Coexistence of RF-powered IoT and a Primary Wireless Network With Secrecy Guard Zones

Mustafa A. Kishk, *Student Member, IEEE*, and Harpreet S. Dhillon, *Member, IEEE*

Abstract*— This paper studies the secrecy performance of a wireless network (primary network) overlaid with an ambient RF energy harvesting Internet of Things (IoT) network (secondary network). The nodes in the secondary network are assumed to be solely powered by ambient RF energy harvested from the transmissions of the primary network. We assume that the secondary nodes can eavesdrop on the primary transmissions due to which the primary network uses *secrecy guard zones*. The primary transmitter goes silent if any secondary receiver is detected within its guard zone. Using tools from stochastic geometry, we derive the probability of successful connection of the primary network as well as the probability of secure communication. Two conditions must be jointly satisfied in order to ensure successful connection: 1) the signal-to-interference-plus-noise ratio (SINR) at the primary receiver is above a predefined threshold, and 2) the primary transmitter is not silent. In order to ensure secure communication, the SINR value at each of the secondary nodes should be less than a predefined threshold. Clearly, when more secondary nodes are deployed, more primary transmitters will remain silent for a given guard zone radius, which will in turn impact the amount of energy harvested by the secondary network. Our results concretely show the existence of an optimal deployment density for the secondary network that maximizes the density of nodes that are able to harvest sufficient amount of energy. Furthermore, we show the dependence of this optimal deployment density on the guard zone radius of the primary network. In addition, we show that the optimal guard zone radius selected by the primary network is a function of the deployment density of the secondary network. This interesting coupling between the performance of the two networks is studied using tools from game theory. We propose an algorithm that can assist the two networks to converge to Nash equilibrium. The convergence of this algorithm is verified using simulations. Overall, this paper is one of the few concrete works that symbiotically merge tools from stochastic geometry and game theory.

***Index Terms*— Stochastic geometry, wireless power transfer, physical layer security, game theory, coverage probability, Poisson point process, Poisson hole process.**

I. Introduction

OWING to rapid technological advances, wireless communication networks are undergoing unprecedented paradigm shifts. One of the most interesting amongst them is the attempt to make wireless networks virtually self-perpetual in terms of their energy requirements. This is especially gaining importance in internet-of-things (IoT) realm where it may not be economical to charge or replace batteries periodically in billions of devices worldwide [2]. In order to achieve this vision of self-perpetual operation, it is necessary to provide energy harvesting capability to such networks in addition to reducing energy expenditures through energy-efficient communication policies [3], [4] and energy efficient hardware [5]. While, in principle, we can use any available source of energy to power these networks, ambient RF energy harvesting is considered a preferred option due to its ubiquity [6]. Further, due to the need of deploying these ambient RF energy harvesting nodes/devices (referred to as *energy receivers* or ERs in the rest of this paper) close to the sources of RF signals, concerns on the secrecy of these RF signals were recently raised in the literature [7]–[13]. While the RF signal source (referred to as *primary transmitter* or PT in this paper) transmits confidential messages to legitimate *information receivers* (IRs), the existence of ERs close to the PT may enable them to decode these messages. Consequently, careful study of physical layer security in such systems is required to glean insights on the new secrecy performance limitations in the presence of ERs. The importance of physical layer security lies in ensuring the ability of legitimate receivers to decode the confidential messages while preventing illegitimate receivers from decoding these messages [14]. Many solutions were proposed to enhance physical layer security including: (i) using protected zones in order to ensure an eavesdropper-free regions around the transmitters [15], [16], (ii) using artificial noise in order to degrade the confidential signal's SNR at the energy receiver [9], [17], (iii) beamforming in multi-antenna systems [10]–[12], and (iv) using guard zones to stop information transmission whenever an eavesdropper is detected within a specific region around the transmitter [18], [19].

In this paper, we limit our attention to single-antenna transmitters and receivers, which means beamforming is not applicable to our setup. In addition, using protected zones assumes some physical control over the eavesdroppers, which will not be considered in this paper. Thus, we have two options to choose from: either use artificial noise or guard zones. In [20], it was recently shown that the guard zone technique outperforms the artificial noise technique in the noise limited regime when the link distance is higher than a specific threshold. No such performance comparison between the two techniques is known when interference is taken into account. Regardless, we focus on the guard zone technique

Manuscript received May 19, 2017; revised September 26, 2017; accepted November 21, 2017. Date of publication December 6, 2017; date of current version March 8, 2018. This work was supported by U.S. NSF under Grant CCF-1464293. This paper was presented in part at the IEEE WCNC, San Francisco, CA, USA, March 2017 [1]. The associate editor coordinating the review of this paper and approving it for publication was S. Wang. *(Corresponding author: Harpreet S. Dhillon.)*

The authors are with Wireless@VT, Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24061 USA (e-mail: mkishk@vt.edu; hdhillon@vt.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2017.2778703

in this paper while leaving the artificial noise technique as a promising direction of future work[1]. In particular, modeling the interaction between a primary network using guard zones to enhance secrecy and an IoT network using RF signals transmitted by the primary network to harvest energy is the main focus of this paper.

A. Related Work

In this subsection, we will provide a brief summary of the related works in four general directions of interest to this paper: (i) stochastic geometry-based analysis of secrecy and/or energy harvesting wireless networks, (ii) game theory-based analysis of secrecy and/or energy harvesting wireless networks, (iii) analysis of secrecy in IoT, and (iv) analysis of secure wireless power transmission.

1) Stochastic Geometry-Based Work: Stochastic geometry has emerged as a powerful mathematical tool for the modeling and analysis of variety of wireless networks [21]–[24]. Out of numerous aspects of wireless networks that have been studied using stochastic geometry, two that are most relevant to this paper are: (i) secrecy [18], [25], [26], and (ii) energy harvesting [27]–[31]. We first discuss the related works on secrecy. The work presented in [18] quantified the loss in network throughput that results from ensuring a specific level of secrecy performance. In addition, possible performance enhancement using guard zones was also studied. Authors in [25] studied the physical layer security of downlink cellular networks assuming that all the existing users in the network are potential cooperating eavesdroppers. In [26], authors studied the secrecy of downlink transmission when the transmitter adopts transmit antenna selection. In particular, they derived the secrecy outage probability for the cases of independent and cooperating eavesdroppers, considering both half and full duplex legitimate receivers.

Stochastic geometry has also been applied to analyze the performance of energy harvesting cellular networks with emphasis on either the downlink channel [27]–[29] or the uplink channel [30]. The work presented in [27] provided a comprehensive framework for analyzing heterogeneous cellular networks with energy harvesting base stations (BSs). The primary focus was on characterizing optimal transmission policies as well as quantifying the availability of different tiers of BSs. In [28] and [29], the joint analysis of the downlink signal quality and the amount of energy harvested at an RF-powered user was performed. In [30] and [31], the uplink counterpart of this problem was explored in which the RF-powered node first harvests energy from ambient RF signals and then uses it to perform data transmission. The work presented in [32] focused on the secrecy analysis of wireless networks where the legitimate transmitters are powered by energy harvesting. To the best of our knowledge, our work provides the first stochastic geometry-based secrecy analysis of wireless power transmission with energy receivers acting as potential eavesdroppers. More details will be provided shortly.

2) Game Theory-Based Work: Tools from game theory have been widely used in the analysis of secrecy in wireless networks [33]–[36]. Using these tools, in [33] authors modeled the interaction between cognitive networks and eavesdroppers, where a channel selection algorithm was proposed to reach the Nash equilibrium (NE). In [34], authors studied the problem of optimizing the uplink path in multi-hop networks in order to maximize the secrecy rate. In [35], authors used matching theory to develop an algorithm that enhances the secrecy of source-destination pairs using jamming nodes. In [36], authors proposed a distributed algorithm that enhances the achievable secrecy rates in wireless networks with cooperative wireless nodes.

These tools have also been used in the analysis of energy harvesting wireless networks. For instance, authors in [37] provided different approaches to manage energy trading among energy harvesting small cell BSs in order to minimize the consumption of non-renewable energy. Authors in [38] used theses tools to model the relay interference channels where the relay divides the received power from the source into two parts: (i) the first part is used to charge its own battery, and (ii) the rest of the received power is used to forward the received packet to its destination. In [39], these tools were used to determine optimal probability of switching from listen to active modes and from sleep to active modes for a solar powered wireless sensor network.

3) Analysis of Secrecy in IoT: Given the wide applications of IoT that require communication confidentiality (e.g. medical and military applications), communication security needs to be ensured in IoT. However, due to the limited processing power and their stringent energy constraints of the IoT devices, existing secrecy enhancing techniques might not always be useful in this paradigm [40]. Hence, there has been a lot of interest in devising physical layer security methods that have lower complexity and higher energy efficiency [41]–[44]. For instance, authors in [45] provide a comparison between existing secrecy enhancing techniques in terms of the computational complexity and energy efficiency in order to decide which is more suitable for using in the IoT paradigm. It can be noted that most of the existing literature on secrecy analysis of IoT focuses on safeguarding the IoT data from potential eavesdroppers. On the contrary, we study a system setup where the IoT devices are themselves acting as potential eavesdroppers for another coexisting wireless network.

4) Secure Wireless Power Transmission: While the idea of having the energy receiver as a potential eavesdropper has not been studied yet in the stochastic geometry literature (with randomly located ERs and legitimate transmitters), recent works have explored this idea for the deterministic system setups [7], [8], [46]–[48]. These works assume that the transmitter aims to maximize secrecy performance with the constraint of providing ERs with the required wireless power. In [7] and [8], authors focused on a single point-to-point link with one ER (potential eavesdropper) in the system. An artificial noise-based solution was proposed to improve secrecy without reducing the amount of wireless power received by the ER. In [46], authors studied the use of a friendly jammer to enhance the performance of the point-to-point system.

[1] Compared to the artificial noise technique, the main advantage of the guard zone technique from the perspective of the primary network is that it incentivizes the secondary network to reduce its deployment density in order to keep more PTs active so that the ERs can harvest sufficient RF energy. More details are provided in Sec. III-B.

The friendly jammer increases the amount of received power by the ER. In addition, it reduces the decodability of the confidential message by the ER. The single link system was extended in [47] to consider one multi-antenna transmitter, one legitimate receiver, and K ERs. Optimal beamforming schemes were provided to either maximize secrecy subject to constraints on harvested energy by the ERs or to maximize harvested energy by the ERs subject to secrecy constraints. Similar approach was adopted in [48] for a more general system model of one macro BS serving M users, N femto BSs each serving K users, and L ERs. Unlike all these works, we will model the locations of ERs and legitimate transmitters using point processes, which will enable us to draw general conclusions that will not be restricted to particular topologies.

