Coverage, Secrecy, and Stability Analysis of Energy Harvesting Wireless Networks

Mustafa A. Kishk

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in Electrical Engineering

Harpreet S. Dhillon, Chair
Allen B. Mackenzie
Walid Saad
Anil Vullikanti
Zhenyu Kong

June 14, 2018
Blacksburg, Virginia

Keywords: Energy harvesting wireless communication, Poisson point process, Poisson hole process, physical layer security

Coverage, Secrecy, and Stability Analysis of Energy Harvesting Wireless Networks

Mustafa A. Kishk

(ABSTRACT)

Including energy harvesting capability in a wireless network is attractive for multiple reasons. First and foremost, powering base stations with renewable resources could significantly reduce their reliance on the traditional energy sources, thus helping in curtailing the carbon footprint. Second, including this capability in wireless devices may help in increasing their lifetime, which is especially critical for devices for which it may not be easy to charge or replace batteries. This will often be the case for a large fraction of sensors that will form the *digital skin* of an Internet of Things (IoT) ecosystem. Motivated by these factors, this work studies fundamental performance limitations that appear due to the inherent unreliability of energy harvesting when it is used as a primary or secondary source of energy by different elements of the wireless network, such as mobile users, IoT sensors, and/or base stations.

The first step taken towards this objective is studying the joint uplink and downlink coverage of radio-frequency (RF) powered cellular-based IoT. Modeling the locations of the IoT devices and the base stations (BSs) using two independent Poisson point processes (PPPs), the joint uplink/downlink coverage probability is derived. The resulting expressions characterize how different system parameters impact coverage performance. Both mathematical expressions and simulation results show how these system parameters should be tuned in order to achieve the performance of the regularly powered IoT (IoT devices are powered by regular batteries).

The placement of RF-powered devices close to the RF sources, to harvest more energy, imposes some concerns on the security of the signals transmitted by these RF sources to their intended receivers. Studying this problem is the second step taken in this dissertation towards better understanding of energy harvesting wireless networks. While these secrecy concerns have been recently addressed for the point-to-point link, it received less attention for the more general networks with randomly located transmitters (RF sources) and RF-powered devices, which is the main contribution in the second part of this dissertation.

In the last part of this dissertation, we study the stability of solar-powered cellular networks. We use tools from percolation theory to study percolation probability of energy-drained BSs. We study the effect of two system parameters on that metric, namely, the energy arrival rate and the user density. Our results show the existence of a critical value for the ratio of the energy arrival rate to the user density, above which the percolation probability is zero. The next step to further improve the accuracy of the stability analysis is to study the effect of correlation between the battery levels at neighboring BSs. We provide an initial study that captures this correlation. The main insight drawn from our analysis is the existence of an optimal overlapping coverage area for neighboring BSs to serve each other's users when they are energy-drained.

Coverage, Secrecy, and Stability Analysis of Energy Harvesting Wireless Networks

Mustafa A. Kishk

(General Audience Abstract)

Renewable energy is a strong potential candidate for powering wireless networks, in order to ensure green, environment-friendly, and self-perpetual wireless networks. In particular, renewable energy gains its importance when cellular coverage is required in off-grid areas where there is no stable resource of energy. In that case, it makes sense to use solar-powered base stations to provide cellular coverage. In fact, solar-powered base stations are deployed already in multiple locations around the globe. However, in order to extend this to a large scale deployment, many fundamental aspects of the performance of such networks needs to be studied. One of these aspects is the stability of solar-powered cellular networks. In this dissertation, we study the stability of such networks by applying probabilistic analysis that leads to a set of useful system-level insights. In particular, we show the existence of a critical value for the energy intensity, above which the system stability is ensured.

Another type of wireless networks that will greatly benefit from renewable energy is internet of things (IoT). IoT devices usually require several orders of magnitude lower power compared to the base stations. In addition, they are expected to be massively deployed, often in hard-to-reach locations. This makes it impractical or at least cost inefficient to rely on replacing or recharging batteries in these devices. Among many possible resources of renewable energy, radio frequency (RF) energy harvesting is the strongest candidate for powering IoT devices, due to ubiquity of RF signals even at hard-to-reach places. However, relying on RF signals as the sole resource of energy may affect the overall reliability of the IoT. Hence, rigorous performance analysis of RF-powered IoT networks is required. In this dissertation, we study multiple aspects of the performance of such networks, using tools from probability theory and stochastic geometry. In particular, we provide concrete mathematical expressions that can be used to determine the performance drop resulting from using renewable energy as the sole source of power.

One more aspect of the performance of RF-powered IoT is the secrecy of the RF signals used by the IoT devices to harvest energy. The placement of RF-powered devices close to the RF sources, to harvest more energy, imposes some concerns on the security of the signals transmitted by these RF sources to their intended receivers. We study the effect of using secrecy enhancing techniques by the RF sources on the amount of energy harvested by the RF-powered devices. We provide performance comparison of three popular secrecy-enhancing techniques. In particular, we study the scenarios under which each of these techniques outperforms the others in terms of secrecy performance and energy harvesting probability.

This material is based upon work supported by the U.S. National Science Foundation (Grant CCF-1464293). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the NSF.

Dedication

To my family and friends.

Acknowledgments

I would like to thank Prof. Harpreet S. Dhillon for his continuous support, flexibility, encouragement, and mentorship. There are not enough words to express my gratitude to all the support and valuable lessons that Prof. Dhillon provided me with. I have learned from Prof. Dhillon a lot on the academic level as well as the personal level. Thanks to Prof. Dhillon, I have learned how to focus on well-motivated research, I have learned that the best way to be a successful academic and scholar is through rigor, accuracy, and paying attention to the details. I have also learned that the best way to be a respected advisor is by respecting your students, listening to them, and treating them as individuals. I would like to thank him for being a great role model that I will always consult at every stage of my life.

I would like to thank my committee members: Prof. Allen MacKenzie, Prof. Walid Saad, Prof. Anil Vullikanti, and Prof. James Kong for their time and efforts. I would also like to thank them for their useful comments and feedback that helped me improve my dissertation.

I would like to thank all my friends in Dr. Dhillon's group: Priyabrata, Kartheek, Mehrnaz, Mohamed, Morteza, Vishnu, Tapan, and Shankar for all the great moments and for making the lab feel like home. I specially thank Priyabrata for being such a great friend and being always there whenever I needed his help. Mehrnaz, thank you for always being there whenever I needed help with Matlab codes or Latex. I'm also thankful for my friends in Wireless@VT lab: Abdelrahman, Mozaffari, Yaman, Anibal, Mehdi, and Tengchan for all the mid-day conversations during work breaks.

I would like to thank my friends in other states in the U.S for all the phone calls we had that kept me sane during tough times: Rashad, Karim, and Ayman. I would also like to thank my friends in Egypt for being my second family and always having my back without a second thought: Adham, Hossam, Yossry, Hatem, Gemi, Omar, Fathy, and Mounir.

I would like to express my sincere gratitude to Mohamed Hassan for helping me settle in Blacksburg since the first day I arrived, for all the late night car rides, and for all the amazing food.

Finally, I would like to thank my parents Mrs. Soad Azzam and Mr. Abdelsalam Kishk (may Allah have mercy on him) for everything I achieved, and everything I will ever achieve in my life. I would also like to thank my siblings: Hassan, Fatima, and Eyman for taking care of my parents during my leave.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Exploiting renewable energy in multiple aspects of our daily life is gaining a continuously increasing attention for many reasons: (i) renewable energy is an environment-friendly (green) resource, (ii) despite possibly high initial installation costs, relying on renewable energy is usually cost-efficient on the long term due to government subsidies and lower operational costs, (iii) on-grid energy can be scarce or even unavailable in some geographical locations, making renewable energy the best candidate to replace on-grid energy in such locations. One of the key applications where renewable energy can play an important role is wireless networks. With the recent advances in the design of power-efficient electronics and high efficiency energy harvesting circuits, renewable energy is often considered a key enabler of multiple applications in next generations wireless networks. Relying on renewable energy as a main resource in wireless networks provides a solution for multiple challenges including but not limited to: (i) high energy efficiency required in the future 5G networks, (ii) the burden of battery replacement of billions of devices in internet of things (IoT), which is highly inefficient and expensive, (iii) environment-friendly solution to provide network coverage in the off-grid geographical areas, and (iv) reducing the energy consumption and carbon emissions caused by wireless communication networks, which amount to roughly 3% of the total global carbon emissions [1].

Renewable energy can be harvested using many different ways such as through solar cells, windmills, piezo-electricity, thermo-electricity, and much more [2]. The renewable energy resource should be selected based on many considerations such as the energy requirements of the used application, the environmental conditions where the energy harvesting devices would be deployed, and any other possible limitations such as cost or size. Consequently, the options of possible renewable energy resources that can be used in wireless networks are, in fact, limited. For example, IoT is considered one of the main wireless technologies that will rely on renewable energy due to the massive deployment of IoT devices, which renders recharging or replacing batteries an im-

practical solution. That said, the IoT devices are characterized by the following features: (i) they are usually low-power devices, (ii) they have small form factors, and (iii) they are often located in hard-to-reach places. Now, based on these limitations, it is clearly impractical to rely on a heavy solar panel to power such small low-power consuming devices. In addition, many IoT applications require indoor placement of IoT devices making it difficult to use solar energy. Based on these limitations, RF-energy harvesting is considered an appealing solution for powering IoT devices.

Beside IoT, another type of wireless networks that will benefit from relying on renewable energy is cellular networks (in particular, the BSs forming these cellular networks). Such BSs are characterized by the following: (i) they are typically placed outdoors in open areas, with abundant sunlight, (ii) they consume relatively high amount of energy in order to support communication and avoid overheating of their components, and (iii) cell towers are usually placed in sites where larger areas are available. This renders solar energy as the preferred source of renewable energy to power BSs deployed outdoors. Placing large solar panels close to the cell sites may not be a problem (especially in remote off-grid areas with no access to grid energy), which allows the BSs to harvest sufficient energy to support their uninterrupted operation. This, in fact, motivated multiple countries around the globe to adopt solar-powered BSs to provide coverage for off-grid areas, as shown in Fig. 1 in [1]. On the flip side, it is worth noting that relying on renewable energy for powering a wireless network has its own challenges. In particular, unlike on-grid power, the availability of renewable energy is not always ensured. This might lead to a scenario where a wireless device is unable to operate due to unavailability of energy. Such scenario can impose higher risk and unique constraints in some critical applications such as the failure of health monitoring device, fire alarming system, or a BS, which might lead to network outages. Hence, before taking the anticipated step of massive deployment of RF-powered IoT devices or solar-powered BSs, we need to make sure that these networks will be reliable and provide the required quality of service. In fact, if we take a careful look at the data presented in Fig. 1 in [1], it can be noticed that developing countries are showing more interest in deploying solar-powered BSs, mainly due to the relatively larger fractions of off-grid land areas compared to the more developed countries in Europe and North-America. This means that there is still a lack of motivation to switch to renewable energy if on-grid energy is available. In the below sections, we discuss in more detail the importance of providing theoretical analysis for each of (i) RF-powered IoT and (ii) solar-powered cellular networks, which are the two key pillars of the work reported in this dissertation. In addition, we list our contributions in each area.

1.2 RF-powered IoT: Chapters 3-7

As explained above, we need to verify that the performance of energy harvesting wireless networks will be acceptable before massive deployment. This verification can be done using two approaches: (i) experimental measurements and (ii) theoretical analysis and performance evaluation. Experimental measurements in that area of research have provided multiple promising insights. For instance, authors in [3] have recently implemented a battery-free cellphone that solely relies

on RF-energy. However, most of the existing measurements in literature rely on placing a dedicated source of RF-energy to transmit wireless power to the RF-powered device at relatively small distance. This, in fact, has motivated some research where the placement of dedicated power beacons (PBs) is assumed. The only job of such PBs is to provide wireless power to the RF-powered wireless devices. Recently, making this vision a reality, products of wireless power transmitting modules have been made commercially available. These modules are designed to be placed inside closed rooms such as homes or coffee shops in order to provide a wireless recharger for mobile devices thus avoiding cumbersome wired connections. While these modules might provide reasonable levels of wireless power within their vicinity, the performance of RF-powered wireless devices is questionable when they are placed in locations where such modules are not available. Hence, it is quite important to provide performance evaluation of RF-powered devices when relying on ambient RF energy without having dedicated sources of RF energy. In this dissertation, we use tools from stochastic geometry to study two main aspects of the performance of RF-powered IoT: (i) coverage probability and (ii) secrecy of RF signals used for harvesting energy. More details on the contributions in each chapter are provided next.

Chapter 3: Uplink/Downlink coverage analysis. Most of the existing work in the area of coverage analysis of RF-powered IoT is focused on either uplink or downlink. However, the joint uplink/downlink coverage probability has recently received attention in the context of performance evaluation of regularly-powered wireless networks. Characterizing this metric for RF-powered IoT devices is quit challenging due to the high correlation between the uplink signal-to-interference-plus-noise-ratio (SINR), downlink SINR, and the amount of harvested energy. To derive joint coverage probability, the joint complementary cumulative distribution function (CCDF) of these three parameters is required. We use tools from stochastic geometry to derive a tight approximation for this metric. The derived expressions are used to glean multiple system-level insights. For instance, we show the existence of an optimal charging duration for the RF-powered device that maximizes the system throughput. In addition, we derive a tuning parameter that can be used to determine the gap between the performance of the RF-powered IoT and a regularly-powered IoT. This tuning parameter captures the effect of all the system parameters on the performance of the RF-powered IoT including the density of the BSs, their transmission power, the charging duration, and the RF-DC conversion efficiency. We show that this tuning parameter also represents a threshold on the distance between an RF-powered IoT device and its nearest BS. If the distance is below this threshold, the performance is similar to that of the regularly powered network. After deriving the coverage probability of RF-powered IoT in this chapter, we turn our attention to another aspect of the performance of the RF-powered IoT devices, which is the secrecy of the RF signals used by the RF-powered IoT devices to harvest energy. Before addressing that problem, we provide a comparison of available secrecy enhancing techniques that can be used by the sources of the RF signals. This comparison is provided in the next chapter.

Chapter 4: Stochastic geometry-based comparison of secrecy enhancing techniques. In order to study the secrecy of RF sources in system setups where wireless networks are using ambient RF energy harvesting, we first need to characterize the effectiveness of different existing secrecy enhancing techniques in order to decide which one to use for different system setups. Hence, we compare the performance of two popular secrecy enhancing techniques: (i) artificial noise addi-

tion to confidential messages and (ii) using guard zones around sources of confidential messages. The results show that each of the two techniques outperforms the other at different system setup regimes. We focus on the guard zone technique in Chapter 5, and study its effect on the levels of ambient RF energy available at RF-powered wireless devices. In Chapter 7, we provide an extended comparison that includes the artificial noise technique, the guard zone technique, and the beamforming technique.

Chapter 5: Secrecy analysis of wireless power transmission. One of the concerns that accompany RF energy harvesting is the need of RF-powered devices to be located as close as possible to the RF sources. Hence, the secrecy performance of the signals transmitted by these RF sources might degrade in case these RF-powered devices start acting as eavesdroppers. This problem has been studied in the prior art for the point-to-point system setup. We study this problem for a system composed of two networks: (i) secrecy enhanced RF sources and (ii) RF-powered devices. In order to enhance its secrecy performance, the RF sources surround themselves with guard zones where they stop transmission whenever an illegitimate receiver is detected within this region. On one hand, massive deployment of RF-powered IoT devices is required to ensure higher density of successfully-operating IoT devices, on the other hand, massive deployment might lead to all the RF sources stopping their transmission. We first use tools from stochastic geometry to derive the performance metrics of each of the RF sources and the RF-powered IoT devices. We then show the existence of an optimal deployment density of RF-powered IoT devices that maximizes the density of successfully powered devices. In addition, we show that this optimal value is a function of the guard zone radius. We show the existence of an interesting coupling between both networks. The interaction between the two networks is modeled using tools from game theory. As a result of using PPP to model the locations of the RF sources, Poisson hole process (PHP) comes to picture in the analysis in this chapter to model the locations of *active* RF sources (the ones that do not have any IoT device in their guard zones). This motivates the analysis of distributional properties of PHP in the next chapter.

Chapter 6: Contact distance distribution of PHP. In the analysis of wireless networks with guard zones considered in the previous chapter, PHP is used to model the locations of active RF sources. Hence, the contact distance distribution of PHP is required. Unlike interference statistics, which received more attention lately for PHP-modeled networks, contact distance distribution received less attention. In this chapter, we provide upper and lower bounds for the contact distance distribution, as well as tight approximations. The results show that, in terms of contact distance distribution, approximating the PHP by a PPP with equivalent density provides a surprisingly tight approximation. In the next chapter, the work provided in Chapter 5 is continued with a more general approach that captures more than one secrecy enhancing technique.

Chapter 7: Performance comparison of secrecy enhancing techniques in secure SWIPT systems. In this chapter, we extend our analysis in Chapter 5 to provide a performance comparison of three different secrecy enhancing techniques: (i) guard zone technique, (ii) artificial noise technique, and (iii) beamforming. Our objective in this chapter is, however, slightly different from Chapter 5. In Chapter 5, we assumed that the sources of the RF signals only care about the secrecy of the transmitted signals. This behavior led to the game theory modeling we provided at the end

of Chapter 5. On the other hand, in this chapter, we assume that the source of the RF signal aims to jointly convey secured information to its intended receiver and, simultaneously, transmit wireless power to the RF-powered devices. We observe that the performance of each of the three considered techniques depends mainly on the interference levels at the RF-powered device. The statistics of the interference levels are required for the analysis of the performance of the ambient RF-energy harvesting. In addition, the statistics of the interference level are also required for studying the secrecy of the RF signal at the RF-powered device. We also observe that the difference between the statistics of this interference for each of the three techniques lies in modeling the locations of active sources as a thinned version of the original PPP with three different thinning probabilities. Building on that, we provide generic expressions for the secrecy performance as well as the energy harvesting probability. This generic expressions can capture any of the three techniques by tuning specific parameters. One of the main insights drawn from our analysis is the optimality of the artificial noise technique for high density of RF-powered IoT devices.

1.3 Solar-powered Cellular Networks: Chapters 8-9

Similar to the RF-powered networks, performance of solar-powered BSs also needs to be carefully studied before massive deployment. However, the nature of the problem is quite different. The failure of an RF-powered IoT device only affects its ability to communicate with its sink or access point. On the other hand, the failure of a solar-powered BS leads to the outage of all its associated mobile users. In other words, energy-drained BSs lead to mobile-coverage holes, which degrades the quality of service provided by the cellular network. Hence, careful analysis of such networks is required. As explained earlier, rigorous analysis with concrete results ensures the reliability of solar-powered BSs and will eventually be the key motivation for massive deployment of such BSs, even in locations with on-grid access. Our contributions in this area are listed below.

Chapter 8: Stability analysis of solar-powered BSs. One of the main concerns related to large scale deployment of solar-powered BSs is their ability to provide a reliable performance. In particular, the reliance on an unreliable resource of energy might lead to complete failure of the BSs due to being energy-drained. This can result from consuming large amount of energy while serving mobile users, or for being placed in a location with lower solar intensity (low energy arrival rate). We consider a square lattice for modeling the locations of the BSs and assume that whenever a BS is energy-drained, its associated mobile users are offloaded to the nearest BS among its eight neighboring BSs. To study the stability of such network, we exploit the resemblance of this setup with site percolation models. In percolation models, each vertex (which represents an energy-drained BS) is retained with probability p. In such models, the percolation probability is defined by the probability of having a giant component of retained vertices. Hence, the percolation probability reflects the instability of the solar-powered network due to having a giant component of energy-drained BSs. We use this analogy to first derive upper and lower bounds on p as a function of the energy arrival rate and the user density. Next, we use these bounds to draw some novel insights on the stability requirements of solar-powered BSs.

Chapter 9: Coupling of battery levels in solar-powered BSs. The most popular approach to study the steady state distribution of battery levels in solar-powered BSs is to use birth-death process with fixed birth and death rates. This approach is indeed correct if each BS is dedicated to serve only the mobile users falling within its coverage area, regardless of whether the neighboring BSs are active or not. However, in solar-powered BSs, whenever a BS x is energy drained the users associated with this BS will naturally associate with the next nearest BS. Hence, the energy consumption of the neighboring BSs of the BS x are affected by the battery state of the BS x. This implies that the battery levels of neighboring BSs are correlated and can not be analyzed separately. In this chapter, we study a system composed of 2 solar-powered base stations and provide the analysis for the steady state distribution of the battery levels while capturing their correlation. For the case of finite-sized batteries, we provide a set of equations that can be solved numerically to compute the steady state distributions. For the special case of unit-sized battery, we provide closed form expressions for the steady state distribution of the battery levels. In addition, for the 2-BSs setup, we show that there exists an optimal user association policy that minimizes the energy outage probability. The optimal policy indicates that when a BS is energy-drained, a user falling in its cell is allowed to associate with the other BS only if the distance is below a specific threshold. Above this threshold, association will not be beneficial due to associating with a distant BS leading to SINR outage.

1.4 List of Publications

1.4.1 Journals

- M. A. Kishk and H. S. Dhillon, "Joint Uplink and Downlink Coverage Analysis of Cellular-based RF-powered IoT Network", *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 2, pp. 446-459, Jun. 2018.
- M. A. Kishk and H. S. Dhillon, "Coexistence of RF-powered IoT and a Primary Wireless Network with Secrecy Guard Zones", *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1460-1473, Mar. 2018.
- M. A. Kishk, and H. S. Dhillon, "Tight Lower Bounds on the Contact Distance Distribution in Poisson Hole Process", *IEEE Wireless Communications Letters*, vol. 6, no. 4, pp. 454-457, Aug. 2017.
- M. A. Kishk, and H. S. Dhillon, "Effect of Cell-Selection on the Effective Fading Distribution in a Downlink K-tier HetNet", *IEEE Wireless Communications Letters*, vol. 6, no. 4, pp. 526-529, Aug. 2017.
- M. A. Kishk, and H. S. Dhillon, "Stochastic Geometry-based Comparison of Secrecy Enhancement Techniques in D2D Networks", *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 394-397, Jun. 2017.

- M. A. Kishk and H. S. Dhillon, "Stability Analysis of Energy Harvesting Wireless Networks: a Percolation Theory Approach", in submission to *IEEE Wireless Communications Letters*.
- M. A. Kishk and H. S. Dhillon, "Enhancing Physical Layer Security in SWIPT Systems with Untrusted Energy Receivers", in submission to *IEEE Transactions on Green Communications and Networking*.
- M. A. Abd-Elmagid, M. Kishk and H. S. Dhillon, "Joint Energy and SINR Coverage in Spatially Clustered RF-powered IoT Network", submitted to *IEEE Transactions on Green Communications and Networking*, 2018, available online: arxiv.org/abs/1804.09689.

1.4.2 Conference Papers

- M. A. Kishk and H. S. Dhillon, "A Comparison of Secrecy Enhancing Techniques for Secure SWIPT System", in *Proc. IEEE ICC Workshops*, Kansas City, MO, May 2018.
- M. A. Kishk and H. S. Dhillon, "Modeling and Analysis of Ambient RF Energy Harvesting in Networks with Secrecy Guard Zones", in *Proc. IEEE WCNC*, San Francisco, CA, March 2017.
- 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.
- Mohamed A. Abd-Elmagid, M. A. Kishk, and H. S. Dhillon, "Coverage Analysis of Spatially Clustered RF-powered IoT Network", in *Proc. IEEE ICC*, Kansas City, MO, May 2018.

1.5 Dissertation Outline

In Chapter 2, we provide a brief discussion of the prior art in the literature related to the theoretical analysis of energy harvesting wireless networks. In Chapters 3-7, we focus on the analysis of the performance of RF-powered IoT. In Chapter 3, we study the performance of cellular-based RF-powered IoT in terms of joint uplink/downlink coverage probability. The next problem that we focus on is the secrecy of the RF signals used by the IoT devices to harvest energy. Before studying this problem, we study a more general problem in Chapter 4 where we compare the performance of two popular secrecy enhancing techniques: (i) guard zone technique and (ii) artificial noise technique. Next, in Chapter 5, we study the secrecy of RF signals harvested by the IoT devices when the sources are using the guard zone technique to ensure secrecy. During the analysis in Chapter 5, we come across a fundamental stochastic geometry problem, which is the distribution of the contact distance in PHP. Hence, in Chapter 6, we provide some bounds and approximations for this distribution. In Chapter 7, we extend the work in Chapter 5 to include even more types of secrecy enhancing techniques, which are the artificial noise technique, and the beamforming

technique. Starting from Chapter 8, we focus on the analysis of solar-powered cellular networks. In Chapter 8, we use tools from percolation theory to study the stability of solar-powered BSs. In Chapter 9, we study a problem that is commonly ignored in literature, which is the correlation between the battery levels of neighboring BSs. Finally, in Chapter 10, we conclude the dissertation.

Chapter 2

Relevant Prior Art

Performance of energy harvesting-powered communication networks has been studied from multiple perspectives including: (i) channel capacity computation when the transmitter is powered by energy harvesting, (ii) studying the optimal transmission policies of an energy harvesting transmitter in point-to-point links, and (iii) stochastic geometry-based modeling and analysis of large scale wireless networks composed of energy harvesting transmitters and/or receivers. In this chapter, we provide a brief overview of these research directions. For completeness, it should be noted that we decided to focus on these directions to keep the discussion concrete and relevant to this dissertation, which is primarily focused on the theoretical analysis of energy harvesting communication networks.

2.1 Channel Capacity

Not surprisingly, one of the fundamental performance limits in energy harvesting communications is the channel capacity. For the simple point-to-point link shown in Fig. 2.1, the usual setup consists of a transmitter with a battery that is solely powered by energy harvesting. The battery size is $E_{\max}$ and the amount of energy arrival at each channel use i is E_i, where the values of E_i's are usually assumed to be independent and identically distributed (i.i.d). At the ith channel use, the ith element X_i of the codeword is sent. For this simple setup, the existing works have focused on evaluating the channel capacity for different values of $E_{\max}$, different channel characteristics, and different system constraints (e.g., latency constraints). While some efforts were directed to evaluate the capacity for the cases of $E_{\max} = \infty$ and $E_{\max} = 0$, most of the research focused on the more realistic case of having finite-sized battery ($E_{\max} = \text{constant}$). The rest of this section will summarize the efforts in the three cases with more emphasis on the finite battery case that attracted most attention in the recent past.

2.1.1 Infinite Battery Case

The energy constraint on the transmitted codeword elements at each channel use k can be represented as follows:

$$\sum_{i=1}^{i=k} {X_i}^2 \leq \sum_{i=1}^{i=k} E_i. \tag{2.1}$$

The above equation means that the energy consumed to send the codeword symbols during the first k channel uses should not exceed the amount of energy harvested till this instant. This constraint is essentially as *energy causality* constraint. Authors in [4] studied the capacity of energy harvesting communication system with infinite battery at the transmitter in an additive white Gaussian noise (AWGN) channel. They concluded that the capacity for the infinite battery case with E_i is a random variable with average recharge rate p is upper bounded by the classic capacity expression with average power constraint p:

$$C_{E_{\max}=\infty} \leq \frac{1}{2}\log(1+p). \tag{2.2}$$

The authors in [4] proposed two transmission schemes that can reach this upper bound: save-and-transmit, and best-effort-transmit. Both schemes rely on the idea of sending infinite length codeword, so negligible number of mismatches at the beginning will not affect the capacity. These negligible number of mismatches happen only in the initial part when energy is still accumulating in the battery. The presented schemes exploited the existence of infinite battery, which implies that on the long term, energy will accumulate in the battery and no codeword mismatches will occur.
Different from [4], authors in [5] focused on the case of finite n-codeword length. They assumed, unlike [4], that the energy arrival statistics are available at the receiver. Also, for tractability, they assumed a noiseless channel. The main target in [5] was to find the maximum codebook size for the n-length codewords such that the error probability doesn't exceed a predefined threshold ϵ. Their work assumed that sending the symbol "1" consumes one energy unit from the battery, while the symbol "0" requires no energy. This means that mismatches due to energy outage can only take place at the positions of 1s in the codeword. Based on this setup, authors showed the appropriate decoding scheme and provided analysis for the possible error events. Finally, they derived a lower bound for the maximum channel coding rate. The gap between the lower bound and the channel capacity is a function of 3 parameters: target error rate ϵ, energy arrival variance, and codeword length n.
While the above work presented analysis for point-to-point links with energy harvesting transmitter, authors in [6, 7] worked on characterizing the capacity region for multiple access channel system with energy harvesting transmitters. The work in [6] studied a Gaussian multiple access channel (GMAC) with energy harvesting transmitters and infinite batteries. They showed that the capacity region is equivalent to that of a GMAC with regularly powered transmitters and average power constraints equal to the recharge rates of the transmitters. The authors proved the validity of this claim by studying the case of 2 users. They presented the coding and decoding schemes that would achieve this capacity. The authors enlisted the error events of the proposed schemes and proved that the error probability would tend to zero as the codeword length tends to ∞. This result

Figure 2.1: Point-to-point energy harvesting system model.

can be considered as an extension to the results in [4] for a point-to-point link with infinite battery at the transmitter. Same result for GMAC channel was proved in [7] for an arbitratry number of users. Authors in [7] also showed that the save-and-transmit policy (mentioned earlier in this section) can achieve the capacity. They also calculated the capacity region for the flat fading multiple access channel and proposed the optimal power control that maximizes the sum-of-rates.

2.1.2 Zero-battery Case

For the zero-battery case, the energy constraint on the transmitted codeword elements at each channel use k can be represented as follows:

$$X_k{}^2 \leq E_k. \tag{2.3}$$

The above equation means that the energy consumed to send the codeword symbol at channel use k should not exceed the amount of energy harvested at that epoch, regardless of the amount of energy harvested in the previous epochs due to the zero capacity battery. Authors in [8] presented the capacity and the capacity achieving input distribution of static amplitude constrained AWGN channel. System with batteryless energy harvesting transmitters is considered a time-varying amplitude constrained AWGN channel, where the amplitude constraints are defined by the energy harvested at each channel use. Authors in [9] used the work in [8] to define the capacity of batteryless energy harvesting transmitter system. First, they gave expressions for capacity when the amplitude constraints are not known at the transmitter or the receiver. They also provide expressions when the amplitude constraints are known at both sides. Next, they derived the capacity for the more realistic case of causal information at the transmitter. Causal information at the transmitter means that the transmitter has information about the amplitude constraint for each channel use only after the energy is harvested at that exact channel use. The authors showed that the support set for the capacity achieving input distribution is finite. Finally, authors showed by numerical results that the capacity in case of infinite battery is much higher that the case of batteryless transmitters.

Different from work in [9], authors in [10] focused on the case of finite length n-codewords. The problem tackled in this work is to find the coding rate back off from the capacity due to using finite length codewords. They showed the encoding and decoding schemes that maximize the coding rate and enlisted the error events to calculate the error probability. The authors proposed a second-order approximation for the achievable rate that had a back off from the capacity as a function of the codeword length n and the target error probability ϵ. The paper included two examples of binary channels, which are noiseless and noisy. It was shown that the input distribution of maximum rate achieving schemes is a function of the energy arrival probability and the binary entropy function.

Authors in [11] extend their work in [9] but for GMAC. They focus their study on a system of two batteryless energy harvesting transmitters. First, they extended the work in [8] for static amplitude constrained transmitters to a GMAC, getting similar results of finite support sets for capacity-region boundary achieving input distributions. Next, they studied the case of time varying amplitude constrained transmitters (energy harvesting), for which they established the equivalence of this system with state-dependent GMAC whose capacity region is still unknown. However, the authors derive the achievable rates using Shannon strategies for the case of joint energy state information available at both users and individual energy state information. Finally, authors show the existence of a large gap between achievable rate region for individual information case and the case of joint information at both users and receiver.

Authors in [12] study the trade-off between achievable capacity maximization and transmitter's energy arrival entropy reduction at the receiver. They derive the maximum achievable capacity in the case that the only target of encoder is to transmit messages. Also, they derive the maximum entropy reduction in case that the only target of encoder is to assist the receiver in decoding the energy arrival sequence. Finally, they define an objective function that captures both capacity and energy arrival entropy, and prove that the input distribution that maximizes this objective function has a finite support set.

2.1.3 Finite Battery Case

The energy constraint on the transmitted codeword elements at each channel use k can be represented as follows:

$$X_k{}^2 \leq B_k, \tag{2.4}$$

where B_k is the amount of energy stored in the battery at the channel use k. The battery storage at any channel use k can be modeled as follows:

$$B_{k+1} = \min\{B_k - x_k{}^2 + E_k, E_{\max}\}. \tag{2.5}$$

The above equation captures the amount of energy consumed $x_k{}^2$ and the amount of energy harvested E_k. The overall battery level is limited by the maximum value $E_{\max}$. The authors of [13] gave initial insights into the considered system. In particular, they considered a communication system with finite battery sized energy harvesting transmitters, and a deterministic energy arrival

Figure 2.2: Equivalent timing channel used in [11].

process. At each energy arrival, the battery is charged with a fixed amount $E_k = \rho$. The capacity for the considered system has an upper and lower bounds as follows:

$$\frac{1}{2}\log(1 + \frac{e^{2\upsilon(E_{\max},\rho)}}{2\pi eN}) \leq C \leq \frac{1}{2}\log(1 + \frac{\rho}{N}), \tag{2.6}$$

where N is the noise power and $\upsilon(E_{\max}, \rho)$ is a function of the volume of the set of all possible sequences that the transmitter can send with the given battery size and energy arrival constraints. The work presented in [14] considered a stochastic (Bernoulli distributed) energy arrival process but limited their solutions to the case of a unity sized battery ($E_{\max} = 1$). This means that the transmitter cannot send a symbol "1" unless a non-zero energy arrival occurred. They proved the equivalence of this channel to a timing channel. The equivalent timing channel, as shown in Fig. 2.2, works as follows:

- The transmitter waits for a non-zero energy arrival (represented by triangles) for time Z_k since the last sent "1".
- After the energy arrival, the transmitter waits for an extra time V_k then sends a "1". The instant of transmission is represented by a circle in Fig. 2.2. The value of V_k represents the channel input, which depends on the symbol required to be transmitted U_k and the battery state Z_k.
- The total time T_k between two sent 1s represents the channel output seen by the receiver (assuming a noiseless channel).

Based on the presented timing channel model, the authors presented the capacity as the maximization of a given objective function. The objective function is maximized over two variables: $p(u)$

and $\nu(u,z)$. Where $p(u)$ is the probability mass function (PMF) of the transmitted symbols, and $\nu(u,z)$ is the mapping function used in the timing channel to select the value of V_k based on U_k and Z_k. Due to the difficulty of the maximization problem, the authors present a specific PMF $p(u)$ with cardinality N and mapping function $\nu(u,z)$ and derive an upper bound for the capacity. They chose the mapping function as
$V_k = (U_k - Z_k \mod N) + 1$,
whereas the receiver decodes the channel output as follows:
$\hat{U_k} = T_k - 1 \mod N$.
Authors in [15, 16] worked on studying upper and lower bounds for the capacity of finite battery aided energy harvesting transmitter communication system with a stochastic energy arrival process. In [15], authors focused on the case of a Bernoulli energy arrival process so that at each energy arrival epoch, $E_k = E$ with probability p and $E_k = 0$ with probability $1-p$. For this setup, they proposed an approximation for the capacity that deviates with a maximum gap of 2.58 bits. Their main result is as follows:

$$\frac{1}{2}\log(1 + p\min\{E_{\max}, E\}) - 2.58 \leq C \leq \frac{1}{2}\log(1 + p\min\{E_{\max}, E\}). \tag{2.7}$$

Note that the above equations are for an AWGN channel with unit variance noise. The authors propose a transmission policy that ensures a transmission rate within 0.973 bits from the maximum achievable rate for each of the two cases: $E_{\max} \geq E$ and $E_{\max} \leq E$. The proposed scheme is to allocate energy $g(k)$ from the battery for the kth transmission that is a function of the period j since the last non-zero energy arrival as shown in Fig. 2.3. They prove that $g(k) = p(1-p)^j E_{\max}$ is a nearly optimal transmission policy. Authors also prove that for the case of $E_{\max} \geq E$, the maximum achievable rate is analogous to the case of the infinite battery. In [16], authors generalized the results of capacity upper and lower bounds for any energy arrival process (distribution of E_k was assumed to be Bernoulli in [15]). They used similar analogy as the one proposed in [15] to define a near optimal transmission policy. They showed that the upper and lower bounds for the capacity in that case are as follows:

$$\frac{1}{2}\log(1 + \mu) - 3.85 \leq C \leq \frac{1}{2}\log(1 + \mu), \tag{2.8}$$

where $\mu = \mathbb{E}[\min\{E_k, E_{\max}\}]$.

The work presented in [17] studies the effect of feedback in the system setup considered in this section,, which means that the transmitter uses the channel output in the $k-1$th channel use to encode the channel input in the kth channel use. The authors assume a binary erasure channel and begin with studying the effect of feedback in case of deterministic energy arrival process (non-zero energy arrivals at odd values of k). For that case, they show that there is a gain in the capacity from using feedback. Next, they extend their work to stochastic energy arrival process (assumed to be Bernoulli) and also prove the existence of gain in the capacity from using feedback.
For studying the performance of limited battery transmitters in flat fading GMAC, authors in [7] presented three different online strategies:

- Single-user channel adaptive transmission (SUCA): Receiver selects the user with the best channel fading, this user transmits with the desired power lever. If there is not enough energy

Figure 2.3: Near optimal transmission policy for finite battery transmitters.

in the battery to transmit with the desired power level, the user transmits using the available energy in the battery.

- Group-power channel adaptive transmission (GPCA): The only difference from the first one is that if the selected user doesn't have enough energy then user with 2nd strongest channel fading is also selected and transmits with the first one. The process continues until a certain stopping criteria is met.
- Group-power battery adaptive transmission (GPBA): Receiver selects the user with the highest battery level. If this user's channel fading is below a certain threshold, then user with 2nd highest battery level is selected. The process also continues until a certain stopping criteria is met and all selected users transmit to the receiver.

Authors showed that GPCA scheme has the best performance, and the capacity in all three strategies converge to the upper bound of the infinite battery case as the battery size increases.

2.2 Optimal Transmission Policies

After getting upper and lower bounds for the capacity for different system setups, the next problem that needed to be solved is to find the optimal online policy that maximizes the system throughput. Initially the focus was on defining the optimal offline transmission policies [18–20]. These policies assume the knowledge of energy arrival values and time instants non-causally. As non-realistic as this assumption seems to be, it gives an initial insight on the system performance upper bounds. In fact, many proposed online transmission strategies were inspired by these offline strategies. Most

Figure 2.4: Water filling scheme for offline optimal transmission policies.

of the work presented in this direction focuses on the assumption of energy harvesting transmitters with finite-sized battery. The next subsection will discuss the key advances in the direction of offline optimal policies.

2.2.1 Offline Transmission Policies

The problem, as defined in [18, 19], was to find the optimal power allocation among consecutive transmissions given the values and the instants of energy arrivals non-causally. In other words, given the energy arrivals $\{E_0, E_1, E_2, \dots\}$, what should be the values of transmission powers $\{P_1, P_2, P_3, \dots\}$ knowing that the epoch lengths between energy arrivals are $\{l_1, l_2, l_3, \dots\}$. In order to handle this problem, the authors constructed two constraints: energy causality constraint, and finite storage constraint. The energy causality constraint means that energy that has not been harvested yet cannot be used. The main target of finite storage constraint is to avoid battery overflow, knowing that the next energy arrival will be E_k the transmitter should not save in its battery more than $E_{\max} - E_k$ to avoid wasting any energy due to battery overflow. The energy causality constraint can be expressed mathematically as follows:

$$\sum_{i=1}^{i=k} l_i P_i \leq \sum_{i=0}^{i=k-1} E_i,$$

while the finite storage constraint can be expressed as follows:

$$\sum_{i=0}^{i=k} E_i - \sum_{i=0}^{i=k} l_i P_i \leq E_{\max}.$$

These two constraints give upper and lower bounds on the optimal power policies.
Authors in [20] proposed the use of directional water-filling scheme as shown in Fig. 2.4 with two constraints equivalent to those presented in [18, 19]. The first constraint is that the water is allowed to flow only to the right, which represents the causality constraint. The second constraint is that the

amount of flow from one transmission epoch l_i to l_{i+1} is limited by $E_{\max} - E_i$, which represents the finite storage constraint that avoids any energy wastage due to limited battery capacity.

2.2.2 Online Transmission Policies

Authors in [21] studied a transmitter with finite-sized battery and Bernoulli energy arrivals, where at each epoch energy $E_k = E_{\max}$ with probability p and $E_k = 0$ with probability $1 - p$. For that system, authors show that the optimal power allocation policy will depend only on the time since the last non-zero energy arrival (similar observation from [15] was discussed earlier in this chapter). In addition, they adapt these policies for the case of fading channels with channel coefficients known non-causally. More general solution is proposed in [22] for the case of general i.i.d energy arrival process.

Authors in [23] extend the problem to study the inefficiency of battery storage due to leakage or other physical reasons. They formulate the problem as follows: At each time k, the energy harvested, E_k, is partitioned into s_k for storage and $E_k - s_k$ for transmission. In addition, an amount r_k is retrieved from the battery for transmission, so the overall transmission energy is $p_k = E_k - s_k + r_k$. The battery has storage efficiency η which means that only ηs_k will be successfully stored. Defining causality and finite storage constraints as discussed earlier in [18, 19], they show that the optimal offline policy does not store and retrieve energy at the same time. In that sense, they propose a double threshold policy where the transmitter stores energy when E_k is above a certain threshold, and retrieves energy when E_k is below a certain threshold, otherwise the whole energy is used for transmission. Next, they propose an online policy that induces some modifications to the double threshold scheme using the Markovian property of the harvesting process. Authors in [24] study the hybrid storage system where the transmitter has a finite-sized super capacitor that has 100% efficiency storage, and an infinite battery with storage efficiency η. They propose an offline optimal transmission policy that maximizes the sum-of-rates over N transmission epochs. The resulting optimal policy is a modified version of the directional water filling scheme discussed earlier in this section.

Authors in [25] proposed optimal offline and online transmission policies for a two way relay channel. The considered system assumes that both communicating nodes and a single relay are powered by energy harvesting with finite-sized batteries. The authors provide the rate regions for four different relaying schemes and show that hybrid strategies that mix these schemes will enhance the results. Authors show that also introducing some modifications to the directional water filling scheme is the answer to the offline transmission problem. An online transmission policy is also proposed using dynamic programming. A more complex diamond channel is used in [26] where a system of energy harvesting source and two relays is studied. The authors divide the channel into a broadcast channel (from the source to the relays) and a multiple access channel (from the relays to the destination), optimal power allocation problem is solved for each of the 2 channels individually.

Modified versions of the directional water filling (DWF) scheme appeared as a solution to many different system setups and different problem statements. For a two user interference system with

energy harvesting transmitters with a delay constraint at the transmitters, authors in [27] solved the sum-of-rates maximization problem and proposed offline and online optimal transmission policies also inspired by DWF scheme. Authors in [28] studied a delay constrained system with limited data buffers at the transmitters for different system setups including single user channel and two way relay channel. Again, a modified DWF scheme was the solution for the offline policies, while optimization problem was formulated for the online policy.
Finally in [29], authors addressed the throughput maximization policies for transmitters that heat up. This problem has a new constraint added to the causality and finite storage constraints which is that the integration of transmitter powers at any time cannot exceed a given heat threshold. They proposed optimal offline transmission policies for the defined system using optimization tools.

2.3 Stochastic Geometry-based Analysis

While information theoretic results discussed above provide sharp characterization of system performance for simpler deterministic topologies, actual wireless networks are usually much more complex. Stochastic geometry provides a useful way to rigorously characterize the performance of large-scale networks [30–32]. Not surprisingly, it have been applied to energy harvesting wireless networks to glean multiple system-level insights and understand key performance trends. Key directions of research based on stochastic geometry include: (i) analysis of the downlink in cellular networks with energy harvesting BSs [33–35], (ii) performance analysis of mobile users or IoT devices that use the harvested energy to transmit information [36–39], (iii) analysis of energy harvesting device-to-device (D2D) and cognitive networks [40–46]. We next provide more details on each of these directions.

2.3.1 Energy Harvesting in Downlink

Authors in [33] studied a multi-tier cellular network where the locations of BSs in the kth tier is modeled as a PPP Φ_k. Also, the locations of the users is modeled as a PPP Φ_u with rate λ_u. The energy arrival at each BS in the kth tier is modeled by a Poisson process with mean μ_k. Each tier is characterized by its own PPP density λ_k, BS transmission power P_k, and BS's battery capacity N_k. Due to the finite size of the battery and randomness in energy arrivals, a BS may become on or off depending on the amount of energy required for a BS to serve a user. Note that for this setup the BS coverage area $\mathcal{A}_k$ may change with time. This is due to the fact that when a BS is off, the users in its coverage area will be served by other neighboring BSs. Authors defined the availability ρ_k of BSs in the kth tier by the probability that a BS of the kth tier has enough energy to serve users (available). The amount of energy required to make a BS available depends on the on/off strategy used by the BSs. An example strategy is $\mathcal{S}_k(N_{k^{\min}}, N_{kc})$, where a BS toggles from on to off state when energy level becomes less than $N_{k^{\min}}$ and toggles back to on state after harvesting enough energy that makes its energy level above N_{kc}. In order to calculate the availabilities of

the tiers, authors used stochastic geometry tools mainly in calculating the energy utilization rate $\nu_k = \mathrm{P}_c \lambda_u \mathbb{E}[|\mathcal{A}_k|]$, where $\mathrm{P}_c = \mathbb{P}(\mathrm{SIR} \geq \beta)$ is the coverage probability, SIR is the signal-to-interference-ratio, and β is the SIR threshold. While the calculation of P_c is straight forward, the calculation of $\mathbb{E}[|\mathcal{A}_k|]$ is more challenging due to the definition of $|\mathcal{A}_k|$ for a BS located at x_k is as follows:

$$|\mathcal{A}_k(x_k)| = \int_{\mathbb{R}^2} \prod_{j \in \mathcal{K}} \prod_{x \in \Phi_j^{(a)}} 1\left(\frac{P_k \mathcal{X}_k^{(z)}}{\|x_k - z\|^\alpha} \geq \frac{P_j \mathcal{X}_j^{(z)}}{\|x - z\|^\alpha} \right) \mathrm{d}z, \tag{2.9}$$

where $\mathcal{K}$ is the set of all tiers, $\mathcal{X}$ is the shadowing, α is the path loss coefficient, and $\Phi_j^{(a)}$ is the set of active BSs in the jth tier. In order to compute the expectation, authors used mathematical manipulations for changing the orders of expectations over the different random variables and then applied PGFL for PPP.

Similar system of energy harvesting BSs locations modeled by PPP was assumed in [35] but instead of being solely powered by energy harvesting, authors assumed a hybrid energy supplied system. In this setup, the BS uses harvested energy stored in the battery when it is enough for the system operation. Otherwise, it connects to the main-grid and purchases on-grid energy. Taking into consideration the dependence between energy demand and on-grid energy price, the authors formulated an optimization problem to minimize overall price paid for on-grid energy while ensuring that coverage probability is above a specific threshold.

