Secrecy Outage Probability of Cognitive Small-Cell Network with Unreliable Backhaul Connections

Jinghua Zhang(✉), Chinmoy Kundu, and Emi Garcia-Palacios

Queen's University Belfast, Belfast BT9 5AH, UK
{jzhang22,c.kundu}@qub.ac.uk, e.garcia@ee.qub.ac.uk

Abstract. In this paper, we investigate the secrecy performance of underlay cognitive small-cell radio network with unreliable backhaul connections. The secondary cognitive small-cell transmitters are connected to macro base station by wireless backhaul links. The small-cell network is sharing the same spectrum with the primary network ensuring that a desired outage probability constraint in the primary network is always satisfied. We propose an optimal transmitter selection (OTS) scheme for small-cell network to transfer information to the destination. The closed-form expression of secrecy outage probability are derived. Our result shows that increasing the primary transmitter's transmit power and the number of small-cell transmitter can improve the system performance. The backhaul reliability of secondary and the desired outage probability of the primary also have significant impact on the system.

Keywords: Unreliable backhaul · Cognitive radio network
Small-cell network · Physical layer security · Secrecy outage probability

1 Introduction

Due to the explosion of data-intensive applications and wireless systems such as the Internet of Things (IoT) and smart cities, the deployment of wireless infrastructure is expected to get more dense and heterogeneous in the near future [1]. To reach such high data rate, the backhaul links connecting the macro-cell and many small-cells in the heterogeneous networks (HetNets) are also expected to become dense. In the conventional wired backhaul network, high reliability wired links and high data rate can be expected, however, the deploying and sustaining the large-scale wired links require excessive capital investment for all the connections [2,3]. This leads wireless backhaul as alternative solution since it has been proven cost-effective and flexible in practical systems. However, wireless

This work was supported in part by the Royal Society-SERB Newton International Fellowship under Grant NF151345.

I. Moerman et al. (Eds.): CROWNCOM 2018, LNICST 261, pp. 89–98, 2019.
https://doi.org/10.1007/978-3-030-05490-8_9

backhaul is unlikely reliable as wired backhaul due to non-line-of-sight (n-LOS) propagation and fading of wireless channels [4].

The aforementioned rapid development in wireless devices and services is also pushing the demand for spectrum while most of licensed spectrum bands are occupied [5]. In recent years, the investigation on cognitive radio (CR) techniques [6] has attracted many experts' attention. CR optimises the current spectrum usage, which allows unlicensed secondary users to share the same spectrum with the licensed primary users in an opportunistic manner. The authors in [7] analysed the impact of the primary network on the secondary network. In [8], the authors optimizing the time and power allocation in the secondary network. To improve the CR or noncognitive network performance, user selection is always among the secondary users and relays in the literature [9–12].

For a complete study, we also consider the challenges of security in the wireless communication network. Due to the broadcasting nature of wireless channels, the confidential information in wireless network is vulnerable to eavesdropping and security attacks. In reality, CR networks are easily susceptable to eavesdropping. The conventional way from upper layer security is deploying data encryption for secure communication, on the other hand, physical layer security (PLS) obtains the advantage from the randomness of the wireless channels for information security extensively. PLS has become increasingly popular to deal with wiretapping and possible loss of confidentiality. Some research has investigated the secrecy performance using PLS [9,13–16].

Nevertheless, all the aforementioned work did not take into account the impact of unreliable backhaul on PLS of CR network. Some literatures in CR network only consider the interference on the primary network. In some literature on backhaul CR networks [4,17–19], authors investigated the secrecy performance but not consider the system with secondary user selection schemes. The impact of guaranteeing outage as a quality-of-service (QoS) in the primary networks was not considered either in aforementioned paper. Our research address these key issues in CR network with backhaul. We investigate the secrecy performance of CR network with unreliable backhaul connections. Based on those considerations, our contribution of this paper is summarised as follows:

1. We take into account the backhaul unreliability in secrecy performance. We develop the close-form expression of the secrecy outage probability.
2. We consider interference both in primary and secondary receiver.
3. We consider primary QoS constraint metric as outage probability, which is different from other works in CR.
4. Our model investigates a small-cell transmitter selection schemes, namely, optimal transmitter selection (OTS) which prioritizes the maximum channel gain S–D, and also assesses the influences of varying the number of small-cell transmitter.

