Proceedings Paper:
Liu, Y, Wang, L, Zaidi, SAR et al. (2 more authors) (2015) Secure D2D Communication in Large-Scale Cognitive Cellular Networks with Wireless Power Transfer. In: ICC 2015 - 2015 IEEE International Conference on Communications. ICC 2015 - 2015 IEEE International Conference on Communications, 08-12 Jun 2015, ExCel London, UK. IEEE , pp. 4309-4314. ISBN 9781467364324

https://doi.org/10.1109/ICC.2015.7249000

Secure D2D Communication in Large-Scale Cognitive Cellular Networks with Wireless Power Transfer

Yuanwei Liu*, Lifeng Wang*, Syed Ali Raza Zaidi†, Maged Elkashlan*, and Trung Q. Duong‡
* Queen Mary University of London, London, UK
† University of Leeds, Leeds, UK
‡ Queen's University Belfast, Belfast, UK

***Abstract*—In this paper, we investigate secure device-to-device (D2D) communication in energy harvesting large-scale cognitive cellular networks. The energy constrained D2D transmitter harvests energy from multi-antenna equipped power beacons (PBs), and communicates with the corresponding receiver using the spectrum of the cellular base stations (BSs). We introduce a power transfer model and an information signal model to enable wireless energy harvesting and secure information transmission. In the power transfer model, we propose a new power transfer policy, namely, best power beacon (BPB) power transfer. To characterize the power transfer reliability of the proposed policy, we derive new closed-form expressions for the exact power outage probability and the asymptotic power outage probability with large antenna arrays at PBs. In the information signal model, we present a new comparative framework with two receiver selection schemes: 1) best receiver selection (BRS), and 2) nearest receiver selection (NRS). To assess the secrecy performance, we derive new expressions for the secrecy throughput considering the two receiver selection schemes using the BPB power transfer policies. We show that secrecy performance improves with increasing densities of PBs and D2D receivers because of a larger multiuser diversity gain. A pivotal conclusion is reached that BRS achieves better secrecy performance than NRS but demands more instantaneous feedback and overhead.**

I. INTRODUCTION

Wireless power transfer (WPT) has recently received significant attention for its attractive energy harvesting capabilities and prolonging the life-time of the wireless network [1]. The motivation behind it is the most devices surrounded by the ambient radio-frequency (RF) signals which can carry energy and information together during transmission. Two practical receiver designs namely time switching (TS) receiver and power splitting (PS) receiver were proposed in a multiple-input multiple-output (MIMO) system in [2], which laid a solid foundation on the research of WPT. In [3], a new concept based on power beacons (PBs) that deploy dedicated power stations to charge the nearby mobile devices with WPT was proposed. In [3], based on stochastic geometry, the uplink performance in cellular networks was investigated under an outage constraint.

Along with improving the energy efficiency through energy harvesting [4], another key design objective is to maximize the spectral efficiency. Cognitive radio (CR) [5] and device-to-device (D2D) technology [6], have rekindled the interest of researchers to achieve a more spectrally efficient cellular networks. In [7], a wireless power transfer protocol for a two-hop decode-and-forward relay system is proposed in a cognitive radio network. In [8], D2D communication in energy harvesting CR networks was proposed using stochastic geometry.

Furthermore, it is currently noted that CR networks are also confronted with security issues since the broadcast nature of the wireless medium is susceptible to potential security threats such as eavesdropping and impersonation. Physical (PHY) layer security, which is initialed by Wyner [9] and recently aroused wide-spread interest, has been considered in CR networks [10]. In [11], the authors revealed the impact of the primary network on the secondary network in the presence of a multi-antenna wiretap channel and presented closed-form expressions for the exact and the asymptotic secrecy outage probability in cognitive secure communications.

In this paper, we consider secure communication underlay cognitive cellular networks with an energy constrained D2D transmitter. A statistical model based on stochastic geometry is used to describe and evaluate the proposed D2D communication in energy harvesting large-scale cognitive cellular networks. Differing from [3] which neglects the small-scale fading and requires energy storage units at the mobile terminals, we deploy a battery-free design [12, 13] for the energy constrained D2D transmitter. Considering the impact of small-scale fading, we propose a new WPT policy, namely, best power beacon (BPB) power transfer, where the transmitter selects the PB with the strongest channel to harvest the energy. We also present a new comparative framework with the best receiver selection (BRS) and the nearest receiver selection (NRS) schemes. For the proposed BPB, we derive a new closed-form expression for the power outage probability. We also derive new analytical expressions for the secrecy throughput with BRS and NRS. Our analytical and numerical results show that BRS achieves higher secrecy throughput than NRS at the cost of more instantaneous feedback and overhead.

