Low-Complexity Transmit Power Control for Secure Communications in Wireless-Powered Cognitive Radio Networks

Kisong Lee

Department of Information and Communication Engineering, Dongguk University, Seoul 04620, Korea; kslee851105@gmail.com; Tel.: +82-2-2260-3233

Abstract: In this study, wireless-powered cognitive radio networks (WPCRN) are considered, in which N sets of transmitters, receivers and energy-harvesting (EH) nodes in secondary networks share the same spectrum with primary users (PUs) and none of the EH nodes is allowed to decode information but can harvest energy from the signals. Given that the EH nodes are untrusted nodes from the point of view of information transfer, the eavesdropping of secret information can occur if they decide to eavesdrop on information instead of harvesting energy from the signals transmitted by secondary users (SUs). For secure communications in WPCRN, we aim to find the optimal transmit powers of SUs that maximize the average secrecy rate of SUs while maintaining the interference to PUs below an allowable level, while guaranteeing the minimum EH requirement for each EH node. First, we derive an analytical expression for the transmit power via dual decomposition and propose a suboptimal transmit power control algorithm, which is implemented in an iterative manner with low complexity. The simulation results confirm that the proposed scheme outperforms the conventional distributed schemes by more than 10% in terms of the average secrecy rate and outage probability and can also considerably reduce the computation time compared with the optimal scheme.

Citation: Lee, K. Low-Complexity Transmit Power Control for Secure Communications in Wireless-Powered Cognitive Radio Networks. *Sensors* **2021**, *21*, 7837. <https://doi.org/10.3390/s21237837>

Academic Editors: Hwangnam Kim, Woonghee Lee, Seungho Yoo, Eun-Chan Park

Received: 2 November 2021

Accepted: 24 November 2021

Published: 25 November 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: secure communication; energy harvesting; cognitive radio network; secrecy rate; transmit power control

1. Introduction

Cognitive radio networks (CRNs) have received considerable attention as a means to use the unused spectrum to enhance the spectral efficiency (SE) [1]. In CRNs, unlicensed secondary users (SUs) can opportunistically access the spectrum unoccupied by primary users (PUs) as long as they do not interfere with the operation of the PUs [2]. To realize effective spectrum sharing between two networks, several researchers have attempted to mitigate co-channel interference, for instance, through transmit power control (TPC) [3,4], subcarrier allocation [5] and transmit beamforming pattern [6].

In addition to spectrum sharing, there exist many opportunities to harvest energy from radio frequency (RF) signals in CRNs; thus, wireless-powered CRNs (WPCRN) have actively been investigated [7–11]. The authors of [7,8] proposed a joint information and energy cooperation strategy between PUs and SUs, while cooperative spectrum sensing was optimized under the constraints of collision and energy causality [9]. Moreover, resource allocation strategies have been suggested to maximize the sum throughput of SUs capable of energy harvesting (EH) [10,11].

Notably, the coexistence of different networks is associated with a security issue owing to the increased risk of eavesdropping. Consequently, a number of studies on physical layer security have been performed to guarantee secure communications without relying on a secret key in CRNs [12–15]. In particular, the security-aware scheduling and power allocation of SUs were optimized to maximize the sum secrecy throughput [12] and resource allocation was proposed to maximize the sum rate of SUs while ensuring the secrecy outage constraint of PUs [13]. In [14], a security-aware proportional fairness

resource allocation was developed to improve the sum secrecy throughput and user fairness of SUs. Furthermore, an optimal relay selection was proposed for WPCRN and the secrecy performances were analyzed with respect to the secrecy outage probability and ergodic rate [15]. Nevertheless, research on WPCRN remains limited and most of the existing security strategies for CRNs are based on a centralized approach, which involves a high computational complexity [12–14]. Distributed TPC strategies were studied in [16,17]; however, these schemes showed not only sub-optimal performances but also could not be directly applied to WPCRN. Therefore, it is necessary to establish a security-aware TPC algorithm that can be implemented with a low complexity for practical WPCRN.