The rest of the paper is organised as follows. In Sect. 2, the system channel models are described. Section 3 demonstrates the secrecy outage probability of propose system. Numerical results from monte-carlo simulations are showcased in Sect. 4. Finally, the paper is concluded in Sect. 5.

2 System and channel models

As illustrated in Fig. 1, the system is consisting of a primary network with one primary transmitter, T, one primary receiver, R and a secondary network consisting of K small-cells transmitters, $\{S_1, ..., S_k, ..., S_K\}$ which are connected to a macro-base station, BS, by unreliable backhaul links, one secondary destination, D, and one eavesdropper, E. All nodes are equipped with single antenna. We assume all nodes are sufficiently separated from each other so that $T-R$, $T-D$, $T-E$, $S-R$, $S-D$ and $S-E$ experience independent and identically distributed Rayleigh fading. The channel between nodes are denoted by h_X where $X = \{ TR, TD, TE, SR, SD, SE \}$ channel power gains are exponential distributed with parameters λ_x for $x = \{ tr, td, te, sr, sd, se \}$, respectively. The noise at R , E and D is modelled as the additive white Gaussian noise (AWGN) with zero mean and variances N_0. One best transmitter will be selected among K small-cell transmitters, to transfer information to D. While the message is sent from the BS to small-cell transmitters, the backhaul link might have certain probability of failure. Backhaul reliability is modelled as Bernoulli process with success probability, $\mathbb{P}(\mathbb{I}_k = 1) = \Lambda$, and failure probability is $\mathbb{P}(\mathbb{I}_k = 0) = 1 - \Lambda$ for each $k = 1, \cdots, K$. We investigate the secrecy outage probability (SOP) of the secondary network.

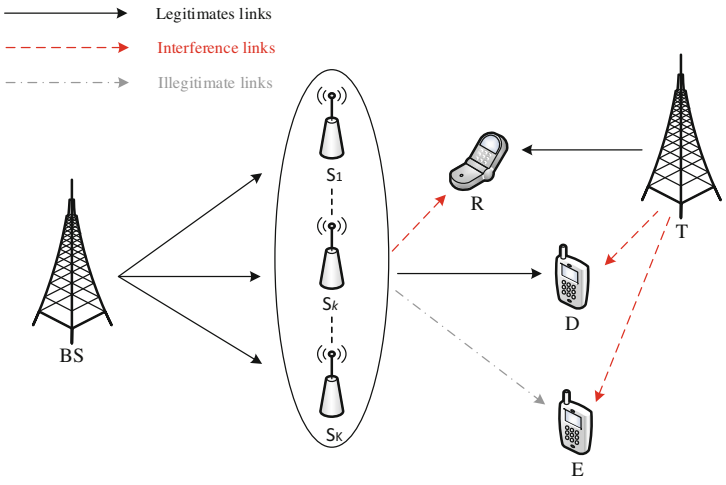

Fig. 1. Underlay cognitive radio network with unreliable backhaul connections.

2.1 Interference at Primary and Secondary Power Constraint

The primary network is interfered from the selected secondary transmitter, S_k, for $k = \{1, ..., K\}$ via interference channels $h_{S_k R}$ during the secondary network transmission. The signal-to-interference-plus-noise-ratio (SINR) at R is given as

$$\Gamma_R = \frac{P_T|h_{TR}|^2}{P_S|h_{S_kR}|^2 + N_0}, \tag{1}$$

where P_S is the maximum allowed transmit power of small-cell transmitter which satisfies the primary network QoS constraint, h_{TR} is the channel coefficient of the T − R link, and h_{S_kR} is the channel coefficient of the S − R link. To protect the primary network, the secondary network transmitters must adapt their transmit power. Moreover, the secondary network transmit power must be limitedly the QoS of the primary network which characterized by its desired outage probability. The primary network outage probability should be below a desired level, Φ. The desired outage probability constraint is defined as follows

$$\mathbb{P}\left[\Gamma_{\mathrm{R}} < \Gamma_0\right] \leq \Phi, \tag{2}$$

where $\Gamma_0 = 2^{\beta} - 1$, β is the target rate of the primary network, and $0 < \Phi < 1$. From (1) and (2), output power of secondary transmitter can be derived from the desired outage probability at the primary network

$$P_S = \begin{cases} P_T\lambda_{sr}\xi, & \text{if} \quad \xi > 0 \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

where

$$\xi = \frac{1}{\lambda_{tr}\Gamma_0}\left[\frac{\exp\left(\frac{-\lambda_{tr}\Gamma_0}{\Gamma_T}\right)}{1-\Phi} - 1\right]. \tag{4}$$