Authors in [34] studied a cooperative system model. The locations of transmitters are again modeled by a PPP Φ and locations of users modeled by PPP Φ_u. Each user is served by a cluster of the nearest K transmitters in Φ, such that the K transmitters cooperatively transmit the same data to the user. The transmitters are solely powered by energy harvesting with finite-sized battery, where the energy arrival process is modeled by a Bernoulli process with probability ρ. For this setup, the authors firstly derive the transmission probability P_{tr} (which basically corresponds to the probability that the battery's energy level is above a certain threshold) as a function of the battery size and the energy arrival rate by solving the balance equations of resulting Markov chain. Next, they use tools from stochastic geometry to derive the link success probability defined by having the signal-to-interference-plus-noise (SINR) γ at the typical user above a certain threshold where the SINR is defined as follows:

$$\gamma = \frac{\sum_{i=1}^{i=K} \mathbb{1}_i d_i^{-\alpha} H_i}{I + \sigma^2}, \tag{2.10}$$

where d_i is the distance between the ith transmitter and the typical user, H_i is the channel fading gain, I is the total interference, and σ^2 is the noise power. Here $\mathbb{1}_i$ represents the uncertainty on the energy level in the transmitter's battery where $\mathbb{P}(\mathbb{1}_i = 1) = P_{tr}$. In case multiple users request connection to a certain cluster, one of them is chosen uniformly at random. Authors derive an approximation for the probability of user selection p_{clus}. For the case of $K = 1$, they approximate p_{clus} by the probability that distance between the typical user and its nearest neighbor user is larger than a certain scaled version of the distance between the typical user and its nearest transmitter. Finally, authors derive the joint probability of link success and user selection.

2.3.2 Energy Harvesting in Uplink

All the work discussed in the previous section assumed a stochastic energy arrival process at the energy harvesting transmitter modeled by Poisson process or Bernoulli process. On the other hand, most of the existing analysis for energy harvesting communication networks in uplink channel focus on ambient RF energy harvesting transmitters. Ambient RF energy harvesting depends on a RF-DC conversion circuit that converts RF signals to energy. The efficiency of the RF-DC conversion can reach up to 80% according to [47]. Stochastic geometry plays an important role in the analysis of such systems in both energy harvesting process and information transmission process. Authors in [36] consider a hybrid network where the locations of BSs and energy harvesting mobile users are modeled by PPP with densities λ_b and λ_u. In addition, a network of power beacons (PBs) with transmission power q is deployed in order to transfer wireless power to the users. The locations of PBs is also modeled by PPP Ψ with density λ_p. For that setup, the authors perform uplink analysis under constraints on the SINR target at the BS and on the aggregate harvested energy P at the mobile user located at U_0, where P is defined as follows:

$$P = q \sum_{x \in \Psi} \|x - U_0\|. \tag{2.11}$$

The cumulative distribution function (CDF) of P is computed and used to derive the feasibility region of the considered system which is all the combinations of λ_b, λ_p, and q that satisfy the constraints. Its proved that the term $q\lambda_p\lambda_q^{\frac{\alpha}{2}}$ should exceed a certain threshold to satisfy the constraints. This result shows that increasing the PB transmission power q leads to less dense PB network required which is consistent with intuition. Authors in [37] considered an almost similar system, the only difference is that no PB network is deployed. The only source of energy for ambient RF energy harvesting users is the RF signals from the BSs in the downlink channel. Another difference is modeling the BSs network by a K-tier network where each tier is modeled by an independent PPP. Different from [36], in this paper the authors assume channel inversion power control is performed by the user. The user associates with its nearest BS, so the required harvested energy for successful transmission is:

$$\gamma = \rho R^{\alpha} \tag{2.12}$$

where ρ is the minimum required received power at the BS (sensitivity), and R is the distance between the user and its nearest BS. The users are assumed to have a finite-sized battery with energy level $P_S(T)$ at any time slot T. Using Markov chain modeling, authors derive the distribution of $P_S(T)$. Hence, the transmission probability is defined by $\eta = \mathbb{P}(P_S(T) \geq \gamma)$. Note that the amount of harvested energy at any time slot is similar to (2.11) except that the harvested energy is coming from the multi-tier network of BSs. Next, authors derive the uplink coverage probability defined by $\tau = \mathbb{P}(\mathrm{SIR} \geq \tau)$ where τ is the SIR minimum threshold and SIR_k is the signal to interference ratio at the associated BS from the kth tier defined as follows:

$$\mathrm{SIR}_k = \frac{\rho_k h}{\sum_{j=1}^{K} \sum_{u_i \in \Phi_j \setminus \{u_o\}} \gamma_j g_i \|u_i\|^{-\alpha}} \tag{2.13}$$

where ρ_k is the sensitivity of the kth tier BSs, h is the channel fading gain between the typical user and its associated BS, Φ_j is the point process of users connected to BSs in the jth tier, u_o is the position of the typical user, γ_j is the transmission power by users connected to the jth tier, and g_i is the fading gain between associated BS and user located at u_i. An approximation is made during the analysis of the uplink coverage probability which is the assumption that Φ_j is PPP with density $\eta\lambda_k$ where η is the transmission probability and λ_j is the density of the jth tier PPP Ψ_j. This approximation assumes that the Φ_j is an independently thinned version of Ψ_j. Another note is that the full channel inversion power control made η and τ independent. This leads to defining the successful transmission probability as the product of η and τ. Similar analysis with similar performance metrics and approximations is done in [38] but for a single tier network and assuming a dynamic motion of either BSs or mobile users. In other words, for fixed mobile users' locations the BSs locations independently change at each frame and stay fixed during the downlink/uplink frame. This assumption introduces more randomness and more complexity to the system.
Different from all aforementioned work, authors in [39] used Ginibre α-determinantal point process (DPP) for modeling the locations of ambient RF sources. The considered system consists of a wireless sensor network where the sensor nodes harvest energy from ambient RF in order to transmit information to data sink. The sensor harvests ambient RF from all existing networks including broadcast tv, radio, cellular networks and others. The advantage of using DPP over PPP is the ability to capture repulsion among points which makes it more general than PPP. While the computation of CDF of the harvested energy P_H, mean and variance of P_H are challenging to derive due to the complexity of analysis of DPP, authors present useful bounds of these metrics. In order to derive upper bounds, authors present a worst case scenario where the sensor node harvests energy only from one RF source.

2.3.3 Device-to-Device Energy Harvesting Networks

Stochastic geometry plays an important role in analyzing energy harvesting device-to-device (D2D) networks consisting of random pairs of transmitters and receivers. Authors in [40] analyze a D2D network where locations of transmitters is modeled by PPP. Each transmitter is associated with a receiver at a unit distance. Each transmitter has finite-sized storage capacity and is solely powered by a stochastic energy arrival process with rate λ_e. For this setup, the authors compute the transmission probability using stochastic geometry and random walk theory. Note that the transmission probability in this setup is defined by the event of having enough stored energy to perform uplink transmission. Next, authors compute SIR outage probability at the typical receiver. A trade off between outage probability and transmission probability is noticed which can be controlled by the transmission power. The existence of optimum transmission power that maximizes the network throughput is also demonstrated analytically.
Authors in [41] consider a different setup of D2D energy harvesting network. The transmitters are assumed to be connected to regular power supply where the locations of transmitters are modeled by PPP. Each transmitter is associated with a receiver at distance d_o where the transmitter harvests energy from ambient RF. The receiver adopts power splitting scheme so that it uses ν_d of the re-

ceived power for data detection and $1-\nu_d$ for energy harvesting. The trade off between the SINR outage probability and mean of energy harvested is studied and transmission power minimization problem is solved with constraints on outage probability and mean energy harvested.
In [42], authors study a heterogeneous network with multi-mode operation. The studied system consists of a K-tier network of access points (APs) with ith tier modeled by a PPP Φ_i with density λ_{a_i} and transmit power P_i. The locations of the users during each frame are modeled by PPP Φ_u with λ_u. The system has two modes of operation: the first one is the AP mode in which AP transmits data directly to the intended associated user, the second mode is the D2D mode where the AP uses one of the users to relay its data to the intended associated user. All the APs have fixed power supplies while the users are powered by energy harvesting using wireless power transfer from APs. The user can harvest energy from an AP in the ith tier whenever it falls in the energy harvesting region (EHR) of this AP, this EHR is defined as follows:

$$R_{h_i} = \left(\eta \frac{P_i}{C}\right)^{\frac{1}{\alpha}}, \tag{2.14}$$

where η is the RF-DC conversion efficiency, α is the path loss coefficient, and C is the threshold for activating the energy harvesting circuit at the user. The probability of a user falling in EHR of any AP is then derived as follows:

$$\begin{aligned} p_{eh} &= 1 - \mathbb{P}\left[\bigcap_{i=1}^{K}\{\Phi_i(b(o, R_{h_i}))\}\right] \\ &= 1 - e^{-\sum_{i=1}^{K} \lambda_{a_i} \pi {R_{h_i}}^2}, \end{aligned} \tag{2.15}$$

where $b(0,r)$ is a circle centered at the origin with radius r, and $\Phi(A)$ is the number of points in the Borel set A. In this system, whenever a user falls in the EHR of an AP and does not need to receive data, this user starts to harvest energy from this AP and keep storing it in its infinite-sized battery. A user can act as a relay whenever it has more than N harvested energy units in its battery. If it is selected by an AP to relay data, its battery energy level will decrease by N units. Also, the battery level increases whenever the user falls in EHR of an AP, and stays the same whenever it is outside EHR. The battery level also stays the same when the user is inside EHR receiving data. Defining the probability of user receiving data by p_{rc}, authors use all these formulations to build the Markov chain of the battery level of users. The balance equations are solved to get the probability of user having battery level higher than N (users ready to relay data or UERs). This probability is used as a thinning probability to model the locations of UERs as a thinned version of the original PPP. Using these results, the outage probability of the system is characterized for both operating modes. The effect of AP density on the interference of downlink channel show the existence of an optimal RF-DC efficiency.

2.3.4 Energy Harvesting Cognitive Networks

Recent advances in the analysis of energy harvesting networks also included cognitive networks. In [43], authors studied a system of primary transmitters (PTs) modeled by PPP Φ_P with density

λ_p coexisting with secondary network of secondary transmitters (STs) modeled by PPP Φ_S with density λ_s. The ST can either harvest ambient RF energy from transmitted signals by a PT, or transmit data to an intended secondary receiver (SR) at distance d_s. Each PT is surrounded by a guard zone with radius r_g, if ST exists inside the guard zone of a PT then it is not allowed to transmit data. From that, the probability that an ST does not lie in the guard zone of any PT will be:

$$p_g = e^{-\pi {r_g}^2 \lambda_p}. \tag{2.16}$$

Similarly, each PT has a harvesting zone with radius r_h. A ST can harvest energy from a PT only if it lies inside its harvesting zone. It is assumed that r_h is small enough such that the harvesting zones of PTs do not overlap. The probability that an ST lies in the harvesting zone of a PT is:

$$p_h = 1 - e^{-\pi {r_h}^2 \lambda_p}. \tag{2.17}$$

Given that each ST has a finite-sized battery and can only transmit when this battery is full, authors use Markov chain analysis to calculate the ST transmission probability $p_t = p_f p_g$, where p_f is the probability of having fully charged battery at the beginning of the slot. Next, outage probability analysis is performed for both primary and secondary networks. Very similar system model was assumed in [44] and analysis was performed in a very similar way. The only difference is that STs are assumed to adopt variable power (VP) mode, unlike [43] which assumed ST transmission power was fixed and needed fully charged battery. A key assumption that was made in both papers to simplify analysis was to model the locations of transmitting STs by a homogeneous PPP with density $p_t \lambda_s$.

Authors in [45] considered a different setup where the primary network consists of access points (APs) and primary users (PUs). The locations of the APs and STs are modeled by PPPs Φ_P and Φ_S with densities λ_p and λ_s, respectively. Each AP is associated with a primary user at distance d_p and each ST is associated with a SR at distance d_s. The novelty of this work comes from the assumption that the only wirelessly powered devices in this system are the PUs. Authors show the weakness of the system where the primary user is solely powered by energy transferred from associated AP. They show that this system can be improved by the cooperation of the secondary network. Cooperation can be done in two way: STs transfer wireless power to PUs whenever they lie in a certain harvesting zone around the PU, or STs act as relays whenever needed for the primary link to enhance robustness. The authors demonstrate that cooperation improves the throughput of the primary network noticeably. Authors in [48] study the performance of a cognitive D2D energy harvesting network. As all the discussed work, PPP is used to model the locations of primary BSs, primary users, and secondary transmitters. The presented analysis considers multiple channels for uplink and downlink that can be accessed opportunistically by STs. Authors study the outage probability for both networks considering the case when ST uses an uplink channel or a downlink channel. The ST is assumed to be able to harvest energy from both primary downlink and uplink channels which adds further complexity to the calculation of mean harvested energy.

In [46] authors extend the problem to study the secrecy rates in an energy harvesting D2D cognitive network. The considered system consists of primary BSs, SRs, power beacons (PBs), and eavesdroppers. Their locations are modeled by PPPs Φ_b, Φ_s, Φ_p, and Φ_e with densities λ_b, λ_s, λ_p, and λ_e, respectively. The energy harvesting ST is assumed to be placed at the origin. The PBs are

used to transfer wireless power to the STs, where it is assumed that the PBs use different bands than the ones used by primary network. In order to ensure that the interference level at the BS does not exceed the threshold I_p, the transmit power of the typical ST should not exceed the following threshold

$$P_A = \min\{\frac{I_p}{\max\limits_{l\in\Phi_b}\{|\,h_l|^2 L(r_l)\}}, p_t\}, \tag{2.18}$$

where p_t is the maximum transmission power by ST, r_l is the Euclidean distance between typical ST and BS l, h_l is the channel fading gain, and $L(r_l)$ is the path loss. The ST uses one of two schemes to select the SR, it either chooses the nearest SR or the strongest SR. For example, in the nearest SR case the signal-to-noise (SNR) at the SR is:

$$\gamma_s = \frac{P_A}{N_o}|h_s|^2 \max_{s\in\Phi_s}\{L(r_s)\}, \tag{2.19}$$

where N_o is the noise power, h_s is the channel fading gain between ST and SR, and r_s is the distance between them. Similarly, the SNR at the eavesdropper with best channel conditions is:

$$\gamma_e = \frac{P_A}{N_o}\max_{e\in\Phi_e}\{L(r_e)|h_e|^2\}. \tag{2.20}$$

Defining the instantaneous secrecy rate by $C_s[\log_2(1+\gamma_s) - \log_2(1+\gamma_e)]^+$, the secrecy outage probability is derived. The secrecy outage happens either because C_s is less than a predefined threshold, or due to energy outage at ST. Energy outage at ST means that the harvested energy from PBs was not enough to perform transmission successfully. On the other hand, in order to solve for the energy outage, the probability distribution of $\mathcal{S}$ is required where:

$$\mathcal{S} = \sum_{p\in\Phi_p} |h_p|^2 L(r_p). \tag{2.21}$$

The authors derive the Laplace transform of $\mathcal{S}$ and perform some mathematical manipulations to get the CDF of $\mathcal{S}$. This concludes our brief description of the prior art on stochastic geometry-based approaches to the analysis of energy harvesting wireless networks. We now summarize the main contributions of this dissertation.

2.4 Summary

In this chapter we have provided a brief of the prior art in the area of theoretical analysis of energy harvesting wireless networks. We now discuss the technical contributions of this dissertation starting next chapter. In particular, in the next chapter, we study the joint uplink/downlink coverage of RF-powered cellular-based IoT.

Chapter 3

Joint Uplink and Downlink Coverage Analysis in RF-powered Communication Networks

As discussed earlier, ambient RF energy harvesting has emerged as a promising solution for powering small devices and sensors in massive Internet of Things (IoT) ecosystem due to its ubiquity and cost efficiency. In this chapter, we study joint uplink and downlink coverage of cellular-based ambient RF energy harvesting IoT where the cellular network is assumed to be the only source of RF energy. We consider a time division-based approach for power and information transmission where each time-slot is partitioned into three sub-slots: (i) *charging sub-slot* during which the cellular BSs act as RF chargers for the IoT devices, which then use the energy harvested in this sub-slot for information transmission and/or reception during the remaining two sub-slots, (ii) *downlink sub-slot* during which the IoT device receives information from the associated BS, and (iii) *uplink sub-slot* during which the IoT device transmits information to the associated BS. For this setup, we characterize the *joint coverage probability*, which is the joint probability of the events that the typical device harvests sufficient energy in the given time slot and is under both uplink and downlink SINR coverage with respect to its associated BS. This metric significantly generalizes the prior art on energy harvesting communications, which usually focused on downlink or uplink coverage separately. The key technical challenge is in handling the correlation between the amount of energy harvested in the charging sub-slot and the information signal quality (SINR) in the downlink and uplink sub-slots. Dominant BS-based approach is developed to derive tight approximation for this joint coverage probability. Several system design insights including comparison with regularly powered IoT network and throughput-optimal slot partitioning are also provided.

3.1 Introduction

IoT is a massive ecosystem of interconnected *things* (referred to as IoT devices) with sensing, processing, and communication capabilities [49]. Due to its ubiquity, cellular network has emerged as an attractive option to provide reliable communication infrastructure for supporting and managing these networks [50–53]. This new communication paradigm will enable a new era of applications including medical applications, transportation, surveillance, and smart homes to name a few. Unlike human-operated cellular devices, such as smart phones and tablets, that can be charged at will, these IoT devices may be deployed at hard-to-reach places, such as underground or in the tunnels, which makes it difficult to charge or replace their batteries. This has led to an increasing interest in energy-efficient communication of IoT devices, both from the system design [51–53], and hardware perspectives [54]. While these efforts will increase the lifetime of these devices, they do not necessarily make them *self-sustained* in terms of their energy requirements. One possible way to develop an almost *self-perpetuating IoT network* is to complement or even circumvent the use of conventional batteries in the IoT devices by energy harvesting. While one can use any energy harvesting method depending upon the deployment scenario, such as solar energy, thermo-electronic, and mechanical energy [2], we focus on the ambient RF energy harvesting [47, 55], where the IoT device harvests energy through wireless RF signals. This is because of the ubiquity of RF signals even at hard-to-reach places where the other popular sources, such as solar or wind, may not be available. Besides, RF energy harvesting modules are usually cheaper to implement, which is another consideration in the deployment of IoT devices [56]. Now if RF energy harvested from the communication network (cellular network in this case) is the only source of energy, there will obviously be some new design considerations due to the limitations in the energy availability and the correlation in the communication and energy harvesting performance [57]. In this chapter, we concretely expose these design considerations using tools from stochastic geometry. In particular, we define and analyze a new *joint coverage probability* metric, which significantly generalizes prior art in this area. Before going into the details of our contributions, we discuss prior art next.

3.1.1 Related Work

As explained in Section 2.3 in Chapter 2, tools from stochastic geometry have received significant attention over the past few years for the system-level analysis of cellular networks. Interested readers are advised to refer to [30, 32, 58, 59] and the references therein for a more pedagogical treatment of this topic. More relevant subset of these works for this chapter is the one that focuses on characterizing the performance of energy harvesting communication networks; see [33, 36–39, 60] for a small subset. In this Subsection, we will discuss these works in the broader context of uplink, downlink, and joint uplink/downlink coverage analyses.

Uplink analysis. Most of the stochastic geometry-based works in this area are focused on the setups in which the device of interest first harvests ambient RF energy and then transmits information to its designated node (which will be its *serving BS* in the uplink cellular network) using this en-

ergy. Since the device that harvests energy is also the one that transmits information, we discuss all these works under the category of *uplink analysis* to put things in the correct context. The general theme of these works is to study the joint energy and uplink SINR coverage, which is defined as the joint probability of harvesting sufficient ambient RF energy to enable uplink transmission, and having uplink SINR above a predefined threshold. The energy and uplink SINR coverage events are independent by construction if one assumes that the ambient RF sources are placed independently of the communication network [36, 39, 60]. A few representative works in this direction are discussed next. Authors in [39] studied a system of energy harvesting wireless sensor network where a sensor node harvests ambient RF energy from the broadcast TV, radio, and cellular signals. The sensor node uses this energy to transmit information to a data sink located at a fixed distance. Authors in [60] studied a point-to-point (source-destination) communication link consisting of an energy harvesting source that is powered by a power beacon (PB). In particular, the source harvests power from the RF signals of PB using which it transmits information to its destination. The assumption of the existence of dedicated PBs was then generalized in [36] which studied the uplink performance of a cellular network in which mobile users are powered by a network of PBs. The other general setup, in which the prior art is significantly sparser, is the one where the same network of BSs is used for charging and communication [37, 38]. This naturally correlates the energy and uplink SINR coverage events. However, to maintain tractability, all prior works study energy and uplink coverage events separately with [37] justifying it by assuming full channel inversion power control. While such simplifications may work in specific system setups, it is desirable to handle correlation in the two coverage events properly, which will be done as a special case of our analysis.

Downlink analysis. Another general theme in the literature is to explore setups in which the device of interest first harvests ambient RF energy and then uses it to receive information. We will discuss all these works under the general category of *downlink analysis*. In small devices with severely limited power budgets, which is the case for IoT devices, energy consumption during information reception can be almost as important as the energy consumption during uplink transmission. For instance, many recent works have shown that receiver energy consumption scales noticeably with the data rates due to increase in the length of decoder interconnects [61–63]. Motivated by this general fact, some aspects of system design have already been explored with the consideration of receiver energy consumption, e.g., see [41, 64, 65] for a subset. For instance, authors in [41] used tools from stochastic geometry to study the SINR outage probability and average energy harvested under power splitting at the receiver in a system of randomly placed transmitter-receiver pairs where each transmitter has a unique receiver at a fixed distance. The main objective is to minimize the SINR outage probability subject to a constraint on the minimum average harvested energy. Authors in [64] explored power splitting receiver architecture in a point-to-point system to study the tradeoff between the average harvested energy and the average data rate. For this setup, the achievable rate-energy regions are also derived for different types of receiver architectures. Finally, [65] explored power control policies for outage minimization in a point-to-point link assuming energy harvesting at both the transmitter and the receiver. The outage is said to occur if the signal-to-noise ratio (SNR) is low or the energy harvested at the transmitter or receiver is not high enough. Contrary to all these works, which are more applicable to ad hoc or decentralized net-

works, the joint analysis of harvested energy and downlink SINR in a cellular setup was recently performed in [66, 67]. In [66], since the exact analysis does not provide insightful results, authors use Frechet's inequality to derive an upper bound on the joint downlink energy and SINR coverage probability. In this chapter, we will derive joint energy and downlink SINR coverage probability as the special case of our general result.

As is evident from the above discussion, all the prior works on stochastic geometry-based analyses of cellular networks with energy harvesting users/devices are either focused on uplink or downlink. To the best of our knowledge, there is no work that deals with joint uplink/downlink coverage probability defined by the joint energy, uplink SINR, and downlink SINR coverage probability, which is the main focus of this chapter. That being said, the joint downlink and uplink coverage has received some attention recently in the *regularly powered networks*[1] [68–70]. For instance, authors in [68] use a 3GPP simulation model to determine whether it is appropriate to assume independence in the uplink and downlink coverage events. The simulation results demonstrate that the two events cannot be treated as independent. This is due to the correlation that results from associating with the same BS in both uplink and downlink. Sometimes this correlation is ignored in the interest of tractability. For instance, in [69], authors derive the joint uplink/downlink coverage probability as the product of two coverage probabilities. For more accurate analysis, one should of course capture this correlation explicitly, as done in [70], where the authors provided the accurate joint distribution of uplink and downlink path-loss for generalized uplink/downlink cell association policies (associating with the same BS in both channels is a special case). Assuming independent interference levels over uplink and downlink channels, they use this joint distribution to derive the joint uplink/downlink coverage.

In this chapter we study the performance of *on-the-fly* reception/transmission in a cellular-based IoT network where the IoT devices first harvest energy and then use it to receive/transmit information in the same time slot. Assuming cellular transmissions to be the only source of RF energy for the IoT devices, we study the joint probability of a typical IoT device harvesting sufficient energy *and* achieving both uplink and downlink SINR thresholds with respect to its associated BS in a given time slot. As noted already, we will refer to this as *uplink/downlink coverage probability* in this chapter. Since the same infrastructure (cellular BSs) is used for charging and communication, there is inherent correlation in the energy and uplink/downlink coverage events, which is carefully incorporated in our analysis. Please refer to Section 3.2 for more details on the system setup. We now summarize the contributions of this chapter.

3.1.2 Contributions and Outcomes

Cellular-based IoT model. We develop a comprehensive model for cellular-based RF-powered IoT network in which the locations of the BSs and the IoT devices are modeled using two independent PPPs. Each time slot is assumed to be partitioned into three sub-slots: (i) *charging sub-slot*, in

[1]Throughout this chapter, we will refer to the IoT networks in which the IoT devices have uninterrupted access to a reliable energy source, such as power grid or a battery, as the regularly powered networks.

which the received power from the cellular network is used for charging devices to enable them to perform information transmission/reception in the next two sub-slots, (ii) *downlink sub-slot*, in which the devices receive information from their associated BSs, and (iii) *uplink sub-slot*, in which the devices transmit information to their associated BSs using *fractional* channel inversion power control. Contrary to the prior works discussed above that focused on the separate analysis of uplink and downlink coverage, in this chapter we focus on the analysis of joint uplink/downlink coverage (defined as the joint probability of energy coverage, uplink SINR coverage, and downlink SINR coverage). Since cellular network is assumed to be the only source of RF energy for the IoT devices, the energy and uplink/downlink coverage events are tightly coupled through the locations of the cellular BSs. In particular, the amount of energy harvested by each device is highly correlated with both the uplink and downlink SINR achieved by that device. Naturally, the uplink and downlink coverage events are also coupled. As discussed next, we carefully handle this correlation in our analysis, which is also one of the main technical contributions of this chapter.

Joint uplink/downlink coverage analysis. As stated already, we define joint uplink/downlink coverage as the joint probability that the typical device harvests sufficient energy in the first sub-slot, achieves high enough downlink SINR in the second sub-slot, and achieves high enough uplink SINR in the third sub-slot. These three events are correlated because of their dependence on the point processes modeling the devices and the BSs. That being said, if we assume independent fading across the three sub-slots and condition on the point processes, the three events become *conditionally* independent. We therefore, derive the conditional probabilities of the three events first. The complexity of this problem should be evident from the following two facts: (i) the exact characterization of uplink SINR in a conventional single-tier cellular setup is not known in the stochastic geometry literature [30], and (ii) the total energy harvested is essentially a power-law shot noise field whose probability distribution function is not known in general. On top of these challenges, we need to jointly decondition (average) over the point processes in order to obtain the joint uplink/downlink coverage, which adds to the complexity of the problem. We overcome all these challenges by developing a dominant BS-based approximation approach that not only provides a tight approximation for the power-law shot noise field (energy harvested) but also facilitates joint deconditioning over the point processes. The tightness of the approximate joint coverage expression is verified by comparing it with the simulation results.

Useful system insights. Our analytical results provide several useful system insights. First, we demonstrate the existence of optimal time-slot partitioning that maximizes system throughput. The effect of other system parameters on this optimal partitioning is studied numerically. We then compare the performance of the RF-powered IoT system with the one in which IoT devices have access to a reliable power source (termed regularly powered network). Our analytical results reveal several interesting thresholds beyond which the performance of this RF-powered network is similar to that of the regularly powered network. For instance, we show that if the distance of the typical device to the second closest BS is below a certain threshold, its downlink coverage performance would be the same as the regularly powered network. We further study the effect of other system parameters including time-slot partitioning parameters, cellular network density, RF-DC conversion efficiency, and cellular network transmission power on the system performance.

Figure 3.1: Illustration of the system setup and the three sub-slots (charging, downlink, and uplink).

We show how these parameters can be tuned in order to get the performance of this RF-powered network closer to that of a regularly powered network. This is done by defining a *tuning parameter* that captures the effect of the aforementioned system parameters. Our analysis shows that in order to get the performance of this RF-powered network closer to the regularly powered network, it is only required to make sure that this tuning parameter is large enough.

3.2 System Model

We consider a cellular-based IoT network in which the IoT devices are solely powered by the ambient RF energy. In this work, we assume that the cellular transmissions are the only source of ambient RF energy for these devices. Quite reasonably, the IoT devices are assumed to be batteryless (similar to [9, 10]). The more general case of finite-sized battery is left for future work. In particular, we assume that all the energy required for uplink and/or downlink communication by a device in a given time slot will need to be harvested by that device in the same time slot[2]. More details will be provided shortly. The locations of the cellular network BSs and the IoT devices are

[2]The IoT device uses a supercapacitor to store the harvested energy. The large charging and discharging rates of the supercapacitor enable using the harvested energy during the same time slot. However, due to supercapacitor's

modeled by two independent PPPs $\Phi_b \equiv \{x_i\} \subset \mathbb{R}^2$ and $\Phi_u \equiv \{u_i\} \subset \mathbb{R}^2$ with densities λ_b and λ_u, respectively [71]. As will be the case in reality, we assume $\lambda_u > \lambda_b$.

As implied in Fig. 3.1, we assume that each IoT device adopts the time-switching receiver architecture (see [55]) in which the antenna is used for energy harvesting for a given fraction of time and for communication for the rest of the time. The time slot duration is assumed to be T (seconds). As shown in Fig. 3.1, each time-slot is further divided into charging, downlink, and uplink sub-slots with durations $T_{\rm ch} = \tau_1 T$, $T_{\rm tr}^{\rm DL} = \tau_2 T$, and $T_{\rm tr}^{\rm UL} = \tau_3 T$, respectively. During the *charging sub-slot*, all the BSs in the network act as RF chargers for the IoT devices. In the downlink and uplink sub-slots, each IoT device receives and sends information to its associated BS, respectively. This system setup will facilitate the analysis of joint uplink/downlink coverage probability thus generalizing the prior work on energy harvesting networks that focused on the analysis of downlink and uplink separately. Naturally, if we substitute $\tau_2 = 0$, we can focus only on the uplink analysis, which we refer to as the *uplink mode*. Similarly, if we substitute $\tau_3 = 0$, we can focus only on the downlink analysis, which we refer to as the *downlink mode*. The general case in which τ_2 and τ_3 are both non-zero will be referred to as the *joint uplink/downlink mode*. Our analysis will be performed under the following assumptions: (i) each IoT device connects to its *nearest* BS (referred to as *tagged* BS in the rest of the chapter), (ii) fading gains across all links are independent, (iii) fading gains across the same link in charging sub-slot (denoted by g_x), downlink sub-slot (denoted by h_x), and uplink sub-slot (denoted by w_x) are independent, (iv) all channels suffer from Rayleigh fading. This means that g_x, h_x, and w_x are all independent exponential random variables with mean 1. Under these assumptions, we focus our analysis on a typical device placed at the origin (without loss of generality due to the stationarity of PPP). We now enrich our notation to express key metrics of interest for each sub-slot.

In the charging sub-slot, we are interested in measuring the amount of energy harvested by the typical device. In order to do that, we first model the received power at the typical device from a BS located at $x \in \Phi_b$ as $P_{\rm t} g_x \|x\|^{-\alpha}$, where $g_x \sim \exp(1)$ is the fading gain, $P_{\rm t}$ is the transmission power (assumed to be the same for all the BSs), and $\|x\|^{-\alpha}$ models standard power law path-loss with exponent $\alpha > 2$. The total energy harvested by the typical device is thus

$$E_{\rm H} = \tau_1 T \eta \sum_{x \in \Phi_b} P_{\rm t} g_x \|x\|^{-\alpha} \text{ Joules}, \tag{3.1}$$

where $\eta < 1$ represents the efficiency of the RF-to-DC conversion.

In the downlink and uplink sub-slots, we are interested in the expressions for the respective SINRs. For the downlink sub-slot, the the SINR at the typical device is

$$\text{SINR}_{\rm DL} = \frac{P_{\rm t} h_{x_1} \|x_1\|^{-\alpha}}{\sum_{x \in \Phi_b \setminus x_1} P_{\rm t} h_x \|x\|^{-\alpha} + \sigma_{\rm DL}^2} = \frac{P_{\rm t} h_{x_1} \|x_1\|^{-\alpha}}{I_1 + \sigma_{\rm DL}^2}, \tag{3.2}$$

where $h_x \sim \exp(1)$ represents the fading gain between the typical device and the BS located at x, x_1 is the location of the nearest (tagged) BS, I_1 denotes the interference power, and $\sigma_{\rm DL}^2$ models

relatively large leakage current, any unused energy remaining by the end of the time-slot is assumed to be unavailable for use during the next time-slot.

Figure 3.2: Key variables used in the uplink analysis.

thermal noise power. For successful reception in the downlink sub-slot, the received SINR needs to be greater than a modulation-and-coding specific target SINR β_{DL}. In addition, the IoT device needs a minimum amount of energy E_{rec} in order to be able to activate its receiving chain circuitry and receive data successfully during the downlink sub-slot.

In the uplink sub-slot, each IoT device is assumed to perform uplink fractional channel inversion power control. Hence, if the distance between the IoT device and its serving BS is R, then the transmitted power is $\rho R^{\epsilon\alpha}$, where ρ is the BS sensitivity, and $\epsilon \in [0,1]$ is the power control parameter. Therefore, the typical IoT device requires $\tau_3 T \rho R^{\epsilon\alpha}$ energy in order to perform uplink transmission. We refer to IoT devices that have enough energy to transmit in the uplink sub-slot as *active* devices. Focusing our analysis on the typical device located at the origin, the uplink SINR for this device measured at its tagged BS is:

$$\mathrm{SINR}_{\mathrm{UL}} = \frac{w_o \rho \|x_1\|^{(\epsilon-1)\alpha}}{\sum\limits_{u_i \in \Phi_a \setminus u_o} \delta_i w_i \rho \left(R_1^{(i)}\right)^{\epsilon\alpha} D_i^{-\alpha} + \sigma^2_{\mathrm{UL}}}, \tag{3.3}$$

where Φ_a is the point process representing all the devices (including the typical device) that are scheduled on the same time-frequency resource as the typical device, σ^2_{UL} models thermal noise power, $w_i \sim \exp(1)$ is the channel fading gain between the device located at u_i and the tagged BS during uplink information sub-slot, x_1 is the location of the tagged BS, $D_i = \|u_i - x_1\|$ is the distance between the device located at u_i and the tagged BS, $R_1^{(i)}$ is the distance between the device located at u_i and its serving BS (which is the closest BS to this device by definition), and u_o is the location of the typical device. Also δ_i is an indicator function that equals to 1 if the IoT device located at u_i is *active*, and 0 otherwise. Please refer to Fig. 3.2 for the summary of this uplink-specific notation. As was the case in downlink, this SINR needs to be greater than a modulation-and-coding specific target SINR threshold β_{UL} for successful transmission.

Table 3.1: Table of Notations for Chapter 3

Notation	Description
Φ_b; λ_b	PPP modeling the locations of BSs in the cellular network; density of the BSs
Φ_u; λ_u	PPP modeling the locations of IoT devices; density of the IoT devices
τ_1; τ_2; τ_3	Time-slot division parameter for charging sub-slot; downlink sub-slot; uplink sub-slot
E_{H}	Amount of energy harvested from ambient RF signals (in Joules)
D_{avg}	Average data rate (throughput)
$P_{\mathrm{cov}}^{\mathrm{DL,RP}}$; $P_{\mathrm{suc}}^{\mathrm{UL,RP}}$	Downlink coverage probability; uplink coverage probability in a regularly powered network
$P_{\mathrm{cov}}^{\mathrm{DL}}$; $P_{\mathrm{suc}}^{\mathrm{UL}}$; $P_{\mathrm{suc}}^{\mathrm{J}}$	Downlink coverage probability; uplink coverage probability; joint uplink/downlink coverage probability in the ambient RF powered network
g_x; h_x; w_x	Fading gains during charging; downlink; uplink sub-slots (assumed to be i.i.d. across all links). Rayleigh fading is assumed
W_D (W_U)	Bandwidth of the downlink channel (uplink channel)
P_t; ρ	BS transmission power; BS sensitivity
ϵ; α	Power control parameter; path loss exponent ($\alpha > 2$)
r_1 (r_2)	Distance between typical IoT device and its nearest BS (2nd nearest BS)

Joint uplink/downlink coverage. With this, we are now ready to formally introduce the key metric of interest for this chapter: the joint uplink/downlink coverage probability. Recall that the total energy harvested by a device in the charging sub-slot is used by that device to receive information from the tagged BS during the downlink sub-slot and transmit information to the tagged BS during the uplink sub-slot. Hence, the energy coverage condition for this case is:

$$E_{\mathrm{H}} \geq E_{\min}, \tag{3.4}$$

where $E_{\min} = E_{\mathrm{rec}} + \tau_3 T \rho r_1{}^{\epsilon\alpha}$, $r_1 = \|x_1\|$ is the distance between the typical IoT device and its nearest BS. For completeness, three conditions need to be satisfied for uplink/downlink coverage: (i) $E_{\mathrm{H}} > E_{\min}$, (ii) $\mathrm{SINR}_{\mathrm{DL}} > \beta_{\mathrm{DL}}$ in the downlink sub-slot, and (iii) $\mathrm{SINR}_{\mathrm{UL}} > \beta_{\mathrm{UL}}$ in the uplink sub-slot. Therefore, the joint uplink/downlink coverage probability is defined as:

$$P_{\mathrm{suc}}^{\mathrm{J}} = \mathbb{E}\left[\mathbb{1}(\mathrm{SINR}_{\mathrm{DL}} \geq \beta_{\mathrm{DL}})\mathbb{1}(\mathrm{SINR}_{\mathrm{UL}} \geq \beta_{\mathrm{UL}})\mathbb{1}(E_{\mathrm{H}} \geq E_{\min})\right]. \tag{3.5}$$

As noted already, when τ_2 and τ_3 are both non-zero, we call this a *joint uplink/downlink mode*. As discussed next, if one of them is zero, we can specialize the above definition of joint coverage to study downlink or uplink coverage probability separately.

Downlink coverage. If we substitute $\tau_3 = 0$, each time slot is partitioned into charging and downlink sub-slots. We referred to this as the *downlink mode* above. Since each device in this mode only needs to perform downlink transmission, the energy coverage condition reduces to $E_{\mathrm{H}} > E_{\mathrm{rec}}$. Consequently, the downlink coverage probability for this case can be defined as:

$$P_{\mathrm{cov}}^{\mathrm{DL}} = \mathbb{E}\left[\mathbb{1}(\mathrm{SINR}_{\mathrm{DL}} \geq \beta_{\mathrm{DL}})\mathbb{1}(E_{\mathrm{H}} \geq E_{\mathrm{rec}})\right]. \tag{3.6}$$

Clearly (3.6) can be obtained from (3.5) by substituting $\tau_3 = 0$, $\beta_{\mathrm{UL}} = 0$ and using $E_{\mathrm{H}} > E_{\mathrm{rec}}$ as the energy condition. If $\mathrm{SINR}_{\mathrm{DL}} \geq \beta_{\mathrm{DL}}$ and $E_{\mathrm{H}} \geq E_{\mathrm{rec}}$ (i.e., the IoT device is able to establish

a communication link with the BS), the downlink data rate is $R = W_D \log(1 + \beta_{\mathrm{DL}})$ bps in the information sub-slot, where W_D is the bandwidth of the downlink channel.

Uplink coverage. Similarly, if we substitute $\tau_2 = 0$, there is no downlink sub-slot and each time slot is partitioned into only charging and uplink sub-slots. This was referred to as the *uplink mode* earlier in this Section. Since each IoT device now needs to perform only uplink communication, the energy coverage condition for this case is $E_{\mathrm{H}} > \tau_3 T \rho R^{\epsilon\alpha}$. This along with the uplink SINR coverage condition gives the following definition for the uplink coverage probability:

$$P_{\mathrm{suc}}^{\mathrm{UL}} = \mathbb{E}\left[\mathbb{1}(\mathrm{SINR}_{\mathrm{UL}} \geq \beta_{\mathrm{UL}})\mathbb{1}(E_{\mathrm{H}} \geq \tau_3 T \rho {r_1}^{\epsilon\alpha})\right]. \tag{3.7}$$

As was the case for downlink coverage above, (3.7) can be obtained from (3.5) by substituting $\tau_2 = 0$, $\beta_{\mathrm{DL}} = 0$ and using $E_{\mathrm{H}} > \tau_3 T \rho r_1^{\epsilon\alpha}$ as the energy condition. If the two coverage conditions ($\mathrm{SINR}_{\mathrm{UL}} \geq \beta_{\mathrm{UL}}$ and $E_{\mathrm{H}} \geq \tau_3 T \rho {r_1}^{\epsilon\alpha}$) are satisfied, the uplink data rate is $R = W_U \log(1 + \beta_{\mathrm{UL}})$ bps in the information sub-slot, where W_U is the bandwidth of the uplink channel.

As evident from the above discussion, joint uplink/downlink coverage probability encompasses the other two as special cases. We will therefore start with the analysis of this general case. The results for the downlink and uplink modes will be provided as special cases of this general setup to provide useful system design insights.

3.3 Joint Uplink and Downlink Mode

This is the first technical section of this chapter in which we will evaluate the joint uplink/downlink coverage probability defined in (3.5). In particular, our goal is to evaluate the joint probability of the following three events: (i) $\mathrm{SINR}_{\mathrm{DL}} \geq \beta_{\mathrm{DL}}$, (ii) $\mathrm{SINR}_{\mathrm{UL}} \geq \beta_{\mathrm{UL}}$, and (iii) $E_{\mathrm{H}} \geq E_{\min}$. Keeping the joint treatment aside, the complexity of this analysis should be evident from the following two facts: (i) the exact characterization of $\mathbb{P}\left(\mathrm{SINR}_{\mathrm{UL}} \geq \beta_{\mathrm{UL}}\right)$ is not known in the stochastic geometry literature [30, 72], and (ii) the total energy harvested is essentially a power-law shot noise field whose probability density function is not known in general. To make matters worse, all these events depend upon the point process Φ_b modeling the locations of the BSs, which necessitates their joint analysis. This dependence on Φ_b is quite evident for both E_{H} and $\mathrm{SINR}_{\mathrm{DL}}$ from their expressions given by (3.1) and (3.2). While $\mathrm{SINR}_{\mathrm{UL}}$ may not appear to depend on Φ_b on the first look (see (3.3)), the point processes of the devices and BSs are correlated though cell selection and resource scheduling (see [30] for the detailed discussion), which couples the uplink coverage event with the other two events. Therefore, the main challenge in our analysis is the joint treatment of these three coverage events. That being said, since the main source of this correlation, as evident from (3.1), (3.2), (3.3), is the dependence of the three events on Φ_b, they can be treated as independent when conditioned on Φ_b since the fading gains (h_x, g_x, and w_x) in the three sub-slots are assumed independent. Consequently, the joint uplink/downlink coverage probability defined in (3.5) can be expressed as

$$P_{\mathrm{suc}}^{\mathrm{J}} = \mathbb{E}_{\Phi_b}\left[\mathbb{P}\left(\mathrm{SINR}_{\mathrm{DL}} \geq \beta_{\mathrm{DL}} \middle| \Phi_b\right) \mathbb{P}\left(\mathrm{SINR}_{\mathrm{UL}} \geq \beta_{\mathrm{UL}} \middle| \Phi_b\right) \mathbb{P}\left(E_{\mathrm{H}} \geq E_{\min} \middle| \Phi_b\right)\right]. \tag{3.8}$$

In the following subsections, we carefully approximate the three conditional probability terms using a dominant BS-based approach. The resulting expressions will then be used to derive our main result for the the joint uplink/downlink coverage probability in Theorem 1.

3.3.1 Conditional Energy Coverage Probability

As discussed above, $\mathrm{SINR}_{\mathrm{DL}}$ and E_{H} both depend upon Φ_b explicitly. However, due to pathloss, the BSs located far away from the typical device do not contribute as much to both these terms as the BSs located close to the typical point. Therefore, we reduce the dimensionality of this problem by considering the effect of closest two BSs to the typical device exactly and approximating the effect of the rest of the BSs. It will be clear shortly why we chose two and not any other number. This dominant BS-based approach is useful when the exact analysis is either too difficult or leads to unwieldy results. It has been used in the past to analyze the coverage of ad hoc networks [73], coverage of downlink cellular networks [74], k-coverage of localization networks [75, 76], and downlink coverage of wireless networks of unmanned aerial vehicles [77, 78]. Since all these works focused on some form of (marginal) SINR-based coverage, they are not applicable to our analysis because of the need to perform conditional analysis of each term separately and then decondition jointly over all the terms. These works are listed here mainly for completeness.

We apply this approach to approximate the total energy harvested by the typical device in the charging sub-slot (given by (3.1)) by the energy harvested from the nearest two BSs (located at distances $r_1 = \|x_1\|$ and $r_2 = \|x_2\|$ from the typical device) and the conditional mean (conditioned on the location of the nearest 2 BSs) of the rest of the terms as follows:

$$E_{\mathrm{H}} = \tau_1 T \eta P_{\mathrm{t}} \sum_{x \in \Phi_b} g_x \|x\|^{-\alpha} \approx \tau_1 T \eta P_{\mathrm{t}} \left(g_{x_1} \|x_1\|^{-\alpha} + g_{x_2} \|x_2\|^{-\alpha} + \Psi(r_2) \right), \tag{3.9}$$

where $\Psi(r_2) = \mathbb{E}\left[\sum_{x \in \Phi_b \setminus x_1, x_2} g_x \|x\|^{-\alpha} \middle| x_1, x_2 \right]$. We will use this approximation to compute the conditioned energy coverage probability $\mathbb{P}(E_H \geq \mathbb{E}_{\min} | \Phi_b)$ which is necessary for the computation of $P_{\mathrm{suc}}^{\mathrm{J}}$ as explained above. In addition to enabling the joint coverage analysis, this approximation will also lead to several crisp system design insights. For instance, as a result of using this approximation, we will be able to define a threshold on r_2 (as well as λ_b and time switching parameters) below which the performance is approximately equivalent to that of a regularly powered cellular-based IoT (further discussion will be provided in Remarks 5 and 8). As discussed already, the typical IoT device needs to harvest a minimum amount of energy $E_{\min} = E_{\mathrm{rec}} + \tau_3 T \rho \|x_1\|^{\epsilon\alpha}$ to be able to receive and transmit information. If it is able to harvest this energy, it is said to be in *energy coverage*. In the following Lemma we derive an expression for the conditional energy coverage probability using the approximation in (3.9).

