Bandwidth and Power Allocation for Wireless Cognitive Network with Eavesdropper

Kecai Gu[1(✉)], Weidang Lu[1], Guomin Zhou[2], Hong Peng[1], Zhijiang Xu[1], and Xin Liu[3]

[1] School of Information Engineering, Zhejiang University of Technology, Hangzhou, China
celus@zjut.edu.cn
[2] Zhejiang Police College, Hangzhou, China
[3] School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China

Abstract. In this paper, we consider secure communications for a five-node cognitive wireless network system including one primary user (PU) pair and one secondary user (SU) pair in presence of one eavesdropper. The secrecy transmission process departs into two equal time phases. To ensure transmission process safety, the primary source and receiver are allowed to deliver artificial noise to interfere the eavesdropper. To obtain higher spectrum efficiency, we propose an anti-interference spectrum access strategy with cooperative trusted DF relaying over flat fading channel, in which secondary user forward primary information and deliver its own information with different part of licensed spectrum. We study how to optimize the bandwidth and power allocation ratio to maximize the secondary user rate while guaranteeing the primary system to achieve its target secrecy rate. The expression of the optimal bandwidth allocation ratio is derived. Simulation results demonstrate that proposed strategy can achieve win-win result.

Keywords: Cognitive radio · Physical layer security · Artificial noise · Achievable secrecy rate · Power allocation

1 Introduction

Spectrum utilization has received a lot of attention during the past decade due to the rarity of radio spectrum and the fixed spectrum allocation strategy which divide the spectrum into two parts: licensed spectrum and unlicensed spectrum [1]. Traditional fixed spectrum allocation strategy authorizes the specific communication system use the specific spectrum but doesn't allow others to use it even when licensed user doesn't use the spectrum sometimes. It leads to low utilization and waste of spectrum resource in time and space. Cognitive radio [2] (CR) is a promising technology to improve the wireless spectrum utilization by supporting the unlicensed systems access to the same spectrum resource already licensed to the primary systems while not degrading the performance of primary system. However, there are two main problems in the existing underlay spectrum access strategy in CR network. One is that there will be interference

X.-L. Huang (Ed.): MLICOM 2016, LNICST 183, pp. 217–227, 2017.
DOI: 10.1007/978-3-319-52730-7_22

between the primary system and secondary system when the cognitive user forward the primary user information and deliver own information simultaneously. The other is the secondary user is allowed to access to the licensed spectrum if and only if the channel of primary system is good enough. Cooperative diversity has been proposed as a spatial diversity technique to solve the above problems [3]. Because it can degrade the influence of path loss in wireless links. Thus we exploit the cooperative diversity technology to overcome the existing shortcomings and improve the utilization of licensed spectrum.

Another issue in wireless communication environment is the security [4]. Wireless communication is not secure as wire communication due to the openness of the wireless medium. Some illegal receivers within the communication range may wiretap and decode the secrecy information, which easily lead to the information leakage. The security of traditional wireless communication depends on the upper layers of the protocol stack through the use of encryption algorithms [5, 6]. But there are still some challenges such as secret key management complexity, key transmission and distribution security issues in open wireless communication environment and so on. Significant works have been done on physical (PHY) layer security and various advanced signal processing and coding techniques have been proposed to improve the secrecy of the wireless communication in the presence of some eavesdroppers. Shannon firstly investigates information theoretic security in 1949 and Wyner introduce the conception of secrecy capacity [7]. The secrecy rate is defined as the difference between achievable rates of the main channel and the wiretap channel with the Gaussian code-book and the maximum of secrecy rate is defined as secrecy capacity. Positive secrecy rate only exist when the main channel is more advantage than wiretap channel. But now, we can achieve a positive secrecy rate even when the main channel is worth than wiretap channel with using the nodes cooperative technology. Generally, there are two main methods to improve the information security. One is cooperative note plays as a jammer to deteriorate the wiretap channel. The other is cooperative node plays as trusted relay to help the primary system improve the channel quality to the legitimate user. Cooperative jamming has been studied in paper [8, 9] to maximum the achievable secrecy rate While Cooperative beam-forming (CB) are studied in [10, 11]. Cooperative nodes can forward the confidential information in above both manners based on DF or AF ways.

In this paper, we exploit the artificial noise [12–15] to confuse the eavesdropper to ensure the security transmission. To improve the utilization of spectrum resource and eliminate the mutual interference between primary and secondary system, a kind of effective spectrum access strategy have been proposed, in which secondary system is allowed to transmit primary and its own information with different bandwidth on the condition that it gets access to the licensed spectrum. Our goal is to study how to optimize the bandwidth and power allocation ratio to maximize the secondary user rate while guaranteeing the primary system to achieve its target secrecy rate.