Considering this aspect, this research study focuses on secure communications for WPCRN. The contributions of our work can be summarized as follows:

- We present a practical system model for WPCRN, in which multiple SUs share the same spectrum with PUs and EH nodes are not allowed to interpret information but are licensed to collect energy from the transmitted signals.
- To prevent eavesdropping of untrusted EH nodes and share the spectrum efficiently, an optimization problem is formulated to derive the optimal transmit powers of SU transmitters (Tx) to maximize the average secrecy rate of SUs while ensuring the requirements of allowable interference on PU receiver (Rx) and minimum amount of energy for each EH node. Given that the formulated problem is non-convex, dual decomposition is performed to identify the suboptimal value of the transmit power and develop a low complexity TPC strategy.
- Performance evaluations based on intensive simulations show that the proposed scheme achieves near-optimal performances in terms of the average secrecy rate and outage probability and significantly reduces the computational complexity compared with the optimal scheme.

The remaining paper is organized as follows: Section 2 presents the system model of the WPCRN, along with the problem statement. Section 3 describes the low-complexity TPC algorithm. Section 4 describes the performance evaluation of the proposed scheme based on extensive simulations. The concluding remarks are presented in Section 5.

2. System Model and Problem Statement

Figure 1 shows the system model of WPCRN for secure communications, in which all nodes are equipped with a single antenna. In particular, N SU Tx–Rx pairs share the same frequency with PUs as long as the amount of interference on PUs is less than an allowable level. Moreover, N EH nodes associated with each SU Tx–Rx pair are not permitted to decode information and are only allowed to harvest energy from the transmitted signals. Consequently, these nodes are regarded as untrusted nodes [18]. The sets of SU Tx–Rx pairs and their associated EH nodes are denoted as $\mathcal{N}$, i.e., $|\mathcal{N}| = N$. The wireless channel between SU Tx i and SU Rx j is denoted as $h_{i,j}$ and that between SU Tx i and EH node j is denoted as $g_{i,j}$. In addition, the index 0 corresponds to PUs, i.e., $h_{i,0}$ is the wireless channel between SU Tx i and PU Rx and $g_{0,i}$ is the wireless channel between PU Tx and EH node i . It is assumed that all wireless channels follow a discrete time block-fading model and $h_{i,0}$ is available at SU Tx i to maintain the amount of interference on PU Rx below an acceptable level [19].

The signal received at SU Rx i is expressed as

$$y_i = \sqrt{p_i}h_{i,i}x_i + \sum_{k \in \mathcal{N} \setminus \{i\}} \sqrt{p_k}h_{k,i}x_k + \sqrt{p_0}h_{0,i}x_0 + z_i, \quad (1)$$

where x_i and x_0 indicate the normalized data sent by SU Tx i and PU Tx with transmit power p_i and p_0 , respectively; $z_i \sim \mathcal{CN}(0, \sigma^2)$ represents additive white Gaussian noise.

Figure 1. Example of WPCRN for secure communications with $N = 2$.

Using (1), the achievable SE can be specified as

$$r_i = \log_2 \left(1 + \frac{p_i |h_{i,i}|^2}{\sum_{k \in \mathbb{N} \setminus \{i\}} p_k |h_{k,i}|^2 + p_0 |h_{0,i}|^2 + \sigma^2} \right). \quad (2)$$

The interference caused by SU Tx i on PU Rx is expressed as

$$I_i = p_i |h_{i,0}|^2. \quad (3)$$

Moreover, the signal received at EH node i is obtained as

$$\hat{y}_i = \sqrt{p_i} g_{i,i} x_i + \sum_{k \in \mathbb{N} \setminus \{i\}} \sqrt{p_k} g_{k,i} x_k + \sqrt{p_0} g_{0,i} x_0 + \hat{z}_i, \quad (4)$$

where $\hat{z}_i \sim \mathcal{CN}(0, \sigma^2)$. Because each EH node can collect energy from the signals sent by all Txs, the total energy harvested at EH node i is represented by

$$e_i = \zeta_i \left(p_0 |g_{0,i}|^2 + \sum_{j \in \mathbb{N}} p_j |g_{j,i}|^2 \right), \quad (5)$$

where ζ_i is the energy conversion efficiency at EH node i . If EH node i stops harvesting energy and decides to eavesdrop on information from SU Tx i , its achievable SE is defined as

$$r_i^e = \log_2 \left(1 + \frac{p_i |g_{i,i}|^2}{\sum_{k \in \mathbb{N} \setminus \{i\}} p_k |g_{k,i}|^2 + p_0 |g_{0,i}|^2 + \sigma^2} \right). \quad (6)$$

Using (2) and (6), the secrecy rate of set i can be defined as follows [20]:

$$r_i^s = [r_i - r_i^e]^+, \quad (7)$$

where $[\cdot]^+ = \max(0, \cdot)$.

