Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 819195, 11 pages
http://dx.doi.org/10.1155/2015/819195

Research Article

Resource Management Based on Security Satisfaction Ratio with Fairness-Aware in Two-Way Relay Networks

Jun Zhao,[1] Zhaoming Lu,[1] Xiangming Wen,[1] Haijun Zhang,[1,2] Shenghua He,[1] and Wenpeng Jing[1]

[1] *Beijing Key Laboratory of Network System Architecture and Convergence, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC, Canada V6T 1Z4*

Correspondence should be addressed to Jun Zhao; xfx_321@bupt.edu.cn

Received 14 July 2014; Accepted 27 January 2015

Academic Editor: Muhammad Khurram Khan

Information security has been received more and more attention for next-generation wireless sensor networks. In this paper, we consider the problem of resource management based on security satisfaction ratio with fairness-aware in two-way relay networks. Multiple source nodes exchange information with the help of relay node in the presence of an eavesdropper, and diverse security requirements are taken into account with coexistence of security users and normal users. The joint problem of power allocation, and subchannel pairing and allocation aims to maximize the security satisfaction ratio for legitimate users subject to limited power and subchannel constraints. We model the security resource management problem as a mixed integer programming problem, which is decomposed into three subproblems, distributed power allocation, distributed subchannel allocation, and distributed subchannel pairing, and then solved it in *constraint particle swarm optimization* (CPSO), *binary CPSO* (B_CPSO), and *classic Hungarian algorithm* (CHA) method, respectively. Moreover, a suboptimal subchannel pairing algorithm is proposed to reduce the computational complexity compared with the CHA. Simulations are conducted to evaluate the effectiveness of the proposed algorithms.

1. Introduction

1.1. Background. Small cell (such as relay and femtocell) is a promising technology in fifth generation (5G) mobile communications [1]. Classical one-way relay channel consists of one sender, one receiver, and one assisting relay. Recently, there has been increasing attention from the research community paid to studying the two-way (bidirectional) relay channel, where two senders exchange information via one assisting relay at the same time. Compared with the traditional one-way relay, two-way relay provides improved spectral/power efficiency for information exchange between two source nodes [2, 3]. Therefore, the research of two-way relay has received much interest in recent years. The basic idea of two-way relay is to exchange information through one or more assisting *relay nodes* (RNs) based on the idea of network coding. The relay can be categorized into the following two types depending on its forwarding protocol [4]: (1) *amplify and forward* (AF): RN receives signal from source node and then amplifies the signal and forwards it to the terminal node. AF relays are beneficial due to their simpleness and short delays; (2) *Decode and forward* (DF): DF relays receive and encode useful signal and then forward a new signal. Such relays are beneficial in interference-limited systems because this type of relays does not amplify noise and interference. Recently, information security has drawn much more attention due to broadcast feature of wireless channels [5, 6], and two-way relay is more vulnerable to eavesdropping due to its transfer character. Therefore, more and more scholars study how to improve the security of two-way relay.

1.2. Related Works. Recently, there are a few literatures focusing on the two-way relay security. In [7], the authors consider the case where the transmit messages and the feedback signals are subject to eavesdropping in two-way relay networks, and the question of how much the feedback signal impacts the secrecy capacity is investigated by studying two fundamental models. In [8], the authors study the bidirectional broadcast channel with confidential messages, and the simulations show that a strong secrecy capacity region is established in two-way relay networks. In [9], secrecy capacity is analyzed in a Gaussian two-way relay wiretap channel, and a jamming strategy is introduced to maximize the achievable secrecy rate regions. In [10], the security of the three-phase two-way relaying system with an eavesdropper is investigated. A cooperative jamming and power allocation scheme is proposed to enhance the system secrecy capacity. In [11], the authors study the secrecy capacity maximization based on power allocation in DF two-way relay systems with the presence of an eavesdropper. But the water-filling-like power allocation [12] is too complex for small cell as relay to complete. These literatures improve the relay security in a certain extent, and secrecy capacity as security model is widely used. However, to the best of our knowledge, users' responses to information security in two-way relay networks has not been studied in the current literatures. As we know, secrecy capacity is just an objective measurement of information security, which cannot well reflect the users' actual feelings to information security. Therefore, new security evaluation criteria from the perspective of users should be studied in two-way relay networks.

1.3. Our Contribution. In this paper, we present a novel problem of resource management based on security satisfaction ratio with fairness-aware in two-way relay networks. Our contribution can be summarized as follows: (1) we introduce a novel security satisfaction ratio model, which is utilized as objection function to analyse the information security problem through resource optimization. Compared with secrecy capacity, security satisfaction ratio can well reflect the users' actual feelings to security. (2) Diverse information security requirements are considered for different legitimate users in this paper. Furthermore, the fairness of users is also guaranteed. (3) *Constrained particle swarm optimization* (CPSO) algorithm, *binary CPSO* (B_CPSO) algorithm, and *classic Hungarian algorithm* (CHA) are jointed to solve this security resource optimization problem. (4) A suboptimal subchannel pairing algorithm is proposed to reduce the computational complexity of subchannel pairing compared with CHA. Performance of the proposed algorithms is verified by simulations.

1.4. Organization. The remainder of this paper is structured as follows. The system model and target problem are presented in Section 2. Section 3 provides the *joint resource allocation based on security satisfaction ratio with fairness-aware* (JRASSFA) algorithm. Performance of the proposed algorithms is described in Section 4. Finally, Section 5 gives the conclusions.

2. System Model

2.1. System Model. A two-way relay OFDMA system consists of one RN, K pairs of mobile users (PMUs), and one eavesdropper (E) in this paper. As shown in Figure 1, PMUs transmit information with the help of a RN, while eavesdropper tries to eavesdrop the exchange information of PMUs. In this scenario, legal users attempt to acquire maximum security information. The relay node works in a half-duplex mode and uses AF protocol. The process of AF two-way relay transmission is divided into two phases: multiple access phase (MA) and broadcast (BC) phase. In MA phase, PMUs transmit signals to RN synchronously and then RN amplifies the received signals and broadcasts them to PMUs in BC phase. In order to avoid interuser interference, each subchannel can only be occupied by no more than one PMU. We set B as the bandwidth of each subchannel and N is the number of subchannels. PMU k consists of A_k and B_k, where $k \in \{1, \ldots, K\}$. The channel fading includes the path loss and the frequency flat Rayleigh fading, which may vary on different subchannels.

We assume that subchannel i is allocated to A_k and B_k in MA phase, while j is allocated to A_k and B_k in BC phase; the received signal for RN in the MA phase can be expressed as

$$Y_{\mathrm{RN}}^{i} = \sqrt{p_{A_k}^{i}} g_{A_k,\mathrm{RN}}^{i} X_{A_k}^{i} + \sqrt{p_{B_k}^{i}} g_{B_k,\mathrm{RN}}^{i} X_{B_k}^{i} + Z_{\mathrm{RN}}^{i}, \quad (1)$$

where, $i \in \{1, \ldots, N\}$, $X_{A_k}^{i}$ and $X_{B_k}^{i}$ are the complex transmit symbols from PMU A_k and B_k on subchannel i, respectively; $p_{A_k}^{i}$ and $p_{B_k}^{i}$ denote the transmit power of A_k and B_k, respectively; $g_{A_k,\mathrm{RN}}^{i}$ and $g_{B_k,\mathrm{RN}}^{i}$ denote the channel gains from A_k to RN and from B_k to RN on subchannel i, respectively; Z_{RN}^{i} denotes the additive noise, which can be seen as an *additive white Gaussian noise* (AWGN) with zero means and variance σ^2 on subchannel i at the RN; and the value of AWGN is assumed the same in this paper.

