Chapter 1

Coverage and Secrecy Analysis of RF-powered Internet-of-Things

Mustafa A. Kishk¹
Mohamed A. Abd-Elmagid and Harpreet S. Dhillon²

The Internet-of-Things (IoT) is an emerging *digital fabric* that will integrate our physical world into computer networks by connecting billions of things, such as small sensors, wearables, vehicles, and actuators, to the Internet. Owing to its massive scale, it is considered highly inefficient and even impractical to replace or recharge batteries of IoT devices, especially the ones that are deployed at hard-to-reach places, such as under the ground or in tunnels. This has naturally led to the consideration of energy harvesting to circumvent or supplement conventional power sources, such as replaceable batteries, in these devices. Due to its ubiquity and cost efficient implementation, radio frequency (RF)-energy harvesting has quickly emerged as an appealing solution for powering IoT devices (majority of which are tiny devices, such as sensors, with very low energy requirement).

The objective of this chapter is to provide a comprehensive performance analysis of RF-powered IoT using tools from stochastic geometry. In order to capture the cyber-physical nature of IoT, our emphasis is on the metrics that jointly characterize the wireless, energy harvesting, and secrecy aspects. In the first part of the chapter, we characterize the joint probability of receiving strong enough signal and harvesting sufficient energy to operate the link. We term this the *joint coverage probability*. In this analysis, we assume that the locations of the sources of RF signals and the locations of the IoT devices are modeled using two independent Poisson point processes (PPPs). For this setup, we derive insightful mathematical expressions for key performance metrics, which collectively provide insights into the effect of the different system parameters on the overall system performance and how these parameters can be tuned to achieve the performance of a regular battery-powered system. In the second part of this chapter, we also incorporate the secrecy aspect in our analysis. In particular, we study the secrecy of RF signals when the RF-powered IoT devices

¹M. A. Kishk is with King Abdullah University of Science and Technology, Saudi Arabia. Email: mustafa.kishk@kaust.edu.sa. This work was done when M. A. Kishk was with Wireless@VT, Department of ECE, Virginia Tech.

²M. A. Abd-Elmagid and H. S. Dhillon are with Wireless@VT, Department of ECE, Virginia Tech, Blacksburg, VA. Email: {maelaziz, hddhillon}@vt.edu. The support of the U.S. NSF (Grants CPS-1739642 and CNS-1814477) is gratefully acknowledged.

are placed close to the sources of RF signals. Rigorous mathematical expressions are derived for various performance metrics, which provide several useful system design insights.

1.1 Introduction

Owing to its ability to transform current towns and cities into smart and connected communities of tomorrow, IoT is widely regarded as one of the next frontiers in information and communications technology. The grand vision for an IoT network is to tightly integrate the cyber and physical worlds by connecting billions of things, such as small sensors, wearables, vehicles, and actuators, to the Internet. This will naturally enable numerous applications across many industrial verticals, such as home automation, intelligent transportation systems, public safety, agriculture, and medicine. A key hindrance in making this vision a reality is the energy-constrained nature of a majority of IoT devices [1]. It is well-known that most of these devices will have to be battery-powered and replacing or recharging these batteries may not be a viable option for many of them. In order to overcome this issue, energy harvesting solutions have been proposed to supplement or even circumvent the use of replaceable batteries in the IoT devices. Due to its ubiquity and cost efficient implementation, ambient RF-energy harvesting has recently been considered as an appealing solution for powering IoT devices.

Ambient RF-energy harvesting IoT devices (sometimes referred to as wirelessly-powered IoT devices) can, in principle, have a *dedicated charging network*, which is deployed specifically for charging IoT devices through broadcasting RF-energy signals. For instance, one can envision a network of *power beacons* (PBs) deployed solely to charge the IoT devices. However, a far more realistic and cost-efficient alternative for the IoT devices is to simply rely on the existing communication infrastructure, such as WiFi access points (APs) or cellular base stations (BSs), for both charging and communication. Given its dual purpose, this network needs to be carefully designed in order to (i) deliver the amount of RF-energy required at each IoT device and (ii) maintain reliable communication links between the APs or the BSs and the IoT devices. Since the same set of BSs (or APs) are used for both charging and communication, the amount of harvested energy and the communication signal quality (signal-to-interference-plus-noise ratio or SINR) are highly correlated. This, in turn, complicates the performance analysis of such system setup. In the first part of this chapter, we use tools from stochastic geometry to rigorously analyze the performance of this setup. In particular, we derive the joint energy and SINR coverage probability and use the derived expressions to provide several system-level insights.

In the second part of this chapter, we focus on secrecy in addition to the energy harvesting and wireless performance. Specifically, we focus on a scenario in which an RF-powered IoT network coexists with a primary network that is also the sole source of RF-energy for the IoT network. We further assume that the coexisting primary network is using the guard zone technique [2, 3] to preserve the privacy of its transmitted signals. In such scenarios, RF-energy harvesting can be challenging since the IoT devices do not belong to the primary network and may hence be

considered as potential eavesdroppers by the primary network. We use tools from stochastic geometry to analyze the performance of the two coexisting networks. In particular, we study the secrecy performance of the primary network and the energy harvesting performance of the IoT devices. Furthermore, we investigate how the performance of the two networks is affected by the key system parameters, such as guard zone radius and the deployment density of the IoT devices, which allows us to obtain useful insights on the coexistence of the two networks.

1.1.1 Literature Review

As noted above already, this chapter considers two aspects of the performance of RF-powered IoT devices: (i) energy and SINR coverage of IoT devices and (ii) secrecy of RF signals used for energy harvesting. We use tools from stochastic geometry to study each of these aspects. The existing literature on the use stochastic geometry for the analysis of energy harvesting wireless networks has focused mainly on the coverage aspect. On the other hand, the works that discussed the secrecy problem have focused mainly on simpler setups composed of a single point-to-point link or a fixed set of nodes, unlike the work in this chapter that considers large-scale networks. Therefore, the literature review will focus on two main research directions: (i) stochastic geometry-based analysis of energy harvesting wireless networks with emphasis on coverage analysis, and (ii) secrecy analysis of RF-signals used to charge RF-powered wireless networks.

Stochastic geometry has emerged as a promising mathematical tool for the system-level performance analysis of wireless networks [4–7]. Not surprisingly, there have also been a lot of recent works that use stochastic geometry to study the performance of large-scale energy harvesting wireless networks [8–12]. This literature has focused mainly on the analysis of a setup where a wireless device harvests energy and then uses it to transmit information to a receiver. The main performance metric of interest in these papers is the joint probability of energy and SINR coverage, which is the joint probability of (i) harvesting sufficient energy to be able to transmit the information signal to the receiver, and (ii) successfully decoding the information signal transmitted by the energy harvesting device. These two events are independent when the locations of RF-energy sources are independent from the locations of the information receivers. For instance, in [8], authors considered a system where a sensor harvests RF-energy from the ambient signals emitted by TV and radio stations, as well as cellular networks. The sensor harvests the RF-energy and then uses it to communicate with a data sink. The authors modeled the locations of the sources of RF-energy using Ginibre α -determinantal point process (DPP). The main advantage of this point process over a PPP is its capability to capture repulsion among the locations of TV, radio stations as well as cellular BSs. Given the technical challenges in deriving exact expressions for DPP, authors derived useful bounds for the energy coverage probability and the average harvested energy by considering a worst case scenario that focuses on the energy harvested from the nearest RF source only. The concept of having a dedicated charging network with the sole purpose of providing RF-energy was proposed in [9] for a simple point-to-point setup. In this setup, the

charging network is represented by a set of PBs. This setup was then extended to a large scale network in [10].

When the IoT device harvests RF-energy from a given network and then uses it to transmit information to the same network, the energy and SINR coverage events become correlated. This is due to implicit correlation between the locations of successfully powered nodes (interferers during information transmission) and the locations of the RF sources. However, capturing this correlation is highly challenging, and hence, is typically ignored in the literature to maintain tractability [11, 12]. For instance, authors in [11] considered a k -tier cellular network where the users harvest RF-energy from the signals emitted by the cellular BSs and then use this energy to communicate with the nearest BS in the uplink channel. The authors assumed the existence of a limited-capacity battery at each user, and derived the energy coverage probability as well as uplink SINR coverage probability by modeling the battery level at each user as a Markov Chain followed by using tools from stochastic geometry.

Another set of relevant works in the first direction considered the scenario where the energy harvesting device uses the harvested energy to activate its processing units and enable information reception [13–22]. This is particularly important in wireless devices with limited power resources, such as the IoT devices. In such devices, the energy consumption during information reception should not be neglected [23–25]. Authors in [13] considered a power-splitting architecture for the RF-energy harvesting devices. This architecture splits the received signal into two portions. One portion is used to charge the device, and the other portion is decoded as an information-carrying signal. This work considered a large scale network of energy harvesting devices, where the distance between each device and its information transmitter was assumed to be fixed. The objective of this system is to maintain the average amount of harvested energy above a predefined threshold while maximizing the SINR coverage probability. For this setup, the SINR and the amount of harvested energy are analyzed separately. The joint analysis of the amount of harvested energy and the SINR at the energy harvesting device is much more challenging due to the high correlation between the two random variables. This correlation is induced by the fact that the same transmitters are used for information reception and energy harvesting. Hence, the amount of harvested energy and the SINR are both functions of the same point process. This problem has not received as much attention in the literature [26, 27]. For instance, authors in [26] derived an upper bound on the joint energy and SINR coverage probability in order to provide tractable expressions which enable drawing system-level insights. In [16, 18, 20, 21], the authors of this chapter proposed a simple approximation that assisted in deriving this joint probability and provided several useful system-level insights. The first part of this chapter will be based on these recent developments.

