

Secure D2D Communication in Large-Scale Cognitive Cellular Networks: A Wireless Power Transfer Model

Liu, Y., Wang, L., Zaidi, S. A. R., Elkashlan, M., & Duong, T. Q. (2015). Secure D2D Communication in Large-Scale Cognitive Cellular Networks: A Wireless Power Transfer Model. *IEEE Transactions on Communications*, *64*(1), 329 - 342. https://doi.org/10.1109/TCOMM.2015.2498171

Published in:
IEEE Transactions on Communications

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
© 2015 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Open Access
This research has been made openly available by Queen's academics and its Open Research team. We would love to hear how access to this research benefits you. – Share your feedback with us: http://go.qub.ac.uk/oa-feedback

Download date:22. Mar. 2026

Secure D2D Communication in Large-Scale Cognitive Cellular Networks: A Wireless Power Transfer Model

Yuanwei Liu, Lifeng Wang, Syed Ali Raza Zaidi, Maged Elkashlan, and Trung Q. Duong

***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 primary 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, three wireless power transfer (WPT) policies are proposed: 1) cooperative power beacons (CPB) power transfer, 2) best power beacon (BPB) power transfer, and 3) nearest power beacon (NPB) power transfer. To characterize the power transfer reliability of the proposed three policies, we derive new expressions for the exact power outage probability. Moreover, the analysis of the power outage probability is extended to the case when PBs are equipped with large antenna arrays. In the information signal model, we present a new comparative framework with two receiver selection schemes: 1) best receiver selection (BRS), where the receiver with the strongest channel is selected, and 2) nearest receiver selection (NRS), where the nearest receiver is selected. To assess the secrecy performance, we derive new analytical expressions for the secrecy outage probability and the secrecy throughput considering the two receiver selection schemes using the proposed WPT policies. We presented Monte-carlo simulation results to corroborate our analysis and show: 1) secrecy performance improves with increasing densities of PBs and D2D receivers due to larger multiuser diversity gain, 2) CPB achieves better secrecy performance than BPB and NPB but consumes more power, and 3) BRS achieves better secrecy performance than NRS but demands more instantaneous feedback and overhead. A pivotal conclusion is reached that with increasing number of antennas at PBs, NPB offers a comparable secrecy performance to that of BPB but with a lower complexity.**

***Index Terms*—Cognitive cellular networks, D2D communication, physical layer security, stochastic geometry, wireless power transfer**

I. Introduction

The unprecedented expansion of new Internet-enabled smart devices, applications, and serves is driving the need for exploring more energy and spectral efficient future wireless networks. Wireless power transfer (WPT) has recently received significant attention for its attractive energy transfer capabilities and prolonging the life-time of mobile devices. More importantly, recent advances (at various frontiers) in hardware development have rendered wireless charging technology as a practically realizable solution for future applications [1]. It is worth noting that WPT can use radio-frequency (RF) signals [2, 3] to transfer energy to low-power devices for charging them. Furthermore, motivated by the potential of energy and information simultaneously carried during transmission, a tremendous amount of researchers paying attention to this field [4–6]. An ideal receiver design, namely simultaneous wireless information and power transfer (SWIPT), which assumed decoding of information and harvesting of energy from the same signal was initially proposed in [4]. However, due to the circuit limitations, this assumption does not hold in practice [5]. To overcome this issue, two practical receiver designs namely time switching (TS) and power splitting (PS) were proposed in a multiple-input multiple-output (MIMO) system [6].

Along with improving the energy efficiency through energy harvesting, another key design challenges for the future wireless networks is to maximize the spectral efficiency. Cognitive radio (CR) [7] and device-to-device (D2D) technology [8], have rekindled the interest of researchers to achieve more spectrally efficient cellular networks. In order to meet rising demands, dense deployment of BSs is critical. However, dense deployment comes at the cost of increased energy consumption. This can be mitigated by offloading traffic in a local manner through D2D communication.

Furthermore, it is currently noted that CR networks are 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 is a promising mechanism which was initialed by Wyner [9] and has recently sparked wide-spread interest, and 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 secure CR networks.

The review of this paper was coordinated by Prof. J. Yuan. This work was presented in part at the IEEE International Conference on Communications (ICC), London, UK, June 2015.

Y. Liu, L. Wang, and M. Elkashlan are with Queen Mary University of London, London, UK (email:{yuanwei.liu, lifeng.wang, maged.elkashlan}@qmul.ac.uk).

S. A. Raza Zaidi is with University of Leeds, Leeds, UK (e-mail: s.a.zaidi@leeds.ac.uk).

T. Duong is with Queen's University Belfast, Belfast, UK (e-mail: trung.q.duong@qub.ac.uk).

This work was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22 and by the Newton Institutional Link under Grant ID 172719890.

A. Related Works

WPT and PHY layer security has been recently developed in cellular and CR networks. In [12], a new concept based on power beacons (PBs) that deploy dedicated power stations to charge the nearby mobile devices with WPT was proposed. Employing the stochastic geometry framework, the authors investigated the uplink performance in cellular networks under an outage constraint. In [13], a CR network where the secondary transmitters can harvest energy from RF signals of the neighboring active primary transmitter was proposed. The authors proposed a stochastic geometry model and maximized the throughput of the secondary transmitters under several outage constraints. In [14], D2D communication in energy harvesting CR networks was proposed using stochastic geometry. It was shown that acceptable outage performance of D2D communication was achieved without affecting the cellular network. In cellular networks, physical layer security is important for adding another level of protection. Secure downlink transmission in cellular networks was investigated In [15]. In [16], the cell association and location information of mobile users play an important role in secrecy performance in multi-cell environments. It was shown in [17] that the interference from D2D transmission can enhance physical layer security of cellular communications. In [18], the robust transmitter design via optimization for secure cognitive radio networks was addressed.

B. Motivation

While the aforementioned literature have played a vital role and laid a solid foundation for fostering new CR and WPT technologies, the impact of PHY layer security in CR networks with WPT is less well understood. Considering the factors mentioned above, we explore the design space of future wireless networks in terms of both reliability and information theoretic security for the D2D networks which are empowered by WPT. To be more specific, in this paper, we consider secure D2D communication in large-scale cognitive cellular networks with an energy constrained D2D transmitter. The D2D transmitter first harvests energy from PBs, then performs secure transmission to the desired D2D receiver. The interference power at the BSs in primary network from the D2D transmitter should not exceed a peak interference power threshold. 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. Since the location of PBs, D2D receivers, and eavesdroppers in the D2D network is not known in advance, it is natural to compute the spatial averages of the desired performance metrics. To this end, the framework of Point processes from the stochastic geometry can be exploited. In recent past, several studies have employed such a framework for exploring design space of D2D communication. However, to the best of our knowledge, dynamics of WPT and its impact of secrecy remains uncharted.

C. Contribution and Organization

In this paper, we apply homogeneous PPP to model the locations of PBs, D2D receivers (Bobs), eavesdroppers (Eves), and base stations (BSs). We propose a new WPT model, different from [12] which requires energy storage units at the mobile terminals, we deploy a battery-free design [19, 20] at the energy constrained D2D transmitter. In this model, we consider the impact of small scale fading when processing the WPT which was not considered in [12]. We also propose a new information signal model, differing from [14] which considers overlay inband D2D communication [21], here we consider secure underlay inband D2D communication.

The primary contribution of this paper is to propose and analyze the PHY layer security in energy constrained D2D communication under a power constraint of BSs in a large-scale cellular network. The detailed contribution of this paper is summarized as follows:

- In the power transfer model, we propose three WPT policies: 1) cooperative power beacons (CPB) power transfer, where all PBs transfer power to the transmitter; 2) best power beacon (BPB) power transfer, where a PB with the strongest channel transfers power to the transmitter; and 3) nearest power beacon (NPB) power transfer, where the nearest PB transfers power to the transmitter. In the signal information model, we present a new comparative framework for each of the three WPT policies with two receiver selection schemes, namely: 1) best receiver selection (BRS) scheme, where the receiver with the strongest channel is selected as the desired receiver; and 2) nearest receiver selection (NRS) scheme, where the nearest receiver is selected as the desired receiver.
- For the three proposed WPT policies, we derive new exact expressions for the power outage probability. We also derive new asymptotic expressions for the power outage probability when the number of antennas M at PBs goes to infinity. We show that the power outage probability significantly decreases with increasing M and increasing density of PBs.
- Based on the exact results for the power outage probability, we derive new expressions for the secrecy outage probability and the secrecy throughput for two receiver selection schemes: BRS and NRS. The aim is to examine the impact of various network parameters, such as density of D2D receivers, threshold transmit power, and information transmission time fraction, on the secrecy performance under different WPT policies and receiver selection schemes.
- Comparing the three WPT policies: CPB, BPB, and NPB, we show that, for the exact analysis: 1) secrecy performance improves with increasing density of PBs because of a larger multiuser diversity gain; 2) CPB achieves better secrecy performance than BPB and NPB but consumes more power; and 3) NPB achieves a comparable secrecy performance to that of BPB but with lower complexity. For the large antenna array analysis, we show that the small scale fading can be neglected for

large values of M.

