EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Secure massive MIMO system with two-way relay cooperative transmission in 6G networks

Yumeng Su[1], Hongyuan Gao[1*] and Shibo Zhang[1]

*Correspondence:
gaohongyuan@hrbeu.edu.cn

[1] College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China

Abstract

With the advent of Internet of Everything and the era of big data, massive multiple-input multiple-output (MIMO) is considered as an essential technology to meet the growing communication requirements for beyond 5G and the forthcoming 6G networks. This paper considers a secure massive MIMO system, where the legitimate user and the base station exchange messages via two-way relays with the presence of passive eavesdroppers. To achieve the trade-off between the physical-layer security and communication reliability, we design a cooperative transmission mode based on multiple-relay collaboration, where some relays broadcast the received signals and other relays act as friendly jammers to prevent the interception by eavesdroppers. A quantum chemical reaction optimization (QCRO) algorithm is proposed to find the most suitable scheme for multiple-relay collaboration. Simulation results highlight excellent performance of the proposed transmission mode under QCRO in different communication scenarios, which can be considered as a potential solution for the security issue in future wireless networks.

Keywords: 6G, Physical-layer security, Massive MIMO, Multiple-relay collaboration, Two-way relaying

1 Introduction

In contemporary society, as the booming development of information technology and the popularity of intelligent equipment, wireless networks have become an essential part of our daily life [1]. Inheriting the benefits achieved in 5G, 6G network is expected to expand to a wider level to realize the full coverage of land and air [2–5]. As networks become denser, how to efficiently utilize the system resources and how to meet the higher transmission demands of ultra-high speed, high quality, and low latency have become key issues in 6G networks [3–5]. Massive multiple-input multiple-output (MIMO) is an effective solution for the increasing challenge of wireless data traffic since it can serve a large number of IoT devices at the same time [6–9]. By utilizing large antenna arrays, massive MIMO can offer a significant improvement in system capacity, and can serve a large variety of devices at the same time, which can greatly improve the quality of service (QoS) and spectral efficiency of communication systems [10].

The openness and sharing of nature of wireless propagation channels make it easy for any smart device to get information. Since more information will be transmitted through

wireless environment in the era of 6G communications, it is crucial to build a secure communication network [11, 12]. Compared with single-antenna transmission architecture, massive MIMO has significant advantages in building secure communication networks. The characteristic of large number of antennas at the base station (BS) makes it easy to transmit several directional beams to the desired terminals. As the size of the antenna array grows infinite, the beam formed by the BS will become narrow and have high directional selectivity, thus effectively reduce the risk of information interception. However, in the actual systems, the number of antennas is finite due to huge hardware cost, and the eavesdroppers will make every effort to intercept or break the information transmission. Typically, cryptographic encryption method was used to maintain the system privacy [13–15], but the implementation complexity is too high due to the cumbersome process of service management. By exploiting wireless transmission properties, physical-layer security has attracted considerable attentions [16, 17]. In order to protect the transmission security, several efforts such as artificial noise [18–20], antenna/relay selection [21–23], and cooperative strategies [24–27] were employed to deal with the information leakage by eavesdroppers. The utilization of antenna correlation diversity was demonstrated to improve the secrecy rate of massive MIMO systems [19]. With the assistance of cooperative relays, the authors in [24] and [25] investigated the secure transmission problem in the presence of passive and active eavesdroppers. The secrecy performance under a practical scenario where the eavesdroppers hide their existence in the system was investigated in [26]. For secure information transmission between the BS and the destination, the authors in [21] proposed a destination-based cooperative jamming scheme to improve the system capacity and transmission confidentiality.

Among recent works on the security issue, the combinations of cooperative relays and secure techniques have shown significant improvements on secrecy capacity and system coverage in massive MIMO networks. Due to the low-complexity relaying process and high spectral efficiency outperforms one-way relay network, two-way relays have attracted extensive attentions [28–31]. In two-way relay networks, eavesdroppers will receive the overlapped information when the two legitimate devices broadcast their signals at the same time [31]. In this condition, both two devices act as source and jammer to prevent the interception by eavesdroppers. By exploiting the dual property, the authors in [32, 33] investigated distributed relay selection criterion to optimize the system security performance. In order to enhance the spatial diversity gains and further improve the system performance, massive MIMO with two-way relay collaboration has become a hotspot in recent researches [34–37]. Feng et al. [35] indicated that the system performance with full-duplex operation outperforms the half-duplex mode under a certain self-loop interference. Zhang et al. [36] investigated the overall performance with hardware impairments. Pan et al. [37] adopted a power allocation strategy based on geometric programming to reduce the information interception of untrusted users. These works, however, did not consider the information leakage happens at the two phases of data transmission.

1.1 Motivation and contributions

Although existing researches have made influential achievements in improving the security performance, there are still some limitations. For better understanding, the

comparison of previous works with our work is presented in Table 1. Many anti-eavesdropping methods [16–20] generally consider the case of direct transmission between the BS and the users, but it's hard to meet the QoS demands of the desired terminals where there are no direct transmission links due to the long-distance fading.

For secure transmission issues with relay collaboration, most of the existing works [21–33, 37] do not simultaneously address the power allocation, resource utilization, and multiple relay selection in a scenario where information leakage happens at both transmission phases in massive MIMO networks with limited time–frequency resources. In this paper, we present a cooperative transmission mode for the security issue of massive MIMO two-way relay networks. Unlike one-way relaying systems, both the two legitimate devices play the roles of source and jammer via two-way relaying operation. However, the duality has not been well exploited in [28, 29, 31] to prevent the interception by eavesdroppers. In order to break through the limitations of previous studies and obtain a higher security performance, we propose a multiple-relay collaboration strategy considering the interception of eavesdroppers during the two phases of information transmission. According to the multiple-relay selection (MRS) scheme, the relays function as receivers/transmitters or friendly jammers to reduce the information leakage between the source and the legitimate user. Considering the energy conservation and communication reliability requirements, we propose a quantum chemical reaction optimization (QCRO) algorithm to obtain the optimal MRS result. The major contributions of our work are summarized in the following:

- We propose a low-complexity cooperative relaying and cooperative jamming (CRCJ) transmission mode to achieve the trade-off between the communication security and reliability of a massive MIMO two-way relay system. The multiple-relay collaboration strategy is employed to enhance the secrecy performance while prevent the interception by eavesdroppers in two transmission phases.

Table 1 Comparison with existing works

References	Category	Power allocation	Security strategy	Cooperative communication	Multiple-relay selection	Using duality
[16–20]	DT	✓	✓	×	×	×
[21]	OWR	✓	✓	✓	×	×
[22]	OWR	×	×	✓	×	×
[23]	OWR	✓	✓	✓	✓	×
[24]	OWR	✓	×	✓	×	×
[25–27]	OWR	✓	✓	✓	×	×
[28]	TWR	×	×	✓	×	×
[29]	TWR	✓	×	✓	×	×
[30]	TWR	✓	✓	✓	×	✓
[31]	TWR	×	✓	✓	×	×
[32, 33]	TWR	×	×	✓	×	✓
[37]	TWR	✓	×	✓	×	✓
Our work	TWR	✓	✓	✓	✓	✓

DT Direct transmission; *OWR* one-way relaying; *TWR* two-way relaying

- Exact expression for secrecy sum-rate is derived considering the information leakage of two transmission phases in massive MIMO relay networks. The expression indicates that secrecy performance is affected by the transmission power of relays and MRS result with QoS and interference constraints in practical scenarios.
- A novel algorithm named QCRO is proposed to tackle the complicated MRS problem for the cooperative transmission in massive MIMO networks. Simulation results illustrate the excellent performance of QCRO over conventional algorithms in various system parameters. Besides, the proposed QCRO algorithm can be considered as a potential solution for other complicated problems in communication domain.

1.2 Organization and notations

The other sections of this work are presented as follows. Section 2 presents the system architecture and the analysis of a secure massive MIMO network with multiple-relay collaboration. The QCRO algorithm for MRS is addressed in Sect. 3, and Sect. 4 presents the simulations. In the end, we conclude this work in the final section.

Notations: The uppercase boldface symbols and lowercase boldface symbols represent matrixes and the vectors, respectively. $\mathbf{0}$ and $\boldsymbol{I}_N$ represent the zero vector and identity matrix, respectively. $\mathcal{CN}(\mu, \sigma^2)$ denotes the complex Gaussian distribution with mean of μ and variance of σ^2. $(.)^{\mathrm{T}}$ and $(.)^{\mathrm{H}}$ represent transpose operator and conjugate transpose operator, respectively. $|.|$, $||.||$, and abs(.) represent modulus, Euclidean norm, and absolute value functions, respectively. $E\{.\}$ denotes the statistical expectation, and $[x]^+$ stands for $\max\{0, x\}$.