In the second part of this chapter, we use tools from stochastic geometry to study the scenario where the IoT devices harvest energy from the RF signals transmitted by a coexisting wireless network. This coexisting network is assumed to adopt a secrecy-enhancing technique to maintain the confidentiality of its transmitted messages. It is instructive to note that, until recently, this problem was only studied in the literature for the point-to-point setup or a setup with a fixed number of transmitters,

RF-powered devices, and legitimate receivers [28–32]. The general theme in these works is the implicit assumption that the transmitter aims to ensure secrecy while providing RF-energy for the RF-powered device. For instance, authors in [28, 29] studied a system of one transmitter-receiver pair with the coexistence of one RF-powered device. In order to satisfy both secrecy and RF-energy delivery needs, the transmitter uses artificial noise to maintain the amount of RF-energy while reducing the probability of decoding the information signal by the RF-energy receiver. Authors in [30] proposed to use a jammer to increase the amount of RF-energy while degrading the information signal quality at the RF-powered device. Authors in [31] considered a setup of a single transmitter-receiver pair with K coexisting RF-powered devices. A more general setup with K transmitters, N receivers, and M RF-powered devices, was considered in [32]. One of the few works that considered secrecy in large-scale networks with RF-powered devices using stochastic geometry is [33]. This work studied a system setup in which the legitimate transmitters are RF-powered, which is different from the setup considered in this chapter. In [17, 19], the authors of this chapter have recently extended the point-to-point setup to a more general system of two coexisting large-scale networks: (i) the IoT network and (ii) the secrecy-enhancing network. These recent works will form the basis of the second part of this chapter.

1.2 RF-energy Harvesting from a Coexisting Cellular Network

1.2.1 System Setup

We consider a system of RF-powered IoT devices and a charging network (cellular network) that dedicates a subset of its resources to serve the IoT devices. The locations of the IoT devices and the cellular BSs are modeled by two independent homogeneous PPPs $\Phi_E \equiv \{x_i\} \subset \mathbb{R}^2$ with density λ_E and $\Phi_R \equiv \{y_i\} \subset \mathbb{R}^2$ with density λ_R , respectively. Hence, without loss of generality, we focus our analysis on a typical IoT device located at the origin due to the stationarity of PPP. To enable simultaneous charging and communication, we consider a time-switching architecture for the IoT device. In particular, each time-slot is divided into two sub-slots: (i) charging sub-slot with duration $\tau_c T$ and (ii) downlink sub-slot with duration $\tau_d T$, where T is the total duration of each time-slot and $\tau_c + \tau_d = 1$. In the charging sub-slot, all the BSs emit RF signals with the purpose of charging the IoT devices. In the downlink sub-slot, each IoT device associates with its nearest BS and receives information-carrying signals from this BS. We assume that fading gains among all sets of BS-IoT device links are independent and exponentially distributed with mean 1. In addition, we assume that for a given link, the fading gains in the charging and downlink sub-slots are independent.

In the charging sub-slot, the amount of power received by the typical device from a BS located at $y \in \Phi_R$ is $\rho g_y \|y\|^{-\alpha}$, where ρ is the transmission power of the BS, $g_y \sim \exp(1)$ is the fading gain in the charging sub-slot, and α is the path-loss exponent. Hence, given that the duration of the charging sub-slot is $\tau_c T$ and that all the BSs are active during the charging sub-slot, the total energy harvested by the

typical IoT device in the charging sub-slot is

$$E_H = \eta \tau_c T \sum_{y \in \Phi_R} \rho_{g_y} \|y\|^{-\alpha}, \quad (1.1)$$

where η is the RF-DC conversion efficiency. We assume that any leftover energy from the previous slots is no longer available for use in the current time slot.

During the downlink sub-slot, the value of the SINR at the typical IoT device is

$$\text{SINR} = \frac{\rho_{h_{y_1}} \|y_1\|^{-\alpha}}{\sum_{y \in \Phi_R \setminus y_1} \rho_{h_y} \|y\|^{-\alpha} + \sigma^2}, \quad (1.2)$$

where σ^2 is the noise power, y_1 is the location of the nearest BS to the typical IoT device, and $h_y \sim \exp(1)$ is the fading gain in the downlink sub-slot.

1.2.2 Performance Metrics

For the system setup described above, our design goal is to ensure that the IoT devices are harvesting sufficient energy and the downlink SINR is above a pre-defined threshold. However, due to the correlation arising from relying on the same set of BSs for both charging and communication, the analysis of IoT charging cannot be separated from that of downlink communication. Hence, we focus on deriving the joint energy and SINR coverage probability, which is defined next.

Definition 1 (Joint coverage probability): *For a given time-slot, the IoT device needs to satisfy two conditions: (i) $E_H \geq \mathcal{E}$ and (ii) $\text{SINR} \geq \beta$, where $\mathcal{E}$ is the minimum threshold on E_H to ensure acceptable energy harvesting performance and β is the minimum threshold on SINR required for successful decoding. The probability of satisfying both conditions is defined as the joint energy and SINR coverage probability, which can be mathematically represented as follows*

$$P_{\text{joint}} = \mathbb{P}(E_H \geq \mathcal{E}, \text{SINR} \geq \beta). \quad (1.3)$$

Another metric that is typically studied in the literature of RF-powered wireless networks is the energy coverage probability, which is defined as

$$P_{\text{energy}} = \mathbb{P}(E_H \geq \mathcal{E}). \quad (1.4)$$

Obviously, the energy coverage probability is a special case of the joint coverage probability, i.e., the joint coverage probability reduces to the energy coverage probability when $\beta = 0$.

Another important metric to quantify the performance of this setup is the average throughput. We assume that when the IoT device fails to harvest the minimum required amount of energy $\mathcal{E}$, it cannot communicate in the downlink sub-slot. Given that the link is only used for communication for a τ_d fraction of time, it is important to study how the parameters τ_c and τ_d should be selected in a way that ensures energy coverage while maximizing the downlink average throughput.

Definition 2 (Average throughput): The average downlink throughput in bits/sec/Hz is

$$\begin{aligned} D_{\text{avg}} &= \tau_d \mathbb{E} \left[\log_2(1 + \beta) \mathbb{1}(\text{SINR} \geq \beta) \mathbb{1}(E_H \geq \mathcal{E}) \right] \\ &= \tau_d \log_2(1 + \beta) P_{\text{joint}}, \end{aligned} \quad (1.5)$$

where $\mathbb{1}(\Xi) = 1$ if the event Ξ happens and $\mathbb{1}(\Xi) = 0$ otherwise.

1.2.3 Analysis and Main Results

We aim to derive the joint coverage probability described in Definition 1, which is the joint probability of the two events: (i) $E_H \geq \mathcal{E}$ and (ii) $\text{SINR} \geq \beta$. Recalling (1.1) and (1.2), we can observe that both E_H and SINR depend on Φ_R , which leads to high correlation between the two random variables. In particular, Φ_R models the locations of the sources of RF-energy signals in E_H as well as the locations of the interferers in SINR . Building on that observation, we can treat E_H and SINR as two independent random variables when we condition our analysis on Φ_R . Hence, we can rewrite (1.3) as follows

$$P_{\text{joint}} = \mathbb{E}_{\Phi_R} [\mathbb{P}(E_H \geq \mathcal{E} | \Phi_R) \mathbb{P}(\text{SINR} \geq \beta | \Phi_R)]. \quad (1.6)$$

Based on the above expression, we first need to derive each of the energy and SINR coverage probabilities conditioned on the point process Φ_R . Next, we need to take the expectation of their product over Φ_R . Before proceeding with this approach, we propose an efficient approximation that has been shown to be remarkably accurate in the literature [34–39]. This approximation is provided below

$$\sum_{y \in \Phi_R} g_y \|y\|^{-\alpha} = g_{y_1} \|y_1\|^{-\alpha} + g_{y_2} \|y_2\|^{-\alpha} + \mathcal{M}(y_1, y_2), \quad (1.7)$$

where y_1 and y_2 are the locations of the two nearest BSs to the typical IoT device, respectively, and $\mathcal{M}(y_1, y_2) = \mathbb{E} [\sum_{y \in \Phi_R \setminus \{y_1, y_2\}} g_y \|y\|^{-\alpha} | y_1, y_2]$. In (1.7), we simply approximate the summation of received RF signal powers by the summation of RF signal powers received from the nearest two BSs and the expectation of the summation of RF signal powers received from the rest of the BSs conditioned on the location of the nearest two BSs. This is motivated by the power-law path-loss because of which the RF signals received from the nearby BSs dominate the total received power. Using this approach, we can approximate the value of E_H in (1.1). This leads to the following approximate expression

$$E_H = \eta \tau_c T \rho (g_{y_1} \|y_1\|^{-\alpha} + g_{y_2} \|y_2\|^{-\alpha} + \mathcal{M}(y_1, y_2)). \quad (1.8)$$

Using similar approach, we can approximate the value interference term in the denominator of the SINR expression in (1.2). This leads to the following approximate expression

$$\text{SINR} = \frac{\rho h_{y_1} \|y_1\|^{-\alpha}}{\rho (h_{y_2} \|y_2\|^{-\alpha} + \mathcal{M}(y_1, y_2)) + \sigma^2}. \quad (1.9)$$

As will be evident shortly, this lends tractability to the analysis of the joint distribution in (1.3). In particular, this approximation reduces (1.6) to

$$P_{\text{joint}} = \mathbb{E}_{y_1, y_2} [\mathbb{P}(E_H \geq \mathcal{E} | y_1, y_2) \mathbb{P}(\text{SINR} \geq \beta | y_1, y_2)]. \quad (1.10)$$

In the following lemma, we derive the first term inside the expectation in (1.10), namely $\mathbb{P}(E_H \geq \mathcal{E} | y_1, y_2)$.