To ensure the information secrecy from untrusted EH nodes while supplying a sufficient amount of energy to each EH node, $E_{\min}$, and maintaining the interference to PU Rx

below an allowable level, $I_{\max}$, the transmit powers of SU Txs must be optimized. Accordingly, the problem of average secrecy rate maximization can be formulated as follows:

$$\begin{aligned} \max_{0 \leq \vec{p}} \quad & \frac{1}{N} \sum_{i \in \mathbb{N}} r_i^s \\ \text{s.t.} \quad & \sum_{i \in \mathbb{N}} I_i \leq I_{\max} \\ & e_i \geq E_{\min}, \quad i \in \mathbb{N} \\ & p_i \leq P_{\max}, \quad i \in \mathbb{N}, \end{aligned} \quad (8)$$

where $\vec{p} = \{p_1, p_2, \dots, p_N\}$ and $P_{\max}$ denotes the maximum transmit power for SU Txs. The co-channel interference of the objective function renders the problem (8) non-convex; thus, it is difficult to derive the optimal value of $\vec{p}$ in an analytical form. The near-optimal solution can be numerically determined through an exhaustive search (ES), in which all possible combinations are examined by quantizing $\vec{p}$ into Q equally spaced values. However, this process requires the complete channel state information (CSI) and extremely high computational complexity of $O(Q^N)$; thus, the process has an exponential complexity with respect to N .

3. Low-Complexity Transmit Power Control Algorithm

In this section, dual decomposition is used to find a suboptimal TPC algorithm with low complexity.

First, the original problem (8) is decomposed into N subproblems and each subproblem is simultaneously solved. In each subproblem, the objective is changed to identify the transmit power of SU Tx that maximizes its own secrecy rate while ensuring the constraints of $I_{\max}$ and $E_{\min}$, which is formulated as follows:

$$\begin{aligned} \max_{0 \leq p_i} \quad & r_i^s \\ \text{s.t.} \quad & I_i \leq \frac{I_{\max}}{N} \\ & e_i \geq E_{\min} \\ & p_i \leq P_{\max}. \end{aligned} \quad (9)$$

In (9), each SU Tx regulates the interference to PU Rx smaller than $\frac{I_{\max}}{N}$ to meet the constraint, $\sum_{i \in \mathbb{N}} I_i \leq I_{\max}$.

To solve problem (9), we develop the Lagrangian function of (9) as follows [21]:

$$\mathcal{L}(p_i, \lambda_i, \mu_i, \kappa_i) = r_i^s + \lambda_i \left(\frac{I_{\max}}{N} - I_i \right) + \mu_i (e_i - E_{\min}) + \kappa_i (P_{\max} - p_i), \quad (10)$$

where $\lambda_i \geq 0$, $\mu_i \geq 0$ and $\kappa_i \geq 0$ are the Lagrange multipliers of each constraint in (9).

The dual problem of (9) can be formulated as follows [22]:

$$\min_{0 \leq \lambda_i, 0 \leq \mu_i, 0 \leq \kappa_i} \quad \mathcal{F}(\lambda_i, \mu_i, \kappa_i), \quad (11)$$

where $\mathcal{F}(\lambda_i, \mu_i, \kappa_i) = \max_{p_i \geq 0} \mathcal{L}(p_i, \lambda_i, \mu_i, \kappa_i)$. In this framework, the transmit power is updated to maximize $\mathcal{L}(p_i, \lambda_i, \mu_i, \kappa_i)$, whereas the Lagrange multipliers are updated to minimize $\mathcal{F}(\lambda_i, \mu_i, \kappa_i)$ in each SU Tx in an iterative manner.