Lemma 1 (Conditional Energy Coverage Probability)**.** *Probability that the harvested energy dur-*

ing the charging sub-slot is greater than $E_{\min}$ conditioned on the point process Φ_b is

$$\mathbb{P}\left(E_{\mathrm{H}} \geq E_{\min}\middle|\Phi_b\right) = \frac{r_2^{\alpha}\exp\left(-r_1^{\alpha}\left[\mathcal{F}(r_1,r_2)\right]^{+}\right) - r_1^{\alpha}\exp\left(-r_2^{\alpha}\left[\mathcal{F}(r_1,r_2)\right]^{+}\right)}{r_2^{\alpha}-r_1^{\alpha}}, \tag{3.10}$$

while the unconditioned probability is

$$\begin{aligned}\mathbb{P}\left(E_{\mathrm{H}} \geq E_{\min}\right) = &\int_0^{\infty}\int_{r_1\in\mathcal{N}_{r_2}} f_{R_1,R_2}(r_1,r_2)\mathrm{d}r_1\mathrm{d}r_2 \\ &+ \int_0^{\infty}\int_{r_1\in\mathcal{P}_{r_2}} f_{R_1,R_2}(r_1,r_2)\frac{r_2^{\alpha}\exp\left(-r_1^{\alpha}\mathcal{F}(r_1,r_2)\right) - r_1^{\alpha}\exp\left(-r_2^{\alpha}\mathcal{F}(r_1,r_2)\right)}{r_2^{\alpha}-r_1^{\alpha}}\mathrm{d}r_1\mathrm{d}r_2,\end{aligned} \tag{3.11}$$

where $\mathcal{F}(r_1,r_2) = \left[C(\tau_1) + \frac{\tau_3\rho r_1^{\epsilon\alpha}}{\tau_1\eta P_{\mathrm{t}}} - \frac{2\pi\lambda_b}{\alpha-2}r_2^{2-\alpha}\right]$, $C(\tau_1) = \frac{E_{\mathrm{rec}}}{\tau_1 T\eta P_{\mathrm{t}}}$, $[x]^{+} = \max\{0,x\}$, $f_{R_1,R_2}(r_1,r_2) = (2\pi\lambda_b)^2 r_1 r_2 e^{-\lambda_b\pi {r_2}^2}$, $\mathcal{N}_{r_2} = \{r_1 : \mathcal{F}(r_1,r_2) \leq 0,\ r_1 < r_2\}$, *and* $\mathcal{P}_{r_2} = \{r_1 : \mathcal{F}(r_1,r_2) \geq 0,\ r_1 < r_2\}$.

Proof: See Appendix A.1.
As explained before, the above expression can be used to compute the energy coverage probability in the downlink mode by eliminating uplink conditions and vice versa for the uplink mode. The complete results for these special cases will be presented in Lemmas 4 and 5.

3.3.2 Conditional SINR Coverage Probability

As a result of using the approximation introduced in (3.9), the conditional energy coverage probability in (3.10) is only a function of the distances r_1 and r_2 (between the typical device and its nearest two BSs). Keeping in mind that we will have to jointly decondition on all the coverage events at the end (as evident from (3.8)), it will be useful to derive conditional downlink SINR coverage also in terms of r_1 and r_2. In order to do that, we use the same dominant BS-based approach that we used in the previous Subsection. In particular, we approximate the interference in the denominator of SINR in (3.2) by the interference from the second nearest BS (strongest interferer) and the expectation of the interference from the rest of the BSs. Under this approximation, the conditional downlink SINR coverage probability becomes $\mathbb{P}\left(\mathrm{SINR}_{\mathrm{DL}} \geq \beta_{\mathrm{DL}}\middle|r_1,r_2\right)$. A tractable expression for this conditional probability is derived next.

Lemma 2 (Conditional Downlink SINR Coverage Probability)**.** *Probability that the downlink SINR at the typical device exceeds β_{DL}, conditioned on r_1 and r_2, is*

$$\mathbb{P}\left(\mathrm{SINR}_{\mathrm{DL}} \geq \beta_{\mathrm{DL}}\middle|r_1,r_2\right) = \exp\left(-\mathcal{G}(r_1,r_2)\right)\frac{1}{1+\frac{\beta_{\mathrm{DL}}r_1^{\alpha}}{r_2^{\alpha}}}, \tag{3.12}$$

where $\mathcal{G}(r_1,r_2) = \frac{\beta_{\mathrm{DL}}\sigma_{\mathrm{DL}}^2 r_1^{\alpha}}{P_{\mathrm{t}}} + \frac{2\pi\lambda\beta_{\mathrm{DL}}r_1^{\alpha}}{(\alpha-2)r_2^{\alpha-2}}$.

Proof: See Appendix A.2.
With this, we are now left with deriving the conditional uplink probability, which we do next. It is noteworthy that uplink analysis is known to be a challenging problem even for regularly powered networks. The locations of the devices scheduled in the same time frequency resource block as the typical device (modeled as point process $\Phi_a \backslash u_o$ in (3.3)) are correlated with the locations of the BSs due to the structure of the Poisson Voronoi tessellation. This correlation is further enhanced due to uplink power control, where the transmission power of each device is a function of its distance to its serving BS. As discussed in [30], the exact analysis of this setup in not known. It has, however, been shown that modeling the locations of the devices by an independent PPP and handling dependence between the distances D_i and $R_1^{(i)}$ (as defined in (3.3)) appropriately leads to a fairly tight approximation. For the latter, it is sufficient to just account for the fact that $R_1^{(i)} < D_i$, i.e., the serving BS must be closer to the interfering device than the tagged BS. Please refer to [30] for more details. Using this general idea, the Laplace transform of the aggregate interference $I_2 = \sum_{u_i \in \Phi_a \backslash u_o} w_i \left(R_1^{(i)}\right)^{\epsilon\alpha} D_i^{-\alpha}$ at the tagged BS in a regularly powered network was given in [30] as follows:

$$\mathcal{L}_{I_2}(s) = \mathbb{E}\left[e^{-I_2 s}\right] = \exp\left(-2\pi\lambda_b \int_0^\infty \int_0^{x^2} \frac{1}{1+(s)^{-1}u^{-\alpha\epsilon/2}x^\alpha} \pi\lambda_b e^{-\lambda_b \pi u} \mathrm{d}u x \mathrm{d}x\right), \quad (3.13)$$

where Φ_a is the point process modeling the locations of the selected devices in a given time-frequency resource. This expression was used to derive the uplink coverage probability for regularly powered networks in [30] as follows:

$$P_{\mathrm{suc}}^{\mathrm{UL,RP}} = \int_0^\infty f_{R_1}(r_1) e^{\left(-\frac{\beta_{\mathrm{UL}}\sigma_{\mathrm{UL}}^2}{\rho {r_1}^{(\epsilon-1)\alpha}}\right)} \mathcal{L}_{I_2}\left(\frac{\beta_{\mathrm{UL}}}{{r_1}^{(\epsilon-1)\alpha}}\right) \mathrm{d}r_1, \quad (3.14)$$

where $f_{R_1}(r_1) = 2\pi\lambda_b r_1 \exp(-\pi\lambda_b r_1^2)$. We will use this expression to compare the performance of the proposed setup to that of the regularly powered networks.

Coming to the conditional uplink coverage in the proposed energy harvesting setup, note that the dominant source of correlation between uplink SINR and the other two terms (downlink SINR and the amount of energy harvested) is the serving distance r_1. If we condition on r_1 and treat Φ_a and Φ_b as independent point processes (as done above), the conditional uplink coverage probability reduces to $\mathbb{P}\left(\mathrm{SINR}_{\mathrm{UL}} \geq \beta_{\mathrm{UL}} \middle| r_1\right)$, which is derived in the next Lemma.

Lemma 3 (Conditional Uplink SINR Coverage Probability)**.** *Probability that the uplink SINR of the typical device at the tagged BS is greater than β_{UL}, conditioned on r_1, is*

$$\mathbb{P}\left(\mathrm{SINR}_{\mathrm{UL}} \geq \beta_{\mathrm{UL}} \middle| r_1\right) = e^{\left(-\frac{\beta_{\mathrm{UL}}\sigma_{\mathrm{UL}}^2}{\rho {r_1}^{(\epsilon-1)\alpha}}\right)} \mathcal{L}_{\tilde{I}_2}\left(\frac{\beta_{\mathrm{UL}}}{{r_1}^{(\epsilon-1)\alpha}}\right), \quad (3.15)$$

where $\mathcal{L}_{\tilde{I}_2}(s)$ is given by (3.13) by replacing λ_b with $\tilde{\lambda}_b = P_h\lambda_b$, where $P_h = \mathbb{P}(E_{\mathrm{H}} \geq E_{\min})$.

Proof: See Appendix A.2.

3.3.3 Joint Uplink/Downlink Coverage Probability

Having derived the three conditional probability terms appearing in (3.8) in Lemmas 1, 2, and 3, we are now ready to derive the joint uplink/downlink coverage probability. The only remaining step is to uncondition their product with respect to the joint distribution of r_1 and r_2, which results in the following Theorem.

Theorem 1 (Joint uplink/downlink coverage probability)**.** *The joint uplink/ downlink coverage probability $P_{\text{suc}}^{\text{J}}$ of the typical IoT device with downlink and uplink SINR thresholds β_{DL} and β_{UL} respectively is given by:*

$$
\begin{aligned}
P_{\text{suc}}^{\text{J}} = &\int_0^{\infty}\int_{r_1\in\mathcal{N}_{r_2}} f_{R_1,R_2}(r_1,r_2)e^{\left(-\frac{\beta_{\text{UL}}\sigma_{\text{UL}}^2}{\rho {r_1}^{(\epsilon-1)\alpha}}\right)}\mathcal{L}_{\tilde{I}_2}\left(\frac{\beta_{\text{UL}}}{{r_1}^{(\epsilon-1)\alpha}}\right)\exp\left(-\mathcal{G}(r_1,r_2)\right)\frac{1}{1+\frac{\beta_{\text{DL}}r_1^{\alpha}}{r_2^{\alpha}}}\mathrm{d}r_1\mathrm{d}r_2\\
&+\int_0^{\infty}\int_{r_1\in\mathcal{P}_{r_2}} f_{R_1,R_2}(r_1,r_2)e^{\left(-\frac{\beta_{\text{UL}}\sigma_{\text{UL}}^2}{\rho {r_1}^{(\epsilon-1)\alpha}}\right)}\mathcal{L}_{\tilde{I}_2}\left(\frac{\beta_{\text{UL}}}{{r_1}^{(\epsilon-1)\alpha}}\right)\frac{\exp\left(-\mathcal{G}(r_1,r_2)-r_1^{\alpha}\mathcal{F}(r_1,r_2)\right)}{r_2^{\alpha}-r_1^{\alpha}}\frac{r_2^{\alpha}}{1+\frac{\beta_{\text{DL}}r_1^{\alpha}}{r_2^{\alpha}}}\mathrm{d}r_1\mathrm{d}r_2\\
&-\int_0^{\infty}\int_{r_1\in\mathcal{P}_{r_2}} f_{R_1,R_2}(r_1,r_2)e^{\left(-\frac{\beta_{\text{UL}}\sigma_{\text{UL}}^2}{\rho {r_1}^{(\epsilon-1)\alpha}}\right)}\mathcal{L}_{\tilde{I}_2}\left(\frac{\beta_{\text{UL}}}{{r_1}^{(\epsilon-1)\alpha}}\right)\frac{\exp\left(-\mathcal{G}(r_1,r_2)-r_2^{\alpha}\mathcal{F}(r_1,r_2)\right)}{r_2^{\alpha}-r_1^{\alpha}}\frac{r_1^{\alpha}}{1+\frac{\beta_{\text{DL}}r_1^{\alpha}}{r_2^{\alpha}}}\mathrm{d}r_1\mathrm{d}r_2,
\end{aligned}
\tag{3.16}
$$

where $f_{R_1,R_2}(r_1,r_2)=(2\pi\lambda_b)^2 r_1 r_2 e^{-\pi\lambda_b r_2^2}$, $\mathcal{F}(r_1,r_2)$, $\mathcal{N}_{r_2}$, $\mathcal{P}_{r_2}$ are as introduced in Lemma 1, $\mathcal{G}(r_1,r_2)$ is as introduced in Lemma 2, and $\mathcal{L}_{\tilde{I}_2}(s)$ is as introduced in Lemma 3.

Proof: This result follows directly by substituting (3.10), (3.12), (3.15) in (3.8) and integrating over r_1 and r_2 using the joint distribution $f_{R_1,R_2}(r_1,r_2)$ as defined in [79, (28)].

Remark 1. *This general result can be used to derive both downlink coverage and uplink coverage probabilities defined in (3.6) and (3.7). For instance, if we remove all the uplink conditions by putting $\beta_{\text{UL}}=0$ (note that $\mathcal{L}_{I_2}(0)=1$) and $\tau_3=0$, then (3.16) will represent the downlink coverage probability P_{cov}^{DL} for the downlink mode. Similarly, if we remove all the downlink conditions by putting $\beta_{\text{DL}}=0$ (note that $\mathcal{G}(r_1,r_2)=0$ in that case), $E_{\text{rec}}=0$, and $\tau_2=0$, then (3.16) will represent the uplink coverage probability $P_{\text{suc}}^{\text{UL}}$ for the uplink mode.*

3.3.4 Average Throughput

We now derive expressions for both the uplink and the downlink average throughput in the joint uplink/downlink mode. The average downlink throughput is

$$
\begin{aligned}
D_{\text{avg}}^{\text{DL}} &= \tau_2 R_{\text{avg}}^{\text{DL}} = \tau_2\mathbb{E}\left[W_D\log(1+\beta_{\text{DL}})\mathbb{1}(\text{SINR}_{\text{DL}}\geq\beta_{\text{DL}})\mathbb{1}(\text{SINR}_{\text{UL}}\geq\beta_{\text{UL}})\mathbb{1}(E_{\text{H}}\geq E_{\min})\right]\\
&= \tau_2 W_D\log(1+\beta_{\text{DL}})P_{\text{suc}}^{\text{J}},
\end{aligned}
\tag{3.17}
$$

where $R_{\text{avg}}^{\text{DL}}$ is the average data rate during downlink sub-slot in the joint mode. The multiplication by τ_2 accounts for the fact that downlink sub-slot lasts for τ_2 fraction of the total time-slot duration. Similarly, the average uplink throughput in the joint mode is:

$$\begin{aligned} D_{\text{avg}}^{\text{UL}} &= \tau_3 R_{\text{avg}}^{\text{UL}} = \tau_3 \mathbb{E}\left[W_U \log(1+\beta_{\text{UL}}) \mathbb{1}(\text{SINR}_{\text{UL}} \geq \beta_{\text{UL}}) \mathbb{1}(\text{SINR}_{\text{DL}} \geq \beta_{\text{DL}}) \mathbb{1}(E_{\text{H}} \geq E_{\min})\right] \\ &= \tau_3 W_U \log(1+\beta_{\text{UL}}) P_{\text{suc}}^{\text{J}}, \end{aligned} \tag{3.18}$$

where $R_{\text{avg}}^{\text{UL}}$ is the average data rate during uplink sub-slot in the joint mode.

Remark 2. *Note that for a given τ_3, it is easier to satisfy the energy constraint for larger values of τ_1. This means both $P_{\text{suc}}^{\text{J}}$ and $R_{\text{avg}}^{\text{DL}}$ are the increasing functions of τ_1. However, increasing τ_1 decreases τ_2 (for a given τ_3), which reduces the downlink transmission time and may therefore reduce average data rate $D_{\text{avg}}^{\text{DL}}$. This indicates the existence of an optimal slot partitioning for maximizing $D_{\text{avg}}^{\text{DL}}$. Similar conclusions can be drawn about the relation between τ_1 and $D_{\text{avg}}^{\text{UL}}$ for a given τ_2. We will discuss more about this optimal slot partitioning in the sequel.*

In the next two Sections, we will specialize the general results of this Section to the downlink and uplink modes, which will provide several useful system design insights.

3.4 Downlink Mode

The coverage probability in the downlink mode defined in (3.6) can be expressed as

$$P_{\text{cov}}^{\text{DL}} = \mathbb{E}_{\Phi_b}\left[\mathbb{P}\left(\text{SINR}_{\text{DL}} \geq \beta_{\text{DL}} \middle| \Phi_b\right) \mathbb{P}\left(E_{\text{H}} \geq E_{\text{rec}} \middle| \Phi_b\right)\right], \tag{3.19}$$

which is the special case of (3.8). As discussed in Section 3.2 and later in Remark 1, we can obtain this definition for $P_{\text{cov}}^{\text{DL}}$ by simply substituting $\tau_3 = 0$, $\beta_{\text{UL}} = 0$ and using $E_{\text{H}} > E_{\text{rec}}$ as the energy condition in the definition of joint uplink/downlink coverage probability given in (3.5) (and hence (3.8)). Therefore, $P_{\text{cov}}^{\text{DL}}$ can be derived directly by making these substitutions in (3.16). Similarly, we can derive the energy coverage for downlink mode by using the same substitutions in (3.11). We first state this energy coverage result next.

Lemma 4 (Energy coverage probability in the downlink mode)**.** *Probability that the harvested energy during the charging sub-slot is greater than the value E_{rec} is*

$$\begin{aligned} \mathbb{P}(E_{\text{H}} \geq E_{\text{rec}}) &= 1 - \exp\left(-\pi\lambda_b \mathcal{A}^2\right) - \pi\lambda_b \mathcal{A}^2 \exp\left(-\pi\lambda_b \mathcal{A}^2\right) \\ &\quad + \int_{\mathcal{A}}^{\infty} \int_{0}^{r_2} f_{R_1,R_2}(r_1,r_2) \frac{r_2^{\alpha} \exp\left(-r_1^{\alpha} \mathcal{F}_{\text{DL}}(r_1,r_2)\right) - r_1^{\alpha} \exp\left(-r_2^{\alpha} \mathcal{F}_{\text{DL}}(r_1,r_2)\right)}{r_2^{\alpha} - r_1^{\alpha}} \mathrm{d}r_1 \mathrm{d}r_2, \end{aligned} \tag{3.20}$$

where $f_{R_1,R_2}(r_1,r_2) = (2\pi\lambda_b)^2 r_1 r_2 e^{-\pi\lambda_b r_2^2}$, $\mathcal{F}_{\text{DL}}(r_1,r_2) = C(\tau_1) - \frac{2\pi\lambda_b r_2^{2-\alpha}}{\alpha-2}$, $C(\tau_1) = \frac{E_{\text{rec}}}{\tau_1 T \eta P_{\text{t}}}$, and $\mathcal{A} = \left(\frac{2\pi\lambda_b}{C(\tau_1)(\alpha-2)}\right)^{\frac{1}{\alpha-2}}$.

Proof: See Appendix A.3.

Remark 3. *The effect of the duration of the charging sub-slot $T_{\rm ch} = \tau_1 T$ appears in the value of $C(\tau_1)$. Consistent with intuition, as this duration increases, the value of $C(\tau_1)$ decreases and the energy coverage probability increases.*

We now state the (downlink) coverage result for the downlink mode (defined in (3.6)).

Theorem 2 (Downlink coverage probability in the downlink mode)**.** *The downlink coverage probability with SINR threshold $\beta_{\rm DL}$ and minimum required energy $E_{\rm rec}$ is given by*

$$P_{\rm cov}^{\rm DL} = \int_0^{\mathcal{A}} \int_0^{r_2} f_{R_1,R_2}(r_1,r_2) \exp(-\mathcal{G}(r_1,r_2)) \frac{1}{1+\frac{\beta_{\rm DL} r_1^\alpha}{r_2^\alpha}} {\rm d}r_1 {\rm d}r_2 \tag{3.21}$$

$$+ \int_{\mathcal{A}}^{\infty} \int_0^{r_2} f_{R_1,R_2}(r_1,r_2) \exp(-\mathcal{G}(r_1,r_2)) \frac{r_2^\alpha \exp\left(-r_1^\alpha \mathcal{F}_{\rm DL}(r_1,r_2)\right) - r_1^\alpha \exp\left(-r_2^\alpha \mathcal{F}_{\rm DL}(r_1,r_2)\right)}{(r_2^\alpha - r_1^\alpha)\left(1+\frac{\beta_{\rm DL} r_1^\alpha}{r_2^\alpha}\right)} {\rm d}r_1 {\rm d}r_2,$$

where $\mathcal{G}(r_1,r_2)$ is defined in Lemma 2, $C(\tau_1)$, $\mathcal{A}$, and $\mathcal{F}_{\rm DL}(r_1,r_2)$ are defined in Lemma 4.

Proof: See Appendix A.3.

Remark 4. *The effect of the duration of the charging sub-slot $T_{\rm ch} = \tau_1 T$ appears mainly in the value of $\mathcal{A}$ (implicitly in the value of $C(\tau_1)$). It can be observed that as this duration increases, the value of $\mathcal{A}$ increases and $P_{\rm cov}^{\rm DL}$ approaches the coverage probability of regularly powered network $P_{\rm cov}^{\rm DL,RP} = \mathbb{P}({\rm SINR} \geq \beta_{\rm DL})$. This is because as $T_{\rm ch}$ increases, it becomes easier to satisfy the energy constraint and the energy coverage probability increases.*

Remark 5. *Conditioned on Φ_b, the variable $\mathcal{A}$ represents an important system parameter. In (*3.21*), it can be interpreted as a threshold on the value of r_2. In particular, as long as the distance to the second nearest BS (which is also the second dominant RF source on average) is less than this threshold, the energy coverage condition is satisfied and the only condition required for coverage is ${\rm SINR}_{\rm DL} \geq \beta_{\rm DL}$, which is represented by the first term in (*3.21*). This useful system insight is a result of using the approximation in (*3.9*) that defines the amount of energy harvested in terms of distances r_1 and r_2. This provides useful characterization of the regime in which the performance of this RF-powered IoT network will be similar to the regularly powered network. Similar observations will be provided for the uplink case in the next Section.*

The general expression for average throughput given in (3.17) can be specialized for the downlink mode as follows:

$$D_{\rm avg}^{\rm DL} = \tau_2 W_D \log(1+\beta_{\rm DL}) P_{\rm cov}^{\rm DL}. \tag{3.22}$$

Remark 6. *Similar to our comments in Remark 2, $R_{\rm avg}^{\rm DL}$ is an increasing function of τ_1. On the other hand, the duration $\tau_2 T$ of the downlink sub-slot decreases with increase in τ_1. This indicates the existence of an optimal value of τ_1 that maximizes $D_{\rm avg}^{\rm DL}$.*

3.5 Uplink Mode

In this Section, we specialize the results of Section 3.3 to the uplink mode. Recall that in the uplink mode, each time-slot is partitioning into two sub-slots: charging sub-slot and uplink sub-slot. As discussed in Section 3.2 and Remark 1, the uplink coverage probability, defined in (3.7), can be obtained from the definition of joint uplink/downlink coverage, given by (3.5), by substituting $\tau_2 = 0$, $\beta_{\rm DL} = 0$ and using $E_{\rm H} > \tau_3 T \rho r_1^{\epsilon\alpha}$ as the energy condition. Consequently, the results for the uplink mode can be obtained from the general results of Section 3.3 by making these substitutions. While these substitutions are quite similar to the ones that we made in the previous Section for the downlink mode, there is a subtle difference in the energy conditions, which is the reason why the final results are slightly different in the two cases. In particular, while the minimum required energy in the downlink mode was fixed ($E_{\rm rec}$), it is a function of the nearest BS location in the uplink mode (due to power control). As in the previous Section, we first state the energy coverage result for the Uplink mode next.

Lemma 5 (Energy coverage probability in the uplink mode)**.** *Energy coverage probability is*

$$\mathbb{P}(E_{\rm H} \geq \tau_3 T \rho \|x_1\|^{\epsilon\alpha}) = 1 - \exp\left(-\pi\lambda_b \tilde{\mathcal{A}}^2\right) - \pi\lambda_b \tilde{\mathcal{A}}^2 \exp\left(-\pi\lambda_b \tilde{\mathcal{A}}^2\right) + \int_{\tilde{\mathcal{A}}}^{\infty} \int_{0}^{\mathcal{H}(r_2)} f_{R_1,R_2}(r_1,r_2) {\rm d}r_1 {\rm d}r_2$$
$$+ \int_{\tilde{\mathcal{A}}}^{\infty} \int_{\mathcal{H}(r_2)}^{r_2} f_{R_1,R_2}(r_1,r_2) \frac{r_2^{\alpha} \exp\left(-r_1^{\alpha}\mathcal{F}_{\rm UL}(r_1,r_2)\right) - r_1^{\alpha}\exp\left(-r_2^{\alpha}\mathcal{F}_{\rm UL}(r_1,r_2)\right)}{r_2^{\alpha} - r_1^{\alpha}} {\rm d}r_1 {\rm d}r_2, \qquad (3.23)$$

where $f_{R_1,R_2}(r_1,r_2) = (2\pi\lambda_b)^2 r_1 r_2 e^{-\pi\lambda_b r_2^2}$, $\mathcal{H}(r_2) = \left(\frac{2\pi\lambda_b}{(\alpha-2)\tilde{C}(\tau_1)}\right)^{\frac{1}{\epsilon\alpha}} r_2^{\frac{2-\alpha}{\epsilon\alpha}}$, $\mathcal{F}_{\rm UL}(r_1,r_2) = \tilde{C}(\tau_1) r_1^{\epsilon\alpha} - \frac{2\pi\lambda_b r_2^{2-\alpha}}{\alpha-2}$, $\tilde{C}(\tau_1) = \frac{\tau_3\rho}{\tau_1\eta P_t}$, $\tilde{\mathcal{A}} = \left(\frac{2\pi\lambda_b}{\tilde{C}(\tau_1)(\alpha-2)}\right)^{\frac{1}{(\epsilon+1)\alpha-2}}$.

Proof: See Appendix A.4.

Remark 7. *It is easy to see that increasing the density λ_b of the BS PPP Φ_b increases energy coverage probability due to two reasons. First, it reduces the distance r_1 between the typical device and its serving BS, which reduces the transmission power ${r_1}^{\epsilon\alpha}$ of this device, this making it easier to satisfy the energy coverage condition. Second, increasing λ_b also increases the aggregate energy $E_{\rm H}$ harvested by the typical device. This is also evident from (*3.23*) where all the terms can be shown to be decreasing functions of λ_b.*

We now present the uplink coverage probability (defined in (3.7)) next. Using this, we will discuss the differences between the regularly powered and energy harvesting networks.

Theorem 3 (Uplink coverage probability in the uplink mode)**.** *The uplink coverage probability* $P_{\rm suc}^{\rm UL}$ *of the IoT device with SINR threshold* $\beta_{\rm UL}$ *and uplink transmission power* $\rho\|x_1\|^{\epsilon\alpha}$ *is*

$$\begin{aligned}P_{\rm suc}^{\rm UL} =& \int_0^{\tilde{\mathcal{A}}}\int_0^{r_2} f_{R_1,R_2}(r_1,r_2)e^{\left(-\frac{\beta_{\rm UL}\sigma_{\rm UL}^2}{\rho {r_1}^{(\epsilon-1)\alpha}}\right)}\mathcal{L}_{\tilde{I}_2}\left(\frac{\beta_{\rm UL}}{{r_1}^{(\epsilon-1)\alpha}}\right){\rm d}r_1{\rm d}r_2\\ &+\int_{\tilde{\mathcal{A}}}^{\infty}\int_0^{\mathcal{H}(r_2)} f_{R_1,R_2}(r_1,r_2)e^{\left(-\frac{\beta_{\rm UL}\sigma_{\rm UL}^2}{\rho {r_1}^{(\epsilon-1)\alpha}}\right)}\mathcal{L}_{\tilde{I}_2}\left(\frac{\beta_{\rm UL}}{{r_1}^{(\epsilon-1)\alpha}}\right){\rm d}r_1{\rm d}r_2\\ &+\int_{\tilde{\mathcal{A}}}^{\infty}\int_{\mathcal{H}(r_2)}^{r_2} f_{R_1,R_2}(r_1,r_2)\frac{r_2^\alpha\exp\left(-r_1^\alpha\mathcal{F}_{\rm UL}(r_1,r_2)-\frac{\beta_{\rm UL}\sigma_{\rm UL}^2}{\rho {r_1}^{(\epsilon-1)\alpha}}\right)}{r_2^\alpha-r_1^\alpha}\mathcal{L}_{\tilde{I}_2}\left(\frac{\beta_{\rm UL}}{{r_1}^{(\epsilon-1)\alpha}}\right){\rm d}r_1{\rm d}r_2\\ &-\int_{\tilde{\mathcal{A}}}^{\infty}\int_{\mathcal{H}(r_2)}^{r_2} f_{R_1,R_2}(r_1,r_2)\frac{r_1^\alpha\exp\left(-r_2^\alpha\mathcal{F}_{\rm UL}(r_1,r_2)-\frac{\beta_{\rm UL}\sigma_{\rm UL}^2}{\rho {r_1}^{(\epsilon-1)\alpha}}\right)}{r_2^\alpha-r_1^\alpha}\mathcal{L}_{\tilde{I}_2}\left(\frac{\beta_{\rm UL}}{{r_1}^{(\epsilon-1)\alpha}}\right){\rm d}r_1{\rm d}r_2,\end{aligned} \tag{3.24}$$

where $\mathcal{H}(r_2)$*,* $\tilde{C}(\tau_1)$*,* $\mathcal{F}_{\rm UL}(r_1,r_2)$*, and* $\tilde{\mathcal{A}}$ *are as defined in Lemma* 5*, and* $\mathcal{L}_{\tilde{I}_2}(s)$ *is defined in Lemma* 3*.*

Proof: See Appendix A.4.
By comparing the above result with the uplink coverage probability of the regularly powered network given by (3.14), we note that the effect of energy harvesting mainly appears in the term $\tilde{\mathcal{A}}$. For instance, if we try to exclude the energy coverage condition ($E_{\rm H}\geq\tau_3 T\rho\|x_1\|^{\epsilon\alpha}$) by putting $\tau_3=0$, we will get $\tilde{C}(\tau_1)=0$, which will tend $\tilde{\mathcal{A}}$ to ∞. This will eventually make all the terms in (3.24) tend to zero except the first term which will be equivalent to (3.14).

Remark 8. *Similar to Remark* 5*, the value of* $\tilde{\mathcal{A}}$ *here represents a threshold on the distance to the second nearest BS* r_2*. In particular, as long as* $r_2\leq\tilde{\mathcal{A}}$*, the uplink coverage probability of the RF-powered network is exactly the same as that of the regularly powered network. This can be deduced from the first term of (*3.24*).*

Similar to (3.18), the average uplink throughput $D_{\rm avg}^{\rm UL}=\tau_3 R_{\rm avg}^{\rm UL}$ can be expressed as

$$D_{\rm avg}^{\rm UL}=\tau_3 W_U\log(1+\beta_{\rm UL})P_{\rm suc}^{\rm UL}. \tag{3.25}$$

Note that, similar to Remark 6, the time-slot division parameter τ_1 has an optimum value that maximizes the throughput $D_{\rm avg}^{\rm UL}$. We conclude this Section with the following remark.

Remark 9. *By comparing the results for downlink and uplink modes (given in Theorems* 2 *and* 3*, respectively), with those of the regularly powered network, we conclude that* $\mathcal{A}=\left(\frac{2\pi\lambda_b}{C(\tau_1)(\alpha-2)}\right)^{\frac{1}{\alpha-2}}$

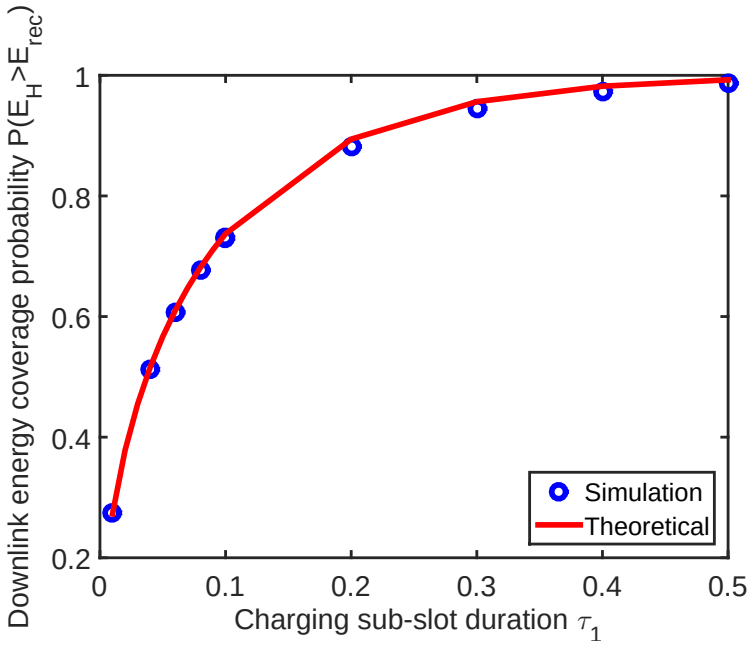

Figure 3.3: Energy coverage probability in the downlink mode as a function of τ_1.

and $\tilde{\mathcal{A}} = \left(\frac{2\pi\lambda_b}{\tilde{C}(\tau_1)(\alpha-2)}\right)^{\frac{1}{(\epsilon+1)\alpha-2}}$ *can be used as tuning parameters for the energy harvesting network. The closer we need the downlink or uplink coverage probability to be to the regularly powered network, the larger the values of* $\mathcal{A}$ *and* $\tilde{\mathcal{A}}$ *need to be. These tuning parameters capture in their definitions the effects of all system parameters including* $P_{\rm t}$, λ_b, τ_1, τ_2, τ_3, *and* η.

3.6 Simulation Results and Discussion

Unless specified otherwise, we will consider the following values for the simulation parameters throughout this section: $E_{\rm rec} = 10^{-5}$ Joules, $\lambda_b = 1$, $\alpha = 4$, $\eta = 10^{-3}$, $W_D = 1$ MHz, $\beta_{\rm DL} = 1$ dB, $P_{\rm t} = 0$ dB, $\frac{P_t}{\sigma^2_{\rm DL}} = 20$ dB, $\rho = 1$ dBm, $\frac{\rho}{\sigma^2_{\rm UL}} = 20$ dB, $\lambda_u = 30\lambda_b$, $\beta_{\rm UL} = 1$ dB, $\epsilon = 0.8$, and $T = 10^{-2}$ sec.

3.6.1 Downlink Mode

In this subsection, we evaluate the performance of the downlink mode using the performance metrics derived in Section 3.4. First, in Fig. 3.3 we plot the energy coverage probability result derived in Lemma 4. As discussed in Remark 3, energy coverage probability is clearly an increasing function of the time division parameter τ_1. The theoretical results are also shown to match perfectly with the simulation results obtained from Monte-Carlo trials, which verifies the accuracy of the

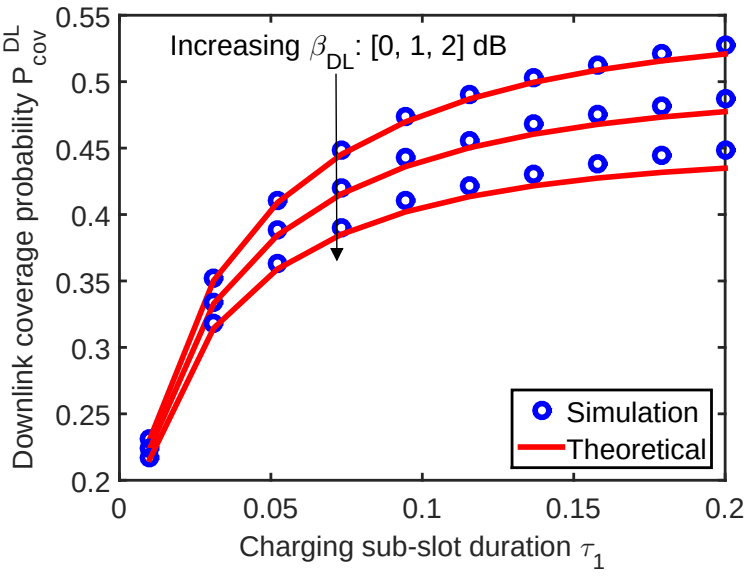

Figure 3.4: Downlink coverage probability $P_{\text{cov}}^{\text{DL}}$ in the downlink mode as a function of τ_1.

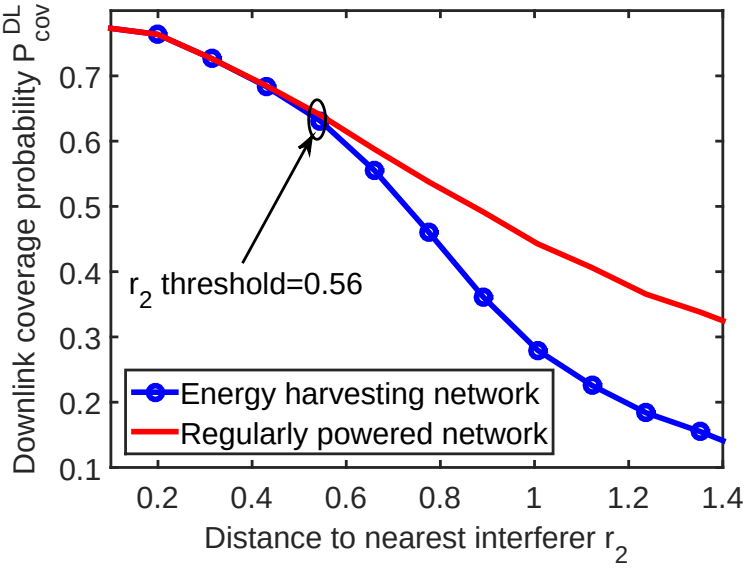

Figure 3.5: Downlink coverage probability conditioned on the value of r_2.

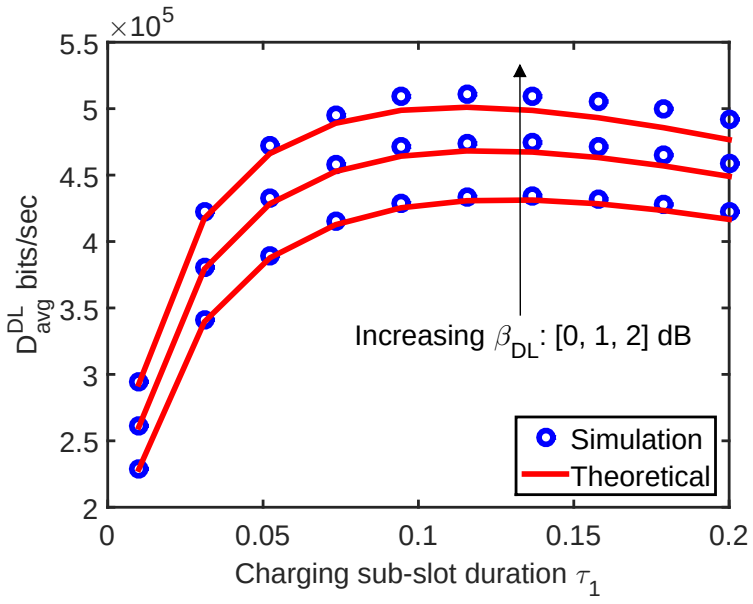

Figure 3.6: Downlink average throughput $D_{\text{avg}}^{\text{DL}}$ in the downlink mode as a function of τ_1.

dominant BS-based approach used to approximate the energy E_{H} in our analysis. The downlink coverage result derived in Theorem 2 is plotted in Fig. 3.4. Comparisons with simulation results again verify the accuracy of the dominant BS-based approximation. As discussed in Remark 4, we notice that the coverage probability $P_{\text{cov}}^{\text{DL}}$ starts converging to the coverage probability of regularly powered networks, given by $\mathbb{P}(\text{SINR}_{\text{DL}} \geq \beta_{\text{DL}})$, at high values of τ_1. To glean sharper insights, we recall Remark 5, where we referred to $\mathcal{A}$ as a threshold on the value of distance to the second nearest BS r_2, below which this RF-powered IoT network has the same downlink coverage as the regularly powered network. In Fig. 3.5, we verify this insight by plotting the coverage probabilities for both RF-powered and regularly powered networks conditioned on r_2 (for $\tau_1 = 0.1$). As predicted in Remark 5, the performance of both the networks is the same when r_2 is below the threshold value, which in this case is $r_2 = \mathcal{A} = 0.56$. Even thought this insight was a byproduct of dominant BS-based approximation, we notice that it is remarkably accurate. Right after the threshold value of $r_2 = \mathcal{A} = 0.56$, the two curves start diverging. Finally, we plot our results in (3.22) for the average throughput in Fig. 3.6. Comparisons with the simulation results verify the accuracy of our analysis. The results also illustrate the existence of an optimum value for τ_1 that maximizes the average throughput in the downlink mode, as predicted in Remark 6.

3.6.2 Uplink Mode

In this section, we focus on the performance analysis of uplink mode. In particular, we will study the effect of τ_1 and λ_b on the performance metrics derived in Section 3.5. In Fig. 3.7, we plot the energy coverage probability in the uplink mode as a function of λ_b. Consistent with Remark 7, the

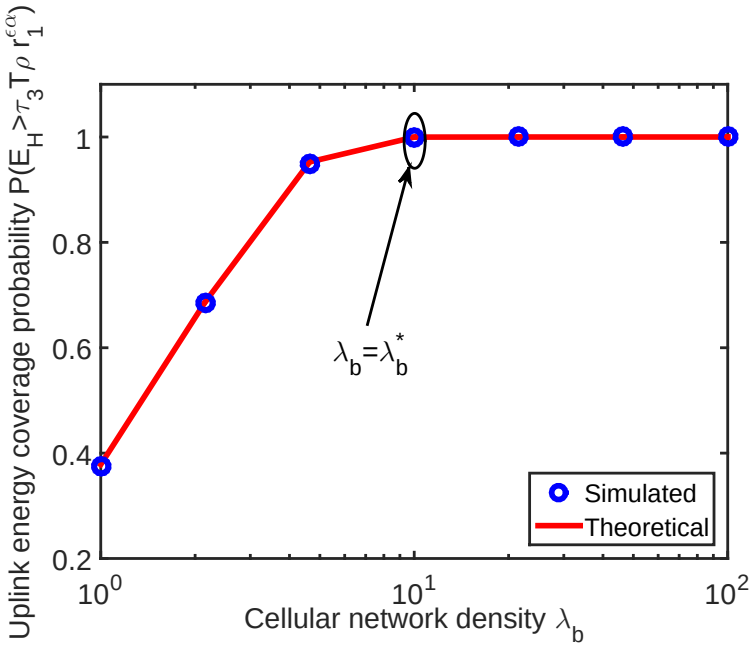

Figure 3.7: Uplink energy coverage probability as a function of cellular network density λ_b.

energy coverage probability increases with λ_b and saturates to unity when λ_b is above a specific value, which we denote by λ_b^*. Beyond this value of density, the energy coverage condition is satisfied with high probability. Consequently, the uplink coverage probability $P_{\text{suc}}^{\text{UL}}$ is expected to converge to the SINR coverage probability, defined as $\mathbb{P}(\text{SINR}_{\text{UL}} \geq \beta_{\text{UL}})$, at λ_b^*. This is verified in Fig. 3.8, where starting from $\lambda_b = \lambda_b^*$, the energy coverage condition is satisfied most of the time and the uplink coverage probability reduces to SINR coverage, i.e., $\mathbb{P}(\text{SINR}_{\text{UL}} \geq \beta_{\text{UL}}, E_H \geq \rho r_1^{\epsilon\alpha}) \simeq \mathbb{P}(\text{SINR}_{\text{UL}} \geq \beta_{\text{UL}})$. We also note that the SINR coverage probability in Fig. 3.8 initially decreases with λ_b until it becomes constant starting from about $\lambda_b = \lambda_b^*$. This is due to the increase in energy coverage probability which leads to increase in the density of active devices, hence increasing the interference value. The value to which they converge starting from $\lambda_b = \lambda_b^*$ is the uplink coverage probability for the case of regularly powered network ($P_{\text{suc}}^{\text{UL,RP}}$ in (3.14)). Similar trends are observed in Fig. 3.9, where we note that the uplink coverage and the SINR coverage probabilities converge at about $\tau_1 = 0.5$, which can be interpreted as the minimum value of τ_1 at which the energy coverage condition is satisfied with a high probability. Also, similar to our discussion above on the effect of λ_b, the SINR coverage probability in Fig. 3.9 initially decreases due to the increase in the energy coverage probability which increases the density of active devices and, consequently, the interference.

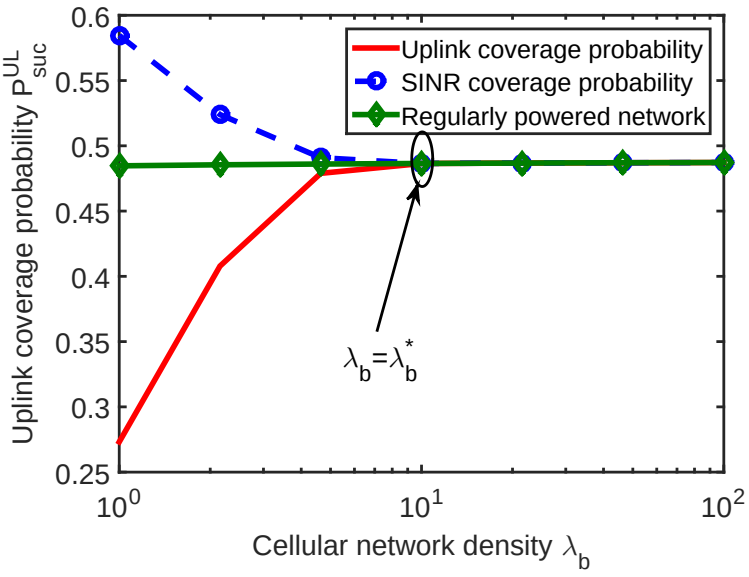

Figure 3.8: Uplink coverage probability $P_{\text{suc}}^{\text{UL}}$ in the uplink mode as a function of λ_b.

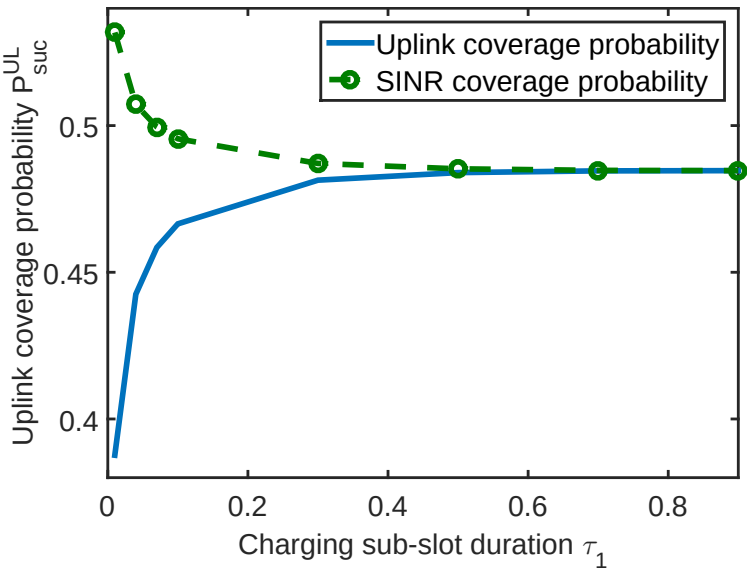

Figure 3.9: Uplink coverage probability as a function of uplink time-slot division parameter τ_1.