- Comparing the BRS and NRS schemes along with the three proposed policies in terms of secrecy outage probability and secrecy throughput, we show that: 1) BRS achieves better secrecy performance than NRS, which comes at the cost of additional overhead; 2) secrecy performance improves with increasing density of D2D receivers due to larger multiuser diversity gain; and 3) optimal value for maximizing the secrecy throughput exits for the information transmission time fraction and the expected transmit power.

The rest of the paper is organized as follows. In Section II, the network model considering three WPT policies and the two receiver selection schemes are presented. In Section III, new expressions are derived for the exact analysis and the large antenna array analysis for the power outage probability of the three WPT policies. In Section IV, taking into account the joint impact of the WPT policies in the power transfer model and the two receiver selection schemes in the signal information model, new expressions are derived for the secrecy outage probability and secrecy throughput. Numerical results are presented in Section V, which is followed by conclusions drawn in Section VI.

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 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. 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 equipped with one antenna operating in half-duplex mode and a battery-free user with rechargeable abilities, 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 signals in the current information transmission slot [1] [19, 20, 22].

1) Cooperative Power Beacons (CPB) Power Transfer: In this case, we consider the scenario that Alice harvests the aggregate received power transmitted by all PBs. The motivation behind the proposed CPB is that in some scenarios, the D2D communication demands high system performance. CPB can maximize the power transferred to Alice for performance enhancement, but this comes at the cost of high energy consumption at PBs. Mathematically, the harvested energy can be quantified as

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

where η is the power conversion efficiency of the receiver, P_S is the total transmit power of all antennas at 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. $L\left(r_p\right) = K r_p^{-\alpha}$ 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 $\alpha > 2$. 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

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

2) Best Power Beacon (BPB) Power Transfer: In this case, we consider the scenario that Alice selects the strongest PB to harvest energy. The motivation behind the proposed BPB is that it is most energy efficient. However, this policy demands instantaneous feedback information of all PBs, which increases the complexity. Therefore, BPB is suitable for scenarios where channel fading changes fast during the transmission. As such, the maximum transmit power of BPB at Alice can be obtained as

$$P_H = \eta P_S \max_{p\in\Phi_p} \left\{ \|\mathbf{h}_p\|^2 L\left(r_p\right)\right\} \frac{(1-\beta)}{\beta}. \tag{3}$$

3) Nearest Power Beacon (NPB) Power Transfer: In this case, we consider the scenario that Alice selects the nearest PB to harvest energy. The motivation behind the proposed NPB is that it reduces the system implementation complexity. However, the price is paid in terms of overall performance. The proposed NPB scheme requires least amount of feedback

[1] In this paper, it is assumed that the power consumption for handshaking between Alice and PB(s) is negligible, compared to that for the information transmission [12] .

amongst all schemes. The maximum transmit power of NPB at Alice can be obtained as

$$P_H = \eta P_S \|\mathbf{h}_{p^*}\|^2 \max_{p\in\Phi_p}\{L(r_p)\}\frac{(1-\beta)}{\beta}, \tag{4}$$

where $\mathbf{h}_{p^*}$ 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 from the nearest PB to Alice.

C. Information Signal Model

We consider the cognitive underlay scheme [23, 24], and assume that the instantaneous CSI of the links between Alice and cellular BSs are available at Alice (a commonly-seen assumption in the cognitive radio literature such as [25]). Consequently, the transmit power P_A at Alice is strictly constrained by the preset maximum transmit power $P_{\rm t}$ at Alice ($P_{\rm t} \leq P_{\max}$ should be satisfied where $P_{\max}$ is the maximum transmit power dictated by both regulatory and amplifier design constraint) and the peak interference power I_p at BSs according to and the peak interference power I_p at BSs according to

$$P_A = \min\left\{\frac{I_p}{\max\limits_{\ell\in\Phi_\ell}\left\{|h_\ell|^2 L(r_\ell)\right\}}, P_{\rm t}\right\}, \tag{5}$$

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 $L(r_\ell) = Kr_\ell^{-\alpha}$ 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.. The D2D communication aims at providing low-power short-range communication links that coexist with the cellular communication. In terms of low-power links, we apply a battery-free design at Alice to harvest energy from the PB/PBs. In terms of short-range links, we consider two receiver selection schemes to select the D2D receiver.

1) Best Receiver Selection (BRS) scheme: In the proposed information signal model, we focus on D2D communication of uplink transmission in cellular networks. In the secondary network, the D2D transmitter can perform concurrent transmissions using the same spectrum band as the primary network as long as the interference to the BS is below a threshold. We assume that the interference from the primary transmitters on the secrecy performance is negligible due to: 1) the D2D receiver is close to the D2D transmitter; 2) the primary transmitters are located far away from the secondary network; and 3) the primary transmitters in the uplink are mobile users with low transmit power. Under BRS, Alice selects one Bob with the strongest channel as the desired receiver. In the wiretap channel, the secrecy performance can be effectively enhanced to prevent information leakage by improving the conditions of the main channel. In our system design, we aim to enhance the main channel condition by proposing two receiver selection schemes to improve the physical layer security. The motivation behind BRS is that the D2D receiver will experience the benefit of multiuser diversity gain to obtain the best main channel condition among all the D2D receivers. As a result, the secrecy performance is enhanced. The instantaneous signal-to-noise ratio (SNR) at the selected Bob is expressed as

$$\begin{aligned}\gamma_{\rm B} =& \frac{P_A}{N_0}\max_{b\in\Phi_b}\left\{|h_b|^2 L(r_b)\right\}\\ =& \zeta\max_{b\in\Phi_b}\left\{|h_b|^2 L(r_b)\right\},\end{aligned} \tag{6}$$

where $\zeta = \min\left\{\frac{\bar{\gamma}_p}{\max\limits_{\ell\in\Phi_\ell}\left\{|h_\ell|^2 L(r_\ell)\right\}}, \bar{\gamma}_0\right\}$, $\bar{\gamma}_p = I_p/N_0$, $\bar{\gamma}_0 = P_{\rm t}/N_0$, N_0 is the noise power, $|h_b|^2 L(r_b)$ 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[2]. The motivation behind this scheme is that while experiencing the benefit of multiuser diversity gain, NRS reduces the system complexity in comparison to BRS since no instantaneous CSI and no instantaneous feedback from Bobs are required. Then the instantaneous SNR at the selected Bob can be expressed as

$$\begin{aligned}\gamma_{\rm B^*} =& \frac{P_A}{N_0}|h_{b^*}|^2\max_{b\in\Phi_b} L(r_b)\\ =& \zeta|h_{b^*}|^2\max_{b\in\Phi_b} L(r_b),\end{aligned} \tag{7}$$

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

$$\begin{aligned}\gamma_{\rm E} =& \frac{P_A}{N_0}\max_{e\in\Phi_e}\left\{|h_e|^2 L(r_e)\right\}\\ =& \zeta\max_{e\in\Phi_e}\left\{|h_e|^2 L(r_e)\right\},\end{aligned} \tag{8}$$

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_{th}, below which 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 with CPB, BPB, and NPB policies (see Section II). In practical scenario, we expect a constant power for the information transmission. Therefore, we also denote the power threshold as the transmit power of Alice when performing information transmission to Bobs with $P_{\rm t} = P_{th}$. Furthermore, in order to guarantee the energy harvesting circuit to be activated, we consider there is a minimum threshold (denoted as P_m) [26]. When

[2]During the information transmission phase, multiuser diversity is exploited to improve the secrecy and D2D receivers are opportunistically selected.

we proceeding system parameter design, we always assume $P_{th} \geq P_m$ in the rest of this paper.

A. Exact Analysis for Power Transfer

In this subsection, we provide exact analysis for the proposed three power transfer policies.

1) Cooperative Power Beacons (CPB) Power Transfer: In this policy, all PBs help to transfer power to Alice. Based on (2), the power outage probability of CPB policy can be expressed as

$$\begin{aligned} H_{out} &= \Pr\left\{\eta P_S \mathcal{S}\frac{(1-\beta)}{\beta} \leq P_{\mathrm{t}}\right\} \\ &= \int_0^{\frac{P_{\mathrm{t}}\beta}{\eta P_S(1-\beta)}} f_{\mathcal{S}}(x)\,dx, \end{aligned} \tag{9}$$

where $\mathcal{S} = \sum_{p\in\Phi_p} \|\mathbf{h}_p\|^2 L(r_p)$ and $f_{\mathcal{S}}(x)$ is the probability density function (PDF) of $\mathcal{S}$. Note that the laplace transformation of $f_{\mathcal{S}}(x)$ is [27, eq. 8]

$$\begin{aligned} \mathcal{L}_{\mathcal{S}}(s) &= \exp\left(-\lambda_p \pi K^{2/\alpha} E\left(\|\mathbf{h}_p\|^{4/\alpha}\right)\Gamma\left(1-\frac{2}{\alpha}\right)s^{2/\alpha}\right) \\ &= \exp\left(-\lambda_p \pi K^{2/\alpha}\frac{\Gamma\left(M+\frac{2}{\alpha}\right)}{\Gamma(M)}\Gamma\left(1-\frac{2}{\alpha}\right)s^{2/\alpha}\right), \end{aligned} \tag{10}$$