In this paper, we study the secrecy performance of a primary network that consists of PTs and information receivers (which will also be referred to as primary receivers or PRs), overlaid with an IoT network that consists of RF-powered devices (energy receivers or ERs). Guard zones are assumed to be present around PTs in order to improve secrecy. The only sources of ambient RF signals for ERs are the PT transmissions. The PT transmits information (becomes *active*) to the PRs only when the guard zone is free of ERs, otherwise it remains silent. On one hand, the IoT network would prefer a dense deployment of ERs so as to increase the overall energy harvested by the IoT network. However, on the other hand, more dense deployment of ERs will mean that more PTs will stay silent (due to the higher likelihood of ERs lying in the guard zones of the PTs) that will ultimately reduce the amount of ambient RF energy harvested, and hence degrade energy harvesting performance. Modeling and analysis of this setup is the main focus of this paper. We summarize the contributions of this paper next.

B. Contributions

Compared to the existing works on secrecy of wireless power transmission, which is restricted to particular topologies where the number of PTs, PRs, and ERs are fixed, our paper assumes a more general setup. In particular, we assume a system of randomly located PTs and ERs which enables us to glean multiple insights on the effect of the system parameters on the coexistence of the two networks. In addition, unlike existing literature, we assume that there is no collaboration between the primary network and the secondary network. This means that the primary network's only objective is to enhance its secrecy performance, whereas, the secondary network's only objective is to enhance the energy harvesting performance. More details on each of our contributions are provided next.

1) Primary Network Performance Analysis: Modeling the locations of PTs and ERs by two independent Poisson point processes (PPPs), we show that the locations of *active* PTs (PTs with ER-free guard zones) follow Poisson hole process. For this setup, we define the probability of successful connection (P_{con}) between the PT and its associated PR by the joint probability of the PT being active and the SINR at the PR being above a predefined threshold. We derive P_{con} as a function of the density of ERs and the guard zone radius r_g. We concretely derive a threshold on the density of the PTs below which P_{con} is a decreasing function of r_g. Above this threshold, we prove the existence of an optimal value of r_g that maximizes P_{con}. For the secrecy analysis, we derive the probability of secure communication (defined by the probability of having the SINR value at any ER less than a predefined threshold). Referring to this metric as P_{sec}, we provide several useful insights on the effect of the PT transmission power as well as the density of ERs on the value of P_{sec}.

2) IoT Network Performance Analysis: For the IoT network (secondary network), we derive the probability of harvesting a minimum amount of energy $E_{\min}$ by the ERs. We define the density of ERs that satisfy this condition as the *density of successfully powered ERs*. We prove the existence of an optimal deployment density of ERs that maximizes this density of successfully powered ERs. In order to capture the relation between this optimal density and the guard zone radius, we derive a useful lower bound on the density of successfully powered ERs. We show that the optimal deployment density that maximizes this lower bound is a decreasing function of r_g. Although this conclusion is drawn using a lower bound, we use numerical results and simulations to demonstrate that it holds for the exact expressions as well.

3) Modeling the Interaction Between the Two Networks: Building on the above results, we show that the interaction between the two networks can be modeled using tools from game theory. In particular, we show that this system can be modeled by a two player non-cooperative static game. The first player is the primary network with the guard zone radius representing its strategy. Its utility function is modeled to capture the successful connection probability as well as the probability of secure communication. The second player is the IoT network with the deployment density representing its strategy. Its utility function is modeled to capture the main performance metric of this network, which is the density of successfully powered ERs. We find the NE for this game using the well-known best response-based learning algorithm.

II. System Model

We consider a system that is composed of two wireless networks: (i) a primary network, and (ii) an IoT network (will be referred to as secondary network in the rest of this paper). The primary network is constructed of PTs and primary receivers (will be referred to as either PRs or *legitimate receivers* interchangeably throughout the paper). The locations of the PTs are modeled by a homogeneous PPP $\Phi_P \equiv \{x_i\} \subset \mathbb{R}^2$ with density λ_P. In order to enhance secrecy performance, each PT is surrounded by a circular guard zone of radius r_g centered at the PT. We assume that each PT is able to detect the presence of any illegitimate receiver within its guard zone [49]. Various detecting devices can be used for this purpose including metal detectors and leaked local oscillator power detectors [15]. The benefits of using secrecy guard zones and their effect on secrecy performance were discussed in [18]. As shown in Fig. 1, before the PT transmits data to its associated PR, it scans the guard zone for any illegitimate

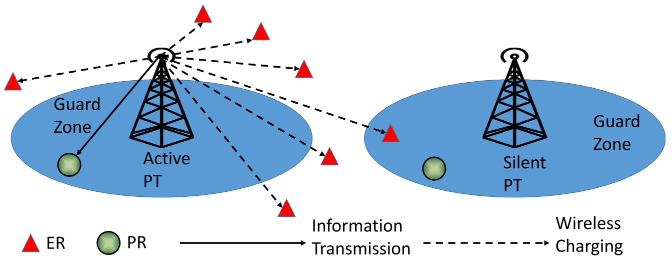

Fig. 1. The PT stops transmission (becomes silent) if any ER is detected within its guard zone.

receivers. If the guard zone is clear, the PT transmits the confidential data, otherwise, the PT stops transmission (becomes *silent*). The secondary network is constructed of RF-powered nodes that harvest RF energy from the signals transmitted by the primary network. We refer to these nodes as energy receivers (will be referred to as either ERs or *eavesdroppers* interchangeably throughout the paper). The locations of the ERs are modeled by a homogeneous PPP $\Phi_S \equiv \{y_i\} \subset \mathbb{R}^2$ with density λ_S. From the primary network's perspective, the ERs are considered illegitimate receivers. Hence, applying the guard zone scheme, the PT stops transmission whenever at least one ER exists within its guard zone. We assume that ERs are the only potential eavesdroppers in the system.

We focus our analysis on the typical PT whose intended PR is located at a given distance r_1 from the PT. Drawing analogy from the Poisson bipolar model, we call this the *typical link* and its constituent PT and PR as typical PT and typical PR, respectively. Note that this terminology is indeed rigorous if we assume a Poisson bipolar model in which *each* PT has an associated PR at a fixed distance. However, since the same setup can be used for cellular networks by treating r_1 as the *conditional* value of the serving distance, we leave the setup general. Overall, the assumption of fixed r_1 enables us to gain several useful insights. In particular, this enables us to better understand how the rest of the system parameters (e.g. r_g, λ_S, and PT's transmission power) affect the interaction between the two networks. Due to the stationarity of PPP, the typical PR can be assumed to be located at the origin without loss of generality. The typical PT is located at x_1 at distance $r_1 = \|x_1\|$ from the typical PR. In case the guard zone is clear of ERs, the typical PT transmits the confidential message to the typical PT. In that case, the received power at the typical PR is $P_t h_1 r_1^{-\alpha}$, where P_t is the PT transmission power, $h_1 \sim \exp(1)$ models Rayleigh fading gain, and $r_1^{-\alpha}$ models power law path-loss with exponent $\alpha > 2$.

A. Primary Network Modeling

According to Wyner's encoding scheme [14], [50] and the approach used in [18], the PT defines the rate of codewords and the rate of confidential messages, $C_{\rm t}$ and $C_{\rm s}$ respectively. The difference, $C_{\rm e} = C_{\rm t} - C_{\rm s}$, can be interpreted as the cost paid to secure the confidential messages. Let the mutual information between PT's channel input and PR's channel output be $I_{\rm t}$ and between PT's channel input and ER's channel output be $I_{\rm e}$. Then, the objective is to ensure that the following

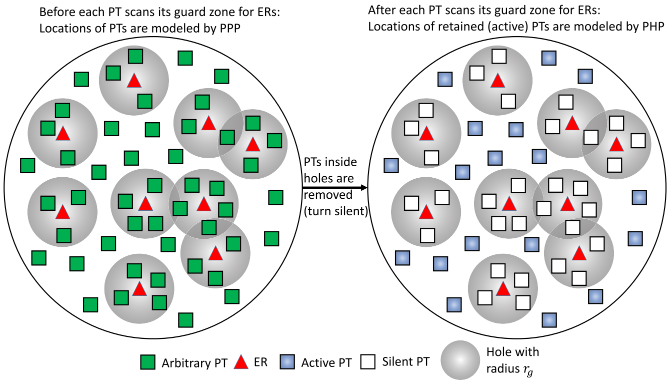
Before each PT scans its guard zone for ERs:
Locations of PTs are modeled by PPP
After each PT scans its guard zone for ERs:
Locations of retained (active) PTs are modeled by PHP
PTs inside holes are removed (turn silent)
Arbitrary PT
ER
Active PT
Silent PT
Hole with radius r_g

Fig. 2. The locations of active PTs is modeled by a PHP where the locations of ERs represent the centers of the holes.

two conditions are satisfied: (i) $C_{\rm t} \leq I_{\rm t}$ to ensure successful decoding at the PR, and (ii) $C_{\rm e} \geq I_{\rm e}$ to ensure perfect secrecy. Equivalently, we can define two SINR thresholds at the legitimate receiver and at the eavesdropper. To ensure successful decoding of the received confidential message at the PR, the condition $\text{SINR}_{\rm P} \geq \beta_P$ should be satisfied, where $\beta_P = 2^{C_{\rm t}} - 1$. Similarly, to ensure perfect secrecy, the SINR at any eavesdropper should satisfy the condition $\text{SINR}_{\rm S} < \beta_S$, where $\beta_S = 2^{C_{\rm t} - C_{\rm s}} - 1$. In order to mathematically define the instantaneous value of SINR at the legitimate receiver, we need to capture the effect of adopting the guard zone scheme on the interference level at the typical PR. According to the guard zone scheme, an interfering PT located at x_i is active only if its guard zone is clear of ERs. Hence, denoting the random variable representing the distance between the typical PT and its nearest eavesdropper by R_e, the probability of a typical PT being active is

$$P_{\rm active} = \mathbb{P}(R_e \geq r_g) = e^{-\lambda_S \pi {r_g}^2}. \tag{1}$$

Next, we formally define the value of SINR at the typical PR as

$$\text{SINR}_{\rm P} = \frac{P_t h_1 r_1^{-\alpha}}{\sum_{x_i \in \Phi_P \setminus x_1} \delta_i P_t h_i \|x_i\|^{-\alpha} + \sigma_P^2}, \tag{2}$$

where $h_i \sim \exp(1)$ models Rayleigh fading gain for the link between the typical PR and the PT located at x_i, and σ_P^2 is the noise power at the PRs. The indicator function δ_i is used to capture only the *active* interfering nodes. Hence, $\delta_i = 1$ if the PT located at x_i is active and equals zero otherwise. The expected value of δ_i is $\mathbb{E}[\delta_i] = P_{\rm acitve}$.