Here, we used CDF of $\Gamma_{\mathrm{R}}(x)$ to find P_S in close-form. The CDF of $\Gamma_{\mathrm{R}}(x)$ can be derived from the definition of CDF as

$$F_{\mathrm{R}}(x) = 1 - \frac{\frac{\lambda_{sr}\Gamma_T}{\lambda_{tr}\Gamma_S}}{x + \frac{\lambda_{sr}\Gamma_T}{\lambda_{tr}\Gamma_S}}\exp\left(\frac{-\lambda_{tr}x}{\Gamma_T}\right), \tag{5}$$

where $\Gamma_T = \frac{P_T}{N_0}$ and $\Gamma_S = \frac{P_S}{N_0}$.

2.2 Proposed Source Selection and Interference at the Secondary

To mitigate the eavesdropping, OTS scheme is proposed where a source is selected to forward the message such that it maximize $\mathrm{S}_k - \mathrm{D}$ link power gain as

$$k^* = \arg\max_{1\leq k\leq K} P_S|h_{S_kD}|^2. \tag{6}$$

Due to the unreliability of the backhaul, the selected link may not be active. To consider backhaul reliability into the performance analysis, we model backhaul reliability using Bernoulli random variable $\mathbb{I}$. The SINR at D can be given as

$$\Gamma_{SD} = \mathbb{I}\tilde{\Gamma}_{SD}, \tag{7}$$

where

$$\tilde{\Gamma}_{SD} = \frac{P_S \max[|h_{S_k D}|^2]}{P_T|h_{TD}|^2 + N_0}. \tag{8}$$

SINR at E can be similarly expressed as

$$\Gamma_{SE} = \frac{P_S|h_{S_k E}|^2}{P_T|h_{TE}|^2 + N_0}. \tag{9}$$

Conditioned on the source has already been selected, E always experience its intercepted signal power as independent exponentially distributed, hence, while finding the distribution of Γ_{SE} no backhaul reliability parameter comes into play in (9). However, that is not true for Γ_{SD} in (7). The distribution of Γ_{SD} will be the mixture distribution of $\mathbb{I}$ and $\tilde{\Gamma}_{SD}$. Now the distribution of Γ_{SD} can be obtained from the mixture distribution due to backhaul reliability as

$$f_{SD}(x) = (1 - \Lambda)\delta(x) + \Lambda \tilde{f}_{SD}, \tag{10}$$

where $f_{SD}(x)$, $\tilde{f}_{SD}(x)$ are the PDFs of Γ_{SD} and $\tilde{\Gamma}_{SD}$, respectively and $\delta(x)$ is delta function. CDF of $f_{SD}(x)$ can be obtained just by integrating it and finding the CDF of $\tilde{\Gamma}_{SD}$.

The CDF of $\tilde{\Gamma}_{SD}$ can be evaluate from the definition of CDF with the help of the CDF of $\max|h_{S_k D}|^2$ and the PDF of $|h_{TD}|^2$ as

$$\begin{aligned}
\tilde{F}_{SD}(x) &= \mathbb{P}\left[\frac{P_S \max|h_{S_k D}|^2}{P_T|h_{TD}|^2 + N_0} < x\right] \\
&= \mathbb{P}\left[P_S \max_{k=1,\ldots,K}|h_{S_k D}|^2 < (P_T|h_{TD}|^2 + N_0)x\right] \\
&= 1 - \sum_{k=1}^{K} \binom{K}{k} \frac{(-1)^{k+1} \frac{\lambda_{td}\Gamma_S}{k\lambda_{sd}\Gamma_T}}{x + \frac{\lambda_{td}\Gamma_S}{k\lambda_{sd}\Gamma_T}} \exp\left(\frac{-k\lambda_{sd}x}{\Gamma_S}\right).
\end{aligned} \tag{11}$$