We denote the received signal of eavesdropper E in the MA phase by

$$Y_{E}^{i} = \sqrt{p_{A_k}^{i}} g_{A_k,E}^{i} X_{A_k}^{i} + \sqrt{p_{B_k}^{i}} g_{B_k,E}^{i} X_{B_k}^{i} + Z_{E}^{i}, \quad (2)$$

where $g_{A_k,E}^{i}$ and $g_{B_k,E}^{i}$ are the channel gains from A_k to E and from B_k to E on subchannel i, respectively, and Z_E^{i} is the AWGN of E on subchannel i.

In the BC phase, we denote the received signal at A_k, B_k and eavesdropper E on subchannel j by

$$Y_{A_{k,i}}^{j} = \xi \sqrt{p_{\mathrm{RN}}^{j}} h_{A_k}^{j} Y_{\mathrm{RN}}^{i} + Z_{A_k}^{j}, \quad (3)$$

$$Y_{B_{k,i}}^{j} = \xi \sqrt{p_{\mathrm{RN}}^{j}} h_{B_k}^{j} Y_{\mathrm{RN}}^{i} + Z_{B_k}^{j}, \quad (4)$$

$$Y_{E,i}^{j} = \xi \sqrt{p_{\mathrm{RN}}^{j}} h_{E}^{j} Y_{\mathrm{RN}}^{i} + Z_{E}^{j}, \quad (5)$$

where, $j \in \{1, \ldots, N\}$, $h_{A_k}^{j}$, $h_{B_k}^{j}$ and h_E^{j} are the channel gains from RN to A_k, from RN to B_k, and from RN to eavesdropper E on subchannel j, respectively. ξ is the amplification factor of relay node and p_{RN}^{j} denotes the RN's transmit power on subchannel j in BC phase. $Z_{A_k}^{j}$, $Z_{B_k}^{j}$, and Z_E^{j} are the AWGNs at A_k, B_k, and eavesdropper E on subchannel j, respectively.

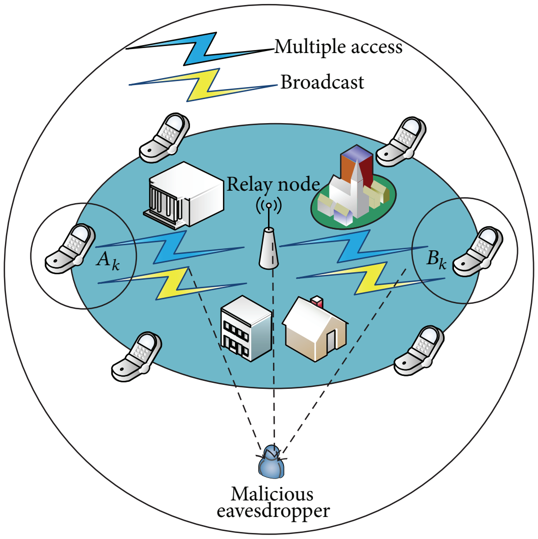


Figure 1: Security transmission model.

We assume that each PMU has perfect capability of self-interference cancelation in the BC phase. Based on (1), (3), and (4), the SNRs (signal-noise ratios) of A_k and B_k can be given by

$$\mathrm{SNR}_{A^j_{k,i}} = \frac{\xi^2 p^j_{\mathrm{RN}} \left|h^j_{A_k}\right|^2 p^i_{B_k} \left|g^i_{B_k,\mathrm{RN}}\right|^2}{\left(\xi^2 p^j_{\mathrm{RN}} \left|h^j_{A_k}\right|^2 + 1\right)\sigma^2},$$
$$\mathrm{SNR}_{B^j_{k,i}} = \frac{\xi^2 p^j_{\mathrm{RN}} \left|h^j_{B_k}\right|^2 p^i_{A_k} \left|g^i_{A_k,\mathrm{RN}}\right|^2}{\left(\xi^2 p^j_{\mathrm{RN}} \left|h^j_{B_k}\right|^2 + 1\right)\sigma^2}. \tag{6}$$

The composite received signal in MA and BC phases at eavesdropper E can be given by

$$\vec{Y}_E = \vec{H}_E \vec{x} + \vec{Z}_E, \tag{7}$$

where

$$\vec{H}_E = \begin{bmatrix} \sqrt{p^i_{A_k}} g^i_{A_k,E} & \sqrt{p^i_{B_k}} g^i_{B_k,E} \\ \xi \sqrt{p^j_{\mathrm{RN}}} h^j_E \sqrt{p^i_{A_k}} g^i_{A_k,\mathrm{RN}} & \xi \sqrt{p^j_{\mathrm{RN}}} h^j_E \sqrt{p^i_{B_k}} g^i_{B_k,\mathrm{RN}} \end{bmatrix},$$
$$\vec{x} = \begin{bmatrix} x^i_{A_k} \\ x^i_{B_k} \end{bmatrix}, \qquad \vec{Z}_E = \begin{bmatrix} Z^i_E \\ \xi \sqrt{p^j_{\mathrm{RN}}} h^j_E Z^i_{\mathrm{RN}} + Z^j_E \end{bmatrix}. \tag{8}$$

The SNR of the eavesdropper can be written as follows:

$$\overrightarrow{\mathrm{SNR}}^j_{E,i} = \vec{H}_E \vec{H}^H_E \vec{N}^{-1}_E, \tag{9}$$

where

$$\vec{N}_E = \sigma^2 \begin{bmatrix} 1 & 0 \\ 0 & 1 + \xi^2 p^j_{\mathrm{RN}} \left|h^j_E\right|^2 \end{bmatrix}. \tag{10}$$

Based on Shannon capacity formula, the capacities of users A_k, B_k, and E are defined as follows, respectively:

$$R^j_{A_{k,i}} = B \lg\left(1 + \mathrm{SNR}^j_{A_{k,i}}\right),$$
$$R^j_{B_{k,i}} = B \lg\left(1 + \mathrm{SNR}^j_{B_{k,i}}\right), \tag{11}$$
$$R^j_{E,i} = B \lg\det\left(\vec{I} + \vec{H}_E \vec{H}^H_E \vec{N}^{-1}_E\right),$$

where $\det(\cdot)$ denotes the value of the determinant.

Definition 1 (secrecy capacity). It is the capacity difference between the legitimate information exchange between the terminals and the information leakage to the eavesdropper.

Then the secrecy capacity for a PMU (A_k, B_k) is shown as

$$R^j_{\mathrm{sec},k,i} = \left[B \log\left(1 + \mathrm{SNR}^j_{A_{k,i}}\right) + B \log\left(1 + \mathrm{SNR}^j_{B_{k,i}}\right) - B \log\det\left(\vec{I} + \vec{H}_E \vec{H}^H_E \vec{N}^{-1}_E\right)\right]^+, \tag{12}$$

where $[x]^+ = \max\{0, x\}$, $B\log(1+\mathrm{SNR}^j_{A_{k,i}}) + B\log(1+\mathrm{SNR}^j_{B_{k,i}})$ is the capacity of PMU k on subchannels i and j in a complete transmission, and $B\log\det(\vec{I} + \vec{H}_E \vec{H}^H_E \vec{N}^{-1}_E)$ is the leakage capacity to the eavesdropper E.

2.2. Secrecy Ratio and Security Satisfaction Ratio.

Secrecy ratio reflects the users' security extent, which means that users can get higher information security guarantee under higher secrecy ratio.

Definition 2 (secrecy ratio). Secrecy capacity accounts for the proportion of the total capacity. It can be described as follows:

$$\chi_k = \frac{R_{\mathrm{sec},k}}{R_k}, \tag{13}$$

where $R_{\mathrm{sec},k}$ and R_k are the total secrecy capacity and total capacity of PMU k, respectively. And $R_{\mathrm{sec},k}$ and R_k will be defined in (21).

Definition 3 (security satisfaction ratio). It is defined as the users' satisfaction extent to their own information security in the process of transmission.