Lemma 1 (Conditional Energy Coverage Probability): *Probability that the harvested energy during the charging sub-slot is greater than $\mathcal{E}$ conditioned on y_1, y_2 is*

$$\mathbb{P}(E_H \geq \mathcal{E} | y_1, y_2) = \frac{r_2^\alpha \exp(-r_1^\alpha [\mathcal{F}(r_2)]^+)}{r_2^\alpha - r_1^\alpha} - \frac{r_1^\alpha \exp(-r_2^\alpha [\mathcal{F}(r_2)]^+)}{r_2^\alpha - r_1^\alpha}, \quad (1.11)$$

while the unconditioned probability is

$$\begin{aligned} \mathbb{P}(E_H \geq \mathcal{E}) &= 1 - \pi \lambda_R \mathcal{A}^2 \exp(-\pi \lambda_R \mathcal{A}^2) - \exp(-\pi \lambda_R \mathcal{A}^2) + \int_{\mathcal{A}}^{\infty} \int_0^{r_2} \left(\frac{r_2^\alpha \exp(-r_1^\alpha \mathcal{F}(r_2))}{r_2^\alpha - r_1^\alpha} \right. \\ &\quad \left. - \frac{r_1^\alpha \exp(-r_2^\alpha \mathcal{F}(r_2))}{r_2^\alpha - r_1^\alpha} \right) \times f_{R_1, R_2}(r_1, r_2) dr_1 dr_2, \end{aligned} \quad (1.12)$$

where $\mathcal{A} = \left(\frac{2\pi\lambda_R}{(\alpha-2)C(\tau_c)} \right)^{\frac{1}{\alpha-2}}$, $r_1 = \|y_1\|$, $r_2 = \|y_2\|$, $\mathcal{F}(r_2) = \left[C(\tau_c) - \frac{2\pi\lambda_R}{\alpha-2} r_2^{2-\alpha} \right]$, $C(\tau_c) = \frac{\mathcal{E}}{\tau_c T \eta \rho}$, $[x]^+ = \max\{0, x\}$, and $f_{R_1, R_2}(r_1, r_2) = (2\pi\lambda_R)^2 r_1 r_2 e^{-\lambda_R \pi r_2^2}$.

Proof. The value of $\mathcal{M}(y_1, y_2)$ can be derived as follows:

$$\begin{aligned} \mathcal{M}(y_1, y_2) &= \mathbb{E} \left[\sum_{y \in \Phi_R \setminus y_1, y_2} g_y \|y\|^{-\alpha} | y_1, y_2 \right] \stackrel{(a)}{=} \mathbb{E} \left[\sum_{y \in \Phi_R \setminus y_1, y_2} \|y\|^{-\alpha} \right] \stackrel{(b)}{=} 2\pi\lambda_R \int_{r_2}^{\infty} \frac{1}{r^\alpha} r dr \\ &= \frac{2\pi\lambda_R}{\alpha-2} (r_2^{2-\alpha}), \end{aligned} \quad (1.13)$$

where (a) follows from the assumption that all $\{g_y\}$ are independent and exponentially distributed random variables with mean one, and (b) follows from Campbell's theorem [40] with conversion from Cartesian to polar coordinates and using $r_2 = \|y_2\|$. Using the approximation introduced in (1.7), the conditional energy coverage probability can be expressed as:

$$\begin{aligned} \mathbb{P}(E_H \geq \mathcal{E} | y_1, y_2) &= \mathbb{P} \left(\tau_c T \eta \rho \left(g_{y_1} r_1^{-\alpha} + g_{y_2} r_2^{-\alpha} + \frac{2\pi\lambda_R}{\alpha-2} r_2^{2-\alpha} \right) \geq \mathcal{E} \right) \\ &= \mathbb{P} \left(g_{y_1} r_1^{-\alpha} + g_{y_2} r_2^{-\alpha} \geq C(\tau_c) - \frac{2\pi\lambda_R}{\alpha-2} r_2^{2-\alpha} \right) \end{aligned}$$

$$\begin{aligned}
&= \mathbb{P}(g_{y_1} r_1^{-\alpha} + g_{y_2} r_2^{-\alpha} \geq \mathcal{F}(r_2)) \\
&\stackrel{(c)}{=} \frac{r_2^\alpha \exp(-r_1^\alpha [\mathcal{F}(r_2)]^+) - r_1^\alpha \exp(-r_2^\alpha [\mathcal{F}(r_2)]^+)}{r_2^\alpha - r_1^\alpha}, \quad (1.14)
\end{aligned}$$

where step (c) is due to hypo-exponential distribution of $g_{y_1} r_1^{-\alpha} + g_{y_2} r_2^{-\alpha}$ (sum of two exponential random variables with rates r_1^α and r_2^α), $C(\tau_c) = \frac{\mathcal{E}}{\tau_c T \eta \rho}$, and $[x]^+ = \max\{0, x\}$. This concludes the proof of (1.11). Given that $\mathbb{P}(E_H \geq \mathcal{E} | y_1, y_2) = 1$ when $\mathcal{F}(r_2) \leq 0$, we define two sets: $\mathcal{N}_{r_2} = \{r_1 : \mathcal{F}(r_2) \leq 0, r_1 < r_2\}$, and $\mathcal{P}_{r_2} = \{r_1 : \mathcal{F}(r_2) \geq 0, r_1 < r_2\}$. We note that the set $\mathcal{N}_{r_2}$ is an empty set for $r_2 \geq \mathcal{A}$, while for $r_2 \leq \mathcal{A}$ the set reduces to $\mathcal{N}_{r_2} = \{r_1 : r_1 \leq r_2\}$. Similarly, the set $\mathcal{P}_{r_2}$ is an empty set for $r_2 \leq \mathcal{A}$ while for $r_2 \geq \mathcal{A}$ the set reduces to $\mathcal{P}_{r_2} = \{r_1 : r_1 \leq r_2\}$. Using these observations and integrating over r_1 and r_2 with $f_{R_1, R_2}(r_1, r_2) = (2\pi\lambda_R)^2 r_1 r_2 e^{-\lambda_R \pi r_2^2}$ [41], the result in (1.12) follows. $\square$

Remark 1: The energy coverage probability is significantly affected by the duration of the charging sub-slot. This intuitive insight is captured clearly in the above theorem by $C(\tau_c)$, which is a decreasing function of τ_c . As this value decreases, the energy coverage probability in (1.12) increases.

Now, in the below lemma, we derive the second term inside the expectation in (1.10), which is $\mathbb{P}(\text{SINR} \geq \beta | y_1, y_2)$.

Lemma 2 (Conditional SINR Coverage Probability): Probability that the downlink SINR at the typical IoT device exceeds β , conditioned on y_1 and y_2 , is

$$\mathbb{P}(\text{SINR} \geq \beta | y_1, y_2) = \exp(-\mathcal{G}(r_1, r_2)) \frac{1}{1 + \frac{\beta r_1^\alpha}{r_2^\alpha}}, \quad (1.15)$$

$$\text{where } r_1 = \|y_1\|, r_2 = \|y_2\|, \mathcal{G}(r_1, r_2) = \frac{\beta \sigma^2 r_1^\alpha}{\rho} + \frac{2\pi\lambda_R \beta r_1^\alpha}{(\alpha-2)r_2^{\alpha-2}}.$$

Proof. Using the definition of SINR in (1.9), we get

$$\begin{aligned}
\mathbb{P}(\text{SINR} \geq \beta | y_1, y_2) &= \mathbb{P}\left(\frac{\rho h_{y_1} r_1^{-\alpha}}{\rho h_{y_2} r_2^{-\alpha} + \rho \mathcal{M}(y_1, y_2) + \sigma^2} \geq \beta | y_1, y_2\right) \\
&\stackrel{(d)}{=} \mathbb{P}\left(\frac{\rho h_{y_1} r_1^{-\alpha}}{\rho h_{y_2} r_2^{-\alpha} + \rho \frac{2\pi\lambda_R r_2^{2-\alpha}}{\alpha-2} + \sigma^2} \geq \beta | y_1, y_2\right) \\
&= \mathbb{P}\left(h_{y_1} r_1^{-\alpha} \geq \frac{\beta \sigma^2}{\rho} + \frac{2\pi\lambda_R \beta r_2^{2-\alpha}}{\alpha-2} + \beta h_{y_2} r_2^{-\alpha} | y_1, y_2\right) \\
&\stackrel{(e)}{=} \mathbb{E}_{h_{y_2}} \left[\exp\left(-r_1^\alpha \left(\frac{\beta \sigma^2}{\rho} + \frac{2\pi\lambda_R \beta r_2^{2-\alpha}}{\alpha-2} + \beta h_{y_2} r_2^{-\alpha}\right)\right) \right] \\
&\stackrel{(f)}{=} \exp(-\mathcal{G}(r_1, r_2)) \frac{1}{1 + \beta \frac{r_1^\alpha}{r_2^\alpha}}, \quad (1.16)
\end{aligned}$$

where (d) follows from substituting for $\mathcal{M}(y_1, y_2)$ as derived in (1.13), and steps (e) and (f) follow from the assumption that $h_y \sim \exp(1)$, and defining $\mathcal{G}(r_1, r_2) = \frac{\beta\sigma^2 r_1^\alpha}{\rho} + \frac{2\pi\lambda_R \beta r_2^{2-\alpha} r_1^\alpha}{\alpha-2}$. $\square$

We can now proceed to the final step of deriving the joint coverage probability described in Definition 1. As can be observed from (1.10), the only remaining step is to take the expectation of the product of $\mathbb{P}(E_H \geq \mathcal{E}|y_1, y_2)$ and $\mathbb{P}(\text{SINR} \geq \beta|y_1, y_2)$ over y_1 and y_2 . The final result is provided in the following theorem.

