Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 587104, 9 pages
http://dx.doi.org/10.1155/2015/587104

Research Article

Energy-Efficient Relay Selection Scheme for Physical Layer Security in Cognitive Radio Networks

Li Jiang and Hui Tian

State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Correspondence should be addressed to Hui Tian; tianhui@bupt.edu.cn

Received 24 October 2014; Accepted 29 December 2014

Academic Editor: Elmetwally Elabbasy

Security is a critical issue in cognitive radio (CR) relay networks. Most previous work concentrates on maximizing secrecy capacity (SC) as a criterion to guarantee the security requirements in CR relay networks. However, under the requirement of "green" radio communication, the energy consumption is largely ignored. This paper proposes a relay selection scheme which jointly considers the best relay selection and dynamic power allocation in order to maximize SC and to minimize energy consumption. Moreover, we consider finite-state Markov channels and residual relay energy in the relay selection and power allocation process. Specifically, the formulation of the proposed relay selection and power allocation scheme is based on the restless bandit problem, which is solved by the primal-dual index heuristic algorithm. Additionally, the obtained optimal relay selection policy has an indexability property that dramatically reduces the computational complexity. Numerical results are presented to show that our proposed scheme has the maximum SC and minimum energy consumption compared to the existing ones.

1. Introduction

Cognitive radio (CR) is a promising technology to improve the utilization efficiency of the wireless spectrum resources [1]. In CR networks, the secondary users (SUs) are allowed to transmit concurrently on the same spectrum bands with the licensed primary users (PUs), as long as the resulting interference power at the PUs' receivers is kept below the interference temperature limit. Such an operation mode is known as spectrum underlay [2]. In the underlay paradigm, the performance of the SUs degrades significantly in fading environments due to the constraints on their transmission power. One of the efficient ways to enhance the performance of SUs is to use cooperative relaying, which is capable of mitigating wireless channel fading [3], saving transmission power [4, 5], and increasing capacity [6–8] through multipath propagation offered by cooperative nodes.

The security concerns in CR relay networks have been attracting continuously growing attention [9]. Due to the open nature of wireless transmission medium, the CR relay networks are particularly susceptible to eavesdropping [10]. Traditionally, the cryptographic techniques have been employed to protect the communication confidentiality against eavesdropping attacks, which, however, increases the computational and communication overheads and introduces additional system complexity for the secret key distribution and management.

As an alternative, physical layer security has emerged as a new secure communication method to defend against eavesdroppers by exploiting the physical characteristics of wireless channels. This work was initiated by Wyner in [11], in which the notion of secrecy capacity is developed from an information-theoretical prospective and shown to be the difference in capacities between the main channel (i.e., the channel from the transmitter to the legitimate receiver) and the wiretap channel (i.e., the channel from the transmitter to the eavesdropper). It was proved in [12, 13] that if the wiretap channel is stronger than the main channel, the eavesdropper will succeed in intercepting the source information. Some recent work has been proposed to overcome this limitation by taking advantage of multiple-antenna [14–17] and cooperative relay [18–21] techniques. For instance, Pei et al. [14, 15] addressed the secrecy capacity optimization problem in multiple-input single-output (MISO) CR networks.

Kwon et al. [16] explored MISO CR systems where the SUs secure the PUs in return for permission to use the spectrum. Zhang et al. [17] proposed efficient algorithms to solve the secrecy capacity maximization problem in multiple-input multiple-output (MIMO) CR networks. Apart from this, Zou et al. [18] proposed user scheduling scheme to achieve multiuser diversity for improving the security level of cognitive transmissions. Sakran et al. [19] proposed a relay selection scheme in CR networks where the considered scheme selects a trusted decode and forward relay to assist SUs and maximize the secrecy capacity that is subjected to the interference power constraints at the PUs. The power allocation strategies for relays were introduced in [20] with the goal of maximizing the total secrecy capacity in CR networks. Authors in [21] studied the relay precoding scheme to improve the secrecy capacity of SUs in CR systems.

Notice that the aforementioned work [14–21] on CR networks addressed the issue of secrecy capacity maximization but did not take into account the energy consumption. In wireless networks, most wireless devices are powered by batteries with limited energy. The network lifetime is an important factor to characterize the performance of such networks. In order to prolong the network lifetime, the battery energy should be consumed efficiently. In CR relay networks, the improvement of energy consumption can be realized by reducing the transmission power and balancing energy consumption among relays. However, the reduction of transmission power leads to degradation of the secrecy capacity. Therefore, the secrecy capacity and the energy consumption should be jointly considered for efficient implementation of CR relay networks. In addition, most previous works for relay selection use the current observed channel conditions to make the relay selection decision for subsequent data transmission. However, this memoryless channel assumption is not realistic in the time-varying radio environments. Finite-state Markov models have been considered as an effective approach to characterize the time-varying nature of the radio environments.

In this paper we propose an energy-efficient relay selection scheme which jointly considers best relay selection and dynamic power allocation in order to maximize SC as well as to minimize energy consumption. The main contributions of this paper are summarized as follows.

(1) A scenario in which a secondary transmitter (S) communicates with a secondary destination (D) with the help of the best relay in the presence of different numbers of PUs and eavesdroppers is considered.

(2) An energy-efficient relay selection scheme which jointly considers best relay selection and dynamic power allocation is proposed to maximize SC and minimize energy consumption.

(3) In order to accurately describe the time-varying characteristic, the spectrum occupancy state, the channel state information (CSI) of the related channels, and residual relay energy are modeled as finite-state Markov model.

(4) The relay selection and dynamic power allocation scheme is formulated as restless bandit problem, which is solved by the primal-dual index heuristic algorithm. The obtained optimal relay selection policy has an indexability property that dramatically reduces the computational complexity. Simulation results show that the proposed scheme outperforms the existing one in terms of the achievable secrecy capacity and energy consumption.

The remainder of this paper is organized as follows. In Section 2, the system model is described. Section 3 formulates the relay selection and dynamic power allocation scheme as a restless bandit problem and solves the problem with the primal-dual index heuristic algorithm. Extensive simulation results are presented and analyzed for performance evaluation in Section 4. Finally, Section 5 concludes the paper.

2. System Model and Secrecy Capacity

We consider an underlay CR system with the coexistence of primary and secondary networks. As depicted in Figure 1, in the primary network, a primary transmitter (PT) communicates with M primary destinations (PDs) denoted by $\mathscr{PD} = \{\text{PD}_m \mid m \in \mathscr{M} = \{1, 2, \ldots, M\}\}$. Meanwhile, in the secondary network, a secondary transmitter (S) wants to send confidential information to a secondary destination (D) assisted by the best relay selected from the candidate relay set, $\mathscr{R} = \{R_n \mid n \in \mathscr{N} = \{1, 2, \ldots, N\}\}$, over the spectrum band that is licensed to the primary network. At the same time, K eavesdroppers, denoted by $E = \{E_k \mid k \in \mathscr{K} = \{1, 2, \ldots, K\}\}$, try to eavesdrop and intercept the message sent by S and relay nodes. A Rayleigh block-fading channel is assumed in this paper. We define $h_{S,D}$, h_{S,R_n}, h_{S,P_m}, h_{S,E_k}, $h_{R_n,D}$, h_{R_n,P_m}, and h_{R_n,E_k}, as the channel coefficient of S-D link, S-R_n link, S-P_m link, S-E_k link, R_n-D link, R_n-P_m link, and R_n-E_k link, respectively, where $n \in \mathscr{N}$, $m \in \mathscr{M}$, and $k \in \mathscr{K}$. In addition, the global channel state information (CSI) is assumed to be available, and even the eavesdroppers' channels are known when the eavesdropper is also a user of the secondary network, but it is not the intended destination for some particular confidential information [22, 23].