The locations of the active PTs can be modeled using Poisson hole process (PHP) Ψ [51], [52]. A PHP is constructed using two independent PPPs: (i) Baseline PPP Φ_1, and (ii) the PPP modeling the locations of the hole centers Φ_2. All points of Φ_1 that are within distance D from any point in Φ_2 are carved out. The remaining points of Φ_1 represent the PHP. In our system, as shown in Fig. 2, we can use the same approach to model the locations of the active PTs. Any PT in Φ_P that is within a distance r_g from any ER in Φ_S is inactive. Hence, the locations of the remaining (active) PTs are modeled by PHP. This can be formally defined as follows

$$\Psi = \left\{ x \in \Phi_P : x \notin \bigcup_{y \in \Phi_S} \mathcal{B}(y, r_g) \right\}, \tag{3}$$

where $\mathcal{B}(y, r_g)$ is a ball of radius r_g centered at y. Since the probability of retention of any point in Φ_P is P_{active}, the density of the resulting PHP Ψ is $\lambda_P P_{\text{acitve}}$.

The primary network tries to jointly optimize two main performance metrics: (i) successful connection probability, and (ii) secure communication probability. While the former is related to the successful delivery of the data from the PT to the PR, the latter is related to the security of the transmitted data when the PT is active. Both metrics are formally defined below.

Definition 1 (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_P. Therefore, the probability of successful connection is

$$P_{\text{con}}(r_g, \lambda_S) = \mathbb{P}(R_e \geq r_g, \text{SINR}_{\text{P}} \geq \beta_P). \tag{4}$$

When a PT is transmitting confidential data (active PT), the condition of $\text{SINR}_{\text{S}} \leq \beta_S$ needs to be satisfied at each ER in order to ensure perfect secrecy. Focusing on the signal transmitted by the typical PT, the SINR value at an ER located at y_j is

$$\text{SINR}_{\text{S}}(y_j) = \frac{P_t g_{1,j} \|x_1 - y_j\|^{-\alpha}}{\sum_{x_i \in \Phi_P \setminus x_1} \delta_i P_t g_{i,j} \|x_i - y_j\|^{-\alpha} + \sigma_S^2}, \tag{5}$$

where $g_{i,j} \sim \exp(1)$ models Rayleigh fading gain for the link between the PT located at x_i and the ER located at y_j, and σ_S^2 is the noise power at the ERs. We now define the second performance metric for the primary network, the secure communication probability, next.

Definition 2 (Secure Communication Probability): Given that a PT is active, the probability that its transmitted data is perfectly secured is

$$P_{\text{sec}}(r_g, \lambda_S) = \mathbb{E}\left[\mathbb{1}\left(\bigcap_{y_j \in \Phi_S} \text{SINR}_{\text{S}}(y_j) \leq \beta_S \middle| R_e \geq r_g \right) \right]. \tag{6}$$

For a given value of λ_S, the primary network selects the value of $r_g = r_g^*$ that maximizes the value of P_{con} while ensuring $P_{\text{sec}} \geq \epsilon$, where $0 < \epsilon \leq 1$. The selection of r_g^* is mathematically formulated next.

Definition 3 (Guard Zone Radius Selection): The primary network selects the guard zone radius r_g^* that satisfies the following

$$r_g^* = \arg \max_{r_g \in \mathcal{G}(\lambda_S)} P_{\text{con}}(r_g, \lambda_S),$$
$$\mathcal{G}(\lambda_S) = \{r_g : P_{\text{sec}}(r_g, \lambda_S) \geq \epsilon\}. \tag{7}$$

Remark 1: From Eq. 7, we note that the value of r_g^* selected by the primary network is a function of the density of the secondary network λ_S. In addition, while P_{active} is obviously a decreasing function of r_g, the exact effect of r_g on either P_{con} or P_{sec} is harder to describe than one expects. More detailed discussion is given in Remarks 3 and 5.

To better understand the behavior of all the aforementioned performance metrics, we will derive some insightful expressions that will, with the help of the numerical results, provide a complete picture for the effect of the system parameters on these metrics.

B. Secondary Network Modeling

For an ambient RF energy harvesting device, the distance to the nearest source is critical and has major effect on the average harvested energy value, as shown in [29]. The energy harvested from the nearest source is frequently used in the literature to study the performance of ambient RF energy harvesting wireless devices. For instance, in [53], authors proposed the concept of harvesting zone where an ER is able to activate its power conversion circuit and harvest energy only if it is within a specific distance from the active PT. Consequently, we focus our analysis of the energy harvested from the nearest PT since it is the dominant source of ambient RF energy. Hence, the energy harvested by the ER located at y_j is

$$E_H = \eta T P_t \|x_{j,1} - y_j\|^{-\alpha} w_j, \tag{8}$$

where η models the RF-DC efficiency of the ER, T is the duration of the transmission slot (assumed to be unity in the rest of the paper), $x_{j,1}$ is the location of the nearest active PT to the ER located at y_j, and $w_j \sim \exp(1)$ models Rayleigh fading gain for the link between the ER located at y_j and its nearest active PT. Most of the relevant existing works use one of two performance metrics for the anlysis of energy harvesting wireless networks: (i) the expected value of the harvested energy $\mathbb{E}[E_H]$ as in [31], or (ii) the energy coverage probability $\mathbb{P}(E_H \geq E_{\text{min}})$ as in [30], where E_{min} is the minimum required value of E_H at each ER. We will use a modified version of the latter metric. In order to maximize the density of ERs that harvest the minimum amount of energy E_{min}, the secondary network selects the network density $\lambda_S = \lambda_S^*$ that maximizes

$$P_{\text{energy}} = \lambda_S \mathbb{P}(E_H \geq E_{\text{min}}). \tag{9}$$

The above metric represents the *density of the successfully powered ERs*.

Remark 2: Note that the distance between an ER and its nearest active PT increases, on average, as the density of active PTs, $\lambda_P P_{\text{acitve}}$, decreases. Recalling, from Eq. 1, that P_{active} is a decreasing function of both r_g and λ_S, we can expect $\mathbb{P}(E_H \geq E_{\text{min}})$ to be a decreasing function of both r_g and λ_S. More detailed discussion will be presented in Remark 6.

From Remarks 1 and 2 we can get some initial observations on the coupling between the two networks. To better understand the relation between the parameters selected by each of the networks (r_g for the primary network, and λ_S for the secondary network), we first need to derive an expression for each of P_{con} and P_{sec} for the primary network, and P_{energy} for the secondary network.

III. Performance Analysis

A. Primary Network

1) Probability of Successful Connection: As stated earlier, for a given value of λ_S, the primary network selects the optimal guard zone radius r_g^* that maximizes P_{con} while ensuring that $P_{\text{sec}} \geq \epsilon$. The process of r_g selection was mathematically formulated in Definition 3. In the following Theorem we derive P_{con}.

Theorem 1 (Probability of Successful Connection): For a given value of λ_S, the probability of successful connection defined in Definition 1 is

$$P_{\text{con}}(r_g, \lambda_S) = \exp\left(-\left[\lambda_S \pi r_g^2 + \beta_P \frac{\sigma_P^2}{P_t} r_1^\alpha + \frac{2\pi^2 \lambda_P P_{\text{active}} \beta_P^{\frac{2}{\alpha}} r_1^2}{\alpha \sin(\frac{2}{\alpha}\pi)}\right]\right). \quad (10)$$

Proof: See Appendix A. ■

Remark 3: According to Definition 1 of P_{con}, the effect of r_g on P_{con} is two fold. On one hand, increasing the value of r_g decreases the probability of the PT being active, which decreases P_{con}. This effect appears in the first term in the exponent in Eq. 10. On the other hand, increasing the value of r_g decreases the density of active interferers. Hence, the probability of having SINR higher than β_P increases, which increases P_{con}. This effect appears in the third term in the exponent in Eq. 10 implicitly in the value of P_{active}.

To better understand the effect of r_g on P_{con}, we derive the value of $\hat{r}_g$ that maximizes P_{con} in the following Theorem.

Theorem 2: Defining $\mathcal{A}_1 = \frac{2\pi^2 \lambda_P \beta_P^{\frac{2}{\alpha}} r_1^2}{\alpha \sin(\frac{2}{\alpha}\pi)}$ then:

- *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 $\hat{r}_g = \sqrt{\frac{\ln(\mathcal{A}_1)}{\pi \lambda_S}}$.*

Proof: See Appendix B. ■

Remark 4: From the above Theorem, we conclude that when $\mathcal{A}_1 \leq 1$ the effect of r_g on the density of active interferers is negligible. This is consistent with intuition. Observing the expression of $\mathcal{A}_1$ in Theorem 2, we note that it is an increasing function of λ_P, β_P, and r_1. Hence, $\mathcal{A}_1 \leq 1$ results from one or more of the following conditions: (i) λ_P is too small to take the effect of interference into consideration (the system is noise limited), (ii) r_1 is too small such that the received signal power from the intended PT is hardly attenuated by the path-loss, and (iii) β_P is a very relaxed threshold. These three consequences of having $\mathcal{A}_1 \leq 1$ make the condition of $R_e \geq r_g$ in Definition 1 of P_{con} dominate the other condition of $\text{SINR}_\text{P} \geq \beta_P$. This eventually makes P_{con} a decreasing function of r_g, similar to $\mathbb{P}(R_e \geq r_g)$.

In the following corollary, an upper bound on the value of $P_{\text{con}}(r_g^*, \lambda_S)$ is provided.

Corollary 1: Using the result in Theorem 2, the value of $P_{\text{con}}(r_g^*, \lambda_S)$ is upper bounded as follows

$$P_{\text{con}}(r_g^*, \lambda_S) \leq P_{\text{con}}\left(\sqrt{\frac{\ln\left(\max\{\mathcal{A}_1, 1\}\right)}{\pi \lambda_S}}, \lambda_S\right), \quad (11)$$

where $\mathcal{A}_1$ is defined in Theorem 2.

Proof: The proof follows by observing that $\hat{r}_g$ is the value of r_g that maximizes P_{con} without any constraints, while r_g^* is the value of r_g that maximizes P_{con} with the constraint of $r_g \in \mathcal{G}(\lambda_S)$, as explained in Definition 3. ■

2) Secure Communication Probability: The secure communication probability, formally defined in Definition 2, is derived in the following theorem.

Theorem 3 (Secure communication probability): For a given value of r_g and λ_S, the probability of secure communication is $P_{\text{sec}}(r_g, \lambda_S) =$

$$\exp\left(-2\pi\lambda_S \int_{r_g}^{\infty} \exp\left(-\frac{\sigma_S^2 \beta_S r_y^\alpha}{P_t}\right) \mathcal{L}_{I_2}(\beta_S r_y^\alpha) r_y \mathrm{d}r_y\right), \quad (12)$$

where $\mathcal{L}_{I_2}(s) = \exp\left(-2\pi\lambda_P P_{\text{active}} \int_0^{s r_g^{-\alpha}} \frac{s^{\frac{2}{\alpha}}}{\alpha(1+z) z^{\frac{2}{\alpha}}} \mathrm{d}z\right)$.