II. NETWORK MODEL

A. Network Description

We consider secure cognitive D2D communication in cellular networks, where the energy constrained D2D transmitter (Alice) communicates with D2D receivers (Bobs) under

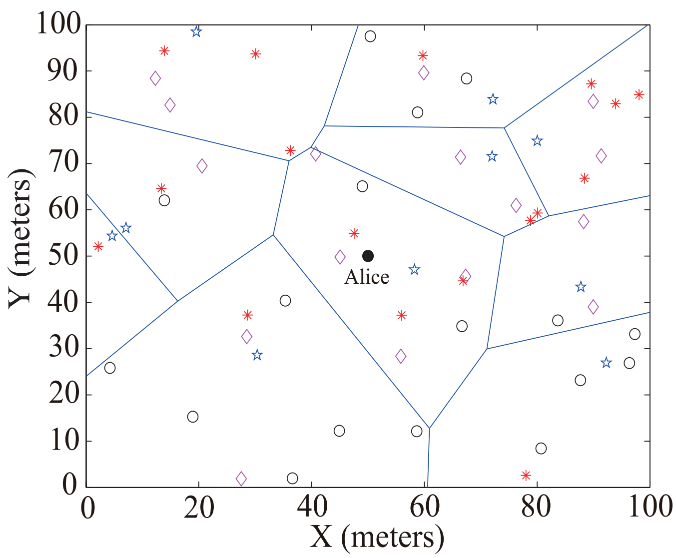


Fig. 1. An example of a part of a network snapshot considering that the spatial distributions of PBs (pink diamonds), Bobs (empty circles), BSs (blue five-pointed stars), and Eves (red stars) follow homogeneous poisson point processes (PPP).

malicious attempt of D2D eavesdroppers (Eves). The eavesdroppers are passive and interpret the signal without trying to modify it. It is assumed that Alice is energy constrained, i.e., the transmission can only be scheduled by utilizing power harvested from PBs. The spatial topology of all PBs, cellular base stations (BSs), Bobs, and Eves, are modeled using homogeneous poisson point process (PPP) Φ_p, Φ_ℓ, Φ_b, and Φ_e with density λ_p, λ_ℓ, λ_b, and λ_e, respectively. As shown in Fig. 1, we consider that Alice is located at the origin in a two-dimensional plane. For Alice, Bob, and Eve, each node is equipped with a single antenna. Each PB is furnished with M antennas and maximal ratio transmission (MRT) is employed at PBs to perform WPT to the energy constrained Alice. All channels are assumed to be quasi-static fading channels where the channel coefficients are constant for each transmission block but vary independently between different blocks. In this network, we assume that the time of each frame is T, which includes two time slots: 1) power transfer time slot, in which Alice harvests the power from PBs during the $(1-\beta)T$ time, with β being the fraction of the information processing time; and 2) information processing time slot, in which Alice transmits the information signal to the corresponding Bob using the harvested energy during the βT time.

B. Power Transfer Model

We consider a simple yet efficient power transfer model. It is assumed that PBs operate on a frequency band which is isolated from the communication band where BSs and D2D transceivers schedule their transmission. Specifically, the power transmitted by PBs does not interfere with the cellular and D2D communication. We also consider that Alice is a battery-free user, which means that there is no battery storage energy for future use and all the harvested energy during the power transfer time slot is used to transmit the information signal [12, 13].

We propose a new best power beacon (BPB) power transfer policy in the power transfer model, where Alice selects the strongest PB to harvest energy. The harvested energy of Alice from the PB can be obtained as follows

$$E_H = \eta P_S \max_{p\in\Phi_p} \{\|\mathbf{h}_p\|^2 L(r_p)\}(1-\beta)T, \tag{1}$$

where η is the power conversion efficiency of the receiver, P_S is the transmit power of PBs. Here, $\mathbf{h}_p$ is $\mathcal{C}^{M\times 1}$ vector, whose entries are independent complex Gaussian distributed with zero mean and unit variance employed to capture the effect of small-scale fading between PBs and Alice. $L(r_p) = K r_p^{-\alpha}$ is the power-law path-loss exponent. The path-loss function depends on the distance r_p, a frequency dependent constant K, and an environment/terrain dependent path-loss exponent $\alpha \geq 2$. All the channel gains are assumed to be independent and identically distributed (i.i.d.). Based on (1), the maximum transmit power at Alice is given by

$$P_H = \max_{p\in\Phi_p} \left\{\|\mathbf{h}_p\|^2 L(r_p)\right\} \frac{\eta P_S (1-\beta)}{\beta}. \tag{2}$$

C. Information Signal Model

We consider the cognitive underlay scheme [14], and assume that the instantaneous CSI of the links between Alice and cellular BSs are available at Alice. Consequently, the transmit power P_A at Alice is strictly constrained by the maximum transmit power P_{t} at Alice and the peak interference power I_p at cellular BSs according to

$$P_A = \min\left\{\frac{I_p}{\max\limits_{\ell\in\Phi_\ell}\left\{|h_\ell|^2 L(r_\ell)\right\}}, P_{\mathrm{t}}\right\}, \tag{3}$$

where $|h_\ell|^2 L(r_\ell)$ is the overall channel gain from Alice to the BS ℓ. Here, h_ℓ is the small-scale fading coefficient with $h_\ell \sim \mathcal{CN}(0,1)$ and $L(r_\ell) = K r_\ell^{-\alpha}$ is the power-law path-loss exponent. The path-loss function depends on the distance r_ℓ. All the channel gains are assumed to be i.i.d.. For D2D communication, we consider two receiver selection schemes.