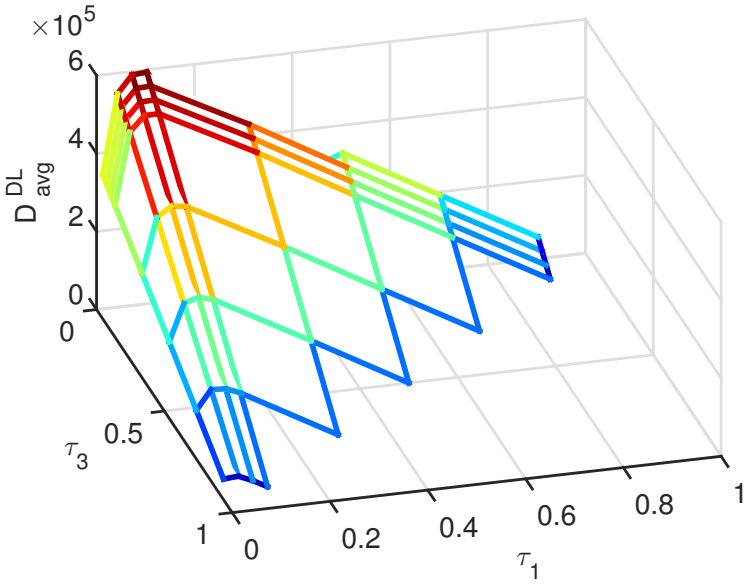

Figure 3.10: Downlink average throughput during joint uplink and downlink mode as a function of τ_1 and τ_3.

3.6.3 Joint Uplink and Downlink Mode

In Fig. 3.10 we provide a 3D plot for $D_{\text{avg}}^{\text{DL}}$ as a function of τ_1 and τ_3. Recall that $\tau_2 = 1 - \tau_1 - \tau_3$. We note that for any given value of τ_1, the value of $D_{\text{avg}}^{\text{DL}}$ decreases as τ_3 increases (equivalently τ_2 decreases). As discussed in Remark 2, for any given value of τ_3, there exists optimal τ_1 (and hence optimal τ_2) that maximizes $D_{\text{avg}}^{\text{DL}}$. A similar behavior has already been seen in Fig. 3.6. Similar observations can be made about the behavior of $D_{\text{avg}}^{\text{UL}}$.

3.7 Summary

In this chapter, we developed an analytical framework to study joint uplink and downlink coverage performance of a cellular-based ambient RF energy harvesting network in which IoT devices are solely powered by the downlink cellular transmissions. Each time-slot is assumed to be partitioned into charging, downlink, and uplink sub-slots. Within each time-slot, the IoT devices (assumed batteryless) first harvest RF energy from cellular transmissions and then use this energy to perform downlink and uplink communication in the subsequent sub-slots. For this setup, we derived the joint probability that the typical device harvests sufficient energy in the charging sub-slot and achieves sufficiently high downlink and uplink SINRs in the following two sub-slots. The main technical contribution is in handling the correlation between these energy and SINR coverage events. Using this result, we also studied system throughput as a function of the time-slot division parameters. Optimal slot partitioning that maximizes this throughput is also discussed. Using

these results, we also compared the performance of this RF-powered IoT network with a regularly powered network in which the IoT devices have uninterrupted access to reliable power source, such as a battery. We derived thresholds on several system parameters beyond which the performance of this RF-powered IoT network converges to that of the regularly powered network.

Finally, we defined a *tuning parameter*, which incorporates the effect of all system parameters, and needs to be sufficiently high for the coverage performance of this RF-powered network to converge to that of the regularly powered network.

This work can be extended in multiple directions. From the energy harvesting perspective, the system model can be extended to include rechargeable batteries (with finite capacities) at the devices. This will require explicit consideration of the temporal dimension, as done in [33], where the BSs were assumed to be self-powered with access to batteries with finite capacities. From the modeling perspective, it is important to consider other BS-device configurations, such as the ones in which devices are clustered around the BSs [80].

In this chapter, we focused on the coverage analysis of RF-powered IoT. Beside coverage, another important aspect of the performance of RF-powered IoT is the secrecy of the RF signals used by the IoT devices to harvest energy. This problem gains more importance when the RF signals are intended to legitimate receivers to convey confidential messages. Given that RF-powered IoT devices naturally locate themselves closer to the sources of RF energy, to harvest more energy, serious concerns are raised regarding the secrecy of the RF signals. We address this problem from a novel perspective in Chapters 5 and 7. But before that, in the next chapter we provide a novel performance comparison between two popular secrecy enhancing techniques: (i) artificial noise addition to confidential messages and (ii) using eavesdropper-clear guard zones around the sources of confidential messages. The results of this comparison motivate the use of the guard zone technique in Chapter 5, as will be discussed in the sequel.

Chapter 4

Stochastic Geometry-based Comparison of Secrecy Enhancement Techniques in D2D Networks

This chapter presents a performance comparison of two popular secrecy enhancement techniques in wireless networks: (i) *creating guard zones* by restricting transmissions of legitimate transmitters whenever any eavesdropper is detected in their vicinity, and (ii) *adding artificial noise* to the confidential messages to make it difficult for the eavesdroppers to decode them. Focusing on a noise-limited regime, we use tools from stochastic geometry to derive the secrecy outage probability at the eavesdroppers as well as the coverage probability at the legitimate users for both these techniques. Using these results, we derive a threshold on the density of the eavesdroppers below which no secrecy enhancing technique is required to ensure a target secrecy outage probability. For eavesdropper densities above this threshold, we concretely characterize the regimes in which each technique outperforms the other. Our results demonstrate that guard zone technique is better when the distances between the transmitters and their legitimate receivers are higher than a certain threshold.

4.1 Introduction

Owing to the broadcast nature of wireless networks, physical layer security techniques are necessary to preserve confidentiality of the transmitted messages [81–84]. Two popular secrecy enhancing techniques that have been investigated in the literature are: (i) *creating guard zones* by restricting transmissions of the legitimate transmitters whenever eavesdroppers are detected in their vicinity [81], and (ii) *adding artificial noise* to the confidential messages to make it difficult for the eavesdroppers to decode them [82]. Despite the attention received by these techniques, to the best of our knowledge their explicit system-level performance comparison is still an open problem,

which is the main focus of this chapter.

The system-level analysis of wireless networks usually requires averaging the performance metric of interest over all possible topologies of the network. While this has traditionally been performed through Monte-Carlo trials, stochastic geometry has recently emerged as an attractive analytic alternative due to its remarkable tractability [30]. In fact, stochastic geometry has also gained popularity in the past few years for the system-level analysis of D2D networks, e.g., see [48, 85, 86], as well as physical layer security, e.g., see [81, 87]. In particular, [81] quantified the loss in system throughput that results from ensuring a specific level of secrecy in decentralized wireless networks. Similarly, [87] studied physical layer security in downlink cellular networks assuming the downlink messages meant for each user can be eavesdropped by all other users (both intra- and inter-cell) in the network.

In this chapter, we will use tools from stochastic geometry for the comparison of secrecy enhancing techniques. In addition to the two techniques introduced already, namely, creating guard zones and adding artificial noise, there are two other techniques usually considered in the literature: (i) *protected zones*, and (ii) *beamforming*. Protected zones are similar to the guard zones defined earlier in this section, except that they are guaranteed to be free of eavesdroppers (physically enforced) [83]. If one assumes multi-antenna nodes, beamforming is also an attractive solution for enhancing secrecy [84]. In this chapter, we consider a system with single-antenna nodes in which we do not have control over the physical removal of eavesdroppers, as a result of which we focus only on the first two techniques (guard zones and artificial noise).

Contributions. We consider a device-to-device (D2D) network that coexists with a network of eavesdroppers modeled by an independent PPP. For this setup, focusing on the noise-limited regime, we first derive the secrecy outage probability at the eavesdroppers and coverage probability at the legitimate receivers for the two secrecy enhancement techniques considered in this chapter. Using these results, we characterize the maximum density of eavesdroppers below which no secrecy enhancing technique is required to ensure the target secrecy outage probability. For eavesdropper densities above this threshold, we concretely characterize the regimes in which a given technique outperforms the other, which leads to useful system design insights.

4.2 System Model

Focusing on the noise-limited regime, we consider a primary D2D link coexisting with a secondary network of potential eavesdroppers modeled as an independent PPP $\Phi_e \equiv \{y_i\} \subset \mathbb{R}^2$ with density λ_e. The D2D link is formed by a primary transmitter (PT) located at the origin and a primary receiver (PR) located at a fixed distance d from the PT (at an arbitrary angle from the origin). We assume independent Rayleigh fading on all wireless links. The PT is assumed to transmit at a fixed power P_t. For this setup, the received power at the PR associated with the PT is $P_t h \|d\|^{-\alpha}$, where $h \sim \exp(1)$ models Rayleigh fading, $\|d\|^{-\alpha}$ is the standard power-law path-loss with exponent $\alpha > 2$. Similarly, the received power at an arbitrary eavesdropper located at $y \in \Phi_e$ from the PT is $P_{\mathrm{t}} g_y \|y\|^{-\alpha}$, where $g_y \sim \exp(1)$ models Rayleigh fading. For the secrecy outage analysis, we

will need to analyze the performance of eavesdroppers that have the best chance of decoding the messages from the PT. The location of this *strongest* eavesdropper corresponding to the PT is:

$$y^* = \arg\max_{y \in \Phi_e} g_y \|y\|^{-\alpha}. \tag{4.1}$$

According to Wyner encoding scheme [88], the transmitter chooses a rate of codeword transmission $\mathcal{C}_t$ and a rate of confidential message transmission $\mathcal{C}_s$. The rate difference, $\mathcal{C}_e = \mathcal{C}_t - \mathcal{C}_s$, represents the cost of securing the confidential message where perfect secrecy is achieved as long as mutual information between the PT and the eavesdropper is lower than $\mathcal{C}_e$. Please refer to Sec. II-B in [89] for further details on Wyner encoding scheme. As is usually the case in the literature, e.g., see [83], we assume a noise-limited scenario for analytical tractability. Therefore, in order to ensure successful decoding at the PR, we need to satisfy the condition $\log_2(1 + \mathrm{SNR_P}) \geq \mathcal{C}_t$, where $\mathrm{SNR_P}$ is the SNR achieved at the PR. On the other hand, to ensure perfect secrecy we require $\log_2(1 + \mathrm{SNR_S}) \leq \mathcal{C}_e$ at the eavesdropper located at y^*, where $\mathrm{SNR_S}$ is the SNR at the eavesdropper. Equivalently, we can define two thresholds $\beta_t = 2^{\mathcal{C}_t} - 1$ and $\beta_e = 2^{\mathcal{C}_e} - 1$ on $\mathrm{SNR_P}$ and $\mathrm{SNR_S}$ respectively. For this setup, we now define two main performance metrics that will be used in this work.

Definition 1 (Coverage probability)**.** *The SNR coverage probability at the PR is defined as*

$$P_{\mathrm{cov}} = \mathbb{P}(\mathrm{SNR_P} \geq \beta_t, \delta_a = 1), \tag{4.2}$$

where $\delta_a = 1$ if the PT is transmitting information (referred to as an active PT), and $\delta_a = 0$ otherwise.

Definition 2 (Secure communication probability [90])**.** *It is the probability of perfect secrecy of the confidential message from the PT (conditioned on the fact that PT is active):*

$$P_{\mathrm{sec}} = \mathbb{P}(\mathrm{SNR_S} \leq \beta_e | \delta_a = 1) \tag{4.3}$$

Our main objective is to maximize the SNR coverage probability at the PR while ensuring that the secure communication probability is above a predefined threshold ϵ.

4.3 Secrecy Enhancing Techniques

4.3.1 Guard Zone Technique

In this technique, a given PT is allowed to transmit confidential messages to its paired PR only if there are no eavesdroppers in a circular *guard zone* of radius r_g around it. Therefore, the probability that the PT is active is:

$$P_{\mathrm{active}} = \mathbb{P}(\delta_a = 1) = \mathbb{P}(\mathcal{N}(\mathcal{B}(o, r_g)) = 0) = e^{-\lambda_e \pi r_g^2}, \tag{4.4}$$

where $\mathcal{N}(\mathcal{B}(o, r_g))$ is the number of eavesdroppers inside a ball of radius r_g centered at the origin. Owing to the independence of $\mathrm{SNR_P}$ and $\mathcal{N}(\mathcal{B}(o, r_g))$, the SNR coverage probability for the D2D link is defined as:

$$\begin{aligned} P_{\text{cov}}^{GZ} &= P_{\text{active}}\mathbb{P}(\mathrm{SNR_P} \geq \beta_t) = P_{\text{active}}\mathbb{P}\left(\frac{P_t\|d\|^{-\alpha}h}{\sigma_P^2} \geq \beta_t\right) \\ &\overset{(a)}{=} P_{\text{active}} \exp\left(-\frac{\beta_t\sigma_P^2\|d\|^{\alpha}}{P_t}\right) \\ &= \exp\left(-\lambda_e\pi r_g^2 - \frac{\beta_t\sigma_P^2\|d\|^{\alpha}}{P_t}\right), \end{aligned} \tag{4.5}$$

where σ_P^2 is the noise power at the PT and step (a) follows from $h \sim \exp(1)$. Now we derive secure communication probability for this technique for which we focus on the SNR achieved at the strongest eavesdropper located at y^* (as defined in (4.1)), which can be defined as $\mathrm{SNR_S} = \frac{P_t g_{y^*}\|y^*\|^{-\alpha}}{\sigma_S^2}$. The secure communication probability is given in the next Lemma.

Lemma 6 (Secure communication probability)**.** *The secure communication probability for the guard zone technique is*

$$\begin{aligned} P_{\text{sec}}^{GZ} &= \mathbb{P}\left(\frac{P_t g_{y^*}\|y^*\|^{-\alpha}}{\sigma_S^2} \leq \beta_e \middle| \mathcal{N}(\mathcal{B}(o, r_g)) = 0\right) \\ &= \exp\left(-\frac{2\pi\lambda_e}{\alpha}\left(\frac{P_t}{\sigma_S^2\beta_e}\right)^{\frac{2}{\alpha}}\Gamma\left(\frac{2}{\alpha}, \frac{r_g^{\alpha}\beta_e\sigma_S^2}{P_t}\right)\right), \end{aligned} \tag{4.6}$$

where $\Gamma(a, b)$ is the upper incomplete gamma function.

Proof: See Appendix B.1.
As evident from (4.5), P_{cov}^{GZ} is a decreasing function of r_g. On the other hand, as noted from (7.8), the value of P_{sec}^{GZ} is an increasing function of r_g. Hence, the optimum value r_g^* is the minimum guard zone radius that ensures $P_{\text{sec}}^{GZ} \geq \epsilon$. The value of r_g^* is derived next.

Lemma 7 (Optimal guard zone radius)**.** *The value of r_g^* that maximizes P_{cov}^{GZ} while satisfying the condition of $P_{\text{sec}}^{GZ} \geq \epsilon$ is is the one that satisfies the following equation:*

$$\Gamma\left(\frac{2}{\alpha}, \frac{(r_g^*)^{\alpha}\beta_e\sigma_S^2}{P_t}\right) = \min\left\{\frac{\alpha\log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e\left(\frac{P_t}{\sigma_S^2\beta_e}\right)^{\frac{2}{\alpha}}}, \Gamma\left(\frac{2}{\alpha}\right)\right\} \tag{4.7}$$

Proof:
Substituting the expression of P_{sec}^{GZ} from (7.8) in $P_{\text{sec}}^{GZ} \geq \epsilon$, we get $\Gamma\left(\frac{2}{\alpha}, \frac{r_g^{\alpha}\beta_e\sigma_S^2}{P_t}\right) \leq \frac{\alpha\log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e\left(\frac{P_t}{\sigma_S^2\beta_e}\right)^{\frac{2}{\alpha}}}$.

Now if $r_g = 0$ satisfies this inequality, then $r_g^* = 0$ and $\Gamma\left(\frac{2}{\alpha}, \frac{(r_g^*)^\alpha \beta_e \sigma_S^2}{P_t}\right) = \Gamma\left(\frac{2}{\alpha}\right)$. Otherwise, the minimum value for r_g^* that satisfies this inequality follows from $\Gamma\left(\frac{2}{\alpha}, \frac{(r_g^*)^\alpha \beta_e \sigma_S^2}{P_t}\right) = \frac{\alpha \log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e \left(\frac{P_t}{\sigma_S^2 \beta_e}\right)^{\frac{2}{\alpha}}}$. Combining the results for these two cases leads to the final result in (4.7).

4.3.2 Artificial Noise Technique

In this secrecy enhancing technique, the transmission power P_t is split into two parts: (i) γP_t, which is used for the transmission of confidential information, and (ii) $(1-\gamma)P_t$, which is used to transmit artificial noise (AN). The AN is generated by using random sequences, which can only be decoded using the keys available at the PRs. Since eavesdroppers do not have access to these keys, they cannot decode AN. Hence, the SNR achieved at the PR is $\mathrm{SNR_P} = \frac{\gamma P_t h \|d\|^{-\alpha}}{\sigma_P^2}$. Please note that unlike the guard zone technique, the PT in this technique is always active, i.e., we have $\delta_a = 1$. Hence, the probability of SNR coverage at the PR can be derived as follows:

$$P_{\text{cov}}^{AN} = \mathbb{P}(\mathrm{SNR_P} \geq \beta_t) \overset{(b)}{=} \exp\left(-\frac{\beta_t \sigma_P^2 \|d\|^\alpha}{\gamma P_t}\right), \tag{4.8}$$

where (b) follows from $h \sim \exp(1)$. On the other hand, we assume that the eavesdropper is unable to decode the AN, which implies that the the SNR at the eavesdropper located at y^* is $\mathrm{SNR_S} = \frac{\gamma P_t g_{y^*} \|y^*\|^{-\alpha}}{(1-\gamma) P_t g_{y^*} \|y^*\|^{-\alpha} + \sigma_S^2}$. Hence, the secure communication probability can be derived as follows:

$$\begin{aligned} P_{\text{sec}}^{AN} &= \mathbb{P}\left(\frac{\gamma P_t g_{y^*} \|y^*\|^{-\alpha}}{(1-\gamma) P_t g_{y^*} \|y^*\|^{-\alpha} + \sigma_S^2} \leq \beta_e\right) \\ &\overset{(c)}{=} \mathbb{P}\left(\frac{(\gamma - (1-\gamma)\beta_e) P_t g_{y^*} \|y^*\|^{-\alpha}}{\sigma_S^2} \leq \beta_e\right), \end{aligned} \tag{4.9}$$

where step (c) results from simple manipulations of the inequality. This implies that $P_{\text{sec}}^{AN} = 1$ as long as $\gamma \leq \frac{\beta_e}{1+\beta_e}$. When $\gamma > \frac{\beta_e}{1+\beta_e}$, we can derive a closed-form expression for P_{sec}^{AN} by replacing β_e with $\frac{\beta_e}{\gamma - (1-\gamma)\beta_e}$ and $r_g = 0$ in (7.8). This provides the following closed-form expression for P_{sec}^{AN}:

$$P_{\text{sec}}^{AN} = \exp\left(-\frac{2\pi\lambda_e}{\alpha}\left(\frac{P_t\left(\gamma - (1-\gamma)\beta_e\right)}{\sigma_S^2 \beta_e}\right)^{\frac{2}{\alpha}} \Gamma\left(\frac{2}{\alpha}\right)\right). \tag{4.10}$$

Since the power used for information transmission is directly proportional to γ, P_{cov}^{AN} is an increasing function of γ, which is evident from (4.8). On the other hand, since the power used for transmitting AN is directly proportional to $1-\gamma$, P_{sec}^{AN} decreases with increase in γ, which is evident from (4.10). Therefore, the optimum value of γ^* is the maximum value of γ that ensures $P_{\text{sec}}^{AN} \geq \epsilon$. This optimal γ^* is derived in the following Lemma.

Lemma 8 (Optimal power split)**.** *The value of γ^* that maximizes P_{cov}^{AN} while satisfying the condition $P_{\text{sec}}^{AN} \geq \epsilon$ is*

$$\gamma^* = \min\left\{1, \frac{\beta_e}{1+\beta_e}\left(1 + \frac{\sigma_S^2}{P_t}\left(\frac{\alpha \log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e \Gamma(\frac{2}{\alpha})}\right)^{\frac{\alpha}{2}}\right)\right\}. \tag{4.11}$$

Proof:
The result follows by substituting (4.10) in the inequality $P_{\text{sec}}^{AN} \geq \epsilon$, and following similar approach as in the proof of Lemma 7.

4.4 Performance Comparison

4.4.1 Useful Threshold on the Density of Eavesdroppers

In this subsection, we first aim to find the threshold on λ_e below which the secrecy enhancing techniques are not required ($r_g^* = 0$ and $\gamma^* = 1$). Note that when $r_g^* = 0$ and $\gamma^* = 1$ the performance is the same for both techniques: $P_{\text{cov}}^{GZ} = P_{\text{cov}}^{AN}$ and $P_{\text{sec}}^{GZ} = P_{\text{sec}}^{AN}$. For the guard zone technique, we can derive this threshold by solving the following inequality:

$$\Gamma\left(\frac{2}{\alpha}\right) \leq \frac{\alpha \log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e \left(\frac{P_t}{\sigma_S^2 \beta_e}\right)^{\frac{2}{\alpha}}}, \tag{4.12}$$

where this inequality ensures that the result of (4.7) is $r_g^* = 0$. Solving this inequality, we deduce that $r_g^* = 0$ as long as

$$\lambda_e \leq \frac{\alpha}{2\pi\Gamma\left(\frac{2}{\alpha}\right)} \log\left(\frac{1}{\epsilon}\right)\left(\frac{P_t}{\sigma_S^2 \beta_e}\right)^{-\frac{2}{\alpha}}. \tag{4.13}$$

Similarly, for the artificial noise technique, we can derive this threshold on λ_e by solving the following inequality:

$$\frac{\beta_e}{1+\beta_e}\left(1 + \frac{\sigma_S^2}{P_t}\left(\frac{\alpha \log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e \Gamma(\frac{2}{\alpha})}\right)^{\frac{\alpha}{2}}\right) \geq 1, \tag{4.14}$$

where the above inequality ensures that the result of (4.11) is $\gamma^* = 1$. Solving the above inequality, we infer that artificial noise addition is not required as long as

$$\lambda_e \leq \frac{\alpha}{2\pi\Gamma\left(\frac{2}{\alpha}\right)} \log\left(\frac{1}{\epsilon}\right)\left(\frac{P_t}{\sigma_S^2 \beta_e}\right)^{-\frac{2}{\alpha}}. \tag{4.15}$$

As can be expected intuitively, the threshold on λ_e derived in (D.4) and (4.15) for the two techniques is the same. We denote this threshold by λ_e^*. As long as $\lambda_e < \lambda_e^*$, the secure communication probability is guaranteed to be above ϵ.

4.4.2 Comparison of Secrecy Enhancement Techniques

In this subsection, we focus on $\lambda_e \geq \lambda_e^*$ for which secrecy enhancement techniques are required to ensure desired secrecy performance level. In particular, we will characterize regimes in which a given technique outperforms the other. Since both techniques select their parameters (r_g^* or γ^*) in order to ensure that $P_{\text{sec}} \geq \epsilon$, optimal parameter choices will naturally satisfy the desired secrecy conditions. As a result, we focus our comparison on the other system performance metric: P_{cov}^{GZ} and P_{cov}^{AN}. Hence, for $\lambda_e \geq \lambda_e^*$, a given secrecy technique is said to perform better than the other if it provides higher coverage probability at the PR while ensuring $P_{\text{sec}} \geq \epsilon$. In the following theorem, we characterize the regimes in which a given secrecy enhancing technique outperforms the other.

Theorem 4 (Secrecy enhancement technique selection)**.** *Defining the functions $\mathcal{F}$, $\mathcal{H}$, and $\mathcal{G}$ as*

$$\mathcal{F} = \frac{\alpha \log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e \left(\frac{P_t}{\sigma_S^2 \beta_e}\right)^{\frac{2}{\alpha}}} - \Gamma\left(\frac{2}{\alpha}, \mathcal{H}\right) \tag{4.16}$$

$$\mathcal{H} = \frac{\beta_e \sigma_S^2}{P_t} \left[\frac{\beta_t d^\alpha \sigma_S^2}{P_t \lambda_e \pi}\left(\frac{1}{\mathcal{G}} - 1\right)\right]^{\frac{\alpha}{2}} \tag{4.17}$$

$$\mathcal{G} = \frac{\beta_e}{1+\beta_e}\left(1 + \frac{\sigma_S^2}{P_t}\left(\frac{\alpha \log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e \Gamma(\frac{2}{\alpha})}\right)^{\frac{\alpha}{2}}\right), \tag{4.18}$$

the guard zone technique is a better choice as long as $\mathcal{F} > 0$, while artificial noise technique is a better choice when $\mathcal{F} \leq 0$.

Proof: See Appendix B.2.

Remark 10. *Observing the dependence of $\mathcal{F}$ on D2D link distance d in (*4.16*), we note that the value of d plays an important role in determining which technique performs better. Since $\mathcal{F}$ is an increasing function of d, it is easy to conclude that for a given set of system parameters, the artificial noise technique provides better performance at lower values of d, while the guard zone technique starts performing better when d exceeds a specific threshold. These comments will be verified next in the numerical results section.*

4.4.3 Numerical Results

For numerical comparisons, we consider the following system parameters: $\alpha = 4$, $P_t = 1$, $\beta_t = 2$, $\beta_e = 1$, $\epsilon = 0.9$, $\sigma_P^2 = 1$, and $\sigma_S^2 = 1$. For this setup, $\lambda_e^* = 0.0378$ because of which we choose $\lambda_e = 0.1 > \lambda_e^*$. In Fig. 4.1.a, we use Monte-Carlo simulations to evaluate the values of P_{sec}^{GZ}, P_{sec}^{AN}, P_{cov}^{GZ}, and P_{cov}^{AN} to determine which technique is better at different values of d. On the same figure, we plot the function $\mathcal{F}$ derived in Theorem 4. The comparison of the simulation and analytical

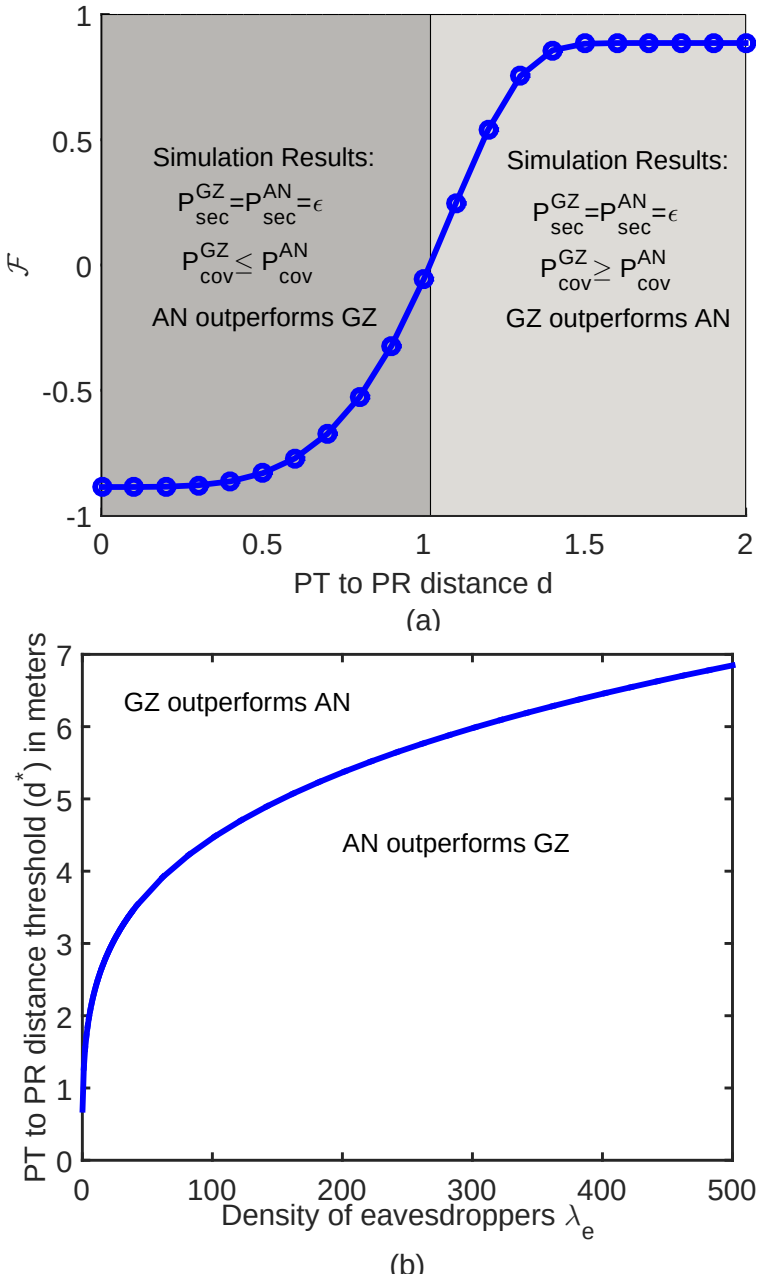

Figure 4.1: (a) Technique selection function $\mathcal{F}$ as a function of d, and (b) PT to PR distance threshold d^* for different values of λ_e.

results supports the main consequence of our analysis that the guard zone technique is a better choice when $\mathcal{F} > 0$ while the artificial noise technique is a better choice when $\mathcal{F} \leq 0$. In addition, our comment in Remark 10 that artificial noise technique is better for lower values of d is verified. It is clear from this comparison that the value of d at which $\mathcal{F}$ switches from being negative to positive is critical to the choice of the secrecy enhancement technique. We refer to this threshold value of d as d^*. In Fig. 4.1.b, we study the effect of λ_e on d^*. The resulting curve partitions the (d^*, λ_e) plane into two parts: lower part in which AN outperforms GZ and the the upper part in which GZ outperforms AN. We notice that with increasing λ_e, d^* increases, which means AN starts becoming optimal choice for a larger range of values for d.

4.5 Summary

In this chapter, we provided a concrete performance comparison of two popular secrecy enhancement techniques: (i) creating guard zones around legitimate transmitters, and (ii) adding artificial noise to the confidential messages. Using tools from stochastic geometry, we first derived a closed-form expression for the threshold on the density of eavesdroppers below which no secrecy enhancement techniques are required. For densities greater than this threshold, we characterized regimes in which a given secrecy enhancement technique outperforms the other. Our results demonstrate that guard zone technique is a better choice when the distances between the D2D pairs are higher than a specific threshold.

A key technical extension for this line of work is the inclusion of interference in the analysis. This requires a significantly more complicated analysis due to spatial correlation between interference levels at the PR and the eavesdropper which requires joint analysis of coverage probability at the PR and secure communication probability at the eavesdropper.

Based on the results of this chapter, we can clearly see that there is no one specific secrecy technique that is useful for all system setups. However, guard zone technique is better for moderate and large link distances. Motivated by this, we use the guard zone technique in the next chapter to discuss the performance of RF-powered networks when the RF sources are using guard zones to enhance secrecy. The analysis when using artificial noise technique to enhance secrecy is provided in Chapter 7 along with a comparison with the performance of the guard zone technique.

Chapter 5

Secrecy Analysis of Wireless Power Transmission

This chapter studies the secrecy performance of a wireless network (primary network) overlaid with an ambient RF energy harvesting 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 PT 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: (i) the SINR at the primary receiver is above a predefined threshold, and (ii) the PT 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 PTs 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 work is one of the few concrete works that symbiotically merge tools from stochastic geometry and game theory.

5.1 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 IoT realm where it may not be economical to charge or replace batteries periodically in billions of devices worldwide [53]. 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 [51,52] and energy efficient hardware [54]. 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 [56]. 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 chapter) close to the sources of RF signals, concerns on the secrecy of these RF signals were recently raised in the literature [91–97]. While the RF signal source (referred to as *primary transmitter* or PT in this chapter) 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 [88]. 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 [83, 98], (ii) using artificial noise in order to degrade the confidential signal's SNR at the energy receiver [82, 93], (iii) beamforming in multi-antenna systems [94–96], and (iv) using guard zones to stop information transmission whenever an eavesdropper is detected within a specific region around the transmitter [81, 99].

In this chapter, 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 chapter. Thus, we have two options to choose from: either use artificial noise or guard zones. In [100], which is discussed in detail in Chapter 4, it was 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 in this chapter while leaving the artificial noise technique for a more extended discussion in Chapter 7. 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 chapter.

5.1.1 Related Work

In this subsection, we will provide a brief summary of the related works in three general directions of interest to this chapter: (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, and (iii) analysis of secure wireless power transmission.

Stochastic geometry-based work. Stochastic geometry has emerged as a powerful mathematical tool for the modeling and analysis of variety of wireless networks [30–32, 58]. Out of numerous aspects of wireless networks that have been studied using stochastic geometry, two that are most relevant to this chapter are: (i) secrecy [81, 87, 101], and (ii) energy harvesting [33, 37, 39, 66, 102]. We first discuss the related works on secrecy. The work presented in [81] 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 [87] studied the physical layer security of downlink cellular networks assuming that all the existing users in the network are potential cooperating eavesdroppers. In [101], 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 [33, 66, 102] or the uplink channel [37]. The work presented in [33] provided a comprehensive framework for analyzing heterogeneous cellular networks with energy harvesting BSs. The primary focus was on characterizing optimal transmission policies as well as quantifying the availability of different tiers of BSs. In [66, 102], the joint analysis of the downlink signal quality and the amount of energy harvested at an RF-powered user was performed. In [37, 39], 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 [46] 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.

Game theory-based work. Tools from game theory have been widely used in the analysis of secrecy in wireless networks [103–106]. Using these tools, in [103] authors modeled the interaction between cognitive networks and eavesdroppers, where a channel selection algorithm was proposed to reach the Nash equilibrium. In [104], authors studied the problem of optimizing the uplink path in multi-hop networks in order to maximize the secrecy rate. In [105], authors used matching theory to develop an algorithm that enhances the secrecy of source-destination pairs using jamming nodes. In [106], 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 in-

stance, authors in [107] 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 [108] 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 [109], 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.

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 [91, 92, 110–112]. These works assume that the transmitter aims to maximize secrecy performance with the constraint of providing ERs with the required wireless power. In [91, 92], 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 [110], authors studied the use of a friendly jammer to enhance the performance of the point-to-point system. 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 [111] 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 [112] 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 chapter, 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. 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 chapter. We summarize the contributions of this chapter next.

5.1.2 Contributions

Compared to the existing works on secrecy of wireless power transmission, which are 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.

Primary network performance analysis. Modeling the locations of PTs and ERs by two independent PPPs, we show that the locations of *active* PTs (PTs with ER-free guard zones) follow PHP. 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}.

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 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.

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 propose a best response-based learning algorithm that helps in achieving the Nash equilibrium of this game.

5.2 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 chapter). The primary network is constructed of PTs and primary receivers (will be referred to as either PRs or *legitimate receivers* interchangeably throughout the chapter). 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 [113]. Various detecting devices can be used for this purpose including metal detectors and leaked local oscillator power detectors [98]. The benefits of using secrecy guard zones and their effect on secrecy performance were discussed in [81]. As shown in Fig. 5.1, before the PT transmits data to its associated PR, it scans the guard zone for any illegitimate 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 chapter). 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 $\alpha > 2$.

5.2.1 Primary Network Modeling

According to Wyner's encoding scheme [88, 114] and the approach used in [81], the PT defines the rate of codewords and the rate of confidential messages, C_{t} and C_{s} respectively. The difference,

Figure 5.1: The PT stops transmission (becomes silent) if any ER is detected within its guard zone.

Table 5.1: Table of Notations for Chapter 5

Notation	Description
Φ_P; λ_P	PPP modeling the locations of the PTs; density of the PTs
Φ_S; λ_S	PPP modeling the locations of ERs; density of the ERs
E_{H}	Amount of energy harvested by ER (in Joules)
P_{con}	The probability of successful connection between a PT and its associated PR
P_{sec}	The probability of secure communication
P_{energy}	The density of successfully powered ERs
h; g; w	Fading gains for the link between the typical PR and an arbitrary PT; the typical PT and an arbitrary ER; an ER and its nearest active PT
r_g; R_e	Guard zone radius; distance between a PT and its nearest ER
$\mathbb{1}(\Xi)$	An indicator function such that $\mathbb{1}(\Xi) = 1$ if the condition Ξ is satisfied and equals zero otherwise
P_{t}; σ_P^2; σ_S^2	PT transmission power; noise power at the PR; noise power at the ER
ϵ; α	Minimum required value for P_{sec}; path loss exponent ($\alpha > 2$)
β_P; β_S	Minimum required SINR value at the PR to ensure successful connection; threshold on SINR at ERs to ensure perfect secrecy

$C_{\mathrm{e}} = C_{\mathrm{t}} - C_{\mathrm{s}}$, 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 $\mathcal{I}_{\mathrm{t}}$ and between PT's channel input and ER's channel output be $\mathcal{I}_{\mathrm{e}}$. Then, the objective is to ensure that the following two conditions are satisfied: (i) $C_{\mathrm{t}} \leq \mathcal{I}_{\mathrm{t}}$ to ensure successful decoding at the PR, and (ii) $C_{\mathrm{e}} \geq \mathcal{I}_{\mathrm{e}}$ 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 $\mathrm{SINR_P} \geq \beta_P$ should be satisfied, where $\beta_P = 2^{C_{\mathrm{t}}} - 1$. Similarly, to ensure perfect secrecy, the SINR at any eavesdropper should satisfy the condition $\mathrm{SINR_S} \geq \beta_S$, where $\beta_S = 2^{C_{\mathrm{t}} - C_{\mathrm{s}}} - 1$. 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

$$P_{\mathrm{active}} = \mathbb{P}(R_e \geq r_g) = e^{-\lambda_S \pi {r_g}^2}. \tag{5.1}$$

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

$$\mathrm{SINR_P} = \frac{P_t h_1 r_1^{-\alpha}}{\sum_{x_i \in \Phi_P \setminus x_1} \delta_i P_t h_i \|x_i\|^{-\alpha} + \sigma_P^2}, \tag{5.2}$$

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 $\mathbb{E}[\delta_i] = P_{\mathrm{acitve}}$.

The locations of the active PTs can be modeled using PHP Ψ [115, 116]. 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.

Figure 5.2: The locations of active PTs is modeled by a PHP where the locations of ERs represent the centers of the holes.

The remaining points of Φ_1 represent the PHP. In our system, as shown in Fig. 5.2, 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

$$\Psi = \left\{ x \in \Phi_P : x \notin \bigcup_{y \in \Phi_S} \mathcal{B}(y, r_g) \right\}, \tag{5.3}$$

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 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_P. Therefore, the probability of successful connection is*

$$P_{\text{con}}(r_g, \lambda_S) = \mathbb{P}(R_e \geq r_g, \text{SINR}_{\text{P}} \geq \beta_P). \tag{5.4}$$

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

$$\text{SINR}_{\text{S}}(y_j) = \frac{P_t g_{1,j} \|x_1 - y_j\|^{-\alpha}}{\sum_{x_i \in \Phi_P \setminus x_1} \delta_i P_t g_{i,j} \|x_i - y_j\|^{-\alpha} + \sigma_S^2}, \tag{5.5}$$

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 4 (Secure communication probability)**.** *Given that a PT is active, the probability that its transmitted data is perfectly secured is*

$$P_{\text{sec}}(r_g, \lambda_S) = \mathbb{E}\left[\mathbb{1}\left(\bigcap_{y_j \in \Phi_S} \text{SINR}_{\text{S}}(y_j) \leq \beta_S \middle| R_e \geq r_g \right) \right]. \tag{5.6}$$

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 5 (Guard zone radius selection)**.** *The primary network selects the guard zone radius r_g^* that satisfies the following*

$$r_g^* = \arg \max_{r_g \in \mathcal{G}(\lambda_S)} P_{\text{con}}(r_g, \lambda_S),$$
$$\mathcal{G}(\lambda_S) = \{r_g : P_{\text{sec}}(r_g, \lambda_S) \geq \epsilon\}. \tag{5.7}$$

Remark 11. *By observing (5.7), 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. It might seem intuitive to expect that as r_g increases the average distance between any PT and its nearest ER will increase, leading to an increase in the probability of secure communication. However, this is actually not always correct. The reason for that is the effect of r_g on the density of the PHP Ψ, $\lambda_P P_{\text{acitve}}$, which is the density of* active *interferers. As the guard zone radius increases, the density of interferers decreases, which means that the interference level at any ER will decrease on average leading to a* larger *SINR value.*

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.

5.2.2 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 [102]. 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 [43], 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

$$E_H = \eta T P_t \|x_{j,1} - y_j\|^{-\alpha} w_j, \tag{5.8}$$

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 chapter), $x_{j,1}$ 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 [39], or (ii) the energy coverage probability $\mathbb{P}(E_H \geq E_{\min})$ as in [37], 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

$$P_{\text{energy}} = \lambda_S \mathbb{P}(E_H \geq E_{\min}). \tag{5.9}$$

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

Remark 12. *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 (5.1), that P_{active} is a decreasing function of both r_g and λ_S, we can expect $\mathbb{P}(E_H \geq E_{\min})$ to be a decreasing function of both r_g and λ_S. This implies two things: (i) the performance metric defined in (5.9) has a local maximum at $\lambda_S = \lambda_S^*$, and (ii) the value of the selected density λ_S^* that maximizes (5.9) is a function of r_g.*

From Remarks 11 and 12 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.

5.3 Performance Analysis

5.3.1 Primary Network

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 5. In the following Theorem we derive P_{con}.

Theorem 5 (Probability of successful connection)**.** *For a given value of λ_S, the probability of successful connection defined in Definition 8 is*

$$P_{\text{con}}(r_g, \lambda_S) = \exp\left(-\left[\lambda_S \pi r_g^2 + \beta_P \frac{\sigma_P^2}{P_t} r_1^{\alpha} + \frac{2\pi^2 \lambda_P P_{\text{active}} \beta_P^{\frac{2}{\alpha}} r_1^2}{\alpha \sin(\frac{2}{\alpha}\pi)}\right]\right). \tag{5.10}$$

Proof: See Appendix C.1.

Remark 13. *According to Definition 8 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 (5.10). 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 (5.10) 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 6. *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 C.2.

Remark 14. *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* 6*, 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* 8 *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* 6*, the value of* $P_{\text{con}}(r_g^*, \lambda_S)$ *is upper bounded as follows*

$$P_{\text{con}}(r_g^*, \lambda_S) \leq P_{\text{con}}\left(\sqrt{\frac{\ln\left(\max\{\mathcal{A}_1, 1\}\right)}{\pi \lambda_S}}, \lambda_S\right), \tag{5.11}$$

where $\mathcal{A}_1$ *is defined in Theorem* 6*.*

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 5.

Secure Communication Probability

The secure communication probability, formally defined in Definition 9, is derived in the following theorem.

Theorem 7 (Secure communication probability)**.** *For a given value of r_g and λ_S, the probability of secure communication is*

$$P_{\text{sec}}(r_g, \lambda_S) = \exp\left(-2\pi\lambda_S \int_{r_g}^{\infty} \exp\left(-\frac{\sigma_S^2 \beta_S r_y^{\alpha}}{P_t}\right) \mathcal{L}_{I_2}(\beta_S r_y^{\alpha}) r_y \mathrm{d}r_y\right), \tag{5.12}$$

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.3.

Remark 15. *The intuitive observations provided in Remark* 11 *can now be verified using Theorem* 7*. 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 $\mathcal{L}_{I_2}(\beta_S r_x^{\alpha})$. As we mentioned earlier, increasing the value of r_g decreases the interference levels at the ER, which increases the value of* $\mathrm{SINR_S}$*, 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 7 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 5 and 7, 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*

$$P_{\text{con}}^{\text{Noise limited}} = \exp\left(-\left[\lambda_S \pi r_g^2 + \beta_P \frac{\sigma_P^2}{P_t} r_1^{\alpha}\right]\right), \tag{5.13}$$

$$\begin{aligned} P_{\text{sec}}^{\text{Noise limited}} &= \exp\left(-2\pi\lambda_S \int_{r_g}^{\infty} \exp\left(-\frac{\sigma_S^2 \beta_S r_y^{\alpha}}{P_t}\right) r_y \mathrm{d}r_y\right) \\ &= \exp\left(-\frac{2\pi\lambda_S}{\alpha}\left(\frac{P_t}{\sigma_S^2 \beta_S}\right)^{\frac{2}{\alpha}} \Gamma\left(\frac{2}{\alpha}, \frac{r_g^{\alpha} \beta_S \sigma_S^2}{P_{\text{t}}}\right)\right). \end{aligned} \tag{5.14}$$

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

$$\Gamma\left(\frac{2}{\alpha}, \frac{(r_g^*)^\alpha \beta_S \sigma_S^2}{P_{\mathrm{t}}}\right) = \min\left\{\frac{\alpha \mathrm{Ln}\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_S\left(\frac{P_t}{\sigma_S^2\beta_S}\right)^{\frac{2}{\alpha}}}, \Gamma\left(\frac{2}{\alpha}\right)\right\}. \tag{5.15}$$

Proof: (5.13) and (5.14) follow directly by removing the interference terms from the results in Theorem 5 and Theorem 7. Since $P_{\mathrm{con}}^{\text{Noise limited}}$ is a decreasing function of r_g, and $P_{\mathrm{sec}}^{\text{Noise limited}}$ 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 (5.14) in the inequality $P_{\mathrm{sec}} \geq \epsilon$ leads to (5.15).
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.*

$$P_{\mathrm{con}}^{\text{Int. limited}} = \exp\left(-\left[\lambda_S \pi r_g^2 + \frac{2\pi^2\lambda_P P_{\mathrm{active}} \beta_P^{\frac{2}{\alpha}} r_1^2}{\alpha \sin(\frac{2}{\alpha}\pi)}\right]\right), \tag{5.16}$$

$$P_{\mathrm{sec}}^{\text{Int. limited}} = \exp\left(-2\pi\lambda_S \int_{r_g}^{\infty} \mathcal{L}_{I_2}(\beta_S r_x^\alpha) r_x \mathrm{d}r_x\right). \tag{5.17}$$

Proof: These results follow by substituting for $\sigma_P^2 = \sigma_S^2 = 0$ in Theorems 5 and 7.
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.

5.3.2 Secondary Network

The objective of the secondary network is to maximize the density of successfully powered ERs P_{energy}, introduced in (5.9), which is derived in the following Theorem.

Theorem 8 (Density of successfully powered ERs)**.** *For a given value of r_g and λ_S, the density of successfully powered ERs is*

$$P_{\mathrm{energy}}(r_g, \lambda_S) = \lambda_S \int_{r_g}^{\infty} 2\pi\lambda_P P_{\mathrm{active}} r_p \exp\left(-\pi\lambda_P P_{\mathrm{active}}(r_p^2 - r_g^2) - \frac{E_{\min} r_p^\alpha}{P_t \eta}\right) \mathrm{d}r_p. \tag{5.18}$$

Proof: See Appendix C.4.
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*

$$P_{\text{energy}} \geq \lambda_S \int_{r_g}^{\infty} 2\pi\lambda_P P_{\text{active}} r_p \exp\left(-\pi\lambda_P(r_p^2 - r_g^2) - \frac{E_{\min} r_p^{\alpha}}{P_t \eta}\right) \mathrm{d}r_p. \tag{5.19}$$

The value of λ_S that maximizes the lower bound is

$$\lambda_S^* = \frac{1}{\pi r_g^2}. \tag{5.20}$$

Proof: The lower bound follows by simply replacing P_{active} inside the exponent in (5.18) with unity. The value of λ_S^* follows by differentiating (5.19) with respect to λ_S.