2 System Model and Problem Formulation

2.1 System Model

The system configuration of the proposed anti-wiretapping access strategy is show in Fig. 1. The whole system consists of primary system including one PT (Primary Transmitter) and one PR (Primary Receiver) and secondary system including one ST (Secondary Transmitter) and one SR (Secondary Receiver) in the presence of one eavesdropper. We assume that ST is trusted. The PR can transmit and receive simultaneously while others operate in a half-duplex mode. All notes are equipped with a single antenna. In this paper, we assume the channel are quasi-static Rayleigh channel, the channel coefficient $h_i > 0$ where $i = \{1, 2, 3, 4, 5, 6\}$ and $r_i = |h_i|^2$ represents the instantaneous channel gain, d_i imply distance between two nodes and v is the path-loss exponent (typically value from 2 to 6). All channels coefficient remain unchanged during both phases. For simplicity, we assume that the noise at all the nodes is complex addictive white Gaussian noise (AWGN) with zero means and variance. The total power of primary and secondary system is constrained by p and p_s respectively.

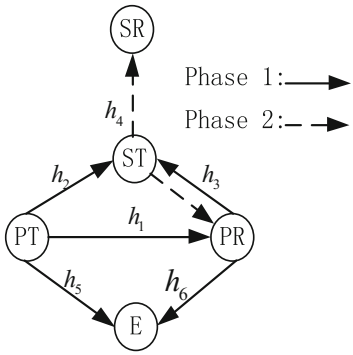

Fig. 1. System model

In order to transmit information safely, the transmission process departs into two equal time phases. We assume transmission time is 1, each phase accounted for 1/2. In phase1, PT delivers the information including artificial noise and the secrecy signal to PR and ST while the PR transmits the no-information-bearing artificial noise concurrently to PR. The eavesdropper is passive and only phase 1 could be tapped. In phase 2, ST forward the message to PR in DF fashion with part of licensed bandwidth and use the rest spectrum to transmit own information. There would be no interference between primary and secondary user with using different spectrum. Note that ST is permitted to operate in the licensed spectrum if and only if it can guarantee the secrecy Rate of the primary system.

2.2 Problem Formulation

The instantaneous secrecy rate of primary system is defined as

$$R_Q = (R_p - R_E)^+ \tag{1}$$

where R_p and R_E represents the instantaneous rate of the primary system and eavesdropper. $(x)^+ = \max(x, 0)$.

Firstly, we consider that the PT only delivers the secrecy information to PR without the help of secondary user. And the received signal at E and PR are given as follows

$$y_{sd} = \sqrt{p}h_2 x + n_{sd} \tag{2}$$

$$y_{se} = \sqrt{p}h_5 x + n_{se} \tag{3}$$

where n_{sd} and n_{se} is noise and follows $CN(0, \sigma^2)$. x implies the secrecy signal. So the rate of the primary system R_D and eavesdropper R_E can be written as

$$R_D = W \log_2(1 + \frac{p_p \gamma_1}{\sigma^2}) \tag{4}$$

$$R_E = W \log_2(1 + \frac{p_p \gamma_5}{\sigma^2}) \tag{5}$$

when $R_D - R_E < R_T$, where R_T is the secrecy rate threshold of the primary system, primary user seeks help from around user. The secondary user judge whether or not it can access to the licensed spectrum through the two time slots.

In phase 1, the transmitted signal by PT(x_1) and PR(x_2) are respectively given by

$$x_1 = \sqrt{p\alpha}s + \sqrt{p(1-\alpha)}u_1 z \tag{6}$$

$$x_2 = \sqrt{p(1-\alpha)}u_2 z \tag{7}$$

where x_1 is a mixture of the information signal and the jamming signal and x_2 is purely artificial jamming signal designed to cancel out the interference at ST while further confuse the eavesdropper. α implies the power allocation ratio of between the information signal s and jamming signal z. both of them are unit-power. u_1 and u_2 are the weight coefficients and satisfy

$$|u_1|^2 + |u_2|^2 = 1 \tag{8}$$

The received signal at ST then given by

$$\begin{aligned} r_{ST} &= \sqrt{p\alpha}h_2 s + \sqrt{p(1-\alpha)}h_2 u_1 z + \sqrt{p(1-\alpha)}h_3 u_2 z + n_{sr} \\ &= \sqrt{p\alpha}h_2 s + \sqrt{p(1-\alpha)}(u_1 h_2 + u_2 h_3) z + n_{sr} \end{aligned} \tag{9}$$