where $\Gamma(.)$ is Gamma function. Hence $f_{\mathcal{S}}(x)$ is the inverse laplace transform of $\mathcal{L}_{\mathcal{S}}(s)$, which can be expressed as $f_{\mathcal{S}}(x) = \mathcal{L}_{\mathcal{S}}^{-1}(s)$. Since the explicit expression for $\mathcal{L}_{\mathcal{S}}^{-1}(s)$ is intractable, there are alternatives to proceed such as using numerical inversion methods for Laplace transform [28]. We should note that some approximation methods using moments such as log-normal distribution in [29] are not applicable, due to the singularity caused by proximity. Although the PDF of $\mathcal{S}$ is not available, with the help of Gil-Pelaez theorem [30], we calculate (9) in an elegant form

$$\begin{aligned} H_{out} &= F_{\mathcal{S}}\left(\frac{P_{\mathrm{t}}\beta}{\eta P_S(1-\beta)}\right) \\ &= \frac{1}{2} - \frac{1}{\pi}\int_0^{\infty} \frac{\mathrm{Im}\left[e^{-jw\frac{P_{\mathrm{t}}\beta}{\eta P_S(1-\beta)}}\varphi^*(w)\right]}{w}dw, \end{aligned} \tag{11}$$

where $F_{\mathcal{S}}(x)$ is the cumulative distribution function (CDF) of $\mathcal{S}$, $j = \sqrt{(-1)}$, and $\varphi(w)$ is the conjugate of the characteristic function, which is given by

$$\begin{aligned} &\varphi(w) = \mathcal{L}_{\mathcal{S}}(s)\,|_{s=jw} \\ &= \exp\left(-\lambda_p \pi K^{2/\alpha}\frac{\Gamma\left(M+\frac{2}{\alpha}\right)}{\Gamma(M)}\Gamma\left(1-\frac{2}{\alpha}\right)(jw)^{2/\alpha}\right). \end{aligned} \tag{12}$$

Special Case: For the special case of path-loss exponent $\alpha = 4$, $\mathcal{L}_{\mathcal{S}}(s)$ in (10) becomes

$$\mathcal{L}_{\mathcal{S}}(s)|_{\alpha=4} = \exp\left(-\lambda_p \pi K^{1/2}\frac{\Gamma(M+1/2)}{\Gamma(M)}\Gamma(1/2)\,s^{1/2}\right), \tag{13}$$

and its inverse-transform is well-known formed as [31, 32]

$$\begin{aligned} f_{\mathcal{S}}(x)|_{\alpha=4} &= \frac{\pi}{2}\lambda_p K^{1/2}\frac{\Gamma(M+1/2)}{\Gamma(M)}x^{-3/2} \\ &\quad \times \exp\left(-\pi^3\frac{\lambda_p^2 K}{4x}\left(\frac{\Gamma(M+1/2)}{\Gamma(M)}\right)^2\right). \end{aligned} \tag{14}$$

Substituting (14) into (9), we can obtain the power outage probability for the special case $\alpha = 4$ as

$$\begin{aligned} H_{out}|_{\alpha=4} &= \int_0^{\frac{P_{\mathrm{t}}\beta}{\eta P_S(1-\beta)}} \frac{\pi}{2}\lambda_p K^{1/2}\frac{\Gamma(M+1/2)}{\Gamma(M)}x^{-3/2} \\ &\quad \times \exp\left(-\pi^3\frac{\lambda_p^2 K}{4x}\left(\frac{\Gamma(M+1/2)}{\Gamma(M)}\right)^2\right)dx. \end{aligned} \tag{15}$$

Using the method of element changing and with the help of complementary error function (CEF) $erfc(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt$, we can express (15) in closed-from as follows:

$$H_{out}|_{\alpha=4} = erfc\left(\frac{\lambda_p}{2}\frac{\Gamma(M+1/2)}{\Gamma(M)}\sqrt{\frac{\pi^3 K\eta P_S(1-\beta)}{P_{\mathrm{t}}\beta}}\right), \tag{16}$$

Remark 1. *Since CEF is a strictly monotonic decreasing function, the derived result in* (16) *indicates that the power outage probability decreases with increasing density of PBs.*

2) Best Power Beacon (BPB) Power Transfer: 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

$$H_{out} = e^{\frac{-\lambda_p \pi\delta}{\mu^\delta}\sum_{m=0}^{M-1}\left(\frac{\Gamma(m+\delta)}{m!}\right)}, \tag{17}$$

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

Proof: Based on (3)*, the power outage probability of BPB can be expressed as*

$$\begin{aligned} &\Pr\{P_H \leq P_{\mathrm{t}}\} = \Pr\left\{\max_{p\in\Phi_p}\left\{\|\mathbf{h}_p\|^2 {r_p}^{-\alpha}\right\} \leq \mu\right\} \\ &= E_{\Phi_p}\left\{\prod_{p\in\Phi_p}\Pr\left\{\|\mathbf{h}_p\|^2 \leq r_p^\alpha \mu\right\}\middle|\,\Phi_p\right\} \\ &= E_{\Phi_p}\left\{\prod_{p\in\Phi_p} F_{\|\mathbf{h}_p\|^2}\left(r_p^\alpha \mu\right)\middle|\,\Phi_p\right\}, \end{aligned} \tag{18}$$

where $F_{\|\mathbf{h}_p\|^2}$ is the CDF of $\|\mathbf{h}_p\|^2$. Since $\mathbf{h}_p$ is $\mathcal{C}^{M\times 1}$ vector, whose entries are independent complex Gaussian distributed with zero mean and unit variance, $\|\mathbf{h}_p\|^2$ follows a chi-squared distribution given by [33, Eq. (26.4)]

$$F_{\|\mathbf{h}_p\|^2}(x) = 1 - \frac{\Gamma(M,x)}{\Gamma(M)}. \tag{19}$$

Since M is an integer value, using [34, Eq. (8.832.2)], we can re-express (19) *as follows:*

$$F_{\|\mathbf{h}_p\|^2}(x) = 1 - e^{-x}\left(\sum_{m=0}^{M-1}\frac{x^m}{m!}\right). \tag{20}$$

Applying the generating functional given by [34], we rewrite (18) *as*

$$H_{out} = \exp\left[-\lambda_p \int_{R^2}\left(1 - F_{\|\mathbf{h}_p\|^2}\left(r_p{}^{\alpha}\mu\right)\right)dr_p\right]. \tag{21}$$

Then changing to polar coordinates and substituting (20) *into* (21)*, the power outage probability of BPB is given by*

$$H_{out} = \exp\left[-2\pi\lambda_p \sum_{m=0}^{M-1}\frac{\mu^m \int_0^{\infty} r_p{}^{m\alpha+1} e^{-r_p{}^{\alpha}\mu} dr_p}{m!}\right]. \tag{22}$$

Then applying [35, Eq. (3.326.2)] and calculating the integral in (22)*, we obtain the closed-form expression in* (17). ■

Remark 2. *The derived result in* **Theorem 1** *indicates that the power outage probability is a strictly monotonic decreasing function of λ_p. Consequently, the power outage probability decreases with increasing density of PBs.*

3) Nearest Power Beacon (NPB) Power Transfer: In this policy, only the nearest PB transfers power to Alice.

Theorem 2. The power outage probability of NPB policy is expressed as

$$H_{out} = 1 - 2\lambda_p\pi \times \sum_{m=0}^{M-1}\left(\frac{\mu^m}{m!}\int_0^{\infty} r_{p^*}{}^{m\alpha+1} e^{-\lambda_p\pi r_{p^*}^2 - \mu r_{p^*}^{\alpha}} dr_{p^*}\right), \tag{23}$$

where $\mu = \frac{\beta P_{\mathrm{t}}}{(1-\beta)\eta P_S K}$ *and* r_{p^*} representing the distance from the nearest PB to Alice.

Proof: Based on (4)*, the power outage probability of NPB can be expressed as*

$$\begin{aligned} H_{out} &= \Pr\left\{P_H \le P_{\mathrm{t}}\right\} = \Pr\left\{\|\mathbf{h}_{p^*}\|^2 \le \mu r_{p^*}{}^{\alpha}\right\} \\ &= \int_0^{\infty} F_{\|\mathbf{h}_p\|^2}\left(r_{p^*}{}^{\alpha}\mu\right) f\left(r_{p^*}\right) dr_{p^*}, \end{aligned} \tag{24}$$

$F_{\|\mathbf{h}_{p^*}\|^2}$ is the CDF of $\|\mathbf{h}_{p^*}\|^2$ which has been expressed similarly in (20)*. We can express the PDF of the nearest PB with*

$$f\left(r_{p^*}\right) = 2\lambda_p\pi r_{p^*} e^{-\lambda_p\pi r_{p^*}^2}. \tag{25}$$

Substituting (25) *and* (20) *into* (24)*, and after some manipulations, we can get the final result in* (23). ■

Special Case: We note that for general case, there is no closed-form expression of (23), however, we can consider the special case and proceed simplifications to allow the path loss exponent $\alpha = 4$.