2 System model

In this paper, we consider a secure massive MIMO two-way relay network where there is a base station (BS) with M_t antennas, a user, L relays, and K eavesdroppers as shown in Fig. 1. In order to facilitate practical implementation, the user, relays, and eavesdroppers are deployed with a single antenna. Since the direct transmission link between the BS and the user is so weak due to the long-distance fading, the BS and the user exchange their information via two-way relays. With the help of two-way relays, the information transmission can be divided into two phases. In the first phase, both the BS and the user transmit their signals to the two-way relays. In the second phase, the relays amplify and forward the received signals to the legitimate devices. The self-interference cancellation (SIC) is performed at the BS/user side [32]. By removing their own self-interference, both the BS and the user can get their desired signals. However, eavesdroppers cannot separate the desired information from the superimposed signal without the knowledge of prior information about the BS and the user, which makes it difficult to decipher the intended information. When eavesdroppers try to intercept the signal of the user, the signal from the BS can be regarded as interference. The same goes for the BS. However, when the eavesdropper is closely located at the legitimate device, it requires a stronger anti-eavesdropping mechanism to protect the transmission security. In this case, we develop a cooperative relaying and cooperative jamming (CRCJ) transmission mode, i.e., a portion of them act as cooperative relays assist in the information transmission

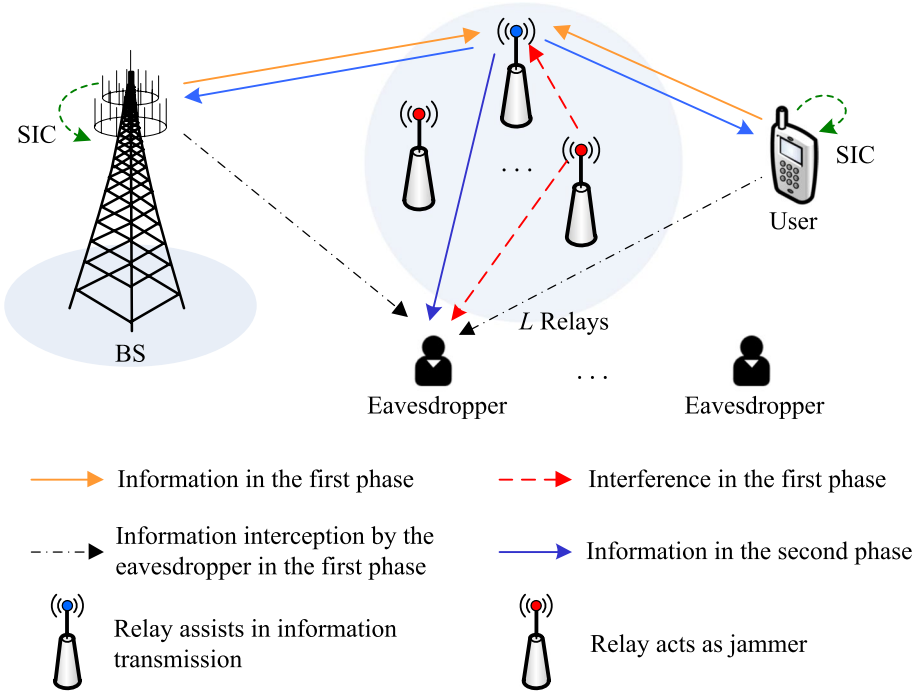

Fig. 1 Diagram of the secure massive MIMO two-way relay network

between the BS and the user, other relays act as jammers to prevent the information leakage by the passive eavesdroppers.

Regarding propagation model, the channel state information (CSI) is defined as $\boldsymbol{g}_{X,Y} = \boldsymbol{h}_{X,Y} d_{X,Y}^{-\xi/2}$ [26], where $\boldsymbol{h}_{X,Y} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{I}_N)$ denotes the small-scale fading factor, and $d_{X,Y}^{-\xi/2}$ denotes the large-scale fading factor. In it, ξ denotes the path loss exponent, and $d_{X,Y}$ denotes the distance between the $X-Y$ link. The global CSI is available by uplink training in time-division duplexed (TDD) massive MIMO networks [11, 38]. We consider the instantaneous CSI remains unchanged in one time slot. The definitions of CSI between the terminals of secure massive MIMO two-way relay networks are as follows:

- CSI from the BS to the i - th relay: $\boldsymbol{g}_{BS,r_i} \in \mathbb{C}^{1\times M_t}$.
- CSI from the BS to the k - th eavesdropper: $\boldsymbol{g}_{BS,e_k} \in \mathbb{C}^{1\times M_t}$.
- CSI from the user to the k - th eavesdropper: g_{u,e_k}.
- CSI from the i - th relay to the user: $g_{r_i,u}$.
- CSI from the i - th relay to the k - th eavesdropper: g_{r_i,e_k}.
- CSI from the i - th relay to the j - th relay ($i \neq j$): g_{r_i,r_j}.

In the following, we will introduce the policy of the CRCJ mode for the secure massive MIMO two-way relay network.

2.1 CRCJ policy

Under CRCJ policy, the relays are divided into two classes for different purposes, i.e., some relays are selected to receive the mixed signal from the BS and the user, while the remaining relays act as jammers to transmit jamming signals to the eavesdroppers.

For simplicity, the MRS scheme is expressed by a binary vector $\boldsymbol{b} = [b_1, b_2, ..., b_L]$, where $b_i \in \{0, 1\}$, $i = 1, 2, ..., L$. If $b_i = 1$, the i - th relay is selected to assist information transmission between the legitimate devices.

In the first phase, the BS and the user simultaneously broadcast their signals with transmit power p_{BS} and p_u. The signal received at the i - th relay is given by

$$y_i = \sqrt{p_{BS}}\boldsymbol{g}_{BS,r_i}\boldsymbol{V}\boldsymbol{s}_{BS} + \sqrt{p_u}g_{r_i,u}s_u + \sum_{j=1}^{L}(1-b_j)\sqrt{p_{r_j}}g_{r_i,r_j}s_{r_j} + \eta_{r_i} \tag{1}$$

where p_{r_j} is the transmit power of the j-th jammer; $\boldsymbol{V}$ is the precoding matrix at the BS; $\boldsymbol{s}_{BS}$, s_u, and s_{r_j} are unit-power signals with $E\{||\boldsymbol{s}_{BS}||^2\} = 1$, $E\{|s_u|^2\} = 1$, and $E\{|s_{r_j}|^2\} = 1$, respectively; η_{r_i} is the additive white Gaussian noise (AWGN). For the k - th eavesdropper, the intercepted signal in the first phase can be expressed as

$$y_{e_k}^{(1)} = \sqrt{p_{BS}}\boldsymbol{g}_{BS,e_k}\boldsymbol{V}\boldsymbol{s}_{BS} + \sqrt{p_u}g_{u,e_k}s_u + \sum_{j=1}^{L}(1-b_j)\sqrt{p_{r_j}}g_{r_j,e_k}s_{r_j} + \eta_{e_k}^{(1)} \tag{2}$$

where $\eta_{e_k}^{(1)}$ is the AWGN. The signal-to-interference plus noise ratio (SINR) received at the k - th eavesdropper from the two legitimate devices (BS and user) can be respectively given by

$$\gamma_{BS\to e_k}^{(1)} = \frac{p_{BS}\left\|\boldsymbol{g}_{BS,e_k}\boldsymbol{V}\right\|^2}{p_u\left|g_{u,e_k}\right|^2 + \sum_{j=1}^{L}(1-b_j)p_{r_j}\left|g_{r_j,e_k}\right|^2 + \sigma_0^2} \tag{3}$$

$$\gamma_{u\to e_k}^{(1)} = \frac{p_u\left|g_{u,e_k}\right|^2}{p_{BS}\left\|\boldsymbol{g}_{BS,e_k}\boldsymbol{V}\right\|^2 + \sum_{j=1}^{L}(1-b_j)p_{r_j}\left|g_{r_j,e_k}\right|^2 + \sigma_0^2} \tag{4}$$

where σ_0^2 denotes the power of AWGN.

In the second phase of data transmission, the selected relays broadcast their received signals to the legitimate devices. We denote p_i as the transmit power of the i - th relay. For the i - th relay, the normalized transmission signal is expressed as

$$y_i^{\text{norm}} = \sqrt{G_i}y_i = \frac{y_i}{\sqrt{p_{BS}\left\|\boldsymbol{g}_{BS,r_i}\boldsymbol{V}\right\|^2 + p_u|g_{r_i,u}|^2 + \sum_{j=1}^{L}(1-b_j)p_{r_j}\left|g_{r_i,r_j}\right|^2 + \sigma_0^2}} \tag{5}$$

where $G_i = \left(p_{BS}\left\|\boldsymbol{g}_{BS,r_i}\boldsymbol{V}\right\|^2 + p_u|g_{r_i,u}|^2 + \sum_{j=1}^{L}(1-b_j)p_{r_j}\left|g_{r_i,r_j}\right|^2 + \sigma_0^2\right)^{-1}$ is the normalization factor. Since the BS and the user can distinguish their transmitted signals, by removing their own self-interference, the corresponding signals at the BS and the user can be respectively expressed by

$$\boldsymbol{y}_{BS} = \sum_{i=1}^{L} b_i\sqrt{G_i p_i}\boldsymbol{W}\boldsymbol{g}_{BS,r_i}^{\mathrm{T}} \cdot \left(\sqrt{p_u}g_{r_i,u}s_u + \sum_{j=1}^{L}(1-b_j)\sqrt{p_{r_j}}g_{r_i,r_j}s_{r_j} + \eta_{r_i}\right) + \boldsymbol{\eta}_{BS} \tag{6}$$

and

$$y_u = \sum_{i=1}^{L} b_i \sqrt{G_i p_i} g_{r_i,u} \cdot \left(\sqrt{p_{BS}} \boldsymbol{g}_{BS,r_i} \boldsymbol{V} \boldsymbol{s}_{BS} + \sum_{j=1}^{L} (1-b_j) \sqrt{p_{r_j}} g_{r_i,r_j} s_{r_j} + \eta_{r_i} \right) + \eta_u \tag{7}$$

where $\boldsymbol{W}$ is the receiving matrix at the BS; $\boldsymbol{\eta}_{BS}$ and η_u are AWGN. The SINRs of the BS and the user are respectively shown by

$$\gamma_{u\to BS} = \frac{\sum_{i=1}^{L} b_i G_i p_i p_u \left\| \boldsymbol{W} \boldsymbol{g}_{BS,r_i}^{\mathrm{T}} \right\|^2 \cdot \left| g_{r_i,u} \right|^2}{\sum_{i=1}^{L} \left[b_i G_i p_i \left\| \boldsymbol{W} \boldsymbol{g}_{BS,r_i}^{\mathrm{T}} \right\|^2 \cdot \left(\sum_{j=1}^{L} (1-b_j) p_{r_j} \left| g_{r_i,r_j} \right|^2 + \sigma_0^2 \right) \right] + \sigma_0^2} \tag{8}$$

and

$$\gamma_{BS\to u} = \frac{\sum_{i=1}^{L} b_i G_i p_i p_{BS} \left| g_{r_i,u} \right|^2 \cdot \left\| \boldsymbol{g}_{BS,r_i} \boldsymbol{V} \right\|^2}{\sum_{i=1}^{L} \left[b_i G_i p_i \left| g_{r_i,u} \right|^2 \cdot \left(\sum_{j=1}^{L} (1-b_j) p_{r_j} \left| g_{r_i,r_j} \right|^2 + \sigma_0^2 \right) \right] + \sigma_0^2} \tag{9}$$