Theorem 1 (Joint coverage probability): *The joint coverage probability, introduced in Definition 1, is given by*

$$P_{\text{joint}} = \int_0^{\mathcal{A}} \int_0^{r_2} f_{R_1, R_2}(r_1, r_2) \exp(-\mathcal{G}(r_1, r_2)) \frac{1}{1 + \frac{\beta r_1^\alpha}{r_2^\alpha}} dr_1 dr_2 \quad (1.17)$$

$$+ \int_{\mathcal{A}}^\infty \int_0^{r_2} f_{R_1, R_2}(r_1, r_2) \exp(-\mathcal{G}(r_1, r_2)) \frac{r_2^\alpha \exp(-r_1^\alpha \mathcal{F}(r_2)) - r_1^\alpha \exp(-r_2^\alpha \mathcal{F}(r_2))}{(r_2^\alpha - r_1^\alpha) \left(1 + \frac{\beta r_1^\alpha}{r_2^\alpha}\right)} dr_1 dr_2,$$

where $\mathcal{G}(r_1, r_2)$ is defined in Lemma 2, $\mathcal{A}$, and $\mathcal{F}(r_2)$ are defined in Lemma 1.

Proof. This result follows directly by substituting (1.11) and (1.15) in (1.10) and integrating over r_1 and r_2 using the joint distribution $f_{R_1, R_2}(r_1, r_2)$ as defined in [41, (28)]. $\square$

Remark 2: *As the duration of the charging sub-slot increases, the probability of satisfying the energy coverage condition increases. Hence, for the large enough τ_c , the joint coverage probability reduces to the probability of satisfying the SINR coverage condition. This insight is captured in the above theorem through the value of $\mathcal{A}$, which is an increasing function of τ_c . Increasing the value of $\mathcal{A}$ decreases the second term in (1.17) and increases the first term. When $\mathcal{A}$ approaches ∞ , the expression in (1.17) reduces to the SINR coverage probability.*

Remark 3: *The value of $\mathcal{A}$ represents a threshold on r_2 . In particular, for a given Φ_R , the energy coverage condition is satisfied when $r_2 \leq \mathcal{A}$. This can be observed from the integration limits in (1.17). The value of $\mathcal{A}$ can be used to optimize the deployment of RF-powered IoT devices in order to ensure high energy coverage probability. Recalling the expression of $\mathcal{A}$ provided in Lemma 1, we observe that increasing its value can be achieved through increasing the density of λ_R or the duration of the charging sub-slot.*

1.2.4 Numerical Results and Discussion

In this section, we demonstrate the accuracy of the derived expressions, verify the insights provided in the remarks, and use the numerical results to draw other important system-level insights and performance trends. The values of system parameters used in the simulation setup are $\mathcal{E} = 1 \mu\text{Joules}$, $\rho = 1$, $\lambda_R = 10^{-4} \text{ m}^{-2}$, $\alpha = 4$, and $\eta = 0.75$.

Figure 1.1 Energy coverage probability against different values of τ_c .

In Fig. 1.1, we plot the energy coverage probability. Clearly, the value of the energy coverage probability increases as we increase τ_c , which agrees with our comments in Remark 1. The perfect match between the theoretical and simulation results demonstrates the remarkable accuracy of the approximation in (1.7). We also observe the high influence of the value of λ_R on the energy coverage probability.

In Fig. 1.2, we plot the joint coverage probability, which was derived in Theorem 1. We observe that as τ_c increases, the joint coverage probability starts saturating to a fixed value, which coincides with the SINR coverage probability. This is due to the high energy coverage probability at higher values of τ_c , as observed from Fig. 1.1, which in turn reduces the P_{joint} to $\mathbb{P}(\text{SINR} \geq \beta)$. We also note that reducing the value of λ_R , which reduces the energy coverage probability, also reduces the joint coverage probability.

Finally, the average throughput, described in Definition 2, is plotted in Fig. 1.3. The results show the existence of an optimum value for τ_c that maximizes the average throughput. We note that this optimal value increases as we reduce λ_R , due to the decrease in the density of RF-chargers, which increases the amount of time needed for charging.

Figure 1.2 Joint coverage probability against different values of τ_c .

Figure 1.3 Average throughput against different values of τ_c .

1.3 RF-energy Harvesting from a Coexisting, Secrecy-enhancing Network

In the previous section, we studied a scenario where there was a coexisting cellular network that allocates some of its resources for powering the IoT devices. On the contrary, we study a scenario where the IoT devices rely on a coexisting *primary network* for harvesting RF-energy. The primary network is composed of primary transmitters and receivers (PTs and PRs) and uses some secrecy-enhancing transmission policy to ensure a certain level of secure communication probability for the primary communication links (between PTs and PRs). As described below in detail, the IoT devices would be secondary devices for this network. Our objective in this section is to investigate the impact of the use of secrecy-enhancing technique on the energy harvesting performance of the RF-powered IoT devices.

1.3.1 System Setup

Similar to the previous section, we model the locations of the IoT devices and the PTs using two independent PPPs $\Phi_E \equiv \{x_i\} \subset \mathbb{R}^2$ and $\Phi_R \equiv \{y_i\} \subset \mathbb{R}^2$, with densities λ_E and λ_R , respectively. Each PT aims to communicate with its associated PR and transmit confidential messages. In order to maintain tractability, we consider a Poisson bipolar model where the distance between each PT and its associated PR is r_1 . Due to the stationarity of PPP, we focus our analysis on a typical PT-PR pair with the PR located at the origin. Different from the system setup studied in the previous section, the charging network (the primary network) in this setup: (i) does not allocate any resources for solely charging the IoT devices, and (ii) is using a secrecy-enhancing technique that affects the energy harvesting performance of the IoT devices. The secrecy-enhancing technique used by the primary network is described next.

There are multiple secrecy-enhancing techniques studied in literature such as (i) beamforming [42–44], (ii) protected zones [45, 46], (iii) artificial noise addition [47, 48], and (iv) guard zones [2, 3]. The guard zone technique was recently proven to outperform other techniques under some specific deployment scenarios [49]. Hence, we focus on this technique in this chapter. The guard zone technique is based on ensuring that the distance between the PT and its nearest illegitimate receiver (from the perspective of PT, any receiver except PRs is an illegitimate receiver) is above a given threshold. Otherwise, the PT stops its transmission (goes silent). While this discussion is not in the scope of the current chapter, the illegitimate receivers can be detected by the primary network using specialized devices such as metal detectors or leaked local oscillator power detectors [45]. To focus on the interaction between the IoT devices and the primary network, we assume that the IoT devices are the only existing illegitimate receivers in the system. The radius of the guard zone is the main design parameter in this secrecy-enhancing technique. The selection of this parameter is based on the performance metrics that the primary network aims to maximize. Before defining the performance metrics used in this chapter, we first provide some physical layer security preliminaries.

In order to ensure secrecy, the PT selects two transmission rates: (i) codeword transmission rate $\mathcal{R}_c$, and (ii) confidential messages transmission rate $\mathcal{R}_m$, where $\mathcal{R}_c > \mathcal{R}_m$. The difference $\mathcal{R}_c - \mathcal{R}_m$ represents the cost paid for secure transmission. To ensure that the PR is able to successfully decode the confidential message, the mutual information between PT's channel input and the PR's channel output should be greater than $\mathcal{R}_c$. In addition, to ensure perfect secrecy, the mutual information between the PT's channel input and any illegitimate receiver's channel output should be less than $\mathcal{R}_c - \mathcal{R}_m$. This can be translated into two conditions. The first one is $\text{SINR}_R \geq 2^{\mathcal{R}_c} - 1$, to ensure successful connection between PT and PR, where

$$\text{SINR}_R = \frac{\rho w_1 r_1^{-\alpha}}{\sum_{y_i \in \Phi_R \setminus y_1} \delta_i \rho w_i \|y_i\|^{-\alpha} + \sigma_p^2}, \quad (1.18)$$

σ_p^2 is the noise power, and $w_i \sim \exp(1)$ models the Rayleigh fading gain for the link between the PT located at y_i and the typical PR. We use the subscript $i = 1$ to refer to the typical PT-PR pair. The value of the indicator function $\delta_i = 1$ if the PT located at y_i is active, which means it does not have any illegitimate receivers in its guard zone. Otherwise, if its guard zone has at least one illegitimate receiver, we have $\delta_i = 0$. This captures the effect of the guard zone radius on the interference levels at both the legitimate and illegitimate receivers. Clearly, as the radius of the guard zone r_g increases, more PTs will go silent, which in turn leads to less interference. The expected value of this indicator function equals to the probability of the PT being active: $\mathbb{E}[\delta_i] = P_{\text{active}}$. The value of P_{active} can be derived as follows. Denoting the distance between the typical PT and its nearest IoT device by D_e , and recalling that the locations of the IoT devices are modeled by a PPP with density λ_E , we then have

$$P_{\text{active}} = \mathbb{P}(D_e \geq r_g) = \exp(-\pi \lambda_E r_g^2). \quad (1.19)$$

The second condition that needs to be satisfied to ensure perfect secrecy is $\text{SINR}_E(x_j) \leq 2^{\mathcal{R}_c - \mathcal{R}_m} - 1$, where $\text{SINR}_E(x_j)$ is the value of SINR at the IoT device located at x_j . This condition should be satisfied at all IoT devices in order to ensure perfect secrecy. The SINR of the confidential signal transmitted by the typical PT measured at the IoT device located at x_j is

$$\text{SINR}_E(x_j) = \frac{\rho g_{1,j} \|y_1 - x_j\|^{-\alpha}}{\sum_{y_i \in \Phi_R \setminus y_1} \delta_i \rho g_{i,j} \|y_i - x_j\|^{-\alpha} + \sigma_S^2}, \quad (1.20)$$

where $g_{i,j} \sim \exp(1)$ is the fading gain for the link between the PT located at y_i and the IoT device located at x_j , and σ_S^2 is the noise power at the IoT device.

Clearly, only those PTs are active that are at a distance greater than r_g from all IoT devices. This can be formally defined as follows

$$\bar{\Phi}_R = \left\{ y \in \Phi_R : x \notin \bigcup_{x \in \Phi_E} \mathcal{B}(x, r_g) \right\}, \quad (1.21)$$

where $\mathcal{B}(x, r_g)$ is a ball centered at x with radius r_g , and $\bar{\Phi}_R$ models the locations of the active PTs. The point process $\bar{\Phi}_R$ in (1.21) is nothing but a Poisson hole

process [50, 51]. The density of the PHP $\bar{\Phi}_R$ that models the locations of active PTs is $P_{\text{active}}\lambda_R$.