To derive the suboptimal value of p_i , the Karush–Kuhn–Tucker (KKT) conditions [21] are established with complementary slackness, as follows:

$$\frac{\partial \mathcal{L}(p_i, \lambda_i, \mu_i, \kappa_i)}{\partial p_i} = \frac{\partial r_i^s}{\partial p_i} - \lambda_i \frac{\partial I_i}{\partial p_i} + \mu_i \frac{\partial e_i}{\partial p_i} - \kappa_i = 0, \quad (12)$$

$$\lambda_i \left(\frac{I_{\max}}{N} - I_i \right) = 0, \quad (13)$$

$$\mu_i (e_i - E_{\min}) = 0, \quad (14)$$

$$\kappa_i (P_{\max} - p_i) = 0, \quad (15)$$

$$0 \leq p_i, \quad 0 \leq \lambda_i, \quad 0 \leq \mu_i, \quad 0 \leq \kappa_i. \quad (16)$$

The transmit power that satisfies the KKT conditions in (12)–(16) can be derived as

$$p_i = \left[\frac{1}{\ln 2 (\lambda_i |h_{i,0}|^2 - \mu_i \zeta_i |g_{i,i}|^2 + \kappa_i) + t_i^{[s]}} - \frac{\Psi_i}{|h_{i,i}|^2} \right]^+, \quad (17)$$

where $\Psi_i = \sum_{j \in \mathbb{N} \setminus \{i\}} p_j |h_{j,i}|^2 + p_0 |h_{0,i}|^2 + \sigma^2$ and $t_i^{[s]}$ is defined as

$$t_i^{[s]} = \frac{|g_{i,i}|^2}{\mathcal{R}_i}, \quad (18)$$

where $\mathcal{R}_i = \sum_{l \in \mathbb{N}} p_l |g_{l,i}|^2 + p_0 |g_{0,i}|^2 + \sigma^2$. In (17), Ψ_i can be easily measured at SU Rx i by subtracting the signal power from SU Tx i from the total received power. Moreover, $t_i^{[s]}$ can be calculated at EH node i because the denominator of (18) is the total received power. Therefore, the transmit power of SU Tx i can be determined as shown in (17) by sharing information within set i without other sets $j \in \mathbb{N} \setminus \{i\}$, which allows the proposed algorithm to operate with low complexity.

Each Lagrange multiplier is updated using a gradient algorithm as follows [22]:

$$\begin{aligned} \lambda_i &\leftarrow \left[\lambda_i - \nu_1 \left(\frac{I_{\max}}{N} - I_i \right) \right]^+, \\ \mu_i &\leftarrow [\mu_i - \nu_2 (e_i - E_{\min})]^+, \\ \kappa_i &\leftarrow [\kappa_i - \nu_3 (P_{\max} - p_i)]^+, \end{aligned} \quad (19)$$

where ν_1 , ν_2 and ν_3 are step sizes to update each Lagrange multiplier.

The proposed algorithm operates as described in Algorithm 1. Because ϵ^{-2} iterations are required to ensure that the norm of the gradient is smaller than ϵ in the worst case [23], the computational complexity of the proposed algorithm is $O(N\epsilon^{-2})$, where N is the number of computations for the calculation of $\vec{p}$. The proposed algorithm exhibits a linear complexity with respect to N , which corresponds to a significant reduction in the computational complexity compared to that of the ES. It is worth noting that the centralized approach hinders real-time operability as it requires a long computation time to determine the TPC strategy, but the low complexity of the proposed scheme improves its practical applicability for WPCRN.

Algorithm 1 Low-complexity transmit power control algorithm

```

1: Randomly initialize  $\vec{p}, \vec{\lambda}, \vec{\mu}$  and  $\vec{\kappa}$ 
2: repeat
3:    $\vec{p}_{\text{old}} \leftarrow \vec{p}$ 
4:   for  $i = 1$  to  $N$ 
5:     Compute  $t_i^{[s]}$  according to (18)
6:     Compute  $p_i$  according to (17)
7:     Update  $\lambda_i, \mu_i$  and  $\kappa_i$  according to (19)
8:   end for
9:    $\vec{p} = \{p_1, p_2, \dots, p_N\}$ 
10: until  $\|\vec{p} - \vec{p}_{\text{old}}\| < \epsilon$ 