Remark 16. *It can be noted from (5.20) 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.

5.4 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 5, which can be rewritten as

$$r_g^* = \arg\max_{r_g \geq 0} P_{\text{con}}(r_g, \lambda_S) \mathbb{1}(P_{\text{sec}}(r_g, \lambda_S) \geq \epsilon), \tag{5.21}$$

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

$$\lambda_S^* = \arg\max_{\lambda_S \geq 0} P_{\text{energy}}(r_g, \lambda_S). \tag{5.22}$$

Observing (5.21) and (5.22), 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

$$U_1(r_g, \lambda_S) = P_{\text{con}}(r_g, \lambda_S)\mathbb{1}(P_{\text{sec}}(r_g, \lambda_S) \geq \epsilon), \tag{5.23}$$

while the utility function of player 2 is

$$U_2(r_g, \lambda_S) = P_{\text{energy}}(r_g, \lambda_S). \tag{5.24}$$

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

$$\begin{aligned} r_g^* &= \arg\max_{r_g \geq 0} P_{\text{con}}(r_g, \lambda_S^*)\mathbb{1}(P_{\text{sec}}(r_g, \lambda_S^*) \geq \epsilon), \\ \lambda_S^* &= \arg\max_{\lambda_S \geq 0} P_{\text{energy}}(r_g^*, \lambda_S). \end{aligned} \tag{5.25}$$

Unfortunately, due to the complexity of the expressions of P_{con} in Theorem 5 and P_{sec} in Theorem 7, it is challenging to provide a closed-form solution for NE. However, based on the comments given in Remark 12 and the result in Theorem 6, we provide a learning algorithm that assists both networks to find NE.

The proposed learning algorithm is a simple best-response based algorithm [117–119]. 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:

$$\begin{aligned} r_g^{(n)} &= r_g^*\left(\lambda_S^{(n-1)}\right), \\ \lambda_S^{(n)} &= \lambda_S^*\left(r_g^{(n-1)}\right), \end{aligned} \tag{5.26}$$

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 (5.21) for $\lambda_S = \lambda_S^{(n-1)}$, and $\lambda_S^*\left(r_g^{(n-1)}\right)$ is computed using (5.22) 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.

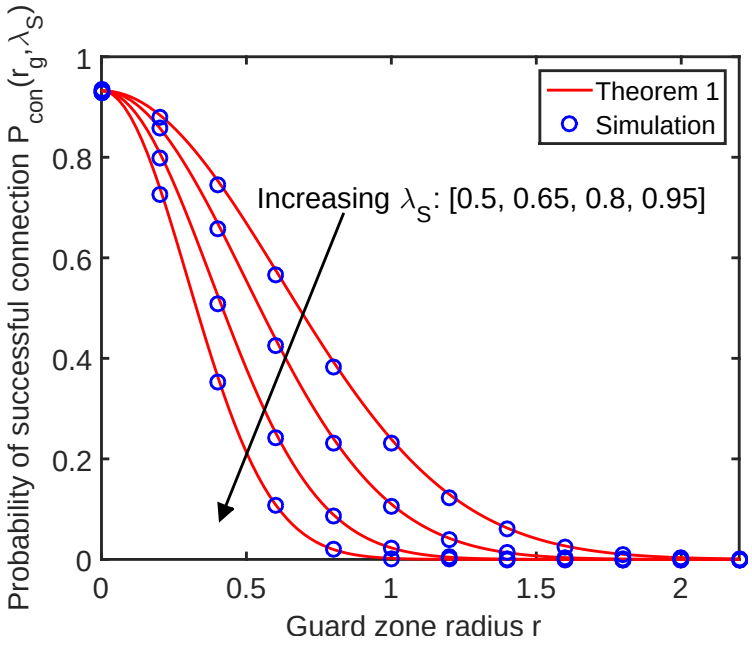

Figure 5.3: The effect of λ_S on the behavior of P_{con} against different values of r_g. The SNR value at the legitimate receiver is $\gamma_P = 7$ dB.

Algorithm: Proposed algorithm for finding the NE network parameters r_g^* and λ_S^*
input: λ_P, $\lambda_{S,\max}$, β_P, β_S, P_t, α, η, and $E_{\min}$.
output: r_g^*, λ_S^*.

Initialization: $r_g^{(0)} = 0$ for all PTs in Φ_{P}, $\lambda_S^{(0)} = \lambda_{S,\max}$, $n = 1$

1: **Repeat**
2: $\quad r_g^{(n)} = r_g^*\left(\lambda_S^{(n-1)}\right)$
3: $\quad \lambda_S^{(n)} = \lambda_S^*\left(r_g^{(n-1)}\right)$
4: $\quad n = n + 1$
5: **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.

5.5 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 chapter. We first study the successful connection probability P_{con} in Fig. 5.3. 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 6. The results in Fig. 5.3 show that increasing the density of ERs decreases P_{con}. Although increasing λ_S decreases the density of active interferers (which should increase P_{con}), it also decreases the probability of the PT being active (which decreases P_{con}). Ultimately, for this setup, P_{con} is a decreasing function of λ_S because of having $\mathcal{A}_1 < 1$. As explained in Remark 14, $\mathcal{A}_1 < 1$ 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_{con} is also a decreasing function of r_g. As a result, r_g^* will be the minimum value of r_g that ensures $P_{\text{sec}} \geq \epsilon$. The value of P_{sec} as a function of r_g is plotted in Fig. 5.4 for different values of γ_S. Consistent with the intuition, increasing γ_S decreases P_{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_{sec}, we plot in Fig. 5.5 the value of P_{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:

- 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 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 $P_{\text{sec}}^{\text{Noise Limited}}$.

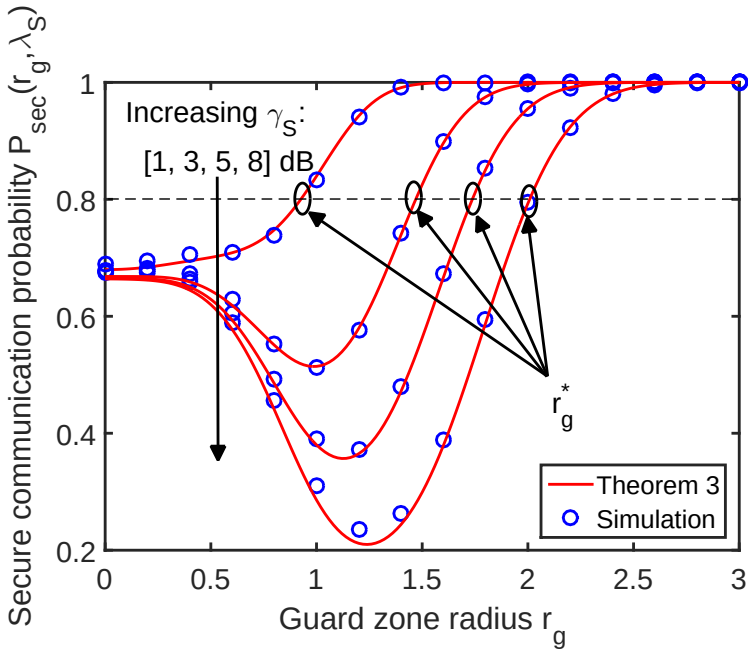

Figure 5.4: The effect of γ_S on the behavior of P_{sec} against different values of r_g. The density of ERs is $\lambda_S = 0.6$.

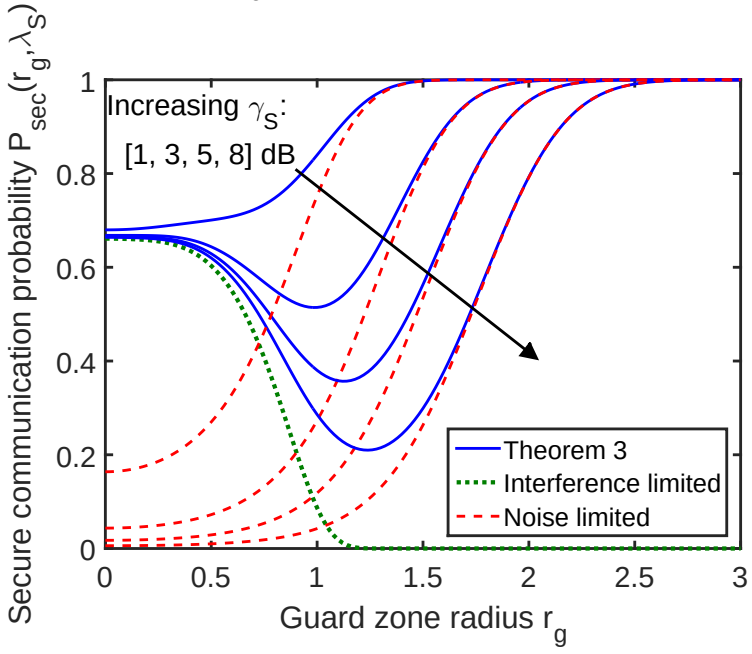

Figure 5.5: Comparing P_{sec}, $P_{\text{sec}}^{\text{NoiseLimited}}$, and $P_{\text{sec}}^{\text{Int.Limited}}$ as functions of r_g for different values of γ_S. The density of ERs is $\lambda_S = 0.6$.

In Fig. 5.6, 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. 5.7 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. 5.6 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. 5.8, 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 $\lambda_{S,\max}$. 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. 5.8, 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 16 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. 5.6 and 5.8, 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. 5.4, we simulate the interaction between both networks 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. 5.9, 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 (5.25). In Fig. 5.10, we evaluate the performance of the algorithm proposed in Sec. 5.4. The results demonstrate the convergence of the proposed algorithm to the NE found from Fig. 5.9 after less than 13 iterations.

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. 5.11. 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 8 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 [102]. 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.

5.6 Summary

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 chapter, 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 proposed a best-response based algorithm and demonstrated with simulations its convergence to Nash equilibrium.

The work in this chapter 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.

As was noticed during the analysis in this chapter, there are multiple open problems in the analysis of PHP modeled networks, including interference distribution and contact distance distribution. While there are some efforts done in literature for deriving the interference distribution, the contact distance analysis has received less attention. Hence, in the next chapter we provide a comprehensive study on the possible bounds and approximations for the contact distance distribution of the PHP. The problem of secrecy of wireless power transmission, which we studied in this chapter, will be extended in Chapter 7 to include more secrecy enhancing techniques, beside the guard zone technique.

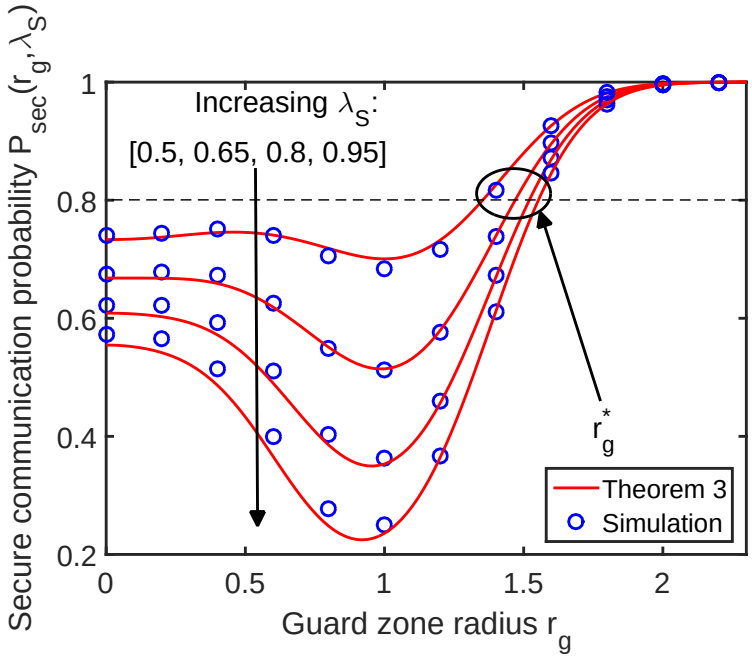

Figure 5.6: The effect of λ_S on the behavior of P_{sec} against different values of r_g. The SNR value at ERs is $\gamma_S = 4.8$ dB.

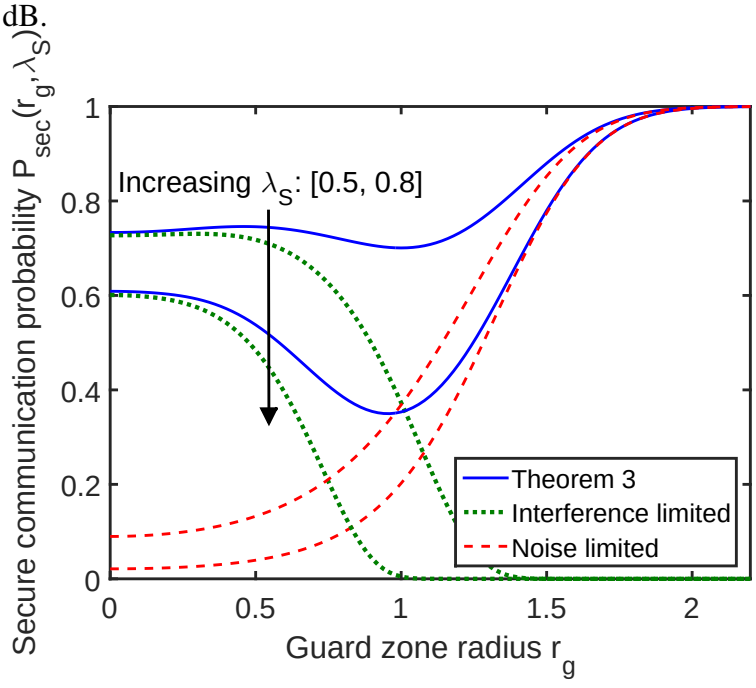

Figure 5.7: Comparing P_{sec}, $P_{\text{sec}}^{\text{NoiseLimited}}$, and $P_{\text{sec}}^{\text{Int.Limited}}$ as functions of r_g for different values of λ_S. The SNR value at ERs is $\gamma_S = 4.8$ dB.

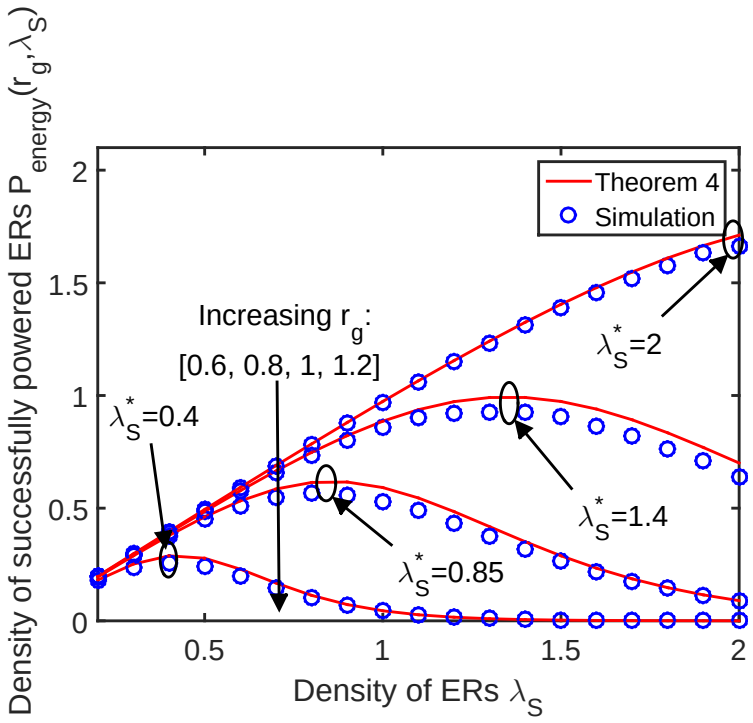

Figure 5.8: The density of successfully powered ERs P_{energy} against λ_S for different values of r_g.

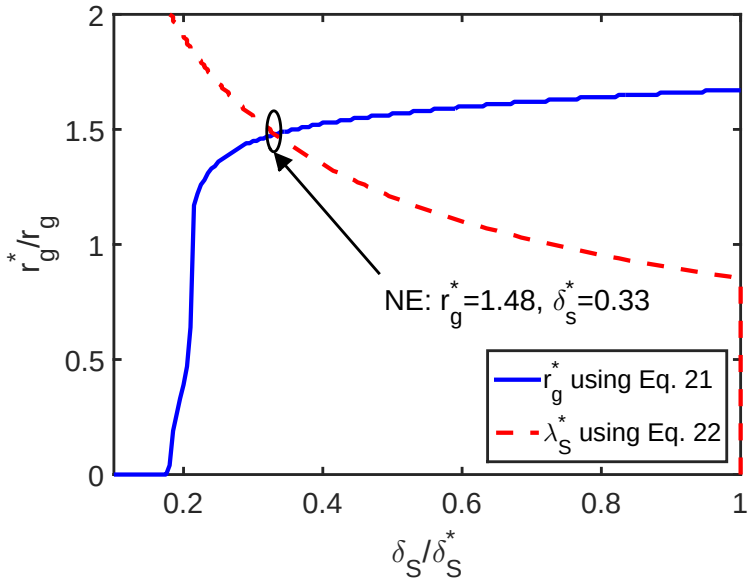

Figure 5.9: Plotting both r_g^* against δ_S and δ_S^* against r_g on the same plot to compute the NE values.

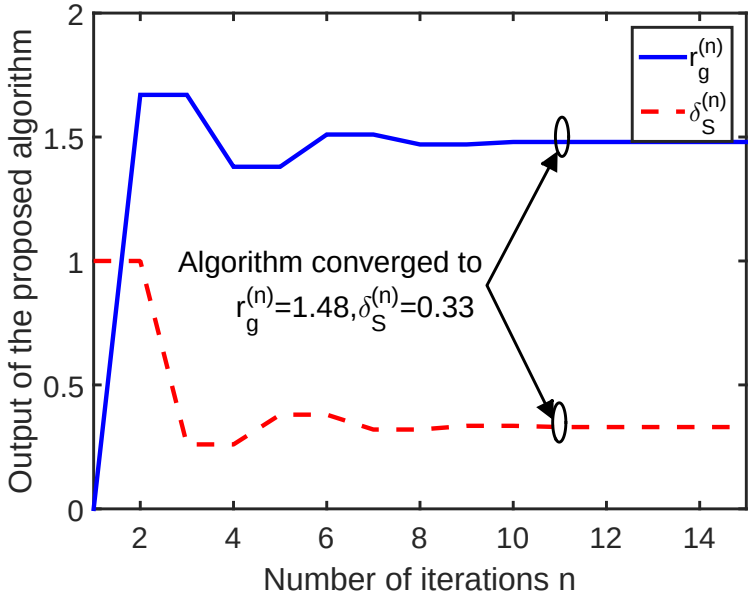

Figure 5.10: The proposed algorithm converges to Nash equilibrium in a finite number of iterations.

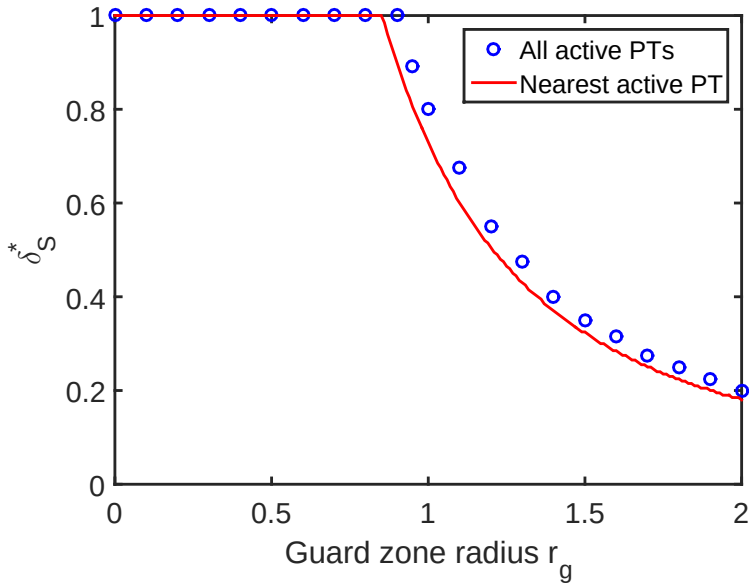

Figure 5.11: Normalized optimal density δ_S^* against guard zone radius r_g for two cases: (i) when the energy harvested only from the nearest active PT is considered, and (ii) when energy harvested from all active PTs is considered.

Chapter 6

Tight Lower Bounds on the Contact Distance Distribution in Poisson Hole Process

In this chapter, we derive new lower bounds on the cumulative distribution function (CDF) of the contact distance in the PHP for two cases: (i) reference point is selected uniformly at random from $\mathbb{R}^2$ independently of the PHP, and (ii) reference point is located at the center of a hole selected uniformly at random from the PHP. While one can derive upper bounds on the CDF of contact distance by simply ignoring the effect of holes, deriving lower bounds is known to be relatively more challenging. As a part of our proof, we introduce a tractable way of *bounding* the effect of all the holes in a PHP, which can be used to study other properties of a PHP as well.

6.1 Introduction

Owing to its ability to provide useful system-level performance insights, stochastic geometry has emerged as an attractive tool for the modeling and analysis of a variety of wireless networks [31]. While PPP is often the default choice due to its simplicity and tractability, its inability to model inter-point interactions makes it an unrealistic choice for modeling scenarios in which locations of active nodes exhibit spatial separation due to interference management. One such general class of scenarios results from the creation of exclusion zones around wireless nodes/links to control aggregate interference received by them from the rest of the network. A more appropriate model for such scenarios is a PHP [115, 116], which is the main focus of this letter.

While one can introduce spatial separation between points in a point process in countless ways, PHP is perhaps one of the most tractable amongst them. It is formed by *carving out* holes from a baseline PPP, where the centers of the holes are assumed to follow an independent PPP. The remaining points of the baseline PPP are said to form a PHP. This model has found numerous

applications in wireless networks. It was used in [116] to model a cognitive radio network, where the hole centers model the locations of the primary receivers and the PHP models the locations of the secondary transmitters. More recently, a very similar setup was used to model underlay device-to-device (D2D) communication in cellular networks, where protection zones are created around cellular links to save them from excessive interference from the D2D links [85,120,121]. Similarly, PHP has also found application in the modeling of inter-tier dependence in a heterogeneous cellular network, where the hole centers represent macrocell BSs and the PHP models the (active) small cell locations [122, 123]. For a more detailed literature survey, interested readers are advised to refer to [124]. For completeness, please note that PHP is also sometimes referred to as the *Hole*-1 *process* [125].

Even though PHP is generated from two independent homogeneous PPPs, its analysis is known to be significantly more challenging compared to a homogeneous PPP. In fact, until recently, the state-of-the-art approach to their analysis was to approximate them using homogeneous PPP whose density is matched to that of the PHP. One can also *bound* the performance of a PHP network by ignoring all the holes and approximating the PHP by its baseline PPP. More accurate bounding techniques were recently developed in [124] that resulted in tight upper and lower bounds on the Laplace transform of interference in a PHP network.

Despite these recent efforts, we still lack complete characterization of several basic properties of a PHP. One of the most important amongst them is the contact distance distribution. In the literature, contact distance distribution is usually approximated by Weibull distribution whose parameters are determined using curve fitting [122]. While this approximation is usually tight, the use of curve fitting curtails the generality of this approach. In particular, since the parameters of Weibull distribution depend upon the system setup, we need to perform the curve fitting step every time the system parameters are changed. Second, somewhat less used approach, is to bound the CDF of contact distance from above by ignoring all the holes. The bound can be tightened slightly with some loss in tractability by incorporating the effect of the nearest hole to the reference point, as done in [126]. In this letter, we derive the first known lower bounds on the CDF, which along with these upper bounds and approximations provide almost complete characterization of the contact distance distribution in a PHP.

Contributions. We derive lower bounds on the CDF of the contact distance in a PHP for two cases. In the first case, the reference point is chosen uniformly at random from $\mathbb{R}^2$ independently of the PHP, which is usually how the contact distance is classically defined. In the second case, the reference point is chosen to be the center of a hole selected uniformly at random from the PHP. This allows us to study the distance between the node which is being protected from the interference (located at the center of the hole) and the strongest interferer (closest point of the PHP from this node). In order to derive the lower bounds on CDF, we carefully *bound* the effect of carving out holes using simple geometric tricks that lend tractability to the analysis. A closed-form lower bound for the first case is also derived. The tightness of all the bounds is verified by comparing them with simulation results.

6.2 Contact Distance Distributions

Before deriving the distributions of the contact distance for the two reference points, we first formally define the PHP.

6.2.1 Poisson Hole Process

The PHP is constructed using two independent PPPs $\Phi_1 \equiv \{y\} \subset \mathbb{R}^2$ and $\Phi_2 \equiv \{x\} \subset \mathbb{R}^2$ with densities λ_1 and λ_2, respectively. The first PPP Φ_1 represents the locations of the hole centers, while the second PPP Φ_2 represents the baseline process from which the holes are carved out. The points retained in Φ_2 after carving out the holes form the PHP Ψ, which can be mathematically defined as

$$\Psi = \{x \in \Phi_2 : x \notin \bigcup_{y \in \Phi_1} \mathcal{B}(y, D)\}, \tag{6.1}$$

where D is the radius of the holes, and $\mathcal{B}(y, D)$ is a circle of radius D centered at y. Using this notation, we now derive the lower bounds on the CDFs of the contact distance for two different cases. Due to the stationarity of this setup, we will place the reference point at the origin in both the cases.

6.2.2 Reference Point is Chosen Uniformly at Random from $\mathbb{R}^2$

In this case, we assume that the reference point is chosen uniformly at random from $\mathbb{R}^2$ independently of the PHP Ψ. Contact distance R_1 for this case is the distance between this reference point and its nearest point of Ψ. For this case, the CDF of the contact distance is defined next.

Definition 6 (Contact distance distribution)**.** *The CDF of the contact distance when the reference point is chosen uniformly at random from $\mathbb{R}^2$ independently of Ψ is*

$$F_{R_1}(r) = \mathbb{P}\left(R_1 < r\right) = \mathbb{P}\left(\mathcal{N}_\Psi\left(\mathcal{B}(o, r)\right) > 0\right), \tag{6.2}$$

where R_1 is the contact distance, and $\mathcal{N}_\Psi\left(\mathcal{B}(o, r)\right)$ is the number of points of the PHP Ψ inside a circle of radius r centered at the origin.

A lower bound on the CDF of R_1 is derived next.

Theorem 9 (Lower bound on $F_{R_1}(r)$)**.** *A lower bound on the CDF of contact distance R_1 is*

$$F_{R_1}(r) \geq 1 - \exp\left(-\lambda_2 \pi r^2\right) \exp\left(-2\pi\lambda_1 \mathcal{G}_1(r)\right), \tag{6.3}$$

where $\mathcal{G}_1(r) = \left(1 - \exp\left(\lambda_2 \pi \min\{r, D\}^2\right)\right) \frac{(D-r)^2}{2} + \int_{|r-D|}^{D+r} \left(1 - \exp(\lambda_2 \mathcal{H}_1(r, r_y))\right) r_y \mathrm{d}r_y$, $|r - D|$ is the absolute value of $r - D$, $\mathcal{H}_1(r, r_y) = \left((r + D)^2 - (r_y)^2\right) \theta(r_y)$, and $\theta(r_y) = \sin^{-1}\left(\frac{D}{D + r_y}\right)$.

Proof: See Appendix D.1.
As discussed in detail in Appendix D.1, the above result is derived using the simple idea of excluding the area covered by the holes from the circle $\mathcal{B}(o,r)$. In order to maintain tractability, we neglect the possible overlaps between holes. As a result, we end up excluding the overlap regions multiple times, which provides a lower bound on the CDF. More details about the derivation can be found in Appendix D.1.

While the lower bound presented in Theorem 9 is fairly straightforward to compute, it is not in closed form since the expression for $\mathcal{G}_1(r)$ contains an integral term. The main challenge in simplifying the integral term in $\mathcal{G}_1(r)$ is the presence of $\sin^{-1}\left(\frac{D}{D+r_y}\right)$ term in the integrand. That being said, we can bound this expression by partitioning the integration interval into N sub-intervals. For each of these sub-intervals, we can use the lower limit in the integral to get an upper bound on the $\sin^{-1}\left(\frac{D}{D+r_y}\right)$ term. This eventually leads to a lower bound on the result in Theorem 9. Obviously, as the value of N increases, this lower bound will converge to the result provided in Theorem 9. As an example, we provide in the next Corollary the closed form bound for $N=1$ obtained using this procedure. It is straightforward to get the corresponding expression for any given value of N.

Corollary 5. *A closed-form lower bound on the contact distance distribution of PHP is* $F_{R_1}(r) \geq$

$$\begin{cases} 1-\exp\left(-\lambda_2\pi r^2\right)\exp\left(-2\pi\lambda_1\mathcal{G}_2(r)\right) & , r \leq D \\ 1-\exp\left(-\lambda_2\pi D^2\right)\exp\left(-2\pi\lambda_1\mathcal{G}_3(r)\right) & , r > D \end{cases}. \tag{6.4}$$

where $\mathcal{G}_2(r) = \mathcal{F}(\theta_1)$, $\mathcal{G}_3(r) = \mathcal{F}(\theta_2)$, $\theta_1 = \sin^{-1}\left(\frac{D}{2D-r}\right)$, $\theta_2 = \sin^{-1}\left(\frac{D}{r}\right)$, *and* $\mathcal{F}(\theta) = \left(1-\exp\left(\lambda_2\pi\min\{r,D\}^2\right)\right)\frac{(D-r)^2}{2} - \frac{\exp(4\theta\lambda_2 Dr)-1}{2\lambda_2\theta} + 2rD$.

6.2.3 Reference Point is One of the Hole Centers

As explained already, hole centers in a wireless network often correspond to the nodes that are being protected from excessive interference. It is therefore important to study the statistics of the distance between a hole center and the closest point of Ψ (closest possible interferer), which corresponds to the contact distance from a reference point placed at the center of a hole chosen uniformly at random from a PHP. We denote this distance by R_2 and its CDF is formally defined next.

Definition 7 (Distribution of the contact distance from a hole center)**.** *The CDF of the contact distance when the reference point belongs to* Φ_1 *is*

$$F_{R_2}(r) = \mathbb{P}\left(R_2 < r\right) = \mathbb{P}\left(\mathcal{N}_\Psi\left(\mathcal{B}(o,r)\right) > 0 \middle| o \in \Phi_1\right), \tag{6.5}$$

where R_2 *is the contact distance, and* $\mathcal{N}_\Psi\left(\mathcal{B}(o,r)\right)$ *is the number of points of the PHP* Ψ *that fall inside a circle of radius* r *centered at the origin.*

By construction, the minimum distance between the hole center and its nearest PHP point is D. Using this fact and following the same approach used in Theorem 9, we derive a lower bound on the contact distance distribution for this case in the following Theorem.

Theorem 10 (Lower bound on $F_{R_2}(r)$)**.** *A lower bound on the CDF of the contact distance R_2 is:* $F_{R_2}(r)$

$$\geq \; 1 - \exp\left(-\lambda_2 \pi (r^2 - D^2)\right) \exp\left(-2\pi\lambda_1 \mathcal{G}_4(r)\right) \quad , r > D \; . \tag{6.6}$$

where $\mathcal{G}_4(r) = \int_0^{r+D} \left(1 - \exp(\lambda_2 \mathcal{H}_2(r, r_y))\right) r_y \mathrm{d}r_y$, *and*
$\mathcal{H}_2(r, r_y) = \left(\min\{r + D, r_y + 2D\}^2 - \max\{r_y, 2D\}^2\right) \theta(r_y)$.

Proof: See Appendix D.2.
As was the case in Theorem 9, it is fairly straightforward to compute the lower bound presented in the above Theorem. The accuracy of both these result as well as the closed-form lower bound for the previous case is investigated next.

6.2.4 Numerical Results

The tightness of the lower bounds on the CDFs of both R_1 and R_2 is verified by comparing them with simulations in Figs. 6.1 and 6.2. We consider $\lambda_1 = 10 \text{ km}^{-2}$ and several combinations of λ_2 and D, which are all indicated in the plots. The closed-form lower bound on the CDF of R_1 is also plotted for completeness. We chose $N = 8$, which was sufficient in this case to converge to the result of Theorem 9. In order to provide a complete picture, we also include an upper bound on the CDF, which is computed by *bounding* the PHP by its baseline PPP Φ_2, and an *approximation* which is computed by approximating the PHP by a PPP with equivalent density $\tilde{\lambda} = \lambda_2 e^{-\lambda_1 \pi D^2}$. In both these PPP-based cases, the contact distance distribution is easily computed using the null probability of the PPP. In both the figures, we notice that new lower bounds along with the PPP-based upper bound and heuristic approximation collectively provide a sharp characterization of the contact distance distribution.

6.3 Summary

In this letter, we derived tight lower bounds on the CDF of the contact distance in a PHP for two different choices of the reference point. The main technical contribution is a new bounding technique using which we carefully handled the effect of all the holes of a PHP while maintaining tractability. The tightness of the new bounds across different scenarios is verified numerically. The proposed approach and new results can be readily used to derive tight bounds for key performance metrics of interest, such as receiver power, coverage probability, and throughput, in wireless networks modeled as a PHP. In the next chapter, we extend our work in Chapter 5 to study the performance of three different secrecy-enhancing techniques, unlike Chapter 5, where we focused on the guard zone technique.

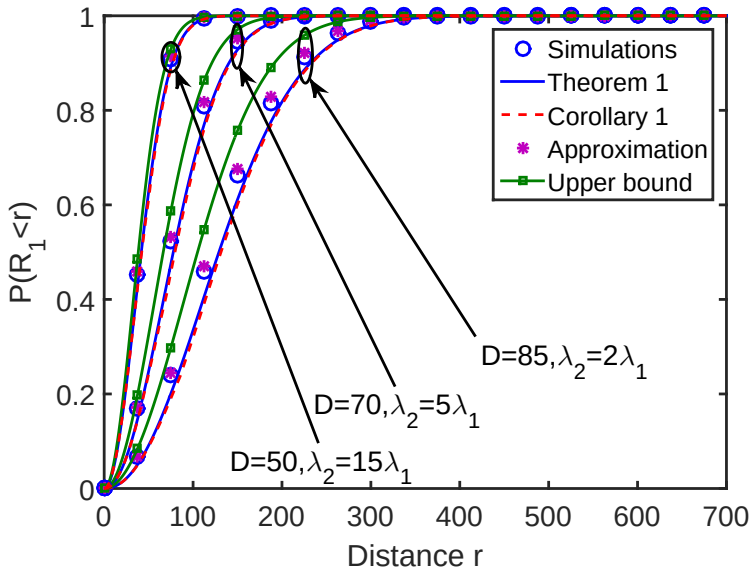

Figure 6.1: The CDF of the contact distance R_1.

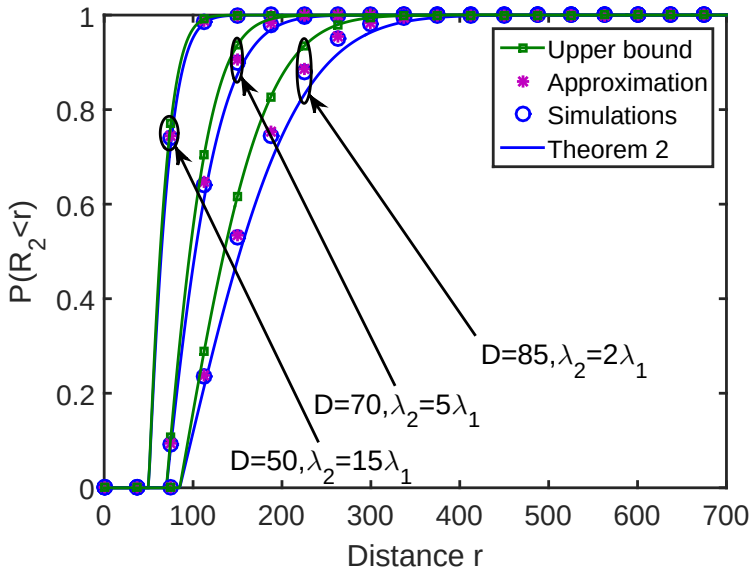

Figure 6.2: The CDF of the contact distance R_2.

Chapter 7

Enhancing Physical Layer Security in SWIPT Systems with Untrusted Energy Receivers

This chapter revisits the problem discussed in Chapter 5 by extending the analysis to two more secrecy enhancing techniques. A system composed of information transmitters (ITs), information receivers (IRs), and energy receivers (ERs) is considered. Each IT transmits an information signal to its intended IR, which should simultaneously be used by the ERs to harvest energy. However, due to the tendency of ERs to be located closer to the ITs, to harvest more energy, the secrecy performance of RF transmissions needs to be carefully studied. To ensure the secrecy of the transmitted signals while providing the ERs with sufficient energy, the ITs need to carefully pick a secrecy enhancing technique that is suitable for such system. We provide a generalized model that can be used for studying the secrecy performance of the transmitted information and the statistics of the energy received by the ERs. This generalized model captures three popular secrecy enhancing techniques: (i) adding artificial noise (AN) to the transmitted signal, (ii) surrounding the information transmitters (ITs) with secrecy guard zones (which was considered in Chapter 5), and (iii) using directional beamforming towards the intended IRs. The proposed model is used to derive the successful connection and the secrecy outage probabilities of the IR ($P_{\rm con}$ and $P_{\rm out}$, respectively) and the energy coverage probability ($P_{\rm energy}$) of the ER for each of the three techniques. We study the influence of the guard zone radius, the AN power splitting ratio, and the beamwidth on these performance metrics. We also study the scenarios under which each of these techniques outperforms the others, in terms of each of the three aforementioned performance metrics. We focus on two parameter selection criteria: (i) minimizing $P_{\rm out}$ for given constraints on $P_{\rm con}$ and $P_{\rm energy}$, and (ii) maximizing $P_{\rm con}$ for given constraints on $P_{\rm out}$ and $P_{\rm energy}$. At lower densities of ERs, the results demonstrate the optimality of the GZ technique for the first selection criterion and the BF technique for the second selection criterion. At higher densities of ERs, however, the AN technique is shown to be optimal for both the selection criteria.

7.1 Introduction

As explained in Chapter 5, it is important to provide secrecy analysis for the RF signals in the systems of RF-powered wireless networks, which results mainly from the tendency of the RF-powered devices to be located closer to the sources of RF energy. This problem gains even more importance in simultaneous wireless information and power transmission (SWIPT) systems. A typical SWIPT system consists of information transmitters (ITs), information receivers (IRs), and energy receivers (ERs). The IT transmits information-carrying signals to the intended IR, which are used at the same time at the ERs for harvesting RF energy. However, in order to avoid signal attentuation, the ERs try to locate themselves closer to ITs in order to harvest more energy. This, in turn, raises serious secrecy concerns when the ERs are not completely trustworthy and can be considered potential eavesdroppers [93,95,97]. In that case, the IT needs to adopt some secrecy enhancing technique that preserves the physical layer security (PLS) of the transmitted signal without affecting the amount of energy harvested by the ERs. PLS-based secrecy enhancing techniques are designed such that the legitimate receivers (the IRs) are able to successfully decode the transmitted signal while the ERs are unable to do so [81]. Among many possible PLS-based solutions, we focus in this chapter on three main techniques: (i) adding artificial noise (AN) to the transmitted signal to degrade the SIR at the ER [98], (ii) surrounding the IT with a guard zone (GZ) where it stops transmission (goes silent) with probability $1-q$ when at least one ER is detected within the guard zone [81, 99], and (iii) in case of multi-antenna transmitters, using directional beamforming (BF) towards the IR [94].

In this chapter, we use tools from stochastic geometry to study the secrecy of the SWIPT system and characterize the energy harvesting statistics at the ERs when each of the three techniques is adopted. To the best of our knowledge, this chapter provides the first system-level comparison of these techniques for the secure SWIPT systems. In addition, unlike existing literature, where the SWIPT secrecy problem is usually studied for deterministic spatial setups, we consider a more general large-scale setup in which ITs and ERs are modeled using point processes.

7.1.1 Related Work

Due to its tractability and realism, stochastic geometry is widely used in literature to model and analyze wireless networks [30, 31]. For this chapter, the most relevant prior art on stochastic geometry can be categorized as: (i) stochastic geometry-based analysis of energy harvesting wireless networks [33, 36, 37, 66, 102, 127], and (ii) stochastic geometry-based analysis of physical layer security in wireless networks [46, 87, 100, 101]. A more detailed discussion on the related work for each of both areas is provided next.

Stochastic geometry-based analysis of energy harvesting wireless networks. Authors in [33] used tools from stochastic geometry and Markov chain to study the performance of cellular network with energy harvesting base stations (BSs). Availability analysis of the BSs as well as optimal transmission policies are proposed. Authors in [66, 102] studied the joint distribution of both downlink

SINR coverage and amount of harvested energy by the wireless device. The joint distribution of uplink SINR and the amount of harvested energy is performed in [37]. A general framework that captures joint downlink and uplink SINR coverage and energy coverage is proposed in [127].

Stochastic geometry-based analysis of physical layer security in wireless networks. Authors in [87] study the secrecy outage probability and the average secrecy rate in a cellular network where all the mobile users are considered potential eavesdroppers with the capability to cooperate. In [100], authors provide comparison of guard zone technique and artificial noise technique in terms of successful connection probability and secure communication probability. The system considered in that paper is composed of a single Tx-Rx and randomly located eavesdroppers. In [101], authors use stochastic geometry to study the secrecy of downlink transmission for both half and full duplex receivers. The locations of the eavesdroppers are assumed to be random and the analysis is provided for both cases of independent and cooperating eavesdroppers. Inčite7320989, authors studied the secrecy performance of energy harvesting systems when the legitimate transmitters are powered by RF energy harvesting.

However, the consideration of secrecy concerns in wireless power transmission using stochastic geometry is an unchartered area, with the only existing work being [128, 129], which presented in Chapter 5. That said, in this work, we focused only on the guard zone technique and assumed no collaboration between the ITs and the ERs. In other words, we assumed the IT's only objective is to ensure secrecy, regardless of whether the ER is able to harvest energy or not.

Secrecy concerns in SWIPT systems where ERs act as eavesdroppers have been explored recently for the deterministic system setups [91, 110–112]. In [91, 110], a simple system of one IT, one IR, and one ER (potential eavesdropper) was studied. A more general setup composed of one IT, one IR, and K ERs was studied in [111]. In [112], the secrecy of SWIPT systems was studied for a setup of one macro BS serving M users, N femto BSs each serving K users, and L ERs. In contrast to these works, in this chapter, we assume random locations for both ITs and ERs. Modeling these locations using point processes and using tools from stochastic geometry enables us to glean multiple useful system-level insights as will be explained next in more detail.

7.1.2 Contributions

The secrecy of SWIPT systems is studied for a general setup where, unlike existing literature, no specific topology of ITs, IRs, and ERs is assumed. In particular, we model the locations of ITs and ERs using PPP, which enables us to draw useful insights. In addition, we provide generalized expressions for the secrecy outage probability and the energy coverage probability of the ERs. These expressions are generalized in the sense that they can be easily specialized to the following three popular secrecy enhancing technique: (i) adding artificial noise to the transmitted signals (will be referred to as AN technique in the rest of the chapter), (ii) surrounding the ITs with guard zones (will be referred to as GZ technique in the rest of the chapter), and (iii) using directional beamforming towards the intended IR (will be referred to as BF technique in the rest of the chapter). These analytical results are then used to study the regimes under which each of the three techniques

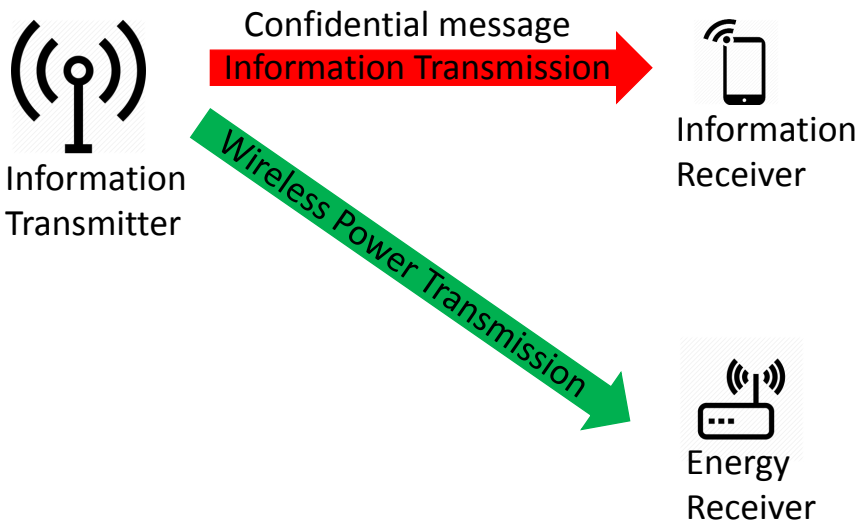

Figure 7.1: The SWIPT system with untrusted energy receiver.

outperforms the other two. For these comparisons, we consider two possible objectives for the IT: (i) minimize the secrecy outage probability while satisfying given constraints on energy coverage and successful connection probabilities and (ii) maximize the successful connection probability while satisfying given constraints on secrecy outage and energy coverage probabilities.

7.2 System Model

We consider a SWIPT system, shown in Fig. 7.4, where the locations of the ITs are modeled using a PPP $\Phi_P \equiv \{x_i\} \subset \mathbb{R}^2$ with density λ_P. Each IT has an intended IR at a distance r_1 in a uniformly random direction. The locations of the ERs are modeled by a homogeneous PPP $\Phi_S \equiv \{y_i\} \subset \mathbb{R}^2$ with density λ_S. The transmit power of each IT is P_t. Hence, the received power at the intended IR is $P_t g r_1^{-\alpha}$, where $g \sim \exp(1)$ models Rayleigh fading gain and $r_1^{-\alpha}$ models the power law path-loss with $\alpha > 2$. Without loss of generality, we focus our analysis on a typical IT located at the origin. The received power by an arbitrary ER located at y_i is $P_t h_{0,i} \|y_i\|^{-\alpha}$, where $h_{0,i} \sim \exp(1)$ models Rayleigh fading gain which is assumed to be independent across all IT-ER links. The IT uses a secrecy enhancing technique in order to preserve the secrecy of the transmitted signal, which can be either AN, GZ, or BF technique. More details on each of these techniques are provided next.