Then, the instantaneous transmission rates of the BS and the user are respectively given by

$$C_{BS\to u} = \frac{1}{2} \log_2 (1 + \gamma_{BS\to u}) \tag{10}$$

and

$$C_{u\to BS} = \frac{1}{2} \log_2 (1 + \gamma_{u\to BS}) \tag{11}$$

Without the knowledge of the CSI between the legitimate devices and cooperative relays, the eavesdroppers cannot separate the superimposed signal [32]. For the k - th eavesdropper, the intercepted signal in the second phase can be given by

$$\begin{aligned} y_{e_k}^{(2)} &= \sum_{i=1}^{L} b_i \sqrt{G_i p_i} g_{r_i,e_k} y_i + \eta_{e_k}^{(2)} \\ &= \sum_{i=1}^{L} b_i \sqrt{G_i p_i} g_{r_i,e_k} \cdot \left(\sqrt{p_{BS}} \boldsymbol{g}_{BS,r_i} \boldsymbol{V} \boldsymbol{s}_{BS} + \sqrt{p_u} g_{r_i,u} s_u + \sum_{j=1}^{L} (1-b_j) \sqrt{p_{r_j}} g_{r_i,r_j} s_{r_j} + \eta_{r_i} \right) + \eta_{e_k}^{(2)} \end{aligned} \tag{12}$$

where $\eta_{e_k}^{(2)}$ is the AWGN. According to (12), the SINR received at the k - th eavesdropper from the BS and the user can be respectively shown by

$$\gamma_{BS\to e_k}^{(2)} = \frac{\sum_{i=1}^{L} b_i G_i p_i p_{BS} \left| g_{r_i,e_k} \right|^2 \cdot \left\| \boldsymbol{g}_{BS,r_i} \boldsymbol{V} \right\|^2}{\sum_{i=1}^{L} \left[b_i G_i p_i \left| g_{r_i,e_k} \right|^2 \cdot \left(p_u \left| g_{r_i,u} \right|^2 + \sum_{j=1}^{L} (1-b_j) p_{r_j} \left| g_{r_i,r_j} \right|^2 + \sigma_0^2 \right) \right] + \sigma_0^2} \tag{13}$$

$$\gamma_{u\to e_k}^{(2)} = \frac{\sum_{i=1}^{L} b_i G_i p_i p_u \left|g_{r_i,e_k}\right|^2 \cdot \left|g_{r_i,u}\right|^2}{\sum_{i=1}^{L}\left[b_i G_i p_i \left|g_{r_i,e_k}\right|^2 \cdot \left(p_{BS}\left\|\boldsymbol{g}_{BS,r_i}\boldsymbol{V}\right\|^2 + \sum_{j=1}^{L}(1-b_j)p_{r_j}\left|g_{r_i,r_j}\right|^2 + \sigma_0^2\right)\right] + \sigma_0^2} \tag{14}$$

Consider the situation that the eavesdroppers are independent of each other, the total received SINR at the passive eavesdroppers from the BS and the user can be respectively expressed by [21].

$$\gamma_{BS}^{\mathrm{E}} = \max_{k\in\{1,2,\ldots,K\}}\left\{\gamma_{BS\to e_k}^{(1)}, \gamma_{BS\to e_k}^{(2)}\right\} \tag{15}$$

$$\gamma_{u}^{\mathrm{E}} = \max_{k\in\{1,2,\ldots,K\}}\left\{\gamma_{u\to e_k}^{(1)}, \gamma_{u\to e_k}^{(2)}\right\} \tag{16}$$

The information leakage from the BS and the user are respectively shown by

$$C_{BS}^{\mathrm{E}} = \frac{1}{2}\log_2\left(1+\gamma_{BS}^{\mathrm{E}}\right) \tag{17}$$

$$C_{u}^{\mathrm{E}} = \frac{1}{2}\log_2\left(1+\gamma_{u}^{\mathrm{E}}\right) \tag{18}$$

Hence, the secrecy transmission rates of the BS and the user can be given by

$$C_{BS\to u}^{\mathrm{S}} = \left[C_{BS\to u} - C_{BS}^{\mathrm{E}}\right]^{+} \tag{19}$$

$$C_{u\to BS}^{\mathrm{S}} = \left[C_{u\to BS} - C_{u}^{\mathrm{E}}\right]^{+} \tag{20}$$

Finally, the secrecy sum-rate of the secure massive MIMO two-way relay network can be expressed by

$$C_{\mathrm{sum}} = \left[C_{BS\to u} - C_{BS}^{\mathrm{E}}\right]^{+} + \left[C_{u\to BS} - C_{u}^{\mathrm{E}}\right]^{+} \tag{21}$$

2.2 Problem formulation

Based on the CRCJ policy, the problem of secrecy sum-rate maximization based on MRS is formulated as

$$\max C_{\mathrm{sum}}(\boldsymbol{b}) = \max\left\{\left[C_{BS\to u}(\boldsymbol{b}) - C_{BS}^{\mathrm{E}}(\boldsymbol{b})\right]^{+} + \left[C_{u\to BS}(\boldsymbol{b}) - C_{u}^{\mathrm{E}}(\boldsymbol{b})\right]^{+}\right\} \tag{22a}$$

subject to

$$b_i \in \{0,1\} \quad \forall i \in \{1,2,\ldots,L\} \tag{22b}$$

$$\sum_{i=1}^{L} b_i \geq 1 \tag{22c}$$

$$0 \leq p_i,\, p_{r_j} \leq p_{\max} \quad \forall i, j \in \{1, 2, \ldots, L\} \tag{22d}$$

$$\sum_{i=1}^{L} \left[b_i G_i p_i \left| g_{r_i,u} \right|^2 \cdot \left(\sum_{j=1}^{L} (1 - b_j) p_{r_j} \left| g_{r_i,r_j} \right|^2 \right) \right] \leq \mathit{Interference} \tag{22e}$$

$$\sum_{i=1}^{L} \left[b_i G_i p_i \left\| \boldsymbol{W} \boldsymbol{g}_{BS,r_i}^{\mathrm{T}} \right\|^2 \cdot \left(\sum_{j=1}^{L} (1 - b_j) p_{r_j} \left| g_{r_i,r_j} \right|^2 \right) \right] \leq \mathit{Interference} \tag{22f}$$

where $p_{\max}$ denotes the maximum transmission power of relays. The relay selection constraints are shown in (22b) and (22c), where (22b) indicates that each relay acts as a jammer or a cooperator to participate in transmission, and (22c) indicates that at least one relay is selected to broadcast confidential signals to the legitimate devices. (22d) denotes the power constraints of cooperative relays and cooperative jammers. (22e) and (22f) are interference constraints, and *Interference* denotes the maximum interference allowed to the legitimate device. Due to the cooperative relaying and cooperative jamming policy, the jamming signals transmitted to eavesdroppers can also cause interference to the BS and the legitimate user. Therefore, in order to guarantee the transmission communication quality of the BS and the legitimate user, we consider interference constraints as in (22e) and (22f). However, these constraints are too complicated to address, which make the problem more difficult to solve. Since the interference is caused by the jammers, it's more convenient to restrict the interference of jammers to the cooperative relays. Hence, to guarantee the system communication quality, we make the interference from the cooperative jammers should not exceed the maximum interference threshold I_{th} of cooperative relays. For the sake of simplifying (22e) and (22f), we can convert them by limiting the transmit power of the relays as follows

$$p_{r_j} = \min \left\{ p_{\max}, \frac{I_{\mathrm{th}}}{L' \left| \max\limits_{i \in \{1,2,\ldots,L\}} \left\{ (1 - b_j) \cdot g_{r_i,r_j} \right\} \right|^2} \right\} \tag{23}$$

where L' denotes the number of cooperative jammers. In this way, the interference constraint can be satisfied for any multiple-relay selection results. Then, we can obtain a higher secrecy rate while ensuring the quality of information transmission, thus achieving the trade-off between communication security and reliability.

Obviously, the optimization problem of (22) is a multi-constraint nonlinear programming problem, and the computational complexity exponentially increases with the number of relays, which is NP-hard to solve. However, traditional algorithms are difficult to get the good performance due to the slow convergence speed and poor convergence

accuracy. To efficiently tackle the complicated problem, we propose a quantum chemical reaction optimization (QCRO) algorithm to obtain the appropriate solution.