2.1. Cooperative Relaying Protocol and Secrecy Capacity. We consider the decode and forward (DF) relaying protocol with two stages. In the first stage, S transmits its encoded information with transmission power P_S to the relay nodes. In the second stage, the selected relay R_n reencodes the message and forwards it to D with transmission power P_{R_n}. Meanwhile, the eavesdroppers can overhear the information at the two stages due to the broadcast nature of wireless medium. For the secondary transmission in the presence of K eavesdroppers, the secrecy capacity is characterized as

$$C_S = \left[C_D - C_E\right]^+, \tag{1}$$

where $[x]^+ = \max(x, 0)$; C_D and C_E are the achievable rates at D and E, respectively. The achievable rate at D can be written as

$$C_D = \frac{1}{2}\log_2\left(1 + \frac{P_S\left|h_{S,D}\right|^2}{\sigma^2} + \frac{P_{R_n}\left|h_{R_n,D}\right|^2}{\sigma^2}\right). \tag{2}$$

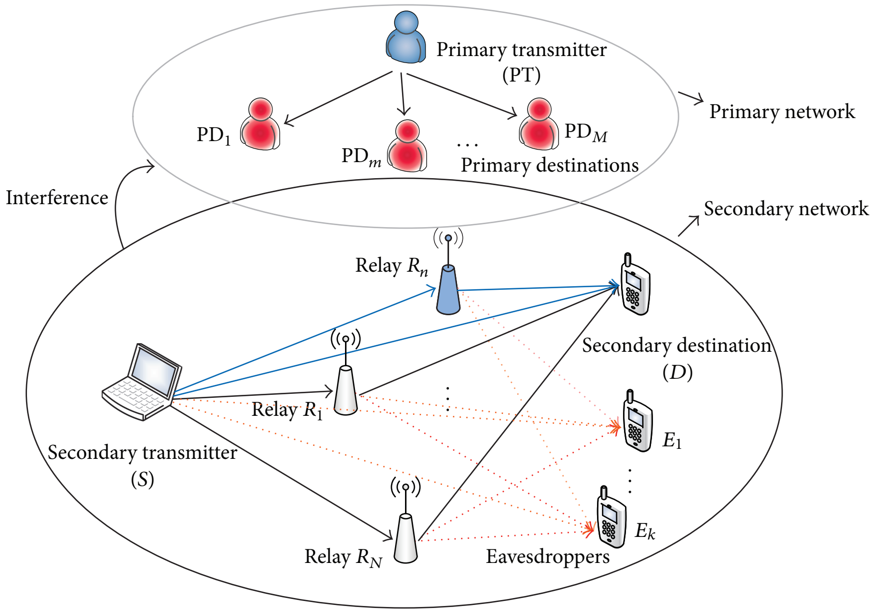


Figure 1: Coexistence of a primary network consisting of one primary transmitter (PT) and M primary destinations (PDs) with a secondary network consisting of one secondary transmitter (S), N relay nodes, and one secondary destination (D) in the presence of K eavesdroppers.

In this paper, we assume that K eavesdroppers independently perform their tasks to intercept the secondary transmission. The overall rate of the wiretap links is the maximum of individual rates achieved at K eavesdroppers. Thus, the overall rate can be obtained as

$$C_E = \max_{E_k \in E} \frac{1}{2} \log_2 \left(1 + \frac{P_S \left| h_{S,E_k} \right|^2}{\sigma^2} + \frac{P_{R_n} \left| h_{R_n,E_k} \right|^2}{\sigma^2} \right), \quad (3)$$

where σ^2 is the noise power of all the links.

To guarantee the QoS of PDs, the transmission power of S and R_n is limited by the interference temperature limit P_{th}; that is,

$$P_S \leq \min \left(P_{T,\max}, \frac{P_{\text{th}}}{\left| h_{S,P_1} \right|^2}, \frac{P_{\text{th}}}{\left| h_{S,P_2} \right|^2}, \ldots, \frac{P_{\text{th}}}{\left| h_{S,P_M} \right|^2} \right), \quad (4)$$

$$P_{R_n} \leq \min \left(P_{T,\max}, \frac{P_{\text{th}}}{\left| h_{R_n,P_1} \right|^2}, \frac{P_{\text{th}}}{\left| h_{R_n,P_2} \right|^2}, \ldots, \frac{P_{\text{th}}}{\left| h_{R_n,P_M} \right|^2} \right), \quad (5)$$

where $P_{T,\max}$ is the maximum transmission power limit.

2.2. Finite-State Markov Channel Model. In this paper, the finite-state Markov channel (FSMC) model is used to characterize the Rayleigh block-fading channel. The range of the channel gain is quantized into L discrete levels, each corresponds with a state in the Markov chain. Specifically, the channel gain of the considered links is modeled as a random variable $\sigma_{ij}(t)$ evolving according to a finite state Markov chain which is characterized by a L-state set $\mathscr{C} = \{\mathscr{C}_0, \mathscr{C}_1, \ldots, \mathscr{C}_{L-1}\}$. Here, (i, j) belongs to $\{(S, R_n), (S, P_m), (R_n, D), (R_n, P_m), (R_n, E_k)\}$. Let $\phi_{g_n h_n}(t)$ denote the probability that $\sigma_{ij}(t)$ transits from state g_n to state h_n at time t. The $L \times L$ channel state transition probability matrix is defined as

$$\Phi_n(t) = \left[\phi_{g_n h_n}(t) \right]_{L \times L}, \quad (6)$$

where $\phi_{g_n h_n}(t) = \Pr(\sigma_{ij}(t+1) = h_n \mid \sigma_{ij}(t) = g_n)$, $\forall g_n, h_n \in \mathscr{C}$.

2.3. Finite-State Markov Spectrum Occupancy and Energy Model. In CR relay networks, the radio spectrum is either occupied by the primary users or not. The spectrum state $\omega(t)$ evolves according to a two-state $\Omega = \{0, 1\}$ Markov model, where $\omega(t) = 1$ means that the spectrum is occupied by the primary users and $\omega(t) = 0$ shows that the spectrum is idle. Let $\varphi_{u_n v_n}(t)$ denote the probability that $\omega(t)$ transits from state u_n to state v_n at time t. The 2×2 spectrum occupancy state transition probability matrix is defined as

$$\Psi_n(t) = \left[\varphi_{u_n v_n}(t) \right]_{2 \times 2}, \quad (7)$$

where $\varphi_{u_n v_n}(t) = \Pr(\omega(t+1) = v_n \mid \omega(t) = u_n)$, $\forall u_n, v_n \in \Omega$.