In two-way relay security OFDMA system, information security is threatening each user. Thus, we need to find a criterion to evaluate the information security extent from the perspective of users, and the security satisfaction ratio (SSR) of users is a good criterion to evaluate users' information security extent. In this paper, secrecy ratio (χ_k) is selected as the security satisfaction factor; thus, the higher the secrecy ratio, the higher the security satisfaction ratio. To model security satisfaction ratio, we need to find a function which satisfies the rule of diminishing marginal returns; that is, SSR ($f(\chi_k)$) increases with the increase of user's secrecy ratio, but the increase value of SSR slows down with the increase of secrecy ratio (this is because we assume the maximum value of security satisfaction ratio is 1, which could not have unlimited growth); that is,

$$\frac{\partial f(\chi_k)}{\partial \chi_k} > 0, \qquad \frac{\partial^2 f(\chi_k)}{\partial^2 \chi_k} < 0. \tag{14}$$

Sigmoid function is one of the monotone functions which satisfy the above characteristics [13–15], and it has been widely used to solve the resource allocation problem in wireless networks. In [13, 15], Sigmoid function based noncooperative access control algorithm is proposed in CDMA and IEEE 802.11e networks, respectively. The Sigmoid function is defined as follows [14]:

$$f(x) = \left(1 + e^{-x}\right)^{-1}. \tag{15}$$

Thus, the SSR function of PMU k is defined as follows based on Sigmoid function:

$$f_k(\chi_k) = \frac{1}{1 + e^{\alpha_k(\beta_k - \chi_k)}}, \tag{16}$$

where α_k and β_k are the security preference parameters of PMU k, whose function can be explained in Figure 2: α_k determines the gradient of the curve, which can be regarded as user's sensitivity to the variation of secrecy ratio. β_k determines the center of the curve, which can be regarded as user's expected secrecy ratio value to acquire half SSR. As Figure 2 shows, for the same expected value of secrecy ratio ($\beta_k = 0.6$), the SSR increases faster with a larger α_k, which means user has higher sensitivity to the variation of secrecy ratio. For the same sensitivity ($\alpha_k = 15$), SSR increases with decreasing β_k, which means that user has lower security requirement with a smaller β_k.

2.3. User Type and Fairness Model. Diverse security requirements are taken into account with coexistence of security users and normal users in this two-way relay system. In this paper, users are divided into three types: VIP (very important person), IP (important person), and NP (normal person). In order to guarantee the security requirement for different users, security tolerability is defined as follows:

$$Q(k) = \begin{cases} \zeta_{\text{VIP}}^{\min}, & \text{if PMU } k \text{ is VIP}, \\ \zeta_{\text{IP}}^{\min}, & \text{if PMU } k \text{ is IP}, \\ \zeta_{\text{NP}}^{\min}, & \text{if PMU } k \text{ is NP}, \end{cases} \tag{17}$$

where $\zeta_{\text{VIP}}^{\min}$, $\zeta_{\text{IP}}^{\min}$, and $\zeta_{\text{NP}}^{\min}$ are the security tolerability for different users, respectively. We can admit that $\zeta_{\text{VIP}}^{\min} > \zeta_{\text{IP}}^{\min} > \zeta_{\text{NP}}^{\min}$ since the VIPs have the highest security priority. In the process of subchannel allocation, if subchannel is allocated to PMU k, that means PMU k could acquire the maximum SSR on this subchannel. If the secrecy ratio of PMU k is greater than PMU k's security tolerability, the allocation process is over. Otherwise, subchannel is reallocated to other PMUs that could reach their security tolerability, but the SSR may not be the maximum on this subchannel.

Fairness is also important in wireless communication systems since all users expect to have better experience whether they are VIPs or not. Plenty of data transmission rate is the assurance of communication quality, especially for NPs, who focus on transmission rate more than information security. Therefore, we should not only pursue SSR maximization, but also consider the users' capacity requirement. In [16], the authors assess the user's capacity by the normalized cumulative distribution function (CDF), which is widely used in 3GPP2 and IEEE802.16j. Therefore, in this paper, we use CDF as fairness index to assess the fairness of system. The normalized capacity $\widetilde{R}(k)$ of PMU k is defined as follows:

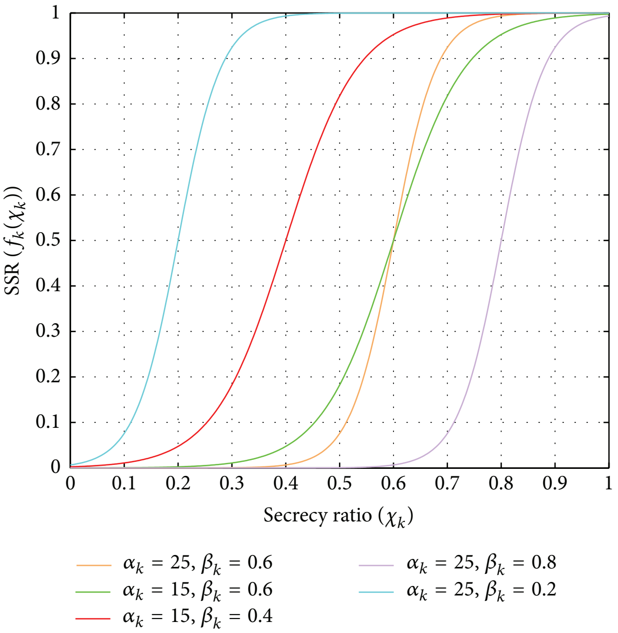


Figure 2: SSR function of users.

$$\widetilde{R}(k) = \frac{R_k}{\operatorname{avg}_{1 \le \hat{k} \le K}\left(R\left(\hat{k}\right)\right)}, \tag{18}$$

where R_k is the total capacity of PMU k and $\operatorname{avg}_{1 \le \hat{k} \le K}(R(\hat{k}))$ is the average capacity of PMUs.

The fairness criterion can be given by

$$\varphi = \frac{N\left(\widetilde{R}(k) \ge 0.3\right)}{K} - 0.9 \ge 0, \tag{19}$$

where $N(\widetilde{R}(k) \ge 0.3)$ represents the number of PMUs whose normalized capacity is greater than or equal to 0.3, and the meaning of this equation is that at least 90% of the effective PMUs should have capacity more than 30% of the average capacity.

2.4. Problem Formulation. In this subsection, a subchannel assignment variable and a subchannel pairing variable are defined by $a_k^{(i,j)}$ and $u_{(i,j)}$, where (i, j) means PMUs transmit signal to RN on subchannel i in MA phase while RN broadcasts signal to PMUs on subchannel j in BC phase. Consider

$$a_k^{(i,j)} = \begin{cases} 1, & \text{if PMU } k \text{ occupies } (i,j) \\ 0, & \text{otherwise,} \end{cases}$$
$$u_{(i,j)} = \begin{cases} 1, & \text{if } i \text{ paired with } j \\ 0, & \text{otherwise.} \end{cases} \tag{20}$$

We consider a two-way relay network with K PMUs and N subchannels. Hence, the total security satisfaction ratio U of PMUs can be defined as

$$U = \max_{P,a,u} \sum_{k=1}^{K} f_k(\chi_k),$$
$$\chi_k = \frac{R_{\sec,k}}{R_k} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} u_{(i,j)} a_k^{(i,j)} R_{\sec,k,i}^{j}}{\sum_{i=1}^{N}\sum_{j=1}^{N} u_{(i,j)} a_k^{(i,j)} R_{k,i}^{j}} \tag{21}$$

subject to

$$\begin{aligned}
&\text{C1: } \sum_{j=1}^{N} p_{\text{RN}}^{j} \le p_{\text{RN}},\\
&\text{C2: } p_{\text{RN}}^{j} \ge 0, \quad \forall j,\\
&\text{C3: } \chi_k \ge Q(k), \quad \forall k,\\
&\text{C4: } \sum_{k=1}^{K} a_k^{(i,j)} \le 1, \quad \forall i, j,\\
&\text{C5: } \varphi = \frac{N\left(\widetilde{R}(k) \ge 0.3\right)}{K} - 0.9 \ge 0, \quad \forall k,\\
&\text{C6: } \sum_{i=1}^{N} u_{(i,j)} \le 1, \quad \forall j, \qquad \sum_{j=1}^{N} u_{(i,j)} \le 1, \quad \forall i,\\
&\text{C7: } u_{(i,j)}, a_k^{(i,j)} \in \{0,1\}, \quad \forall k, i, j,
\end{aligned} \tag{22}$$

where $\mathbf{p} = \{p_{\text{RN}}^{j}\}$, $\mathbf{u} = \{u_{(i,j)}\}$, and $\mathbf{a} = \{a_k^{(i,j)}\}$, subject to $k \in \{1,\ldots,K\}$, $i \in \{1,\ldots,N\}$, and $j \in \{1,\ldots,N\}$. Constraint C1 limits the transmit power of RN under p_{RN}; C2 denotes the nonnegative of transmit power on each subchannel; C3 represents the minimum security requirement guarantee of PMU k; C5 represents the requirement of fairness; C6 means each subchannel is pairing with no more than one other subchannels; C4 and C7 show that each subchannel pair is occupied by one PMU at most.