The ST decodes the secrecy information and re-encodes it with the same code-words of source in phase 2. To avoid the interference of artificial noise at ST, we design

$$u_1 h_2 + u_2 h_3 = 0 \tag{10}$$

So the received signal can be rewritten as

$$r_{ST} = \sqrt{p\alpha} h_2 s + n_{sr} \tag{11}$$

The eavesdropper is passive and only wiretap the signal in phase 1 while keep silence in phase 2. It couldn't remove the jamming signal, so the received signal is given by

$$\begin{aligned} r_E &= \sqrt{p\alpha} h_5 s + \sqrt{p(1-\alpha)} h_5 u_1 z + \sqrt{p(1-\alpha)} h_6 u_2 z + n_{sr} \\ &= \sqrt{p\alpha} h_2 s + \sqrt{p(1-\alpha)} (u_1 h_5 + u_2 h_6) z + n_{sr} \end{aligned} \tag{12}$$

Due to the mixture signal, PR receives the signal with artificial noise

$$r_d = \sqrt{p\alpha} h_1 s + \sqrt{p(1-\alpha)} h_1 u_1 z + n_{sd} \tag{13}$$

The rate of PR(R_d^1), ST(R_p^1) and E(R_E) are given respectively by

$$R_p^1 = \frac{1}{2} w \log_2 (1 + \frac{p\alpha\gamma_2}{\sigma^2}), \tag{14}$$

$$\begin{aligned} R_E &= \frac{1}{2} w \log_2 (\frac{P\alpha |h_5|^2}{\sigma^2 + p(1-\alpha)|u_1 h_5 + u_2 h_6|^2}) \\ &= \frac{1}{2} w \log_2 (\frac{P\alpha\gamma_5}{\sigma^2 + p(1-\alpha)\gamma_m}), \end{aligned} \tag{15}$$

$$R_d^1 = \frac{1}{2} w \log_2 (1 + \frac{p\alpha\gamma_1}{\sigma^2 + p\alpha u_1^2 \gamma_1}). \tag{16}$$

where $\gamma_m = |u_1 h_5 + u_2 h_6|^2$, w represents the licensed bandwidth. The coefficient factor 1/2 is due to the fact that every transmission process needs two phases.

During phase 2, ST allocate a fraction of bandwidth and half of power to forward the secrecy message to PR, the rate $ST \rightarrow PR$ is

$$R_d^2 = \frac{1}{2} bw \log_2 (1 + \frac{\frac{1}{2} p_s \gamma_3}{\sigma^2}) \tag{17}$$

where b represents the bandwidth allocation ratio between primary user and secondary user.

Then ST use the remaining bandwidth and the other half of power to transmit its own information, the rate ST → SR is given by

$$R_s = \frac{1}{2}(1-b)w\log_2(1+\frac{\frac{1}{2}p_s\gamma_4}{\sigma^2}) \tag{18}$$

The eavesdropper is not interested in ST and keeps silence in phase 2. If ST can decode successfully, PR apply the maximum ratio combination (MRC) to received message over two phases, then the primary system rate R_p^2 can be given as

$$\begin{aligned} R_p^2 = &\frac{1}{2}bw\log_2(1+\frac{P_s\gamma_3}{2\sigma_2}+\frac{p\gamma_1\alpha}{\sigma^2+P(1-\alpha)u_1^2\gamma_1}) \\ &+\frac{1}{2}(1-b)w\log_2(1+\frac{p\gamma_1\alpha}{\sigma^2+P(1-\alpha)u_1^2\gamma_1}) \end{aligned} \tag{19}$$

So after the two transmission process, the primary system rate R_p can be written as $R_p = \min\left\{R_p^1, R_p^2\right\}$.

ST can forward the Primary user information only when ST can decode successfully. So operation symbol min means the performance of the primary link is limited to the worse the link of $PT \rightarrow PR$ and $PT \rightarrow ST$.

With the help of ST, if R_p can achieve the target secrecy rate, that is $R_p - R_E > R_T$, the primary system authorizes the secondary user to use the licensed spectrum. If not, the secondary user will do nothing.