The residual energy of the battery powered relay R_n ($n \in \mathscr{N}$) can also be modeled by a finite-state Markov energy model [24]. In this model, the continuous battery residual energy is divided into discrete levels denoted by $\mathscr{E} = \{\mathscr{E}_0, \mathscr{E}_1, \ldots, \mathscr{E}_{H-1}\}$, each corresponds to an energy state in Markov chain; H is the number of energy sate levels. Let $\theta_{f_n y_n}(t)$ denote the probability that residual energy $e_n(t)$ of R_n transits from state f_n to state y_n at time t. The $H \times H$ energy state transition probability matrix is defined as

$$\Theta_n = \left[\theta_{f_n y_n}(t) \right]_{H \times H}, \quad (8)$$

where $\theta_{f_n y_n}(t) = \Pr(e_n(t+1) = y_n \mid e_n(t) = f_n)$, $\forall f_n, y_n \in \mathscr{E}$.

We need to find out the optimal relay selection and power allocation scheme, which can set one relay to be active at time slot t according to the relays' states that contain their channel state $\sigma_{ij}(t) \in \mathscr{C}$, where (i, j) belongs to $\{(S, R_n), (S, P_m), (R_n, D), (R_n, P_m), (R_n, E_k)\}$, residual energy state $e_n(t) \in \mathscr{E}$, and the spectrum state $\omega(t) \in \Omega$. Our optimization objective is to maximize the secrecy capacity as well as to minimize the energy consumption.

3. Stochastic Formulation

In this section, we propose the relay selection and power allocation scheme to defend against eavesdropping attacks and to save the energy consumption. The proposed scheme can be formulated as a restless bandit problem which has been widely used to solve the stochastic selection issues [25]. In the restless bandit system, the relay is equivalent to the arm, the relay selection and power allocation are the actions of the arm, and the secrecy capacity and energy consumption correspond to the reward. The restless bandit problem can be solved according to the indices of the arms, which is calculated by a primal-dual index heuristic algorithm.

3.1. Formulation of the Restless Bandit Problem

3.1.1. Action Space of Relay. At time slot t, each relay node decides whether to cooperate with the confidential communication between S and D or not and then decides how much power is provided if it joins the cooperation. Thus, the action of relay R_n $(n \in \mathscr{N})$ in time slot t is represented by $a_n(t) = (a_n^S(t), a_n^P(t))$, where $a_n^S(t) \in \{0, 1\}$, 0 denotes that the relay is passive and 1 denotes that the relay is active. If the relay is active, $a_n^P(t)$ is the corresponding power allocation which must satisfy the power constraint in (5). For N relays in time slot t, the action space is $\mathscr{A} = \{a_1(t), a_2(t), \ldots, a_N(t)\}$. In our proposed scheme, we only select a single relay to assist with data transmission. Hence, the relay selection satisfies $\sum_{n=1}^{N} a_n^S(t) = 1$.

3.1.2. State Space and Transition Probabilities. The state of relay R_n $(n \in \mathscr{N})$ in time slot t is determined by the channel states, the spectrum state, and the residual energy state. Consequently, the state of relay R_n can be modeled as

$$i_n(t) = \left[\sigma_{SR_n}(t), \sigma_{SP_m}(t), \sigma_{R_nD}(t), \sigma_{R_nP_m}(t), \sigma_{R_nE_k}(t), \omega(t), e_n(t)\right]. \tag{9}$$

The changes of the channel states $\sigma_{SR_n}(t), \sigma_{SP_m}(t), \sigma_{R_nD}(t), \sigma_{R_nP_m}(t)$, and $\sigma_{R_nE_k}(t)$, spectrum state $\omega(t)$, and residual energy state $e_n(t)$ are independent of each other. The relay state $i_n(t)$ evolves in a Markov fashion with a finite-state space $\mathscr{S}_n$, $i_n(t) \in \mathscr{S}_n$. The state transition probablity matrix of relay R_n is defined as

$$\mathscr{P}_n^a(t) = \left[\phi_{g_nh_n}^{SR_n}, \phi_{g_nh_n}^{SP_m}, \phi_{g_nh_n}^{R_nD}, \phi_{g_nh_n}^{R_nP_m}, \phi_{g_nh_n}^{R_nE_k}, \varphi_{u_nv_n}, \theta_{f_ny_n}^a\right]_{U\times U}, \tag{10}$$

where $\phi_{g_nh_n}^{SR_n}$, $\phi_{g_nh_n}^{SP_m}$, $\phi_{g_nh_n}^{R_nD}$, $\phi_{g_nh_n}^{R_nP_m}$, $\phi_{g_nh_n}^{R_nE_k}$, $\varphi_{u_nv_n}$ and $\theta_{f_ny_n}^a$ are defined in (6), (7), and (8), respectively, and $U = |L|^4 \times 2 \times H$. The element of $\mathscr{P}_n^a(t)$ is $p_{i_nj_n}^a$, denoting the transition probability that the state of relay R_n transits from i_n to j_n, where $i_n, j_n \in \mathscr{S}_n$ and $a \in \mathscr{A}$.

3.1.3. System Reward. The goal of our proposed relay selection and power allocation scheme is to maximize SC and to minimize energy consumption in CR relay networks. Thus, we formulate the system reward to be the function of the SC, the residual relay energy, and the energy consumption. At time slot t, if relay R_n, in state $i_n(t)$, takes action $a_n(t)$, then the immediate reward is earned:

$$R_{i_n(t)}^{a_n(t)} = a_n(t) \cdot \left(\mu_1 \cdot C_S(i_n(t), a_n(t)) + \mu_2 \cdot e_n(t) + \mu_3 \cdot P_{R_n}(i_n(t), a_n(t))\right), \tag{11}$$

where μ_1, μ_2, and μ_3 are weights and $C_S(i_n(t), a_n(t))$ is the achievable secrecy capacity and calculated by (1) while $e_n(t)$ and P_{R_n} are the residual energy and power consumption.

The immediate reward $R_{i_n(t)}^{a_n(t)}$ is earned when relay R_n takes action $a_n(t)$ in state $i_n(t)$. For a stochastic process, a maximum immediate value is not equivalent to the maximum expected long-term accumulated value. We assume that the duration of the whole communication is long enough and that T is approximately infinite. We denote by β the discount factor and denote by $\mathscr{U}$ the set of admissible Markovian policies. The relay selection and power allocation problem is to find an optimal scheduling policy $u \in \mathscr{U}$ that maximizes the expected total discounted reward over an infinite horizon and compute its optimum value:

$$\mathscr{Z}^* = \max_{u\in\mathscr{U}} E_u\left[\sum_{t=0}^{T-1}\left(R_{i_1(t)}^{a_1(t)} + R_{i_2(t)}^{a_2(t)} + \cdots + R_{i_N(t)}^{a_N(t)}\right)\beta^t\right], \tag{12}$$

where $\mathscr{Z}^*$ is the optimal expected total discounted reward. The discount factor is required to be $0 < \beta < 1$ to ensure that the expected total discounted reward is converged over an infinite horizon.