3 Methods

In this section, a novel intelligent algorithm named QCRO is proposed for multiple-relay selection in a secure massive MIMO two-way relay network. Inspired by the chemical reaction optimization (CRO) algorithm [39] and quantum evolutionary theory [9], QCRO employs a set of quantum molecules, which is varied by different quantum evolutionary rules. Here we introduce the principle of QCRO.

3.1 QCRO for optimization problem

In an L-dimensional space, (where L is the maximal dimension of the problem), there exist N quantum molecules. The n-th quantum molecule ($n = 1, 2, \ldots, N$) of the t - th iteration is given by

$$\boldsymbol{x}_n^t = \left[x_{n,1}^t, x_{n,2}^t, \ldots, x_{n,L}^t\right] \tag{24}$$

where $0 \le x_{n,l}^t \le 1$; $n = 1, 2, ..., N$; $l = 1, 2, ..., L$; $x_{n,l}^t$ denotes the l - th quantum bit of the n - th quantum molecule. For each quantum molecule, the quantum bits should be measured to the solution domain. The measurement state of the n-th quantum molecule can be obtained by the following rule:

$$\overline{x}_{n,l}^t = \begin{cases} 1, & \alpha_{n,l}^t > (x_{n,l}^t)^2 \\ 0, & \alpha_{n,l}^t \le (x_{n,l}^t)^2 \end{cases} \tag{25}$$

where $\overline{x}_{n,l}^t$ denotes the l - th measurement state of the n-th quantum molecule, and $\alpha_{n,l}^t$ is a random number distributed in [0,1].

The fitness value of the n - th quantum molecule is calculated by the fitness function, which can be expressed as $f(\overline{\boldsymbol{x}}_n^t)$. For the maximum optimization problem, the global optimal solution $\overline{\boldsymbol{\rho}}_{\text{best}}^t = \left[\overline{\rho}_{\text{best},1}^t, \overline{\rho}_{\text{best},2}^t, \ldots, \overline{\rho}_{\text{best},L}^t\right]$ is denoted as the measurement state of the quantum molecule with the maximum fitness value until the t - th iteration.

In QCRO, the quantum molecules are updated by collision, decomposition, and synthesis. These processes are related to the kinetic energy (KE) of quantum molecules, where the top $\mu_1 N$ quantum molecules with the highest KE are updated by collision, $\mu_2 N$ quantum molecules with the smallest KE are updated by synthesis, and the remaining $\mu_3 N$ quantum molecules are updated by decomposition. μ_1, μ_2, and μ_3 are constants which respectively represent the reaction ratio of collision, synthesis, and decomposition. To make it easy, we sort the quantum molecules in a descending order according to the level of KE, and the n' - th quantum molecule is denoted by $\boldsymbol{x}_{n'}^t = \left[x_{n',1}^t, x_{n',2}^t, \ldots, x_{n',L}^t\right]$ with the KE of $e_{n'}^t$. The generation of new quantum molecules is related to the quantum rotation angle and measurement states of previous quantum molecules. For collision, the n' - th quantum molecule is updated to a quantum molecule m, the quantum rotation angle and KE are given by

$$\theta_{m,l}^{t+1} = c_1 \cdot \left(\bar{x}_{g,l}^{t} - \bar{x}_{n',l}^{t}\right) \tag{26}$$

$$e_{m}^{t+1} = e_{n'}^{t} \cdot (1 - \triangle\, e) \tag{27}$$

where $m = n'$; $n' = 1, 2, \ldots, \mu_1 N$; $l = 1, 2, \ldots, L$; $\bar{x}_{g,l}^{t}$ denotes the l - th measurement state of the g - th quantum molecule with higher fitness value in the t - th iteration,$g \in \{1, 2, \ldots, N\}$, $g \neq n'$. c_1 represents the weight coefficient, and $\triangle\, e$ represents the loss rate of KE.

For decomposition, the n' - th quantum molecule is decomposed into quantum molecule m and $m + 1$, and the quantum rotation angles are respectively shown as

$$\theta_{m,l}^{t+1} = \begin{cases} c_2 \cdot \left(\bar{\rho}_{\text{best},l}^{t} - \bar{x}_{n',l}^{t}\right) + c_3 \cdot (\bar{x}_{a,l}^{t} - \bar{x}_{n',l}^{t}), & \varphi_{m,l}^{t+1} < \kappa_1 \\ c_4 \cdot \left(\bar{x}_{g,l}^{t} - \bar{x}_{n',l}^{t}\right), & \text{else} \end{cases} \tag{28}$$

$$\theta_{m+1,l}^{t+1} = \begin{cases} c_2 \cdot \left(\bar{\rho}_{\text{best},l}^{t} - \bar{x}_{n',l}^{t}\right) + c_3 \cdot \left(\bar{x}_{a,l}^{t} - \bar{x}_{n',l}^{t}\right), & \varphi_{m+1,l}^{t+1} < \kappa_1 \\ c_4 \cdot \left(\bar{x}_{g,l}^{t} - \bar{x}_{n',l}^{t}\right), & \text{else} \end{cases} \tag{29}$$

where $m = 2n' - \mu_1 N - 1$; $n' = \mu_1 N + 1, \mu_1 N + 2, ..., \mu_1 N + \mu_3 N$; $l = 1, 2, ..., L$; $g \in \{1, 2, ..., N\}$, $g \neq n'$; $\bar{x}_{a,l}^{t}$ denotes the l - th measurement state of a random quantum molecule in the t - th iteration, $a \in \{1, 2, ..., N\}$, $a \neq n'$; c_2, c_3 and c_4 are weight coefficients. κ_1 is the mutation probability which is a fixed parameter that determines the decomposition style, $\varphi_{m,l}^{t+1}$ and $\varphi_{m+1,l}^{t+1}$ are random variables distributed from 0 to 1. The KE of quantum molecule m and $m + 1$ can be expressed by

$$e_{m}^{t+1} = e_{n'}^{t} \cdot (1 - \triangle\, e)/2 \tag{30}$$

$$e_{m+1}^{t+1} = e_{n'}^{t} \cdot (1 - \triangle\, e)/2 \tag{31}$$

For synthesis, the n' - th quantum molecule and the $(n' + 1)$ - th quantum molecule are synthesized into a new quantum molecule m, the quantum rotation angle and KE are given by

$$\theta_{m,l}^{t+1} = c_5 \cdot \omega_{m,l}^{t} \cdot \left(\bar{x}_{n'+1,l}^{t} - \bar{x}_{n',l}^{t}\right) \tag{32}$$

$$e_{m}^{t+1} = \left(e_{n'}^{t} + e_{n'+1}^{t}\right) \cdot (1 - \triangle\, e) \tag{33}$$

where $m = (n' + \mu_1 N + 3\mu_3 N + 1)/2$; $n' = \mu_1 N + \mu_3 N + 1, \mu_1 N + \mu_3 N + 3, ..., N - 1$; $l = 1, 2, ..., L$; c_5 represents the weight coefficient; and $\omega_{m,l}^{t}$ is a random variable distributed from 0 to 1.

The m - th and $(m + 1)$ - th updated quantum molecules can be respectively obtained by

$$x_{m,l}^{t+1} = \begin{cases} \sqrt{1-(x_{n',l}^{t})^2}, & \theta_{m,l}^{t+1} = 0 \text{ and } \hat{\varphi}_{m,l}^{t+1} \le \kappa_2 \\ \text{abs}\left(x_{n',l}^{t} \cdot \cos\theta_{m,l}^{t+1} - \sqrt{1-(x_{n',l}^{t})^2} \cdot \sin\theta_{m,l}^{t+1}\right), & \text{else} \end{cases} \tag{34}$$

$$x_{m+1,l}^{t+1} = \begin{cases} \sqrt{1-\left(x_{n',l}^{t}\right)^2}, & \theta_{m+1,l}^{t+1} = 0 \text{ and } \hat{\varphi}_{m+1,l}^{t+1} \le \kappa_2 \\ \text{abs}\left(x_{n',l}^{t} \cdot \cos\theta_{m+1,l}^{t+1} - \sqrt{1-(x_{n',l}^{t})^2} \cdot \sin\theta_{m+1,l}^{t+1}\right), & \text{else} \end{cases} \tag{35}$$

where $\hat{\varphi}_{m,l}^{t+1}$ and $\hat{\varphi}_{m+1,l}^{t+1}$ are random variables distributed from 0 to 1, κ_2 denotes the conversion probability, and abs(.) represents the absolute value function. For collision, $m = n'$; $n' = 1, 2, ..., \mu_1 N$. For decomposition, $m = 2n' - \mu_1 N - 1$; $n' = \mu_1 N + 1, \mu_1 N + 2, ..., \mu_1 N + \mu_3 N$. For synthesis, $m = (n' + \mu_1 N + 3\mu_3 N + 1)/2$; $n' = \mu_1 N + \mu_3 N + 1, \mu_1 N + \mu_3 N + 3, \ldots, N - 1$.

Then, we obtain the corresponding measurement states of the updated quantum molecules and calculate the fitness value. The measurement state of the quantum molecule with the maximum fitness value until the $(t+1)$ - th iteration is updated as the global optimal solution $\overline{\boldsymbol{\rho}}_{\text{best}}^{t+1}$. The iteration ends when the QCRO algorithm achieves the terminal condition.

3.2 Computational complexity analysis

For the iterations of quantum molecules in QCRO, it is required to rank the kinetic energy of quantum molecules. The computational complexity is $O(N)$. According to their kinetic energy, the quantum molecules are updated by collision, decomposition, or synthesis reactions separately. The quantum rotation angles and new quantum molecules are generated according to different reactions, with the computational complexity of $O(2N \times L)$. These reactions also change the kinetic energy of quantum molecules, and the computational complexity is $O(N)$. Based on (25), the measurement states of the updated quantum molecules can be obtained. The computational complexity is $O(N \times L)$. Then, calculate the fitness value of the updated quantum molecules and update the global optimal solution of QCRO. The computational complexity is $O(2N)$.