Substituting $\alpha = 4$ into (23) and after some manipulations, we have

$$H_{out}|_{\alpha=4} = 1 - \lambda_p\pi \times \sum_{m=0}^{M-1}\left(\frac{\mu^m}{m!}\int_0^{\infty} r_{p^*}{}^{4m} e^{-\lambda_p\pi r_{p^*}^2 - \mu r_{p^*}^4} dr_{p^*}^2\right). \tag{26}$$

Then applying [35, Eq. (3.462.1)], we express (26) in closed-form for the special case when $\alpha = 4$ as

$$H_{out}|_{\alpha=4} = 1 - \frac{\lambda_p\pi e^{\frac{(\lambda_p\pi)^2}{8\mu}}}{\sqrt{\mu}} \times \sum_{m=0}^{M-1}\left(2^{-\frac{2m+1}{2}}\frac{\Gamma(2m+1)}{m!}D_{-(2m+1)}\left(\frac{\lambda_p\pi}{\sqrt{2\mu}}\right)\right), \tag{27}$$

where $D_p(x)$ is the parabolic cylinder functions.

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

$$\|\mathbf{h}_p\|^2 \overset{a.s.}{\to} M, \tag{28}$$

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

1) Large Antenna Array Analysis for CPB: Similar as (11), we obtain the expression of power outage probability for large antenna array analysis as

$$H_{out}^{\infty} = \frac{1}{2} - \frac{1}{\pi}\int_0^{\infty}\frac{\mathrm{Im}\left[e^{-jw\frac{P_{\mathrm{t}}\beta}{\eta P_S(1-\beta)}}\varphi_{\infty}^*(w)\right]}{w}dw, \tag{29}$$

Based on (10), with the help of (28), we express the Laplace transform of the large antenna array as

$$\mathcal{L}_S^{\infty}(s) = \exp\left(-\lambda_p\pi K^{2/\alpha}M^{2/\alpha}\Gamma\left(1-\frac{2}{\alpha}\right)s^{2/\alpha}\right). \tag{30}$$

Then applying $s = jw$ into (30), $\varphi_{\infty}(w)$ can be expressed as

$$\varphi_{\infty}(w) = \exp\left(-\lambda_p\pi K^{2/\alpha}M^{2/\alpha}\Gamma\left(1-\frac{2}{\alpha}\right)(jw)^{2/\alpha}\right). \tag{31}$$

Special Case: For the special case when the path-loss exponent $\alpha = 4$, based on (2), the power outage probability is given by

$$\begin{aligned} H_{out}^{\infty}|_{\alpha=4} &= \Pr\left\{\eta P_S \mathcal{S}^{\infty}\frac{(1-\beta)}{\beta} \le P_{\mathrm{t}}\right\} \\ &= \int_0^{\frac{P_{\mathrm{t}}\beta}{\eta P_S(1-\beta)}} f_{\mathcal{S}}^{\infty}(x)\,dx, \end{aligned} \tag{32}$$

where $\mathcal{S}^{\infty} = M\sum_{p\in\Phi_p} L(r_p)$ and $f_{\mathcal{S}}^{\infty}(x)$ is the PDF of $\mathcal{S}^{\infty}$.

We have the inverse-transform of $\varphi_{\infty}(w)$

$$f_{\mathcal{S}}^{\infty}(x) = \frac{\pi}{2}\lambda_p K^{1/2}M^{1/2}x^{-3/2}\exp\left(-\pi^3\frac{\lambda_p^2 KM}{4x}\right). \tag{33}$$

Substituting (33) into (32), we obtain

$$H_{out}^{\infty}|_{\alpha=4} = \frac{\pi}{2}\lambda_p K^{1/2} M^{1/2} \times \int_0^{\frac{P_{\rm t}\beta}{\eta P_S(1-\beta)}} x^{-3/2} \exp\left(-\pi^3 \frac{\lambda_p^2 K M}{4x}\right) dx. \quad (34)$$

Similarly as (16), we apply the CEF to derive (34) in closed-from as follows:

$$H_{out}^{\infty}|_{\alpha=4} = erfc\left(\frac{\lambda_p}{2}\sqrt{\frac{M\pi^3 K\eta P_S(1-\beta)}{P_{\rm t}\beta}}\right). \quad (35)$$

Remark 3. *Since CEF is a strictly monotonic decreasing function, the derived result in* (35) *indicates that the power outage probability decreases with increasing number of attennas and density of PBs.*

2) Large Antenna Array Analysis for BPB and NPB: Substituting (28) into (23) and (17), we find that the expressions of the power outage probability for BPB policy and NPB policy are identical.

Theorem 3. The power outage probability for the BPB or NPB can be expressed in closed-form as

$$H_{out}^{\infty} = e^{-\frac{\lambda_p \pi}{\theta^{\delta}}}, \quad (36)$$

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

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

$$H_{out}^{\infty} = \Pr\{P_H \le P_{\rm t}\} = \Pr\left\{r_{p^*}^{-\alpha} \le \theta\right\} = 1 - F_{r_{p^*}}\left(\sqrt[\alpha]{\frac{1}{\theta}}\right), \quad (37)$$

where $F_{r_{p^*}}$ is the CDF of r_{p^*} and can be expressed as

$$F_{r_{p^*}}(x) = \int_0^x f(r_{p^*}) dr_{p^*} = 1 - e^{-\lambda_p \pi x^2}, \quad (38)$$

with PDF of r_{p^*} is given by $f(r_{p^*}) = 2\lambda_p \pi r_{p^*} e^{-\lambda_p \pi r_{p^*}^2}$.

Substituting (38) *into* (37)*, we can obtain* (36). ∎

Remark 4. *The derived result in* **Theorem 3** *indicates that for a large number of transmit antenna M, the small scale fading is averaged out. It also indicates that* (36) *is a strictly monotonic decreasing function of λ_p and M.*

IV. Secrecy Performance Evaluations

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

A. New Statistics

Theorem 4. The PDF of $\zeta = \frac{P_A}{N_0}$ is given by

$$f_{\zeta}(x) = \begin{cases} \left(\frac{\omega_\ell \delta x^{(\delta-1)}}{\bar{\gamma}_p^{\delta}}\right) e^{-\frac{\omega_\ell x^{\delta}}{\bar{\gamma}_p^{\delta}}}, & 0 < x < \bar{\gamma}_0 \\ e^{-\frac{\omega_\ell \bar{\gamma}_0^{\delta}}{\bar{\gamma}_p^{\delta}}} Dirac(x - \bar{\gamma}_0), & x \ge \bar{\gamma}_0 \end{cases}, \quad (39)$$

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

Proof: See Appendix A . ∎

Theorem 5. For BRS scheme, the CDF of γ_B conditioned on ζ is given by

$$F_{\gamma_B|\zeta}(z) = e^{-\frac{\omega_B \zeta^{\delta}}{z^{\delta}}}, \quad (40)$$

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

$$F_{\gamma_{B^*}|\zeta}(z) = 1 - 2\lambda_b \pi \int_0^{\infty} r_{b^*} e^{-\lambda_b \pi r_{b^*}^2 - \frac{z}{K\zeta} r_{b^*}^{\alpha}} dr_{b^*}. \quad (41)$$

Proof: See Appendix B . ∎

Similar to (40), we can obtain the CDF of γ_E conditioned on ζ as

$$F_{\gamma_E|\zeta}(z) = e^{-\frac{\omega_E \zeta^{\delta}}{z^{\delta}}}, \quad (42)$$

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

Taking the derivative of $F_{\gamma_E|\zeta}$ in (42), we obtain the PDF of γ_E conditioned on ζ as

$$f_{\gamma_E|\zeta}(z) = \frac{\omega_E \delta \zeta^{\delta}}{z^{\delta+1}} e^{-\frac{\omega_E \zeta^{\delta}}{z^{\delta}}}. \quad (43)$$

B. Secrecy Performance Evaluation of BRS scheme

In this scheme, the instantaneous secrecy rate is defined as

$$C_s^{\rm BRS} = [\log_2(1+\gamma_B) - \log_2(1+\gamma_E)]^+, \quad (44)$$

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

1) Secrecy Outage Probability: In the classical case, a secrecy outage is declared when the secrecy capacity $C_s^{\rm BRS}$ is less than the expected secrecy rate R_s. As such, the secrecy outage probability for BRS can be expressed as

$$P_{out}^{\rm BRS} = \Pr\left(C_s^{\rm BRS} < R_s\right) = \int_0^{\infty}\int_0^{\infty} f_{\gamma_E|\zeta}(x_2) F_{\gamma_B|\zeta}\left(2^{R_s}(1+x_2) - 1\right) \times f_{\zeta}(x_1) dx_2 dx_1. \quad (45)$$

Theorem 6. The secrecy outage probability for BRS is derived on the top of next page in (46), where $a_1 = \frac{\omega_\ell \omega_E \delta}{\bar{\gamma}_p^{\delta}}$ and $a_2 = \omega_E \delta \bar{\gamma}_0^{\delta} e^{-\frac{\omega_\ell \bar{\gamma}_0^{\delta}}{\bar{\gamma}_p^{\delta}}}$.