```

4. Simulation Results and Discussion

To evaluate the performance of the proposed scheme, the following system parameters, shown in Table 1, were set as default: $N = 3$, $P_{\max} = p_0 = 30$ dBm, $\sigma^2 = -100$ dBm, $E_{\min} = -15$ dBm, $I_{\max} = -50$ dBm and $\zeta_i = 0.5$ for $i \in \mathbb{N}$ [19,24]. Considering device-to-device communications underlay cellular networks as the target system of WPCRN [16], the SUs and EH nodes were generated randomly over an area of $50 \text{ m} \times 50 \text{ m}$, with the maximum distances of each signal link and EH link in the same node set defined as 15 m and 10 m, respectively. Moreover, the secondary network was located, on average 1 km, from PUs for reliable spectrum sharing. To generate the wireless channels, a simplified path loss model with a path loss exponent of 2.7 was considered for urban areas [18]. In addition, for multi-path fading, Rayleigh fading was used for the signal links to reflect the characteristics of non-line-of-sight (nLoS), while Rician fading with a K -factor of six was used for the EH links to reflect the characteristics of line-of-sight (LoS) [24]. The performance metrics are the average secrecy rate and outage probability, which can be mathematically expressed as $\mathbb{E} \left[\left(\mathbb{1}_{\sum_{i \in \mathbb{N}} I_i \leq I_{\max}} \right) \cdot \left(\prod_{i \in \mathbb{N}} \mathbb{1}_{e_i \geq E_{\min}} \right) \cdot \frac{1}{N} \sum_{i \in \mathbb{N}} r_i^s \right]$ and $\mathbb{E} \left[1 - \left(\mathbb{1}_{\sum_{i \in \mathbb{N}} I_i \leq I_{\max}} \right) \cdot \left(\prod_{i \in \mathbb{N}} \mathbb{1}_{e_i \geq E_{\min}} \right) \right]$, respectively. The average secrecy rate was set as zero if the constraint of $I_{\max}$ or $E_{\min}$ was violated to impose a penalty. We also considered the following five schemes for performance evaluation:

- Optimal scheme: With the complete CSI at SU TxS, the ES can attain near-optimal performance with $Q = 100$.
- Proposed TPC scheme: The transmit powers of SU TxS are determined using the proposed algorithm described in Algorithm 1.
- Barrier scheme: The transmit powers of SU TxS are determined by a centralized barrier method [21,25], which is one of interior-point methods.
- Binary TPC scheme: The transmit power of each SU Tx is determined as either $P_{\max}$ or zero in the direction of maximizing the average secrecy rate [17].
- Maximum power scheme: The transmit powers of SU TxS are always determined as their maximum transmit powers, $P_{\max}$.
- Random power scheme: The transmit powers of SU TxS are randomly determined.

Figure 2 shows the average secrecy rate and outage probability against the allowable interference level ($I_{\max}$). As $I_{\max}$ decreased, it became more difficult to satisfy the constraint of $I_{\max}$. Therefore, for conventional distributed schemes, e.g., binary TPC, maximum power and random power schemes, the outage probability increased and the average secrecy rate significantly degraded. Specifically, although the binary scheme took values of either $P_{\max}$ or zero for the transmit power, it implemented adaptive TPC and exhibited the highest performance among the conventional distributed schemes. The maximum power scheme outperformed the random power scheme, but the performance trend reverses as $I_{\max}$ decreased due to a critical violation of the constraint of $I_{\max}$. In contrast, the proposed scheme effectively regulated the amount of interference to PU Rx to the allowable level by the effective TPC even when $I_{\max} = -60$ dBm. Therefore, the performance is comparable

to that of the optimal scheme and centralized barrier scheme and the proposed scheme outperformed the conventional distributed schemes for the entire range of $I_{\max}$.

Table 1. Parameter Setup.

Parameter	Value
Number of node sets	$N = 3$
Maximum transmit power for SU Tx	$P_{\max} = 30$ dBm
Transmit power for PU Tx	$p_0 = 30$ dBm
Noise power	$\sigma^2 = -100$ dBm
Required harvested energy	$E_{\min} = -15$ dBm
Allowable interference level	$I_{\max} = -50$ dBm
Energy conversion efficiency for EH nodes	$\zeta_i = 0.5$ for $i \in \mathbb{N}$
Size of area for distributing nodes	$50 \text{ m} \times 50 \text{ m}$
Path loss exponent	2.7
K -factor of Rician fading	6

Figure 2. Performance comparison against allowable interference level ($I_{\max}$). (a) Average secrecy rate vs. $I_{\max}$. (b) Outage probability vs. $I_{\max}$.