3. JRASSFA Scheduling Algorithm

JRASSFA scheduling algorithm consists of three subalgorithms: powering allocation based on CPSO algorithm, subchannel allocation based on B_CPSO algorithm, and subchannel pairing algorithm. These three subalgorithms are joint to optimize (21), aiming to maximize the SSR by appropriate power allocation, subchannel allocation, and subchannel pairing. Moreover, in this section, two subchannel pairing algorithms are presented: CHA algorithm and suboptimal subchannel pairing algorithm.

3.1. Powering Allocation Based on CPSO Algorithm. In this section, we first introduce particle swarm optimization (PSO) algorithm. PSO is a swarm intelligence algorithm that models social behavior to guide swarms of particles towards the most promising regions of the search space and has been proved to be efficient in solving engineering problems. The basic idea of PSO algorithm is to find an optimal solution by sharing information among individuals in the group. The standard form for PSO can be given in [17]

$$v_m^{l+1} = \varpi\left[v_m^{l} + c_1 \partial_m^{l}\left(x_m^{\text{best},l} - x_m^{l}\right) + c_2 \beta_m^{l}\left(x_{\text{swarm}}^{\text{best},l} - x_m^{l}\right)\right],$$
$$x_m^{l+1} = x_m^{l} + v_m^{l+1}, \tag{23}$$

where x_m represents the position of particle m, $m \in \{1,\ldots,M\}$, v_m is the velocity of particle m, l is the current iteration number, and ∂_m^{l} and β_m^{l} are random numbers with value $[0,1]$, which means the randomness of stochastic behavior. c_1 and c_2 denote learning factors, which represent the individual cognition ability and interaction of society, respectively, $x_m^{\text{best},l}$ represents the optimal position searched by particle m, and $x_{\text{swarm}}^{\text{best},l}$ represents the optimal position of entire swarm. In order to guarantee convergence, inertia weight factor ϖ is introduced, which is defined by

$$\varpi = \frac{2}{\left|2 - \omega - \sqrt{\omega^2 - 4\omega}\right|}, \tag{24}$$

where $\omega = c_1 + c_2 > 4$. c_1 and c_2 are set as 2.05 usually. Next we will discuss the solution of the above complicated mixed integer problem mentioned in (21).

In 2010, Kim et al. proposed a simple and efficient constrained PSO (CPSO) for engineering optimization problems containing various constraints and mixed integer-discrete-continuous type of design variables [18]. CPSO is constrained PSO algorithm which is used to solve the problem subject to constrained conditions. In this paper, we will use CPSO algorithm to solve our power allocation problem in the case of given $(\mathbf{u}^*, \mathbf{a}^*)$. Equations (21) and (22) can be formulated to standard form of CPSO as follows:

$$\min f(p_m) = -\sum_{k=1}^{K} f_k(\chi_k),$$
$$\chi_k = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} u^{*}_{(i,j)} a^{*(i,j)}_{k} R_{\sec,k,i}^{j}}{\sum_{i=1}^{N}\sum_{j=1}^{N} u^{*}_{(i,j)} a^{*(i,j)}_{k} R_{k,i}^{j}} \tag{25}$$

subject to following constraints:

$$\begin{aligned}
h_1(\mathbf{p}_m) &= \sum_{j=1}^{N} p_{\mathrm{RN}}^{j} - p_{\mathrm{RN}} \le 0, \\
h_2(\mathbf{p}_m) &= -p_{\mathrm{RN}}^{j} \le 0, \quad \forall j, \\
h_3(\mathbf{p}_m) &= Q(k) - \chi_k \le 0, \quad \forall k, \\
h_4(\mathbf{p}_m) &= 0.9 - \frac{N\left(\widetilde{R}(k) \ge 0.3\right)}{K} \le 0, \quad \forall k,
\end{aligned} \tag{26}$$

where $\mathbf{p}_m$ is the power of each article m and each $\mathbf{p}_m$ is N-dimensional vector. Next we convert the original constrained optimization problem into an unconstrained problem:

$$\min \hbar(\mathbf{p}_m) = \begin{cases} \widehat{h}(\mathbf{p}_m) = h_{\max}(\mathbf{p}_m), & \text{if } h_{\max}(\mathbf{p}_m) > 0 \\ \widehat{f}(\mathbf{p}_m) = a\tan\left[f(\mathbf{p}_m)\right] - \dfrac{\pi}{2}, & \text{otherwise}, \end{cases} \tag{27}$$

where $h_{\max}(\mathbf{p}_m) = \max[h_1(\mathbf{p}_m), \ldots, h_4(\mathbf{p}_m)]$ and $\hbar(\mathbf{p}_m)$ is the fitness function.

Next, we will rewrite (23) according to power allocation variable $\mathbf{p}$:

$$\begin{aligned}
\mathbf{v}_m^{l+1} &= \varpi\left[\mathbf{v}_m^{l} + c_1\partial_m^{l}\left(\mathbf{p}_m^{\mathrm{best},l} - \mathbf{p}_m^{l}\right) + c_2\beta_m^{l}\left(\mathbf{p}_{\mathrm{swarm}}^{\mathrm{best},l} - \mathbf{p}_m^{l}\right)\right], \\
\mathbf{p}_m^{l+1} &= \mathbf{p}_m^{l} + \mathbf{v}_m^{l+1},
\end{aligned} \tag{28}$$

where $\mathbf{p}_m^l$ and $\mathbf{v}_m^l$ are the current position (the current position represents power allocation here) and the velocity of particle m, respectively, and $\mathbf{p}_m^l$ and $\mathbf{v}_m^l$ are both N-dimensional vectors. $\mathbf{p}_m^{\mathrm{best},l}$ represents the optimal power allocation of individual particle m and $\mathbf{p}_{\mathrm{swarm}}^{\mathrm{best},l}$ represents the optimal power allocation of entire swarm. $\mathbf{p}_m^{\mathrm{best},l}$ and $\mathbf{p}_{\mathrm{swarm}}^{\mathrm{best},l}$ can be updated by

$$\begin{aligned}
\mathbf{p}_m^{\mathrm{best},l} &= \arg\min\left\{\hbar\left(\mathbf{p}_m^{j}\right),\ 0 \le j \le l\right\}, \\
\mathbf{p}_{\mathrm{swarm}}^{\mathrm{best},l} &= \arg\min\left\{\hbar\left(\mathbf{p}_m^{j}\right),\ \forall m\right\}.
\end{aligned} \tag{29}$$

In order to understand easily, Figure 3 shows the search process under CPSO, which could be described as follows: in the initial stages of iteration, all the particles in nonfeasible region are trying to move to a feasible region which satisfy the constraint conditions and then find the optimal solution which is satisfied with both the objective function and the constraint conditions in the feasible region.

The brief power allocation algorithm is given in Algorithm 1.