Proof: By plugging (39) *into* (45)*, the secrecy outage probability for BRS is given by*

$$P_{out}^{\rm BRS} = \int_0^{\bar{\gamma}_0}\int_0^{\infty} f_{\gamma_E|\zeta}(x_2) F_{\gamma_B|\zeta}\left(2^{R_s}(1+x_2) - 1\right) \times \left(\frac{\omega_\ell \delta x_1^{\delta-1}}{\bar{\gamma}_p^{\delta}}\right) e^{-\frac{\omega_\ell x_1^{\delta}}{\bar{\gamma}_p^{\delta}}} dx_2 dx_1 + e^{-\frac{\omega_\ell \bar{\gamma}_0^{\delta}}{\bar{\gamma}_p^{\delta}}} \int_0^{\infty} f_{\gamma_E|\zeta=\bar{\gamma}_0}(x_2) F_{\gamma_B|\zeta=\bar{\gamma}_0}\left(2^{R_s}(1+x_2) - 1\right) dx_2. \quad (47)$$

$$P_{out}^{\mathrm{BRS}} = \int_0^\infty \frac{a_1}{x_2^{\delta+1} Q_1} \left(\frac{1}{Q_1} - \frac{e^{-Q_1 \bar{\gamma}_0^\delta}}{Q_1} - \bar{\gamma}_0^\delta e^{-Q_1 \bar{\gamma}_0^\delta} \right) + a_2 x_2^{-(\delta+1)} e^{-\frac{\omega_E \bar{\gamma}_0^\delta}{x_2^\delta} - \frac{\omega_B \bar{\gamma}_0^\delta}{(2^{R_s}(1+x_2)-1)^\delta}} dx_2, \tag{46}$$

Then plugging (40) *and* (43) *into* (47) *and after some manipulations, we obtain*

$$P_{out}^{\mathrm{BRS}} = \int_0^\infty \frac{1}{x_2^{\delta+1}} \underbrace{\int_0^{\bar{\gamma}_0} x_1^{2\delta-1} e^{-Q_1 x_1^\delta} dx_1}_{\Psi} dx_2 + \omega_E \delta \bar{\gamma}_0^\delta e^{-\frac{\omega_\ell \bar{\gamma}_0^\delta}{\bar{\gamma}_p^\delta}} \int_0^\infty x_2^{-(\delta+1)} e^{\left(-\frac{\omega_E \bar{\gamma}_0^\delta}{x_2^\delta} - \frac{\omega_B \bar{\gamma}_0^\delta}{(2^{R_s}(1+x_2)-1)^\delta} \right)} dx_2, \tag{48}$$

where $Q_1 = \frac{\omega_\ell}{\bar{\gamma}_p^\delta} + \frac{\omega_E}{x_2^\delta} + \frac{\omega_B}{(2^{R_s}(1+x_2)-1)^\delta}$.

Applying partial integral method and after some manipulations, we express Ψ *as*

$$\Psi = \frac{1}{Q_1} \left(\frac{1}{Q_1} - \frac{1}{Q_1} e^{-Q_1 \bar{\gamma}_0^\delta} - \bar{\gamma}_0^\delta e^{-Q_1 \bar{\gamma}_0^\delta} \right). \tag{49}$$

Substituting (49) *into* (48)*, we can obtain* (46). ∎

For a D2D energy constrained transmitter, a secrecy outage also occurs when the harvested energy is not sufficient. Thus the secrecy outage probability with WPT in our system model is expressed as [3]

$$P_{H_{out}}^{\mathrm{BRS}} = H_{out} + (1 - H_{out}) P_{out}^{\mathrm{BRS}}, \tag{50}$$

where H_{out} can be obtained from (11), (17), and (23) for CPB, BPB, and NPB policies, respectively and P_{out}^{BRS} can be obtained from (46).

2) Secrecy Throughput: The secrecy throughput is the average of the instantaneous secrecy rate C_s. As such, the secrecy throughput is given by

$$\bar{C}_s^{\mathrm{BRS}} = (1 - H_{out}) \frac{\beta}{\ln 2} \int_0^\infty \int_0^\infty \frac{F_{\gamma_E|\zeta}(x_2)}{1+x_2} \times \left(1 - F_{\gamma_B|\zeta}(x_2)\right) f_\zeta(x_1) dx_2 dx_1. \tag{51}$$

Substituting (39), (40), and (42) into (51), after some manipulation, the secrecy throughput is derived as

$$\bar{C}_s^{\mathrm{BRS}} = (1 - H_{out}) \frac{\omega_\ell \delta \beta}{\bar{\gamma}_p^\delta \ln 2} \int_0^\infty \frac{1}{1+x_2} \underbrace{\int_0^{\bar{\gamma}_0} e^{-\frac{\omega_E x_1^\delta}{x_2^\delta} - \frac{\omega_\ell x_1^\delta}{\bar{\gamma}_p^\delta}} x_1^{\delta-1} \left(1 - e^{-\frac{\omega_B x_1^\delta}{x_2^\delta}}\right) dx_1}_{\Theta} dx_2 + (1 - H_{out}) \frac{\beta e^{-\frac{\omega_\ell \bar{\gamma}_0^\delta}{\bar{\gamma}_p^\delta}}}{\ln 2} \int_0^\infty \frac{e^{-\frac{\omega_E \bar{\gamma}_0^\delta}{x_2^\delta}}}{1+x_2} \left(1 - e^{-\frac{\omega_B \bar{\gamma}_0^\delta}{x_2^\delta}}\right) dx_2. \tag{52}$$

We calculate the integral Θ as

$$\Theta = \frac{1}{\delta} \left(\frac{1}{Q_2} - \frac{1}{Q_3} + \frac{1}{Q_3} e^{-\bar{\gamma}_0^\delta Q_3} - \frac{1}{Q_2} e^{-\bar{\gamma}_0^\delta Q_2} \right), \tag{53}$$

[3]In this paper, we analyze the secrecy performance under power constraint at Alice.

where $Q_2 = \frac{\omega_E}{x_2^\delta} + \frac{\omega_\ell}{\bar{\gamma}_p^\delta}$ and $Q_3 = \left(\frac{\omega_B}{x_2^\delta} + \frac{\omega_E}{x_2^\delta} + \frac{\omega_\ell}{\bar{\gamma}_p^\delta} \right)$.

Substituting (53) into (52), we obtain secrecy throughput of BRS (54) on the top of next page.

C. Secrecy Performance Evaluation of NRS scheme

In this scheme, the instantaneous secrecy rate is defined as

$$C_s^{\mathrm{NRS}} = \left[\log_2(1 + \gamma_{B^*}) - \log_2(1 + \gamma_E) \right]^+. \tag{55}$$

1) Secrecy Outage Probability: In the NRS scheme, the secrecy outage probability is derived as

$$P_{out}^{\mathrm{NRS}} = \Pr\left(C_s^{\mathrm{NRS}} < R_s\right) = \int_0^\infty \int_0^\infty f_{\gamma_E|\zeta}(x_2) F_{\gamma_{B^*}}\left(2^{R_s}(1+x_2) - 1\right) \times f_\zeta(x_1) dx_2 dx_1. \tag{56}$$

Substituting (39), (41) and (43) into (56), we can obtain the secrecy outage probability for NRS scheme.

Similar as (50), the secrecy outage probability with WPT in our system model is expressed as

$$P_{H_{out}}^{\mathrm{NRS}} = H_{out} + (1 - H_{out}) P_{out}^{\mathrm{NRS}}, \tag{57}$$

where H_{out} can be obtained from (11), (17), and (23) for CPB, BPB, and NPB policies, respectively and P_{out}^{NRS} can be obtained from (56).

2) Secrecy Throughput: In this NRS scheme, the secrecy throughput is given by

$$\bar{C}_s^{\mathrm{NRS}} = (1 - H_{out}) \frac{\beta}{\ln 2} \int_0^\infty \int_0^\infty \frac{F_{\gamma_E|\zeta}(x_2)}{1+x_2} \times \left(1 - F_{\gamma_{B^*}|\zeta}(x_2)\right) f_\zeta(x_1) dx_2 dx_1. \tag{58}$$

Substituting (39), (41), and (42) into (58), 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 outage probability, and secrecy throughput for three WPT policies in the power transfer model and two receiver selection schemes in the information signal model.