Figure 3 shows the average secrecy rate and outage probability against the required harvested energy ($E_{\min}$). As in the case shown in Figure 2, it was hard to provide adequate energy to EH nodes to satisfy the EH requirements as $E_{\min}$ increased. Consequently, the average secrecy rate decreased and the outage probability increased for all considered schemes when $E_{\min} > -10$ dBm. In particular, the performance of the binary and random schemes was inferior to that of the proposed scheme because these schemes could not adaptively perform TPC according to variations in the channel realization or constraints. The performance of the maximum power scheme was relatively constant against the change in $E_{\min}$ because it always uses the maximum transmit power; however, the scheme achieved the worst performance due to excessive interference among node sets. In contrast, the proposed scheme exhibited near-optimal performance for the entire range of $E_{\min}$.

Figure 4 shows the average secrecy rate, outage probability and computation time against the number of node sets (N). As N increased, the node sets exhibited severe interference with one another. Therefore, the average secrecy rate decreased with N for all the considered schemes. The maximum and random power schemes corresponded to the least computation time because no computation was required to determine the transmit powers in these schemes and computation time for the binary scheme was less than that for the proposed scheme. Although the proposed scheme required a relatively high computation time to determine the transmit powers, it outperformed the conventional distributed schemes in terms of the average secrecy rate and outage probability owing to the implementation of proper TPC to reduce interference. Moreover, the performance of the proposed scheme is comparable to that of the optimal scheme with a significantly reduced computation time. The centralized barrier scheme performed slightly better than

the proposed method, but required high computation time and knowledge of perfect CSI. This result demonstrates the effectiveness of the proposed scheme in achieving secure communications with a reasonable computational complexity.

Figure 3. Performance comparison against required harvested energy (E_{min}). (a) Average secrecy rate vs. E_{min} . (b) Outage probability vs. E_{min} .

Figure 4. Performance comparison against number of node sets (N). (a) Average secrecy rate vs. N . (b) Outage probability vs. N . (c) Computation time vs. N .

Figure 5 shows the cumulative distribution function (CDF) versus the average secrecy rate. The CDF of the proposed scheme was the closest to that of the optimal scheme, which demonstrates the near-optimality of the proposed TPC strategy. Moreover, higher average secrecy rates were noted in the CDFs of the optimal and proposed schemes than in the existing distributed schemes, which indicates that the adaptive TPC is crucial to enhance the average secrecy rate.

Figure 5. CDF vs. average secrecy rate.

5. Conclusions

A low-complexity TPC algorithm to realize secure communications in WPCRN was developed, in which the transmit powers of SU Tx are optimized to maximize the average secrecy rate while ensuring the requirements of allowable interference on PUs and the minimum amount of energy for each EH node. In particular, the closed-form equation for the transmit power of each SU Tx was mathematically derived via dual decomposition and a low-complexity TPC algorithm implemented in an iterative manner was established. Simulations performed under various scenarios highlight that the proposed scheme could enhance the average secrecy rate and outage probability, e.g., at least 10% or more compared to the existing schemes at default settings, owing to the use of the adaptive TPC strategy. Moreover, the proposed scheme reduced the computation time compared to the optimal scheme, such that its computation time was less than tens of milliseconds even when the number of nodes was large.

Funding: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2021R1A2C4002024).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Chen, X.; Chen, H.; Meng, W. Cooperative communications for cognitive radio networks - From theory to applications. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1180–1192. [\[CrossRef\]](#)
- Salam, A.O.A.; Sheriff, R.E.; Al-Araji, S.R.; Mezher, K.; Nasir, Q. Adaptive threshold and optimal frame duration for multi-taper spectrum sensing in cognitive radio. *ICT Exp.* **2019**, *5*, 31–36. [\[CrossRef\]](#)
- Chen, Y.; Yu, G.; Zhang, Z.; Chen, H.; Qiu, P. On cognitive radio networks with opportunistic power control strategies in fading channels. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2752–2761. [\[CrossRef\]](#)
- Ren, W.; Zhao, Q.; Swami, A. Power control in cognitive radio networks: How to cross a multi-lane highway. *IEEE J. Sel. Areas Commun.* **2009**, *27*, 1283–1296. [\[CrossRef\]](#)
- Almalfouh, S.M.; Stuber, G.L. Interference-aware radio resource allocation in OFDMA-based cognitive radio networks. *IEEE Trans. Veh. Technol.* **2011**, *60*, 1699–1713. [\[CrossRef\]](#)
- Zhang, Y.; So, A.M. Optimal spectrum sharing in MIMO cognitive radio networks via semidefinite programming. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 362–373. [\[CrossRef\]](#)