When the QCRO algorithm terminates after running t iterations, the computational complexity is $O_{\text{iteration}} = O(t \times N \times (4 + 3L))$.

3.3 Process of multiple-relay selection based on QCRO

In order to tackle the MRS problem of (22) in secure massive MIMO two-way relay networks, the fitness function of QCRO algorithm is set as $f\left(\overline{\boldsymbol{x}}_n^t\right) = \begin{cases} C_{\text{sum}}(\overline{\boldsymbol{x}}_n^t), & \text{satisfy constraint conditions} \\ 0, & \text{else} \end{cases}$. For each quantum molecule, the measurement state is corresponding to a MRS result, the global optimal solution of QCRO algorithm corresponds to the optimal MRS result. Then, the problem of finding the best MRS vector with the maximized secrecy sum-rate can be transformed into finding the global optimal solution of QCRO. Based on the iteration process of QCRO, we can easily get the global optimal solution. In general, the process of MRS based on QCRO for secrecy sum-rate optimization can be shown in Algorithm 1.

Algorithm 1 Multiple-relay selection based on QCRO

1 Input parameters of the secure massive MIMO two-way relay network;

2 Initialize the population of quantum molecules and other parameters of QCRO;

3 Set $t = 1$;

4 Obtain measurement states of all quantum molecules by (25);

5 Calculate the fitness value by the fitness function;

6 Obtain the global optimal solution $\bar{\boldsymbol{\rho}}_{\text{best}}^{t}$;

7 repeat

8 Sort the quantum molecules in a descending order according to the kinetic energy;

9 Update the quantum molecules and by collision, decomposition, and synthesis;

10 Obtain measurement states of the newly generated quantum molecules by (25);

11 Calculate the fitness value of each updated quantum molecule;

12 Update the global optimal solution until the $(t+1)$-th iteration;

13 Set $t = t+1$;

14 until the QCRO algorithm achieves the terminal condition

15 Obtain the optimal MRS result according to the global optimal solution;

16 Output the optimal MRS result.

4 Results and discussion

Here we present the secrecy performance in the secure massive MIMO two-way relay network. We consider a two-dimensional network topology where the BS and the legitimate user are located at the positions (0, 0) and (100, 0) (unit: meters), respectively, L relays are randomly located at (50, 0) with the radius of 20, and K eavesdroppers are randomly located in the system. We set $L = 20$, $I_{\text{th}} = -20\,\text{dBm}$, $\xi = 3.8$, and $M_t = 128$ [9]. The system bandwidth $B = 1\,\text{MHz}$, and noise power spectral density $N_0 = -174\,\text{dBm/Hz}$ [7]. To reduce the implementation complexity, maximum ratio transmission (MRT) and maximum ratio combining (MRC) methods are adopted at the BS for precoding and receiving [6]. The comparisons of the proposed QCRO algorithm, existing intelligent algorithms and relay selection strategies are presented in the first part. For the second part, we illustrate the impact on the secrecy sum-rate of the cooperative transmission mode based on QCRO algorithm with various system parameters. All results are the average of 200 Monte-Carlo simulations.

4.1 Performance comparisons with QCRO

The comparisons of QCRO algorithm, particle swarm optimization (PSO) algorithm [40], chemical reaction optimization (CRO) algorithm [39], single-relay selection (SRS) strategy [32], and random multiple-relay selection (RMRS) strategy on the secrecy performance are presented in this section. To tackle the MRS problem of (22), the PSO, CRO, SRS, and RMRS adopt the same fitness function as QCRO. The specific operations of PSO, CRO, and SRS are depicted in [40], [39], and [32], respectively.

Table 2 Parameter settings of QCRO algorithm

Parameter	Values
Population size (N)	60
Maximum iteration number	500
Loss rate of kinetic energy (Δe)	0.2
Reaction ratio of collision (μ_1)	0.55
Reaction ratio of synthesis (μ_2)	0.15
Reaction ratio of decomposition (μ_3)	0.3
Weight coefficient (c_1)	0.1
Weight coefficient (c_2)	0.1
Weight coefficient (c_3)	0.03
Weight coefficient (c_4)	0.03
Weight coefficient (c_5)	0.03
Mutation probability (κ_1)	0.5
Conversion probability (κ_2)	0.1/L

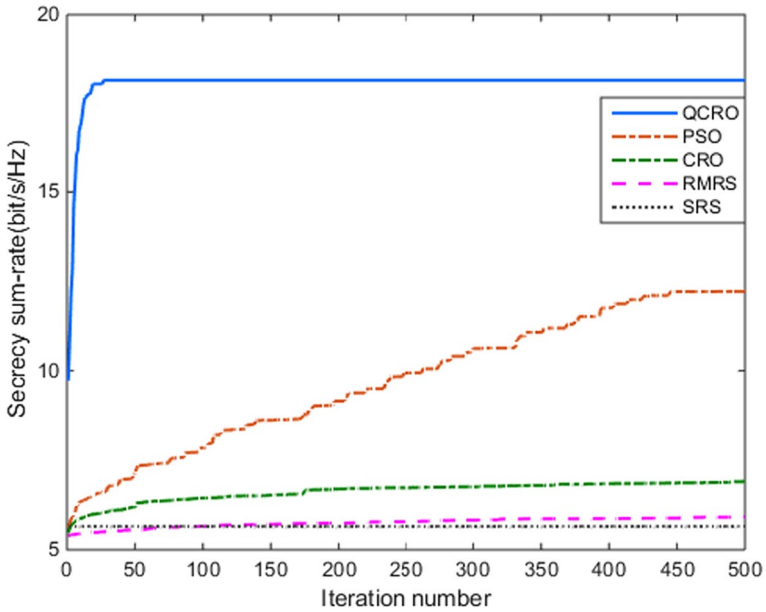

Fig. 2 Convergence performance comparisons. Blue line: QCRO; yellow line: PSO; green line: CRO; pink line: RMRS; black line: SRS

For the SRS, only one relay is selected to forward the received signal, while other relays transmits jamming signals. For the RMRS, all relays are randomly predefined as helper or jammer. To facilitate comparison, we set the maximum number of iterations for QCRO, PSO, and CRO algorithms to the same value, and all these algorithms are set to the same population size. The other parameters of PSO and CRO algorithms are set to the optimal values cited in [40] and [39], respectively. For QCRO algorithm, all quantum bits are initialized to 0.5 and the initial kinetic energy each quantum molecule is set to 1000. The parameter settings of QCRO algorithm are shown in Table 2.

The convergence performance of QCRO algorithm, PSO algorithm, CRO algorithm, SRS, and RMRS strategies are presented in Fig. 2 with $p_{BS} = 35\,\text{dBm}$, $p_u = 30\,\text{dBm}$,

$p_{\max} = 30\,\text{dBm}$, and $K = 1$. For the MRS problem, both PSO and CRO fall into the local optimum. We observe that QCRO algorithm has a rather fast convergence speed (converges after 30 iterations) and a higher convergent accuracy throughout the iterations. The reason is that QCRO algorithm combines the merit of chemical reaction process and the thought of quantum intelligence computation theory. In QCRO, the quantum molecules are updated via different quantum evolution strategies of collision, decomposition, and synthesis. The designed quantum evolution strategies can make full use of the interactions of quantum molecules, which increases the diversity of solutions. In addition, the searching speed and searching accuracy can be greatly improved by designing new quantum evolutionary rules (28) and (29). Simulation result shows that QCRO has strong search ability and ideal convergence compared with other algorithms. The results also illustrate that the prominent advantage of QCRO over the SRS and RMRS strategies on secrecy sum-rate in a massive MIMO system.

The secrecy performance of QCRO, PSO, CRO, RMRS and SRS with the variation of p_{BS}, p_u, $p_{\max}$, and K are shown in Figs. 3, 4, 5, and 6. In Fig. 3, for most strategies, the secrecy sum-rate of the massive MIMO system increases along with p_{BS}. For QCRO, the rising tendency begins to slow down when p_{BS} is over 15 dBm. This phenomenon is caused by information leakage. Since the eavesdropper tries to intercept the desired signals during the information transmission process, the signal strength received at the eavesdropper will become stronger as p_{BS} increases. According to (3) and (13), the eavesdropper may obtain more information from the BS in a higher p_{BS}. When the level of p_{BS} exceeds a certain threshold, the increment of the eavesdropping rate will be greater than that of legitimate transmission rate, which will lead to the reduction of secrecy sum-rate. From the simulation result, we can conclude that

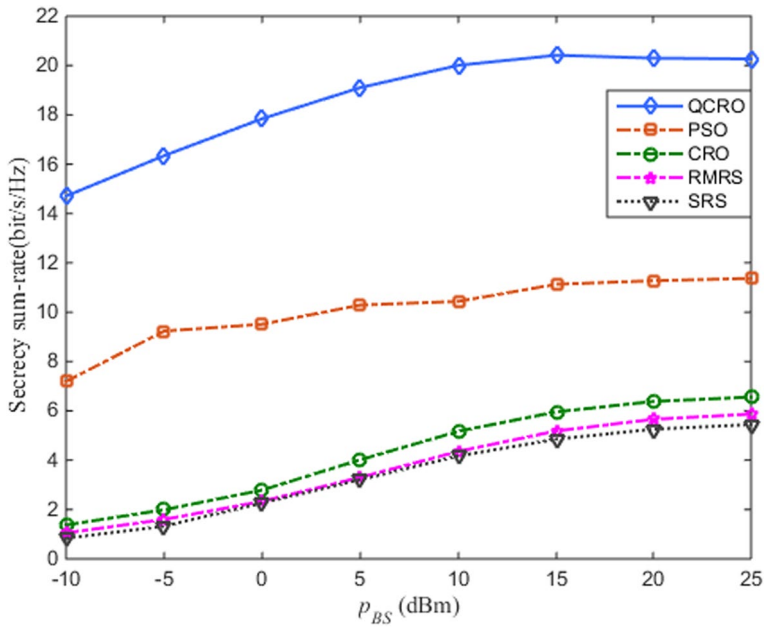

Fig. 3 Secrecy sum-rate in different p_{BS} with $p_u = 30\,\text{dBm}$, $p_{\max} = 30\,\text{dBm}$, and $K = 1$. Blue line: QCRO; yellow line: PSO; green line: CRO; pink line: RMRS; black line: SRS