The CDF of Γ_{SD} then can be evaluate with the help of (10) as

$$F_{SD}(x) = 1 - \Lambda \sum_{k=1}^{K} \binom{K}{k} \frac{(-1)^{k+1} \frac{\lambda_{td}\Gamma_S}{k\lambda_{sd}\Gamma_T}}{x + \frac{\lambda_{td}\Gamma_S}{k\lambda_{sd}\Gamma_T}} \exp\left(\frac{-k\lambda_{sd}x}{\Gamma_S}\right). \tag{12}$$

The CDF of $\Gamma_{S_k E}$ can be obtained from the definition of CDF similar to $\tilde{F}_{SD}$ as

$$F_{SE}(x) = 1 - \frac{\frac{\lambda_{te}\Gamma_S}{\lambda_{se}\Gamma_T}}{x + \frac{\lambda_{te}\Gamma_S}{\lambda_{se}\Gamma_T}} \exp\left(\frac{-\lambda_{se}x}{\Gamma_S}\right), \tag{13}$$

and the PDF of Γ_{SE} can be expressed after differentiating (13) as

$$f_{SE}(x) = \frac{\frac{\lambda_{te}}{\Gamma_T} \exp\left(\frac{-\lambda_{se}x}{\Gamma_S}\right)}{x + \frac{\lambda_{te}\Gamma_S}{\lambda_{se}\Gamma_T}} + \frac{\frac{\lambda_{te}\Gamma_S}{\lambda_{se}\Gamma_T} \exp\left(\frac{-\lambda_{se}x}{\Gamma_S}\right)}{\left(x + \frac{\lambda_{te}\Gamma_S}{\lambda_{se}\Gamma_T}\right)^2}. \tag{14}$$

3 Secrecy Outage Probability

In this section, we investigate the SOP of the secondary network where the eavesdropper's CSI is assumed unavailable in the proposed network. So, the transmitters encode and transfer the information with the certain target rate of ρ. We denoted the instantaneous secrecy capacity by C_S in bits/s/HZ, and the secrecy gain is guaranteed when C_S is greater than R_{th}. Otherwise, information-theoretic security is compromised [20]. Towards deriving those performances, the secrecy capacity is required to be defined first. The secrecy capacity can be expressed for as [21,22]

$$C_S = \left[\log_2(1+\Gamma_{SD}) - \log_2(1+\Gamma_E)\right]^+, \tag{15}$$

where $\log_2(1+\Gamma_{SD})$ is the instantaneous capacity at D, $\log_2(1+\Gamma_E)$ is the instantaneous capacity of the wiretap channel at E, $\Gamma_E = \Gamma_{SE}$ and $[x]^+ = \max(x, 0)$. The SOP is defined as the probability that the secrecy rate is lower than a certain threshold, R_{th}, can be expressed as

$$\begin{aligned}\mathcal{P}_{out}(R_{th}) &= Pr(C_S < R_{th}) \\ &= \mathbb{P}\left[\Gamma_{SD} < R_{th}(1+\Gamma_E) - 1\right] \\ &= \int_0^\infty F_{SD}(\rho(x+1)-1) f_{SE}(x) dx,\end{aligned} \tag{16}$$

where $\rho = 2^{R_{th}} - 1$, R_{th} is the target rate of the secondary network. Substituting (11) and (14) into (16), outage secrecy probability can be evaluated as

$$\mathcal{P}_{out}(R_{th}) = 1 - A \cdot I_1 - B \cdot I_2, \tag{17}$$

where I_1 and I_2 can be expressed respectively as

$$I_1 = \int_0^\infty \frac{1}{(x+a)(x+b)} \exp\left(-cx\right) dx, \tag{18}$$

$$I_2 = \int_0^\infty \frac{1}{(x+a)\left(x+b\right)^2} \exp\left(-cx\right) dx, \tag{19}$$

with $a = \frac{\lambda_{td}\Gamma_S + k\rho\lambda_{sd}\Gamma_T - k\lambda_{sd}\Gamma_T}{k\rho\lambda_{sd}\Gamma_T}$, $b = \frac{\lambda_{te}\Gamma_S}{\lambda_{se}\Gamma_T}$ and $c = \frac{k\rho\lambda_{sd}+\lambda_{se}}{\Gamma_S}$