7. Zheng, G.; Ho, Z.; Jorswieck, E.A.; Ottersten, B. Information and energy cooperation in cognitive radio networks. *IEEE Trans. Signal Process.* **2014**, *62*, 2290–2303. [\[CrossRef\]](#)
8. Yin, S.; Zhang, E.; Qu, Z.; Yin, L.; Li, S. Optimal cooperation strategy in cognitive radio systems with energy harvesting. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 4693–4707. [\[CrossRef\]](#)
9. Liu, X.; Zheng, K.; Chi, K.; Zhu, Y.H. Cooperative spectrum sensing optimization in energy-harvesting cognitive radio networks. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 7663–7676. [\[CrossRef\]](#)
10. Liu, X.; Li, F.; Na, Z. Optimal resource allocation in simultaneous cooperative spectrum sensing and energy harvesting for multichannel cognitive radio. *IEEE Access* **2017**, *5*, 3801–3812. [\[CrossRef\]](#)
11. Wang, Y.; Wang, Y.; Zhou, F.; Wu, Y.; Zhou, H. Resource allocation in wireless powered cognitive radio networks based on a practical non-linear energy harvesting model. *IEEE Access* **2017**, *5*, 17618–17626. [\[CrossRef\]](#)
12. Xu, L.; Nallanathan, A.; Pan, X.; Yang, J.; Liao, W. Security-aware resource allocation with delay constraint for NOMA-based cognitive radio network. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 366–376. [\[CrossRef\]](#)
13. Xu, D.; Li, Q. Resource allocation for cognitive radio with primary user secrecy outage constraint. *IEEE Syst. J.* **2018**, *12*, 893–904. [\[CrossRef\]](#)
14. Xu, L.; Cai, L.; Gao, Y.; Xia, J.; Yang, Y.; Chai, T. Security-aware proportional fairness resource allocation for cognitive heterogeneous networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11694–11704. [\[CrossRef\]](#)
15. Li, M.; Yin, H.; Huang, Y.; Wang, Y.; Yu, R. Physical layer security in overlay cognitive radio networks with energy harvesting. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11274–11279. [\[CrossRef\]](#)
16. Lee, W.; Ban, T.; Jung, B.C. Distributed transmit power optimization for device-to-device communications underlying cellular networks. *IEEE Access* **2019**, *7*, 87617–87633. [\[CrossRef\]](#)
17. Gjendemsj, A.; Gesbert, D.; ien, G.E.; Kiani, S.G. Binary power control for sum rate maximization over multiple interfering links. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 3164–3173. [\[CrossRef\]](#)
18. Kalamkar, S.S.; Banerjee, A. Secure communication via a wireless energy harvesting untrusted relay. *IEEE Trans. Veh. Technol.* **2017**, *66*, 2199–2213. [\[CrossRef\]](#)
19. Lee, W.; Lee, K. Resource allocation scheme for guarantee of QoS in D2D communications using deep neural network. *IEEE Commun. Lett.* **2021**, *25*, 887–891. [\[CrossRef\]](#)
20. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [\[CrossRef\]](#)
21. Boyd, S.; Vandenberghe, L. *Convex Optimization*; Cambridge University Press: Cambridge, UK, 2004.
22. Yu, W.; Lui, R. Dual methods for nonconvex spectrum optimization of multicarrier systems. *IEEE Trans. Commun.* **2006**, *54*, 1310–1321. [\[CrossRef\]](#)
23. Fliege, J.; Vaz, A.I.F.; Vicente, L.N. Complexity of gradient descent for multiobjective optimization. *Optim. Methods Softw.* **2018**, *34*, 949–959. [\[CrossRef\]](#)
24. Lu, X.; Wang, P.; Niyato, D.; Kim, D.I.; Han, Z. Wireless networks with RF energy harvesting: A contemporary survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 757–789. [\[CrossRef\]](#)
25. Sengly, M.; Lee, K.; Lee, J.-R. Joint optimization of spectral efficiency and energy harvesting in D2D networks using deep neural network. *IEEE Trans. Veh. Technol.* **2021**, *70*, 8361–8366. [\[CrossRef\]](#)