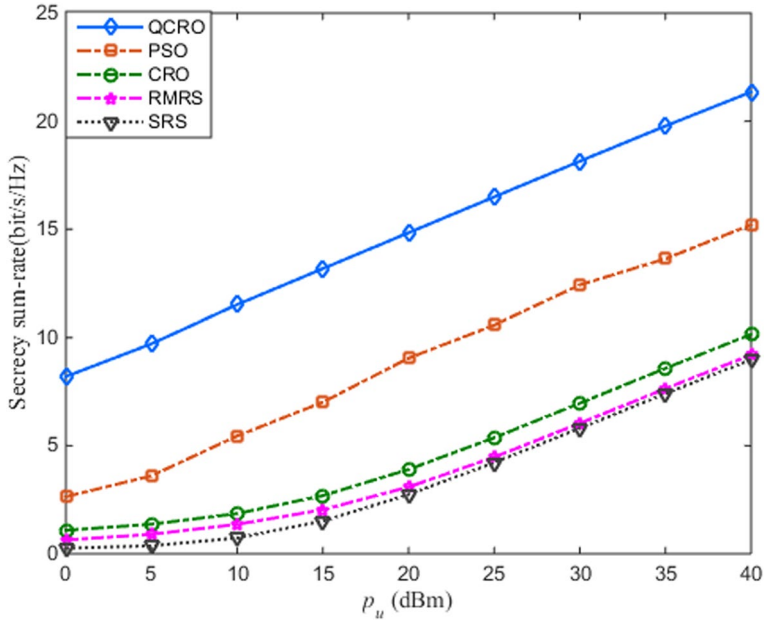

Fig. 4 Secrecy sum-rate in different p_u with $p_{BS} = 35$ dBm, $p_{\max} = 30$ dBm, and $K = 1$. Blue line: QCRO; yellow line: PSO; green line: CRO; pink line: RMRS; black line: SRS

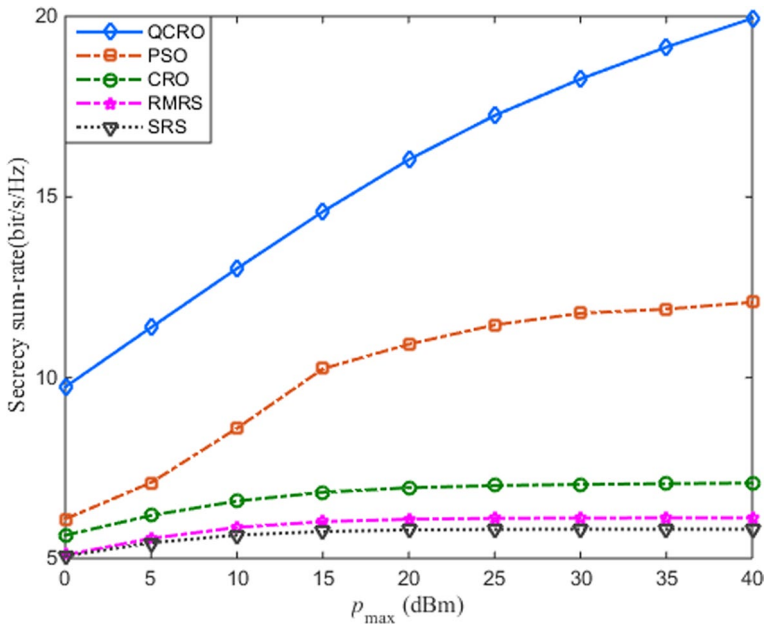

Fig. 5 Secrecy sum-rate in different $p_{\max}$ with $p_{BS} = 35$ dBm, $p_u = 30$ dBm, and $K = 1$. Blue line: QCRO; yellow line: PSO; green line: CRO; pink line: RMRS; black line: SRS

the secrecy sum-rate may tends to decrease when p_{BS} is over 25 dBm. Compared with other schemes, QCRO can achieve the highest secrecy sum-rate in any p_{BS}.

Figures 4 and 5 illustrate the impact of different transmit power of the user and maximum transmit power of the cooperative relays on the security performance. For

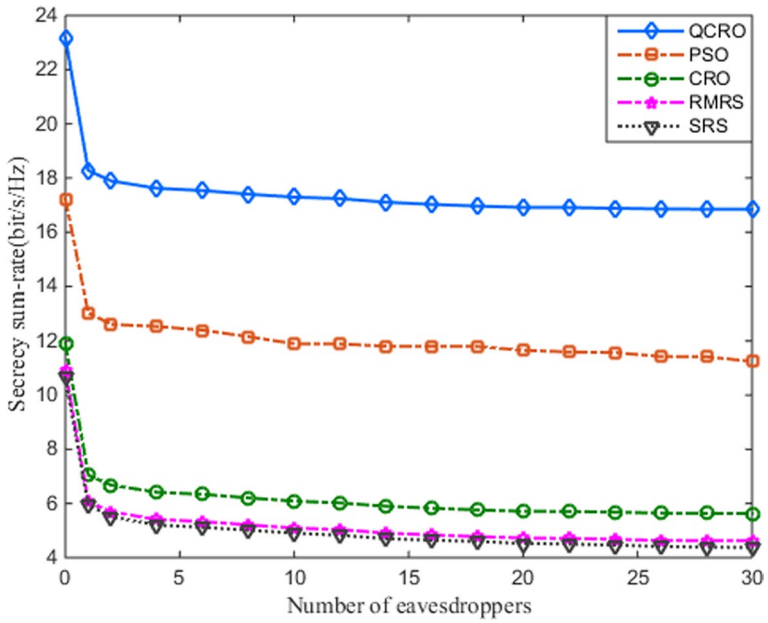

Fig. 6 Secrecy sum-rate in different K with $p_{BS} = 35$ dBm, $p_u = 30$ dBm, and $p_{\max} = 30$ dBm. Blue line: QCRO; yellow line: PSO; green line: CRO; pink line: RMRS; black line: SRS

all strategies in Fig. 4, a higher secrecy sum-rate can be achieved by increasing p_u. The results in Fig. 5 also illustrate that increasing $p_{\max}$ can boost the security performance. The reason is that a larger $p_{\max}$ will permit relays to broadcast the signals at a higher transmission power under certain interference conditions. After self-interference elimination, the increment of SINR at the legitimate devices is higher than that of the eavesdroppers.

The impact of different number of eavesdroppers on the secrecy sum-rate is presented in Fig. 6. The result shows that the existence of eavesdroppers has an adverse effect on the secrecy performance, and the information leakage increases along with K. That is because by increasing K, the probability of emerging an eavesdropper with a higher channel gain increases accordingly. For the non-colluding eavesdroppers, the information leakage is determined by the maximum received SINR at the eavesdroppers during the two transmission phases. From Figs. 3, 4, 5, and 6, we conclude that QCRO has great advantages over other strategies in improving the communication security of secure massive MIMO two-way relay networks.

4.2 Impact of different system parameters

The performance of the proposed cooperative transmission mode based on QCRO algorithm in different p_u and p_{BS} is studied in Fig. 7, where p_u increases from 0 to 40 dBm, $p_{BS} = 0$ dBm, 3 dBm, 5 dBm, and 10 dBm, respectively. From the simulations, the system can obtain a higher secrecy sum-rate with a larger level of p_u at first. But when p_u is over 30 dBm, the increment of secrecy sum-rate begins to slow down. For the cases of $p_{BS} = 3$ dBm, 5 dBm, and 10 dBm, the secrecy sum-rate decreases with p_u when p_u is over 35 dBm. The reason is that the SINR received at the eavesdropper

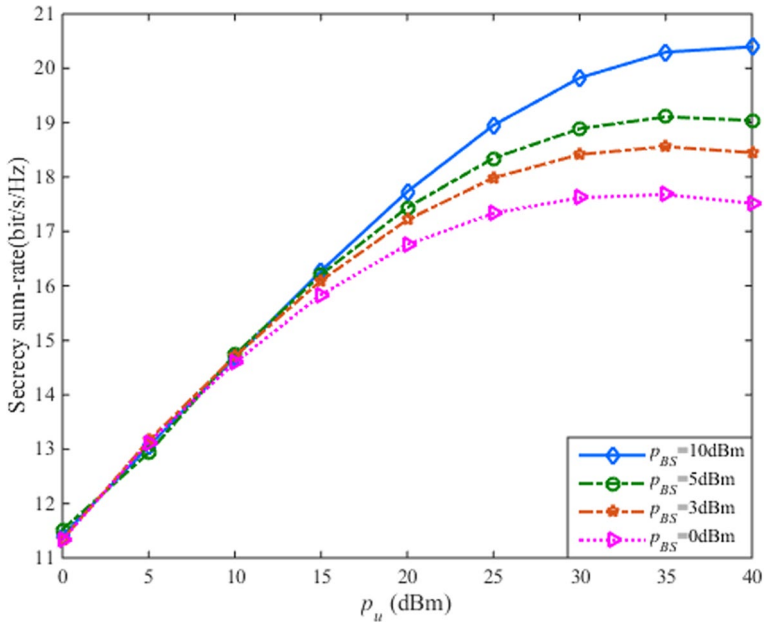

Fig. 7 Secrecy sum-rate in different p_u and p_{BS} with $p_{\max} = 30$ dBm and $K = 1$. Blue line: $p_{BS} = 10$ dBm; green line: $p_{BS} = 5$ dBm; yellow line: $p_{BS} = 3$ dBm; pink line: $p_{BS} = 0$ dBm