Proof: See Appendix C. ■

Remark 5: The intuitive observations provided in Remark 1 can now be verified using Theorem 3. For instance, the effect of r_g on the distance between the PT and its nearest ER is captured in the integration limits in the above equation. Obviously, as we increase r_g, the integration interval will decrease, which increases the value of P_{sec}. On the other hand, the effect of r_g on the density of active interferers at the ER is captured in the term $\mathcal{L}_{I_2}(\beta_S r_y^\alpha)$. As we mentioned earlier, increasing the value of r_g decreases the interference levels at the ER, which increases the value of SINR_S*, which eventually reduces P_{sec}. This is verified here by observing that $\mathcal{L}_{I_2}(s)$ is an increasing function of r_g.*

Due to the complexity of the expression provided in Theorem 3 for P_{sec}, it is not straightforward to derive expressions for either $\mathcal{G}(\lambda_S)$ or r_g^*. However, using the results for P_{con} and P_{sec} in Theorems 1 and 3, it is easy to compute r_g^* numerically. In order to better understand the behavior of the system, we will provide expressions for P_{con} and P_{sec} in both noise-limited as well as interference-limited regimes. In the discussion section, results for both regimes will be compared with the results of the system at different values of r_g resulting in several meaningful insights. In the case of a noise limited regime, the interference terms in the expressions of both P_{con} and P_{sec} will be removed leading to the following corollary.

Corollary 2: In the noise limited regime, P_{con} will be a decreasing function of r_g, while P_{sec} will be an increasing function of r_g as follows

$$P_{\text{con}}^{\text{Noise limited}} = \exp\left(-\left[\lambda_S \pi r_g^2 + \beta_P \frac{\sigma_P^2}{P_t} r_1^\alpha\right]\right), \quad (13)$$

$$\begin{aligned} P_{\text{sec}}^{\text{Noise limited}} &= \exp\left(-2\pi\lambda_S \int_{r_g}^{\infty} \exp\left(-\frac{\sigma_S^2 \beta_S r_y^\alpha}{P_t}\right) r_y \mathrm{d}r_y\right) \\ &= \exp\left(-\frac{2\pi\lambda_S}{\alpha}\left(\frac{P_t}{\sigma_S^2 \beta_S}\right)^{\frac{2}{\alpha}} \Gamma\left(\frac{2}{\alpha}, \frac{r_g^\alpha \beta_S \sigma_S^2}{P_\text{t}}\right)\right). \end{aligned} \quad (14)$$

And the value of r_g^* is presented by the following equation

$$\Gamma\left(\frac{2}{\alpha}, \frac{(r_g^*)^\alpha \beta_S \sigma_S^2}{P_{\mathrm{t}}}\right) = \min\left\{\frac{\alpha \ln\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_S\left(\frac{P_t}{\sigma_S^2\beta_S}\right)^{\frac{2}{\alpha}}}, \Gamma\left(\frac{2}{\alpha}\right)\right\}. \tag{15}$$

Proof: Eq. 13 and 14 follow directly by removing the interference terms from the results in Theorem 1 and Theorem 3. Since $P_{\mathrm{con}}^{\mathrm{Noise\ limited}}$ is a decreasing function of r_g, and $P_{\mathrm{sec}}^{\mathrm{Noise\ limited}}$ is an increasing function of r_g, the primary network picks the minimum value of r_g that satisfies the condition $P_{\mathrm{sec}} \geq \epsilon$. Substituting for P_{sec} using Eq. 14 in the inequality $P_{\mathrm{sec}} \geq \epsilon$ leads to Eq. 15. ■

In the case of an interference-limited regime, the noise terms in the expressions of both P_{con} and P_{sec} will be ignored leading to the following corollary.

Corollary 3: In the interference limited regime, expressions for P_{con} and P_{sec} are provided below.

$$P_{\mathrm{con}}^{\mathrm{Int.\ limited}} = \exp\left(-\left[\lambda_S\pi r_g^2 + \frac{2\pi^2\lambda_P P_{\mathrm{active}}\beta_P^{\frac{2}{\alpha}} r_1^2}{\alpha\sin(\frac{2}{\alpha}\pi)}\right]\right), \tag{16}$$

$$P_{\mathrm{sec}}^{\mathrm{Int.\ limited}} = \exp\left(-2\pi\lambda_S\int_{r_g}^{\infty}\mathcal{L}_{I_2}(\beta_S r_x^\alpha) r_x \mathrm{d}r_x\right). \tag{17}$$

Proof: These results follow by substituting for $\sigma_P^2 = \sigma_S^2 = 0$ in Theorems 1 and 3. ■

The main take-away from this subsection is that each of P_{con} and P_{sec} are functions of λ_S, which consequently implies that r_g^* is a function of λ_S. In the next subsection, we will show that optimal density λ_S^* selected by the secondary network is also a function of r_g.

B. Secondary Network

The objective of the secondary network is to maximize the density of successfully powered ERs P_{energy}, introduced in Eq. 9, which is derived in the following Theorem.

Theorem 4 (Density of successfully powered ERs): For a given value of r_g and λ_S, the density of successfully powered ERs is

$$P_{\mathrm{energy}}(r_g, \lambda_S) = \lambda_S\int_{r_g}^{\infty} 2\pi\lambda_P P_{\mathrm{active}} r_p \times \exp\left(-\pi\lambda_P P_{\mathrm{active}}(r_p^2 - r_g^2) - \frac{E_{\min} r_p^\alpha}{P_t\eta}\right)\mathrm{d}r_p. \tag{18}$$

Proof: See Appendix D. ■

The above equation is a product of two terms: (i) the density of ERs λ_S, and (ii) the integral term, which is the expression derived for the probability $\mathbb{P}(E_H \geq E_{\min})$. Consequently, we can claim the existence of an optimal value of λ_S that maximizes the density of successfully powered ERs P_{energy}. The reason behind that is the dependence of the density of active sources of RF energy (active PTs) on the density of ERs. This interesting trade-off arises due to the use of secrecy guard zones by the primary network. Obviously, the value of P_{energy} is a function of r_g. Hence, the value of λ_S^*, that maximizes P_{energy}, is also a function of r_g. Unfortunately, λ_S^* can not be computed from the above expression due to its complexity. Hence, to get more insights on the relation between λ_S^* and r_g, we derive a lower bound on P_{energy} in the following corollary. We use this lower bound to compute λ_S^* as a function of r_g.

Corollary 4: The value of P_{energy} is lower bounded as follows

$$P_{\mathrm{energy}} \geq \lambda_S\int_{r_g}^{\infty} 2\pi\lambda_P P_{\mathrm{active}} r_p \times \exp\left(-\pi\lambda_P(r_p^2 - r_g^2) - \frac{E_{\min} r_p^\alpha}{P_t\eta}\right)\mathrm{d}r_p. \tag{19}$$

The value of λ_S that maximizes the lower bound is

$$\lambda_S^* = \frac{1}{\pi r_g^2}. \tag{20}$$

Proof: The lower bound follows by simply replacing P_{active} inside the exponent in Eq. 18 with unity. The value of λ_S^* follows by differentiating Eq. 19 with respect to λ_S. ■

Remark 6: It can be noted from Eq. 20 that the value of λ_S^* is a decreasing function of r_g. This agrees with intuition since when the value of r_g increases, the secondary network needs to decrease λ_S in order to maintain the density of active PTs, which are the sources of RF energy.

The mutual coupling between r_g^* and λ_S as well as λ_S^* and r_g can be best modeled using tools from game theory. This will be the core of the next section.

IV. Game Theoretical Modeling

Building on all the insights and comments given in the previous section, we can model the interaction between the two networks using tools from game theory. For a given value of λ_S, the primary network selects r_g^* as presented in Definition 3, which can be rewritten as

$$r_g^* = \arg\max_{r_g\geq 0} P_{\mathrm{con}}(r_g, \lambda_S)\mathbb{1}(P_{\mathrm{sec}}(r_g, \lambda_S) \geq \epsilon), \tag{21}$$

where $\mathbb{1}(\Xi) = 1$ if the condition Ξ is satisfied, and equals zero otherwise. On the other hand, for a given value of r_g, the secondary network selects λ_S^* as follows

$$\lambda_S^* = \arg\max_{\lambda_S\geq 0} P_{\mathrm{energy}}(r_g, \lambda_S). \tag{22}$$

Observing Eq. 21 and 22, it is fairly straightforward to see that the system setup can be modeled as a non-cooperative static game with two players: (i) the primary network is *player 1*, and (ii) the secondary network is *player 2*. The utility function of player 1 is

$$U_1(r_g, \lambda_S) = P_{\mathrm{con}}(r_g, \lambda_S)\mathbb{1}(P_{\mathrm{sec}}(r_g, \lambda_S) \geq \epsilon), \tag{23}$$

while the utility function of player 2 is

$$U_2(r_g, \lambda_S) = P_{\mathrm{energy}}(r_g, \lambda_S). \tag{24}$$

For this game, the main objective is to find the values of r_g^* and λ_S^* where each of the two networks has no tendency to change its tuning parameter. This is the definition of Nash equilibrium (NE). This can be mathematically modeled as

$$\begin{aligned} r_g^* &= \arg\max_{r_g \geq 0} \; P_{\rm con}(r_g, \lambda_S^*) \mathbb{1}(P_{\rm sec}(r_g, \lambda_S^*) \geq \epsilon), \\ \lambda_S^* &= \arg\max_{\lambda_S \geq 0} \; P_{\rm energy}(r_g^*, \lambda_S). \end{aligned} \tag{25}$$

Unfortunately, due to the complexity of the expressions of $P_{\rm con}$ in Theorem 1 and $P_{\rm sec}$ in Theorem 3, it is challenging to provide a closed-form solution for NE. However, based on the comments given in Remark 2 and the result in Theorem 2, we provide a learning algorithm that assists both networks to find NE. This algorithm is based on a simple best-response based algorithm [54]–[56]. In each iteration, each network updates its parameters according to the opponent's network parameter in the previous iteration. This can be mathematically presented as follows:

$$\begin{aligned} r_g^{(n)} &= r_g^* \left(\lambda_S^{(n-1)}\right), \\ \lambda_S^{(n)} &= \lambda_S^* \left(r_g^{(n-1)}\right), \end{aligned} \tag{26}$$

where $r_g^{(n)}$ and $\lambda_S^{(n)}$ are the outputs of the algorithm in the n-th iteration, $r_g^* \left(\lambda_S^{(n-1)}\right)$ is computed using Eq. 21 for $\lambda_S = \lambda_S^{(n-1)}$, and $\lambda_S^* \left(r_g^{(n-1)}\right)$ is computed using Eq. 22 for $r_g = r_g^{(n-1)}$. Assuming that the secondary network has a maximum possible deployment density, $\lambda_S \leq \lambda_{S,\max}$, the algorithm is provided next.