3.2. Subchannel Allocation Based on B_CPSO Algorithm. Because the value of subchannel assignment variable $a_k^{(i,j)}$ in (21) can only be 0 and 1, we should therefore find an improved PSO algorithm to solve this problem. In [19], Zhang et al. firstly proposed a binary PSO (BPSO) algorithm for binary code forms in 1997. Based on [18, 19], we propose a B_CPSO algorithm to solve our subchannel allocation problem. Given subchannel pairing $\mathbf{u}^*$ (reuse the value in Section 3.1) and power allocation $\mathbf{p}^*$ (reuse the power allocation result of Section 3.1), the subchannel allocation $\mathbf{a}$ can be obtained by B_CPSO algorithm. Next we formulate (21) and (22) to standard form of CPSO under subchannel allocation as follows:

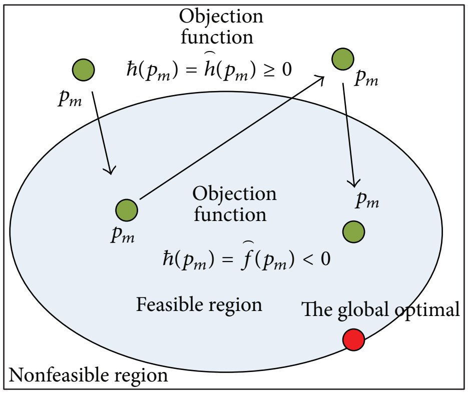


Figure 3: Change graph of objective function.

$$\begin{aligned}
\min f(\mathbf{a}_m) &= -\sum_{k=1}^{K} f_k(\chi_k), \\
\chi_k &= \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} u^{*}{}_{(i,j)} a_k^{(i,j)} R_{\sec,k,i}^{j}}{\sum_{i=1}^{N}\sum_{j=1}^{N} u^{*}{}_{(i,j)} a_k^{(i,j)} R_{k,i}^{j}}
\end{aligned} \tag{30}$$

subject to the following constraints:

$$\begin{aligned}
h_1(\mathbf{a}_m) &= Q(k) - \chi_k \le 0, \\
h_2(\mathbf{a}_m) &= \sum_{k=1}^{K} a_k^{(i,j)} - 1 \le 0, \quad \forall i, j, \\
h_3(\mathbf{a}_m) &= 0.9 - \frac{N\left(\widetilde{R}(k) \ge 0.3\right)}{K} \le 0, \quad \forall k,
\end{aligned} \tag{31}$$

where $\mathbf{a}_m$ is the subchannel allocation of each article m and each $\mathbf{a}_m$ is a $[K \times N]$-dimensional vector. The search process of B_CPSO is similar to CPSO; therefore, we only present the difference between them due to space limit.

First we rewrite velocity part of (23) according to subchannel allocation variable $\mathbf{a}$:

$$\mathbf{v}_m^{l+1} = \varpi\left[\mathbf{v}_m^{l} + c_1\partial_m^{l}\left(\mathbf{a}_m^{\mathrm{best},l} - \mathbf{a}_m^{l}\right) + c_2\beta_m^{l}\left(\mathbf{a}_{\mathrm{swarm}}^{\mathrm{best},l} - \mathbf{a}_m^{l}\right)\right], \tag{32}$$

where $\mathbf{v}_m$ is $[K \times N]$-dimensional vector of velocity for each article m in this section. The only difference between B_CPSO and CPSO is that a conversion needs to be done in the process

```
Begin
Step 1. Particle swarm initiation.
    Denote the particle swarm as $\Pi = \{1, \ldots, M\}$, then their positions and velocities are
    respectively initialized as $\mathbf{p}_m^0 = \{p_m^{0,1}, p_m^{0,2}, \ldots, p_m^{0,N}\}$ and $\mathbf{v}_m^0 = \{v_m^{0,1}, v_m^{0,2}, \ldots, v_m^{0,N}\}$
    for each particle, where $\forall m \in \Pi$.
    Initialize subchannel assignment variable and subchannel pairing variable
    $(\mathbf{u}^*, \mathbf{a}^*)$, which can be given randomly.
    Initialize each personal optima $\mathbf{p}_m^{\text{best}.0} = \mathbf{p}_m^0$.
    Initialize global optima $\mathbf{p}_{\text{swarm}}^{\text{best}.0} = \arg\min\{\hbar(\mathbf{p}_m^0), \forall m\}$.
Step 2. Begin to search the global optima.
    while $(l \le l_{\max})$ do
     Update $\mathbf{v}_m^l$ and $\mathbf{p}_m^l$ for each particle according to (28).
       for $(m = 1 : M)$
         if $\hbar(\mathbf{p}_m^l) < \hbar(\mathbf{p}_m^{\text{best},(l-1)})$
          then $\mathbf{p}_m^{\text{best},(l)} = \mathbf{p}_m^l$, else $\mathbf{p}_m^{\text{best},(l)} = \mathbf{p}_m^{l-1}$
       end for
         $\mathbf{p}^* = \arg\min\{\hbar(\mathbf{p}_m^l), \forall m\}$
         if $\hbar(\mathbf{p}^*) < \hbar(\mathbf{p}_{\text{swarm}}^{\text{best},(l-1)})$
          then $\mathbf{p}_{\text{swarm}}^{\text{best},(l)} = \mathbf{p}^*$, else $\mathbf{p}_{\text{swarm}}^{\text{best},(l)} = \mathbf{p}_{\text{swarm}}^{l-1}$
       end while
Step 3. Output result
      Output the best position $\mathbf{p}_{\text{swarm}}^{\text{best}}$ as the optimal power allocation scheme.
```

Algorithm 1: Power allocation algorithm based on CPSO.

of velocity updating, a Sigmoid function is introduced to update velocity after updating (32) in B_CPSO [19]:

$$\operatorname{sig}(\mathbf{v}_m) = \frac{1}{1 + e^{-\mathbf{v}_m}} \qquad (33)$$

and then each particle updates current subchannel allocation according to following equation:

$$\mathbf{a}_m^{l+1} = \begin{cases} 0, & \lambda_m^l \ge \operatorname{sig}\left(\mathbf{v}_m^{l+1}\right) \\ 1, & \lambda_m^l \le \operatorname{sig}\left(\mathbf{v}_m^{l+1}\right), \end{cases} \qquad (34)$$

where λ_m^l is a random number with value in $[0, 1]$. The brief subchannel allocation algorithm is given in Algorithm 2.

3.3. Subchannel Pairing Based on CHA Algorithm. The remaining problem is the subchannel pairing, which can be formulated as

$$\max_u \frac{\sum_{i=1}^N \sum_{j=1}^N u_{(i,j)} a^{*(i,j)}_k R^j_{\text{sec},k,i}\left(p^{*j}_{\text{RN}}\right)}{\sum_{i=1}^N \sum_{j=1}^N u_{(i,j)} a^{*(i,j)}_k R^j_{k,i}\left(p^{*j}_{\text{RN}}\right)}, \qquad (35)$$

where $a^{*(i,j)}_k$ and p^{*j}_{RN} are the optimal results in the above discussion. This is a standard *two-dimensional assignment* problem, inspired by [20, 21]; the optimal subchannel pairing can be obtained by the classic Hungarian algorithm. The complexity of the proposed CHA algorithm is $O(N^3)$.

3.4. Suboptimal Subchannel Pairing Algorithm. The previous subsection presents a subchannel pairing algorithm based on CHA, the complexity of which may will be high with large values of K and N. In this subsection, we propose a suboptimal subchannel algorithm to reduce the computational complexity by decomposing the subchannel pairing into two phases: MA phase and BC phase.