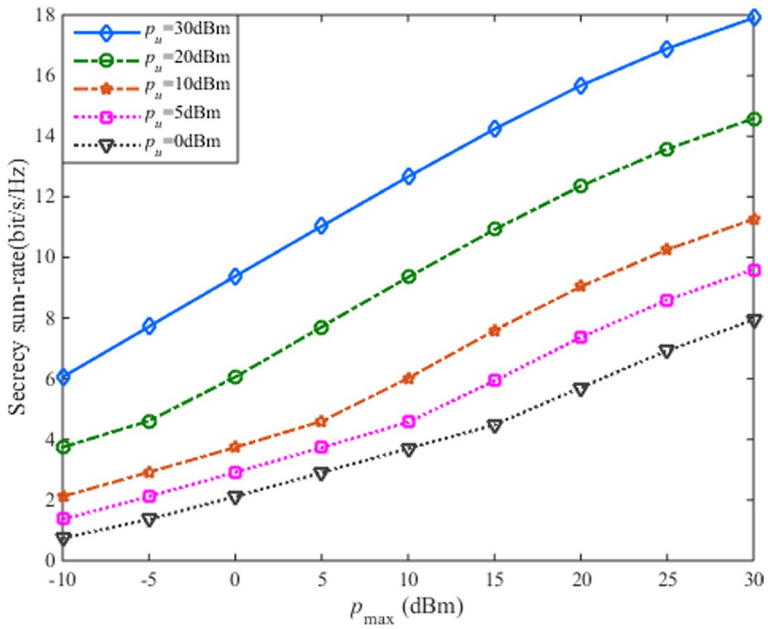

Fig. 8 Secrecy sum-rate in different $p_{\max}$ and p_u with $p_{BS} = 35$ dBm and $K = 1$. Blue line: $p_u = 30$ dBm; green line: $p_u = 20$ dBm; yellow line: $p_u = 10$ dBm; pink line: $p_u = 5$ dBm; black line: $p_u = 0$ dBm

increases with p_u, which may cause more information leakage. Hence, we can appropriately increase p_{BS} to confuse the eavesdroppers.

In Fig. 8, we investigate the impact of different $p_{\max}$ and p_u levels with $p_{\max}$ varying from 0 to 40 dBm, $p_u = 0$ dBm, 5 dBm, 10 dBm, 20 dBm, and 30 dBm, respectively.

From the simulations, the increasing trend of secrecy sum-rate with p_u is in accordance with the results of Fig. 4. We also observe that both higher levels of $p_{\max}$ and p_u can help boost the communication security. The reason is that a higher $p_{\max}$ can permit each relay to use more power for its own transmission. With the increment of $p_{\max}$, the desired terminals can obtain higher transmission rates than that of the eavesdroppers according to the SIC criterion.

The influence of p_{BS} and number of eavesdroppers are studied in Fig. 9. In simulations, p_{BS} varying from − 10 to 20 dBm, and $K = 1, 3, 10, 20$, respectively. The results indicate that a larger number of eavesdroppers can cause more information leakage, which jeopardizes the communication security of massive MIMO system. For a certain value of K, we can see that the secrecy sum-rate increases with p_{BS} at first. However, the growth starts to slow down as p_{BS} increases. Take $K = 1$ as an example, there is a dropping trend in the secrecy sum-rate when p_{BS} is over 15 dBm. Since the eavesdropper may intercept more information from the BS at a higher p_{BS}, when the increment of the eavesdropping rate exceeds the increment of legitimate transmission rate, the secrecy sum-rate will no longer increase with p_{BS}. Therefore, appropriate p_{BS} plays a significant role in improving the secrecy sum-rate.

The influence of different $p_{\max}$ and L in single and multiple eavesdropper cases are investigated in Fig. 10. We consider $K = 1$ and $K = 10$, $p_{\max}$ varies from − 10 to 20 dBm, and L increases from 5 to 20. The simulation results indicate that both higher $p_{\max}$ and more relays can boost the transmission security. Obviously, the secrecy sum-rate in the case of single eavesdropper is higher than that of multiple eavesdroppers.

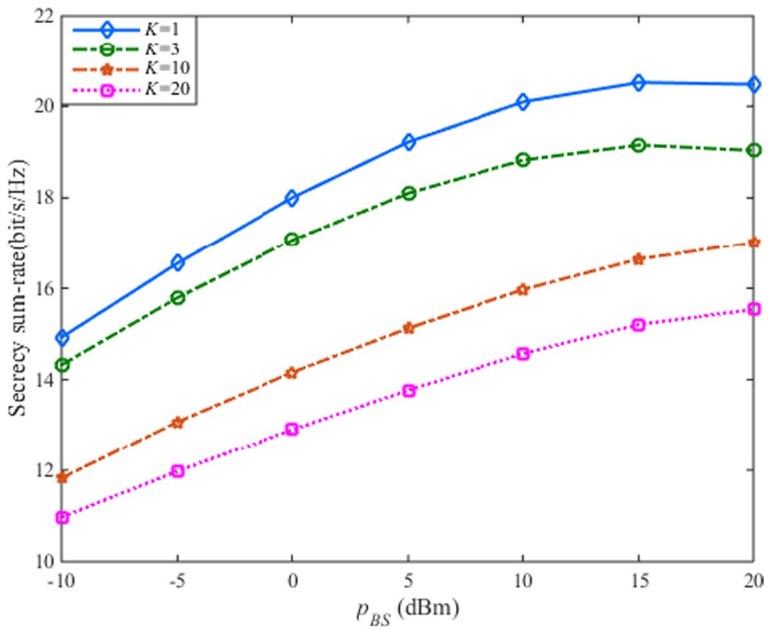

Fig. 9 Secrecy sum-rate in different p_{BS} and K with $p_u = 30$dBm and $p_{\max} = 30$dBm. Blue line: $K = 1$; green line: $K = 3$; yellow line: $K = 10$; pink line: $K = 20$

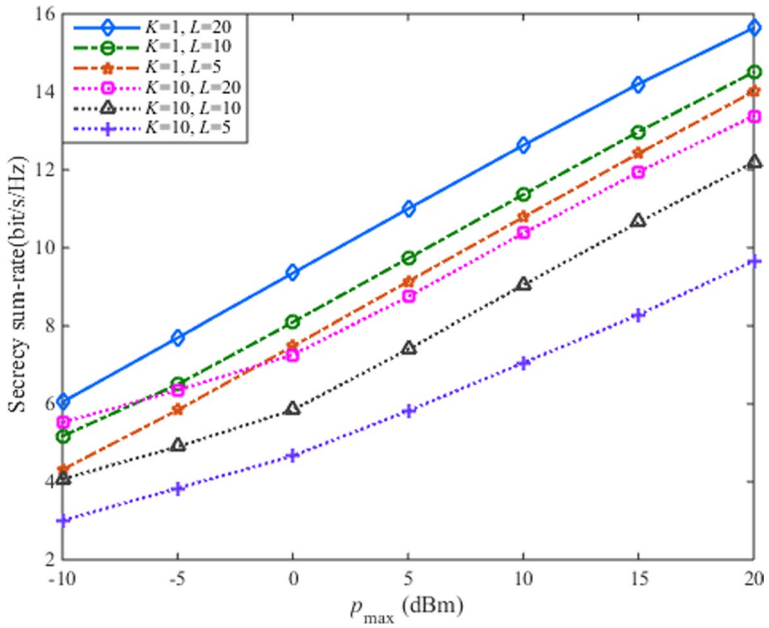

Fig. 10 Secrecy sum-rate in different $p_{\max}$ and L with $p_{BS} = 35$dBm, $p_u = 30$dBm, and $K = \{1, 10\}$. Blue line: $K = 1$, $L = 20$; green line: $K = 1$, $L = 10$; yellow line: $K = 1$, $L = 5$; pink line: $K = 10$, $L = 20$; black line: $K = 10$, $L = 10$; purple line: $K = 10$, $L = 5$

5 Conclusions

In this paper, we have designed a cooperative transmission mode to achieve the trade-off between the communication security and reliability in a massive MIMO system with two-way relay cooperation. Based on the multiple-relay collaboration strategy, some relays function as helper while other relays act as jammer to against the interception of eavesdroppers. Considering the system capacity, energy conservation, and QoS requirements, we have formulated the MRS problem in a secure massive MIMO two-way relay network. Then, we have introduced the implementation of multiple-relay collaboration strategy based on QCRO to optimize the secrecy sum-rate and simulation results have demonstrated its effectiveness in different communication scenarios. In future research, we will incorporate the efforts of this work with energy harvesting, network slicing, and ultra-dense heterogeneous networks to meet the increasing demands of future wireless communication systems.