3 Optimal Solution

In this section, we study how to optimize the allocation coefficient of the bandwidth b and power allocation ratio α to maximum the secondary user rate R_s while keep the primary system secrecy rate achieve the target secrecy rate threshold RT. First, we give the solution to the designed artificial noise parameters u_1, u_2

$$s.t. \qquad \begin{cases} u_1h_2 + u_2h_3 = 0 \\ |u_1|^2 + |u_2|^2 = 1 \end{cases} \tag{20}$$

We can easily solve the equation and get

$$\begin{cases} u_1 = -\sqrt{\frac{|h_3|^2}{|h_2|^2+|h_3|^2}} \\ u_2 = \sqrt{\frac{|h_2|^2}{|h_2|^2+|h_3|^2}} \end{cases} \tag{21}$$

Or

$$\begin{cases} u_1 = \sqrt{\frac{|h_3|^2}{|h_2|^2+|h_3|^2}} \\ u_2 = -\sqrt{\frac{|h_2|^2}{|h_2|^2+|h_3|^2}} \end{cases} \tag{22}$$

In the following part, we derive the explicit expression of optimal b. The optimization problem can be translated into the follows

$$\max_{b,\alpha} Rs \tag{23}$$

It yields

$$\begin{cases} R_p - R_E \geq R_T \\ 0 < b < 1 \\ 0 < \alpha < 1 \end{cases} \tag{24}$$

For simplicity, this paper introduce some auxiliary variables R_2, R_3, R_4, R_d are given as following

$$\begin{cases} R_2 = w\log_2(1+\frac{p\alpha\gamma_2}{\sigma^2}) \\ R_3 = w\log_2(1+\frac{p_s\gamma_3}{2\sigma^2}+\frac{p\alpha\gamma_1}{p(1-\alpha)u_1^2\gamma_1+\sigma^2}) \\ R_4 = w\log_2(1+\frac{p_s\gamma_4}{\sigma^2}) \\ R_d = w\log_2(1+\frac{p\alpha\gamma_1}{p(1-\alpha)u_1^2\gamma_1+\sigma^2}) \end{cases} \tag{25}$$

Then we can rewrite R_p^1, R_p^2 and get $R_p^1 = \frac{1}{2}R_2$, $R_p^2 = \frac{1}{2}bR_3 + \frac{1}{2}(1-b)R_d$. According to the constraints, we can obtain

$$\begin{cases} \frac{1}{2}R_2 - R_E \geq R_T \\ \frac{1}{2}bR_3 + \frac{1}{2}(1-b)R_d - R_E \geq R_T \\ 0 < b < 1 \\ 0 < \alpha < 1 \end{cases} \tag{26}$$

From condition, we can derive the linear inequality about b given by

$$b \geq \frac{2(R_T+R_E)-R_d}{R_3-R_d} \tag{27}$$

We can easily observe that R_s is monotonically decreasing function of b, so the optimal bandwidth allocation coefficient b can expressed

$$b^* = \frac{2(R_T+R_E)-R_d}{R_3-R_d} \tag{28}$$

Subject to

$$\begin{cases} R_2 \geq 2(R_T + R_E) \\ R_D \leq 2(R_T + R_E) \\ R_3 \geq 2(R_T + R_E) \end{cases} \tag{29}$$

We can get the maximization rate of secondary user and is given by

$$R_s^* = \frac{[R_3 - 2(R_T + R_E)]R_4}{2(R_3 - R_d)} \tag{30}$$

Our goal is to maximize R_s, so we can obtain optimal α through minimize the power allocation ratio b.

4 Simulation Results

In this section, we investigate the performance of the proposed strategy numerically. The simulation setting is as follows. The five nodes are located in a 2-D square topology we set the PT, PR, ST in the same line. PT, PR are located in (0,0) and (1,0) respectively. So the distance between PT and PR is 1. ST moves from (0,0) to (1,0). The distance between ST and SR is constant $d_4 = 0.5$ and the eavesdropper is fixed in the place where $d_5 = 0.14$, $d_6 = 1$; In our simulation, we assume that the path-loss exponent v is -3, the licensed spectrum bandwidth is 1, and the noise variance is 1. The power of the primary system and secondary system is p = 8 dB, p_s = 10 dB respectively.