3.2. Solution to the Restless Bandit Problem. The restless bandit problem mentioned above can be solved by the primal-dual index heuristic algorithm based on the first-order LP relaxation, which has been demonstrated to have less complexity and very close performance compared to the optimal one [25].

3.2.1. Linear Programming (LP) Relaxation. In order to formulate the restless bandit problem as a linear program we introduce performance measures:

$$x_{i_n}^{a_n}(u) = E_u\left[\sum_{t=0}^{T-1} I_{i_n}^{a_n}(t)\beta^t\right], \tag{13}$$

where $u \in \mathscr{U}$ is an admissible scheduling policy,

$$I^{a_n}_{i_n}(t) = \begin{cases} 1, & \text{if } R_n \text{ is in state } i_n \text{ and its action is } a_n \text{ at time } t, \\ 0, & \text{otherwise.} \end{cases} \tag{14}$$

Notice that $x^{a_n}_{i_n}(u)$ represents the expected total discounted time that R_n in state $i_n(t)$ takes action $a_n(t)$ under policy u, where $I^{a_n}_{i_n} = 1$ if action $a_n(t)$ is taken in time t and $I^{a_n}_{i_n} = 0$ otherwise. The corresponding performance region, spanned by performance vector $(x^{a_n}_{i_n}(u))_{i_n\in\mathcal{S}_n, a_n\in\mathscr{A}}$ under all admissible policies, is denoted by X:

$$X = \left\{ x = \left(x^{a_n}_{i_n}(u)\right)_{i_n\in\mathcal{S}_n, a_n\in\{0,1\}, n\in\mathcal{N}} \mid u \in \mathscr{U} \right\}. \tag{15}$$

Reference [25] proved that the performance region X is the *restless bandit polytope* Q. The restless bandit problem can thus be formulated as the linear program:

$$\mathscr{Z}^* = \max_{x\in X} \sum_{n\in\mathcal{N}} \sum_{i_n\in\mathcal{S}_n} \sum_{a_n\in\{0,1\}} R^{a_n}_{i_n} x^{a_n}_{i_n}. \tag{16}$$

The approach developed in [25] is to construct relaxations of polytope X so as to yield polynomial-size relaxations of linear program. Denote by $\widehat{X} \supseteq X$ the relaxations not on the original variables $x^{a_n}_{i_n}$, but in a higher-dimensional space that includes new auxiliary variables. Define $Q^1_n = \{x_n = (x^{a_n}_{i_n}(u))_{i_n\in\mathcal{S}_n, a_n\in\{0,1\}, n\in\mathcal{N}} \mid u \in \mathscr{U}\}$, which is precisely the projection of *restless bandit polytope* Q over the space of the variable $x^{a_n}_{i_n}$ for R_n. A complete formulation of Q^1_n is given by [25]:

$$Q^1_n = \left\{ x_n \in \mathfrak{R}_+^{|\mathcal{S}_n\times\{0,1\}|} \mid x^0_{j_n} + x^1_{j_n} = \pi_{j_n} + \beta \sum_{i_n\in\mathcal{S}_n} \sum_{a_n\in\{0,1\}} p^{a_n}_{i_nj_n} x^{a_n}_{i_n},\ j_n \in \mathcal{S}_n \right\}, \tag{17}$$

where π_{j_n} denotes the probability that the initial state of relay R_n is j_n. According to Whittle's condition, the average number of active relay can be written as

$$\begin{aligned} \sum_{n\in\mathcal{N}} \sum_{i_n\in\mathcal{S}_n} x^1_{i_n}(u) &= \sum_{t=0}^{\infty} E_u \left[\sum_{n\in\mathcal{N}} \sum_{i_n\in\mathcal{S}_n} I^1_{i_n}(t) \right] \beta^t \\ &= \sum_{t=0}^{\infty} M\beta^t = \frac{M}{1-\beta}. \end{aligned} \tag{18}$$

In our scheme, only one relay is selected at each time slot, so $M = 1$.

Therefore, the first-order relaxation can be formulated as the linear program

$$\begin{aligned} (\text{LP}^1)\quad \mathscr{Z}^1 = \max\ & \sum_{n\in\mathcal{N}} \sum_{i_n\in\mathcal{S}_n} \sum_{a_n\in\{0,1\}} R^{a_n}_{i_n} x^{a_n}_{i_n} \\ \text{subject to}\ & x_n \in Q^1_n, \quad n \in \mathcal{N}, \\ & \sum_{n\in\mathcal{N}} \sum_{i_n\in\mathcal{S}_n} x^1_{i_n} = \frac{1}{1-\beta}. \end{aligned} \tag{19}$$

There are $\mathcal{O}(N|U|)$ variables and constraints of this linear program (LP^1), with the polynomial size in the problem dimensions.

3.2.2. Primal-Dual Priority Index Heuristic. In this section, we present a heuristic for the restless bandit problem, which uses information contained in optimal primal and dual solutions to the first-order relaxation (LP^1). The primal-dual heuristic is interpreted as a priority-index heuristic as well. The dual of linear program (LP^1) is

$$\begin{aligned} (D^1)\quad \mathscr{Z}^1 = \min\ & \sum_{n\in\mathcal{N}} \sum_{j_n\in\mathcal{S}_n} \pi_{j_n}\lambda_{j_n} + \frac{1}{1-\beta}\lambda, \quad \lambda \geqslant 0 \\ \text{subject to}\ & \lambda_{i_n} - \beta \sum_{j_n\in\mathcal{S}_n} p^0_{i_nj_n}\lambda_{j_n} \geqslant R^0_{i_n}, \\ & i_n(t) \in \mathcal{S}_n,\ n \in \mathcal{N} \\ & \lambda_{i_n} - \beta \sum_{j_n\in\mathcal{S}_n} p^1_{i_nj_n}\lambda_{j_n} \geqslant R^1_{i_n}, \\ & i_n(t) \in \mathcal{S}_n,\ n \in \mathcal{N}. \end{aligned} \tag{20}$$

Let $\{\overline{x}^{a_n}_{i_n}\}$ and $\{\overline{\lambda}_{i_n}, \lambda\}$ be an optimal primal and dual solution pair to the first-order relaxation (LP^1) and its dual (D^1). The corresponding optimal reduced cost coefficients $\{\overline{\gamma}^{a_n}_{i_n}\}$ are defined as

$$\begin{aligned} \overline{\gamma}^0_{i_n} &= \overline{\lambda}_{i_n} - \beta \sum_{j_n\in\mathcal{S}_n} p^0_{i_nj_n}\overline{\lambda}_{j_n} - R^0_{i_n}, \\ \overline{\gamma}^1_{i_n} &= \overline{\lambda}_{i_n} - \beta \sum_{j_n\in\mathcal{S}_n} p^1_{i_nj_n}\overline{\lambda}_{j_n} + \overline{\lambda} - R^1_{i_n}, \end{aligned} \tag{21}$$

which must be nonnegative. $\overline{\gamma}^0_{i_n}$ and $\overline{\gamma}^1_{i_n}$ are the rates of decrease in the objective value of linear program (19) per unit increase in the value of variables $x^0_{i_n}$ and $x^1_{i_n}$, respectively. Based on the cost coefficients, the index of relay R_n in state i_n is defined as

$$\delta_{i_n} = \overline{\gamma}^1_{i_n} - \overline{\gamma}^0_{i_n}. \tag{22}$$

The priority-index rule is that the relay with the smallest index is selected to be active.