1) Best Receiver Selection (BRS) scheme: Under BRS, Alice selects one Bob with the strongest channel as the desired receiver. The instantaneous signal-to-noise ratio (SNR) at the selected Bob is expressed as

$$\begin{aligned}\gamma_{\mathrm{B}} &= \frac{P_A}{N_0}\max_{b\in\Phi_b}\left\{|h_b|^2 L(r_b)\right\}\\ &= \zeta \max_{b\in\Phi_b}\left\{|h_b|^2 L(r_b)\right\},\end{aligned} \tag{4}$$

where $\zeta = \min\left\{\frac{\bar{\gamma}_p}{\max\limits_{\ell\in\Phi_\ell}\{|h_\ell|^2 L(r_\ell)\}}, \bar{\gamma}_0\right\}$, N_0 is the noise power, $\bar{\gamma}_p = I_p/N_0$, $\bar{\gamma}_0 = P_{\mathrm{t}}/N_0$, $|h_b|^2 L(r_b)$ is the channel power gain between Alice and Bobs, h_b is the small-scale fading coefficient with $h_b \sim \mathcal{CN}(0,1)$, r_b is the distance between Alice and Bobs.

2) Nearest Receiver Selection (NRS) scheme: Under NRS, Alice selects the nearest Bob as the desired receiver. The advantage of this scheme is that it reduces the system complexity since no instantaneous CSI and feedback from Bobs are required. Then the instantaneous SNR at the selected Bob can be expressed as

$$\begin{aligned}\gamma_{\mathrm{B}^*} &= \frac{P_A}{N_0}|h_{b^*}|^2 \max_{b\in\Phi_b} L\left(r_b\right)\\ &= \zeta|h_{b^*}|^2 \max_{b\in\Phi_b} L\left(r_b\right),\end{aligned}\tag{5}$$

where h_{b^*} is the small-scale fading coefficient of Alice to the nearest Bob with $h_{b^*}\sim\mathcal{CN}(0,1)$.

For the eavesdroppers, the instantaneous SNR at the most detrimental eavesdropper that has the strongest SNR between itself and Alice is expressed as

$$\begin{aligned}\gamma_{\mathrm{E}} &= \frac{P_A}{N_0}\max_{e\in\Phi_e}\left\{|h_e|^2 L\left(r_e\right)\right\}\\ &= \zeta\max_{e\in\Phi_e}\left\{|h_e|^2 L\left(r_e\right)\right\},\end{aligned}\tag{6}$$

where $h_e\sim\mathcal{CN}(0,1)$, r_e is the distance between Alice and Eves.

III. Power Outage Probability

We assume there exists a threshold transmit power P_{t}, below which the transmission cannot be scheduled, the transmission cannot be scheduled and Alice is considered to be in a power limited regime. In order to characterize the power limited regime of Alice, we introduce power outage probability, i.e., probability that the harvested power is not sufficient to carry out the transmission at a certain desired quality-of-service (QoS) level. The objective of this section is to quantify the power outage probability using BPB policy. In practical scenario, we expect a constant power for the information transmission. Therefore, we also denote the power threshold P_{t} as the transmit power of Alice when performing information transmission to Bobs.

A. Exact Analysis for Power Transfer

In this subsection, we provide exact analysis for the proposed BPB power transfer policy. In this policy, only the PB with the strongest channel transfers power to Alice.

Theorem 1: The power outage probability of BPB policy can be expressed in closed-form as

$$H_{out} = e^{\frac{-\lambda_p\pi\delta}{\mu^{\delta}}\sum\limits_{m=0}^{M-1}\left(\frac{\Gamma(m+\delta)}{m!}\right)},\tag{7}$$

where $\mu=\frac{\beta P_{\mathrm{t}}}{\eta P_S K(1-\beta)}$, $\delta=2/\alpha$, and $\Gamma(.)$ is Gamma function.