7.2.1 AN Technique

In this technique, the IT splits the transmission power (P_t) into: (i) γP_t used for information transmission and (ii) $(1-\gamma)P_t$ used for AN. As discussed in [93], the AN is generated using

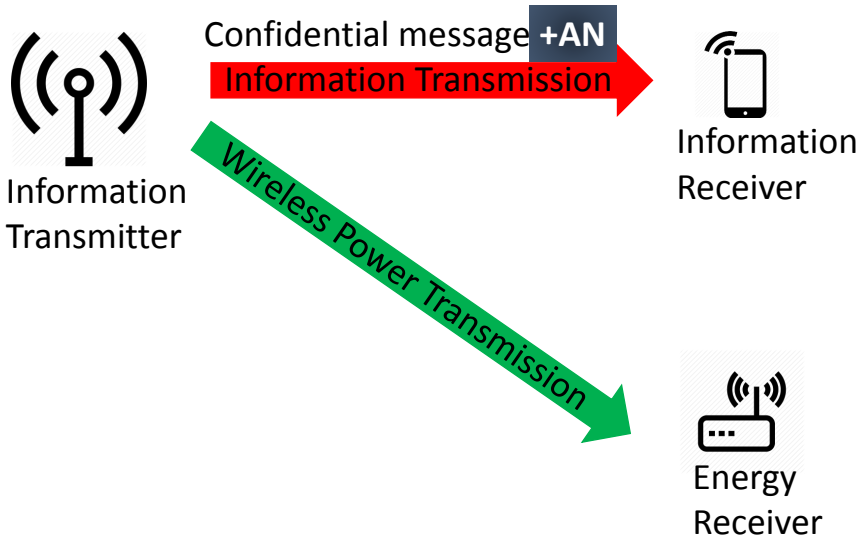

Figure 7.2: The SWIPT system with untrusted energy receiver and AN technique for enhancing data secrecy.

random sequences whose indices (keys) are shared with the IRs. Hence, the AN can be decoded only by the IRs. The received power of the information signal at the intended IR is $\gamma P_t g r_1^{-\alpha}$ while the total received power at an arbitrary ER located at y_i is $P_t h_{0,i} \|y_i\|^{-\alpha}$.

7.2.2 GZ Technique

In this technique, the IT surrounds itself with a guard zone of radius r_g. If the guard zone is free of ERs, the IT transmits the information to the IR. If the guard zone is not free of ERs, the IT transmits with probability q, and stays silent with probability $1-q$. Hence, the probability that the IT transmits the signal is

$$\begin{aligned} P_{\text{active}} &= \mathbb{P}(\mathcal{N}_{\Phi_S}(\mathcal{B}(0,r_g)) = 0) + q \times \mathbb{P}(\mathcal{N}(\mathcal{B}(0,r_g)) > 0) \\ &= e^{-\lambda_S \pi r_g^2} + q\left(1 - e^{-\lambda_S \pi r_g^2}\right), \end{aligned} \tag{7.1}$$

where $\mathcal{N}_{\Phi_S}(\mathcal{B}(0,r_g))$ is the number of ERs inside a ball of radius r_g centered at the origin. In the case of active IT, the received power by the intended IR is $P_t g r_1^{-\alpha}$, while the received power by an arbitrary ER located at y_i is $P_t h_{0,i} \|y_i\|^{-\alpha}$.

7.2.3 BF Technique

In this technique, a multi-antenna IT is assumed where we consider the sectored antenna model, which is commonly used in literature [67, 130]. In particular, the antenna beam pattern is charac-

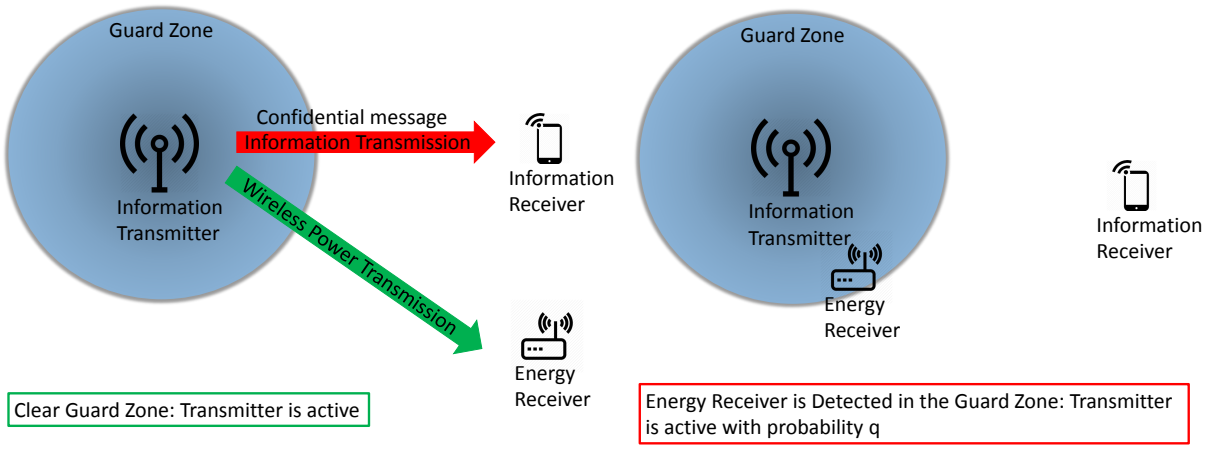

Figure 7.3: The SWIPT system with untrusted energy receiver and guard zone technique for enhancing data secrecy.

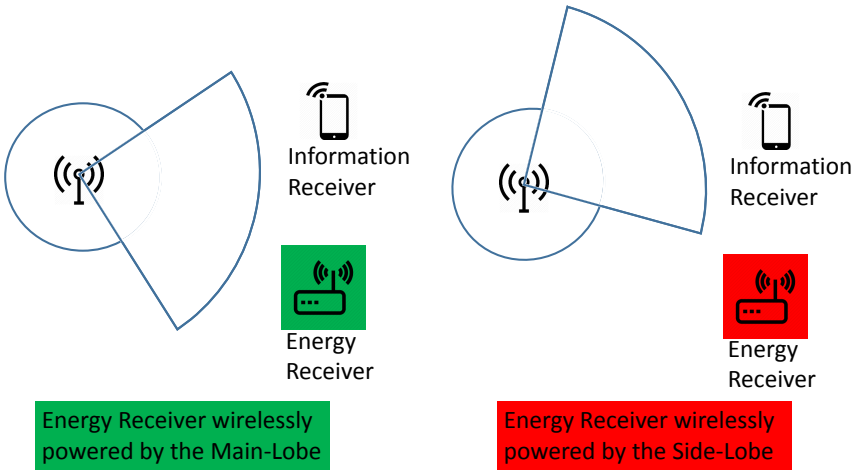

Figure 7.4: The SWIPT system with untrusted energy receiver and beamforming technique for enhancing data secrecy.

terized by the main lobe directivity gain (G_m) and the side lobe directivity gain (G_s). Furthermore, the beamwidth of the main lobe is θ_m while the beamwidth of the side lobe is θ_s. The IT is assumed to know the location of the intended IR. Hence, the received power by the IR is $G_m P_t g r_1^{-\alpha}$ while the received power by an arbitrary ER located at y_i is either $G_m P_t h_{0,i} \|y_i\|^{-\alpha}$ with probability $\frac{\theta_m}{2\pi}$ or $G_s P_t h_i \|y_i\|^{-\alpha}$ with probability $\frac{\theta_s}{2\pi}$.

7.2.4 Performance Metrics

Now, we provide a generic expression for the SIR at the typical IR, which is valid for an arbitrary secrecy enhancing technique $\mathrm{S} \in \{\mathrm{AN}, \mathrm{GZ}, \mathrm{BF}\}$.

$$\mathrm{SIR}_{\mathrm{I}} = \frac{\tau^S g r_1^{-\alpha}}{\sum_{x_j \in \Phi_P \setminus x_0} \delta_j^S w_j \|x_j - z\|^{-\alpha}}, \tag{7.2}$$

where z is the location of the typical IR, x_0 is the location of the typical IT, and $w_j \sim \exp(1)$ models Rayleigh fading gain. The values of τ^S and δ^S are given below.

$$\tau^{\mathrm{AN}} = \gamma,\ \tau^{\mathrm{GZ}} = 1,\ \tau^{\mathrm{BF}} = G_m, \tag{7.3}$$

$$\delta^S = \begin{cases} a^S & \text{with probability } p_a^S \\ b^S & \text{with probability } p_b^S \end{cases}. \tag{7.4}$$

and

$$\begin{aligned} &a^{\mathrm{AN}} = 1,\ b^{\mathrm{AN}} = 0,\ p_a^{\mathrm{AN}} = 1,\ p_b^{\mathrm{AN}} = 0, \\ &a^{\mathrm{GZ}} = 1,\ b^{\mathrm{GZ}} = 0,\ p_a^{\mathrm{GZ}} = P_{\mathrm{active}},\ p_b^{\mathrm{GZ}} = 1 - P_{\mathrm{active}}, \\ &a^{\mathrm{BF}} = G_m,\ b^{\mathrm{BF}} = G_s,\ p_a^{\mathrm{BF}} = \frac{\theta_m}{2\pi},\ p_b^{\mathrm{BF}} = \frac{\theta_s}{2\pi}. \end{aligned} \tag{7.5}$$

On the other hand, the SIR at an arbitrary ER located at y_i is

$$\mathrm{SIR}_{\mathrm{E}}(y_i) = \frac{\sigma^S h_{0,i} \|y_i\|^{-\alpha}}{\sum_{x_j \in \Phi_P \setminus x_0} \delta_j^S h_j \|x_j - y_i\|^{-\alpha} + \kappa^S h_{0,i} \|y_i\|^{-\alpha}}, \tag{7.6}$$

where $\kappa^{\mathrm{AN}} = (1 - \gamma)$, $\kappa^{\mathrm{GZ}} = 0$, $\kappa^{\mathrm{BF}} = 0$ and

$$\sigma^S = \begin{cases} c^S & \text{with probability } p_c^S \\ d^S & \text{with probability } p_d^S \end{cases}. \tag{7.7}$$

In addition, $c^{\mathrm{AN}} = \gamma$, $d^{\mathrm{AN}} = 0$, $p_c^{\mathrm{AN}} = 1$, $p_d^{\mathrm{AN}} = 0$, $c^{\mathrm{GZ}} = 1$, $d^{\mathrm{GZ}} = 0$, $p_c^{\mathrm{GZ}} = 1$, $p_d^{\mathrm{GZ}} = 0$, $c^{\mathrm{BF}} = G_m$, $d^{\mathrm{BF}} = G_s$, $p_c^{\mathrm{BF}} = \frac{\theta_m}{2\pi}$, and $p_d^{\mathrm{BF}} = \frac{\theta_s}{2\pi}$.

Before defining the secrecy-related performance metrics, we briefly discuss Wyner's encoding scheme [88]. In this scheme, the IT defines two rates: (i) the rate of codewords $C_{\rm t}$ and the rate of messages $C_{\rm s}$ [81]. In order to ensure successful decoding at the IR and perfect secrecy, two conditions need to be satisfied: (i) $C_{\rm t} \leq \mathcal{I}_{\rm t}$, where $\mathcal{I}_{\rm t}$ is the mutual information between IT's channel input and IR's channel output and (ii) $C_{\rm e} \geq \mathcal{I}_{\rm e}$, where $\mathcal{I}_{\rm e}$ is the mutual information between IT's channel input and ER's channel output and $C_{\rm e} = C_{\rm t} - C_{\rm s}$. Alternatively, we can rewrite both conditions as: (i) $\mathrm{SIR}_{\rm I} \geq \beta_I$, where $\beta_I = 2^{C_{\rm t}} - 1$ and (ii) $\mathrm{SIR}_{\rm E} \leq \beta_E$, where $\beta_E = 2^{C_{\rm e}} - 1$. Now, we define both successful connection and secrecy outage probabilities below.

Definition 8 (Probability of successful connection)**.** *To achieve a successful connection between the typical IT and IR, the typical IT needs to be active, and the SIR at the IR needs to be greater than β_I. Hence, the successful connection probability is*

$$P_{\rm con}^{S} = \mathbb{P}(R_e \geq \mu^{S}, \mathrm{SIR}_{\rm I} \geq \beta_I) + q\mathbb{P}(R_e < \mu^{S}, \mathrm{SIR}_{\rm I} \geq \beta_I). \tag{7.8}$$

where R_e is the distance between the typical IR and its nearest ER, $\mu^{\rm GZ} = r_g$, $\mu^{\rm AN} = 0$, and $\mu^{\rm BF} = 0$.

Definition 9 (Secrecy outage probability)**.** *Given that the typical IT is active, secrecy outage takes place if the condition $\mathrm{SIR}_{\rm E} \leq \beta_E$ is violated at any ER, which can be mathematically expressed as*

$$P_{\rm out}^{S} = 1 - \mathbb{E}\left[\mathbf{1}\left(\bigcap_{y_i \in \Phi_S} \mathrm{SIR}_{\rm E}(y_i) \leq \beta_E \middle| \mathcal{E}_{\rm active}^{S}\right)\right], \tag{7.9}$$

where $\mathcal{E}_{\rm active}^{S}$ is the event of the typical IR being active.

On the other hand, the energy harvested by an arbitrary ER located at y_i is

$$E_{\rm rec}^{S} = \eta T P_t \sum_{x_j \in \Phi_P} \delta_j^{S} h_j \|x_j - y_i\|^{-\alpha}, \tag{7.10}$$

where η is the RF-DC conversion efficiency and T is the duration of the time slot during which the ER is harvesting RF energy.

For each of the three considered secrecy techniques, the IRs select the parameter (γ for AN, r_g for GZ, θ_m for BF) that satisfies a given set of requirements. In this chapter, we will focus on two possible approaches for parameter selection, which are formally defined below.
Approach 1. Minimize $P_{\rm out}^{S}$ while ensuring $\mathbb{P}(E_{\rm rec}^{S} \geq E_{\min}) \geq \epsilon$ and $P_{\rm con}^{S} \geq \xi$.
Approach 2. Maximize $P_{\rm con}^{S}$ while ensuring $\mathbb{P}(E_{\rm rec}^{S} \geq E_{\min}) \geq \epsilon$ and $P_{\rm out}^{S} \leq \zeta$.

7.3 Performance Analysis

In this section, we derive expressions for each of $P_{\rm con}^{S}$, $P_{\rm out}^{S}$, and $\mathbb{P}(E_{\rm rec} \geq E_{\min})$. In the following theorem we derive $P_{\rm con}^{S}$.

Theorem 11 (Probability of successful connection)**.** *The successful connection probability, which is defined in Definition* 8*, is*

$$P_{\text{con}}^{S} = \left(\mathcal{C}^{S} + q(1-\mathcal{C}^{S})\right) \exp\left(-\mathcal{A}\left(\frac{\beta_I r_1^{\alpha}}{\tau^{S}}\right)\right), \tag{7.11}$$

where $\mathcal{C}^{S} = \exp\left(-\lambda_S \pi \left(\mu^{S}\right)^2\right)$ *and* $\mathcal{A}(t) = \frac{2\pi^2 \lambda_P \left(a^{S} p_a^{S} + b^{S} p_b^{S}\right) t^{\frac{2}{\alpha}}}{\alpha \sin\left(\frac{2\pi}{\alpha}\right)}$.

Proof: See Appendix E.1.

Remark 17. *The above expression provides insights on each of the three considered techniques. For the case of AN,* $\mu^{S} = 0$, $\tau^{S} = \gamma$, *and* $a^{S} p_a^{S} + b^{S} p_b^{S} = 1$. *We note that as* γ *increases, which means that the power allocated for information transmission increases, the probability of successful connection increases. In the case of GZ,* $\mu^{S} = r_g$, $\tau^{S} = 1$, *and* $a^{S} p_a^{S} + b^{S} p_b^{S} = P_{\text{active}}$. *We notice that the effect of increasing* r_g *on the value of* P_{con}^{S} *is two fold: (i) it decreases the probability of being active, which appears in the expression of* $\mathcal{C}^{S}$ *and (ii) it decreases the amount of perceived interference at the IR, which appears in expression of* $\mathcal{A}$. *In the case of BF,* $\mu^{S} = 0$, $\tau^{S} = G_m$, *and* $a^{S} p_a^{S} + b^{S} p_b^{S} = \frac{G_m \theta_m + G_s \theta_s}{2\pi}$. *We can easily observe that decreasing the beamwidth of the main lobe* θ_m *increases the value of* P_{con}^{S}.

In the following theorem we derive the secrecy outage probability.

Theorem 12 (Secrecy outage probability)**.** *For a given value of* λ_S, P_{out}^{S} *is given as follows*

$$\begin{aligned} P_{\text{out}}^{S} = 1 &- \frac{p_c^{S} \mathcal{C}^{S} \exp\left(-\frac{\pi\lambda_S}{\mathcal{A}(\bar{\beta}_E)} \exp\left(-\mathcal{A}(\bar{\beta}_E)\left(\mu^{S}\right)^2\right)\right)}{\mathcal{C}^{S} + q\left(1-\mathcal{C}^{S}\right)} \\ &- \frac{p_c^{S} q\left(\exp\left(-\frac{\pi\lambda_S}{\mathcal{A}(\bar{\beta}_E)}\right) - \mathcal{C}^{S} \exp\left(-\frac{\pi\lambda_S}{\mathcal{A}(\bar{\beta}_E)} \exp\left(-\mathcal{A}(\bar{\beta}_E)\left(\mu^{S}\right)^2\right)\right)\right)}{\mathcal{C}^{S} + q\left(1-\mathcal{C}^{S}\right)} \\ &- \frac{p_d^{S} \mathcal{C}^{S} \exp\left(-\frac{\pi\lambda_S}{\mathcal{A}(\hat{\beta}_E)} \exp\left(-\mathcal{A}(\hat{\beta}_E)\left(\mu^{S}\right)^2\right)\right)}{\mathcal{C}^{S} + q\left(1-\mathcal{C}^{S}\right)} \\ &- \frac{p_d^{S} q\left(\exp\left(-\frac{\pi\lambda_S}{\mathcal{A}(\hat{\beta}_E)}\right) - \mathcal{C}^{S} \exp\left(-\frac{\pi\lambda_S}{\mathcal{A}(\hat{\beta}_E)} \exp\left(-\mathcal{A}(\hat{\beta}_E)\left(\mu^{S}\right)^2\right)\right)\right)}{\mathcal{C}^{S} + q\left(1-\mathcal{C}^{S}\right)}. \end{aligned} \tag{7.12}$$

where $\mathcal{C}^{S}$ *and* $\mathcal{A}(t)$ *are given in Theorem* 11, $\bar{\beta}_E = \frac{\beta_E}{c^{S} - \kappa^{S}\beta_E}$, *and* $\hat{\beta}_E = \frac{\beta_E}{d^{S} - \kappa^{S}\beta_E}$.

Proof: See Appendix E.2.

Remark 18. *Similar to Theorem* 11 *and our comments in Remark* 17*, the expression in* (7.12) *(at the top of the next page) provides insights on each of the three considered techniques. Note that the term* $\mathcal{A}(t)$ *can be thought of as a measure of the interference perceived at the ER, which is*

required to be maximized to decrease the secrecy outage probability. For the case of AN, $\mu^S = 0$, $c^S = \gamma$, $d^S = 0$, and $a^S p_a^S + b^S p_b^S = 1$, we note that as γ increases, which decreases the power allocated for artificial noise, the value of $\mathcal{A}(\bar{\beta}_E)$ decreases. This eventually increases the secrecy outage probability. For the case of GZ, $\mu^S = r_g$, $c^S = 1$, $d^S = 0$, and $a^S p_a^S + b^S p_b^S = P_{\text{active}}$, increasing r_g decreases the value of P_{active}, which decreases the value of $\mathcal{A}(\bar{\beta}_E)$. In the case of BF, $\mu^S = 0$, $c^S = G_m$, $d^S = G_s$, and $a^S p_a^S + b^S p_b^S = \frac{G_m\theta_m + G_s\theta_s}{2\pi}$, we note that decreasing the value of θ_m decreases the value of $a^S p_a^S + b^S p_b^S$ which in turn decreases the interference levels at the ER, which increases the secrecy outage probability. On the other hand, it decreases P_c^S, which is the probability of the ER falling within the main lobe of the typical IR, hence, decreasing the secrecy outage probability.

The next step is to provide an expression for the energy coverage probability of the ERs, which is provided in the following theorem

Theorem 13 (Energy coverage probability)**.** *The energy coverage probability of the ERs is*

$$\mathbb{P}(E_{\text{rec}}^S \geq E_{\min}) = p_a^S \Bigg(1 - e^{-\lambda_P \pi \mathcal{K}^2} + \int_{\mathcal{K}}^{\infty} 2\pi\lambda_P r e^{-\lambda_P \pi r^2 - \frac{C}{a^S}\left(r^\alpha - r^2\mathcal{K}^{\alpha-2}\right)} \mathrm{d}r \Bigg) + p_b^S \Bigg(1 - e^{-\lambda_P \pi \mathcal{K}^2} + \int_{\mathcal{K}}^{\infty} 2\pi\lambda_P r e^{-\lambda_P \pi r^2 - \frac{C}{b^S}\left(r^\alpha - r^2\mathcal{K}^{\alpha-2}\right)} \mathrm{d}r \Bigg), \tag{7.13}$$

where $\mathcal{K} = \left(\frac{2\pi\lambda_P \left(a^S p_a^S + b^S P_b^S\right)}{C(\alpha-2)} \right)^{\frac{1}{\alpha-2}}$ *and* $C = \frac{E_{\min}}{T\eta P_t}$.

Proof: See Appendix E.3.

Remark 19. *The value of $\mathcal{K}$ in the above theorem captures the amount of energy harvested from all IRs except the nearest one. As the value of $a^S p_a^S + b^S P_b^S$ decreases, which results from decreasing r_g or θ_m, the overall amount of harvested energy tends to zero. This is consistent with intuition since decreasing r_g reduces the density of active IRs while reducing θ_m decreases the probability of the ER falling within the beamwidth of the main lobe of the IRs. On the other hand, the value of γ has no effect on the energy coverage probability, which is also consistent with intuition since the value of γ only controls the power of the information signal not the overall signal power (information plus AN).*

7.4 Results and Discussion

Now that we have derived the required metrics, we will use numerical results to study the performance of each of the three considered techniques under Approaches 1 and 2. The following

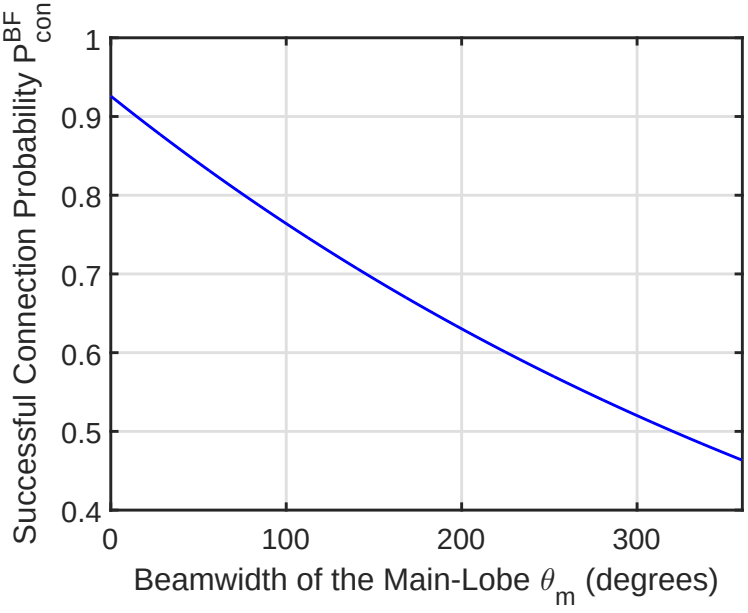

Figure 7.5: The successful connection probability of the beamforming technique against different values of θ_m.

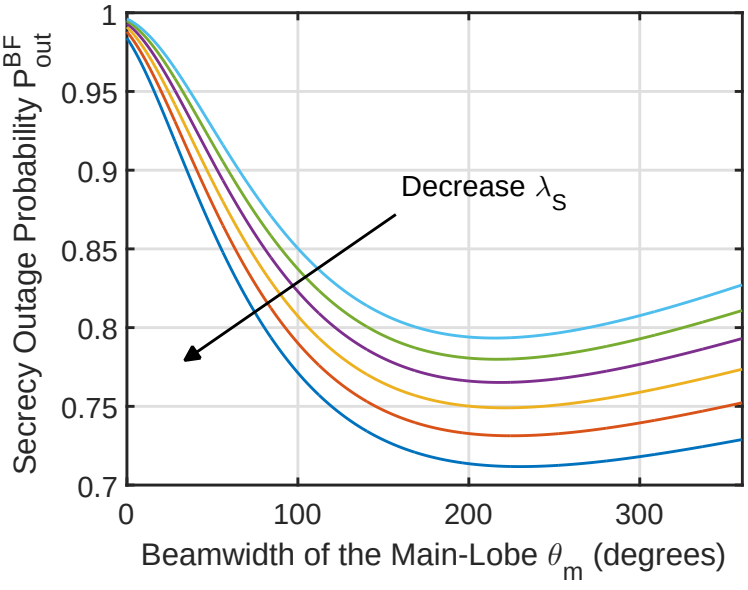

Figure 7.6: The secrecy outage probability of the beamforming technique against different values of θ_m.

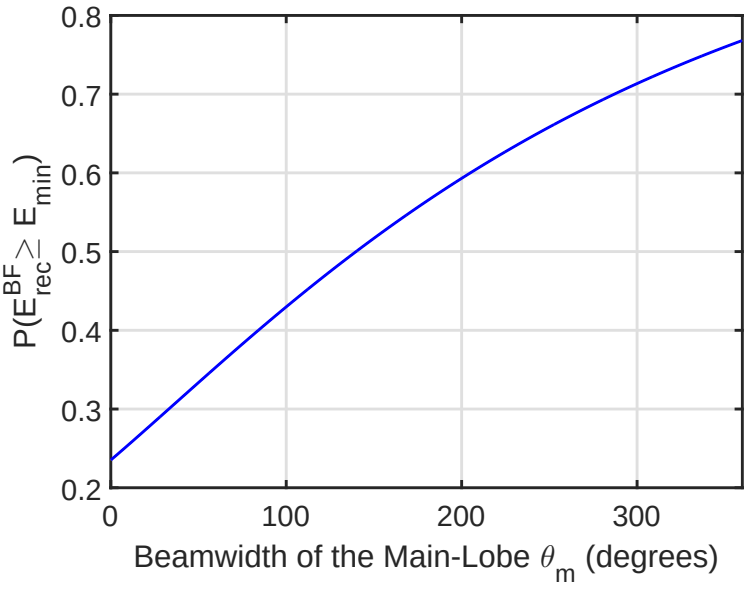

Figure 7.7: The energy coverage probability of the beamforming technique against different values of θ_m.

simulation setup is considered: $\lambda_P = 1$, $\frac{G_m}{G_s} = 10$ dB, $P_t = 10$ dBm, $\eta = 1$, $q = 0.5$, $E_{\min} = 0.1$ Joules, $T = 1$ s, $\epsilon = 0.5$, $\zeta = 0.6$, and $\xi = 0.4$. We first study the performance of each of the three techniques separately. In Fig. 7.5, we plot the successful connection probability for the beamforming technique for different values of θ_m. We note that as the value of θ_m decreases, the successful connection probability increases, which is due to the reduction of the interference experienced by the legitimate receiver. In Fig. 7.6, we plot the secrecy outage probability of the beamforming technique. We note the existence of an optimal value for θ_m that minimizes the secrecy outage probability. Below this value, the beamwidth is too small that the illegitimate receiver is experiencing very low interference and high quality of the signal. Above this optimal value, the beamwidth is too large that the probability of the illegitimate receiver falling within the main beam is high. In Fig. 7.7, we plot the energy coverage probability for the beamforming technique. Agreeing with intuition, as the beamwidth decreases, the energy coverage probability decreases, which is mainly a result of the very narrow beam that reduces amount of interference at the energy receiver. In Fig. 7.8, we plot the successful connection probability for the artificial noise technique for different values of γ. We note that as the value of γ decreases, the successful connection probability decreases, which is due to allocating less power to the information-carrying signal and more power to the artificial noise. In Fig. 7.9, we plot the secrecy outage probability of the artificial noise technique. We note that at low values of γ, the secrecy outage probability is zero, due to allocating more power to the artificial noise. In Fig. 7.10, we plot the energy coverage probability for the artificial noise technique. Agreeing with intuition, the energy coverage probability is constant for different values of γ, due to receiving the same overall power regardless how it is split between information carrying signal and artificial noise. In Fig. 7.11, we plot the successful connection probability for the guard zone technique for different values of the guard zone radius. We note that

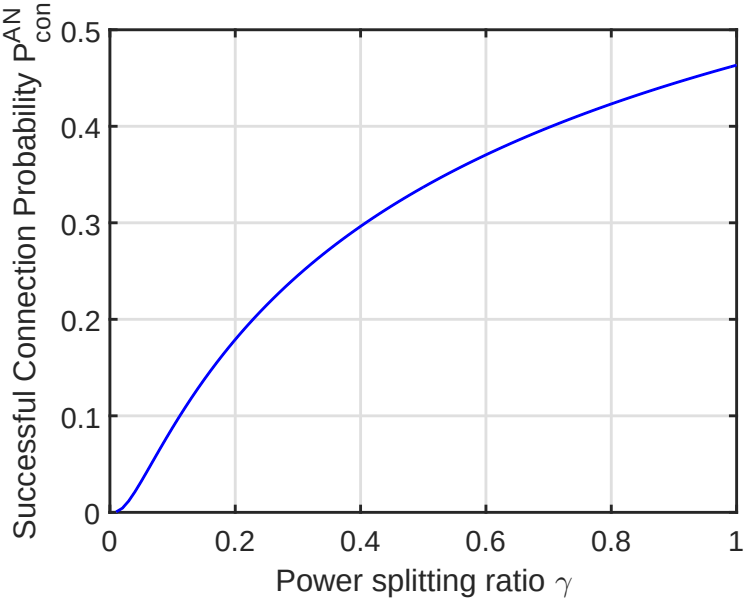

Figure 7.8: The successful connection probability of the artificial noise technique against different values of γ.

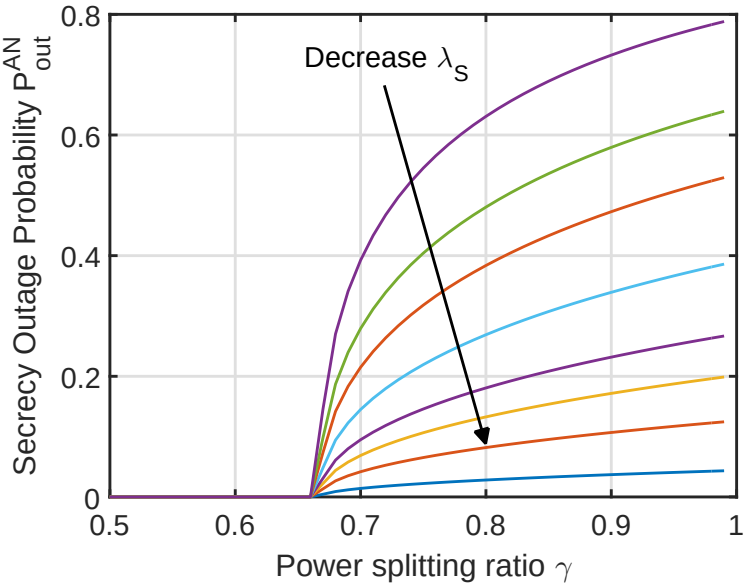

Figure 7.9: The secrecy outage probability of the artificial noise technique against different values of γ.

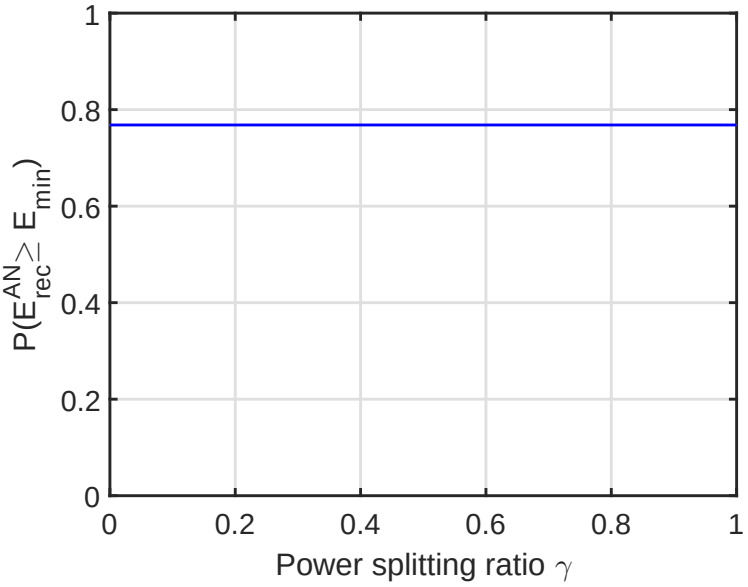

Figure 7.10: The energy coverage probability of the artificial noise technique against different values of γ.

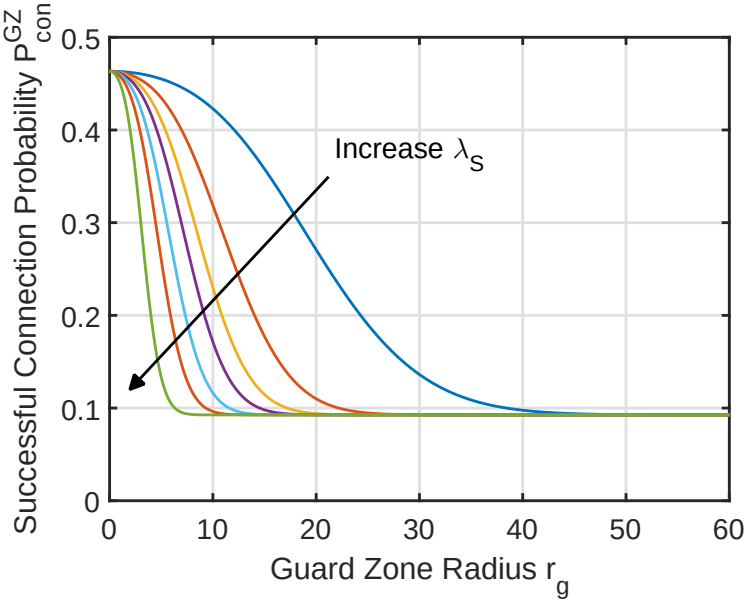

Figure 7.11: The successful connection probability of the guard zone technique against different values of the guard zone radius.

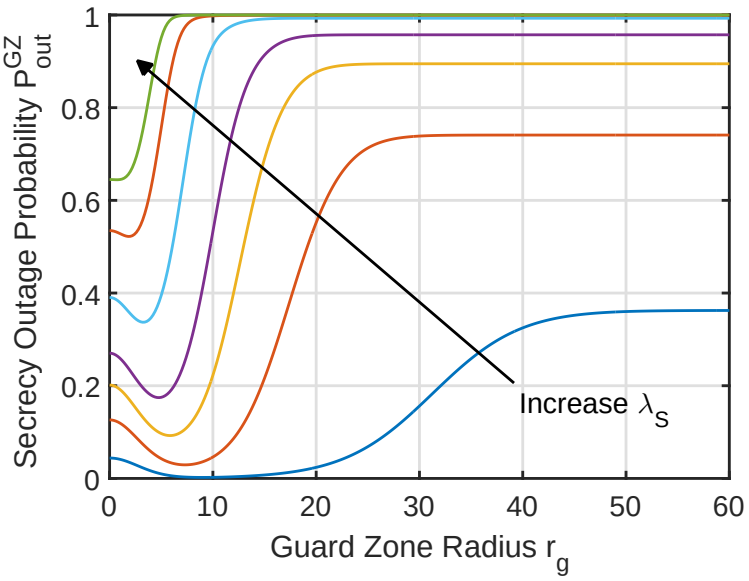

Figure 7.12: The secrecy outage probability of the guard zone technique against different values of the guard zone radius.

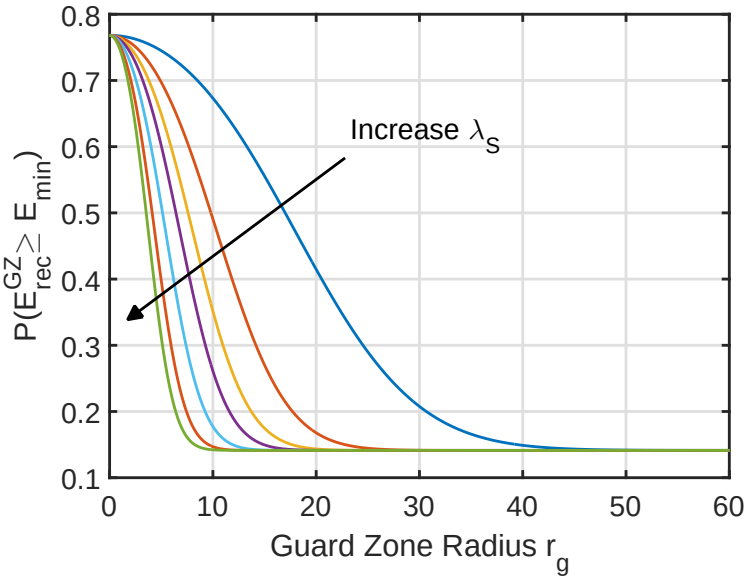

Figure 7.13: The energy coverage probability of the guard zone technique against different values of the guard zone radius.

as the value of the guard zone radius increases, the successful connection probability decreases, which is due to increasing the probability of finding an illegitimate receivers within the guard zone. At large values of the guard zone radius, the successful connection probability converges to a fixed value, because the guard zone is always unclear and the transmission probability is only function of q. In Fig. 7.12, we plot the secrecy outage probability of the guard zone technique. We note that the existence of an optimal value for the guard zone radius that minimizes the secrecy outage probability. Below this value, the radius is too small that the transmitter can be located too close to the illegitimate receiver. above this optimal value, the radius is too large that the density of inactive transmitters is large, which reduces the interference at the illegitimate receiver. In Fig. 7.13, we plot the energy coverage probability for the guard zone technique. Agreeing with intuition, increasing either the λ_S or the guard zone radius leads to decreasing the energy coverage probability, which is a result of increasing the density of inactive transmitters.

In Fig. 7.14, we plot the secrecy outage probabilities against different values of λ_S for each of AN, GZ, and BF techniques when Approach 1 is used. Consistent with intuition, we notice the decrease in the secrecy outage probability for the three techniques as λ_S increases. Furthermore, at lower values of λ_S, we note that the GZ technique is providing lowest secrecy outage probability. However, as λ_S increases, the AN technique becomes the optimal choice when Approach 1 is used.

In Fig. 7.15, we plot the successful connection probability against different values of λ_S for the three techniques when Approach 2 is used. At higher values of λ_S, both GZ and BF fail to meet the secrecy outage and energy coverage constraints. To capture this behavior in this result, we assign a zero value for P_{con}^{S}. The figure shows the optimality of the BF technique, with respect to Approach 2, at lower values of λ_S. However, as λ_S increases, the AN becomes the only choice due to the failure of BF and GZ to meet the secrecy outage and energy coverage constraints.

7.5 Summary

In this chapter, we studied a secure SWIPT system consisting of ITs, IRs, and ERs, where the ERs act as potential eavesdroppers. We considered three possible secrecy enhancing techniques to preserve information secrecy while ensuring wireless power transmission to the ERs: (i) artificial noise techique, (ii) guard zone technique, and (iii) beamforming technique. We characterized the performance of each of the three techniques by deriving generalized expressions for successful connection, secrecy outage, and energy coverage probabilities. A key outcome of this analysis is the superior performance of the AN technique, compared to the other two, at higher values of density of ERs in secure SWIPT systems. However, at lower values of ERs density, BF technique outperforms the others when priority is given to energy coverage and secrecy outage constraints, while GZ is the best when priority is given to energy coverage and successful connection constraints.

Till this point of the dissertation, we have focused on RF-powered IoT. In particular, we have studied the performance of such networks in terms of coverage and secrecy. Another type of en-

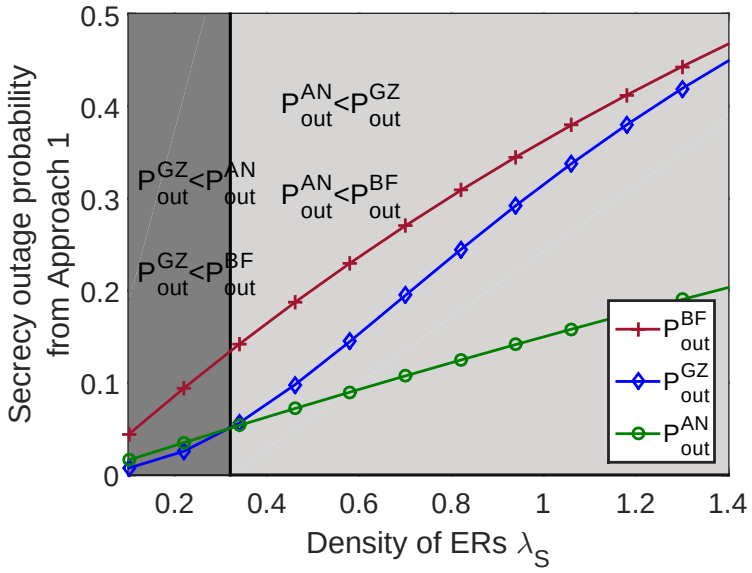

Figure 7.14: The secrecy outage probability resulting from Approach 1 for each of the three techniques against different values of λ_S.

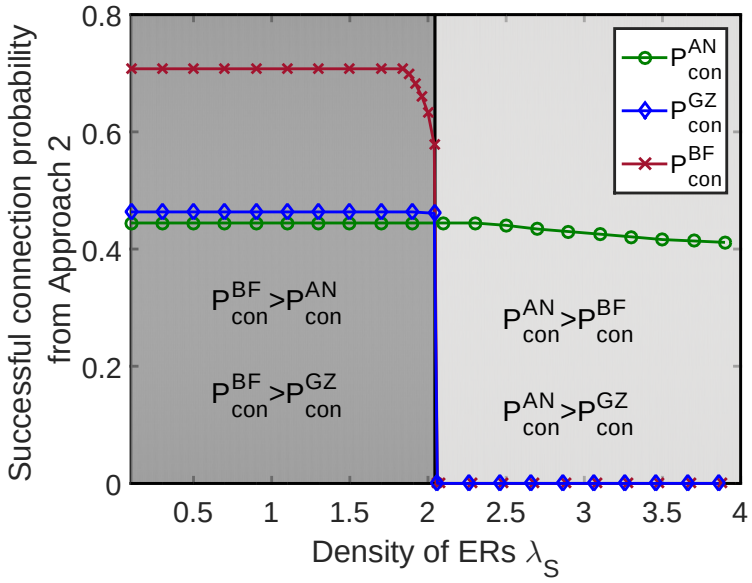

Figure 7.15: The successful connection probability resulting from Approach 2 for each of the three techniques against different values of λ_S.

ergy harvesting wireless networks that requires careful analysis is solar-powered cellular networks. While the nature of the problem might seem similar, which is using an unreliable resource of energy, the type of analysis and performance metrics are quite different. In particular, the focus in the analysis of RF-powered wireless networks is on ensuring that the IoT devices, are able to maintain their capability to operate and communicate with their associated access points. On the other hand, in solar-powered cellular networks, renewable energy is used as resource for a vital component of the network, which is the BSs. Maintaining a certain level of energy at the battery of the BS is critical to the operation of the whole network. Unlike an RF-powered IoT device, the failure of one BS, due to energy drainage, leads to the connection outage of many users falling in its vicinity. In the next chapter, we study the stability of solar-powered cellular networks using tools from percolation theory.

Chapter 8

Stability Analysis of Solar-powered Cellular Networks

In this chapter, we study the stability of cellular networks where the BSs are solely powered by solar energy. Due to the dependence on a random resource of energy, the BS might be energy-drained in some scenarios. This can result, for example, from being located in a shaded area where the intensity of solar energy is low, or from serving too many users which leads to consuming more energy than the amount harvested. To this end, our objective in this chapter is to study the effect of both the user density and the energy arrival rate on the population of energy-drained BSs. To achieve that, we use tools from percolation theory as well as Markov chain.

8.1 Introduction

Renewable energy have recently shown great potential to be used for powering cellular networks [57, 131, 132]. This gains special importance when the BSs are deployed at off-grid locations. In these locations, there are two options for powering BSs: (i) diesel generators and (ii) solar power. Continuous increase in the prices of Diesel, and the lower annual expenditure of solar panel (despite the high expenses of initial installations) have motivated many countries around the globe to consider deploying solar-powered BSs. In fact, a significant number of solar-powered BSs are already deployed and working in many locations in Asia and Africa [1]. However, they are mainly used to cover off-grid locations. In order to extend the deployment of solar-powered BSs to more countries and to cover even on-grid locations, careful performance analysis of solar-powered cellular networks needs to be provided first. One of the many aspects that need to be taken into consideration is the stability of such networks. The reliance on solar power solely as a resource of energy makes the BS vulnerable to the intensity of solar energy and to the overall energy consumption during operation. This, in turns, leads to the possibility of having *energy-drained* BSs. The BS can reach the energy-drained state due to lack of solar energy or due to consuming a lot of energy

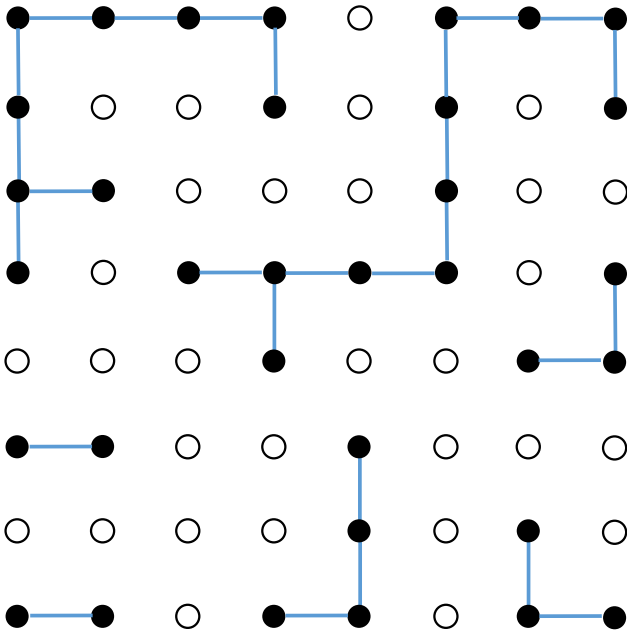

Figure 8.1: An Illustration of the percolation model. Filled circles represent open (retained) vertices, while shallow circles represent closed vertices. The lines connecting the vertices represent the retained edges.

while serving mobile users. Hence, the main two parameters that affect the performance of a solar-powered BS are: (i) the energy arrival rate, and (ii) the density of mobile users. In particular, this two parameters affect the probability of the BS being energy-drained, which in turns affects the probability of having a high population of energy-drained BSs, which could be interpreted as the probability of the network being *unstable*. As we discuss next, this problem can be easily mapped to standard constructs studied in the area of percolation theory. In particular, the idea of the *giant component* formation can be used to formally characterize network stability. In the next section, we provide some mathematical preliminaries on percolation theory.

8.2 Percolation Theory Preliminaries

Percolation theory is a useful mathematical tool that has been used for more than a decade now for analyzing connectivity in wireless networks [31]. While it was originally proposed to study porosity of materials, it has since then found applications in many different areas of research. The main importance of percolation models lies in exhibiting phase transition in the connectivity behavior [133–136]. The components of such models are either composed of finite disconnected structures, or form one *giant component* of finitely connected structure. In our application, the components represent sets of neighboring energy-drained BSs. Hence, the formation of a giant component can be connected with the notion of network stability in this setup.