Similar to the previous section, one of the main aspects of the performance of the IoT devices that we focus on is their ability to harvest sufficient amount of energy. The amount of energy harvested by the IoT device located at x_j , assuming an RF-energy harvesting time-slot of duration T , is

$$E_H = \eta T \rho \|y_{j,1} - x_j\|^{-\alpha} g_j, \quad (1.22)$$

where $g_j \sim \exp(1)$ models the Rayleigh fading gain of the link between the IoT device located at x_j and its nearest active PT. Here, we are focusing on the energy harvested from the nearest active PT, located at $y_{j,1}$. This is motivated by many recent studies that showed the dominance of the RF-energy harvested from the nearest transmitter in the total amount of harvested energy, such as [16]. This assumption lends tractability to an otherwise intractable analysis. For instance, this enables us to study the effect of some important system parameters, such as r_g and λ_E on the statistics of the harvested energy. In particular, using this approach, we can capture an interesting behavior in this system, which is how increasing the density of the IoT devices λ_E decreases the average distance between a typical IoT device and its nearest active PT, and hence, decreases the average amount of harvested energy. This results from (1.19) where we showed that the value of P_{active} is a decreasing function of λ_E and the density of active PTs is $\lambda_R P_{\text{active}}$.

1.3.2 Performance Metrics

Our objective in this section is two-fold: (i) study the effect of the deployment density of the RF-powered IoT devices on the performance of the primary network, and (ii) study the effect of the guard zone radius r_g on the energy harvesting performance of the IoT devices. For the primary network, we consider two performance metrics to capture: (i) the connectivity between the PT and its associated PR, and (ii) the secrecy of the transmitted confidential signal through studying its SINR at the illegitimate receivers (i.e., the IoT devices). We define these two performance metrics next.

Definition 3 (Probability of successful connection): *In order to ensure successful connection between the typical PT and PR, two conditions need to be satisfied: (i) the typical PT is active, and (ii) the SINR at the typical PR is greater than the threshold β_R . Therefore, the probability of successful connection is*

$$P_{\text{con}}(r_g, \lambda_E) = \mathbb{P}(D_e \geq r_g, \text{SINR}_R \geq \beta_R), \quad (1.23)$$

where $\beta_R = 2^{\mathcal{R}_c} - 1$.

The second performance metric for the primary network focuses on the secrecy of the transmitted signals when the PT is active, which is provided next.

Definition 4 (Secure communication probability): *Given that a PT is active, the probability that its transmitted data is perfectly secure is*

$$P_{\text{sec}}(r_g, \lambda_E) = \mathbb{E} \left[\mathbb{1} \left(\bigcap_{x_j \in \Phi_E} \text{SINR}_E(x_j) \leq \beta_E \middle| D_e \geq r_g \right) \right], \quad (1.24)$$

where $\beta_E = 2^{\mathcal{R}_c - \mathcal{R}_m} - 1$.

The goal of the primary network is to maximize the value of P_{con} while ensuring that P_{sec} is above a predefined threshold ε . The parameter tuned to achieve this objective is r_g . Hence, the value of r_g selected by the primary network is

$$r_g^* = \arg \max_{r_g \in \mathcal{G}(\lambda_E)} P_{\text{con}}(r_g, \lambda_E),$$

$$\mathcal{G}(\lambda_E) = \{r_g : P_{\text{sec}}(r_g, \lambda_E) \geq \varepsilon\}. \quad (1.25)$$

There are many metrics that have been used in the literature to study the performance of the energy harvesting aspect. For instance, the average amount of harvested energy $\mathbb{E}[E_H]$, or the energy coverage probability $\mathbb{P}(E_H \geq \mathcal{E})$. In this section, we focus on a modified version of the latter (defined next), which enables us to better understand the relation between the two coexisting networks, which is one of the main objectives of this section.

Definition 5 (Average density of successfully charged devices): *The average density of devices that successfully harvest at least $\mathcal{E}$ amount of energy is*

$$\bar{\lambda}_E = \lambda_E \mathbb{P}(E_H \geq \mathcal{E}). \quad (1.26)$$

The goal of the IoT network is to optimize the value of λ_E with the objective of maximizing the above performance metric. While this may seem counter intuitive, one can make sense of it (based on the discussion provided earlier) by observing that increasing the value of λ_E reduces the density of active PTs, which are the main sources of RF-energy for the IoT devices.

1.3.3 Analysis and Main Results

We start our analysis by deriving the performance metrics for the primary network. In the next theorem, we provide an expression for the successful connection probability, introduced in Definition 3.

Theorem 2 (Probability of successful connection): *For a given value of λ_E , the probability of successful connection introduced in Definition 3 is*

$$P_{\text{con}}(r_g, \lambda_E) = \exp \left(- \left[\lambda_E \pi r_g^2 + \beta_R \frac{\sigma_R^2}{\rho} r_1^\alpha + \frac{2\pi^2 \lambda_R P_{\text{active}} \beta_R^{\frac{2}{\alpha}} r_1^2}{\alpha \sin(\frac{2}{\alpha} \pi)} \right] \right). \quad (1.27)$$

Proof. Recalling the expression for SINR_R given in (1.18), specifically the indicator function δ_i that indicates which interferer is active and which is silent, we

concluded that the locations of active PTs can be modeled by PHP $\bar{\Phi}_R$ in (1.21). However, before using $\bar{\Phi}_R$ in our analysis, we need to make it clear that δ_i for different $y_i \in \bar{\Phi}_R$ are correlated. This implicit correlation arises from the dependence of δ_i for all i on the PPP Φ_E . However, capturing this correlation in our analysis will significantly reduce the tractability of the results. Hence, this correlation will be ignored here. The accuracy of this approximation will be verified in Section 1.3.4. Now, revisiting the expression of P_{con} in Definition 3, we note that the correlation between δ_1 at the typical PT and δ_i values at each of the interferers in the expression of SINR_R is the only source of correlation between the events $(D_e \geq r_g)$ and $(\text{SINR}_R \geq \beta_R)$. Hence, ignoring this correlation, for the reasons stated earlier, will lead to the following

$$P_{\text{con}} = \mathbb{P}(D_e \geq r_g) \mathbb{P}(\text{SINR}_R \geq \beta_R). \quad (1.28)$$

The first term in the above expression represents $P_{\text{active}} = \exp(-\pi\lambda_R r_g^2)$ (please recall (1.19) where P_{active} was derived). To derive the second term in the above expression, characterizing the statistics of the interference from a PHP modeled network at a randomly located reference point (the typical PR) is required. However, ignoring the correlation between $\{\delta_i\}$ is equivalent to approximating the PHP $\bar{\Phi}_R$ with a PPP Ψ of equivalent density $\tilde{\lambda}_R = \lambda_R P_{\text{active}}$. Defining $I = \sum_{y_i \in \Psi} w_i \|y_i\|^{-\alpha}$, then

$$\begin{aligned} \mathbb{P}(\text{SINR}_R \geq \beta_R) &= \mathbb{P}\left(\frac{w_1 r_1^{-\alpha}}{I + \frac{\sigma_R^2}{\rho}} \geq \beta_R\right) \\ &\stackrel{(a)}{=} \mathbb{E}_I \left[\exp\left(-\beta_R \left(I + \frac{\sigma_R^2}{\rho}\right) r_1^\alpha\right) \right] \\ &= \exp\left(-\beta_R \frac{\sigma_R^2}{\rho} r_1^\alpha\right) \mathbb{E}_I [\exp(-\beta_R I r_1^\alpha)] \\ &\stackrel{(b)}{=} \exp\left(-\beta_R \frac{\sigma_R^2}{\rho} r_1^\alpha\right) \mathcal{L}_I(\beta_R r_1^\alpha), \end{aligned} \quad (1.29)$$

where $w_1 \sim \exp(1)$ leads to step (a), and in step (b) we use the definition of Laplace transform of I which is $\mathcal{L}_I(s) = \mathbb{E}[\exp(-sI)]$. The Laplace transform of the interference in PPP is a well established result in literature [4]. For completeness, its derivation is provided next.

$$\begin{aligned} \mathcal{L}_I(s) &= \mathbb{E}_{\Psi, \{w_i\}} \left[\exp\left(-s \sum_{y_i \in \Psi} w_i \|y_i\|^{-\alpha}\right) \right] \\ &= \mathbb{E}_{\Psi, \{w_i\}} \left[\prod_{y_i \in \Psi} \exp(-s w_i \|y_i\|^{-\alpha}) \right] \\ &\stackrel{(c)}{=} \mathbb{E}_{\Psi} \left[\prod_{y_i \in \Psi} \frac{1}{1 + s \|y_i\|^{-\alpha}} \right] \\ &\stackrel{(d)}{=} \exp\left(-\tilde{\lambda}_R \int_{y \in \mathbb{R}^2} 1 - \frac{1}{1 + s \|y\|^{-\alpha}} dy\right) \end{aligned}$$

$$\begin{aligned}
&\stackrel{(e)}{=} \exp \left(-2\pi\tilde{\lambda}_R \int_0^\infty \frac{sr_y^{-\alpha}}{1+sr_y^{-\alpha}} r_y dr_y \right) \\
&\stackrel{(f)}{=} \exp \left(-\frac{2\pi^2\tilde{\lambda}_R s^{\frac{2}{\alpha}} \csc\left(\frac{2\pi}{\alpha}\right)}{\alpha} \right), \tag{1.30}
\end{aligned}$$

where knowing that the set of fading gains w_i are i.i.d with $w_i \sim \exp(1)$ leads to step (c), step (d) results from using the probability generating function (PGFL) of PPP [40], step (e) results from converting to polar co-ordinates, and step (f) follows after some mathematical manipulations. Substituting (1.30) in (1.29) and then in (1.28) leads to the final result in Theorem 2. $\square$

Remark 4: The expression in Theorem 2 captures two important insights on the effect of r_g on P_{con} . Recalling the definition of P_{con} , we notice that successful connection requires: (i) the typical PT being active (guard zone free of illegitimate receivers), and (ii) the SINR at the typical PR is above a predefined threshold β_R . The first condition gets harder to satisfy as the value of r_g increases, due to the difficulty of ensuring that the guard zone is free of ERs when its radius is large. This effect is captured in the first term inside the exponential in Theorem 2. For the second condition, namely the SINR value, we observe that increasing the value of r_g decreases the density of active interferers, leading to higher values of SINR_R . Hence, increasing r_g makes it easier to satisfy the SINR condition. This is also captured in the third term inside the exponential in Theorem 2, implicitly in the expression of P_{active} .