Proof: Based on (2), the power outage probability of BPB policy can be expressed as

$$\begin{aligned}\Pr\left\{P_H\le P_{\mathrm{t}}\right\} &= \Pr\left\{\max_{p\in\Phi_p}\left\{\|\mathbf{h}_p\|^2 {r_p}^{-\alpha}\right\}\le\mu\right\}\\ &= E_{\Phi_p}\left\{\prod_{p\in\Phi_p}\Pr\left\{\|\mathbf{h}_p\|^2\le {r_p}^{\alpha}\mu\right\}\right\}\\ &= E_{\Phi_p}\left\{\prod_{p\in\Phi_p}F_{\|\mathbf{h}_p\|^2}\left({r_p}^{\alpha}\mu\right)\right\},\end{aligned}\tag{8}$$

where $F_{\|\mathbf{h}_p\|^2}$ is the CDF of $\|\mathbf{h}_p\|^2$ and is expressed as

$$F_{\|\mathbf{h}_p\|^2}\left(x\right) = 1-e^{-x}\left(\sum_{m=0}^{M-1}\frac{x^m}{m!}\right).\tag{9}$$

Applying the generating functional given by [15], we rewrite (8) as

$$H_{out} = \exp\left[-\lambda_p\int_{R^2}\left(1-F_{\|\mathbf{h}_p\|^2}\left({r_p}^{\alpha}\mu\right)\right)dr_p\right].\tag{10}$$

Then changing to polar coordinates and substituting (9) into (10), the power outage probability of BPB is given by

$$H_{out} = \exp\left[-2\pi\lambda_p\sum_{m=0}^{M-1}\frac{\mu^m\int_0^\infty {r_p}^{m\alpha+1}e^{-{r_p}^{\alpha}\mu}dr_p}{m!}\right].\tag{11}$$

Then applying [16, Eq. (3.326.2)] and calculating the integral in (11), we obtain the closed form expression in (7). ■

B. large antenna array analysis for Power Transfer

In this subsection, we present large antenna array analysis for power transfer. We first examine the distribution of $\|\mathbf{h}_p\|^2$ when $M\to\infty$. Since $\|\mathbf{h}_p\|^2$ is i.i.d. exponential random variables (RVs), using law of large numbers, we have

$$\|\mathbf{h}_p\|^2 \overset{a.s.}{\to} M,\tag{12}$$

where $\overset{a.s.}{\to}$ denotes the almost sure convergence.

Theorem 2: The power outage probability of large antenna array analysis for the BPB power transfer policy is given by

$$H_{out}^{large} = e^{-\frac{\lambda_p\pi}{\theta^{\delta}}},\tag{13}$$

where $\theta=\frac{\beta P_{\mathrm{t}}}{M\eta P_S K(1-\beta)}$.

Proof: The power outage probability of BPB for large antenna arrays analysis can be expressed as

$$H_{out}^{large} = \Pr\left\{P_H\le P_{\mathrm{t}}\right\} = 1-F_{r_{p^*}}\left(\frac{1}{\sqrt[\alpha]{\theta}}\right),\tag{14}$$

where $F_{r_{p^*}}$ is the cumulative distribution function (CDF) of r_{p^*} and can be expressed as

$$F_{r_{p^*}}\left(x\right) = \int_0^x f\left(r_{p^*}\right)dr_{p^*} = 1-e^{-\lambda_p\pi x^2},\tag{15}$$

where r_{p^*} representing the distance from the nearest PB to Alice and its probability density function (PDF) is given by $f\left(r_{p^*}\right)=2\lambda_p\pi r_{p^*}e^{-\lambda_p\pi r_{p^*}^2}$.

Substituting (15) into (14), we obtain (13). ■

IV. Secrecy Throughput

In this section, a comparative framework is presented with two receiver selection schemes, namely, best receiver selection scheme and nearest receiver selection scheme. We use secrecy throughput as a metric to characterize the secrecy performance.

A. New Statistics

Theorem 3: The PDF of $\zeta = \frac{P_A}{N_0}$ is given by

$$f_\zeta(x) = \begin{cases} \left(\frac{\omega_\ell \delta x^{(\delta-1)}}{\bar{\gamma}_p^\delta}\right) e^{-\frac{\omega_\ell x^\delta}{\bar{\gamma}_p^\delta}}, & 0 < x < \bar{\gamma}_0 \\ e^{-\frac{\omega_\ell \bar{\gamma}_0^\delta}{\bar{\gamma}_p^\delta}} Dirac(x - \bar{\gamma}_0), x \geq \bar{\gamma}_0 \end{cases}, \quad (16)$$

where $\omega_\ell = K^\delta \delta \pi \lambda_\ell \Gamma(\delta)$, $Dirac(\cdot)$ is the Dirac delta function.

Proof: See Appendix A . ■

Theorem 4: For BRS scheme, the CDF of γ_B conditioned on ζ is given by

$$F_{\gamma_B|\zeta}(z) = e^{-\frac{\omega_B \zeta^\delta}{z^\delta}}, \quad (17)$$

where $\omega_B = K^\delta \delta \pi \lambda_b \Gamma(\delta)$.