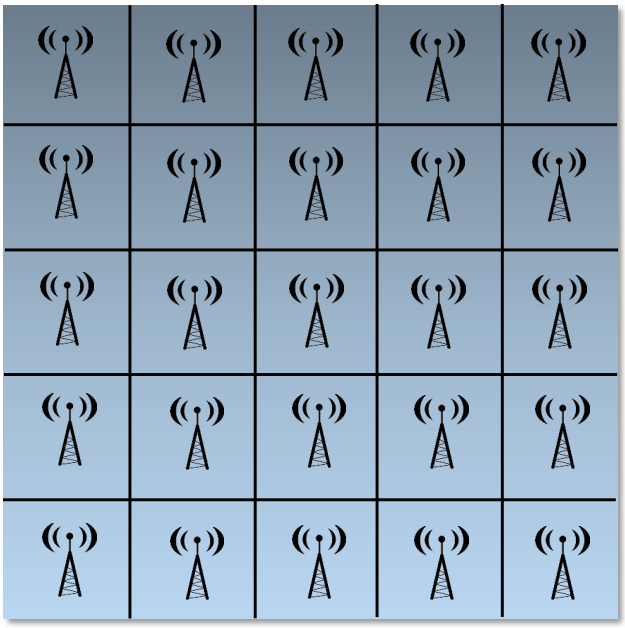

Figure 8.2: The locations of the BSs are modeled using a square grid model.

There are two main types of percolation setups considered in the literature: (i) bond percolation and (ii) site percolation. For understanding these, consider a square lattice on the 2-D plane. In bond percolation, each edge in this lattice is removed with probability $1-p$, or retained with probability p. In site percolation, a vertex is retained with probability p (along with its edges) and removed with probability $1-p$. In percolation theory, a retained vertex or edge is usually referred to as *open*, while a removed vertex or edge is referred to as *closed*. In Fig. 8.1, we show an example of a percolation model. A *component* is structure where if two vertices x and y belong to the component, then you can walk from x to y through only edges that belong to the component.

Now, let C represent the set of vertices in the component that contains the origin. The percolation probability is defined as

$$\theta(p) = \mathbb{P}(|C| = \infty), \tag{8.1}$$

where $|C|$ is the number of vertices in C. There exists a critical value p_c so that if $p \leq p_c$ then $\theta(p) = 0$ and if $p \geq p_c$ then $\theta(p) > 0$. It can be noticed how necessary it is to carefully derive the probability p in order to be able to apply percolation theory tools.

8.3 System Model and Performance Analysis

We consider a cellular network composed of solar-powered BSs that are located according to a square lattice on the 2-D plane, as shown in Fig. 8.2. Each BS has a battery of size $\beta_{\max}$. As shown

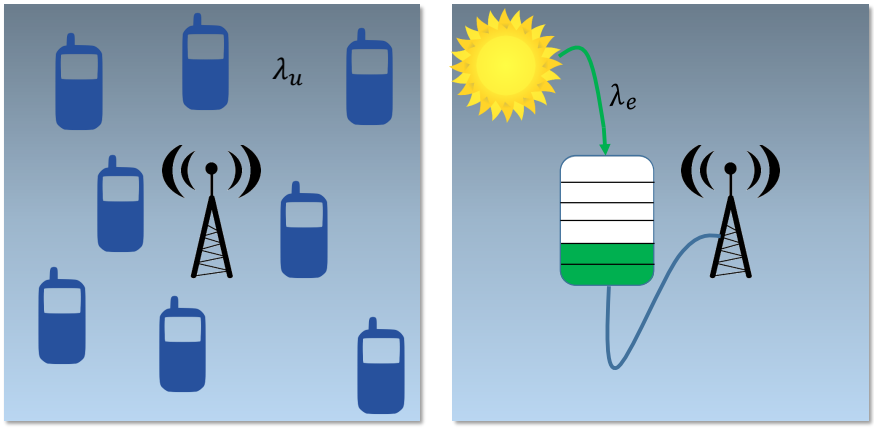

Figure 8.3: (a) The arrival rate of mobile users in each cell is λ_u, (b) the arrival rate of energy packets at the battery of each BS is λ_e.

in Fig. 8.3, the arrival rate of mobile users in each square cell is λ_u, while the energy arrival process at each BS is modeled as a Poisson process with arrival rate λ_e. Whenever a BS is energy-drained, each user inside its cell associates with the nearest BS among the eight BSs neighboring the energy-drained BS. If all of them are also energy-drained, then the user is in outage. It will have to wait until one of the 9 BSs harvests enough energy to be able to serve users again. Notice the correlation between the battery levels of each BS and its neighbors, as well as farther BSs. Capturing this correlation is quite challenging. For instance, if we ignore correlation with farther BSs and focus on the correlation with the eight neighboring BSs, we need to solve a 9-D Markov chain in order to find the steady state distribution of the battery levels. Recall that the main objective is to derive the probability of the BS being energy-drained, which represents the parameter p in the percolation model explained in the previous section. In addition, the percolation probability $\theta(p)$ in this system represents the probability of having a *giant component* of energy-drained BSs, which is equivalent to having an unstable network. To this end, we propose two simpler models that can be used to derive upper and lower bounds on p in the following subsections.

8.3.1 Lower Bound on p

In order to derive a lower bound on p, we consider relaxed version of the considered model where each BS only serves users located in its own cell. Hence, energy consumption is reduced due to serving less number of users. More specifically, if the serving BS of a given user is energy drained, that user will be simply considered in outage and hence dropped from the system. This approach enables us to decorrelate the battery level of the BS from the battery levels of its neighbors and analyze it independently using a 1-D Markov Chain. The probability of being energy drained in that case can be computed by deriving the stationary distribution of the birth-death process

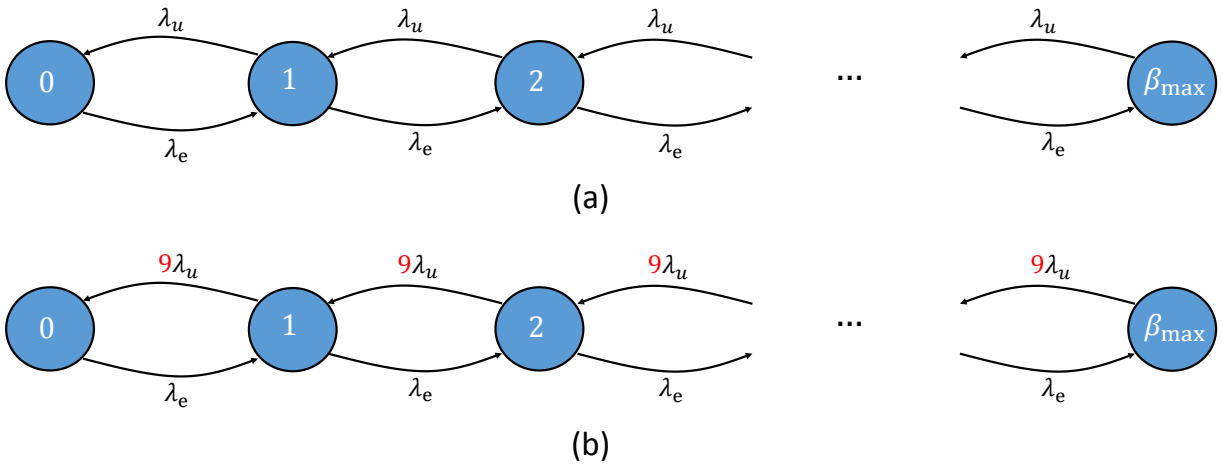

Figure 8.4: (a) represents the birth-death process used for computing the lower bound of p, while (b) represents the birth-death process used for computing the upper bound of p.

shown in the upper part of Fig. 8.4 with birth rate λ_e and death rate λ_u. Conditioned on having $\frac{\lambda_e}{\lambda_u}\frac{1-\left(\frac{\lambda_e}{\lambda_u}\right)^{\beta_{\max}}}{1-\frac{\lambda_e}{\lambda_u}} < \infty$, then

$$p^{\mathrm{LB}} = \frac{1-\frac{\lambda_e}{\lambda_u}}{1-\left(\frac{\lambda_e}{\lambda_u}\right)^{\beta_{\max}+1}} \tag{8.2}$$

Remark 20. *Note that the lower bound here is derived using the similar approach commonly used in literature, which ignores the correlation between the battery levels of neighboring BSs. According to the results in [137], the critical value of p in the site percolation model for the square lattice considered in this chapter is $p_c = 0.593$. This means that, for the case of infinite battery with each BS only serving users within its own cell, $p < p_c$ is ensured by maintaining $\frac{\lambda_e}{\lambda_u} > 1 - 0.593 = 0.407$.*

8.3.2 Upper Bound on p

In order to derive an upper bound on p, we consider a stricter version of the considered model where each BS serves all the users located in its own cell and the cells of the neighboring BSs. Hence, energy consumption is increased due to serving larger number of users. Similar to the approach used for computing the lower bound, this approach also enables us to decorrelate the battery level of the BS from those of its neighbors. The probability of being energy drained in that case can be derived by computing the stationary distribution of the birth-death process shown in

the lower part of Fig. 8.4. Conditioned on having $\frac{\lambda_e}{9\lambda_u}\frac{1-\left(\frac{\lambda_e}{9\lambda_u}\right)^{\beta_{\max}}}{1-\frac{\lambda_e}{9\lambda_u}} < \infty$, then

$$p^{\mathrm{UB}} = \frac{1-\frac{\lambda_e}{9\lambda_u}}{1-\left(\frac{\lambda_e}{9\lambda_u}\right)^{\beta_{\max}+1}} \tag{8.3}$$

Remark 21. *As stated earlier, according to [137], $p_c = 0.593$. In addition, according to Theorem 10.8 in [31], we know that if $p_1 < p_2$, then $\theta(p_1) \leq \theta(p_2)$. Hence, given that $p \leq p^{\mathrm{UB}}$, we can ensure that the percolation probability is zero by maintaining $p^{\mathrm{UB}} < p_c$. Hence, for the system considered in this chapter and described in Sec.* 8.3*, in case of infinite battery, we can ensure that the percolation probability is zero by maintaining the upper bound on p below the critical value $p_c = 0.593$, which leads to the condition $\frac{\lambda_e}{\lambda_u} > 9 \times 0.407 = 3.66$.*

8.4 Results and Discussion

We consider a simulation setup with the following parameters: $\beta_{\max} = 1$ and a square-shaped simulation area with increasing side length in order to improve accuracy. In Fig. 8.5, we plot the percolation probability for different values of $\frac{\lambda_e}{\lambda_u}$. We observe the existence of a critical value for $\frac{\lambda_e}{\lambda_u}$ above which the percolation probability of energy-drained BSs is zero. We also notice the tightness of the lower bound derived in the previous section.

8.5 Summary

In this chapter, we studied the stability of solar-powered cellular networks. We first introduced mathematical basics of percolation theory and some important definitions such as bond percolation and site percolation. Next, we used tools from percolation theory to study the probability of having a high population (giant component) of energy-drained BSs, which we refer to as the percolation probability and use it as an indicator of instability. The results showed the existence of critical value for the ratio $\frac{\lambda_e}{\lambda_u}$ above which the percolation probability goes to zero. In the next chapter, we study the correlation between neighboring BSs and its effect on the performance of the system.

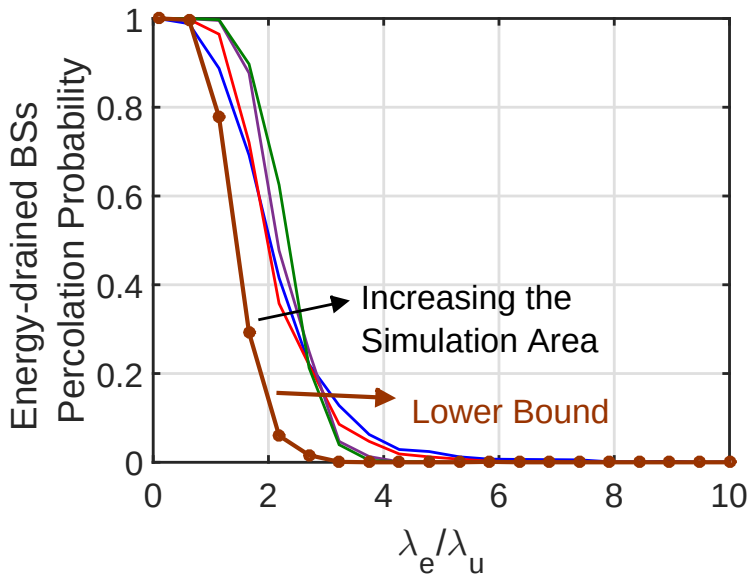

Figure 8.5: The probability of percolation of energy-drained BSs for different values of λ_e/λ_u.

Chapter 9

Coupling of Battery Levels in Energy Harvesting Wireless Networks

One of the major concerns that accompany the deployment of a cellular network where BSs are solely powered by solar energy is the energy outage. The usual approach to study that metric is to derive the steady state distribution of the battery levels of the BSs in the network. However, this is usually done with the assumption that these battery levels are independent, which is not quite accurate. This chapter studies the coupling between battery levels of the BSs in solar-powered cellular networks. This coupling arises as a result of serving the same set of users, even if the energy arrival process is independent at each BS. We study a system composed of two BSs. For this system, we show that the dynamics of the battery levels is analogous to that of a queuing system with two coupled processors. While the steady state analysis of the coupled processors system is a challenging problem, we use the analogy to define a system of equations that govern the steady state distribution of the battery levels for the two-BSs system. Next, we study the special case of unit-sized batteries. For that system, we show the existence of an optimal user-association policy that minimizes the outage probability.

9.1 Introduction

Motivated by the scarcity of energy resources in many geographical areas around the globe, the high energy consumption of cellular networks, and eco friendly wireless communication initiatives, renewable energy-powered wireless networks have gained great potential recently. In fact, many countries in Africa and Asia are already using solar-powered BSs to provide coverage for off-grid regions [1]. However, more developed countries like the USA and most of Europe are still less interested in deploying solar-powered BSs due to the abundance of on-grid energy everywhere. In order to make massive deployment of solar-powered BSs more appealing, reliability of such networks needs to be ensured through theoretical analysis and practical measurements. Many

works in the current literature provide concrete theoretical analysis of such networks, studying multiple aspects of the performance. One of these aspects, that we focus on in this chapter, is the dynamics of the battery level in the solar-powered BS. The usual approach is to use Markov chain-based analysis to derive the steady state distribution of the battery levels. However, in the existing literature, there is a common implicit assumption that the battery levels of neighboring BSs are independent. This is, in fact, not quite accurate. Imagine a user falling in the coverage area of a given BS x. If this BS becomes energy-drained, this user will associate with the nearest *active* BS y. Hence, the BS y will consume energy to serve a user falling in the cell of the BS x. Clearly, the battery level of y is correlated with that of x. Taking that issue into consideration while applying Markov chain-based analysis to derive the steady state distribution of the BSs is our main contribution in this chapter.

9.1.1 Related Work

As specified earlier, the subset of literature that is most relevant to the work in this chapter is the papers that rely on using Markov chain for analyzing the dynamics of the battery levels in systems of solar-powered BSs. In [138], authors study a heterogeneous cellular network that is composed of a Macro BS and a set of small-cell BS (SBS). The SBSs are categorized into three types: (i) solely powered by on-grid power, (ii) solely powered by energy harvesting, or (iii) jointly powered by energy harvesting and on-grid power. The authors model the variation of the battery level in energy harvesting SBS using birth-death Markov chain. The correlation with the battery levels at neighboring BSs is not taken into consideration. In [139], authors study the performance of downlink in heterogeneous cellular network composed of grid-powered BSs and energy harvesting access points. The access points form personal non-overlapping areas to serve only their priority users. Hence, there is no correlation between the battery levels of different access points. This enables using 1-D birth-death Markov chain to analyze accurately the dynamics of the battery level of the access points. Authors in [140] also study the deployment of small cell energy harvesting BSs. However, unlike [139], no personal area is assumed. In fact, they assume a cooperative strategy to offload user requests from one BS to another if it is energy-drained. However, 1-D birth-death Markov chain is used to model the dynamics of the battery level, without capturing the possible correlation with neighboring BSs.

9.1.2 Contributions

In this chapter we consider a system composed of 2 solar-powered BSs. For this system, we provide a Markov chain-based analysis to derive the steady state distribution of the battery levels of the BSs. Unlike existing work, our analysis captures the correlation between the battery levels of both BSs. For the case of finite-sized batteries, we show that this system is analogous to a queuing system with two coupled processors. We use this analogy to provide a system of equations that can be used to derive the steady state distribution. For the case of unit-sized batteries, we provide

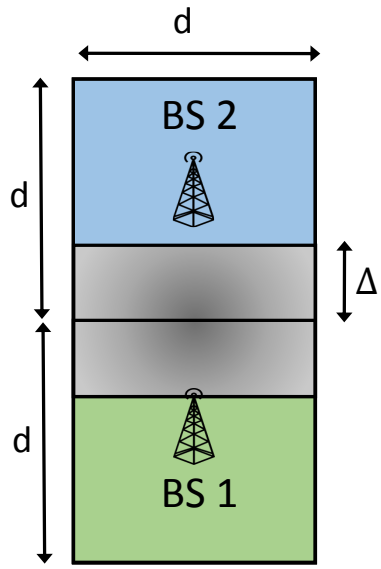

Figure 9.1: The 2-BSs model.

closed form expressions for the steady state distributions. Furthermore, we show the existence of an optimal user association policy that minimizes the outage probability.

9.2 System Model

We assume a system model composed of 2 BSs, each with a square shaped cell with side length d. Each BS has a battery of size N. The energy arrival is modeled by a Poisson process with rate λ. The users are uniformly distributed in the considered area. Each user is assumed to associate with its nearest BS. However, some users associate with the other BS if the nearest BS is energy-drained. Users belonging to the cell of an energy-drained BS associate with the other BS, if it is active, only if the users fall in a specific area of the cell. This area is modeled by a $\Delta \times d$ rectangle as shown in Fig. 9.1. The arrival rate of the user association requests in each cell is μ.

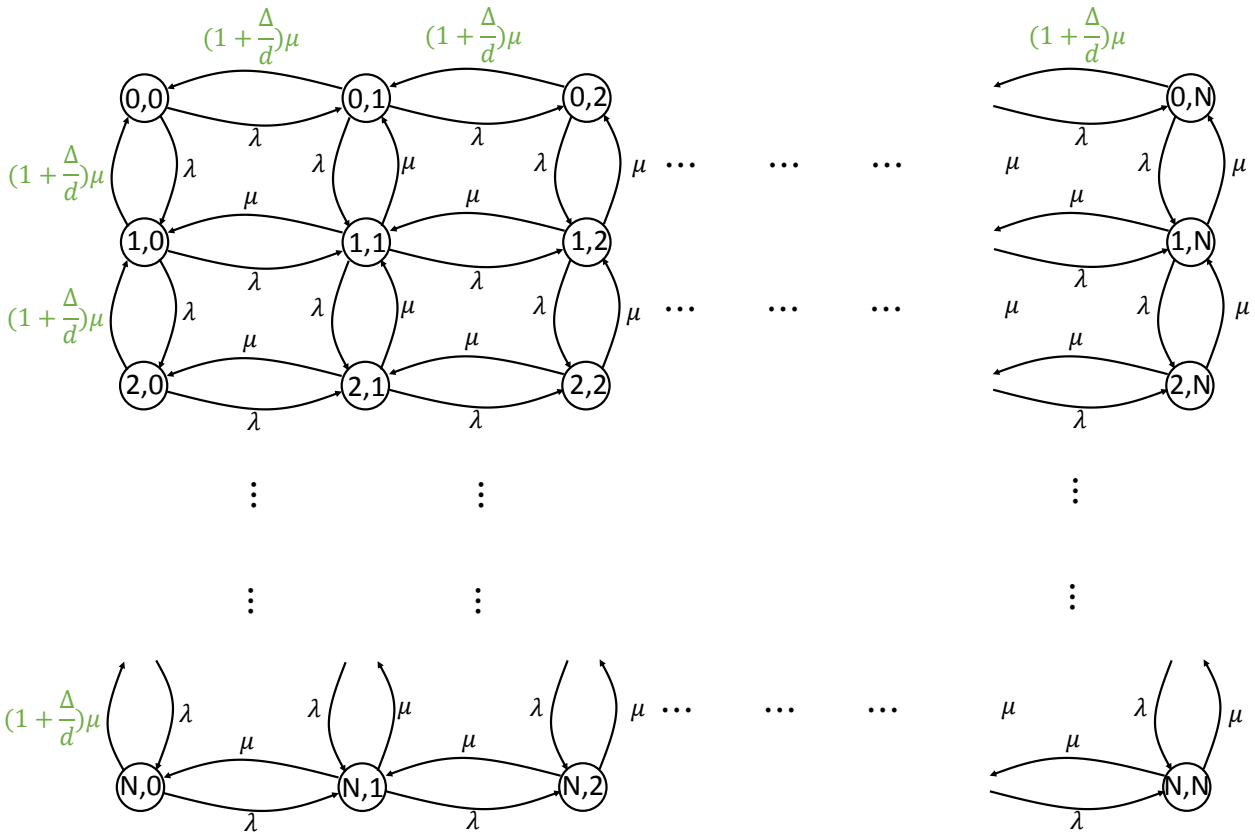

Figure 9.2: The 2-dimensional Markov chain for the case of finite-sized battery.

9.3 Performance Analysis

9.3.1 Finite-sized Battery

The battery dynamics in the case of having a battery of size N can be modeled using a 2-D Markov chain as show in Fig. 9.2. This system is equivalent to a queuing system with coupled processor. In that system, the arrival is modeled as a Poisson process with rate λ_1 for queue 1 and λ_2 for queue 2. The service rate for each queue S_1 and S_2 is represented as follows:

- If both queues are busy: $S_1 = \mu_1,\ S_2 = \mu_2$.
- If queue 1 is empty: $S_2 = \mu_2^*$.
- If queue 2 is empty: $S_1 = \mu_1^*$.

Observing the analogy with our system, an empty queue represents an empty battery, arrival rate represents the energy arrival rate, and service rate represents user arrival rate. Hence, we can model

our system as follows

- $\lambda_1 = \lambda_2 = \lambda$.
- $\mu_1 = \mu_2 = \mu$.
- $\mu_1^* = \mu_2^* = \left(1 + \frac{\Delta}{d}\right)\mu$.

The Kolmogeroff forward equations equations for that system and computationally-reasonable solutions are provided in [141]. We only provide the forward equations here for simplicity while incorporating the analysis in [141] into our system is left for future work. The forward equations are given as follows

$$
\begin{aligned}
(2\lambda + 2\mu)P_{m,n} &= \lambda(P_{m-1,n} + P_{m,n-1}) + \mu(P_{m+1,n} + P_{m,n+1}), \quad 0 < m, n < N, \\
(\lambda + 2\mu)P_{m,N} &= \lambda(P_{m-1,N} + P_{m,N-1}) + \mu P_{m+1,N}, \ \ 0 < m < N, \\
(\lambda + 2\mu)P_{N,n} &= \lambda(P_{N-1,n} + P_{N,n-1}) + \mu P_{N,n+1}, \quad 0 < n < N, \\
\left(2\lambda + \left(1 + \frac{\Delta}{d}\right)\mu\right) P_{m,0} &= \lambda P_{m-1,0} + \left(1 + \frac{\Delta}{d}\right)\mu P_{m+1,0} + \mu P_{m,1}, \ \ 0 < m < N, \\
\left(2\lambda + \left(1 + \frac{\Delta}{d}\right)\mu\right) P_{0,n} &= \lambda P_{0,n-1} + \left(1 + \frac{\Delta}{d}\right)\mu P_{0,n+1} + \mu P_{1,n}, \quad 0 < n < N, \\
2\mu P_{N,N} &= \lambda(P_{N-1,N} + P_{N,N-1}), \\
\left(\lambda + \left(1 + \frac{\Delta}{d}\right)\mu\right) P_{N,0} &= \lambda P_{N-1,0} + \mu P_{N,1}, \\
\left(\lambda + \left(1 + \frac{\Delta}{d}\right)\mu\right) P_{0,N} &= \lambda P_{0,N-1} + \mu P_{1,N}, \\
2\lambda P_{0,0} &= \left(1 + \frac{\Delta}{d}\right)\mu(P_{0,1} + P_{1,0}).
\end{aligned} \tag{9.1}
$$

9.3.2 Unit Sized battery

The 2-dimensional Markov chain representing the different states of the battery levels is shown in Fig. 9.3. The balance equations for the Markov chain are provided below.

$$
\begin{aligned}
P_{0,0} \times (2\lambda) &= \mu\left(1 + \frac{\Delta}{d}\right)(P_{0,1} + P_{1,0}), \\
P_{0,1} \times \left(\lambda + \mu\left(1 + \frac{\Delta}{d}\right)\right) &= \mu P_{1,1} + \lambda P_{0,0}, \\
2\mu P_{1,1} &= \lambda(P_{0,1} + P_{1,0}), \\
P_{0,0} + P_{0,1} + P_{1,0} + P_{1,1} &= 1.
\end{aligned} \tag{9.2}
$$

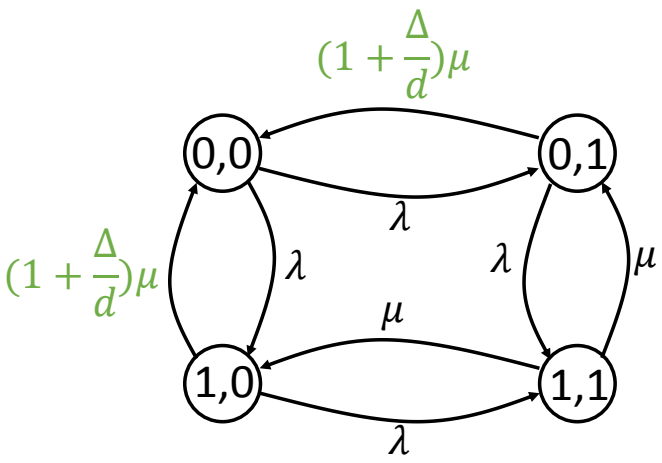

Figure 9.3: The 2-dimensional Markov chain for the case of unit-sized battery.

Using the above equations, the steady state values of the distributions of the battery levels can be computed.

$$\begin{aligned}
P_{0,0} &= \frac{\mu^2\left(1+\frac{\Delta}{d}\right)}{\lambda^2+2\lambda\mu+\ u^2\left(1+\frac{\Delta}{d}\right)},\\
P_{0,1} &= \frac{\lambda\mu}{\lambda^2+2\lambda\mu+\ u^2\left(1+\frac{\Delta}{d}\right)},\\
P_{1,0} &= \frac{\lambda\mu}{\lambda^2+2\lambda\mu+\ u^2\left(1+\frac{\Delta}{d}\right)},\\
P_{1,1} &= \frac{\lambda^2}{\lambda^2+2\lambda\mu+\ u^2\left(1+\frac{\Delta}{d}\right)}.
\end{aligned} \tag{9.3}$$

Next, the outage probability is computed as follows:

$$P_{\text{outage}} = P_{0,0} + \mathbb{P}\left(\text{SNR}^{\text{in cell}} \leq \beta\right)\left(P_{1,0}+P_{1,1}\right) + P_{0,1}\left(\frac{\Delta}{d}\mathbb{P}\left(\text{SNR}^{\text{out cell}} \leq \beta\right) + \frac{d-\Delta}{d}\right), \tag{9.4}$$

where $\mathbb{P}\left(\text{SNR}^{\text{in cell}} \leq \beta\right)$ is the SNR outage probability when a user is associated with the BS in its own cell, while $\mathbb{P}\left(\text{SNR}^{\text{out cell}} \leq \beta\right)$ is the outage probability when a user is associated with the BS in the other cell. The value β is the minimum threshold on the SNR value to ensure coverage. The results for this system show the existence of an optimal value of Δ that minimizes the outage probability P_{outage}, as shown in Fig. 9.4.

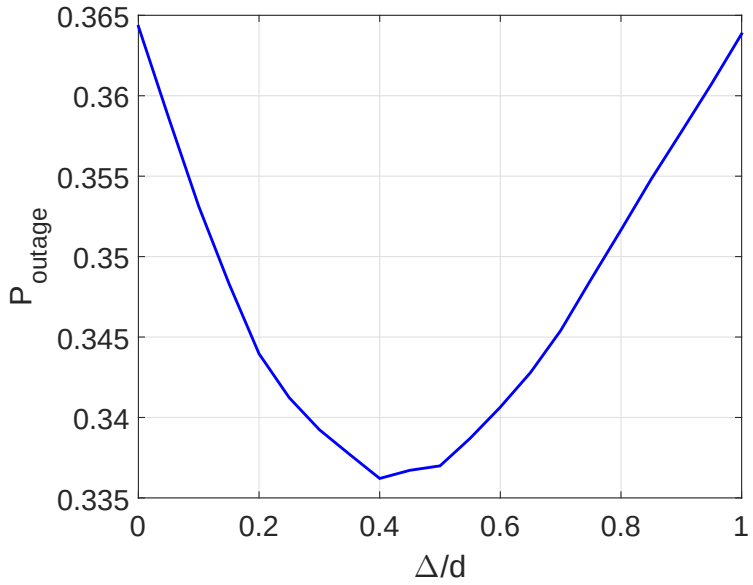

Figure 9.4: The outage probability for the 2-BS model against different values of Δ.

9.4 Summary

In this chapter, we studied the correlation between the battery levels of neighboring solar-powered BSs. Using Markov chain-based analysis, we showed that users should not always associate with the nearest active BS. In terms of outage probability, we showed that only if the distance is below a specific threshold, association is encouraged, above that threshold, the outage probability increases due to associating with too far BSs. Note that outage probability in that case is defined by the joint probability of SINR outage and energy outage.

Chapter 10

Conclusion

In this dissertation, two types of energy harvesting wireless networks were studied: (i) RF-powered IoT and (ii) solar-powered cellular networks. For (i), we studied the coverage probability and throughput of RF-powered IoT networks. In addition, we studied the secrecy of RF signals harvested by RF-powered IoT devices in SWIPT systems. For (ii), we studied the stability of solar-powered cellular networks in a square lattice modeled network. Furthermore, we studied the correlation between the battery levels of neighboring BSs in such networks. More details are provided next.

In Chapter 3, we provided a novel framework for studying the joint probability of uplink and downlink coverage in RF-powered cellular-based IoT networks. We considered a system where each time slot is divided into three sub-slots: (i) charging sub-slot, (ii) downlink transmission sub-slot, and (iii) uplink transmission sub-slot. Modeling the locations of the BSs using PPP, we used tools from stochastic geometry to derive the joint distribution of the amount of harvested energy, downlink SINR and the uplink SINR. Furthermore, we showed the existence of an optimal duration for the charging sub-slot that maximizes the throughput of the network. In addition, we derived a tuning parameter that can be used to determine how close is the performance of the RF-powered IoT to the performance of a regularly-powered IoT, in terms of coverage and throughput.

In Chapter 5, we studied the secrecy of RF signals transmitted by sources of RF energy when RF-powered energy receivers, which act as potential eavesdroppers, exist in the network. We first performed a comparison of possible options for secrecy enhancing techniques (specifically, artificial noise and guard zone techniques) in Chapter 4. We derived a mathematical expression that can be used to determine which technique outperforms the other depending on the parameters of the system setup, such as the distance between the legitimate transmitter and the legitimate receiver. Back to Chapter 5, we considered a system composed of two coexisting networks: (i) the primary network, which is composed of primary transmitters and primary receivers and using the guard zone technique to enhance secrecy, and (ii) the secondary network, which is composed of the energy receivers that harvest RF energy from the signals transmitted by the primary transmitters. We first used tools from stochastic geometry to derive the performance metrics of each of the

two networks. Next, we used tools from game theory to model the interaction between the two networks. One of the most interesting drawn insights from our analysis is the existence of an optimal deployment density of energy receivers, that maximizes the density of successfully powered devices.

During the analysis performed in Chapter 5, we used Poisson hole process (PHP) to model the locations of active primary transmitters when the guard zone technique is adopted. In Chapter 6, we derive lower and upper bounds for the contact distance distribution in PHP networks.

In Chapter 7, we extend out work in Chapter 5 to consider more secrecy enhancing techniques. In particular, we compared the performance of the same system explained in Chapter 5 for 3 different secrecy enhancing techniques: (i) beamforming, (ii) artificial noise addition, and (iii) guard zone technique. In addition, different from Chapter 5, we assumed that the primary transmitter's objective is both to ensure secrecy of transmitted signal and ensure transmission of wireless power to the energy receiver. We provide a general framework that leads to generic expressions that can be used to compute the performance metrics of any of the three techniques. We considered two parameter selection approaches: (i) maximize successful connection probability for given constraints on secrecy and wireless power transmission, and (ii) minimize secrecy outage probability for given constraints on successful connection and wireless power transmission. For the first approach, our results show that the beamforming technique outperforms the other two techniques at low densities of energy receivers. For the second approach, the guard zone technique outperforms the other two techniques at low densities of energy receiver. For both approaches, artificial noise technique is optimal at higher values of the density of the energy receivers. In addition, we provided some system-level insights for the performance of each of the three techniques. For instance, we showed the existence of an optimal beamwidth for the beamforming technique, which minimizes the secrecy outage probability. Similarly, we showed the existence of an optimal value for the radius of the guard zone that minimizes the secrecy outage probability.

In Chapter 8, we studied the stability of solar-powered cellular networks. We considered a square lattice model for the locations of the BSs and assumed an energy arrival rate of λ_e and user arrival rate of λ_u at each cell. For that setup, we applied tools from Markov chain to derive lower and upper bounds on the probability of the BS being energy-drained. Next, we used tools from percolation theory to study the probability of having a *giant component* of energy-drained BSs. We showed the existence of a critical value for the ration $\frac{\lambda_e}{\lambda_u}$. Above this value, the probability of having a giant component of energy-drained BSs is zero. During the work in this Chapter, we noticed the complexity of deriving the accurate probability of the BS being energy-drained. This complexity results from the correlation between the battery levels of each BS and its neighbors, which made us focus on computing upper and lower bounds. In Chapter 9, we studied the correlation between the battery levels of neighboring BSs in a system composed of 2 BSs. We use Markov chain-based analysis to study the steady state distribution of the battery levels. The main insight drawn from the analysis in this chapter is the existence of an optimal area in each cell where users can associate with the other BS if their own BS is energy-drained. This optimal area minimizes the outage probability.

Appendices

Appendix A

Appendices for Chapter 3

A.1 Proof of Lemma 1

The value of $\Psi(r_2)$ can be derived as follows:

$$\Psi(r_2) = \mathbb{E}\left[\sum_{x\in\Phi_b\setminus x_1,x_2} g_x\|x\|^{-\alpha}\Big|x_1,x_2\right]$$
$$\overset{(a)}{=} \mathbb{E}\left[\sum_{x_i\in\Phi_b\setminus x_1,x_2} \|x_i\|^{-\alpha}\right] \overset{(b)}{=} 2\pi\lambda_b\int_{r_2}^{\infty}\frac{1}{r^{\alpha}}r\mathrm{d}r = \frac{2\pi\lambda_b}{\alpha-2}({r_2}^{2-\alpha}), \tag{A.1}$$

where (a) follows from the assumption that all $\{g_x\}$ are independent and exponentially distributed random variables with mean one, and (b) follows from Campbell's theorem [31] with conversion from Cartesian to polar coordinates and using $r_2 = \|x_2\|$. Using the approximation introduced in (3.9), the conditional energy coverage probability can be expressed as:

$$\mathbb{P}\left(E_{\mathrm{H}} \geq E_{\min}\Big|\Phi_b\right) = \mathbb{P}\left(\tau_1 T\eta P_{\mathrm{t}}\left(g_{x_1}r_1^{-\alpha} + g_{x_2}r_2^{-\alpha} + \frac{2\pi\lambda_b}{\alpha-2}r_2^{2-\alpha}\right) \geq E_{\mathrm{rec}} + \tau_3 T\rho r_1^{\epsilon\alpha}\right)$$
$$= \mathbb{P}\left(g_{x_1}r_1^{-\alpha} + g_{x_2}r_2^{-\alpha} \geq C(\tau_1) + \frac{\tau_3\rho r_1^{\epsilon\alpha}}{\tau_1\eta P_{\mathrm{t}}} - \frac{2\pi\lambda_b}{\alpha-2}r_1^{2-\alpha}\right) = \mathbb{P}\left(g_{x_1}r_1^{-\alpha} + g_{x_2}r_2^{-\alpha} \geq \mathcal{F}(r_1,r_2)\right)$$
$$\overset{(c)}{=} \frac{r_2^{\alpha}\exp(-r_1^{\alpha}[\mathcal{F}(r_1,r_2)]^{+}) - r_1^{\alpha}\exp(-r_2^{\alpha}[\mathcal{F}(r_1,r_2)]^{+})}{r_2^{\alpha}-r_1^{\alpha}}, \tag{A.2}$$

where step (c) is due to hypo-exponential distribution of $g_{x_1}r_1^{-\alpha} + g_{x_2}r_2^{-\alpha}$ (sum of two exponential random variables with rates r_1^{α} and r_2^{α}), $C(\tau_1) = \frac{E_{\mathrm{rec}}}{\tau_1 T\eta P_{\mathrm{t}}}$, and $[x]^{+} = \max\{0,x\}$. This concludes the proof of (D.3). Noting that $\mathbb{P}\left(E_{\mathrm{H}} \geq E_{\min}\Big|\Phi_b\right) = 1$ when $\mathcal{F}(r_1,r_2) \leq 0$ and integrating over r_1 and r_2 with $f_{R_1,R_2}(r_1,r_2) = (2\pi\lambda_b)^2 r_1 r_2 e^{-\lambda_b\pi {r_2}^2}$ [79], the result in (3.11) follows.

A.2 Proof of Lemma 2 and Lemma 3

Using the definition of $\mathrm{SINR}_{\mathrm{DL}}$ in (3.2) and approximating the interference I_1 by the sum of interference from the nearest interferer and the expectation of the interference from the rest of the interference field, we get

$$\begin{aligned}
\mathbb{P}(\mathrm{SINR}_{\mathrm{DL}} \geq \beta_{\mathrm{DL}} | r_1, r_2) &= \mathbb{P}\left(\frac{P_{\mathrm{t}} h_{x_1} \|x_1\|^{-\alpha}}{I_1 + \sigma^2_{\mathrm{DL}}} \geq \beta_{\mathrm{DL}} \Big| r_1, r_2 \right) \\
&= \mathbb{P}\left(\frac{P_{\mathrm{t}} h_{x_1} r_1^{-\alpha}}{P_{\mathrm{t}} h_{x_2} r_2^{-\alpha} + P_{\mathrm{t}} \Psi(r_2) + \sigma^2_{\mathrm{DL}}} \geq \beta_{\mathrm{DL}} \Big| r_1, r_2 \right) \\
&\overset{(d)}{=} \mathbb{P}\left(\frac{P_{\mathrm{t}} h_{x_1} r_1^{-\alpha}}{P_{\mathrm{t}} h_{x_2} r_2^{-\alpha} + P_{\mathrm{t}} \frac{2\pi\lambda_b r_2^{2-\alpha}}{\alpha-2} + \sigma^2_{\mathrm{DL}}} \geq \beta_{\mathrm{DL}} \Big| r_1, r_2 \right) \\
&= \mathbb{P}\left(h_{x_1} r_1^{-\alpha} \geq \frac{\beta_{\mathrm{DL}} \sigma^2_{\mathrm{DL}}}{P_{\mathrm{t}}} + \frac{2\pi\lambda_b \beta_{\mathrm{DL}} r_2^{2-\alpha}}{\alpha-2} + \beta_{\mathrm{DL}} h_{x_2} r_2^{-\alpha} \right) \\
&\overset{(e)}{=} \mathbb{E}_{h_{x_2}}\left[\exp\left(-r_1^{\alpha} \left(\frac{\beta_{\mathrm{DL}} \sigma^2_{\mathrm{DL}}}{P_{\mathrm{t}}} + \frac{2\pi\lambda_b \beta_{\mathrm{DL}} r_2^{2-\alpha}}{\alpha-2} + \beta_{\mathrm{DL}} h_{x_2} r_2^{-\alpha} \right) \right) \right] \\
&\overset{(f)}{=} \exp(-\mathcal{G}(r_1, r_2)) \frac{1}{1 + \beta_{\mathrm{DL}} \frac{r_1^{\alpha}}{r_2^{\alpha}}},
\end{aligned} \tag{A.3}$$

where (d) follows from substituting for $\Psi(r_2)$ as derived in (A.1), and steps (e) and (f) follow from the assumption that $h_x \sim \exp(1)$, and defining $\mathcal{G}(r_1, r_2) = \frac{\beta_{\mathrm{DL}} \sigma^2_{\mathrm{DL}} r_1^{\alpha}}{P_{\mathrm{t}}} + \frac{2\pi\lambda_b \beta_{\mathrm{DL}} r_2^{2-\alpha} r_1^{\alpha}}{\alpha-2}$.

In the uplink sub-slot, the locations of *active* IoT devices (IoT devices in energy coverage) in a given time-frequency resource can be approximately modeled by the PPP $\tilde{\Phi}_u$ with density $\tilde{\lambda}_u = P_h \times \lambda_b$ where $P_h = \mathbb{P}(E_{\mathrm{H}} \geq E_{\min})$. This will lead to the following expression for $\mathrm{SINR}_{\mathrm{UL}}$:

$$\mathrm{SINR}_{\mathrm{UL}} = \frac{w_o \|x_1\|^{(\epsilon-1)\alpha}}{\sum\limits_{u_i \in \tilde{\Phi}_u \setminus u_o} w_i \left(R_1^{(i)} \right)^{\epsilon\alpha} D_i^{-\alpha} + \frac{\sigma^2_{\mathrm{UL}}}{\rho}}. \tag{A.4}$$

Defining $\tilde{I}_2 = \sum\limits_{u_i \in \tilde{\Phi}_u \setminus u_o} w_i \left(R_1^{(i)} \right)^{\epsilon\alpha} D_i^{-\alpha}$, we have:

$$\begin{aligned}
\mathbb{P}\left(\mathrm{SINR}_{\mathrm{UL}} \geq \beta_{\mathrm{UL}} \Big| r_1 \right) &= \mathbb{P}\left(\frac{w_0 {r_1}^{(\epsilon-1)\alpha}}{\tilde{I}_2 + \frac{\sigma^2_{\mathrm{UL}}}{\rho}} \geq \beta_{\mathrm{UL}} \Big| r_1 \right) = \mathbb{E}_{\tilde{I}_2}\left[\mathbb{P}\left(w_0 \geq \frac{(\tilde{I}_2 + \frac{\sigma^2_{\mathrm{UL}}}{\rho}) \beta_{\mathrm{UL}}}{{r_1}^{(\epsilon-1)\alpha}} \Big| r_1, \tilde{I}_2 \right) \right] \\
&\overset{(g)}{=} \mathbb{E}_{\tilde{I}_2}\left[\exp\left(-\frac{(\tilde{I}_2 + \frac{\sigma^2_{\mathrm{UL}}}{\rho}) \beta_{\mathrm{UL}}}{{r_1}^{(\epsilon-1)\alpha}} \right) \right] \overset{(h)}{=} e^{\left(-\frac{\beta_{\mathrm{UL}} \sigma^2_{\mathrm{UL}}}{\rho {r_1}^{(\epsilon-1)\alpha}} \right)} \mathcal{L}_{\tilde{I}_2}\left(\frac{\beta_{\mathrm{UL}}}{{r_1}^{(\epsilon-1)\alpha}} \right),
\end{aligned} \tag{A.5}$$

where step (g) is due to the assumption that w_0 is exponentially distributed with mean one, and step (h) results from using the Laplace transform of $\tilde{I}_2$, which can be found by replacing λ_b with $\tilde{\lambda}_b = P_h \lambda_b$ in (3.13), where $P_h = \mathbb{P}(E_{\mathrm{H}} \geq E_{\min})$.

A.3 Proof of Lemma 4 and Theorem 2

We apply the substitutions in Remark 1 for the downlink case to both Lemma 1 and Theorem 1 to get both energy coverage probability and $P_{\text{cov}}^{\text{DL}}$. Applying these substitutions reduces the value of $\mathcal{F}(r_1, r_2)$ to $\mathcal{F}_{\text{DL}}(r_1, r_2) = C(\tau_1) - \frac{2\pi\lambda_b r_2^{2-\alpha}}{\alpha-2}$, where $C(\tau_1)$ is as defined in Lemma 1. Letting $\mathcal{A} = \left(\frac{2\pi\lambda_b}{(\alpha-2)C(\tau_1)}\right)^{\frac{1}{\alpha-2}}$, we note that the set $\mathcal{N}_{r_2}$ will be empty set for $r_2 \geq \mathcal{A}$ while for $r_2 \leq \mathcal{A}$ the set will be simply $\mathcal{N}_{r_2} = \{r_1 : r_1 \leq r_2\}$. Similarly, the set $\mathcal{P}_{r_2}$ will be empty set for $r_2 \leq \mathcal{A}$ while for $r_2 \geq \mathcal{A}$ the set will reduce to $\mathcal{P}_{r_2} = \{r_1 : r_1 \leq r_2\}$. Applying these integration limits on our result in Lemma 1 leads to the final result in Lemma 4. Similarly, applying these new integration limits to the result in Theorem 1 and noting that the substitutions explained in Remark 1 include $\beta_{\text{UL}} = 0$ (which leads to $\mathcal{L}_{\tilde{I}_2}(0) = 1$ in (3.16)), the final result in Theorem 2 follows.

A.4 Proof of Lemma 5 and Theorem 3

Similar to the approach in the downlink case, we apply the substitutions in Remark 1 for the uplink case to both Lemma 1 and Theorem 1. Applying these substitutions reduces the value of $\mathcal{F}(r_1, r_2)$ to $\mathcal{F}_{\text{UL}}(r_1, r_2) = \tilde{C}(\tau_1) r_1^{\epsilon\alpha} - \frac{2\pi\lambda_b r_2^{2-\alpha}}{\alpha-2}$, where $\tilde{C}(\tau_1) = \frac{\tau_3\rho}{\tau_1\eta P_t}$. Letting $\tilde{\mathcal{A}} = \left(\frac{2\pi\lambda_b}{\tilde{C}(\tau_1)(\alpha-2)}\right)^{\frac{1}{(\epsilon+1)\alpha-2}}$, we note that the set $\mathcal{N}_{r_2} = \{r_1 : r_1 < \left(\frac{2\pi\lambda_b}{\tilde{C}(\tau_1)(\alpha-2)}\right)^{\frac{1}{\epsilon\alpha}} r_2^{\frac{2-\alpha}{\epsilon\alpha}}\}$ for $r_2 \geq \tilde{\mathcal{A}}$ while for $r_2 \leq \tilde{\mathcal{A}}$ the set will be simply $\mathcal{N}_{r_2} = \{r_1 : r_1 \leq r_2\}$. Similarly, the set $\mathcal{P}_{r_2}$ will be empty set for $r_2 \leq \tilde{\mathcal{A}}$ while for $r_2 \geq \tilde{\mathcal{A}}$ the set will reduce to $\mathcal{P}_{r_2} = \{r_1 : \left(\frac{2\pi\lambda_b}{\tilde{C}(\tau_1)(\alpha-2)}\right)^{\frac{1}{\epsilon\alpha}} r_2^{\frac{2-\alpha}{\epsilon\alpha}} \leq r_1 \leq r_2\}$. Applying these integration limits on our result in Lemma 1 leads to the final result in Lemma 5. Similarly, applying these new integration limits to the result in Theorem 1 and noting that the substitutions explained in Remark 1 include $\beta_{\text{DL}} = 0$ (which makes $\mathcal{G}(r_1, r_2) = 0$ in (3.16)), the final result in Theorem 3 follows.