Algorithm 1 Proposed Algorithm for Finding the NE Network Parameters r_g^* and λ_S^*

```
input: $\lambda_P$, $\lambda_{S,\max}$, $\beta_P$, $\beta_S$, $P_t$, $\alpha$, $\eta$, and $E_{\min}$.
output: $r_g^*$, $\lambda_S^*$.
Initialization: $r_g^{(0)} = 0$ for all PTs in $\Phi_{\rm P}$, $\lambda_S^{(0)} = \lambda_{S,\max}$, and $n = 1$.
Repeat
    $r_g^{(n)} = r_g^* \left(\lambda_S^{(n-1)}\right)$
    $\lambda_S^{(n)} = \lambda_S^* \left(r_g^{(n-1)}\right)$
    $n = n + 1$
Until $r_g^{(n)} = r_g^{(n-1)}$ & $\lambda_S^{(n)} = \lambda_S^{(n-1)}$
```

Note that we assume the ability of each network to estimate perfectly the opponent's action in the previous iteration. Including the possibility of the estimation error and its effect on convergence is left as a promising direction of future work. In the next section, we will show using simulations the convergence of the proposed algorithm to the NE of the modeled game.

V. Results and Discussion

In this section, we will use both theoretical and simulation results (obtained from Monte-Carlo trials) to analyze the performance of both primary and secondary networks. The values of the system parameters used for the simulation setup are: $\lambda_P = 1$, $\eta = 0.75$, $E_{\min} = 10^{-4}$ Joules, $\alpha = 4$, $\lambda_{S,\max} = 2$, $P_t = 1$, $\beta_P = 3$ dB, $\beta_S = 0$ dB, $r_1 = 0.1$, and $\epsilon = 0.8$. The values of the rest of the parameters will be defined either on the figures or in their captions. We also refer to the SNR values at the primary and secondary receivers as $\gamma_P = \frac{P_t}{\sigma_S^2}$ and $\gamma_S = \frac{P_t}{\sigma_S^2}$ respectively. In addition, we define the ratio of λ_S to its maximum value by $\delta_S = \frac{\lambda_S}{\lambda_{S,\max}}$. Our main goals in this section are: (i) to validate the approximations used in our derivations, (ii) to get further insights on the behavior of both the networks, and (iii) to verify the comments provided in the Remarks throughout the paper. We first study the successful connection probability $P_{\rm con}$ in Fig. 3. First note that the simulation parameters chosen above are such that we get $\mathcal{A}_1 < 1$, where $\mathcal{A}_1$ is defined in Theorem 2. The results in Fig. 3 show that increasing the density of ERs decreases $P_{\rm con}$. Although increasing λ_S decreases the density of active interferers (which should increase $P_{\rm con}$), it also decreases the probability of the PT being active (which decreases $P_{\rm con}$). Ultimately, for this setup, $P_{\rm con}$ is a decreasing function of λ_S because of having $\mathcal{A}_1 < 1$. As explained in Remark 4, $\mathcal{A}_1 < 1$ leads to a noise limited system from the perspective of the successful connection probability, which means that the effect of λ_S on the density of active interferers is negligible compared to its effect on the probability of the PT being active. Further, note that because of having $\mathcal{A}_1 < 1$, $P_{\rm con}$ is also a decreasing function of r_g. As a result, r_g^* will be the minimum value of r_g that ensures $P_{\rm sec} \geq \epsilon$. The value of $P_{\rm sec}$ as a function of r_g is plotted in Fig. 4 for different values of γ_S. Consistent with the intuition, increasing γ_S decreases $P_{\rm sec}$. We also note that at low values of r_g the effect of γ_S is hardly noticeable, while at higher values of r_g, the effect of γ_S becomes significant. Furthermore, we note that r_g^* is an increasing function of γ_S. To better understand the effect of γ_S on the behavior of $P_{\rm sec}$, we plot in Fig. 5 the value of $P_{\rm sec}$ for both the noise limited and the interference limited regimes, which are derived in Corollary 2 and 3, respectively. These results lead to the following key insights:

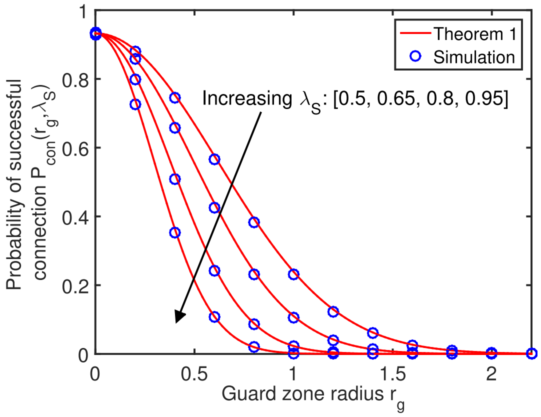

Fig. 3. The effect of λ_S on the behavior of $P_{\rm con}$ against different values of r_g. The SNR value at the legitimate receiver is $\gamma_P = 7$ dB.

- At lower values of r_g, the density of active interferers is relatively high. Hence, we observe that from the secure communication probability perspective, the system is interference limited in this regime. Furthermore, increasing the SNR value γ_S has a negligible effect. This is a

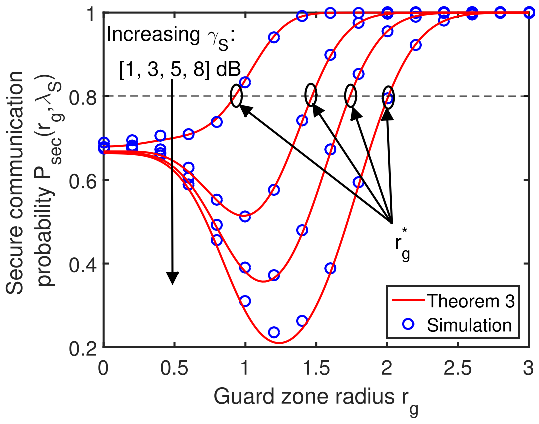

Fig. 4. The effect of γ_S on the behavior of P_{sec} against different values of r_g. The density of ERs is $\lambda_S = 0.6$.

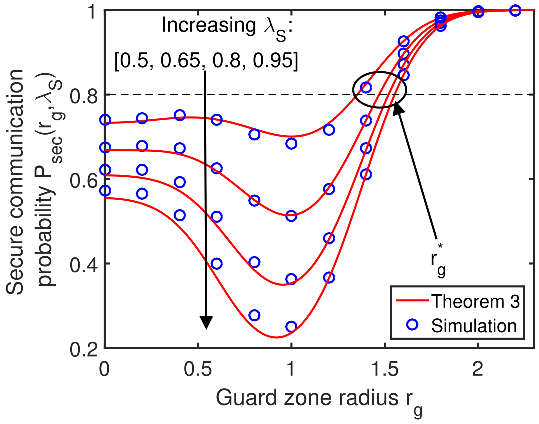

Fig. 6. The effect of λ_S on the behavior of P_{sec} against different values of r_g. The SNR value at ERs is $\gamma_S = 4.8$ dB.

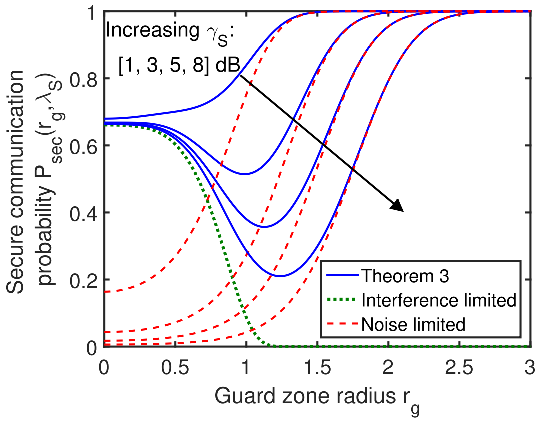

Fig. 5. Comparing P_{sec}, $P_{\text{sec}}^{\text{NoiseLimited}}$, and $P_{\text{sec}}^{\text{Int.Limited}}$ as functions of r_g for different values of γ_S. The density of ERs is $\lambda_S = 0.6$.

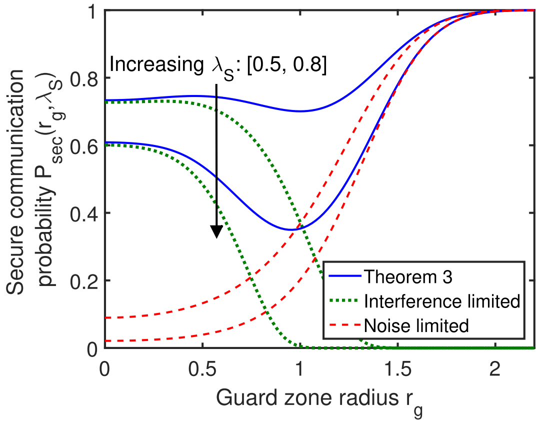

Fig. 7. Comparing P_{sec}, $P_{\text{sec}}^{\text{NoiseLimited}}$, and $P_{\text{sec}}^{\text{Int.Limited}}$ as functions of r_g for different values of λ_S. The SNR value at ERs is $\gamma_S = 4.8$ dB.

direct consequence of being in the interference-limited regime.

- At higher values of r_g, the density of active interferers decreases, which drives the system to the noise limited regime. As a result, the noise power has more noticeable effect on P_{sec}. Equivalently, increasing value of γ_S decreases the value of P_{sec} at higher values of r_g.
- Obviously, $P_{\text{sec}}^{\text{Int. Limited}}$ is a decreasing function of r_g, while $P_{\text{sec}}^{\text{Noise Limited}}$ is an increasing function of r_g. However, the behavior of P_{sec} is harder to describe. We note the existence of a local minimum of P_{sec} below which it behaves more like $P_{\text{sec}}^{\text{Int. Limited}}$, whereas above this local minimum, P_{sec} behaves similar to $P_{\text{sec}}^{\text{Noise Limited}}$.

