Pei, and H. Y. Guo, “Intelligent reflecting surface: A programmable wireless environment for physical layer security,” *IEEE Access*, vol. 7, pp. 82599-82612, 2019. Article(CrossRefLink)

[20] H. Y. Guo, Y. C. Liang, J. Chen, and E. G. Larsson, "Weighted sum-rate maximization for intelligent reflecting surface enhanced wireless networks," in *Proc. of IEEE Global Communications Conference (Globecom)*, pp. 1-6, 2019. Article(CrossRefLink)

[21] F. Shu, T. Shen, L. Xu, Y. L. Qin, S. M. Wan, S. Jin, X. H. You, and J. Z. Wang, "Directional modulation: A physical-layer security solution to B5G and future wireless networks," *IEEE Network*, vol. 34, no. 2, pp. 210-215, Mar-Apr. 2020. Article(CrossRefLink)

[22] X. H. Yu, D. F. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Robust and secure wireless communications via intelligent reflecting surfaces," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2637-2652, Nov. 2020. Article(CrossRefLink)

[23] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1773-1828, 2nd Quart. 2019. Article(CrossRefLink)

[24] S. Hong, C. H. Pan, H. Ren, K. Z. Wang, and A. Nallanathan, "Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface," *IEEE Transactions on Communications*, vol. 68, no. 12, pp. 7851-7866, Dec. 2020. Article(CrossRefLink)

[25] Q. Q. Wu, and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5394-5409, Nov. 2019. Article(CrossRefLink)

[26] Y. Huang, S. He, J. Wang, and J. Zhu, "Spectral and energy efficiency tradeoff for massive MIMO," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 6991-7002, Aug. 2018. Article(CrossRefLink)

[27] C. W. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 4157-4170, Aug. 2019. Article(CrossRefLink)

[28] H. Y. Gao, Y. M. Su, S. B. Zhang, Y. Y. Hou, and M. Jo, "Joint antenna selection and power allocation for secure co-time co-frequency full-duplex massive MIMO systems," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 655-665, Jan. 2021. Article(CrossRefLink)

[29] A. Faramarzi, M. Heidarinejad, S. Mirjalili, and A. H. Gandomi, "Marine predators algorithm: A nature-inspired metaheuristic," *Expert Systems with Applications*, vol. 152, Aug. 2020, Art no. 113377. Article(CrossRefLink)

[30] S. Wang, X. Y. Da, M. D. Li, and T. Han, "Adaptive backtracking search optimization algorithm with pattern search for numerical optimization," *Journal of Systems Engineering and Electronics*, vol. 27, no. 2, pp. 395-406, Apr. 2016. Article(CrossRefLink)

[31] S. C. Zhou, L. N. Xing, X. Zheng, N. Du, L. Wang, and Q. F. Zhang, "A self-adaptive differential evolution algorithm for scheduling a single batch-processing machine with arbitrary job sizes and release times," *IEEE Transactions on Cybernetics*, vol. 51, no. 3, pp. 1430-1442, Mar. 2021. Article(CrossRefLink)

[32] J. Xu, C. C. Guo, and H. Zhang, "Joint channel allocation and power control based on PSO for cellular networks with D2D communications," *Computer Networks*, vol. 133, pp. 104-119, Mar. 2018. Article(CrossRefLink)

[33] X. Z. Wang, X. F. Xu, Q. Z. Sheng, Z. J. Wang, and L. N. Yao, "Novel artificial bee colony algorithms for QoS-aware service selection," *IEEE Transactions on Services Computing*, vol. 12, no. 2, pp. 247-261, Mar-Apr. 2019. Article(CrossRefLink)

[34] Y. Yu, X. Bu, K. Yang, Z. Wu, and Z. Han, "Green large-scale fog computing resource allocation using joint benders decomposition, Dinkelbach algorithm, ADMM, and branch-and-bound," *IEEE Internet of Things Journal* vol. 6, no. 3, pp. 4106-4117, Jun. 2019. Article(CrossRefLink)

[35] H. Y. Gao, S. B. Zhang, Y. M. Su, and M. Diao, "Joint resource allocation and power control algorithm for cooperative D2D heterogeneous networks," *IEEE Access*, vol. 7, pp. 20632-20643, 2019. Article(CrossRefLink)

Yumeng Su received her B.E. degree in Electronic Information Engineering from Harbin Engineering University, Harbin, Heilongjiang, P. R. China, in June 2016. She is currently a doctoral student in Harbin Engineering University. Her current research interests include intelligent computing, resource management, secure communications, massive MIMO, co-frequency co-time full-duplex systems, intelligent reflecting surface, and beyond 5G technologies.

Hongyuan Gao received the Ph.D. degree from the Department of Communication and Information Systems, College of Information and Communication Engineering, Harbin Engineering University, China, in 2010. He has been a Visiting Research Professor under supervision of Prof. Minho Jo with the Department of Computer and Information Science, Korea University, Sejong Metropolitan City, South Korea, from 2015 to 2016. He is currently an Associate Professor with the College of Information and Communication Engineering, Harbin Engineering University, China. Areas of his current interests include wireless energy harvesting communications, intelligent computing, artificial intelligence, radio signal recognition and classification, array signal processing, cognitive radio, HetNets in 5G, communication theory, image processing, and massive MIMO.

Shibo Zhang received his B.E. degree in Electronic Information Engineering from Harbin Engineering University, Harbin, Heilongjiang, P. R. China, in June 2016. He is currently a doctoral student in Harbin Engineering University. His current research interests include fog/edge computing, cognitive relays, energy harvesting, heterogeneous networks, the Internet-of-Things, network slicing, intelligent reflecting surface, and future 6G networks.