Subchannel pairing for given power allocation and subchannel allocation: subchannel pairing for PMU k in the MA phase is in accordance with

$$\hat{i} = \arg\max_{i \in S_k} \Delta_k, \qquad (36)$$

where S_k is the set of subchannels occupied by PMU k and Δ_k is defined by the following:

$$\begin{gathered} \Delta_k = \frac{(G_k) + (H_k)}{L_k}, \\ G_k = p^i_{A_k}\left|g^i_{A_k,\text{RN}}\right|^2 - p^i_{A_k}\left|g^i_{A_k,E}\right|^2, \\ H_k = p^i_{B_k}\left|g^i_{B_k,\text{RN}}\right|^2 - p^i_{B_k}\left|g^i_{B_k,E}\right|^2, \\ L_k = p^i_{A_k}\left|g^i_{A_k,\text{RN}}\right|^2 + p^i_{B_k}\left|g^i_{B_k,\text{RN}}\right|^2. \end{gathered} \qquad (37)$$

In the BC phase, subchannel j can be selected as

$$\hat{j} = \arg\max_{j \in S_k} \frac{R^j_{\text{sec},k,\hat{i}}}{R^j_{k,\hat{i}}}, \qquad (38)$$

where subchannel $\hat{i}$ in BC phase is paired with subchannel $\hat{j}$ in MA phase; that is, $u_{(\hat{i},\hat{j})} = 1$. The computational complexity of the suboptimal subchannel pairing algorithm is $O(2N)$, which is much lower than the CHA algorithm, especially in a larger N.

```
Begin
Step 1. Particle swarm initiation.
    Denote the particle swarm as $\Pi = \{1, \ldots, M\}$, Their positions and velocities are
    respectively initialized as $\mathbf{a}_m^0 = \{a_m^{0,1\times 1}, a_m^{0,1\times 2}, \ldots, a_m^{0,2\times 1}, a_m^{0,2\times 2}, \ldots, a_m^{0,K\times N}\}$ and
    $\mathbf{v}_m^0 = \{v_m^{0,1\times 1}, v_m^{0,1\times 2}, \ldots, v_m^{0,2\times 1}, v_m^{0,2\times 2}, \ldots, v_m^{0,K\times N}\}$ for each particle, where $\forall m \in \Pi$.
  Initialize subchannel assignment variable and power allocation variable $(\mathbf{u}^*, \mathbf{p}^*)$.
  Initialize each personal optima $\mathbf{a}_m^{\text{best}.0} = \mathbf{a}_m^0$.
  Initialize global optima $\mathbf{a}_{\text{swarm}}^{\text{best}.0} = \arg\min\{\hbar(\mathbf{a}_m^0), \forall m\}$.
Step 2. Begin to search the global optima.
  while $(l \le l_{\max})$ do
   Update $\mathbf{v}_m^l$ and $\mathbf{a}_m^l$ for each particle according to (32), (33), and (34).
      for $(m = 1 : M)$
        if $\hbar(\mathbf{a}_m^l) < \hbar(\mathbf{a}_m^{\text{best},(l-1)})$
          then $\mathbf{a}_m^{\text{best},(l)} = \mathbf{a}_m^l$, else $\mathbf{a}_m^{\text{best},(l)} = \mathbf{a}_m^{l-1}$
      end for
      $\mathbf{a}^* = \arg\min\{\hbar(\mathbf{a}_m^l), \forall m\}$
      if $\hbar(\mathbf{a}^*) < \hbar(\mathbf{a}_{\text{swarm}}^{\text{best},(l-1)})$
        then $\mathbf{a}_{\text{swarm}}^{\text{best},(l)} = \mathbf{a}^*$, else $\mathbf{a}_{\text{swarm}}^{\text{best},(l)} = \mathbf{a}_{\text{swarm}}^{l-1}$
      end while
Step 3. Output result
    Output the best position $\mathbf{a}_{\text{swarm}}^{\text{best}}$ as the optimal subchannel allocation scheme.
```

Algorithm 2: Subchannel allocation algorithm based on B_CPSO.

4. Simulation Result

We consider one relay with multiusers and one eavesdropper in this simulation. The legitimate users are uniformly located on a circle centered at the RN and with radius of 50 meters. The eavesdropper is assumed to locate at a distance of $d = 150$ m from the RN except in Figure 4. All users have the maximum power constraints 400 mW. The noise power is defined as $\sigma^2 = BN_0$, where $B = 150$ kHz denotes the bandwidth for each subchannel and $N_0 = 10^{-21}$ mW/Hz denotes the AWGN power spectral density. There are $N = 50$ subchannels assumed in the OFDM bandwidth, and the number of PMUs is 18. The flat fading channel gains are modeled as i.i.d. exponentially distributed random variables in a six-tap channel; the path loss exponent is set to 3.

4.1. Average SSR versus Eavesdropper Distance. Figure 4 illustrates the average SSR of *JRASSFA using CHA* (JRASSFA_C), *JRASSFA using suboptimal subchannel pairing* (JRASSFA_S), and *equal power allocation* (EPA) [22] algorithms for different security preference parameters, assuming that the eavesdropper exists between 100 m and 450 m from the RN. We can see that the average SSR of PMUs increases when the eavesdropper is far away from the RN, particularly when the eavesdropper is far away from relay node at a distance within 250 m. There are two reasons that can explain this result: (1) the farther the distance between eavesdroppers and relay nodes, the worse the SINR eavesdropper received and thus the less the communication information the eavesdropper eavesdrop, so the security satisfaction ratio of users increases; (2) the path loss is a major factor deteriorating the received signal of the eavesdropper within 250 m in the simulation, so the average SSR of PMUs increases rapidly at a distance within 250 m. Moreover, smaller β_k result in higher performance of SSR, because user has lower security requirement with a smaller β_k; in other words, information security is not important to these users with a smaller β_k. In Figure 4, we can also find that the JRASSFA_S and EPA algorithm perform worse than JRASSFA_C, especially within 200 m.

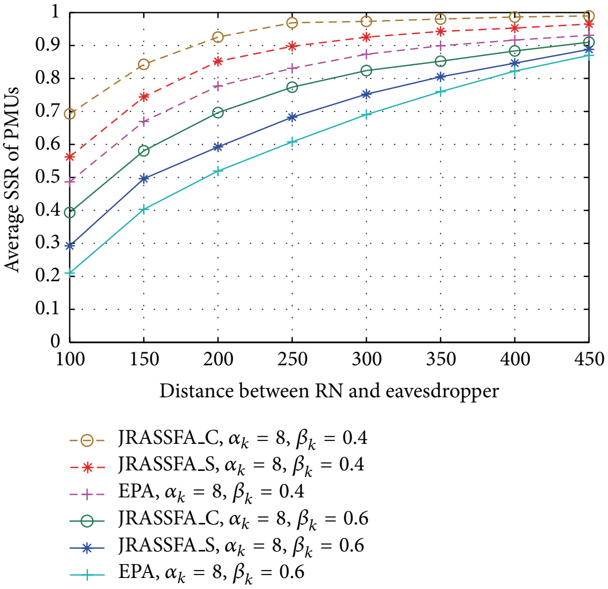


Figure 4: Average SSR versus distance.

4.2. Secrecy Ratio versus Individual PMU. Figure 5 shows the effectiveness of our proposed algorithm in security

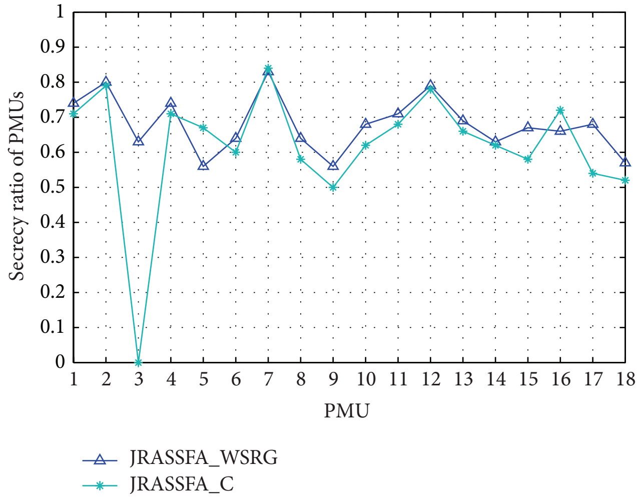


Figure 5: Secrecy ratio versus PMU k.