3.3. Process of Relay Selection and Power Allocation Scheme. In this section, we present the indexable relay selection and power allocation scheme in CR relay networks. Our proposed scheme is divided into offline computation and online selection. The specific procedure is given in Algorithm 1.

Algorithm 1 (process of relay selection and power allocation scheme). Consider the following steps.

Step 1 (offline computation). (1) According to the spectrum state, channel state, and residual relay energy state, the state space and transition probability matrices under different actions can be determined.

(2) Input the state transition probability $p^{a}_{i_n j_n}$, the reward $R^{a_n}_{i_n}$, the discount factor β, and initial state probability π_{j_n} and then compute the priority indices $\{\delta_{i_n}\}$ according to (20)–(22); the indices $\{\delta_{i_n}\}$ are stored in an index-table.

(3) Each relay stores this index-table.

Step 2 (online selection). (1) At the beginning of each time slot t, all the candidate relays sense the spectrum occupancy state, estimate the channel gain, and detect the residual energy to obtain the spectrum state, channel state, and residual energy state.

(2) Each candidate relay shares its state i_n with each other.

(3) Each candidate relay looks the indices up for all relays in the index-table; the relay with the smallest index is selected to be active, and the corresponding power allocation can be obtained.

4. Numerical Results and Analysis

In this section, numerical results are provided to show the physical-layer security and energy consumption improvement by exploiting the proposed relay selection and power allocation scheme. The maximum transmission power limit $P_{T,\max}$ for S and R_n is set as 150 mw; the battery capacity of each relay is set to be 1000 mAh with the output voltage 1 Volt. The discount factor β is 0.7. The links S-R_n, S-P_m, R_n-D, R_n-P_m, and R_n-E_k are divided into "bad" and "good" states; the spectrum occupancy state is "busy" and "idle." For both $\Phi_n(t)$ and $\Psi_n(t)$, the transition probability between the different states is 0.3 and the probability of staying in the same state is 0.7. The residual energy of each relay is divided into "high," "low," and "dead" states; set Θ^1_n to be the residual energy state transition probability matrix when the relay R_n is active and Θ^0_n when it is passive; that is,

$$\Theta^0_n = \begin{pmatrix} 1.00 & 0.00 & 0.00 \\ 0.01 & 0.99 & 0.00 \\ 0.00 & 0.01 & 0.99 \end{pmatrix},$$
$$\Theta^1_n = \begin{pmatrix} 1.00 & 0.00 & 0.00 \\ 0.08 & 0.92 & 0.00 \\ 0.00 & 0.08 & 0.92 \end{pmatrix}. \qquad (23)$$

The following methods are simulated for comparison:

(i) the proposed relay selection and power allocation scheme;

(ii) the memoryless relay selection scheme, in which the relay node is selected for subsequent data transmission according to the current channel condition;

Table 1: Complexity comparison.

Relay selection and power allocation scheme	Order of operations
Proposed selection scheme	$\mathcal{O}((N-1)\times T)$
Memoryless selection scheme	$\mathcal{O}((2N-1)\times T)$
Traditional selection scheme	$\mathcal{O}((N-1)\times T)$
Arbitrary selection scheme	$\mathcal{O}(T)$

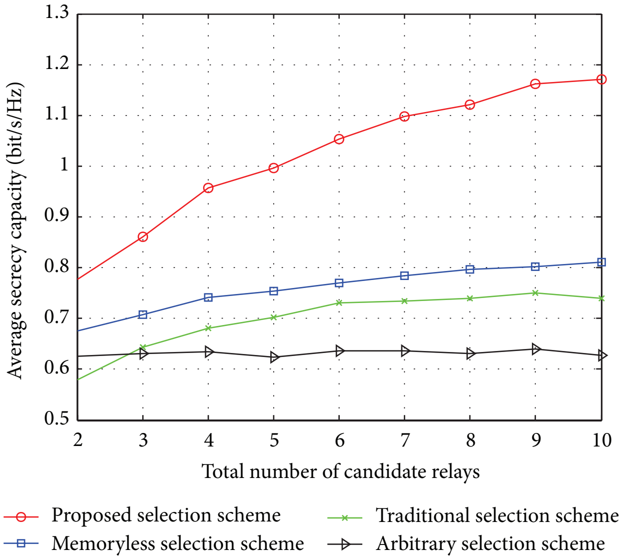


Figure 2: Average secrecy capacity versus the number of candidate relays for different relaying schemes with $K = 1$ and $P_{\text{th}} = 5$ mw.

(iii) the traditional relay selection scheme [8], in which the eavesdroppers' channel condition is not taken into account;

(iv) the arbitrary relay selection scheme.

The computational complexity of the proposed relay selection and power allocation scheme and that of those existing schemes are tabulated in Table 1. N denotes the number of candidate relays and T denotes the time horizon. Compared to the memoryless selection scheme with $\mathcal{O}((2N-1)\times T)$ order of operations, the complexity of the proposed selection scheme is reduced due to the indexability property. It also shows that the complexity of the arbitrary selection scheme is independent of the number of candidate relays.

4.1. Secrecy Capacity Performance Improvement. This subsection presents the numerical secrecy capacity results of the proposed relay selection scheme. We do not consider the energy issue here, which will be considered later. Thus, the weighs can be specified as $\mu_1 = 1$, $\mu_2 = 0$, and $\mu_3 = 0$.