In the Fig. 2, we let x axis implies the location of ST, and y axis implies the optimal allocation ratio of bandwidth b. From the picture, when ST is close to PT, $b^* = 1$, $\alpha^* = 0$, $R_s = 0$. The reason is the primary system secrecy rate R_Q is small and ST can't help primary system achieve the target secrecy rate, so it can't get access to the licensed spectrum. With ST is far from PT, R_Q is getting large and exceed the target rate, so the secondary user allocates part of bandwidth to forward secrecy information to PR. However, R_Q is getting low again along with ST move further away from PT, R_2 will decrease and can't satisfy the condition $R_2 - 2R_E \geq 2R_T$, the secondary user can't acquire opportunity to access to the primary system, so b skip to 0. From the Fig. 2, the access range when $R_T = 1.2\,\text{bps/HZ}$ is large than $R_T = 1.5\,\text{bps/HZ}$ due to the secondary system is easier to help primary system get the lower target secrecy rate.

Figure 3 describes the secondary system rate under different target secrecy rate with the different location of ST, when $d_2 < 0.249$ under $R_T = 1.2\,\text{bps/HZ}$, $R_s = 0$, this implies that R_Q is not large enough to support ST to help the primary user to achieve the target rate. With ST move far from PT and near to PR, R_Q is getting high. So the secondary user access to the licensed spectrum and R_s becomes positive. But when ST further gets close to PR, as $d_2 > 0.704, R_s$ return to 0 due to R_Q decrease again. Therefore, secondary system can't provide support and get to access. Compared with $R_T = 1.2\,\text{bps/HZ}$, secondary system get narrower access ranges when $R_T = 1.5\,\text{bps/HZ}$. The higher R_T is, the more difficult for secondary system to help

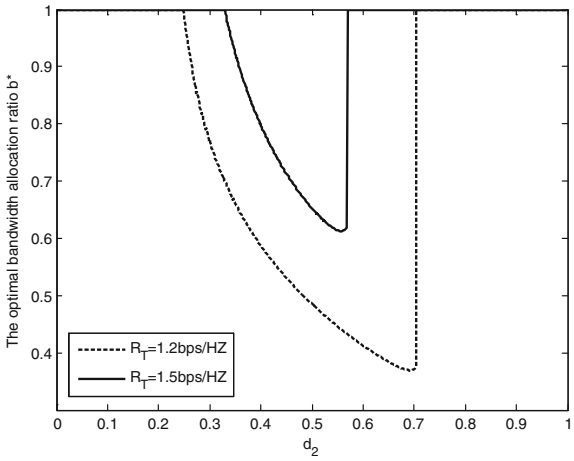

Fig. 2. The optimal bandwidth allocation ratio b^* vs. the distance between PT and ST d_2.

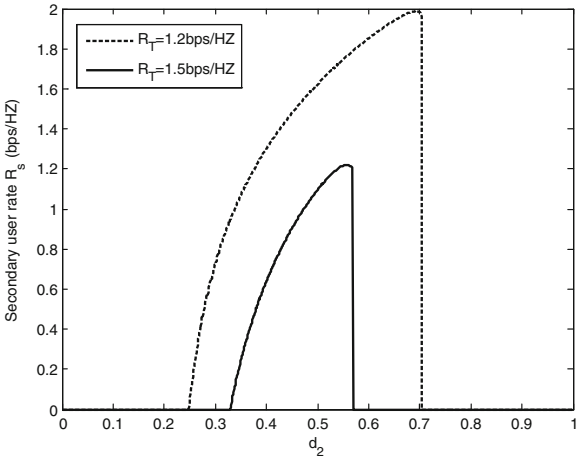

Fig. 3. Secondary user rate R_s vs. the distance between PT and ST d_2.

primary system to achieve the target secrecy rate. There are less left bandwidth for secondary system to transmit own information. So R_s is lower.

Figure 4 represents the optimal power allocation ratio between secrecy information and artificial noise for ST. The optimal α can be obtained through minimize the bandwidth allocation ratio. In other word, we get optimal a by maximizing the secondary user target rate R_s. In our communication scenario, the eavesdropper E is close to ST, to confuse eavesdropper and transmit confidential information, more power are allocated to transmit artificial noise. Therefore, we can see that α is relatively small and

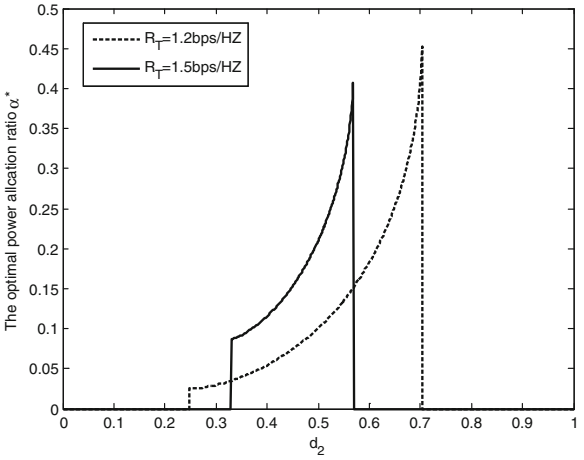

Fig. 4. The optimal power allocation ratio vs. the distance between PT and PR d_2

the maximum value of α is about 0.45 from the picture. Due to the same reason, α can get larger access ranges when $R_T = 1.2\,\mathrm{bps/HZ}$.