For NRS scheme, the CDF of γ_{B^*} conditioned on ζ is given by

$$F_{\gamma_{B^*}|\zeta}(z) = 1 - 2\lambda_b \pi \int_0^\infty r_{b^*} e^{-\lambda_b \pi r_{b^*}^2 - \frac{z}{K\zeta} r_{b^*}^\alpha} dr_{b^*}. \quad (18)$$

Proof: See Appendix B . ■

Similar to (17), we can obtain the CDF of γ_E conditioned on ζ as

$$F_{\gamma_E|\zeta}(z) = e^{-\frac{\omega_E \zeta^\delta}{z^\delta}}, \quad (19)$$

where $\omega_E = K^\delta \delta^2 \pi \lambda_e \Gamma(\delta)$.

B. Best Receiver Selection (BRS) scheme

In this scheme, the instantaneous secrecy rate is defined as

$$C_s^{\mathrm{BRS}} = [\log_2(1+\gamma_B) - \log_2(1+\gamma_E)]^+, \quad (20)$$

where $[x]^+ = \max\{x, 0\}$.

The secrecy throughput is the average of the instantaneous secrecy rate C_s^{BRS} over γ_B and γ_E. As such, the secrecy throughput using BPB power transfer policy is given by

$$\bar{C}_s^{\mathrm{BRS}} = (1 - H_{out}) \frac{\beta}{\ln 2} \int_0^\infty \int_0^\infty \frac{F_{\gamma_E|\zeta}(x_2)}{1+x_2} \times \left(1 - F_{\gamma_B|\zeta}(x_2)\right) f_\zeta(x_1) \, dx_2 dx_1. \quad (21)$$

where F_{γ_B} and F_{γ_E} can be obtained in (17) and (19), separately, H_{out} is the power outage probability in the power transfer model.

Substituting (16), (17), and (19) into (21), after some manipulation, the secrecy throughput is derived as (22) on the top of next page, where $Q_2 = \frac{\omega_E}{x_2^\delta} + \frac{\omega_\ell}{\bar{\gamma}_p^\delta}$ and $Q_3 = \left(\frac{\omega_B}{x_2^\delta} + \frac{\omega_E}{x_2^\delta} + \frac{\omega_\ell}{\bar{\gamma}_p^\delta}\right)$.

C. Nearest Receiver Selection (NRS) Scheme

In this scheme, the instantaneous secrecy rate is defined as

$$C_s^{\mathrm{NRS}} = [\log_2(1+\gamma_{B^*}) - \log_2(1+\gamma_E)]^+. \quad (23)$$

As such, the secrecy throughput is given by

$$\bar{C}_s^{\mathrm{NRS}} = (1 - H_{out}) \frac{\beta}{\ln 2} \int_0^\infty \int_0^\infty \frac{F_{\gamma_E|\zeta}(x_2)}{1+x_2} \times \left(1 - F_{\gamma_{B^*}|\zeta}(x_2)\right) f_\zeta(x_1) \, dx_2 dx_1. \quad (24)$$

Substituting (16), (18), and (19) into (24), we can obtain the secrecy throughput of NRS scheme.

V. Numerical Results

In this section, representative numerical results are presented to illustrate performance evaluations including power outage probability secrecy throughput for BPB power transfer policy in the power transfer model and two receiver selection schemes in the information signal model. In the considered network, we set the transmit power of PBs as $P_S = 43$ dBm. The carrier frequency for power transfer and information transmission is set as 800 MHz and 900 MHz respectively. Furthermore, the bandwidth of the information transmission signal is assumed to be 10 MHz and the information receiver noise is assumed to be white Gaussian noise with average power -55dBm. In addition, we assume that the energy conversion efficiency of WPT is $\eta = 0.8$. In each figure, we see precise agreement between the Monte Carlo simulation points marked as "•" and the analytical curves, which validates our derivation.

Fig. 2 plots the power outage probability versus density of PBs with different power threshold P_{t}. The black solid curve, representing the BPB policy, is obtained from (7). We observe that as density of PBs increases, the power outage probability dramatically decreases. This is because the multiuser diversity gain is improved with increasing number of PBs when charging with WPT. We also see that as the power threshold increases, the outage occurs more frequently.

Fig. 3 plots the power outage probability versus M of PBs using the exact analysis and the large antenna array analysis. The dashed curve, representing the large antenna array analysis of BPB is obtained from (13). We see that the power outage probability decreases with increasing M. This is because larger antenna array gain is achieved with increasing M. As M increases, the large antenna array analysis and the exact analysis have precise agreement. This is due to the fact that when M grows large, the effect of small-scale fading is averaged out.