A. Network Parameters

In the considered network, 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.

$$\bar{C}_s^{\mathrm{BRS}} = (1-H_{out})\,\frac{\beta}{\ln 2}\left(\int_0^{\infty}\frac{\omega_\ell}{\bar{\gamma}_p^{\delta}\,(1+x_2)}\left(\frac{1}{Q_2}-\frac{1}{Q_3}+\frac{e^{-\bar{\gamma}_0^{\delta}Q_3}}{Q_3}-\frac{e^{-\bar{\gamma}_0^{\delta}Q_2}}{Q_2}\right)+\frac{e^{-\frac{\omega_\ell\bar{\gamma}_0^{\delta}}{\bar{\gamma}_p^{\delta}}-\frac{\omega_E\bar{\gamma}_0^{\delta}}{x_2^{\delta}}}}{1+x_2}\left(1-e^{-\frac{\omega_B\bar{\gamma}_0^{\delta}}{x_2^{\delta}}}\right)dx_2\right). \tag{54}$$

B. Power Outage Probability

Fig. 1 plots the power outage probability versus different numbers of antennas at PBs using the exact analysis and the large antenna array analysis. The dashed black curve, representing the large antenna array analysis of CPB is obtained from (29) as well as (35). The dashed red curve, representing the large antenna array analysis of BPB and NPB (which we refer to as B(N)PB in the figure) is obtained from (36). We see that the power outage probability decreases with increasing M. This is because a larger array gain is achieved with increasing M. As M increases, the large antenna array analysis and the exact analysis have good agreement. We also see that as M increases, the exact analysis of BPB and NPB performs identically. This is due to the fact that as M grows large, the effect of small scale fading is averaged out. In this case, we should select NPB due to its lower complexity.

Fig. 2 plots the power outage probability versus density of PBs with different M. The black, red, and blue curves, representing the CPB, BPB, and NPB policies are obtained from (9), (17), and (27), respectively. Several observations are drawn as follows: 1) the power outage probability significantly decreases with increasing density of PBs, this is because multiuser diversity gain is improved with increasing number of PBs; 2) for small M, there is a gap between BPB and NPB as λ_p approaches 10^{-1}, however, for large M, they achieve identical performance, the reason is, once again, the effect of small scale fading is averaged out with large M; and 3) CPB achieves lower power outage probability than BPB and NPB, since it transfers more power from PBs to D2D transmitter.

Fig. 3 plots the power outage probability versus density of PBs with different values of α. The solid black, red, and blue curves, representing the general case of CPB, BPB, and NPB are obtained from (11), (17), and (23), respectively. The dash black, red, and blue curves, representing the special case of CPB, BPB, and NPB are obtained from (16), (17), and (27), respectively. We see that the power outage probability decreases with decreasing α. This is because smaller path loss is achieved with decreasing α. It is observed that for small number of antennas with $M = 2$, BPB outperforms NPB.

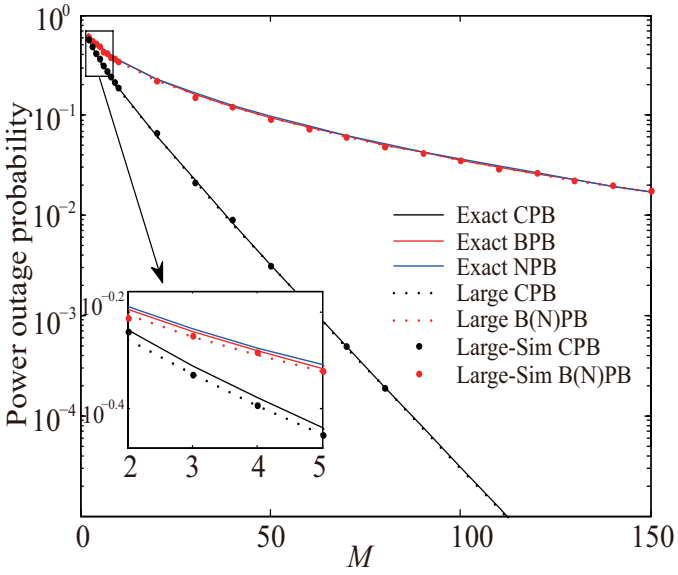


Fig. 1: Power outage probability with $P_S = 43$ dBm, $P_{\mathrm{t}} = 10$ dBm, and $\lambda_p = 10^{-1}$.

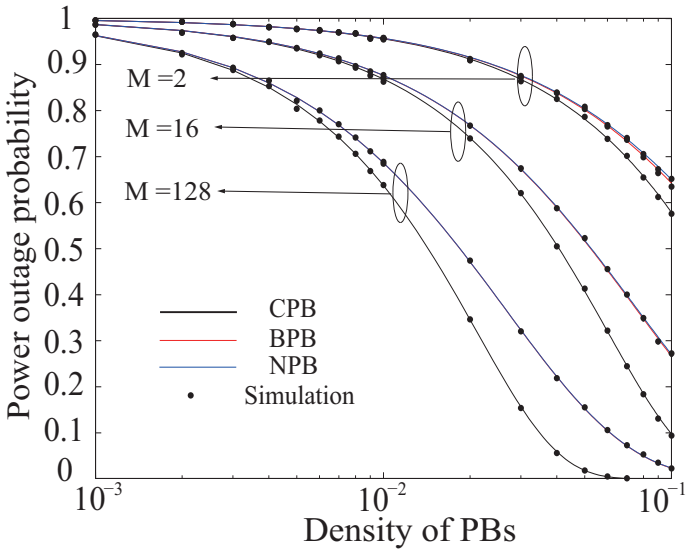


Fig. 2: Power outage probability with different M, where $P_S = 43$ dBm and $P_{\mathrm{t}} = 10$ dBm.

C. Secrecy Outage Probability

In this subsection, we set $M = 32$. In Fig. 4 and Fig. 5, the solid and dashed curves, representing the BRS and NRS schemes are obtained from (50) and (57), respectively.

Fig. 4 plots the secrecy outage probability versus density of Bobs for the BRS and the NRS schemes. We observe that the secrecy outage probability dramatically decreases as density of Bobs increases, this is because multiuser diversity gain is improved with the increasing number of Bobs. We see that the BRS scheme achieves lower secrecy outage probability than NRS scheme but demands more instantaneous feedbacks and overheads. We also see that BPB and NPB achieves identical secrecy outage probability with large M.

Fig. 5 plots the secrecy outage probability versus power threshold for the BRS and the NRS schemes. We observe

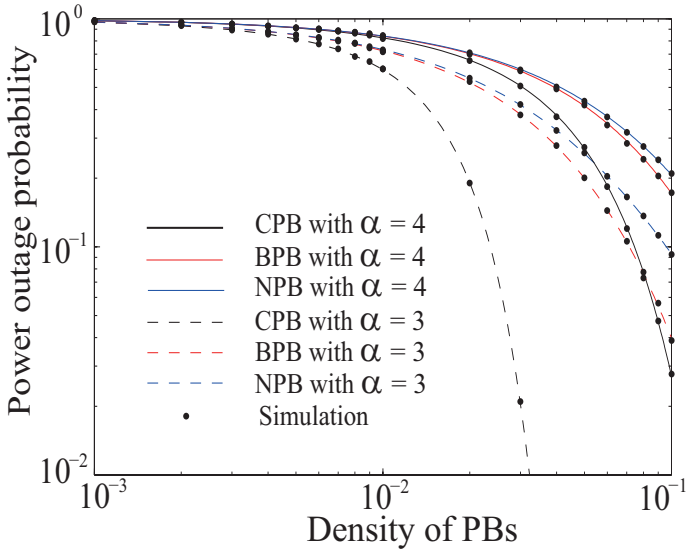


Fig. 3: Power outage probability with different α, where $M = 2$, $P_S = 50$ dBm, and $P_{\rm t} = 5$ dBm.

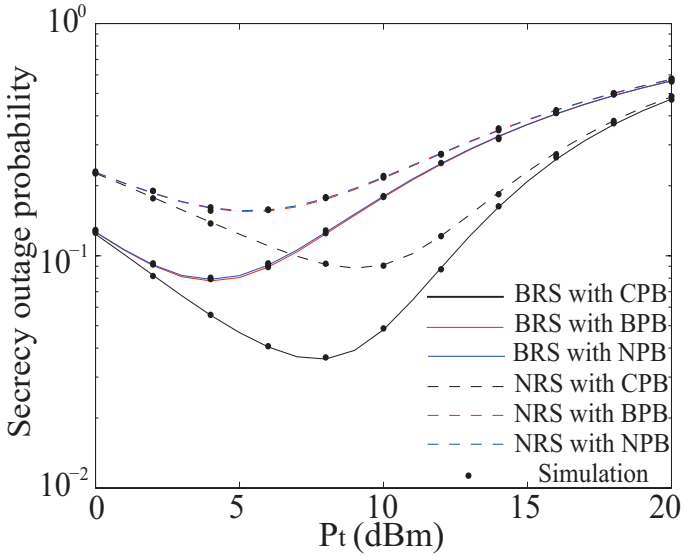


Fig. 5: Secrecy outage probability with $M = 32$, $P_S = 43$ dBm, $\beta = 0.5, \lambda_p = 10^{-1}, \lambda_b = 5 \times 10^{-2}, \lambda_e = 10^{-3}$, and $\lambda_l = 10^{-3}$.