Abbreviations

IoE	Internet of Everything
MIMO	Multiple-input multiple-output
BS	Base station
QCRO	Quantum chemical reaction optimization
QoS	Quality of service
DT	Direct transmission
OWR	One-way relaying
TWR	Two-way relaying
MRS	Multiple-relay selection
CSI	Channel state information
TDD	Time-division duplexed
CRCJ	Cooperative relaying and cooperative jamming
AWGN	Additive white Gaussian noise
SINR	Signal-to-interference plus noise ratio

SIC	Self-interference cancellation
CRO	Chemical reaction optimization
KE	Kinetic energy
MRT	Maximum ratio transmission
MRC	Maximum ratio combining
PSO	Particle swarm optimization
SRS	Single-relay selection
RMRS	Random multiple-relay selection

Acknowledgements
The authors would like to acknowledge the anonymous reviewers and editors for their efforts in valuable comments and suggestions.

Author contributions
YS conceived of the study, and participated in its network design, and was a major contributor in writing the manuscript. HG mainly provided the guidance for deriving these expressions. SZ carried out experiments and theoretical analysis. All authors read and approved the final manuscript.

Funding
This work was supported by the National Natural Science Foundation of China (No. 61571149), the Special China Postdoctoral Science Foundation (2015T80325), Fundamental Research Funds for the Central Universities (HEUCFP201808 and HEUCF190801), and the China Postdoctoral Science Foundation (2013M530148).

Availability of data and materials
All data generated or analysed during this study are included in this article.

Declarations

Competing interests
The authors declare that they have no competing interests.

Received: 18 May 2020 Accepted: 18 July 2023
Published online: 29 July 2023

References

1. S. Verma, S. Kaur, M.A. Khan et al., Toward green communication in 6G-enabled massive Internet of Things. IEEE Internet Things J. **8**(7), 5408–5415 (2021)
2. D.C. Nguyen, M. Ding, P.N. Pathirana et al., 6G Internet of Things: A comprehensive survey. IEEE Internet Things J. **9**(1), 359–383 (2022)
3. P. Yang, Y. Xiao, M. Xiao et al., 6G wireless communications: Vision and potential techniques. IEEE Netw. **33**(4), 70–75 (2019)
4. H. Viswanathan, P.E. Mogensen, Communications in the 6G era. IEEE Access **8**, 57063–57074 (2020)
5. L. Zhang, Y.C. Liang, D. Niyato, 6G visions: Mobile ultra-broadband, super Internet-of-Things, and artificial intelligence. China Commun. **16**(8), 1–14 (2019)
6. H.Y. Gao, Y.M. Su, S.B. Zhang et al., Joint antenna selection and power allocation for secure co-time co-frequency full-duplex massive MIMO systems. IEEE Trans. Veh. Technol. **70**(1), 655–665 (2021)
7. A. Zappone, L. Sanguinetti, G. Bacci, E. Jorswieck et al., Energy-efficient power control: a look at 5G wireless technologies. IEEE Trans. Signal Process. **64**(7), 1668–1683 (2016)
8. B.M. Lee, Cell-free massive MIMO for massive low-power Internet of Things networks. IEEE Internet Things J. **9**(9), 6520–6535 (2022)
9. H.Y. Gao, Y.M. Su, S.B. Zhang et al., Antenna selection and power allocation design for 5G massive MIMO uplink networks. China Commun. **16**(4), 1–15 (2019)
10. B.M. Lee, H. Yang, Energy-efficient massive MIMO in massive industrial Internet of Things networks. IEEE Internet Things J. **9**(5), 3657–3671 (2022)
11. L.X. Li, A.P. Petropulu, Z. Chen, MIMO secret communications against an active eavesdropper. IEEE Trans. Inf. Forensic Secur. **12**(10), 2387–2401 (2017)
12. K.W. Jiang, T. Jing, Y. Huo et al., SIC-based secrecy performance in uplink NOMA multi-eavesdropper wiretap channels. IEEE Access **6**, 19664–19680 (2018)
13. S.Y. Liu, Y. Hong, E. Viterbo, Unshared secret key cryptography. IEEE Trans. Wirel. Commun. **13**(12), 6670–6683 (2014)
14. S.X. Wang, W. Li, J. Lei, Physical-layer encryption in massive MIMO systems with spatial modulation. China Commun. **15**(10), 159–171 (2018)
15. I. Grigg, P. Gutmann, The curse of cryptographic numerology. IEEE Secur. Priv. **9**(3), 70–72 (2011)
16. R. Zi, J. Liu, L. Gu et al., Enabling security and high energy efficiency in the Internet of Things with massive MIMO hybrid precoding. IEEE Internet Things J. **6**(5), 8615–8625 (2019)
17. Y.O. Basciftci, C.E. Koksal, A. Ashikhmin, Physical-layer security in TDD massive MIMO. IEEE Trans. Inf. Theory **64**(11), 7359–7380 (2018)
18. F.C. Zhu, F.F. Gao, H. Lin et al., Robust beamforming for physical layer security in BDMA massive MIMO. IEEE J. Sel. Areas Commun. **36**(4), 775–787 (2018)

19. Y.P. Wu, R. Schober, D.W.K. Ng et al., Secure massive MIMO transmission with an active eavesdropper. IEEE Trans. Inf. Theory **62**(7), 3880–3900 (2016)
20. W. Xu, B. Li, L. Tao et al., Artificial noise assisted secure transmission for uplink of massive MIMO systems. IEEE Trans. Veh. Technol. **70**(7), 6750–6762 (2021)
21. A. Kuhestani, A. Mohammadi, M. Mohammadi, Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers. IEEE Trans. Inf. Forensic Secur. **13**(2), 341–355 (2018)
22. Y.L. Zou, X.B. Wang, W.M. Shen et al., Security versus reliability analysis of opportunistic relaying. IEEE Trans. Veh. Technol. **63**(6), 2653–2661 (2014)
23. C. Wang, H.M. Wang, X.G. Xia, Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks. IEEE Trans. Wirel. Commun. **14**(2), 589–605 (2015)
24. J. Chen, X.M. Chen, T. Liu et al., Toward green and secure communications over massive MIMO relay networks: joint source and relay power allocation. IEEE Access **5**, 869–880 (2017)
25. D. Kudathanthirige, S. Timilsina, G.A.A. Baduge, Secure communication in relay-assisted massive MIMO downlink with active pilot attacks. IEEE Trans. Inf. Forensic Secur. **14**(11), 2819–2833 (2019)
26. T.M. Hoang, T.Q. Duong, H.D. Tuan et al., Secure massive MIMO relaying systems in a Poisson field of eavesdroppers. IEEE Trans. Commun. **65**(11), 4857–4870 (2017)
27. X.M. Chen, J. Chen, T. Liu, Secure transmission in wireless powered massive MIMO relaying systems: performance analysis and optimization. IEEE Trans. Veh. Technol. **65**(10), 8025–8035 (2016)
28. T. Mekkawy, R.G. Yao, N. Qi et al., Secure relay selection for two way amplify-and-forward untrusted relaying networks. IEEE Trans. Veh. Technol. **67**(12), 11979–11987 (2018)
29. D. Wang, B. Bai, W. Chen et al., Secure green communication via untrusted two-way relaying: A physical layer approach. IEEE Trans. Commun. **64**(5), 1861–1874 (2016)
30. K. Lee, J.P. Hong, H.H. Choi et al., Wireless-powered two-way relaying protocols for optimizing physical layer security. IEEE Trans. Inf. Forensic Secur. **14**(1), 162–174 (2019)
31. J.C. Chen, R.Q. Zhang, L.Y. Song et al., Joint relay and jammer selection for secure two-way relay networks. IEEE Trans. Inf. Forensic Secur. **7**(1), 310–320 (2012)
32. C.S. Zhang, J.H. Ge, F.K. Gong et al., Improving physical-layer security for wireless communication systems using duality-aware two-way relay cooperation. IEEE Syst. J. **13**(2), 1241–1249 (2019)
33. C.S. Zhang, J.H. Ge, J. Li, F.K. Gong et al., Complexity-aware relay selection for 5G large-scale secure two-way relay systems. IEEE Trans. Veh. Technol. **66**(6), 5462–5466 (2017)
34. B. Dutta, R. Budhiraja, R.D. Koilpillai et al., Analysis of quantized MRC-MRT precoder for FDD massive MIMO two-way AF relaying. IEEE Trans. Commun. **67**(2), 988–1003 (2019)
35. J.J. Feng, S.D. Ma, G.H. Yang et al., Power scaling of full-duplex two-way massive MIMO relay systems with correlated antennas and MRC/MRT processing. IEEE Trans. Wirel. Commun. **16**(7), 4738–4753 (2017)
36. J.Y. Zhang, X.P. Xue, E. Bjornson et al., Spectral efficiency of multipair massive MIMO two-way relaying with hardware impairments. IEEE Wirel. Commun. Lett. **7**(1), 14–17 (2018)
37. X. Pan, L. Guo, C. Dong, et al., in *Proc. IEEE International Conference on Communications (ICC)*, Secure multi-pair massive MIMO two-way amplify-and-forward relay network with power allocation scheme (IEEE, Paris, 2017), pp. 1–5.
38. R. Hamdi, E. Driouch, W. Ajib, Energy management in hybrid energy large-scale MIMO systems. IEEE Trans. Veh. Technol. **66**(11), 10183–10193 (2017)
39. Y. Liu, H. Zhang, K. Long et al., Fog computing vehicular network resource management based on chemical reaction optimization. IEEE Trans. Veh. Technol. **70**(2), 1770–1781 (2021)
40. X. Liu, Z. Li, P. Xu et al., Joint optimization for bandwidth utilization and delay based on particle swarm optimization. IEEE Access **9**, 92125–92133 (2021)

Publisher's Note