Fig. 4 plots the secrecy throughput versus density of the receivers. The solid and dashed curves, representing the BRS and NRS schemes, are obtained from (22) and (24), separately. Several observations are drawn as follows: 1) the secrecy throughput increases with increasing density of Bobs, this is because multiuser diversity gain is improved with increasing number of Bobs; 2) the secrecy throughput also increases with number of antennas at PBs M since lower power outage

$$\bar{C}_s^{\mathrm{BRS}} = (1-H_{out})\frac{\beta}{\ln 2}\left(\int_0^\infty \frac{\omega_\ell}{\bar{\gamma}_p^\delta(1+x_2)}\left(\frac{1}{Q_2}-\frac{1}{Q_3}+\frac{e^{-\bar{\gamma}_0^\delta Q_3}}{Q_3}-\frac{e^{-\bar{\gamma}_0^\delta Q_2}}{Q_2}\right)+\frac{e^{-\frac{\omega_\ell\bar{\gamma}_0^\delta}{\bar{\gamma}_p^\delta}-\frac{\omega_E\bar{\gamma}_0^\delta}{x_2^\delta}}}{1+x_2}\left(1-e^{-\frac{\omega_B\bar{\gamma}_0^\delta}{x_2^\delta}}\right)dx_2\right). \tag{22}$$

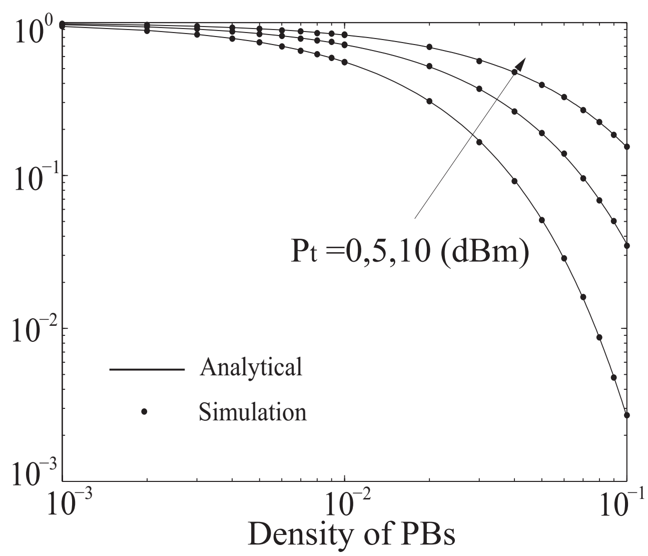


Fig. 2. Power outage probability versus density of PBs with $M = 32$, $P_S = 43$ dBm, $P_{\mathrm{t}} = 10$ dBm, and $\beta = 0.5$.

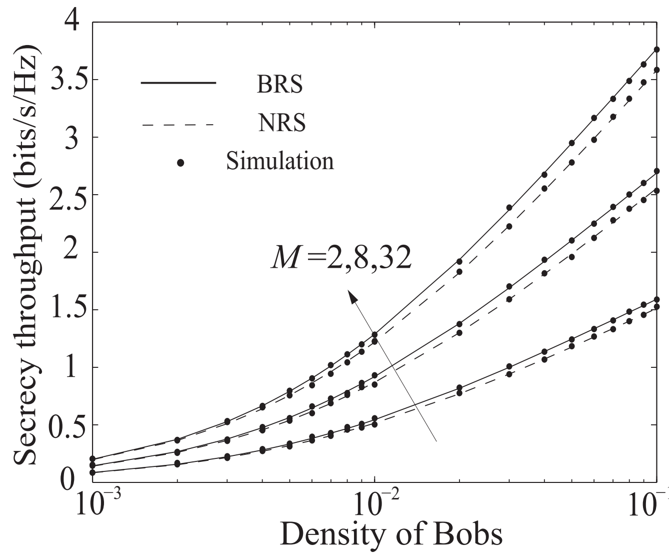


Fig. 4. Secrecy throughput versus density of Bobs λ_b with different M, where $P_S = 43$ dBm, $P_{\mathrm{t}} = 10$ dBm, $\beta = 0.5$, $\lambda_p = 10^{-1}, \lambda_e = 10^{-3}$, and $\lambda_l = 10^{-3}$.