To further investigate the effect of r_g on P_{con} , we derive the value of $r_g = \hat{r}_g$ that maximizes P_{con} in the below theorem.

Theorem 3: Defining $\mathcal{A}_1 = \frac{2\pi^2\lambda_R\beta_R^{\frac{2}{\alpha}}r_1^2}{\alpha\sin(\frac{2}{\alpha}\pi)}$, we have:

- If $\mathcal{A}_1 \leq 1$, then P_{con} is a decreasing function of r_g , and $\hat{r}_g = 0$.
- If $\mathcal{A}_1 > 1$, then $\hat{r}_g = \sqrt{\frac{\ln(\mathcal{A}_1)}{\pi\lambda_E}}$.

Proof. From the expression of P_{con} in Theorem 2, we note that it can be rewritten as a function of $P_{\text{active}} = \exp(-\lambda_E\pi r_g^2)$ as follows

$$P_{\text{con}} = \exp \left(-\beta_R \frac{\sigma_R^2}{\rho} r_1^\alpha \right) P_{\text{active}} \exp(-P_{\text{active}}\mathcal{A}_1), \tag{1.31}$$

To get more information about the behavior of P_{con} against P_{active} , we compute the first derivative (with respect to P_{active}). Given that P_{active} is a decreasing function of r_g (recall (1.19)), we conclude the following

1. If $1 - \mathcal{A}_1 P_{\text{active}} \geq 0$, then P_{con} is a decreasing function of r_g ,
2. If $1 - \mathcal{A}_1 P_{\text{active}} < 0$, then P_{con} is an increasing function of r_g .

Consequently, we can infer that, since $0 \leq P_{\text{active}} \leq 1$, P_{con} is a decreasing function of r_g as long as $\mathcal{A}_1 \leq 1$. In the case of $\mathcal{A}_1 \geq 1$, the relation between P_{con} and r_g can be explained as follows: (i) P_{con} is an increasing function of r_g as long as $P_{\text{active}} \geq \frac{1}{\mathcal{A}_1}$

(or $r_g \leq \sqrt{\frac{\ln(\mathcal{A}_1)}{\lambda_E \pi}}$), and (ii) P_{con} is a decreasing function of r_g as long as $P_{\text{active}} \leq \frac{1}{\mathcal{A}_1}$ (or $r_g \geq \sqrt{\frac{\ln(\mathcal{A}_1)}{\lambda_E \pi}}$). This concludes the proof. $\square$

Remark 5: Consistent with the intuition, we observe from the above theorem that when $\mathcal{A}_1 \leq 1$, the effect of r_g on the event $D_E \geq r_g$ dominates its effect on the density of interferers, because of which P_{con} is a decreasing function of r_g . This is because $\mathcal{A}_1$ is an increasing function of each of λ_R , r_1 , and β_R . At lower values of $\mathcal{A}_1$, one or more of these parameters are small enough to ignore the effect of the interference level on P_{con} .

Now we derive the secure communication probability, introduced in Definition 4, in the following theorem.

Theorem 4 (Secure communication probability): For a given value of r_g and λ_E , the probability of secure communication is $P_{\text{sec}}(r_g, \lambda_E) =$

$$\exp \left(-2\pi\lambda_E \int_{r_g}^{\infty} \exp \left(-\frac{\sigma_E^2 \beta_E r_x^\alpha}{\rho} \right) \mathcal{L}_2(\beta_E r_x^\alpha) r_x dr_x \right), \quad (1.32)$$

where $\mathcal{L}_2(s) = \exp \left(-2\pi\lambda_R P_{\text{active}} \int_0^{sr_g^{-\alpha}} \frac{s^{\frac{2}{\alpha}}}{\alpha(1+z)z^{\frac{2}{\alpha}}} dz \right)$.

Proof. From Definition 4 of P_{sec} , we observe that we need to jointly analyze the values of $\text{SINR}_E(x_j)$ at all the locations $x_j \in \Phi_E$. Despite the usual assumption throughout most of the stochastic geometry-based literature on secrecy analysis that these values are uncorrelated, this is actually not precise. The reason for that is the dependence of $\text{SINR}_E(x_j)$, by definition, on the PPP Φ_R for all $x_j \in \Phi_E$. Some recent works focused on characterizing the correlation between interference levels at different locations [52]. However, most of these works focus on characterizing the correlation between only two locations assuming the knowledge of the distance between them. Unfortunately, these results are not directly applicable to our analysis. Hence, aligning with the existing literature, we will ignore this correlation in our analysis with the knowledge that this will provide an approximation. Furthermore, the accuracy of this approximation is expected to get worse as the value of λ_E increases. This is due to the fact that the distances between ERs decrease as λ_E increases, which was shown in [52] to increase the correlation. For notational simplicity, and without any loss of generality due to the stationarity of PPP, we will assume that the typical PT is placed at the origin, i.e. $y_1 = o$, in the rest of this proof. All the analysis provided in this section is conditioned on the event $D_e \geq r_g$. Following the same approach as in the proof of Theorem 2 of approximating the PHP Φ_R with a PPP Ψ , and defining $I_2(x_j) = \sum_{y_i \in \Psi \setminus y_1} g_{i,j} \|y_i - x_j\|^{-\alpha}$, P_{sec} can be derived as follows

$$P_{\text{sec}} = \mathbb{E}_{\Phi_E, I_2, \{g_{1,j}\}} \left[\mathbb{1} \left(\bigcap_{x_j \in \Phi_E} \frac{g_{1,j} \|x_j\|^{-\alpha}}{I_2(x_j) + \frac{\sigma_E^2}{\rho}} \leq \beta_E \right) \right]$$

$$\begin{aligned}
&\stackrel{(g)}{=} \mathbb{E}_{\Phi_E, I_2, \{g_{1,j}\}} \left[\prod_{x_j \in \Phi_E} \mathbb{1} \left(\frac{g_{1,j} \|x_j\|^{-\alpha}}{I_2(x_j) + \frac{\sigma_E^2}{\rho}} \leq \beta_E \right) \right] \\
&\stackrel{(h)}{=} \mathbb{E}_{\Phi_E, I_2} \left[\prod_{x_j \in \Phi_E} \left(1 - \exp \left(- \frac{\beta_E \left(I_2(x_j) + \frac{\sigma_E^2}{\rho} \right)}{\|x_j\|^{-\alpha}} \right) \right) \right] \\
&\stackrel{(i)}{=} \mathbb{E}_{\Phi_E} \left[\prod_{x_j \in \Phi_E} \left(1 - \exp \left(- \frac{\beta_E \left(\frac{\sigma_E^2}{\rho} \right)}{\|x_j\|^{-\alpha}} \right) \mathbb{E} \left[\exp \left(- \frac{\beta_E I_2(y_j)}{\|x_j\|^{-\alpha}} \right) \right] \right) \right], \quad (1.33)
\end{aligned}$$

where step (g) (and step (i)) follow from assuming that the values of $\text{SINR}_E(x_j)$ (and $I_2(x_j)$) are uncorrelated. Step (h) is due to assuming the set of fading gains $\{g_{1,j}\}$ to be i.i.d with $g_{1,j} \sim \exp(1)$. Defining the Laplace transform of $I_2(x_j)$ by $\mathcal{L}_{I_2(x_j)}(s) = \mathbb{E}[\exp(-sI_2(x_j))]$, we note that there is only one difference in the derivation of $\mathcal{L}_{I_2(x_j)}(s)$ compared to that of $\mathcal{L}_I(s)$ in the proof of Theorem 2. The difference is in the reference point from where we are observing the interference. In the proof of Theorem 2, the reference point was the PR, which does not have a minimum distance from any active interfering PT. In the current derivation, the reference point is an IoT device, which has a minimum distance of r_g from any active interfering PT. Hence, the derivation of $\mathcal{L}_{I_2(x_j)}(s)$ will be exactly the same as in (1.30) until step (e), where the minimum distance effect will appear in the lower limit of the integral as follows

$$\mathcal{L}_{I_2(x_j)}(s) = \exp \left(-2\pi\tilde{\lambda}_R \int_{r_g}^{\infty} \frac{sr_y^{-\alpha}}{1+sr_y^{-\alpha}} r_y dr_y \right). \quad (1.34)$$