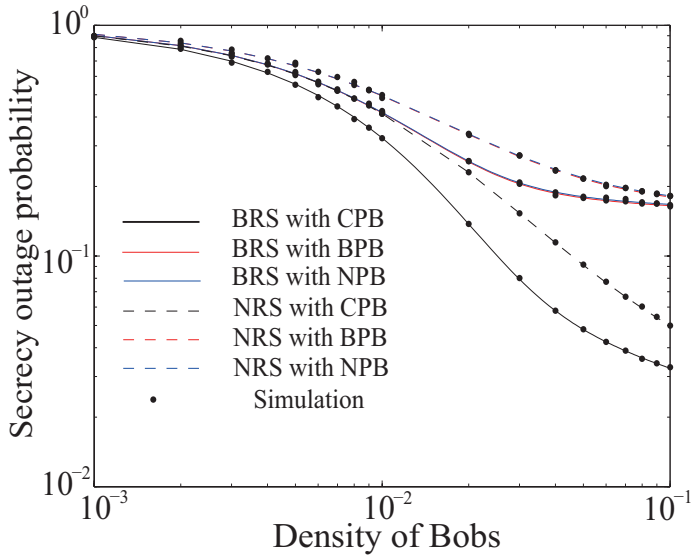


Fig. 4: Secrecy outage probability with $M = 32$, $P_S = 43$ dBm, $P_{\rm t} = 10$ dBm, $\beta = 0.5, \lambda_p = 10^{-1}, \lambda_e = 10^{-3}$, and $\lambda_l = 10^{-3}$.

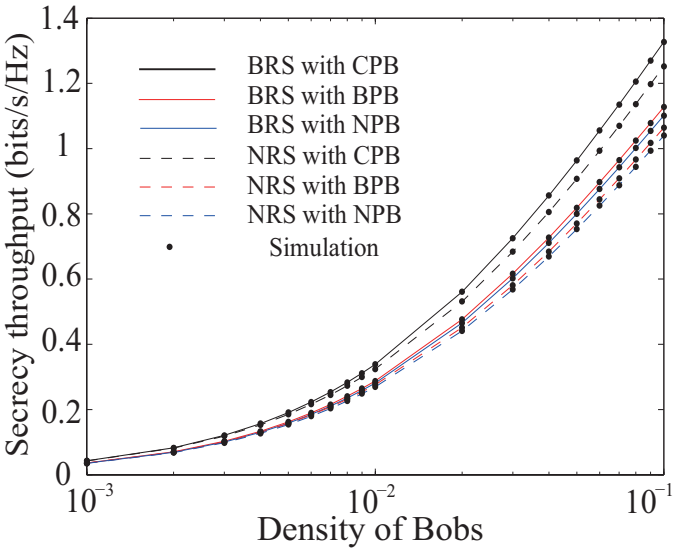


Fig. 6: Secrecy throughput with $M = 2$, $P_S = 43$ dBm, $P_{\rm t} = 10$ dBm, $\beta = 0.5, \lambda_p = 10^{-1}, \lambda_e = 10^{-2}$, and $\lambda_l = 10^{-3}$.

that as the power threshold increases, the secrecy outage probability decreases then increases. This is because the power outage probability increases with increasing power threshold. However, 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 other words, an optimal power threshold value which achieves the lowest secrecy outage probability.

D. Secrecy Throughput

In this subsection, we set $M = 2$. In Fig. 6, Fig. 7, and Fig. 8, the solid and dashed curves, representing the BRS and NRS schemes are obtained from (54) and (58), respectively.

Fig. 6 plots the secrecy throughput versus density of Bobs. 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) receiver selection with BPB achieves higher secrecy throughput than that with NPB, this is because when M is small, the small scale fading has an impact on

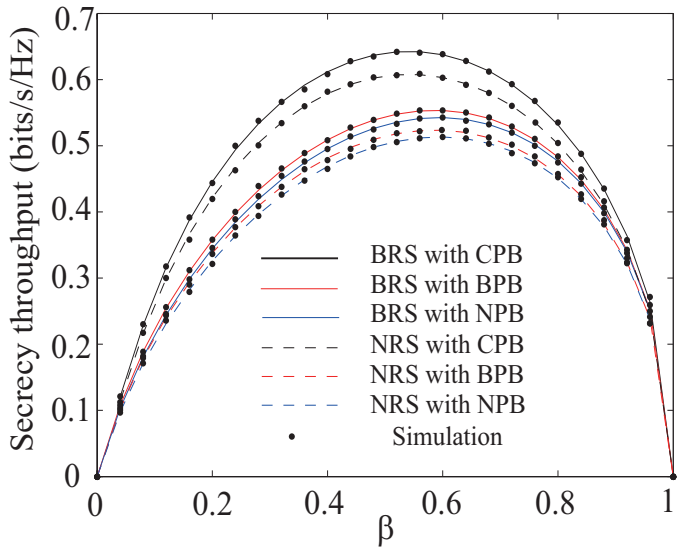


Fig. 7: Secrecy throughput with $M = 2$, $P_S = 43$ dBm, $P_{\rm t} = 10$ dBm, $\lambda_p = 10^{-1}, \lambda_b = 10^{-2}, \lambda_e = 10^{-3}$, and $\lambda_l = 10^{-3}$.

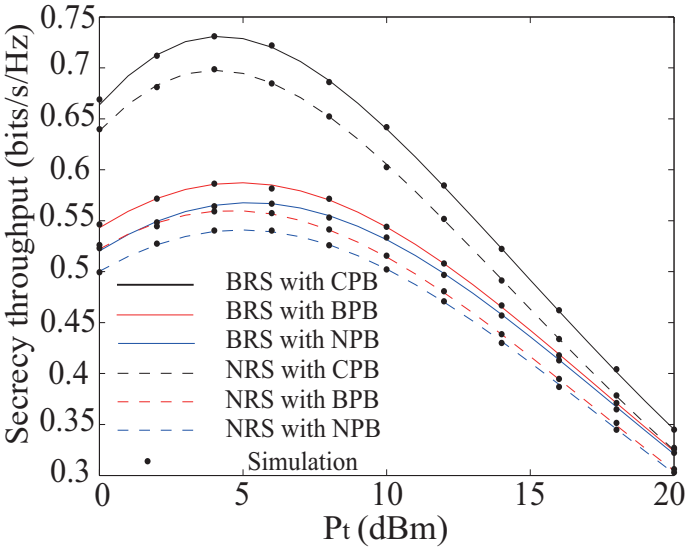
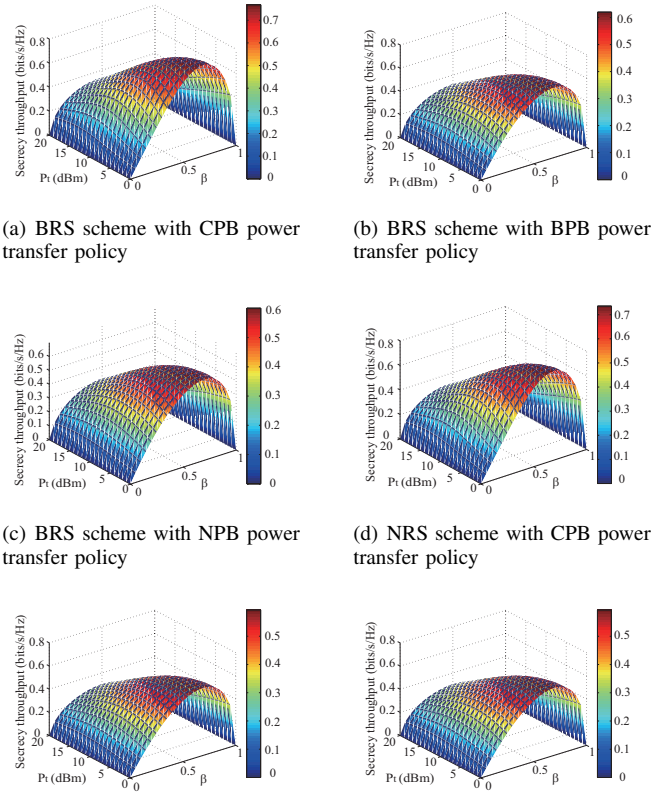


Fig. 8: Secrecy throughput with $M = 2$, $P_S = 43$ dBm, $\beta = 0.5, \lambda_p = 10^{-1}, \lambda_b = 10^{-2}, \lambda_e = 10^{-3}$, and $\lambda_l = 10^{-3}$.

the power outage probability, which results in influencing the secrecy throughput.

Fig. 7 plots the secrecy throughput versus information transmission fraction time β. We observe that there is a maximum value for each case. This behavior is explained as follows: as β increases, the time for power transfer decreases and hence, Alice receives less power, but the time for information transmission increases. As such, there exits an optimal value which provides a good tradeoff between power transfer and information transmission. We also see that as β approaches the optimal value, CPB achieves higher secrecy throughput than BPB and NPB.

Fig. 8 plots the secrecy throughput versus power threshold



(a) BRS scheme with CPB power transfer policy

(b) BRS scheme with BPB power transfer policy

(c) BRS scheme with NPB power transfer policy

(d) NRS scheme with CPB power transfer policy

(e) NRS scheme with BPB power transfer policy

(f) NRS scheme with NPB power transfer policy

Fig. 9: Secrecy throughput with $M = 2$, $P_S = 43$ dBm, $\lambda_p = 10^{-1}, \lambda_b = 10^{-2}, \lambda_e = 10^{-3}$, and $\lambda_l = 10^{-3}$.

$P_{\rm t}$. We observe that as the power threshold increases, the secrecy throughput increases then decreases. This behavior is explained as follows: 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.