Figure 2 shows the average secrecy capacity improvement of the proposed scheme with the different number of candidate relays. We assume that the interference temperature limit $P_{\text{th}} = 5$ mw and eavesdropper $K = 1$. We can see that as the number of candidate relays increases; the probability that there exists a candidate relay with better state is high so

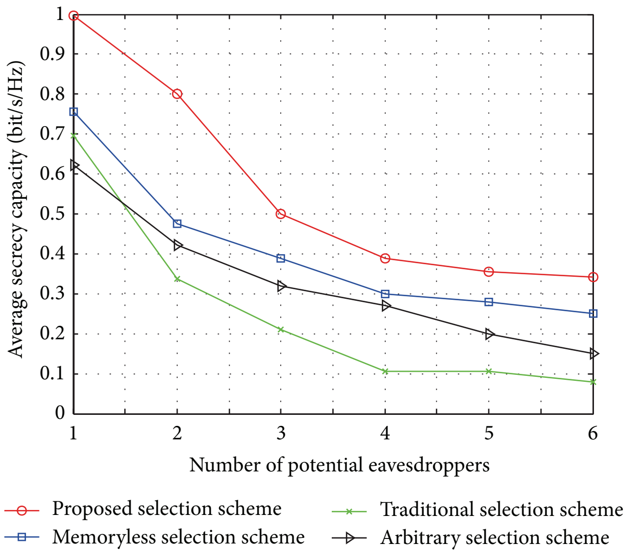


FIGURE 3: Average secrecy capacity versus the number of potential eavesdroppers for different relaying schemes with $N = 5$ and $P_{\text{th}} = 5$ mw.

that there is always a good candidate for the relay selection schemes. It also can be seen that the proposed scheme always has the larger average secrecy capacity compared with the memoryless scheme, the traditional scheme, and the arbitrary scheme. This is because the memoryless scheme selects the relay node for subsequent data transmission according to the current channel condition, which may change during the subsequent data transmission. The traditional scheme does not take the eavesdropper channels into account; it is not able to support systems with secrecy constraint. The arbitrary selection scheme has the worst secrecy capacity performance.

Figure 3 shows the average secrecy capacity versus the number of eavesdroppers for different schemes with candidate relays $N = 5$ and interference temperature limit $P_{\text{th}} = 5$ mw. We can see that as the number of eavesdroppers increases, the achievable secrecy capacity of all the schemes is significantly reduced. This is because with the number of eavesdroppers increasing, the probability that the wiretap links become much better than the main link is high. As a result, the eavesdroppers will most likely succeed to intercept the legitimate transmission. However, the proposed scheme defends more effectively against eavesdropping attacks than the existing schemes, which confirms the advantage of the proposed scheme.

Figure 4 illustrates the average secrecy capacity under different interference temperature limits P_{th} with candidate relays $N = 5$ and eavesdropper $K = 1$. We can observe that the average secrecy capacity of all schemes changes nonsignificantly when $P_{\text{th}} \geqslant 10$ dBm and increases with the increasing P_{th} when $P_{\text{th}} < 10$ dBm. This is due to the fact that when the interference temperature limit P_{th} is less than 10 dBm and the spectrum is sensed to be "busy," R_n's transmission power directly depends on P_{th} to guarantee the QoS of primary users.

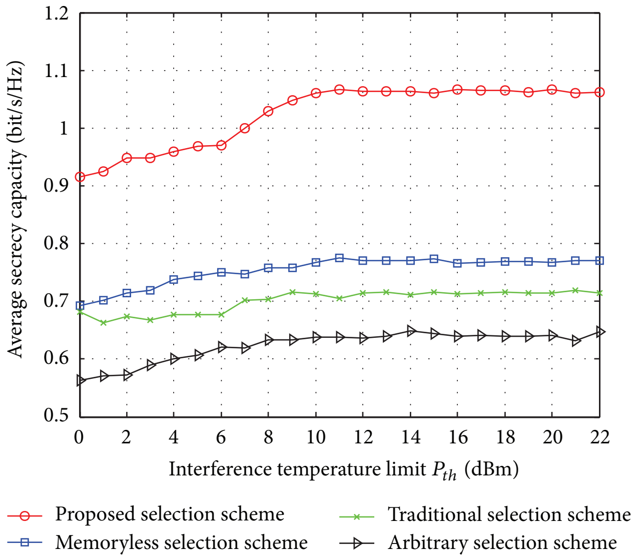


FIGURE 4: Average secrecy capacity versus interference temperature limit for different relaying schemes with $N = 5$ and $K = 1$.

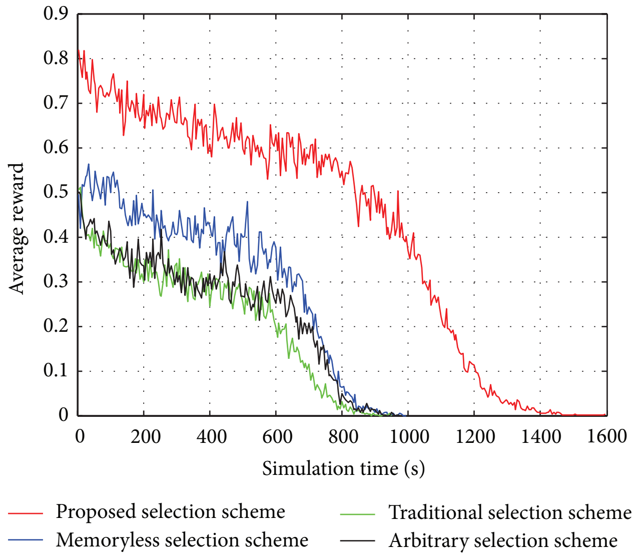


FIGURE 5: Average reward versus simulation time for different relay selection schemes with $N = 5$, $K = 1$, and $P_{\text{th}} = 5$ mw.

4.2. Energy Consumption Improvement. In this subsection, we demonstrate the energy consumption improvement of the proposed scheme. We set the weights as $\mu_1 = 0.5$, $\mu_2 = 0.3$, and $\mu_3 = 0.2$. For fair comparison, the memoryless selection scheme is revised to select relay with the highest residual energy without considering the energy consumption. The traditional selection scheme selects relay to maximize the achievable data rate and minimize the energy consumption without considering eavesdroppers while the arbitrary selection scheme selects relay among the alive relay nodes.

Figure 5 shows the average reward comparison among the proposed scheme, the memoryless scheme, the traditional scheme, and the arbitrary scheme. There are $N = 5$ candidate

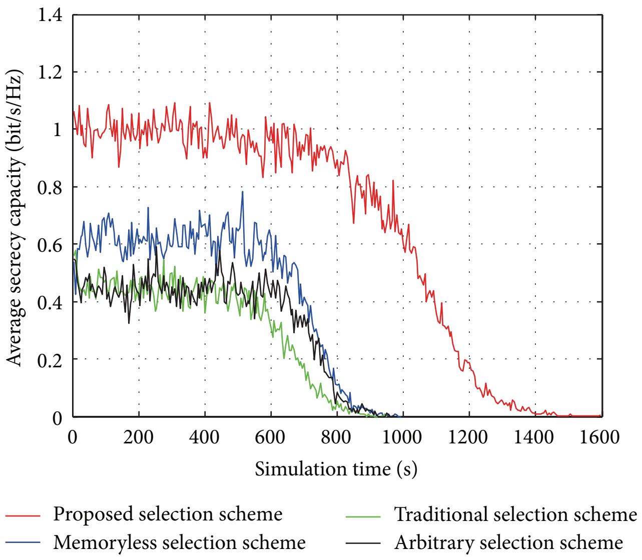


FIGURE 6: Average secrecy capacity versus simulation time for different relay selection schemes with $N = 5$, $K = 1$, and $P_{th} = 5$ mw.