5 Conclusion

In this paper, we have proposed an anti-interference strategy to solve the secure transmission problem in flat fading channel for the cognitive radio network in present of an eavesdropper. To improve the bandwidth utilization while ensuring information transmission safety, we allowed PT allocates part of available power for artificial noise to confuse the eavesdropper. Meanwhile, we derived the optimization bandwidth allocation ratio for ST and analyzed the optimal power allocation ratio of PT which can maximum the secondary transmission rate while the secrecy rate throughout constraint of primary user is satisfied. Further work includes the explicit derivation and analysis of power allocation problems.

Acknowledgments. This work was supported by China National Science Foundation under Grand No. 61402416 and 61303235, Natural Science Foundation of Zhejiang Province under Grant No. LQ14F010003 and LQ14F020005, NSFC-Zhejiang Joint Fund for the Integration of Industrialization and Informatization under grant No. U1509219, Natural Science Foundation of Jiangsu Province under Grant No. BK20140828, the Fundamental Research Funds for the Central Universities under Grant No. DUT16RC(3)045 and the Scientific Foundation for the Returned Overseas Chinese Scholars of State Education Ministry.

References

1. Goldsmith, A., Jafar, S., Maric, I., Srinivasa, S.: Breaking spectrumgridlock with cognitive radios: an information theoretic perspective. Proc. IEEE **97**(5), 894–914 (2009)
2. Wang, C., Wang, H.M.: On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels. IEEE Trans. Inf. Forensics Secur. **9**(11), 1814–1827 (2014)
3. Ikki, S.S., Ahmed, M.H.: Performance analysis of decode-and-forward incremental relaying cooperative-diversity networks over Rayleigh fading channels. In: 2009 IEEE 69th Vehicular Technology Conference, VTC Spring 2009, Barcelona, pp. 1−6 (2009)
4. Liu, R., Trappe, W. (eds.): Securing Wireless Communications at the Physical Layer. Springer, New York (2010)
5. Liang, Y., Poor, H.V., Shamai, S.: Information Theoretic Security. NowPublishers, Delft (2009)
6. Ramesh, A., Suruliandi, A.: Performance analysis of encryption algorithms for information security. In: 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), Nagercoil, pp. 840–844 (2013)
7. Wyner, A.D.: The wire-tap channel. Bell Sys. Tech. J. **54**, 1355–1387 (1975)
8. Dong, L., Han, Z., Petropulu, A.P., Poor, H.V.: Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)
9. Huang, J., Swindlehurst, A.L.: Cooperative jamming for secure communications in MIMO relay networks. IEEE Trans. Signal Process. **59**(10), 4871–4884 (2011)
10. AbolfathBeigi, M., Mohammad Razavizadeh, S.: Cooperative beamforming in cognitive radio networks. In: 2009 2nd IFIP Wireless Days (WD), Paris, pp. 1–5 (2009)
11. Yi, T., Guo, L., Niu, K., Cai, H., Lin, J., Ai, W.: Cooperative beam-forming in cognitive radio network with hybrid relay. In: 2012 19th International Conference on Telecommunications (ICT), Jounieh, pp. 1–5 (2012)
12. Kabeya, J., Takyu, O., Ohtsuki, T., Sasamori, F., Handa, S.: Performance evaluation of the physical layer security using artificial noise and relay station. In: 2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), Hong Kong, pp. 834–839 (2015)
13. Zhou, X., McKay, M.R.: Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation. IEEE Trans. Veh. Technol. **59**(8), 3831–3842 (2010)
14. Deng, H., Wang, H.M., Wang, W., Yin, Q.: Secrecy transmission with a helper: to relay or not to relay. In: 2014 IEEE International Conference on Communications Workshops (ICC), Sydney, NSW, pp. 825–830 (2014)
15. Deng, H., Wang, H.-M., Guo, W., Wang, W.: Secrecy transmission with a helper: to relay or to jam. IEEE Trans. Inf. Forensics Secur. **10**(2), 293–307 (2015)