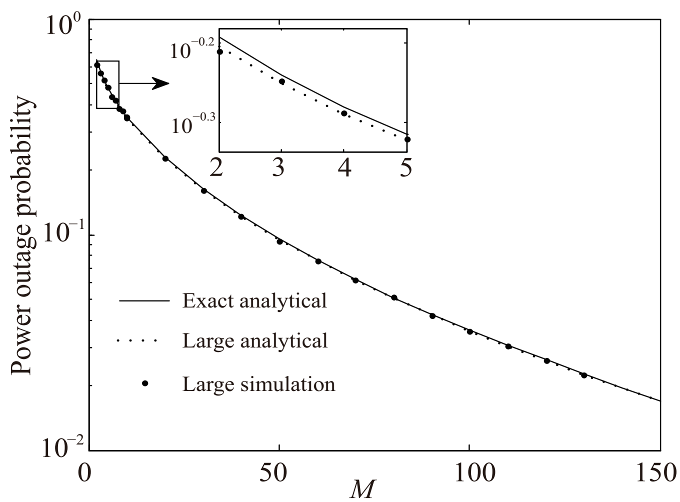


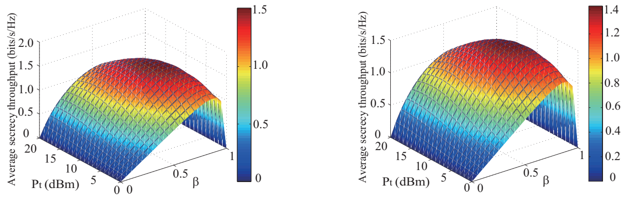
Fig. 3. Power outage probability versus M for large antenna array analysis with $P_S = 43$ dBm, $P_{\mathrm{t}} = 10$ dBm, and $\beta = 0.5$.

probability is achieved with larger antenna array gain, which results in improving secrecy throughput; and 3) BRS achieves better secrecy performance than NRS but demands more instantaneous feedbacks and overheads.

Fig. 5 shows the secrecy throughput versus P_{t} and β for BRS and NRS schemes using BPB power transfer policy. We see that β and P_{t} have joint effects on the secrecy throughput. By jointly considering β and P_{t}, we observe that there exits an optimal value for each of these two receiver selection schemes. This behavior is explained as follows: 1) as β increases, the time for power transfer decreases and the transmitter receives less power, but the time for information transmission increases; and 2) on the one hand, the power outage probability increases with increasing power threshold. On the other hand, the transmit power of Alice also increases since the power threshold is the transmit power of Alice, which results in a lower power outage probability. As such, there exits a tradeoff between the power outage probability and the transmit power. In this case, it is of significance to select a suitable P_{t} and β to transmit information to maximize the secrecy throughput. These results provide us guidelines when proceeding the system parameters in the networks.

VI. Conclusions

In this paper, secure transmission in large-scale cognitive cellular networks with an energy constrained device-to-device transmitter was considered. We proposed a novel wireless power transfer policy in the power transfer model, namely, best power beacon power transfer. We also considered best receiver selection and nearest receiver selection schemes in the information signal model. We used stochastic geometry



(a) BRS scheme (b) NRS scheme

Fig. 5. Secrecy throughput of BRS and NRS versus β and power threshold P_t, with $M = 32$, $P_S = 43$ dBm, $\lambda_p = 10^{-1}$, $\lambda_b = 10^{-2}$, $\lambda_e = 10^{-3}$, and $\lambda_l = 10^{-3}$.

approach to provide a complete framework to model, analyze, and evaluate the performance of the proposed network. New analytical expressions in terms of power outage probability and secrecy throughput are derived to determine the system security performance. Numerical results were presented to verify our analysis and provide useful insights into practical design. We concluded that by carefully setting the network design parameters, along with wireless power transfer, an acceptable secure transmission can be achieved in device-to-device networks without affecting the base stations.

Appendix A: Proof of Theorem 3

We compute the CDF of ζ as follows:

$$\begin{aligned}
&F_\zeta(x) = \Pr\{\zeta \le x\} \\
&= \Pr\left\{\min\left\{\frac{\bar{\gamma}_p}{\max\limits_{\ell\in\Phi_\ell}\left\{|h_\ell|^2 L(r_\ell)\right\}}, \bar{\gamma}_0\right\} \le x\right\} \\
&= \Pr\left\{\max_{\ell\in\Phi_\ell}\left\{|h_\ell|^2 L(r_\ell)\right\} \ge \max\left\{\frac{\bar{\gamma}_p}{x}, \frac{\bar{\gamma}_p}{\bar{\gamma}_0}\right\}\right\} \\
&+ \Pr\left\{\max_{\ell\in\Phi_\ell}\left\{|h_\ell|^2 L(r_\ell)\right\} \le \frac{\bar{\gamma}_p}{\bar{\gamma}_0}, \bar{\gamma}_0 \le x\right\} \\
&= \begin{cases} 1, \bar{\gamma}_0 \le x \\ \underbrace{\Pr\left\{\max\limits_{\ell\in\Phi_\ell}\left\{|h_\ell|^2 L(r_\ell)\right\} \ge \frac{\bar{\gamma}_p}{x}\right\}}_{G_\ell}, \bar{\gamma}_0 > x \end{cases}. \qquad \text{(A.1)}
\end{aligned}$$

Following the similar procedure getting (7), we obtain G_ℓ as

$$G_\ell = 1 - e^{-\frac{K^\delta \delta\pi\lambda_\ell\Gamma(\delta)x^\delta}{\bar{\gamma}_p^\delta}}. \qquad \text{(A.2)}$$