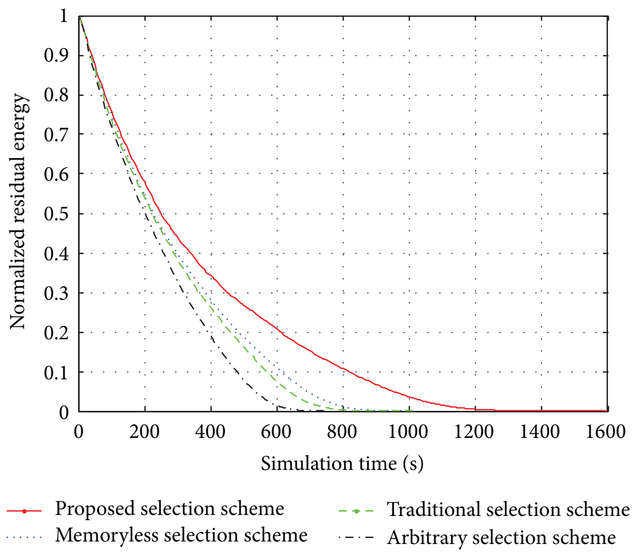


FIGURE 7: Normalized residual energy versus simulation time for different relay selection schemes with $N = 5, K = 1$, and $P_{th} = 5$ mw.

relays and $K = 1$ potential eavesdropper. Since more and more relays run out of energy with the increase of simulation time, the number of available relays decreases. As a result, the average reward for all the schemes declines with time. The proposed scheme outperforms the other three schemes. This is because the achievable secrecy capacity and the energy consumption contribute to the reward. The proposed scheme selects relay node that costs less energy at the decision time, while the memoryless scheme and the arbitrary schemes do not take the energy consumption into consideration, and the traditional scheme's objective is to maximize the achievable data rate and minimize the energy consumption without considering eavesdroppers, so it cannot support the secure secondary transmission.

The energy consumption also has some effects on the average secrecy capacity. As shown in Figure 6, the average secrecy capacity declines with increasing simulation time. This is due to the fact that increasingly more relay nodes run out of energy after data transmission for some time slots. It can be seen that there is hardly any live relay at about 1000 s, and the average secrecy capacity of the proposed scheme outperforms the other selection schemes.

Figure 7 compares the energy consumption for different relaying schemes with $N = 5$ available relays and $K = 1$ potential eavesdropper. We can see that the energy of the memoryless selection scheme, the traditional selection scheme, and the arbitrary selection scheme run out earlier than that of the proposed scheme, which further confirms the advantage of the proposed scheme.

Figure 8 reveals the average network lifetime of different relaying schemes with $N = 5$ available relays and $K = 1$ potential eavesdropper. In this paper, the network lifetime is defined as that the number of dead relays that reach a threshold, Nth, such that the considered cognitive network can no longer achieve the target secrecy performance. As expected, the network lifetime of all schemes increases with Nth. In addition, our proposed scheme always has the best performance.

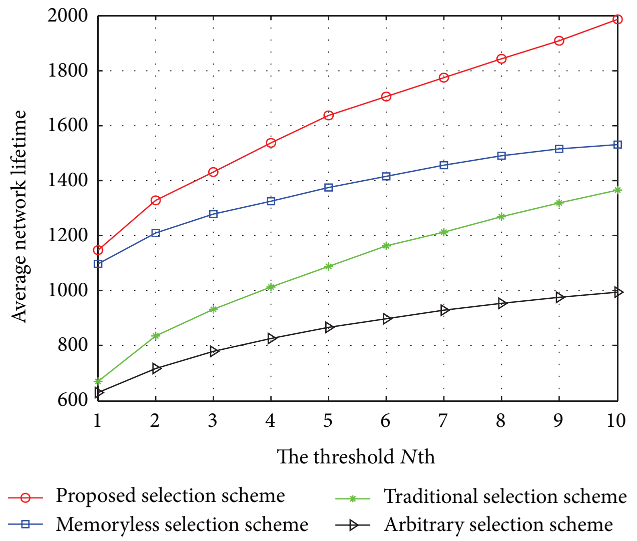


FIGURE 8: Average network lifetime versus the threshold Nth for different relay selection schemes with $N = 5, K = 1$, and $P_{th} = 5$ mw.

5. Conclusion

In this paper, we have explored the physical layer security and efficient energy consumption of the secondary transmission and proposed the best relay selection and dynamic power allocation scheme. Moreover, the spectrum occupancy state, the wireless channels, and residual relay energy are characterized as finite-state Markov model in order to accurately describe the time-varying radio environment. Specifically, we formulated the relay selection and power allocation problem as a restless bandit system and solved this stochastic control problem with a primal-dual index heuristic algorithm. Finally, simulation results have been presented to illustrate that the proposed relay selection and power allocation scheme can significantly maximize the secrecy capacity as well as minimize the energy consumption compared to the existing schemes.

Conflict of Interests

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

Acknowledgments

This work is supported by the National Natural Science Foundation of China (no. 61471060), National High Technology Research and Development Program of China (863 Program) (no. 2014AA01A706), and Funds for Creative Research Groups of China (no. 61421061).

References

[1] H. Simon, “Cognitive radio: brain-empowered wireless communications,” *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.

[2] Q. Zhao and B. M. Sadler, “A survey of dynamic spectrum access,” *IEEE Signal Processing Magazine*, vol. 24, no. 3, pp. 79–89, 2007.

[3] J. Jia, J. Zhang, and Q. Zhang, “Cooperative relay for cognitive radio networks,” in *Proceedings of the IEEE INFOCOM*, pp. 2304–2312, IEEE, Rio de Janeiro, Brazil, April 2009.

[4] J. Mietzner, L. Lampe, and R. Schober, “Distributed transmit power allocation for multihop cognitive-radio systems,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5187–5201, 2009.

[5] D. Chen, H. Ji, and V. C. M. Leung, “Distributed best-relay selection for improving TCP performance over cognitive radio networks: a cross-layer design approach,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 315–322, 2012.

[6] S. Sagong, J. Lee, and D. Hong, “Capacity of reactive DF scheme in cognitive relay networks,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3133–3138, 2011.

[7] P. Li, S. Guo, W. Zhuang, and B. Ye, “Capacity maximization in cooperative CRNs: joint relay assignment and channel allocation,” in *Proceedings of the IEEE International Conference on Communications (ICC ’12)*, pp. 5097–5101, Ottawa, Canada, June 2012.

[8] C. Luo, G. Min, F. R. Yu, M. Chen, L. T. Yang, and V. C. M. Leung, “Energy-efficient distributed relay and power control in cognitive radio cooperative communications,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 11, pp. 2442–2452, 2013.

[9] C. T. Clancy and N. Goergen, “Security in cognitive radio networks: threats and mitigation,” in *Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom ’08)*, pp. 1–8, May 2008.