$$A = \sum_{k=1}^{K} \binom{K}{k} \Lambda(-1)^{k+1} \frac{\lambda_{te}\lambda_{td}\Gamma_S}{k\rho\lambda_{sd}\Gamma_T^2} \exp\left(\frac{-k\lambda_{sd}\left(\rho-1\right)}{\Gamma_S}\right), \tag{20}$$

$$B = \sum_{k=1}^{K} \binom{K}{k} \Lambda(-1)^{k+1} \frac{\lambda_{te}\lambda_{td}\Gamma_S^2}{k\rho\lambda_{se}\lambda_{sd}\Gamma_T^2} \exp\left(\frac{-k\lambda_{sd}\left(\rho-1\right)}{\Gamma_S}\right). \tag{21}$$

We can utilize the partial fraction to transform multiplication into summation and solve (18) and (19) using

$$\frac{1}{(x+a)(x+b)} = -\frac{1}{(a-b)(x+a)} + \frac{1}{(a-b)(x+b)}, \tag{22}$$

$$\frac{1}{(x+a)(x+b)^2} = \frac{1}{(a-b)^2(x+a)} - \frac{1}{(a-b)^2(x+b)} + \frac{1}{(a-b)(x+b)^2}. \quad (23)$$

For the final solution, we have used the integral solution of the form [23], eq.(3.352.4) and [23], eq.(3.353.3) to get

$$I_1 = \frac{1}{a-b}\exp(ac)\,\mathrm{Ei}(-ac) - \frac{1}{a-b}\exp(bc)\,\mathrm{Ei}(-bc), \quad (24)$$

$$I_2 = -\frac{1}{(a-b)^2}\exp(ac)\,\mathrm{Ei}(-ac) + \frac{1}{(a-b)^2}\exp(bc)\,\mathrm{Ei}(-bc) + \frac{1}{a-b}\left(c\exp(bc)\,\mathrm{Ei}(-bc) + \frac{1}{b}\right). \quad (25)$$

4 Numerical Results and Discussions

In this section, Monte Carlo simulations are provide to validate the theoretical analyses. Without loss of generality, we assume all nodes are affected by the same noise power N_0, and the following parameters are set: $\beta = 0.5$ bits/s/Hz, $R_{th} = 0.5$ bits/s/Hz, $\lambda_{tr} = 3, \lambda_{td} = -6, \lambda_{sd} = 3, \lambda_{sr} = -3, \lambda_{te} = 6, \lambda_{se} = -3$ dB.

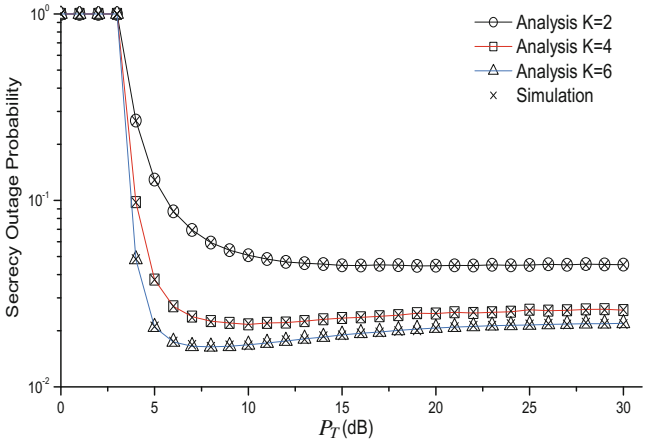

Fig. 2. SOP versus P_T(dB) for different numbers of secondary users.

Figure 2 shows the SOP versus P_T for different number of small-cell transmitters, K = 2, K = 4, and K = 6. The network parameters are set as $\Phi = 0.1$ and $\Lambda = 0.99$. It shows that the analysis match with simulation. It can be observed that the number of small-cell transmitters strongly affects the SOP. As the number of smell-cell transmitter increase, SOP improves. However, the increase of transmitter i.e. K = 2 to K = 4 has more improvement compared to