Fig. 9 shows the secrecy throughput versus $P_{\rm t}$ and β for BRS and NRS with three power transfer policies. We see that β and $P_{\rm t}$ have joint effects on the secrecy throughput. By jointly considering these two factors, we observe that there exits an optimal value for each receiver selection and power transfer combination. We see that CPB achieves higher optimal value of secrecy throughput than BPB and NPB. We also see BRS achieves higher optimal value of secrecy throughput than NRS.

VI. Conclusions

In this paper, secure device-to-device transmission in cognitive cellular networks with an energy constrained transmitter harvesting energy with wireless power transfer was considered. Based on the recently widely adopted time switching receiver and the concept of power beacons, we proposed three wireless

power transfer policies in the power transfer model, namely, cooperative power beacons power transfer, best power beacon power transfer, and nearest power beacon power transfer. We also considered best receiver selection case and suboptimal selection case in the information signal model. We used stochastic geometry 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, secrecy 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. Our future work will be focus on optimizing the network design parameters (e.g., information transmission time fraction and the expected transmit power).

APPENDIX A: PROOF OF THEOREM 4

We compute the CDF of ζ as follows:

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

Following the similar procedure getting (17), 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 (39).

APPENDIX B: PROOF OF THEOREM 5

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 (40).

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

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

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 (41).

REFERENCES

[1] J. Lin, "Wireless power transfer for mobile applications, and health effects [telecommunications health and safety]," *IEEE Trans. Antennas Propag*, vol. 55, no. 2, pp. 250–253, April 2013.

[2] 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.

[3] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: wireless communication out of thin air," in *Proc. ACM SIGCOMM*, 2013, pp. 39–50.

[4] L. Varshney, "Transporting information and energy simultaneously," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2008, pp. 1612–1616.

[5] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2012, pp. 3982–3987.

[6] 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.

[7] 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.

[8] 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.

[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] 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.

[13] S. Lee, R. Zhang, and K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 09, pp. 4788–4799, 2013.

[14] 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.

[15] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, June 2014.

[16] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, June 2013.

[17] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan 2015.

[18] 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.

[19] 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.

[20] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, 2013.

[21] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surv. Tut*.

[22] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 418–428, 2014.

[23] S. A. R. Zaidi, M. Ghogho, D. C. McLernon, and A. Swami, "Achievable spatial throughput in multi-antenna cognitive underlay networks with multi-hop relaying." *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1543–1558, 2013.

[24] 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.

[25] T. Q. Duong, P. L. Yeoh, V. N. Q. Bao, M. Elkashlan, and N. Yang, "Cognitive relay networks with multiple primary transceivers under spectrum-sharing," *IEEE Signal Process. Lett.*, vol. 19, no. 11, pp. 741–744, 2012.

[26] L. Xiao, P. Wang, D. Niyato, D. Kim, and Z. Han, "Wireless networks with rf energy harvesting: A contemporary survey," *IEEE Commun. Surv. Tut*, 2014.

[27] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, 2009.

[28] K. J. Hollenbeck, Invlap.m: A Matlab Function for Numerical Inversion of Laplace Transforms by the de Hoog Algorithm 1998. [Online]. Available: http://www.mathworks.com/matlabcentral/fileexchange/32824-numerical-inversion-of-Laplace-transforms-in-matlab/content/INVLAP.m.

[29] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, 2014.

[30] J. G. Wendel, "The non-absolute convergence of Gil-Pelaez' inversion integral," *The Annals of Mathematical Statistics*, vol. 32, no. 1, pp. 338–339, Mar. 1961.

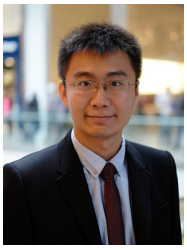
[31] E. S. Sousa and J. A. Silvester, "Optimum transmission ranges in a direct-sequence spread-spectrum multihop packet radio network," *IEEE J. Sel. Areas Commun.*, vol. 8, no. 5, pp. 762–771, Jun. 1990.

[32] J. Venkataraman, M. Haenggi, and O. Collins, "Shot noise models for outage and throughput analyses in wireless ad hoc networks," in *IEEE Military Commun. Conf. (MILCOM)*, 2006, pp. 1–7.

[33] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*. Courier Corporation, 1964, no. 55.

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

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



Yuanwei Liu (S'13) is currently working toward the Ph.D. degree in Electronic Engineering at Queen Mary University of London. Before that, he received his M.S. degree and B.S. degree from the Beijing University of Posts and Telecommunications in 2014 and 2011, respectively.

His research interests include wireless energy harvesting, non-orthogonal multiple access, cognitive radio, physical layer security, multiple-antenna systems and cooperative networks.



Lifeng Wang is the research associate in the Department of Electronic and Electrical Engineering, University College London (UCL). He received Ph.D. degree in Electronic Engineering at Queen Mary University of London in 2015. He received the Exemplary Reviewer Certificate of the IEEE Communications Letters in 2013.

His research areas include millimeter-wave communications, Massive MIMO, HetNets, cognitive radio, physical layer security and wireless energy harvesting.



Syed Ali Raza Zaidi (M13) is currently with University of Leeds. He received his B.Eng degree in information and communication system engineering from the School of Electronics and Electrical Engineering, NUST, Pakistan in 2008. He was awarded the NUST's most prestigious Rector's gold medal for his final year project. From September 2007 till August 2008, he served as a Research Assistant in Wireless Sensor Network Lab on a collaborative research project between NUST, Pakistan and Ajou University, South Korea. In 2008, he was awarded overseas research student scholarship along with Tetley Lupton and Excellence Scholarships to pursue his PhD at the School of Electronics and Electrical Engineering, University of Leeds, U.K. He was also awarded with COST IC0902, DAAD and Royal Academy of Engineering grants to promote his research. Dr. Zaidi was a visiting research scientist at Qatar Innovations and Mobility Centre from October to December 2013. He has served as an invited reviewer for IEEE flagship journals and conferences. His research is focused towards design and analysis of the large scale ad-hoc wireless networks by employing tools from stochastic geometry and random graph theory. Dr. Zaidi is also UK Liasion for the European Association for Signal Processing (EURASIP). He has served on the program committees and as a chair in various IEEE flagship conferences. He is the technical program chair for EAI STEMCOM 2016 and workshop chair for the IEEE CAMAD 2015 special session on "Performance Analysis and Modelling of Large-scale 5G networks", IEEE WCMC 2015 workshop on 'Recent Advances at Physical Layer for 5G Wireless Networks' and IEEE VTC workshop on 'Emerging device centric communication'. He has also served as a track chair for 'Theory and modeling track' at IEEE/ICST CROWNCOM 2015. Dr. Zaidi is also a Lead Guest Editor for IET Signal Processing SI on Recent Advances in Signal Processing for 5G Wireless Networks and associate editor for IEEE Communication Letters.



Maged Elkashlan (M'06) received the Ph.D. degree in Electrical Engineering from the University of British Columbia, Canada, 2006. From 2006 to 2007, he was with the Laboratory for Advanced Networking at University of British Columbia. From 2007 to 2011, he was with the Wireless and Networking Technologies Laboratory at Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia. During this time, he held an adjunct appointment at University of Technology Sydney, Australia. In 2011, he joined the School of Electronic Engineering and Computer Science at Queen Mary University of London, UK, as an Assistant Professor. He also holds visiting faculty appointments at the University of New South Wales, Australia, and Beijing University of Posts and Telecommunications, China. His research interests fall into the broad areas of communication theory, wireless communications, and statistical signal processing for distributed data processing and heterogeneous networks.

Dr. Elkashlan currently serves as an Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and IEEE COMMUNICATIONS LETTERS. He also serves as Lead Guest Editor for the special issue on "Green Media: The Future of Wireless Multimedia Networks" of the IEEE WIRELESS COMMUNICATIONS MAGAZINE, Lead Guest Editor for the special issue on "Millimeter Wave Communications for 5G" of the IEEE COMMUNICATIONS MAGAZINE, Guest Editor for the special issue on "Energy Harvesting Communications" of the IEEE COMMUNICATIONS MAGAZINE, and Guest Editor for the special issue on "Location Awareness for Radios and Networks" of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He received the Best Paper Award at the IEEE International Conference on Communications (ICC) in 2014, the International Conference on Communications and Networking in China (CHINACOM) in 2014, and the IEEE Vehicular Technology Conference (VTC-Spring) in 2013. He received the Exemplary Reviewer Certificate of the IEEE Communications Letters in 2012.



Trung Q. Duong (S'05, M'12, SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen's University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include cooperative communications, cognitive radio networks, physical layer security, massive MIMO, cross-layer design, mm-waves communications, and localization for radios and networks. He is the author or co-author of 170 technical papers published in scientific journals and presented at international conferences.

Dr. Duong currently serves as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, IET COMMUNICATIONS, WILEY TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES, and ELECTRONICS LETTERS. He has also served as the Guest Editor of the special issue on some major journals including IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, IET COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS MAGAZINE, IEEE COMMUNICATIONS MAGAZINE, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, EURASIP JOURNAL ON ADVANCES SIGNAL PROCESSING. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014.