In Fig. 6, we study the effect of λ_S on the behavior of P_{sec} against different values of r_g. We note that r_g^* increases with λ_S. We also note that, unlike γ_S, the effect of λ_S is more prominent at the lower values of r_g. As explained above, the reason is that the system is interference limited at lower values of r_g, where increasing λ_S decreases the density of interferers, which in turn decreases $P_{\text{sec}}^{\text{Int. Limited}}$. We plot P_{sec}, $P_{\text{sec}}^{\text{Int. Limited}}$, and $P_{\text{sec}}^{\text{Noise Limited}}$ in Fig. 7 to verify these arguments. We also note that at higher values of r_g, as we stated earlier, the system is noise limited, where λ_S has less effect on $P_{\text{sec}}^{\text{Noise Limited}}$ compared to $P_{\text{sec}}^{\text{Int. Limited}}$. This can be verified from Fig. 6 by observing that the gaps between the P_{sec} curves for different values of λ_S get tighter as r_g increases.

Now that we have better understanding of the behavior of P_{con} and P_{sec}, we study the energy harvesting performance of the secondary network. In Fig. 8, we illustrate the behavior of P_{energy} against λ_S for different values of r_g. We note that at lower values of r_g, the optimal value of λ_S is its maximum value $\lambda_{S,\text{max}}$. This is consistent with intuition that at lower values of r_g, the density of active PTs (sources of RF energy) will hardly get affected by increasing λ_S. As r_g increases, the impact of λ_S on the density of active PTs becomes noticeable. As shown in Fig. 8, this eventually leads to the existence of a local maximum of P_{energy}. We also note that as the value of r_g increases, the optimal value λ_S^* decreases. This is also consistent with our comments in Remark 6 that as r_g increases, the secondary network needs to decrease its density in order to maintain the density of active PTs that provide the RF energy to the ERs.

Taking a second look at Figs. 6 and 8, we can easily verify our earlier comments that the parameters selected by each of the networks (r_g for the primary network and λ_S for the secondary network) affect the value of the optimal parameter of the other network. Using the procedure provided in Sec. IV, we simulate the interaction between both networks

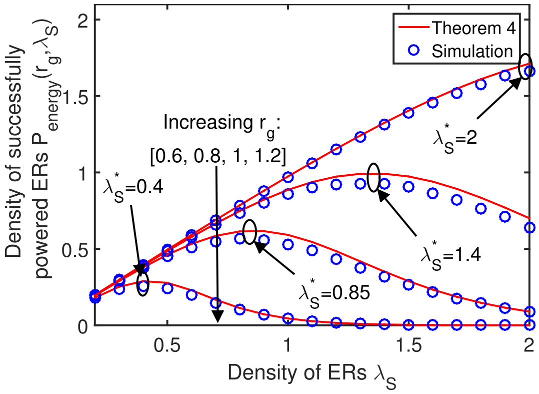

Fig. 8. The density of successfully powered ERs P_{energy} against λ_S for different values of r_g.

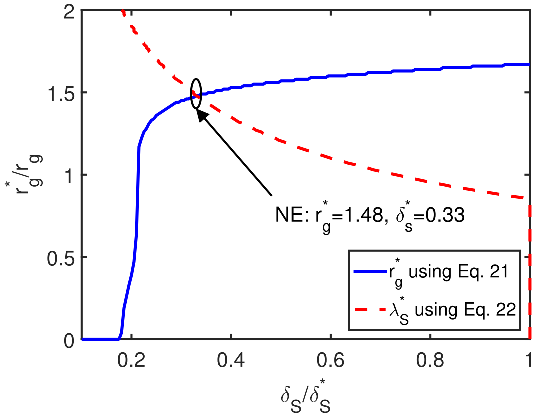

Fig. 9. Plotting both r_g^* against δ_S and δ_S^* against r_g on the same plot to compute the NE values.

by simulating the relations between r_g^* and δ_S as well as δ_S^* and r_g, where $\delta_S = \frac{\lambda_S}{\lambda_{S,\max}}$ is the normalized value of the density of ERs. In Fig. 9, we plot r_g^* (on the y-axis) for different values of δ_S (on the x-axis). On the same figure, we plot δ_S^* (on the x-axis) for different values of r_g (on the y-axis). The intersection of both curves represents the value of NE where each of the two networks has no intention to deviate as explained in Eq. 25. In Fig. 10, we evaluate the performance of the algorithm proposed in Sec. IV. The results demonstrate the convergence of the proposed algorithm to the NE found from Fig. 9 after less than 13 iterations. Further studies were also done on the effect of the value of λ_P on the convergence of the learning algorithm. The results showed that the number of iterations required to find the NE values increases from 11 to 13 as the value of λ_P increases from 0.2 to 1.

Due to the inherent intractability of energy coverage analysis when the locations of RF sources are modeled by a PHP, we focused on the energy harvested from the nearest active PT in this paper. This enabled us to provide some useful insights on the existence of an optimal density of IoT devices λ_S^* and the effect of r_g on λ_S^* as discussed in Corollary 4. That said, it is natural to ask how the conclusions would differ if we account for the energy harvested from all the active PTs (instead of just the nearest active PT). We perform this comparison in Fig. 11. In particular, we compare the values of the normalized optimal IoT density $\delta_S^* = \frac{\lambda_S^*}{\lambda_{S,\max}}$ for different values of r_g for two cases: (i) when the energy harvested only from the nearest active PT is considered (our analysis), and (ii) when the energy harvested from all active PTs is considered. For (i), we use the results from Theorem 4 of this paper, while for (ii), we rely on the commonly used approach of approximating PHP with a PPP of equivalent density and then we use the energy coverage expressions derived in [29]. Note that obtaining these plots for either of the two cases using brute-force simulations is prohibitively difficult. This is because for a given value of r_g, we would need to simulate the system for a very fine grid of values of δ_S in order to accurately approximate optimal δ_S^*. Further, for each value of tuple (δ_S, r_g), we need to average over sufficient number of PHP realizations, which are not as *easy* to generate as a homogeneous PPP. Regardless, we observe a surprisingly close match in the two cases, which shows that the conclusions and insights drawn from our analysis are not the artifacts of this assumption.

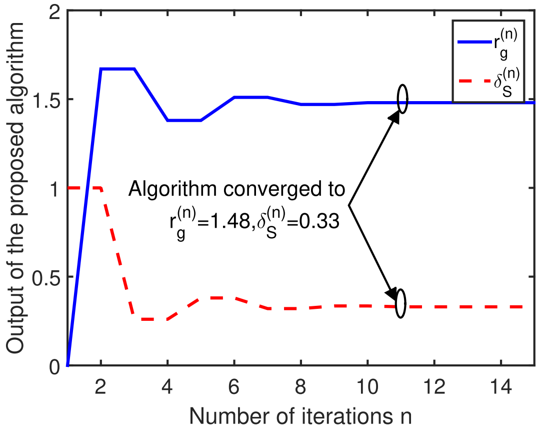

Fig. 10. The proposed algorithm converges to NE in a finite number of iterations.

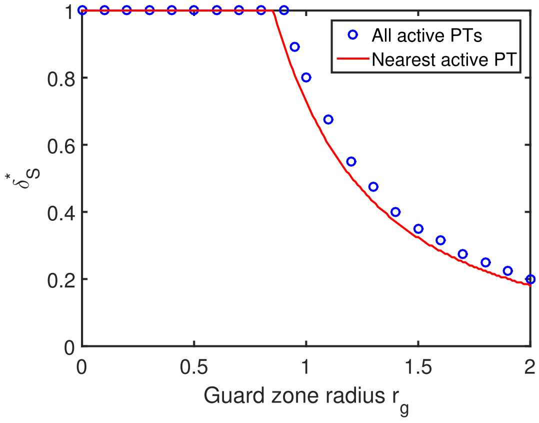

Fig. 11. Normalized optimal density δ_S^* against guard zone radius r_g for two cases: (i) when the energy harvested only from the nearest active PT is considered, and (ii) when energy harvested from all active PTs is considered.

VI. Conclusions and Future Work

The emergence of IoT regime is characterized by the deployment of billions of devices some of which may be equipped with energy harvesting capability. Due to the ubiquity of RF signals, harvesting energy from the ambient RF signals is perhaps the most attractive option for such devices.

This raises the possibility of some of these devices acting as eavesdroppers, which motivates the need to study secure wireless power transfer to energy receivers acting as potential eavesdroppers. While this problem received some attention in the literature, the existing works are limited to simple point-to-point or simple deterministic topologies, which are not sufficient to accurately model the massive scale of IoT. In this paper, we developed the first comprehensive stochastic geometry-based model to study the performance of an ambient RF energy harvesting network (secondary network) when the sources of RF signals are transmitters with secrecy guard zones (primary network). First, using tools from stochastic geometry, we derived the successful connection and secure communication probabilities of the primary network. Next, we derived the density of successfully powered nodes in the secondary network. Furthermore, we showed that the performance metrics of the two networks are coupled. In particular, we showed that the optimal guard zone radius (that maximizes the successful connection probability while maintaining the secure communication probability above a predefined threshold) is a function of the deployment density of the secondary network. In addition, we showed that the optimal deployment density of the secondary network (that maximizes the density of successfully powered nodes) is a function of the guard zone radius of the primary network. Hence, we used tools from game theory to model this interesting coupling between the two networks. In particular, we showed that such system can be modeled as a two player non-cooperative game. In addition, we used a best-response based algorithm and demonstrated with simulations its convergence to Nash equilibrium.

This paper is one of the few concrete works that symbiotically merge tools from stochastic geometry and game theory. It can be extended in many directions. From the secrecy perspective, it will be useful to extend the proposed model to incorporate other secrecy enhancing techniques, such as beamforming and artificial noise technique. From the modeling perspective, it is worthwhile to investigate other meaningful morphologies, such as the one in which ERs are clustered around the RF sources. From game theory perspective, it will be interesting to consider the effect of imperfect estimation of the opponent's action on the performance of the proposed algorithm.

One possible extension to this work is considering the communication between the IoT devices. Adding this new dimension to the system setup will lead to multiple new system insights. For instance, assuming an IoT device can be either in energy harvesting state or communication state, the interference caused by the IoT devices in the communication state will affect most of the performance metrics studied in this paper.