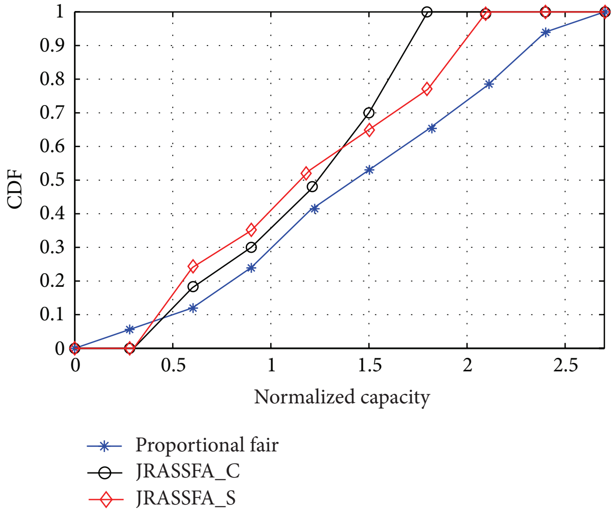


Figure 6: CDF versus normalized capacity.

requirement guarantee in the case of $\zeta_{\mathrm{VIP}}^{\min} = 0.7$, $\zeta_{\mathrm{IP}}^{\min} = 0.5$, $\zeta_{\mathrm{NP}}^{\min} = 0.2$. Assume that PMU 1~PMU 4 are VIPs, PMU 5~PMU 8 are IPs, and others are NPs; *JRASSFA without security requirement guarantee* (JRASSFA_WSRG) and JRASSFA_C are compared in Figure 5. We first observe that the proposed JRASSFA_C gets zero in PMU 3, because when the secrecy ratio of PMU 3 is less than its security tolerability, the subchannel could not be allocated to PMU 3 in order to guarantee the communication security. But in JRASSFA_WSRG, this issue is ignored. We also observe that the average secrecy ratio in JRASSFA_C is less than that in JRASSFA_WSRG. This is because, in JRASSFA_C, subchannels should have been allocated to PMU 3 in order to get the maximum secrecy ratio originally; however, since the secrecy ratio of PMU 3 could not reach the security tolerability, these subchannels are allocated to other PMUs that can reach the security tolerability, but these other PMUs could not get the maximum secrecy ratio on these subchannels, which means the average secrecy ratio is lower down. In this case, we get a tradeoff between secrecy ratio maximization and information security.

4.3. CDF versus Normalized Capacity. Figure 6 shows the fairness performance of JRASSFA_C, JRASSFA_S, and proportional fair (PF) algorithm [23]. From this simulation, we can find that the ratio of PMUs whose normalized capacity is larger than 0.3 is 90%, which is consistent with the fairness index we defined in Section 2.4. Compared with proportional fair algorithm, the normalized capacity of the proposed algorithms is concentrated in 0.5~2; this is to say, most of capacity of users is concentrated within a small range and, thus, most of users can get rational transfer capacities to avoid the polarization. Figure 6 indicates that the fairness can be significantly improved in our proposed JRASSFA_C and JRASSFA_S algorithms.

4.4. Average SSR versus Total Transmit Power of RN. Figure 7 shows the better performance of the proposed JRASSFA_C and JRASSFA_S in terms of the average SSR versus p_{RN}, compared to the EPA algorithm. From this simulation result, we can find that the average SSR increases with larger transmit power of RN, because PMUs can get better SINR than eavesdropper with larger transmit power of RN. However, the SSR is difficult to improve obviously when $p_{\mathrm{RN}} > 1600\,\mathrm{mW}$ and this indicates that unlimited increase of the transmit power does not improve SSR obviously.

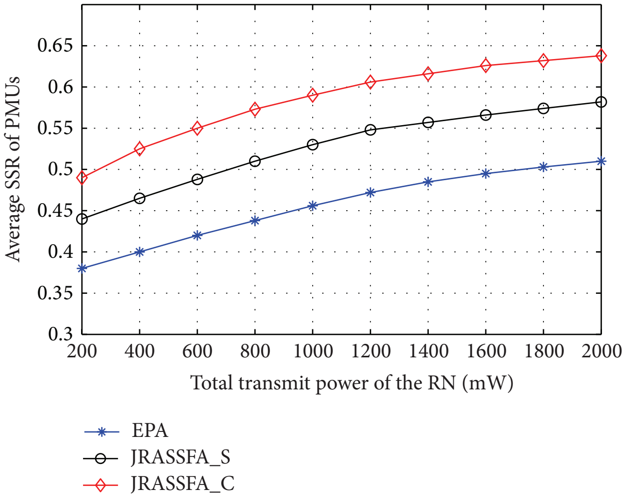


Figure 7: Average SSR versus total transmit power of RN.

4.5. Average SSR versus Total Transmit Power of User. Figure 8 depicts the average SSR versus the total transmit power of user and we can see that the SSR increases with the increased transmit power of user. The reason for this result is that the increased transmit power of user leads to larger SNR than eavesdropper. Thus it will cause increase in the SSR. Moreover, our proposed JRASSFA_C and JRASSFA_S provide the better performance compared to the EPA algorithm. Still,

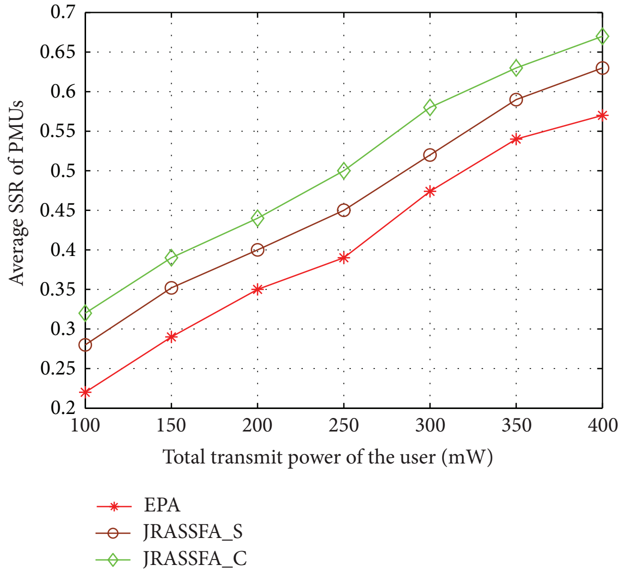


Figure 8: Average SSR versus total transmit power of user.

the JRASSFA_C outperforms the JRASSFA_S. However, we can get a tradeoff between algorithm complexity and SSR performance due to the fact that the JRASSFA_S has lower complexity.

5. Conclusions

In this paper, we have investigated the joint resource management for orthogonal frequency division multiple access (OFDMA) security two-way relay networks in next-generation wireless sensor networks. A novel security satisfaction ratio model is introduced as the objection function to evaluate the information security of users. Meanwhile, in order to guarantee diverse information security requirements and fairness for different users, secrecy ratio and CDF are also presented in this paper. We model this security resource optimization problem as a mixed integer programming problem and then solve it in constraint particle swarm optimization (CPSO), binary CPSO (B_CPSO), and classic Hungarian algorithm (CHA) method, respectively. Moreover, a suboptimal subchannel pairing algorithm is presented to reduce the computational complexity of subchannel pairing CHA algorithm.

Simulation results indicate that JRASSFA_C and JRASSFA_S provide better security performance than the other two algorithms. However, a number of open problems still remain. Indeed, the expected value of secrecy ratio is different among different users, but in this paper we only consider the same expected value among different users in order to simplify the analysis. In addition, how to improve the secrecy ratio in order to satisfy users' security tolerability and, furthermore, to avoid the interruption of transmission under the total power constraint should be further studied in the future.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research is supported by the 863 Project no. 2014AA01A701, the Three Links and Two Platforms of Beijing Education Network and Information Center, and the WLAN Schievement Transformation Based on SDN of Beijing Municipal Commission of Science and Technology, National Natural Science Foundation of China (61271179, 61101109).

References

[1] H. Zhang, X. Chu, W. Guo, and S. Wang, "Coexistence of Wi-Fi and heterogeneous small cell networks sharing unlicensed spectrum," *IEEE Communications Magazine*, 2014, http://www.researchgate.net/publication net/publication/268218888.