Note that the above expression is not a function of x_j , so we drop it from the notation of Laplace transform. The final expression for $\mathcal{L}_{I_2}(s)$ as provided in Theorem 4 follows after simple mathematical manipulations. Substituting (1.34) in (1.33), we get

$$\begin{aligned}
P_{\text{sec}} &= \mathbb{E}_{\Phi_E} \left[\prod_{x_j \in \Phi_E} \left(1 - \exp \left(-\beta_E \left(\frac{\sigma_E^2}{\rho} \right) \|x_j\|^\alpha \right) \mathcal{L}_{I_2}(\beta_E \|x_j\|^\alpha) \right) \right] \\
&\stackrel{(k)}{=} \exp \left(-2\pi\lambda_E \int_{x \in \mathbb{R}^2 \cap \mathcal{B}(o, r_g)} \exp \left(-\beta_E \left(\frac{\sigma_E^2}{\rho} \right) \|x\|^\alpha \right) \mathcal{L}_{I_2}(\beta_E \|x\|^\alpha) dx \right), \quad (1.35)
\end{aligned}$$

where step (k) results from applying PGFL of PPP, and the integration is over $y \in \mathbb{R}^2 \cap \mathcal{B}(o, r_g)$ because the analysis in this section is conditioned on the event $D_e \geq r_g$, which means that the typical PT is active. Since we assumed that the typical PT is placed at the origin in this derivation, the ball $\mathcal{B}(o, r_g)$ is clear of ERs. Converting from Cartesian to polar co-ordinates leads to the final result in Theorem 4. $\square$

Remark 6: As stated in the earlier remarks, the value of r_g has a significant effect on the density of active interferers. Hence, the total interference at any receiver,

legitimate or not, decreases as we increase the value of r_g . This is captured in the Laplace transform term of the expression derived in Theorem 4. In addition, since transmitting signals is already conditioned on the guard zone being free of the illegitimate receivers, there is a minimum distance r_g between the typical PT and the nearest illegitimate receiver. Hence, increasing the value of r_g reduces the quality of the confidential signal transmitted by the PT at the illegitimate receivers. This is captured in Theorem 4 in the integration interval, which decreases as we increase r_g . This trade-off in the effect of r_g on the secure communication probability will be further investigated and visualized with the aid of numerical results in the next subsection.

In the following theorem, we provide the main performance metric for the IoT devices, which is the density of successfully charged devices.

Theorem 5 (Density of successfully charged devices): For a given value of r_g and λ_E , the density of successfully charged IoT devices is

$$\bar{\lambda}_E = \lambda_E \int_{r_g}^{\infty} 2\pi\lambda_R P_{\text{active}} r_p \exp\left(-\pi\lambda_R P_{\text{active}}(r_p^2 - r_g^2) - \frac{\mathcal{E} r_p^\alpha}{\rho\eta}\right) dr_p. \quad (1.36)$$

Proof. The density of successfully charged IoT devices can be derived as follows

$$\begin{aligned} P_{\text{energy}} &= \lambda_E \mathbb{P}(\eta\rho R_p^{-\alpha} g \geq \mathcal{E}) \\ &\stackrel{(l)}{=} \mathbb{E}_{R_p} \left[\exp\left(-\frac{\mathcal{E} R_p^\alpha}{\eta\rho}\right) \right], \end{aligned} \quad (1.37)$$

where R_p is the distance between the ER and its nearest active PT, and step (l) is due to $g \sim \exp(1)$. The distance R_p represents the contact distance of a PHP observed from a hole center. Unfortunately, the exact distribution of this distance is unknown. However, the approach of approximating the PHP $\bar{\Phi}_R$ with a PPP Ψ is known to provide fairly tight approximation of the contact distance distribution of PHP [53]. Given that the nearest active PT to the ER is at a distance of at least r_g , the distribution of R_p is

$$f_{R_p}(r_p) = 2\pi\tilde{\lambda}_R \exp\left(-\pi\tilde{\lambda}_R(r_p - r_g)^2\right), \quad r_p \geq r_g. \quad (1.38)$$

Using this distribution to compute the expectation in (1.37) leads to the final result in Theorem 5. $\square$

1.3.4 Numerical Results and Discussion

In this section, unless otherwise specified, we use the following values for the simulation parameters: $\eta = 0.75$, $\varepsilon = 0.9$, $\lambda_R = 10^{-1} \text{ m}^{-2}$, $\rho = 1$, $T = 1$, $\alpha = 4$, $\beta_R = 3 \text{ dB}$, $\beta_E = 0 \text{ dB}$, and $\mathcal{E} = 1 \text{ } \mu\text{Joules}$. We also refer to the SNR value at the IoT devices as $\gamma = \frac{\rho}{\sigma_E^2}$.

In Fig. 1.4, we plot the successful connection probability for different values of r_g . Given that the simulation setup captures a scenario with $\mathcal{A}_1 < 1$ (introduced in

Figure 1.4 Successful connection probability against different values of r_g .

Theorem 3), P_{con} is a decreasing function of r_g . This is consistent with our observations in Theorem 3 and the following remarks. Hence, recalling (1.25), we conclude that for the considered simulation setup, r_g^* is the minimum value of r_g that ensures $P_{\text{sec}} \geq \varepsilon$.

In Fig. 1.5, we plot the secure communication probability for different values of r_g . The effect of r_g on the secure communication probability, discussed in Theorem 4 and the following remarks, can be observed in Fig. 1.5. At low values of r_g , the performance is dominated by the high interference at the illegitimate receivers, due to the high density of the active PTs. This reflects the stronger effect of λ_S on P_{sec} at lower values of r_g . At high values of r_g , despite the low density of active PTs, the performance is dominated by the large distance between the PT and its nearest illegitimate receiver. We observe the existence of a minimum value for P_{sec} , at which the value of r_g is not small enough to result in high level of interference at the illegitimate receivers, nor it is high enough to result in large distance between the active PT and its nearest illegitimate receiver. We also observe that increasing the value of λ_E increases the value of r_g^* that ensures $P_{\text{sec}} = \varepsilon$, where $\varepsilon = 0.9$.

In Fig. 1.6, we study the effect of $\gamma = \frac{\rho}{\sigma_E^2}$ on the value of P_{sec} . Unlike λ_E , the effect of γ on P_{sec} is more prominent at higher values of r_g . As stated earlier, this is due to the dominance of the interference on the performance at lower values of r_g , leading to negligible effect of γ in this regime.

In Fig. 1.7, we plot the density of successfully charged devices for different values of λ_E . As reported earlier, there exists an optimal value of λ_E that maximizes this density. Furthermore, we observe that increasing the value of r_g has a clear negative effect on the performance of the IoT devices. This can be noticed from the

Figure 1.5 Secure communication probability against different values of r_g and λ_E

Figure 1.6 Secure communication probability against different values of r_g and γ

Figure 1.7 Density of successfully charged devices against different values of λ_E and r_g .

decrease in the value of the maximum achievable density of successfully charged devices as we increase the value of r_g .

We can observe from Fig. 1.5 and Fig. 1.7 that the parameter selection of the two networks (r_g selection by the primary network and λ_E selection by the IoT devices) is inter-twined. This interaction can actually be modeled as a two-player non-cooperative game. The Nash equilibrium of such game would capture a state where the primary network has no incentive to change the value of r_g given the value of λ_E , and the IoT devices have no incentive to change the value of λ_E given the value of r_g . However, the main complexity of analyzing such a game arises from the relatively complicated expressions of P_{sec} and $\bar{\lambda}_E$, because of which it is challenging to prove the existence of a Nash equilibrium. This actually is one of the main challenges that arise whenever the objective is to optimize an expression derived using stochastic geometry tools. Interested readers are advised to refer to [19] for more details.

1.4 Summary

This chapter focused on the application of stochastic geometry to the performance analysis of RF-powered IoT networks. In particular, we focused on two scenarios of general interest: (i) the same wireless network provides connectivity and RF charging to the IoT devices, and (ii) IoT devices rely on a coexisting, secrecy-enhancing network for harvesting RF-energy. In the first part of the chapter, we considered an IoT network that relies on the cellular infrastructure for communication and RF charging. For this setup, we studied the joint probability of harvesting sufficient energy and maintaining sufficiently high downlink SINR. We proposed a dominant-

interferer approximation that enabled the derivation of the joint probability and resulted in several system-level insights. One of the main insights obtained from this analysis is the existence of an optimal charging slot duration that maximizes the downlink average throughput. We also derived a *tuning parameter* that captures the effect of the system parameters on the system performance, such as the density of the BSs.

In the second part of this chapter, we considered an RF-powered IoT network coexisting with a secrecy-enhanced primary network. The IoT network relies on the RF transmissions of the primary network for RF charging. The primary network is assumed to use the guard zones technique. This technique maintains a minimum distance between any active primary transmitter and its nearest IoT device. For that setup, we derived the secrecy performance metrics of the primary network and the energy harvesting performance metrics of the IoT network. We showed that the performance of both networks is correlated, because both secrecy and energy harvesting performance metrics depend on the deployment density of the IoT devices and the guard-zone radius of the primary network. A useful insight obtained from this study is the existence of an optimal deployment density for the IoT network that maximizes the density of successfully charged devices.

References

- [1] Dhillon HS, Huang H, Viswanathan H. Wide-area Wireless Communication Challenges for the Internet of Things. *IEEE Commun Mag.* 2017 Feb;55(2):168–174.
- [2] Zhou X, Ganti RK, Andrews JG, et al. On the Throughput Cost of Physical Layer Security in Decentralized Wireless Networks. *IEEE Trans on Wireless Commun.* 2011 Aug;10(8):2764–2775.
- [3] Pinto PC, Barros J, Win MZ. Secure Communication in Stochastic Wireless Networks—Part I: Connectivity. *IEEE Trans on Info Forensics and Security.* 2012 Feb;7(1):125–138.
- [4] Andrews JG, Gupta AK, Dhillon HS. A Primer on Cellular Network Analysis Using Stochastic Geometry;2016, available online: arxiv.org/abs/1604.03183.
- [5] ElSawy H, Hossain E, Haenggi M. Stochastic Geometry for Modeling, Analysis, and Design of Multi-tier and Cognitive Cellular Wireless Networks: A Survey. *IEEE Communications Surveys and Tutorials.* 2013;15(3):996 – 1019.
- [6] Mukherjee S. Analytical Modeling of Heterogeneous Cellular Networks: Geometry, Coverage, and Capacity. New York: Cambridge University Press; 2014.
- [7] ElSawy H, Sultan-Salem A, Alouini MS, et al. Modeling and Analysis of Cellular Networks Using Stochastic Geometry: A Tutorial. *IEEE Communications Surveys Tutorials.* 2017 Firstquarter;19(1):167–203.