Appendix A
Proof of Theorem 1

Recalling the expression for SINR_P given in Eq. 2, 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 Ψ in Eq. 3. However, before using Ψ in our analysis, we need to make it clear that δ_i for different $x_i \in \Phi_P$ are correlated. This implicit correlation arises from the dependence of δ_i for all i on the PPP Φ_S. However, capturing this correlation in our analysis will significantly reduce the tractability of the results. Hence, this correlation will be ignored in our analysis for the sake of tractability. The tightness of this approximation will be verified in the Numerical Results section. Now revisiting the expression of P_con in Eq. 4, 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_P is the only source of correlation between the events $(R_e \geq r_g)$ and $(\text{SINR}_\text{P} \geq \beta_P)$. Hence, ignoring this correlation will lead to the following

$$P_\text{con} = \mathbb{P}(R_e \geq r_g)\mathbb{P}(\text{SINR}_\text{P} \geq \beta_P). \tag{27}$$

The first term in the above expression represents $P_\text{active} = \exp\left(-\pi \lambda_S r_g^2\right)$ (please recall Eq. 1 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 $\{\delta_i\}$, for the sake of tractability as explained above, is equivalent to approximating the PHP Ψ with a PPP Ψ_P of equivalent density $\tilde{\lambda}_P = \lambda_P P_\text{active}$. Defining $I = \sum_{x_i \in \Psi_P} h_i \|x_i\|^{-\alpha}$, then

$$\begin{aligned}\mathbb{P}(\text{SINR}_\text{P} \geq \beta_P) &= \mathbb{P}\left(\frac{h_1 r_1^{-\alpha}}{I + \frac{\sigma_P^2}{P_t}} \geq \beta_P\right)\\ &\overset{(a)}{=} \mathbb{E}_I\left[\exp\left(-\beta_P\left(I + \frac{\sigma_P^2}{P_t}\right)r_1^\alpha\right)\right]\\ &= \exp\left(-\beta_P \frac{\sigma_P^2}{P_t} r_1^\alpha\right)\mathbb{E}_I\left[\exp\left(-\beta_P I r_1^\alpha\right)\right]\\ &\overset{(b)}{=} \exp\left(-\beta_P \frac{\sigma_P^2}{P_t} r_1^\alpha\right)\mathcal{L}_I\left(\beta_P r_1^\alpha\right),\end{aligned} \tag{28}$$

where $h_1 \sim \exp(1)$ leads to step (a), and in step (b) we use the definition of Laplace transform of I which is $\mathcal{L}_I(s) = \mathbb{E}\left[\exp\left(-sI\right)\right]$. The Laplace transform of the interference in PPP is a well established result in the literature [23]. For completeness, the derivation of $\mathcal{L}_I(s)$ is provided next.

$$\begin{aligned}\mathcal{L}_I(s) &= \mathbb{E}_{\Psi_P,\{h_i\}}\left[\exp\left(-s\sum_{x_i \in \Psi_P} h_i \|x_i\|^{-\alpha}\right)\right]\\ &= \mathbb{E}_{\Psi_P,\{h_i\}}\left[\prod_{x_i \in \Psi_P} \exp\left(-s h_i \|x_i\|^{-\alpha}\right)\right]\\ &\overset{(c)}{=} \mathbb{E}_{\Psi_P}\left[\prod_{x_i \in \Psi_P} \frac{1}{1 + s\|x_i\|^{-\alpha}}\right]\\ &\overset{(d)}{=} \exp\left(-\tilde{\lambda}_P \int_{x \in \mathbb{R}^2} 1 - \frac{1}{1 + s\|x\|^{-\alpha}} \mathrm{d}x\right)\\ &\overset{(e)}{=} \exp\left(-2\pi\tilde{\lambda}_P \int_0^\infty \frac{s r_x^{-\alpha}}{1 + s r_x^{-\alpha}} r_x \mathrm{d}r_x\right)\\ &\overset{(f)}{=} \exp\left(-\frac{2\pi^2 \tilde{\lambda}_P s^{\frac{2}{\alpha}} \csc\left(\frac{2\pi}{\alpha}\right)}{\alpha}\right),\end{aligned} \tag{29}$$

where knowing that the set of fading gains h_i are i.i.d with $h_i \sim \exp(1)$ leads to step (c), step (d) results from using the probability generating function (PGFL) of PPP [24], step (e) results from converting to polar co-ordinates, and step (f) follows after some mathematical manipulations. Substituting Eq. 29 in Eq. 28 and then in Eq. 27 leads to the final result in Theorem 1.

Appendix B
Proof of Theorem 2

Observing the expression of P_{con} in Theorem 1, we note that it can be rewritten as a function of $P_{\text{active}} = \exp(-\lambda_S \pi r_g^2)$ as follows

$$P_{\text{con}} = \exp\left(-\beta_P \frac{\sigma_P^2}{P_t} r_1^{\alpha}\right) P_{\text{active}} \exp\left(-P_{\text{active}} \mathcal{A}_1\right), \quad (30)$$

where $\mathcal{A}_1 = \frac{2\pi^2 \lambda_P \beta_P^{\frac{2}{\alpha}} r_1^2}{\alpha \sin(\frac{2}{\alpha}\pi)}$. 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 Eq. 1), 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 $1 - \mathcal{A}_1 P_{\text{active}} \leq 0$, then P_{con} is an increasing function of r_g.

Consequently, we can infer that, since $0 \leq P_{\text{acitve}} \leq 1$, 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 $r_g \leq \sqrt{\frac{\ln(\mathcal{A}_1)}{\lambda_S \pi}}$), and (ii) P_{con} is a decreasing function of r_g as long as $P_{\text{active}} \leq \frac{1}{\mathcal{A}_1}$ (or $r_g \geq \sqrt{\frac{\ln(\mathcal{A}_1)}{\lambda_S \pi}}$). This concludes the proof.

Appendix C
Proof of Theorem 3

From Definition 2 of P_{sec}, we observe that we need to jointly analyze the values of $\text{SINR}_\text{S}(y_j)$ at all the locations $y_j \in \Phi_S$. 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 $\text{SINR}_\text{S}(y_j)$, by definition, on the PPP Φ_P for all $y_j \in \Phi_S$. Some recent works started working on characterizing the correlation between intereference levels at different locations [57]. 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 will not be useful for 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_S increases. This is due to the fact that the distances between ERs decrease as λ_S increases, which was shown in [57] 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. $x_1 = o$, in the rest of this proof. All the analysis provided in this section is conditioned on the event $R_e \geq r_g$. Following the same approach as in Appendix A of approximating the PHP Ψ with a PPP Ψ_P, and defining $I_2(y_j) = \sum_{x_i \in \Psi_P \setminus x_1} g_{i,j} \|x_i - y_j\|^{-\alpha}$, P_{sec} can be derived as follows

$$\begin{aligned} P_{\text{sec}} &= \mathbb{E}_{\Phi_S, I_2, \{g_{1,j}\}}\left[\mathbb{1}\left(\bigcap_{y_j \in \Phi_S} \frac{g_{1,j}\|y_j\|^{-\alpha}}{I_2(y_j) + \frac{\sigma_S^2}{P_t}} \leq \beta_S\right)\right] \\ &\overset{(g)}{=} \mathbb{E}_{\Phi_S, I_2, \{g_{1,j}\}}\left[\prod_{y_j \in \Phi_S} \mathbb{1}\left(\frac{g_{1,j}\|y_j\|^{-\alpha}}{I_2(y_j) + \frac{\sigma_S^2}{P_t}} \leq \beta_S\right)\right] \\ &\overset{(h)}{=} \mathbb{E}_{\Phi_S, I_2}\left[\prod_{y_j \in \Phi_S}\left(1 - \exp\left(-\frac{\beta_S\left(I_2(y_j) + \frac{\sigma_S^2}{P_t}\right)}{\|y_j\|^{-\alpha}}\right)\right)\right] \\ &\overset{(i)}{=} \mathbb{E}_{\Phi_S}\Bigg[\prod_{y_j \in \Phi_S}\Bigg(1 - \exp\left(-\frac{\beta_S\left(\frac{\sigma_S^2}{P_t}\right)}{\|y_j\|^{-\alpha}}\right) \\ &\quad \times \mathbb{E}\left[\exp\left(-\frac{\beta_S I_2(y_j)}{\|y_j\|^{-\alpha}}\right)\right]\Bigg)\Bigg], \end{aligned} \quad (31)$$

where step (g) (and step (i)) follow from assuming that the values of $\text{SINR}_\text{S}(y_j)$ (and $I_2(y_j)$) are uncorrelated, as we discussed earlier in this Appendix. 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 $I_2(y_j)$ by $\mathcal{L}_{I_2(y_j)}(s) = \mathbb{E}[\exp(-s I_2(y_j))]$, we note that there is only one difference in the derivation of $\mathcal{L}_{I_2(y_j)}(s)$ compared to that of $\mathcal{L}_I(s)$ in Eq. 29. The difference is in the reference point from where we are observing the interference. In Appendix A, 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 ER, which has a minimum distance of r_g from any active interfering PT. Hence, the derivation of $\mathcal{L}_{I_2(y_j)}(s)$ will be exactly the same as in Eq. 29 until step (e), where the minimum distance effect will appear in the lower limit of the integral as follows

$$\mathcal{L}_{I_2(y_j)}(s) = \exp\left(-2\pi\tilde{\lambda}_P \int_{r_g}^{\infty} \frac{s r_x^{-\alpha}}{1 + s r_x^{-\alpha}} r_x \mathrm{d}r_x\right). \quad (32)$$

Note that the above expression is not a function of y_j, so we drop it from the notation of Laplace transform. The final expression for $\mathcal{L}_{I_2}(s)$ as provided in Theorem 3 follows after simple mathematical manipulations. Substituting Eq. 32 in Eq. 31, we get

$$\begin{aligned} P_{\text{sec}} &= \mathbb{E}_{\Phi_S}\Bigg[\prod_{y_j \in \Phi_S}\Bigg(1 - \exp\left(-\beta_S\left(\frac{\sigma_S^2}{P_t}\right)\|y_j\|^{\alpha}\right) \\ &\qquad \times \mathcal{L}_{I_2}\left(\beta_S\|y_j\|^{\alpha}\right)\Bigg)\Bigg] \\ &\overset{(k)}{=} \exp\Bigg(-2\pi\lambda_S \int_{y \in \mathbb{R}^2 \cap \mathcal{B}^c(o, r_g)} \exp\left(-\beta_S\left(\frac{\sigma_S^2}{P_t}\right)\|y\|^{\alpha}\right) \\ &\qquad \times \mathcal{L}_{I_2}\left(\beta_S\|y\|^{\alpha}\right)\mathrm{d}y\Bigg), \end{aligned} \quad (33)$$

where step (k) results from applying PGFL of PPP, and the integration is over $y \in \mathbb{R}^2 \cap \mathcal{B}^c(o, r_g)$ because the analysis in this section is conditioned on the event $R_e \geq r_g$, 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 3.

Appendix D
Proof of Theorem 4

The density of successfully powered ERs can be derived as follows

$$P_{\text{energy}} = \lambda_S \mathbb{P}\left(\eta P_t R_p^{-\alpha} w \geq E_{\min}\right) \overset{(l)}{=} \mathbb{E}_{R_p}\left[\exp\left(-\frac{E_{\min} R_p^{\alpha}}{\eta P_t}\right)\right], \quad (34)$$

where R_p is the distance between the ER and its nearest active PT, and step (l) is due to $w \sim \exp(1)$. 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 Ψ with a PPP Ψ_P is known to provide fairly tight approximation of the contact distance distribution of PHP [58]. Given that the nearest active PT to the ER is at a distance of at least r_g, the distribution of R_p is

$$f_{R_p}(r_p) = 2\pi \tilde{\lambda}_P \exp\left(-\pi \tilde{\lambda}_P (r_p - r_g)^2\right), \quad r_p \geq r_g. \quad (35)$$

Using this distribution to compute the expectation in Eq. 34 leads to the final result in Theorem 4.