[10] Z. Shu, Y. Qian, and S. Ci, “On physical layer security for cognitive radio networks,” *IEEE Network*, vol. 27, no. 3, pp. 28–33, 2013.

[11] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[12] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap channel,” *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[13] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Transaction on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[14] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, “Secure communication over MISO cognitive radio channels,” *IEEE Transactions on Wireless Communications*, vol. 9, no. 4, pp. 1494–1502, 2010.

[15] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, “Secure communication in multiantenna cognitive radio networks with imperfect channel state information,” *IEEE Transactions on Signal Processing*, vol. 59, no. 4, pp. 1683–1693, 2011.

[16] T. Kwon, V. W. S. Wong, and R. Schober, “Secure MISO cognitive radio system with perfect and imperfect CSI,” in *Proceedings of the IEEE Global Communications Conference (GLOBECOM ’12)*, pp. 1236–1241, December 2012.

[17] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, “On the relationship between the multi-antenna secrecy communications and cognitive radio communications,” *IEEE Transactions on Communications*, vol. 58, no. 6, pp. 1877–1886, 2010.

[18] Y. Zou, X. Wang, and W. Shen, “Physical-layer security with multiuser scheduling in cognitive radio networks,” *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5103–5113, 2013.

[19] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm, “Proposed relay selection scheme for physical layer security in cognitive radio networks,” *IET Communications*, vol. 6, no. 16, pp. 2676–2687, 2012.

[20] T. Wang, L. Song, Z. Han, X. Cheng, and B. Jiao, “Power allocation using Vickrey auction and sequential first-price auction games for physical layer security in cognitive relay networks,” in *Proceedings of the IEEE International Conference on Communications (ICC ’12)*, pp. 1683–1687, June 2012.

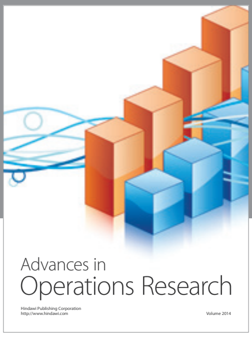
[21] M. Z. I. Sarkar and T. Ratnarajah, “Enhancing security in the cognitive relay assisted co-existing radio systems with interferences,” in *Proceedings of the IEEE International Conference on Communications (ICC ’13)*, pp. 4729–4733, June 2013.

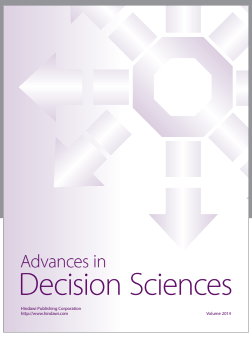
[22] M. Bloch, J. O. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

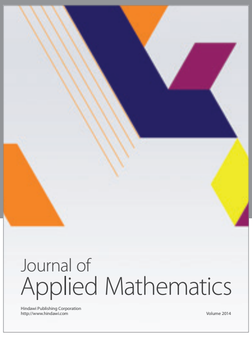
[23] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, “Improving wireless physical layer security via cooperating relays,” *IEEE Transactions on Signal Processing*, vol. 58, no. 3, part 2, pp. 1875–1888, 2010.

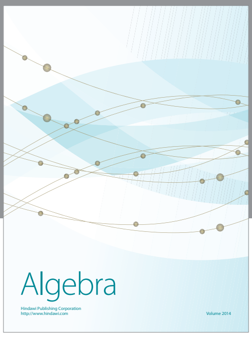
[24] P. Hu, Z. Zhou, Q. Liu, and F. Li, “The HMM-based modeling for the energy level prediction in wireless sensor networks,” in *Proceedings of the 2nd IEEE Conference on Industrial Electronics and Applications (ICIEA ’07)*, pp. 2253–2258, May 2007.

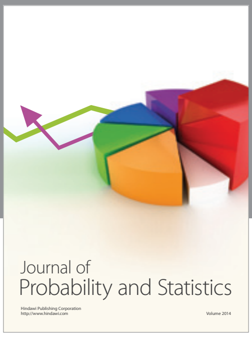
[25] D. Bertsimas and J. Niño-Mora, “Restless bandits, linear programming relaxations, and a primal-dual index heuristic,” *Operations Research*, vol. 48, no. 1, pp. 80–90, 2000.


Advances in
Operations Research

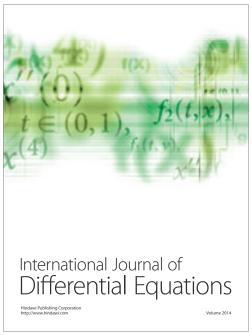

Advances in
Decision Sciences


Journal of
Applied Mathematics

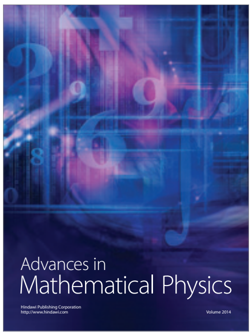

Algebra

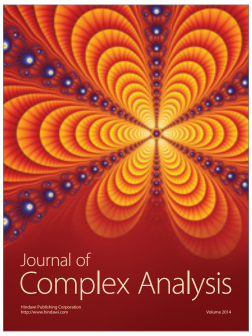

Journal of
Probability and Statistics

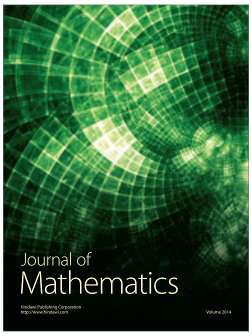
The Scientific
World Journal

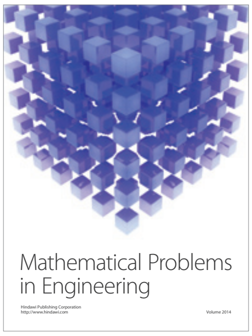

International Journal of
Differential Equations

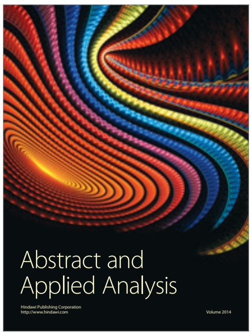
International Journal of
Combinatorics

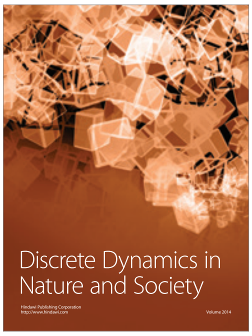

Advances in
Mathematical Physics

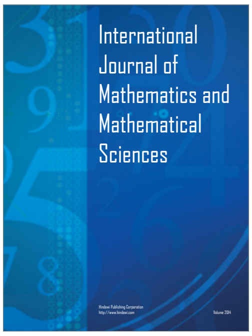

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

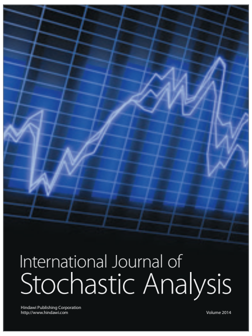

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization