SCIENCE CHINA
Information Sciences

• LETTER •

February 2018, Vol. 61 029305:1–029305:3
doi: 10.1007/s11432-016-9201-7

Secure resource allocation for green and cognitive device-to-device communication

Chi XU[1,2,3], Peng ZENG[1,2], Wei LIANG[1,2] & Haibin YU[1,2*]

[1]*Key Laboratory of Networked Control Systems, Chinese Academy of Sciences, Shenyang* 110016*, China;*
[2]*State Key Laboratory of Robotics, Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang* 110016*, China;*
[3]*University of Chinese Academy of Sciences, Beijing* 100049*, China*

Received 23 December 2016/Revised 15 May 2017/Accepted 5 August 2017/Published online 20 November 2017

Citation Xu C, Zeng P, Liang W, et al. Secure resource allocation for green and cognitive device-to-device communication. Sci China Inf Sci, 2018, 61(2): 029305, doi: 10.1007/s11432-016-9201-7

Dear editor,

Spectrum efficiency, energy efficiency and communication security are the most significant concerns in the 5G era [1]. Cognitive radio which employs dynamic spectrum sharing, energy harvesting which scavenges energy from ambient sources, and physical layer security which exploits the time varying wireless channels are three promising techniques to enhance spectrum efficiency, energy efficiency and communication security [2, 3]. Although energy harvesting cognitive radio networks [4, 5] and physical layer security [6, 7] have been widely studied in recent years, very few existing work comprehensively address the above three concerns. Thus, cognitive, green and secure communication still remains an open research topic, which motivates this work.

In this letter, we study the cognitive, green and secure device to device (D2D) communication underlaying a small cell network. To be specific, a pair of cognitive devices without constant energy supplies first harvest energy from the RF signals of a small cell base station (SCBS), and then communicate with each other in the cellular channel currently with a cellular user (CU). Thus, the transmit powers of cognitive devices are subject to both the interference power constraint from CU and the energy causality constraint imposed by energy harvesting and processing cost. However, due to the openness of wireless communication, an active eavesdropper can overhear the confidential messages in the cellular channel. Thus, to guarantee the communication security, we study the secrecy rate maximization problem to realize optimal secure resource allocation.

System model. A pair of cognitive devices communicate with each other underlaying a small cell network, in which a SCBS consistently serves a CU in the cellular channel. The cognitive D2D transmitter (CDT) transmits confidential messages to the cognitive D2D receiver (CDR) in the same cellular channel which is also wiretapped by an active eavesdropper (EAV). The channel power gains from SCBS to CDT, CDR and EAV are denoted as $g_{\rm t}$, $g_{\rm r}$ and $g_{\rm e}$, respectively. Similarly, the channel power gains from CDT to CU, CDR and EAV are denoted as $h_{\rm c}$, $h_{\rm r}$ and $h_{\rm e}$, respectively.

Both CDT and CDR are battery-free devices, but can harvest green energy from the RF signals of SCBS. The cognitive devices with single-antenna work in the half-duplex mode and operate in the harvest-then-transmit fashion in each frame T. In the first phase with duration τT, both CDT and CDR harvest energy from SCBS, where $0 \leqslant \tau \leqslant 1$ is the harvesting ratio. The harvested energy of CDT is given by $\xi P_{\rm s} g_{\rm t} \tau T$, where $P_{\rm s}$ is

* Corresponding author (email: yhb@sia.cn)
The authors declare that they have no conflict of interest.

the transmit power of SCBS and $0 < \xi < 1$ is the energy harvesting efficiency. The noise energy is ignored since the noise power is too small to be harvested by the cognitive devices.

With the harvested energy, CDT transmits confidential messages to CDR in the second phase with duration $(1-\tau)T$. The transmit power of CDT $P_{\rm t}$ must satisfy $(P_{\rm t}+P_{\rm c})(1-\tau) \leqslant \xi P_{\rm s} g_{\rm t} \tau$, where $P_{\rm c}$ is the power for the non-negligible processing cost. Note that there is no initial energy in each frame as CDT and CDR are battery-free devices without energy storage and management. Moreover, CDT must strictly control its transmit power such that $P_{\rm t} h_{\rm c} \leqslant Q_{\rm c}$, where $Q_{\rm c}$ is the peak interference power that CU can tolerate.

With τ and $P_{\rm t}$, the secrecy rate [3] of the cognitive D2D communication is calculated as

$$R_{\rm s}(\tau, P_{\rm t}) = \left((1-\tau)\log_2\left(\frac{1+\gamma_{\rm r}P_{\rm t}}{1+\gamma_{\rm e}P_{\rm t}}\right)\right)^+, \quad (1)$$

where $\gamma_{\rm r} = \frac{h_{\rm r}}{P_{\rm s}g_{\rm r}+\sigma_{\rm r}^2}$ and $\gamma_{\rm e} = \frac{h_{\rm e}}{P_{\rm s}g_{\rm e}+\sigma_{\rm e}^2}$ with $\sigma_{\rm r}^2$ and $\sigma_{\rm e}^2$ denoting the noise powers at CDR and EAV, respectively. $(x)^+ \triangleq \max(x,0)$ is the ramp function.

As $P_{\rm s}$ and $Q_{\rm c}$ are prespecified by the small cell network, we optimize τ and $P_{\rm t}$ to maximize the secrecy rate. The secrecy rate maximization problem with respect to the harvesting time and the transmit power is formulated as

$$\begin{aligned} &\max_{\tau, P_{\rm t}} \; R_{\rm s}(\tau, P_{\rm t}), \\ &\;\text{s.t. } C1: (P_{\rm t}+P_{\rm c})(1-\tau) \leqslant \xi P_{\rm s} g_{\rm t} \tau, \\ &\quad\;\; C2: P_{\rm t} h_{\rm c} \leqslant Q_{\rm c}, \\ &\quad\;\; C3: 0 \leqslant \tau \leqslant 1, \end{aligned} \quad (2)$$

where $C1$ is the energy causality constraint imposed by energy harvesting and processing cost, $C2$ is the interference power constraint from CU, and $C3$ is the harvesting time constraint.

Secure resource allocation. Due to the non-convexity of the objective function and the products of optimization variables in $C1$, problem (2) is non-convex and cannot be solved by standard optimization method. To make this problem tractable, we first introduce two auxiliary variables $t = 1-\tau$ and $E = P_{\rm t} t$ which denote the communication ratio and the consumed energy, respectively. Then, without considering the ramp function $(x)^+$, we formulate the secrecy rate maximization problem with respect to the communication time and the consumed energy as follows:

$$\begin{aligned} &\max_{t, E} \; R_{\rm s}(t, E) = t\log_2\left(\frac{t+\gamma_{\rm r}E}{t+\gamma_{\rm e}E}\right), \\ &\;\text{s.t. } C1': E \leqslant \xi P_{\rm s} g_{\rm t}(1-t) - P_{\rm c} t, \\ &\quad\;\; C2': E \leqslant \frac{Q_{\rm c} t}{h_{\rm c}}, \\ &\quad\;\; C3': 0 \leqslant t \leqslant 1, \end{aligned} \quad (3)$$

where $C1'$, $C2'$, $C3'$ are equivalently transformed from $C1$, $C2$, $C3$, respectively.

Given $\gamma_{\rm r}$ and $\gamma_{\rm e}$, we can prove that problem (3) is a convex optimization problem, wherein the proof is omitted for brevity. In this way, the original non-convex problem is converted into a convex problem. Then, we employ the primary decomposition method [8] to decompose the problem into two levels of optimization problem. At the lower level, we solve the subproblem in terms of E for given t, while at the higher level, we solve the master problem in terms of t. Following this idea, we can solve problem (3) and obtain the optimal solution with respect to t and E. The detail solution process is not presented here due to the space limited. Note that the dropper of the ramp function can be fully compensated when solving problem (3). Based on the optimal solution for problem (3), we can calculate the optimal solution for problem (2). The optimal secure resource allocation is summarized as the following theorem.

Theorem 1. The optimal harvesting time τ^* and the optimal transmit power $P_{\rm t}^*$ are given by

Case 1. When $\gamma_{\rm r} \leqslant \gamma_{\rm e}$,

$$P_{\rm t}^* = 0, \quad \tau^* = 0; \quad (4)$$

Case 2. When $\gamma_{\rm r} > \gamma_{\rm e}$,

$$\begin{cases} P_{\rm t}^* = 0, \tau^* = 0, \text{ if } \rho \geqslant \alpha, & (5) \\ P_{\rm t}^* = \dfrac{\xi P_{\rm s} g_{\rm t}(1-\rho)}{\rho} - P_{\rm c}, \; \tau^* = 1-\rho, & \\ \qquad\qquad\qquad\qquad \text{if } \beta < \rho < \alpha, & (6) \\ P_{\rm t}^* = \dfrac{Q_{\rm c}}{h_{\rm c}}, \tau^* = 1-\beta, \text{ if } \rho \leqslant \beta, & (7) \end{cases}$$

where $\alpha = \frac{\xi P_{\rm s} g_{\rm t}}{\xi P_{\rm s} g_{\rm t} + P_{\rm c}}$, $\beta = \frac{\xi P_{\rm s} g_{\rm t} h_{\rm c}}{\xi P_{\rm s} g_{\rm t} h_{\rm c} + P_{\rm c} h_{\rm c} + Q_{\rm c}}$, and ρ is the root of the transcendental equation

$$\ln\left(\frac{\mu_{\rm r} t + \omega_{\rm r}}{\mu_{\rm e} t + \omega_{\rm e}}\right) - \left(\frac{\omega_{\rm r}}{\mu_{\rm r} t + \omega_{\rm r}} - \frac{\omega_{\rm e}}{\mu_{\rm e} t + \omega_{\rm e}}\right) = 0, \quad (8)$$

with $\mu_{\rm r} = 1 - \gamma_{\rm r}(\xi P_{\rm s} g_{\rm t} + P_{\rm c})$, $\mu_{\rm e} = 1 - \gamma_{\rm e}(\xi P_{\rm s} g_{\rm t} + P_{\rm c})$, $\omega_{\rm r} = \gamma_{\rm r} \xi P_{\rm s} g_{\rm t}$, and $\omega_{\rm e} = \gamma_{\rm e} \xi P_{\rm s} g_{\rm t}$.

Proof. For brevity, the proof is omitted here.

It is obvious that the optimal secure resource allocation is significantly dependent upon the instantaneous channel state and the setup of the small cell (i.e., $P_{\rm s}$ and $Q_{\rm c}$). Thus, with the given setup of the small cell, the cognitive devices can perform secure resource allocation by evaluating the channel state information. In this way, we realizes green, cognitive and secure D2D communication underlaying the small cell network.

Simulation results and discussion. The simulation parameters are set as follows: $T = 1$, $\xi = 0.8$, $\sigma_{\rm r}^2 = \sigma_{\rm e}^2 = 1$, and $P_{\rm c} = 0.5$ dB. As the secure resource allocation depends on the setup of the small cell, we depict Figure 1 to demonstrate the relationship between $R_{\rm s}^*$ and ($P_{\rm s}$, $Q_{\rm c}$). As shown, $R_{\rm s}^*$ first increases and then decreases with $P_{\rm s}$ increasing. When $P_{\rm s}$ is small, a large τ^* is allocated for energy harvesting to enhance the harvested energy. As the harvested energy is limited, $P_{\rm t}^*$ cannot be large, which results in a small $R_{\rm s}^*$. With $P_{\rm s}$ increasing, $R_{\rm s}^*$ increases accordingly since τ^* decreases and $P_{\rm t}^*$ increases under the constraint of $Q_{\rm c}$. For this case, the impact of $Q_{\rm c}$ on $R_{\rm s}^*$ is very limited as $P_{\rm t}^*$ by all the harvested energy still cannot achieve $Q_{\rm c}$. However, when $P_{\rm s}$ is very large, $R_{\rm s}^*$ decreases since $P_{\rm t}^*$ constrained by $Q_{\rm c}$ cannot be further enhanced while the interference from SCBS to CDR keeps on increasing. For this case, $R_{\rm s}^*$ increases with the increase of $Q_{\rm c}$ as more harvested energy can be utilized for communication. Obviously, the cognitive devices may not always benefit from the small cell. Thus, to gain the maximum secrecy rate, we should execute secure resource allocation according to the instantaneous channel state information and the setup of the small cell.

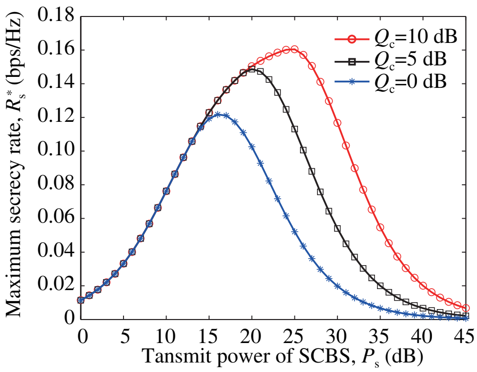

Figure 1 (Color online) Maximum secrecy rate versus the transmit power of SCBS under different interference power constraints.

Conclusion. In this letter, we investigated the green, cognitive and secure D2D communication underlaying a small cell, wherein cognitive devices capture both energy and spectrum of the small cell to enhance energy and spectrum efficiencies. To ensure the communication security, we studied the secrecy rate maximization problem subject to the interference power constraint and the energy causality constraint, and obtained the closed-form expressions for optimal secure resource allocation. Simulations results verified the validity of the green, cognitive and secure D2D communication.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61233007, 61533015, 71661147005).

References

1 Ma Z, Zhang Z Q, Ding Z G, et al. Key techniques for 5G wireless communications: network architecture, physical layer, and MAC layer perspectives. Sci China Inf Sci, 2015, 58: 041301
2 Huang X Q, Han T, Ansari N. On green-energy-powered cognitive radio networks. IEEE Commun Surv Tuts, 2015, 17: 827–842
3 Wang H-M, Xia X-G. Enhancing wireless secrecy via cooperation: signal design and optimization. IEEE Commun Mag, 2015, 53: 47–53
4 Xu C, Zheng M, Liang W, et al. End-to-end throughput maximization for underlay multi-hop cognitive radio networks with RF energy harvesting. IEEE Trans Wirel Commun, 2017, 16: 3561–3572
5 Sakr A H, Hossain E. Cognitive and energy harvesting-based D2D communication in cellular networks: stochastic geometry modeling and analysis. IEEE Trans Commun, 2015, 63: 1867–1880
6 Wang W, Teh K C, Li K H. Enhanced physical layer security in D2D spectrum sharing networks. IEEE Wirel Commun Lett, 2017, 6: 106–109
7 Liu Y, Wang L, Zaidi S A R, et al. Secure D2D communication in large-scale cognitive cellular networks: a wireless power transfer model. IEEE Trans Commun, 2016, 64: 329–342
8 Palomar D P, Chiang M. A tutorial on decomposition methods for network utility maximization. IEEE J Sel Areas Commun, 2006, 24: 1439–1451