References

[1] M. A. Kishk and H. S. Dhillon, "Modeling and analysis of ambient RF energy harvesting in networks with secrecy guard zones," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.

[2] H. S. Dhillon, H. Huang, and H. Viswanathan, "Wide-area wireless communication challenges for the Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 168–174, Feb. 2017.

[3] H. S. Dhillon, H. C. Huang, H. Viswanathan, and R. A. Valenzuela, "Power-efficient system design for cellular-based machine-to-machine communications," *IEEE Trans. Wireless Commun.*, vol. 12, no. 11, pp. 5740–5753, Nov. 2013.

[4] H. S. Dhillon, H. C. Huang, H. Viswanathan, and R. A. Valenzuela, "Fundamentals of throughput maximization with random arrivals for M2M communications," *IEEE Trans. Wireless Commun.*, vol. 62, no. 11, pp. 4094–4109, Nov. 2014.

[5] V. Jelicic, M. Magno, D. Brunelli, V. Bilas, and L. Benini, "Analytic comparison of wake-up receivers for WSNs and benefits over the wake-on radio scheme," in *Proc., ACM Workshop Perform. Monitor. Meas. Heterogeneous Wireless Wired Netw.*, Oct. 2012, pp. 99–106.

[6] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, "Wireless energy harvesting for the Internet of Things," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 102–108, Jun. 2015.

[7] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 180–190, Jan. 2016.

[8] Q. Li, W.-K. Ma, and A. M.-C. So, "Robust artificial noise-aided transmit optimization for achieving secrecy and energy harvesting," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, May 2014, pp. 1596–1600.

[9] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3085–3096, Apr. 2016.

[10] M. R. Khandaker and K.-K. Wong, "Robust secrecy beamforming with energy-harvesting eavesdroppers," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 10–13, Feb. 2015.

[11] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[12] J. Xu, L. Liu, and R. Zhang, "Multiuser MISO beamforming for simultaneous wireless information and power transfer," *IEEE Trans. Signal Process.*, vol. 62, no. 18, pp. 4798–4810, Sep. 2014.

[13] K. Banawan and S. Ulukus, "MIMO wiretap channel under receiver-side power constraints with applications to wireless power transfer and cognitive radio," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3872–3885, Sep. 2016.

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

[15] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1617–1628, Oct. 2014.

[16] W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6146–6158, Aug. 2016.

[17] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[18] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[19] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[20] M. A. Kishk and H. S. Dhillon, "Stochastic geometry-based comparison of secrecy enhancement techniques in D2D networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 394–397, Jun. 2017.

[21] H. Elsawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 996–1019, 3rd Quart., 2013.

[22] H. ElSawy, A. Sultan-Salem, M. S. Alouini, and M. Z. Win, "Modeling and analysis of cellular networks using stochastic geometry: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 167–203, 1st Quart., 2017.

[23] J. G. Andrews, A. K. Gupta, and H. S. Dhillon. (2016). "A primer on cellular network analysis using stochastic geometry." [Online]. Available: https://arxiv.org/abs/1604.03183

[24] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[25] 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, Jun. 2014.

[26] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1195–1206, May 2017.

[27] H. S. Dhillon, Y. Li, P. Nuggehalli, Z. Pi, and J. G. Andrews, "Fundamentals of heterogeneous cellular networks with energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2782–2797, May 2014.

[28] M. Di Renzo and W. Lu, "System-level analysis and optimization of cellular networks with simultaneous wireless information and power transfer: Stochastic geometry modeling," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2251–2275, Mar. 2017.

[29] M. A. Kishk and H. S. Dhillon, "Downlink performance analysis of cellular-based IoT network with energy harvesting receivers," in *Proc. IEEE GLOBECOM*, Dec. 2016.

[30] A. H. Sakr and E. Hossain, "Analysis of K-tier uplink cellular networks with ambient RF energy harvesting," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2226–2238, Oct. 2015.

[31] I. Flint, X. Lu, N. Privault, D. Niyato, and P. Wang, "Performance analysis of ambient RF energy harvesting with repulsive point process modeling," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5402–5416, Oct. 2015.

[32] Y. Liu, L. Wang, S. A. R. Zaidi, M. Elkashlan, and T. Q. Duong, "Secure D2D communication in large-scale cognitive cellular networks: A wireless power transfer model," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 329–342, Jan. 2016.

[33] A. Houjeij, W. Saad, and T. Bascar, "A game-theoretic view on the physical layer security of cognitive radio networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2013, pp. 2095–2099.

[34] W. Saad, X. Zhou, B. Maham, T. Basar, and H. V. Poor, "Tree formation with physical layer security considerations in wireless multi-hop networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3980–3991, Nov. 2012.

[35] S. Bayat, R. H. Y. Louie, Z. Han, B. Vucetic, and Y. Li, "Physical-layer security in distributed wireless networks using matching theory," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 5, pp. 717–732, May 2013.

[36] W. Saad, Z. Han, T. Başar, M. Debbah, and A. Hjørungnes, "Distributed coalition formation games for secure wireless transmission," *Mobile Netw. Appl.*, vol. 16, no. 2, pp. 231–245, Apr. 2011.

[37] N. Reyhanian, B. Maham, V. Shah-Mansouri, W. Tushar, and C. Yuen, "Game-theoretic approaches for energy cooperation in energy harvesting small cell networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7178–7194, Aug. 2017.

[38] H. Chen, Y. Li, Y. Jiang, Y. Ma, and B. Vucetic, "Distributed power splitting for SWIPT in relay interference channels using game theory," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 410–420, Jan. 2015.

[39] D. Niyato, E. Hossain, M. M. Rashid, and V. K. Bhargava, "Wireless sensor networks with energy harvesting technologies: A game-theoretic approach to optimal energy management," *IEEE Wireless Commun.*, vol. 14, no. 4, pp. 90–96, Aug. 2007.

[40] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things," *IEEE Security Privacy*, vol. 13, no. 1, pp. 14–21, Jan. 2015.

[41] A. Soni, R. Upadhyay, and A. Jain, *Internet of Things and Wireless Physical Layer Security: A Survey*. Singapore: Springer, 2017, pp. 115–123.

[42] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl. (SOCA)*, Nov. 2014, pp. 230–234.

[43] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2014, pp. 417–423.

[44] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Security*, Dec. 2013, pp. 663–667.

[45] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[46] M. Liu and Y. Liu, "Power allocation for secure SWIPT systems with wireless-powered cooperative jamming," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1353–1356, Jun. 2017.

[47] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Apr. 2014.

[48] Y. Ren, T. Lv, H. Gao, and Y. Li, "Secure wireless information and power transfer in heterogeneous networks," *IEEE Access*, vol. 5, pp. 4967–4979, 2017.

[49] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.

[50] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[51] Z. Yazdanshenasan, H. S. Dhillon, M. Afshang, and P. H. J. Chong, "Poisson hole process: Theory and applications to wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7531–7546, Nov. 2016.

[52] C.-H. Lee and M. Haenggi, "Interference and outage in Poisson cognitive networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 4, pp. 1392–1401, Apr. 2012.

[53] S. Lee, R. Zhang, and K. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, pp. 4788–4799, Sep. 2013.

[54] W. H. Sandholm, *Population Games and Evolutionary Dynamics*. Cambridge, MA, USA: MIT Press, 2010.

[55] A. Cortes and S. Martinez, "Self-triggered best-response dynamics for continuous games," *IEEE Trans. Autom. Control*, vol. 60, no. 4, pp. 1115–1120, Apr. 2015.

[56] E. N. Barron, R. Goebel, and R. R. Jensen, "Best response dynamics for continuous games," *Proc. Amer. Math. Soc.*, vol. 138, no. 3, pp. 1069–1083, 2010.

[57] S. Krishnan and H. S. Dhillon, "Spatio-temporal interference correlation and joint coverage in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 5659–5672, Sep. 2017.

[58] M. A. Kishk and H. S. Dhillon, "Tight lower bounds on the contact distance distribution in poisson hole process," *IEEE Wireless Commun. Lett.*, vol. 6, no. 4, pp. 454–457, Aug. 2017.

Mustafa A. Kishk (S'16) received the B.Sc. and M.Sc. degrees in electronics and electrical communications engineering from Cairo University, Egypt, in 2013 and 2015, respectively. He is currently pursuing the Ph.D. degree with the Bradley Department of Electrical and Computer Engineering, Virginia Tech. His research interests include stochastic geometry, energy harvesting wireless networks, and physical layer security.

Harpreet S. Dhillon (S'11–M'13) received the B.Tech. degree in Electronics and Communication Engineering from IIT Guwahati, India, in 2008; the M.S. degree in Electrical Engineering from Virginia Tech, Blacksburg, VA, USA, in 2010; and the Ph.D. degree in Electrical Engineering from the University of Texas at Austin, TX, USA, in 2013. In academic year 2013-14, he was a Viterbi Postdoctoral Fellow at the University of Southern California, Los Angeles, CA, USA. He joined Virginia Tech in August 2014, where he is currently an Assistant Professor of Electrical and Computer Engineering. He has held internships at Alcatel-Lucent Bell Labs in Crawford Hill, NJ, USA; Samsung Research America in Richardson, TX, USA; Qualcomm Inc. in San Diego, CA, USA; and Cercom, Politecnico di Torino in Italy. His research interests include communication theory, stochastic geometry, geolocation, and wireless *ad hoc* and heterogeneous cellular networks.

Dr. Dhillon is a Clarivate Analytics Highly Cited Researcher and has coauthored five best paper award recipients including the 2016 IEEE Communications Society (ComSoc) Heinrich Hertz Award, the 2015 IEEE ComSoc Young Author Best Paper Award, the 2014 IEEE ComSoc Leonard G. Abraham Prize, and two conference best paper awards at IEEE ICC 2013 and European Wireless 2014. His other academic honors include the 2017 Outstanding New Assistant Professor Award from the Virginia Tech College of Engineering, the 2013 UT Austin Wireless Networking and Communications Group (WNCG) leadership award, the UT Austin Microelectronics and Computer Development (MCD) Fellowship, and the 2008 Agilent Engineering and Technology Award. He currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, and the IEEE WIRELESS COMMUNICATIONS LETTERS.