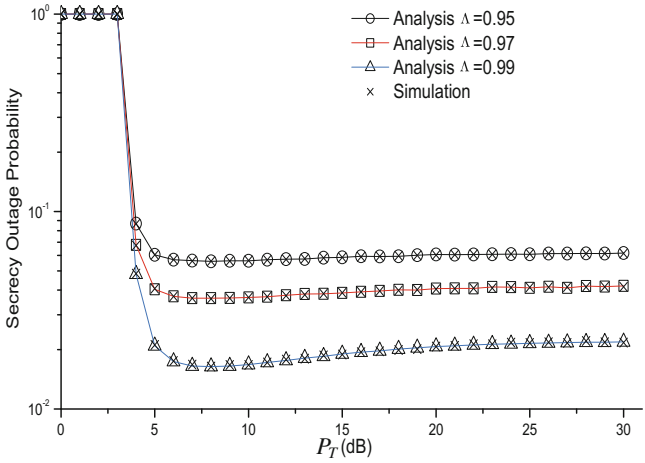

Fig. 3. SOP versus P_T(dB) for different values of Λ .

k = 4 to K = 6. As we increase P_T SOP decreases first and converges to its floor after certain values.

Figure 3 plots the SOP versus P_T for different value of backhaul reliability, $\Lambda = 0.95$, $\Lambda = 0.97$ and $\Lambda = 0.99$ with K = 6, $\Phi = 0.1$. We observed that the SOP reduces when the Λ increases. This is intuitive that as the reliability of the backhaul link improve of secrecy also improves.

In Fig. 4, the SOP is investigated versus P_T with three different value of primary QoS constraint, $\Phi = 0.01$, $\Phi = 0.05$ and $\Phi = 0.1$ with K = 6, $\Lambda = 0.99$. We observed that increasing Φ result in a reduction in the SOP. This is because

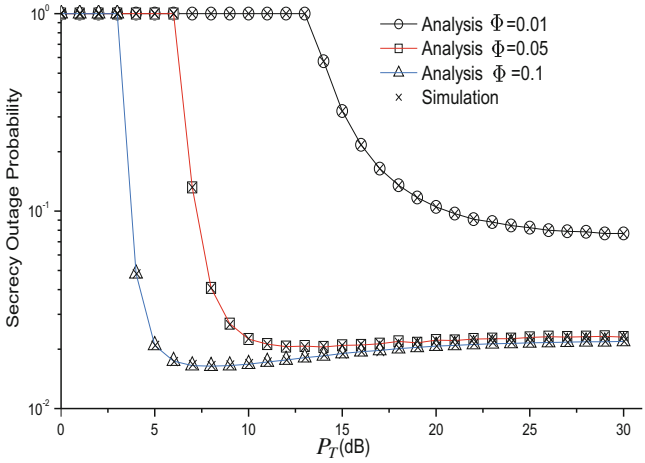

Fig. 4. SOP versus P_T(dB) for different values of Φ.

the secondary network are allowed to have higher transmit power by relaxing the QoS requirement of the primary network.

5 Conclusion

In this paper, we have taken into account the backhaul connection reliability of studying the SOP of underlay cognitive radio network. A proposed selection scheme enhance the system's secrecy performance. The small-cell transmitter power met the desired outage probability. The results have proved that increasing the primary transmitter's power and the number of small-cell transmitter enhance the system's secrecy performance. In addition, our results shows that the backhaul reliability and the desired outage probability of the primary network are important parameter relative to the scaling of the secrecy performance. Increasing backhaul reliability will result in base station having higher success rate to connect with small-cell transmitters, and relaxing the QoS requirement of the primary network will allow small-cell transmitter to have higher transmit power, which will improve over all secrecy of the system.

Acknowledgment. This work was supported in part by the Royal Society-SERB Newton International Fellowship under Grant NF151345.