[2] T. Cui, F. Gao, T. Ho, and A. Nallanathan, "Distributed space-time coding for two-way wireless relay networks," *IEEE Transactions on Signal Processing*, vol. 57, no. 2, pp. 658–671, 2009.

[3] K. Jitvanichphaibool, R. Zhang, and Y. C. Liang, "Optimal resource allocation for two-way relay-assisted OFDMA," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3311–3321, 2009.

[4] J. A. Aldhaibani, A. Yahya, R. B. Ahmad, N. Omar, and Z. G. Ali, "Effect of relay location on two-way DF and AF relay for multi-user system in LTE-A cellular networks," in *Proceedings of the IEEE Business Engineering and Industrial Applications Colloquium (BEIAC '13)*, pp. 380–385, April 2013.

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

[6] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4529–4542, 2009.

[7] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8115–8130, 2013.

[8] R. F. Wyrembelski, M. Wiese, and H. Boche, "Strong secrecy in bidirectional broadcast channels with confidential messages," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 324–334, 2013.

[9] S. Kim, W.-Y. Shin, and K. Ishibashi, "The Gaussian two-way relay channel with wiretapper," in *Proceedings of the 45th Asilomar Conference on Signals, Systems and Computers (ASILOMAR '11)*, pp. 1987–1991, Pacific Grove, Calif, USA, November 2011.

[10] H. Long, W. Xiang, J. Wang, Y. Zhang, and W. Wang, "Cooperative jamming and power allocation in three-phase two-way relaying wiretap systems," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '13)*, pp. 4175–4179, April 2013.

[11] H.-M. Wang, Q. Yin, and X.-G. Xia, "Improving the physical-layer security of wireless two-way relaying via analog network coding," in *Proceedings of the 54th Annual IEEE Global Telecommunications Conference: Energizing Global Communications (GLOBECOM '11)*, pp. 1–6, Houston, Tex, USA, December 2011.

[12] H. Zhang, C. Jiang, N. C. Beaulieu, X. Chu, X. Wen, and M. Tao, "Resource allocation in spectrum-sharing OFDMA

femtocells with heterogeneous services," *IEEE Transactions on Communications*, vol. 62, no. 7, pp. 2366–2377, 2014.

[13] H. Lin, M. Chatterjee, S. K. Das, and K. Basu, "ARC: an integrated admission and rate control framework for competitive wireless CDMA data networks using noncooperative games," *IEEE Transactions on Mobile Computing*, vol. 4, no. 3, pp. 243–257, 2005.

[14] M. Abadi and S. Jalili, "Using binary particle swarm optimization for minimization analysis of large-scale network attack graphs," *Scientia Iranica*, vol. 15, no. 6, pp. 605–619, 2008.

[15] Y.-L. Kuo and E. H.-K. Wu, "Noncooperative admission control for differentiated services in IEEE 802.11 WLANs," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '04)*, vol. 5, pp. 2981–2986, November-December 2004.

[16] Z. M. Lu, Y. Yang, X. M. Wen, Y. Ju, and W. Zheng, "A cross-layer resource allocation scheme for ICIC in LTE-Advanced," *Journal of Network and Computer Applications*, vol. 34, no. 6, pp. 1861–1868, 2011.

[17] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proceedings of the IEEE International Conference on Neural Networks (ICNN '95)*, pp. 1942–1948, December 1995.

[18] T. H. Kim, I. Maruta, and T. Sugie, "A simple and efficient constrained particle swarm optimization and its application to engineering design problems," *Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science*, vol. 224, no. 2, pp. 389–400, 2010.

[19] H. Zhang, H. Xing, X. Chu, A. Nallanathan, W. Zheng, and X. Wen, "Secure resource allocation for OFDMA two-way relay networks," in *Proceedings of the IEEE Global Communications Conference (GLOBECOM '12)*, pp. 3649–3654, Anaheim, Calif, USA, December 2012.

[20] H. Zhang, Y. Liu, and M. Tao, "Resource allocation with subcarrier pairing in OFDMA two-way relay networks," *IEEE Wireless Communications Letters*, vol. 1, no. 2, pp. 61–64, 2012.

[21] G. A. S. Sidhu, F. Gao, W. Chen, and A. Nallanathan, "A joint resource allocation scheme for multiuser two-way relay networks," *IEEE Transactions on Communications*, vol. 59, no. 11, pp. 2970–2975, 2011.

[22] Y. Shim, H. Park, and H. M. Kwon, "Optimal power allocation for two-way decode-and-forward relay networks with equal transmit power at source nodes," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '13)*, pp. 3335–3340, April 2013.

[23] P. Tarasak and S. M. Sumei, "Joint cooperative diversity and proportional fair scheduling in OFDMA relay systems," in *Proceedings of the 68th IEEE Vehicular Technology Conference*, pp. 1–5, September 2008.

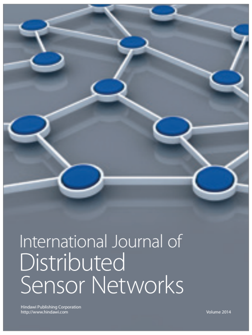
The Scientific World Journal

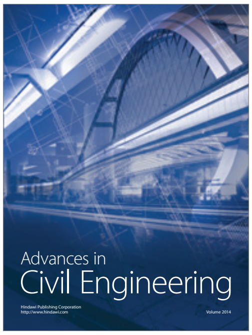
International Journal of
Rotating Machinery

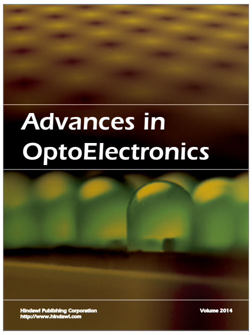
Journal of
Engineering

Journal of
Sensors

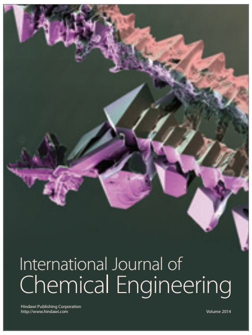
Advances in
Mechanical Engineering


International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering

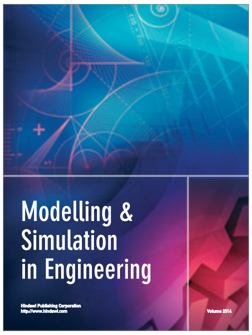

Advances in
OptoElectronics

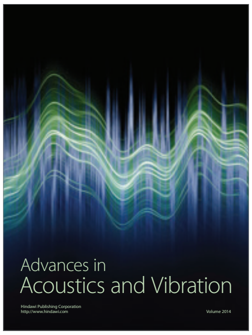
Journal of
Robotics


International Journal of
Chemical Engineering

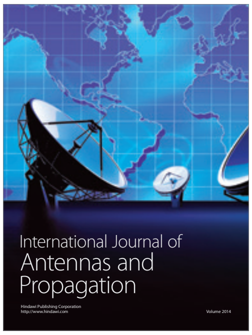
VLSI Design

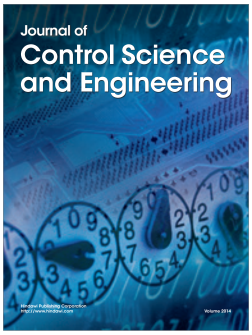
International Journal of
Navigation and Observation

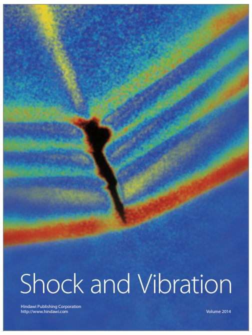

Modelling &
Simulation
in Engineering


Advances in
Acoustics and Vibration

Active and Passive
Electronic Components


International Journal of
Antennas and Propagation


Journal of
Control Science and Engineering


Shock and Vibration

Journal of
Electrical and Computer Engineering