Substituting (A.2) into (A.1), we obtain

$$\begin{aligned}
F_\zeta(x) &= \begin{cases} 1, \bar{\gamma}_0 \le x \\ 1 - e^{-\frac{K^\delta \delta\pi\lambda_\ell\Gamma(\delta)x^\delta}{\bar{\gamma}_p^\delta}}, \bar{\gamma}_0 > x \end{cases} \\
&= 1 - \mathrm{U}(\bar{\gamma}_0 - x)\, e^{-\frac{K^\delta \delta\pi\lambda_\ell\Gamma(\delta)x^\delta}{\bar{\gamma}_p^\delta}}, \qquad \text{(A.3)}
\end{aligned}$$

where $\mathrm{U}(x)$ is the unit step function as $\mathrm{U}(x) = \begin{cases} 1, x > 0 \\ 0, x \le 0 \end{cases}$. By taking the derivative of $F_\zeta(x)$ in (A.3), we obtain the PDF of ζ in (16).

Appendix B: Proof of Theorem 4

The CDF of γ_B conditioned on ζ is given by

$$F_{\gamma_B|\zeta}(z) = \Pr\{\gamma_B \le z\} = \Pr\left\{\max_{b\in\Phi_b}\left\{|h_b|^2 L(r_b)\right\}\zeta \le z\right\}. \qquad \text{(B.1)}$$

Following the similar procedure getting (A.2), we obtain (17).

The CDF of γ_{B^*} conditioned on ζ is given by

$$\begin{aligned}
&F_{\gamma_{B^*}|\zeta}(z) = \Pr\{\gamma_{B^*} \le z\} = \Pr\left\{|h_b|^2 \le \frac{r_{b^*}^\alpha z}{K\zeta}\right\} \\
&= \int_0^\infty \left(1 - e^{-\frac{r_{b^*}^\alpha z}{K\zeta}}\right) f(r_{b^*}) dr_{b^*} \\
&= 1 - 2\lambda_b\pi \int_0^\infty r_{b^*} e^{-\lambda_b\pi r_{b^*}^2 - \frac{z}{K\zeta} r_{b^*}^\alpha} dr_{b^*}, \qquad \text{(B.2)}
\end{aligned}$$

where r_{b^*} represents the distance form the nearest Bob to Alice with the PDF given by $f(r_{b^*}) = 2\lambda_b\pi r_{b^*} e^{-\lambda_b\pi r_{b^*}^2}$. Thus, we can obtain (18).

References

[1] T. Le, K. Mayaram, and T. Fiez, "Efficient far-field radio frequency energy harvesting for passively powered sensor networks," *IEEE J. Solid-State Circuits*, vol. 43, no. 5, pp. 1287–1302, 2008.

[2] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Commun.*, vol. 12, no. 5, pp. 1989–2001, 2013.

[3] K. Huang and V. Lau, "Enabling wireless power transfer in cellular networks: architecture, modeling and deployment," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 902–912, 2014.

[4] D. Liu, Y. Chen, K. K. Chai, and T. Zhang, "Optimal user association for delay-power tradeoffs in hetnets with hybrid energy sources," *In Proc. IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Washington, DC, USA 2014.

[5] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, 2009.

[6] K. Doppler, M. Rinne, C. Wijting, C. B. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 42–49, 2009.

[7] S. A. Mousavifar, Y. Liu, C. Leung, M. Elkashlan, and T. Q. Duong, "Wireless energy harvesting and spectrum sharing in cognitive radio," in *in Proc. IEEE Vehicular Technology Conference (VTC Fall), 80th*, 2014, pp. 1–5.

[8] A. H. Sakr and E. Hossain, "Cognitive and energy harvesting-based D2D communication in cellular networks: Stochastic geometry modeling and analysis," *http://arxiv.org/abs/1405.2013*, 2014.

[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[10] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, 2010.

[11] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *Accepted by IEEE Trans. Veh. Technol.*, 2014.

[12] I. Krikidis, S. Sasaki, S. Timotheou, and Z. Ding, "A low complexity antenna switching for joint wireless information and energy transfer in mimo relay channels," *IEEE Trans. Commun.*, 2014.

[13] Y. Liu, L. Wang, M. Elkashlan, T. Q. Duong, and A. Nallanathan, "Two-way relaying networks with wireless power transfer: Policies design and throughput analysis," *In Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Austin Texas, USA 2014.

[14] S. A. R. Zaidi, D. C. McLernon, and M. Ghogho, "Breaking the area spectral efficiency wall in cognitive underlay networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, 2014.

[15] W. K. D. Stoyan and J. Mecke, *Stochastic Geometry and its Applications*, 2nd ed. John Wiley and Sons, 1996.

[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. New York, NY, USA: Academic Press, 2000.