References

1. Andrews, J.G., Buzzi, S., Choi, W., et al.: What will 5G be? IEEE Trans. Signal Process. **32**(6), 1065–1082 (2014)
2. Tipmongkolsilp, O., Zaghloul, S., Jukan, A.: The evolution of cellular backhaul technologies: current issues and future trends. IEEE Commun. Surv. Tutor. **13**(1), 97–113 (2011)
3. Ge, X.H., Cheng, H., Guizani, M., et al.: 5G wireless backhaul networks: challenges and research advances. IEEE Netw. **28**(6), 6–11 (2014)
4. Kim, K.J., Yeoh, P.L., Orlik, P.V., et al.: Secrecy performance of finite-sized cooperative single carrier systems with unreliable backhaul connections. IEEE Trans. Signal Process. **64**(17), 4403–4416 (2016)
5. Kolodzy, P.: Avoidance, interference: spectrum policy task force. Federal Communications Commission, Washington, DC, Report ET Docket, vol. 40, no. 4, pp. 147–158 (2002)
6. Mitola, J., Maguire, G.Q.: Cognitive radio: making software radios more personal. IEEE Pers. Commun. **6**(4), 13–18 (1999)
7. Zhang, J.H., Nguyen, N.P., Zhang, J.Q., et al.: Impact of primary networks on the performance of energy harvesting cognitive radio networks. IET Commun. **10**(18), 2559–2566 (2016)
8. Lee, S., Zhang, R.: Cognitive wireless powered network: spectrum sharing models and throughput maximization. IEEE Trans. Cogn. Commun. Netw. **1**(3), 335–346 (2015)
9. Nguyen, N.P., Duong, T.Q., Ngo, H.Q., et al.: Secure 5G wireless communications: a joint relay selection and wireless power transfer approach. IEEE Access **4**, 3349–3359 (2016)

10. Bao, V.N.Q., Duong, T.Q., Da Costa, D.B., et al.: Cognitive amplify-and-forward relaying with best relay selection in non-identical Rayleigh fading. IEEE Commun. Lett. **17**(3), 475–478 (2013)
11. Kundu, C., Ngatched, T.M.N., Dobre, O.A.: Relay selection to improve secrecy in cooperative threshold decode-and-forward relaying. In: Proceedings of IEEE GLOBECOM 2016, Washington, DC, USA, 4–8 (2016)
12. Zhang, J., Kundu, C., Nguyen, N.P., et al.: Cognitive wireless powered communication networks with secondary user selection and primary QoS constraint. IET Commun. **12**, 1873–1879 (2018)
13. Huang, Y.Z., Wang, J.L., Zhong, C.J., et al.: Secure transmission in cooperative relaying networks with multiple antennas. IEEE Trans. Wirel. Commun. **15**(10), 6843–6856 (2016)
14. Yin, C., Nguyen, H.T., Kundu, C., et al.: Secure energy harvesting relay networks with unreliable backhaul connections. IEEE Access **6**, 12074–12084 (2018)
15. Vu, T., Nguyen, M.N., Kundu, C., et al.: Secure cognitive radio networks with source selection and unreliable backhaul connections. IET Commun. **12**, 1771–1777 (2017)
16. Kundu, C., Jindal, A., Bose, R.: Secrecy outage of dual-hop amplify-and-forward relay system with diversity combining at the eavesdropper. Wireless Pers. Commun. **97**, 539–563 (2017)
17. Khan, T.A., Orlik, P., Kim, K.J., et al.: Performance analysis of cooperative wireless networks with unreliable backhaul links. IEEE Commun. Lett. **19**(8), 1386–1389 (2015)
18. Nguyen, H.T., Duong, T.Q., Hwang, W.J.: Multiuser relay networks over unreliable backhaul links under spectrum sharing environment. IEEE Commun. Lett. **21**(10), 2314–2317 (2017)
19. Nguyen, H.T., Zhang, J.Q., Yang, N., et al.: Secure cooperative single carrier systems under unreliable backhaul and dense networks impact. IEEE Access **5**, 18310–18324 (2017)
20. Wang, L.F., Elkashlan, M., Huang, J., et al.: Secure transmission with antenna selection in MIMO Nakagami-m fading channels. IEEE Trans. Wireless Commun. **13**(11), 6054–6067 (2014)
21. Wang, L.F., Kim, K.J., Duong, T.Q., et al.: Security enhancement of cooperative single carrier systems. IEEE Trans. Inf. Forensics Secur. **10**(1), 90–103 (2015)
22. Yang, N., Yeoh, P.L., Elkashlan, M., et al.: Transmit antenna selection for security enhancement in MIMO wiretap channels. IEEE Trans. Commun. **61**(1), 144–154 (2013)
23. Jeffrey, A., Zwillinger, D.: Table of Integrals, Series and Products, 7th edn. Academic Press, Cambridge (2007)