- [8] Flint I, Lu X, Privault N, et al. Performance Analysis of Ambient RF Energy Harvesting with Repulsive Point Process Modeling. *IEEE Transactions on Wireless Communications*. Oct 2015;14(10):5402–5416.
- [9] Zhong C, Chen X, Zhang Z, et al. Wireless-Powered Communications: Performance Analysis and Optimization. *IEEE Transactions on Communications*. Dec 2015;63(12):5178–5190.
- [10] Huang K, Lau VK. Enabling Wireless Power Transfer in Cellular Networks: Architecture, Modeling and Deployment. *IEEE Transactions on Wireless Communications*. Feb 2014;13(2):902–912.
- [11] Sakr AH, Hossain E. Analysis of K-Tier Uplink Cellular Networks With Ambient RF Energy Harvesting. *IEEE Journal on Selected Areas in Communications*. Oct 2015;33(10):2226–2238.
- [12] Che YL, Duan L, Zhang R. Spatial Throughput Maximization of Wireless Powered Communications Networks. *IEEE Journal on Selected Areas in Communications*. 2015 Aug;33(8):1534–1548.
- [13] Krikidis I. Simultaneous Information and Energy Transfer in Large-Scale Networks with/without Relaying. *IEEE Transactions on Communications*. Mar 2014;62(3):900–912.
- [14] Zhou X, Zhang R, Ho CK. Wireless Information and Power Transfer: Architecture Design and Rate-Energy Tradeoff. *IEEE Transactions on Communications*. Nov 2013;61(11):4754–4767.
- [15] Zhou S, Chen T, Chen W, et al. Outage Minimization for a Fading Wireless Link with Energy Harvesting Transmitter and Receiver. *IEEE Journal on Selected Areas in Communications*. Mar 2015;33(3):496–511.
- [16] Kishk MA, Dhillon HS. Downlink Performance Analysis of Cellular-Based IoT Network with Energy Harvesting Receivers. In: *IEEE GLOBECOM*; 2016. .
- [17] Kishk MA, Dhillon HS. Modeling and Analysis of Ambient RF Energy Harvesting in Networks with Secrecy Guard Zones. In: *2017 IEEE Wireless Communications and Networking Conference (WCNC)*; 2017. p. 1–6.
- [18] Kishk MA, Dhillon HS. Joint Uplink and Downlink Coverage Analysis of Cellular-based RF-powered IoT Network. *IEEE Transactions on Green Communications and Networking*. 2018 June;2(2):446–459.
- [19] Kishk MA, Dhillon HS. Coexistence of RF-powered IoT and a Primary Wireless Network With Secrecy Guard Zones. *IEEE Transactions on Wireless Communications*. 2018 March;17(3):1460–1473.
- [20] Abd-Elmagid MA, Kishk MA, Dhillon HS. Joint Energy and SINR Coverage in Spatially Clustered RF-Powered IoT Network. *IEEE Transactions on Green Communications and Networking*. 2019 March;3(1):132–146.
- [21] Abd-Elmagid MA, Kishk MA, Dhillon HS. Coverage Analysis of Spatially Clustered RF-Powered IoT Network. In: *Proc., IEEE ICC*; 2018. p. 1–7.
- [22] Kishk MA, Dhillon HS. A Comparison of Secrecy Enhancing Techniques for Secure SWIPT System. In: *Proc. IEEE ICC workshops*; 2018. p. 1–6.

- [23] Ganesan K, Grover P, Rabaey J. The Power Cost of Over-designing Codes. Proc, IEEE Workshop on Signal Processing Systems (SiPS). Oct 2011;p. 128–133.
- [24] Blake CG, Kschischang FR. Energy Consumption of VLSI Decoders. IEEE Transactions on Information Theory. June 2015;61(6):3185–3198.
- [25] Grover P. Bounds on the Tradeoff Between Decoding Complexity and Rate for Sparse-Graph Codes. In: Proc., IEEE Information Theory Workshop (ITW); 2007. p. 196–201.
- [26] Di Renzo M, Lu W. System-Level Analysis and Optimization of Cellular Networks With Simultaneous Wireless Information and Power Transfer: Stochastic Geometry Modeling. IEEE Transactions on Vehicular Technology. 2017 March;66(3):2251–2275.
- [27] Khan TA, Alkhateeb A, Heath RW. Millimeter Wave Energy Harvesting. IEEE Transactions on Wireless Communications. 2016 Sept;15(9):6048–6062.
- [28] Li Q, Ma WK, So AMC. Robust artificial noise-aided transmit optimization for achieving secrecy and energy harvesting. In: Proc., IEEE Intl. Conf. on Acoustics, Speech, and Sig. Proc. (ICASSP); 2014. p. 1596–1600.
- [29] Xing H, Liu L, Zhang R. Secrecy Wireless Information and Power Transfer in Fading Wiretap Channel. IEEE Trans on Veh Technology. 2016 Jan;65(1):180–190.
- [30] Liu M, Liu Y. Power Allocation for Secure SWIPT Systems With Wireless-Powered Cooperative Jamming. IEEE Communications Letters. 2017 June;21(6):1353–1356.
- [31] Liu L, Zhang R, Chua KC. Secrecy Wireless Information and Power Transfer With MISO Beamforming. IEEE Trans on Signal Processing. 2014 April;62(7):1850–1863.
- [32] Ren Y, Lv T, Gao H, et al. Secure Wireless Information and Power Transfer in Heterogeneous Networks. 2017;IEEE Access, to appear.
- [33] Liu Y, Wang L, Zaidi SAR, et al. Secure D2D Communications in Large-Scale Cognitive Cellular Networks: A Wireless Power Transfer Model. IEEE Transactions on Communications. 2016 Jan;64(1):329–342.
- [34] Weber S, Andrews JG, Jindal N. The Effect of Fading, Channel Inversion, and Threshold Scheduling on Ad Hoc Networks. IEEE Transactions on Information Theory. 2007 Nov;53(11):4127–4149.
- [35] Madhusudhanan P, Restrepo JG, Liu Y, et al. Downlink Performance Analysis for a Generalized Shotgun Cellular System. IEEE Transactions on Wireless Communications. 2014 Dec;13(12):6684–6696.
- [36] Schloemann J, Dhillon HS, Buehrer RM. Toward a Tractable Analysis of Localization Fundamentals in Cellular Networks. IEEE Transactions on Wireless Communications. 2016 March;15(3):1768–1782.
- [37] Bhandari T, Dhillon HS, Buehrer RM. The Impact of Proximate Base Station Measurements on Localizability in Cellular Systems. In: Proc., IEEE SPAWC; 2016. .

- [38] Chetlur VV, Dhillon HS. Downlink Coverage Probability in a Finite Network of Unmanned Aerial Vehicle (UAV) Base Stations. In: Proc., IEEE SPAWC; 2016. .
- [39] Chetlur VV, Dhillon HS. Downlink Coverage Analysis for a Finite 3-D Wireless Network of Unmanned Aerial Vehicles. *IEEE Transactions on Communications*. 2017 Oct;65(10):4543–4558.
- [40] Haenggi M. *Stochastic Geometry for Wireless Networks*. Cambridge University Press; 2012.
- [41] Moltchanov D. Distance Distributions in Random Networks. *Ad Hoc Networks*. 2012;10(6):1146–1166.
- [42] Khandaker MR, Wong KK. Robust secrecy beamforming with energy-harvesting eavesdroppers. *IEEE Wireless Commun Letters*. 2015;4(1):10–13.
- [43] Ng DWK, Lo ES, Schober R. Robust beamforming for secure communication in systems with wireless information and power transfer. *IEEE Trans on Wireless Commun*. 2014;13(8):4599–4615.
- [44] Xu J, Liu L, Zhang R. Multiuser MISO beamforming for simultaneous wireless information and power transfer. *IEEE Trans on Signal Processing*. 2014;62(18):4798–4810.
- [45] Chae SH, Choi W, Lee JH, et al. Enhanced Secrecy in Stochastic Wireless Networks: Artificial Noise With Secrecy Protected Zone. *IEEE Trans on Information Forensics and Security*. 2014 Oct;9(10):1617–1628.
- [46] Liu W, Ding Z, Ratnarajah T, et al. On Ergodic Secrecy Capacity of Random Wireless Networks With Protected Zones. *IEEE Trans on Vehicular Technology*. 2016 Aug;65(8):6146–6158.
- [47] Zhou X, McKay MR. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. *IEEE Trans on Vehicular Technology*. 2010;59(8):3831–3842.
- [48] Zhang M, Liu Y, Zhang R. Artificial noise aided secrecy information and power transfer in OFDMA systems. *IEEE Trans on Wireless Commun*. 2016;15(4):3085–3096.
- [49] Kishk MA, Dhillon HS. Stochastic Geometry-Based Comparison of Secrecy Enhancement Techniques in D2D Networks. *IEEE Wireless Communications Letters*. 2017 June;6(3):394–397.
- [50] Yazdanshenasan Z, Dhillon HS, Afshang M, et al. Poisson Hole Process: Theory and Applications to Wireless Networks. *IEEE Trans on Wireless Commun*. 2016 Nov;15(11):7531–7546.
- [51] h Lee C, Haenggi M. Interference and Outage in Poisson Cognitive Networks. *IEEE Trans on Wireless Commun*. 2012 April;11(4):1392–1401.
- [52] Krishnan S, Dhillon HS. Spatio-Temporal Interference Correlation and Joint Coverage in Cellular Networks. *IEEE Transactions on Wireless Communications*. 2017 Sept;16(9):5659–5672.
- [53] Kishk MA, Dhillon HS. Tight Lower Bounds on the Contact Distance Distribution in Poisson Hole Process; *IEEE Wireless Commun. Letters*, to appear.