Appendix B

Appendices for Chapter 4

B.1 Proof of Lemma 6

By definition, the secure communication probability is

$$\begin{aligned} P_{\text{sec}}^{GZ} &= \mathbb{P}\left(\frac{P_t}{\sigma_S^2}\max_{y\in\Phi_e\cap\mathcal{B}(0,r_g)^c}\{g_y\|y\|^{-\alpha}\}\leq\beta_e\right) \\ &\overset{(a)}{=} \mathbb{E}_{\Phi_e}\left[\prod_{y\in\Phi_e\cap\mathcal{B}(0,r_g)^c}\mathbb{P}\left(g_y\leq\|y\|^{\alpha}\beta_e\frac{\sigma_S^2}{P_t}\Big|\Phi_e\right)\right] \\ &\overset{(b)}{=} \mathbb{E}_{\Phi_e}\left[\prod_{y\in\Phi_e\cap\mathcal{B}(0,r_g)^c}\left(1-e^{-\|y\|^{\alpha}\beta_e\frac{\sigma_S^2}{P_t}}\right)\right] \\ &\overset{(c)}{=} \exp\left(-2\pi\lambda_e\int_{r_g}^{\infty}e^{-r_y^{\alpha}\beta_e\frac{\sigma_S^2}{P_t}}r_y\mathrm{d}r_y\right), \end{aligned} \tag{B.1}$$

where $\mathcal{B}(0,r_g)^c$ is the compliment of the area covered by the ball centered at the origin with radius r_g. Step (a) follows from the independence of g_y across all wireless links, (b) is due to $g_y\sim\exp(1)$, (c) follows from applying PGFL of PPP and converting to polar coordinates. With simple algebraic manipulations, the final result presented in Lemma 6 follows.

B.2 Proof of Theorem 4

Technique selection is done using the following inequality:

$$
\begin{aligned}
& P_{\text{cov}}^{GZ} \underset{AN}{\overset{GZ}{\gtrless}} P_{\text{cov}}^{AN} \\
\Rightarrow & \exp\left(-\lambda_e \pi r_g^{*2} - \frac{\beta_t \sigma_P^2 \|d\|^\alpha}{P_t}\right) \underset{AN}{\overset{GZ}{\lessgtr}} \exp\left(-\frac{\beta_t \sigma_P^2 \|d\|^\alpha}{\gamma^* P_t}\right) \\
\Rightarrow & \frac{\beta_t \sigma_P^2 \|d\|^\alpha}{\gamma^* P_t} \underset{AN}{\overset{GZ}{\gtrless}} \lambda_e \pi r_g^{*2} + \frac{\beta_t \sigma_P^2 \|d\|^\alpha}{P_t} \\
\Rightarrow & \frac{\beta_t \sigma_P^2 \|d\|^\alpha}{P_t}\left(\frac{1}{\gamma^*} - 1\right) \underset{AN}{\overset{GZ}{\gtrless}} \lambda_e \pi r_g^{*2} \qquad \text{(B.2)}
\end{aligned}
$$

Since $\lambda_e \geq \lambda_e^*$, then $\Gamma\left(\frac{2}{\alpha}, \frac{(r_g^*)^\alpha \beta_e \sigma_S^2}{P_t}\right) = \frac{\alpha \log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e \left(\frac{P_t}{\sigma_S^2 \beta_e}\right)^{\frac{2}{\alpha}}}$ and $\gamma^* = \mathcal{G} = \frac{\beta_e}{1+\beta_e}\left(1 + \frac{\sigma_S^2}{P_t}\left(\frac{\alpha \log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e \Gamma(\frac{2}{\alpha})}\right)^{\frac{\alpha}{2}}\right)$.

Substituting this in (B.2), we get:

$$
\begin{aligned}
& \frac{\beta_e \sigma_S^2}{P_t}\left(\frac{\beta_t \sigma_P^2 \|d\|^\alpha}{\lambda_e \pi P_t}\left(\frac{1}{\gamma^*} - 1\right)\right)^{\frac{\alpha}{2}} \underset{AN}{\overset{GZ}{\gtrless}} \frac{(r_g^*)^\alpha \beta_e \sigma_S^2}{P_t} \\
\Rightarrow & \Gamma\left(\frac{2}{\alpha}, \frac{(r_g^*)^\alpha \beta_e \sigma_S^2}{P_t}\right) \underset{AN}{\overset{GZ}{\lessgtr}} \Gamma\left(\frac{2}{\alpha}, \mathcal{H}\right) \qquad \text{(B.3)} \\
\Rightarrow & \frac{\alpha \log\left(\frac{1}{\epsilon}\right)}{2\pi\lambda_e \left(\frac{P_t}{\sigma_S^2 \beta_e}\right)^{\frac{2}{\alpha}}} \underset{AN}{\overset{GZ}{\gtrless}} \Gamma\left(\frac{2}{\alpha}, \mathcal{H}\right) \Rightarrow \mathcal{F} \underset{AN}{\overset{GZ}{\gtrless}} 0, \qquad \text{(B.4)}
\end{aligned}
$$

where (B.3) follows by substituting $\gamma^* = \mathcal{G}$ and substituting for $\mathcal{H}$ as defined in Theorem 4 and taking Γ on both sides, while the last step follows by substituting for $\mathcal{F}$ as defined in Theorem 4. This concludes the proof.

Appendix C

Appendices for Chapter 5

C.1 Proof of Theorem 5

Recalling the expression for $\mathrm{SINR_P}$ given in (5.2), 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 (5.3). 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 (5.4), 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 $\mathrm{SINR_P}$ is the only source of correlation between the events $(R_e \geq r_g)$ and $(\mathrm{SINR_P} \geq \beta_P)$. Hence, ignoring this correlation will lead to the following

$$P_{\mathrm{con}} = \mathbb{P}(R_e \geq r_g)\mathbb{P}(\mathrm{SINR_P} \geq \beta_P). \tag{C.1}$$

The first term in the above expression represents $P_{\mathrm{active}} = \exp\left(-\pi\lambda_S r_g^2\right)$ (please recall (5.1) 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

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

where $h_1 \sim \exp(1)$ leads to step (i), and in step (j) 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 [30]. For completeness, the derivation of $\mathcal{L}_I(s)$ is provided next.

$$\begin{aligned}\mathcal{L}_I(s) &= \mathbb{E}_{\Psi_P,\{h_i\}}\left[\exp\left(-s\sum_{x_i\in\Psi_P} h_i\|x_i\|^{-\alpha}\right)\right] = \mathbb{E}_{\Psi_P,\{h_i\}}\left[\prod_{x_i\in\Psi_P}\exp\left(-sh_i\|x_i\|^{-\alpha}\right)\right] \\ &\overset{(k)}{=} \mathbb{E}_{\Psi_P}\left[\prod_{x_i\in\Psi_P}\frac{1}{1+s\|x_i\|^{-\alpha}}\right] \overset{(l)}{=} \exp\left(-\tilde{\lambda}_P\int_{x\in\mathbb{R}^2} 1 - \frac{1}{1+s\|x\|^{-\alpha}}\mathrm{d}x\right) \\ &\overset{(m)}{=} \exp\left(-2\pi\tilde{\lambda}_P\int_0^\infty \frac{s r_x^{-\alpha}}{1+s r_x^{-\alpha}} r_x \mathrm{d}r_x\right) \overset{(n)}{=} \exp\left(-\frac{2\pi^2\tilde{\lambda}_P s^{\frac{2}{\alpha}}\csc\left(\frac{2\pi}{\alpha}\right)}{\alpha}\right),\end{aligned} \tag{C.3}$$

where knowing that the set of fading gains h_i are i.i.d with $h_i \sim \exp(1)$ leads to step (k), step (l) results from using the probability generating function (PGFL) of PPP [31], step (m) results from converting to polar co-ordinates, and step (n) follows after some mathematical manipulations. Substituting (E.3) in (E.2) and then in (E.1) leads to the final result in Theorem 5.

C.2 Proof of Theorem 6

Observing the expression of P_{con} in Theorem 5, we note that it can be rewritten as a function of $P_{\text{active}} = \exp(-\lambda_S \pi r_g^2)$ as follows

$$P_{\text{con}} = \exp\left(-\beta_P \frac{\sigma_P^2}{P_t} r_1^\alpha\right) P_{\text{active}} \exp\left(-P_{\text{active}}\mathcal{A}_1\right), \tag{C.4}$$

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 (5.1)), 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.

C.3 Proof of Theorem 7

From Definition 9 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 [142]. 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 [142] 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 C.1 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

$$
\begin{aligned}
P_{\text{sec}} &= \mathbb{E}_{\Phi_S, I_2, \{g_{1,j}\}} \left[\mathbb{1} \left(\bigcap_{y_j \in \Phi_S} \frac{g_{1,j} \|y_j\|^{-\alpha}}{I_2(y_j) + \frac{\sigma_S^2}{P_t}} \leq \beta_S \right) \right] \\
&\overset{(o)}{=} \mathbb{E}_{\Phi_S, I_2, \{g_{1,j}\}} \left[\prod_{y_j \in \Phi_S} \mathbb{1} \left(\frac{g_{1,j} \|y_j\|^{-\alpha}}{I_2(y_j) + \frac{\sigma_S^2}{P_t}} \leq \beta_S \right) \right] \\
&\overset{(p)}{=} \mathbb{E}_{\Phi_S, I_2} \left[\prod_{y_j \in \Phi_S} \left(1 - \exp\left(- \frac{\beta_S \left(I_2(y_j) + \frac{\sigma_S^2}{P_t} \right)}{\|y_j\|^{-\alpha}} \right) \right) \right] \\
&\overset{(q)}{=} \mathbb{E}_{\Phi_S} \left[\prod_{y_j \in \Phi_S} \left(1 - \exp\left(- \frac{\beta_S \left(\frac{\sigma_S^2}{P_t} \right)}{\|y_j\|^{-\alpha}} \right) \mathbb{E}\left[\exp\left(- \frac{\beta_S I_2(y_j)}{\|y_j\|^{-\alpha}} \right) \right] \right) \right],
\end{aligned}
\tag{C.5}
$$

where step (o) (and step (q)) 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 (p) 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 $\mathcal{L}_{I_2(y_j)}(s) = \mathbb{E}[\exp(-sI_2(y_j))]$, 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 (E.3). The difference is in the reference point from where we are observing the interference. In Appendix C.1, 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 (E.3) until step (e), where the minimum distance effect will appear in the lower limit of the integral as follows

$$\mathcal{L}_{I_2(y_j)}(s) = \exp\left(-2\pi\tilde{\lambda}_P \int_{r_g}^{\infty} \frac{s r_x^{-\alpha}}{1 + s r_x^{-\alpha}} r_x \mathrm{d}r_x\right). \tag{C.6}$$

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 7 follows after simple mathematical manipulations. Substituting (C.6) in (E.5), we get

$$\begin{aligned} P_{\text{sec}} &= \mathbb{E}_{\Phi_S}\left[\prod_{y_j \in \Phi_S}\left(1 - \exp\left(-\beta_S\left(\frac{\sigma_S^2}{P_t}\right)\|y_j\|^{\alpha}\right)\mathcal{L}_{I_2}\left(\beta_S\|y_j\|^{\alpha}\right)\right)\right] \\ &\overset{(r)}{=} \exp\left(-2\pi\lambda_S \int_{y \in \mathbb{R}^2 \cap \mathcal{B}(o,r_g)} \exp\left(-\beta_S\left(\frac{\sigma_S^2}{P_t}\right)\|y\|^{\alpha}\right)\mathcal{L}_{I_2}\left(\beta_S\|y\|^{\alpha}\right)\mathrm{d}y\right), \end{aligned} \tag{C.7}$$

where step (r) 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 $R_e \geq r_g$, 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 7.

C.4 Proof of Theorem 8

The density of successfully powered ERs can be derived as follows

$$P_{\text{energy}} = \lambda_S \mathbb{P}\left(\eta P_t R_p^{-\alpha} w \geq E_{\min}\right) \overset{(s)}{=} \mathbb{E}_{R_p}\left[\exp\left(-\frac{E_{\min} R_p^{\alpha}}{\eta P_t}\right)\right], \tag{C.8}$$

where R_p is the distance between the ER and its nearest active PT, and step (s) 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 [143]. Given that the nearest active PT to the ER is at a distance of at least r_g, the distribution of R_p is

$$f_{R_p}(r_p) = 2\pi\tilde{\lambda}_P \exp\left(-\pi\tilde{\lambda}_P(r_p - r_g)^2\right), \quad r_p \geq r_g. \tag{C.9}$$

Using this distribution to compute the expectation in (C.8) leads to the final result in Theorem 8.

Appendix D

Appendices for Chapter 6

D.1 Proof of Theorem 9

To derive a lower bound on $F_{R_1}(r)$, we need an upper bound on the CCDF $\bar{F}_{R_1}(r) = 1 - F_{R_1}(r) = \mathbb{P}(R_1 > r)$. The exact expression of the CCDF is

$$\begin{aligned}\bar{F}_{R_1}(r) &= \mathbb{E}_{\Phi_1}\mathbb{E}_{\Phi_2}\left[\mathbb{1}\left(\mathcal{N}_{\Phi_2}\left(\mathcal{B}(o,r)\setminus\mathcal{A}(r)\right)=0\middle|\Phi_1,\Phi_2\right)\right]\\ &= \mathbb{E}_{\Phi_1}\left[\mathbb{P}\left(\mathcal{N}_{\Phi_2}\left(\mathcal{B}(o,r)\setminus\mathcal{A}(r)\right)=0\middle|\Phi_1\right)\right], \end{aligned} \tag{D.1}$$

where $\mathcal{N}_{\Phi_2}(\Xi)$ is the number of points of Φ_2 in the area covered by any *generic* region $\Xi \subset \mathbb{R}^2$, $\mathcal{A}(r) = \mathcal{B}(o,r) \cap \mathcal{A}_1$, and $\mathcal{A}_1 = \bigcup_{y\in\Phi_1} \mathcal{B}(y,D)$. The region $\mathcal{A}_1$ represents the whole area covered by the holes, and $\mathcal{A}(r)$ is the portion of this area enclosed within the circle centered at the origin with radius r. Modeling $\mathcal{A}_1$ is the main challenge in this analysis. Since we are interested in getting an upper bound on $\bar{F}_{R_1}(r)$, we will use an upper bound on the area of the region $\mathcal{A}_1$ which is $|\tilde{\mathcal{A}}_1| = \sum_{y\in\Phi_1} |\mathcal{B}(y,D)|$, where $|\Xi|$ is the area of the region Ξ. This upper bound on $\mathcal{A}_1$ overestimates the area covered by the holes since it accounts for the overlaps between holes multiple times. Hence, it overestimates the CCDF $\bar{F}_{R_1}(r)$ leading to an upper bound. Defining an upper bound on $\mathcal{A}(r)$ as $\tilde{\mathcal{A}}(r) = \mathcal{B}(o,r) \cap \tilde{\mathcal{A}}_1$, we have

$$\begin{aligned}\bar{F}_{R_1}(r) &\le \mathbb{E}_{\Phi_1}\left[\mathbb{P}\left(\mathcal{N}_{\Phi_2}\left(\mathcal{B}(o,r)\setminus\tilde{\mathcal{A}}(r)\right)=0\middle|\Phi_1\right)\right]\\ &\overset{(a)}{=} \mathbb{E}_{\Phi_1}\left[\exp\left(-\lambda_2\left(\pi r^2 - |\tilde{\mathcal{A}}(r)|\right)^+\right)\right]\\ &\overset{(b)}{\le} \mathbb{E}_{\Phi_1}\left[\exp\left(-\lambda_2\left(\pi r^2 - |\tilde{\mathcal{A}}(r)|\right)\right)\right]\\ &= \exp\left(-\lambda_2\pi r^2\right)\mathbb{E}_{\Phi_1}\left[\exp\left(\lambda_2|\tilde{\mathcal{A}}(r)|\right)\right], \end{aligned} \tag{D.2}$$

where step (a) results from the null probability of the homogeneous PPP Φ_2 ($x^+ = \max\{0, x\}$ in this step). Step (b) follows from that fact that $x^+ \geq x$. The main challenge in the rest of this derivation is to accurately determine $|\tilde{\mathcal{A}}(r)|$ for different values of r while maintaining tractability. For the case of $r < D$, the area covered by $\tilde{\mathcal{A}}(r)$ is represented by two types of holes. The first type is when $\|y\| < D - r$. In that case, as shown in Fig. D.1 (left), the circle $\mathcal{B}(o, r)$ is completely enclosed inside the hole. The second type is when $D - r < \|y\| < D + r$. In that case, as shown in Fig. D.1 (right), we need to model the intersection between the hole and the circle $\mathcal{B}(o, r)$. To facilitate that, we assume a virtual point y_2 at distance D from the origin. From this point, we draw two lines tangent to the hole that encloses this intersection. This leads to the shaded area shown in Fig. D.1 (right), which is $\mathcal{H}_1(r, \|y\|)$. Although the shaded area is larger than the required intersection, it gives much more tractable expressions. Hence, when $r < D$, the CCDF is upper bounded as follows

$$
\begin{aligned}
&\bar{F}_{R_1}(r) \\
&\leq \exp\left(-\lambda_2 \pi r^2\right) \mathbb{E}_{\Phi_1}\left[\exp\left(\lambda_2\left(\sum_{y \in \Phi_1 \cap \mathcal{B}(o, D-r)} \pi r^2 + \sum_{y \in \Phi_1 \cap \mathcal{B}(o, D-r)^c \cap \mathcal{B}(o, r+D)} \mathcal{H}_1(r, \|y\|)\right)\right)\right] \\
&= \exp\left(-\lambda_2 \pi r^2\right) \mathbb{E}_{\Phi_1}\left[\prod_{y \in \Phi_1 \cap \mathcal{B}(o, D-r)} \exp(\lambda_2 \pi r^2) \times \prod_{y \in \Phi_1 \cap \mathcal{B}(o, D-r)^c \cap \mathcal{B}(o, r+D)} \exp(\lambda_2 \mathcal{H}_1(r, \|y\|))\right] \\
&\overset{(c)}{=} \exp\left(-\lambda_2 \pi r^2\right) \mathbb{E}_{\Phi_1}\left[\prod_{y \in \Phi_1 \cap \mathcal{B}(o, D-r)} \exp(\lambda_2 \pi r^2)\right] \\
&\times \mathbb{E}_{\Phi_1}\left[\prod_{y \in \Phi_1 \cap \mathcal{B}(o, D-r)^c \cap \mathcal{B}(o, r+D)} \exp(\lambda_2 \mathcal{H}_1(r, \|y\|))\right] \\
&\overset{(d)}{=} \exp\left(-\lambda_2 \pi r^2\right) \exp\left(-\lambda_1 \int_{\mathcal{B}(o, D-r)} (1 - \exp(\lambda_2 \pi r^2)) \mathrm{d}y\right) \\
&\exp\left(-\lambda_1 \int_{\mathcal{B}(o, D-r)^c \cap \mathcal{B}(o, D+r)} (1 - \exp(\lambda_2 \mathcal{H}_1(r, \|y\|))) \mathrm{d}y\right), \qquad \text{(D.3)}
\end{aligned}
$$

where Ξ^c is the compliment of Ξ, step (c) is due to the fact that $\mathcal{B}(o, D - r)$ and $\mathcal{B}(o, D - r)^c \cap \mathcal{B}(o, r + D)$ are disjoint regions, and step (d) results from the direct application of the probability generating functional (PGFL) of the PPP [31]. For the case of $r > D$, we will follow the same approach as above. The area covered by $\tilde{\mathcal{A}}(r)$ is represented by two types of holes. The first type is when $\|y\| < r - D$. In that case, as shown in Fig. D.2 (left), the hole is completely enclosed inside the circle $\mathcal{B}(o, r)$. The second type is when $r - D < \|y\| < r + D$. In that case, as shown in Fig. D.2 (right), we model the intersection between the hole and the circle $\mathcal{B}(o, r)$ using the virtual point y_2 and the tangent lines as explained earlier. Following the same steps as above in the case

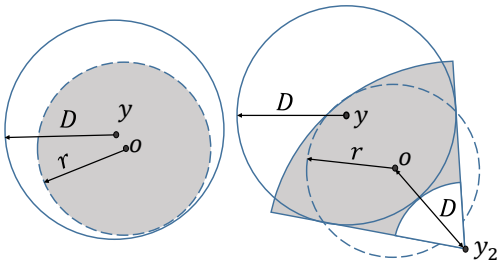

Figure D.1: The areas covered by $\tilde{A}(r)$ when the reference point is chosen uniformly at random from $\mathbb{R}^2$ independently of Ψ ($r \leq D$).

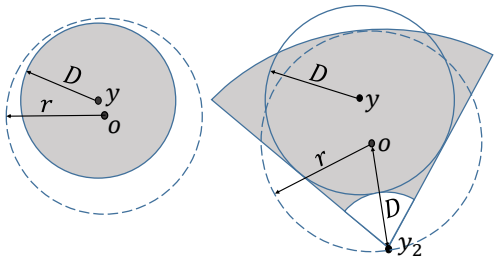

Figure D.2: The areas covered by $\tilde{A}(r)$ when the reference point is chosen uniformly at random from $\mathbb{R}^2$ independently of Ψ ($r > D$).

of $r \leq D$ we get an upper bound on the CCDF as follows

$$\begin{aligned}
&\bar{F}_{R_1}(r) \leq \exp\left(-\lambda_2 \pi r^2\right) \times \\
&\exp\left(-\lambda_1 \int_{\mathcal{B}(o,r-D)} (1 - \exp(\lambda_2 \pi D^2)) \mathrm{d}y\right) \times \\
&\exp\left(-\lambda_1 \int_{\mathcal{B}(o,r-D)^c \cap \mathcal{B}(o,D+r)} (1 - \exp(\lambda_2 \mathcal{H}_1(r, \|y\|))) \mathrm{d}y\right). \qquad \text{(D.4)}
\end{aligned}$$

The final result follows from simple algebraic manipulations of the expressions in (D.3) and (D.4).

D.2 Proof of Theorem 10

Since the reference point belongs to Φ_1, the circle $\mathcal{B}(o, D)$ does not contain any points of the PHP. In other words, the minimum value of R_2 is D. When $r > D$, following the same approach as in Appendix D.1 to upper bound the CCDF, the area covered by holes outside $\mathcal{B}(o, D)$ is upper bounded by $\tilde{A}(r) = \mathcal{B}(o, D)^c \cap \mathcal{B}(o, r) \cap \tilde{A}_1$ and $|\tilde{A}_1| = \sum_{y \in \Phi_1} |\mathcal{B}(y, D)|$. Hence, the CCDF is:

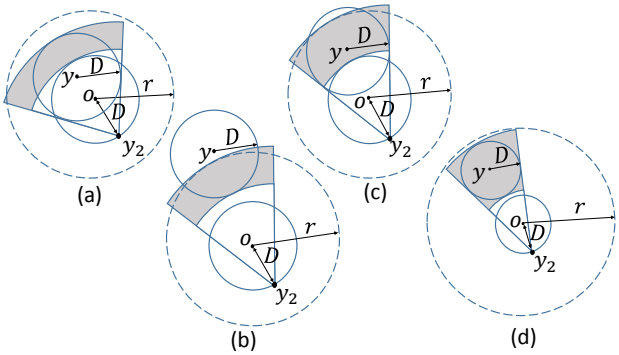

Figure D.3: The areas covered by $\tilde{A}(r)$ when the reference point is a hole center.

$\bar{F}_{R_2}(r) \leq$

$$\mathbb{E}_{\Phi_1}\left[\mathbb{P}\left(\mathcal{N}_{\Phi_2}\left(\mathcal{B}(o,r)\setminus\{\mathcal{B}(o,D)\cup\tilde{\mathcal{A}}(r)\}\right)=0\middle|\Phi_1\right)\right]$$
$$=\exp\left(-\lambda_2\pi(r^2-D^2)\right)\mathbb{E}_{\Phi_1}\left[\exp\left(\lambda_2|\tilde{\mathcal{A}}(r)|\right)\right]. \quad \text{(D.5)}$$

The area covered by $\tilde{\mathcal{A}}(r)$ is represented by four types of holes. The first type is when $\|y\| \leq 2D, \|y\| \leq r-D$. The area in that case is as shown in Fig. D.3.a. The second type, shown in Fig. D.3.b, is when $\|y\| > 2D, r-D < \|y\| \leq r+D$. The third type, shown in Fig. D.3.c, is when $\|y\| < 2D, r-D < \|y\| \leq r+D$. The fourth type, shown in Fig. D.3.d, is when $\|y\| > 2D, \|y\| \leq r-D$. The areas of the shaded sectors in the four cases can be combined in one mathematical expression, which is $\mathcal{H}_2(r, r_y)$ as defined in Theorem 10. Following similar procedure as in Appendix D.1 leads to the final expression.

Appendix E

Appendices for Chapter 7

E.1 Proof of Theorem 11

Recalling the expression for $\mathrm{SIR_I}$ given in (7.2), specifically δ^S which appears in the interference term, we introduce two PPPs to capture the overall interference: (i) Φ_P^a with density $p_a^S\lambda_P$ and (ii) Φ_P^b with density $p_b^S\lambda_P$. Hence, the expression of $\mathrm{SIR_I}$ can be given as $\frac{\tau^S g r_1^{-\alpha}}{I_{c_1}+I_{c_2}}$, where $I_{c_1} = \sum_{x_j\in\Phi_P^a} a^S w_j \|x_j - z\|^{-\alpha}$ and $I_{c_2} = \sum_{x_j\in\Phi_P^b} b^S w_j \|x_j - z\|^{-\alpha}$.

Please note that δ^S for different $x_i \in \Phi_P$ are correlated for the case of GZ. This correlation is due to the dependence of each of the δ_i's on the PPP Φ_S. However, taking this correlation into consideration in our analysis complicates it and leads to intractability. Hence, this correlation will be ignored in our analysis for the sake of tractability. Recalling the mathematical expression for P_{con}^S in Definition 8, we observe that the correlation between δ_1^S and δ_i^S's in the expression of $\mathrm{SIR_I}$ is the only source of correlation between the events $(R_e \geq \mu^S)$ and $(\mathrm{SIR_I} \geq \beta_I)$. Given that this correlation is ignored in our analysis, for the sake of tractability as explained earlier, then $P_{\mathrm{con}}^S = \mathbb{P}(R_e \geq \mu^S)\mathbb{P}(\mathrm{SIR_I} \geq \beta_I) + q\left(1 - \mathbb{P}(R_e \geq \mu^S)\right)\mathbb{P}(\mathrm{SIR_I} \geq \beta_I)$. Hence,

$$P_{\mathrm{con}}^S \overset{(a)}{=} \left(\mathcal{C}^S + q\left(1 - \mathcal{C}^S\right)\right)\mathbb{P}(\mathrm{SIR_I} \geq \beta_I) \tag{E.1}$$

where (a) follows by using the contact distance distribution of PPP for R_e [31], and $\mathcal{C}_S$ is given in Theorem 11.

$$\begin{aligned}
\mathbb{P}(\mathrm{SIR_I} \geq \beta_I) &= \mathbb{P}\left(\frac{\tau^S g r_1^{-\alpha}}{I_{c_1} + I_{c_2}} \geq \beta_I\right) \\
&\overset{(b)}{=} \mathbb{E}_{I_{c_1},I_{c_2}}\left[\exp\left(-\frac{\beta_I}{\tau^S}\left(I_{c_1} + I_{c_2}\right) r_1^{\alpha}\right)\right] \\
&\overset{(c)}{=} \mathbb{E}_{I_{c_1}}\left[\exp\left(-\frac{\beta_I}{\tau^S}\left(I_{c_1}\right) r_1^{\alpha}\right)\right]\mathbb{E}_{I_{c_2}}\left[\exp\left(-\frac{\beta_I}{\tau^S}\left(I_{c_2}\right) r_1^{\alpha}\right)\right],
\end{aligned} \tag{E.2}$$

where step (b) is due to the Rayleigh fading assumption, and step (c) is from the assumption of independent thinning leading to Φ_P^a and Φ_P^b. Each of the above expectations can be derived in the same way, which is shown below for I_{c_1}. Without loss of generality, we can assume z to be placed at the origin.

$$\begin{aligned}
&\mathbb{E}_{I_{c_1}}\left[\exp\left(-sI_{c_1}\right)\right] = \mathbb{E}_{I_{c_1}}\left[\exp\left(-s\sum_{x_j\in\Phi_P^a} a^S w_j \|x_j\|^{-\alpha}\right)\right] \\
&= \mathbb{E}_{\Phi_P^a,\{w_j\}}\left[\prod_{x_j\in\Phi_P^a}\exp\left(-sa^S w_j\|x_j\|^{-\alpha}\right)\right] \\
&\overset{(d)}{=} \mathbb{E}_{\Phi_P^a}\left[\prod_{x_j\in\Phi_P^a}\frac{1}{1+sa^S\|x_j\|^{-\alpha}}\right] \\
&\overset{(e)}{=} \exp\left(-p_a^S\lambda_P\int_{x\in\mathbb{R}^2} 1-\frac{1}{1+sa^S\|x\|^{-\alpha}}\mathrm{d}x\right) \\
&\overset{(f)}{=} \exp\left(-2\pi a^S p_a^S\lambda_P\int_0^\infty \frac{sr_x^{-\alpha}}{1+sr_x^{-\alpha}} r_x \mathrm{d}r_x\right) \\
&\overset{(g)}{=} \exp\left(-\frac{2\pi^2 a^S p_a^S\lambda_P s^{\frac{2}{\alpha}}\csc\left(\frac{2\pi}{\alpha}\right)}{\alpha}\right),
\end{aligned} \tag{E.3}$$

where step (d) results from the independence of the set of fading gains w_i with $w_i \sim \exp(1)$, step (e) results from applying the probability generating function (PGFL) of PPP [31], step (f) results from converting Cartesian to polar co-ordinates, and step (g) follows after some mathematical manipulations. Following the same procedure for I_{c_2} leads to the same expression with $b^S P_b^S$ instead $a^S P_a^S$, where

$$\mathbb{E}_{I_{c_1}}\left[\exp\left(-sI_{c_1}\right)\right] \times \mathbb{E}_{I_{c_2}}\left[\exp\left(-sI_{c_2}\right)\right] = \exp\left(-\mathcal{A}(s)\right). \tag{E.4}$$

Substituting (E.4) in (E.2) and then in (E.1) leads to the final result in Theorem 11.

E.2 Proof of Theorem 12

Recalling Definition 9 of P_{out}^S, we note that joint analysis of $\mathrm{SIR}_{\mathrm{E}}(y_j)$ at all the locations $y_j \in \Phi_S$ is required. All the analysis provided in this section is conditioned on the event $\mathcal{E}_{\text{active}}$. Following the same approach as in Appendix C.1 of independently thinning Φ_P into Φ_P^a and Φ_P^b, we define the interference terms as $I_{s_1} = \sum_{x_j\in\Phi_P^a} a^S h_j\|x_j - y_i\|^{-\alpha}$ and $I_{s_2} = \sum_{x_j\in\Phi_P^b} b^S h_j\|x_j - y_i\|^{-\alpha}$.

Hence,

$$P_{\text{out}}^{S} = 1 - \frac{\mathbb{P}\left(\sum_{y_i \in \Phi_S} \mathbf{1}\left(\text{SIR}_{\text{E}}(\text{y}_\text{i}) \geq \beta_{\text{E}}\right) = 0, \mathcal{E}_{\text{active}}\right)}{\mathbb{P}(\mathcal{E}_{\text{active}})} \tag{E.5}$$

where $\mathbb{P}(\mathcal{E}_{\text{active}}) = \mathcal{C}^S + q(1-\mathcal{C}^S)$, and

$$\begin{aligned}
&\mathbb{P}\left(\sum_{y_i \in \Phi_S} \mathbf{1}\left(\text{SIR}_{\text{E}}(\text{y}_\text{i}) \geq \beta_{\text{E}}\right) = 0, \mathcal{E}_{\text{active}}\right) \\
&= \mathcal{C}^S \mathbb{P}\left(\sum_{y_i \in \Phi_S} \mathbf{1}\left(\text{SIR}_{\text{E}}(\text{y}_\text{i}) \geq \beta_{\text{E}}\right) = 0 \Big| R_e \geq \mu^S\right) \\
&+ q(1-\mathcal{C}^S)\mathbb{P}\left(\sum_{y_i \in \Phi_S} \mathbf{1}\left(\text{SIR}_{\text{E}}(\text{y}_\text{i}) \geq \beta_{\text{E}}\right) = 0 \Big| R_e \leq \mu^S\right).
\end{aligned} \tag{E.6}$$

Let $\mathcal{T}$ be the event $\left(\sum_{y_i \in \Phi_S} \mathbf{1}\left(\text{SIR}_{\text{E}}(\text{y}_\text{i}) \geq \beta_{\text{E}}\right) = 0\right)$. Hence, by applying the rule of total probability and using Bayes Theorem we can show that $\mathbb{P}\left(\mathcal{T}|R_e \leq \mu^S\right) = \frac{\mathbb{P}(\mathcal{T}) - \mathbb{P}\left(R_e \geq \mu^S\right)\mathbb{P}(\mathcal{T}|R_e \geq \mu^S)}{\mathbb{P}(R_e \leq \mu^S)}$, which equals $\frac{\mathbb{P}(\mathcal{T}) - \mathcal{C}^S\mathbb{P}(\mathcal{T}|R_e \geq \mu^S)}{1-\mathcal{C}^S}$. We derive each of $\mathbb{P}(\mathcal{T})$ and $\mathbb{P}(\mathcal{T}|R_e \geq \mu^S)$ in the following lines. Note that the only difference between the two probabilities is in the condition, which only appears in the final step of the derivation, as will be shown in the sequel.

$$\begin{aligned}
&\mathbb{P}\left(\sum_{y_i \in \Phi_S} \mathbf{1}\left(\text{SIR}_{\text{E}}(\text{y}_\text{i}) \geq \beta_{\text{E}}\right) = 0 \Big| R_e \geq \mu^S\right) = \mathbb{E}\left[\mathbf{1}\left(\bigcap_{y_i \in \Phi_S} \frac{\sigma^S h_{0,i}\|y_i\|^{-\alpha}}{I_{s_1} + I_{s_2} + \kappa^S h_{0,i}\|y_i\|^{-\alpha}} \leq \beta_E\right)\right] \\
&= \mathbb{E}_{\Phi_S, I_{s_1}, I_{s_2}, \{h_{0,i}\}}\left[\prod_{y_i \in \Phi_S} \mathbf{1}\left(\frac{h_{0,i}\|y_i\|^{-\alpha}}{I_{s_1} + I_{s_2}} \leq \frac{\beta_E}{\sigma^S - \kappa^S \beta_E}\right)\right] \\
&\overset{(h)}{=} \mathbb{E}_{\Phi_S, I_{s_1}, I_{s_2}}\left[\prod_{y_i \in \Phi_S}\left(1 - \exp\left(-\frac{\beta_E\left(I_{s_1} + I_{s_2}\right)}{(\sigma^S - \kappa^S\beta_E)\|y_i\|^{-\alpha}}\right)\right)\right] \\
&\overset{(i)}{=} \mathbb{E}_{\Phi_S}\left[\prod_{y_i \in \Phi_S}\left(1 - \mathbb{E}_{I_{s_1}, I_{s_2}}\left[\exp\left(\frac{-\beta_E\left(I_{s_1} + I_{s_2}\right)}{(\sigma^S - \kappa^S\beta_E)\|y_i\|^{-\alpha}}\right)\right]\right)\right] \\
&\overset{(k)}{=} p_c^S \mathbb{E}_{\Phi_S}\left[\prod_{y_i \in \Phi_S}\left(1 - \exp\left(-\mathcal{A}\left(\frac{\beta_E}{(c^S - \kappa^S\beta_E)\|y_i\|^{-\alpha}}\right)\right)\right)\right] \\
&+ p_d^S \mathbb{E}_{\Phi_S}\left[\prod_{y_i \in \Phi_S}\left(1 - \exp\left(-\mathcal{A}\left(\frac{\beta_E}{(d^S - \kappa^S\beta_E)\|y_i\|^{-\alpha}}\right)\right)\right)\right],
\end{aligned} \tag{E.7}$$

where step (h) follows from the assumption that $h_{0,i} \sim \exp(1)$ are independent. Step (i) follows from assuming that the interference levels are independent at different ER locations and step (k) follows directly from (E.4) in Appendix C.1 and using the definition of σ^S. The only difference between the two expectations in the above expression is replacing c^S with d^S. In order to avoid repetition, we will show the final expression for d^S. When the expectation is conditioned on $R_e \geq \mu^S$, the final expression follows by applying PGFL of the PPP Φ_S as follows

$$\exp\left(-\lambda_S \int_{y\in\Xi} \exp\left(-\mathcal{A}\left(\frac{\beta_E}{(d^S-\kappa^S\beta_E)\|y\|^{-\alpha}}\right)\right)\mathrm{d}y\right), \tag{E.8}$$

where $\Xi = \mathbb{R}^2 \cap \mathcal{B}(0,\mu^S)^c$, D^c is the compliment of the region covered by D, and $\mathcal{B}(0,\mu^S)$ is a ball centered at the origin with radius μ^S. When the expectation is unconditioned then

$$\exp\left(-\lambda_S \int_{y\in\mathbb{R}^2} \exp\left(-\mathcal{A}\left(\frac{\beta_E}{(d^S-\kappa^S\beta_E)\|y\|^{-\alpha}}\right)\right)\mathrm{d}y\right), \tag{E.9}$$

Substituting (E.9) and (E.8) in (E.7) and then in (E.6) and (E.5) leads to the final expression.

E.3 Proof of Theorem 13

We follow the same approach used in [102], which approximates E_{rec} with the energy harvested from the nearest IT and the expectation of the energy harvested from the rest of the ITs. To use this approach in our analysis, the only changes in the derivation are (i) considering $\delta^S = a^S$ for the nearest IR with probability P_a^S and $\delta^S = b^S$ with probability P_b^S and (ii) deriving the expectation conditioned on the location of the nearest IR: $\mathbb{E}\left[\sum_{x_j\in\Phi_P\setminus x_1} \delta_j^S h_j \|x_j - y_i\|^{-\alpha}\right] = \frac{2\pi\lambda_P\|x_1\|^{2-\alpha}}{\alpha-2}\left(a^S p_a^S + b^S p_b^S\right)$. Considering both changes and following similar approach as Appendix A in [102] leads to the final expression.

Chapter 11

Bibliography

[1] V. Chamola and B. Sikdar, "Solar powered cellular base stations: current scenario, issues and proposed solutions," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 108–114, May 2016.

[2] A. Somov and R. Giaffreda, "Powering IoT Devices: Technologies and Opportunities", *IEEE IoT Newsletter*, Nov. 2015.

[3] V. Talla, B. Kellogg, S. Gollakota, and J. R. Smith, "Battery-free cellphone," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 2, pp. 25:1–25:20, Jun. 2017. [Online]. Available: http://doi.acm.org/10.1145/3090090

[4] O. Ozel and S. Ulukus, "Achieving AWGN capacity under stochastic energy harvesting," *IEEE Trans. on Info. Theory*, vol. 58, no. 10, pp. 6471–6483, 2012.

[5] J. Yang, "Achievable rate for energy harvesting channel with finite blocklength," in *IEEE International Symposium on Information Theory (ISIT)*, 2014, pp. 811–815.

[6] R. Rajesh, P. Deekshith, and V. Sharma, "Capacity of a gaussian MAC with energy harvesting transmit nodes," in *Information Theory and Applications Workshop (ITA)*, 2012, pp. 338–343.

[7] R. A. Raghuvir, D. Rajan, and M. D. Srinath, "Capacity of the multiple access channel in energy harvesting wireless networks," in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2012, pp. 898–902.

[8] J. G. Smith, "The information capacity of amplitude-and variance-constrained scalar gaussian channels," *Information and Control*, vol. 18, no. 3, pp. 203–219, 1971.

[9] O. Ozel and S. Ulukus, "AWGN channel under time-varying amplitude constraints with causal information at the transmitter," in *Proc., IEEE Asilomar*, Nov. 2011, pp. 373–377.

[10] E. MolavianJazi and A. Yener, "Low-latency communications over zero-battery energy harvesting channels," in *Proc., IEEE GLOBECOM*, Dec. 2015, pp. 1–6.

[11] O. Ozel and S. Ulukus, "On the capacity region of the gaussian MAC with batteryless energy harvesting transmitters," in *IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 2385–2390.

[12] ——, "Energy state amplification in an energy harvesting communication system," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, 2012, pp. 1351–1355.

[13] V. Jog and V. Anantharam, "An energy harvesting AWGN channel with a finite battery," in *IEEE International Symposium on Information Theory (ISIT)*, 2014, pp. 806–810.

[14] K. Tutuncuoglu, O. Ozel, A. Yener, and S. Ulukus, "Binary energy harvesting channel with finite energy storage," in *IEEE International Symposium on Information Theory Proceedings (ISIT)*, 2013, pp. 1591–1595.

[15] Y. Dong, F. Farnia, and A. Ozgur, "Near optimal energy control and approximate capacity of energy harvesting communication," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 3, pp. 540–557, 2015.

[16] D. Shaviv, P. M. Nguyen, and A. ozgur, "Capacity of the energy-harvesting channel with a finite battery," *IEEE Transactions on Information Theory*, vol. 62, no. 11, pp. 6436–6458, Nov. 2016.

[17] D. Shaviv, A. Ozgur, and H. Permuter, "Can feedback increase the capacity of the energy harvesting channel?" in *IEEE Information Theory Workshop (ITW)*, 2015, pp. 1–5.

[18] J. Yang and S. Ulukus, "Optimal packet scheduling in an energy harvesting communication system," *IEEE Transactions on Communications*, vol. 60, no. 1, pp. 220–230, 2012.

[19] K. Tutuncuoglu and A. Yener, "Optimum transmission policies for battery limited energy harvesting nodes," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 1180–1189, 2012.

[20] O. Ozel, K. Tutuncuoglu, J. Yang, S. Ulukus, and A. Yener, "Transmission with energy harvesting nodes in fading wireless channels: Optimal policies," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 8, pp. 1732–1743, 2011.

[21] A. Kazerouni and A. Ozgur, "Optimal online strategies for an energy harvesting system with bernoulli energy recharges," in *2015 13th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, May 2015, pp. 235–242.

[22] D. Shaviv and A. ozgur, "Universally near optimal online power control for energy harvesting nodes," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 12, pp. 3620–3631, Dec. 2016.

[23] K. Tutuncuoglu, A. Yener, and S. Ulukus, "Optimum policies for an energy harvesting transmitter under energy storage losses," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 3, pp. 467–481, 2015.

[24] O. Ozel, K. Shahzad, and S. Ulukus, "Optimal energy allocation for energy harvesting transmitters with hybrid energy storage and processing cost," *IEEE Transactions on Signal Processing*, vol. 62, no. 12, pp. 3232–3245, 2014.

[25] K. Tutuncuoglu, B. Varan, and A. Yener, "Throughput maximization for two-way relay channels with energy harvesting nodes: The impact of relaying strategies," *IEEE Transactions on Communications*, vol. 63, no. 6, pp. 2081–2093, 2015.

[26] B. Gurakan and S. Ulukus, "Cooperative diamond channel with energy harvesting nodes," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1604–1617, May 2016.

[27] K. Tutuncuoglu and A. Yener, "Sum-rate optimal power policies for energy harvesting transmitters in an interference channel," *Journal of Communications and Networks*, vol. 14, no. 2, pp. 151–161, 2012.

[28] B. Varan and A. Yener, "Delay constrained energy harvesting networks with limited energy and data storage," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1550–1564, May 2016.

[29] O. Ozel, S. Ulukus, and P. Grover, "Energy harvesting transmitters that heat up: Throughput maximization under temperature constraints," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5440–5452, Aug. 2016.

[30] J. G. Andrews, A. K. Gupta, and H. S. Dhillon, "A primer on cellular network analysis using stochastic geometry," 2016, available online: arxiv.org/abs/1604.03183.

[31] M. Haenggi, *Stochastic geometry for wireless networks*. Cambridge University Press, 2012.

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

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

[34] T. A. Khan, P. V. Orlik, K. J. Kim, R. W. Heath, and K. Sawa, "A stochastic geometry analysis of large-scale cooperative wireless networks powered by energy harvesting," *IEEE Transactions on Communications*, vol. 65, no. 8, pp. 3343–3358, Aug. 2017.

[35] Y. L. Che, L. Duan, and R. Zhang, "Dynamic base station operation in large-scale green cellular networks," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 12, pp. 3127–3141, Dec. 2016.

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

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

[38] Y. L. Che, L. Duan, and R. Zhang, "Spatial throughput maximization of wireless powered communication networks," *IEEE Journal on Sel. Areas in Commun.*, vol. 33, no. 8, pp. 1534–1548, Aug. 2015.

[39] 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. on Wireless Commun.*, vol. 14, no. 10, pp. 5402–5416, Oct. 2015.

[40] K. Huang, "Spatial throughput of mobile ad hoc networks powered by energy harvesting," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7597–7612, 2013.

[41] I. Krikidis, "Simultaneous information and energy transfer in large-scale networks with/without relaying," *IEEE Trans. on Commun.*, vol. 62, no. 3, pp. 900–912, Mar. 2014.

[42] H. H. Yang, J. Lee, and T. Q. S. Quek, "Heterogeneous cellular network with energy harvesting-based D2D communication," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1406–1419, Feb 2016.

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

[44] Y. Yao, X. Song, C. Yin, and S. Huang, "Opportunistic energy harvesting and energy-based opportunistic spectrum access in cognitive radio networks," in *Cognitive Radio Oriented Wireless Networks*. Springer, 2015, pp. 187–198.

[45] C. Zhai, J. Liu, and L. Zheng, "Cooperative spectrum sharing with wireless energy harvesting in cognitive radio network," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, 2015.

[46] 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. on Commun.*, vol. 64, no. 1, pp. 329–342, Jan. 2016.

[47] K. Huang and X. Zhou, "Cutting the last wires for mobile communications by microwave power transfer," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 86–93, June 2015.

[48] A. H. Sakr and E. Hossain, "Cognitive and energy harvesting-based D2D communication in cellular networks: Stochastic geometry modeling and analysis," *IEEE Trans. on Commun.*, vol. 63, no. 5, pp. 1867–1880, May 2015.

[49] A. Whitmore, A. Agarwal, and L. Da Xu, "The internet of things: A survey of topics and trends," *Information Systems Frontiers*, vol. 17, no. 2, pp. 261–274, Apr. 2015.

[50] Ericsson, "Ericsson Mobility Report: One the Pulse of the Networked Society", white paper, Nov. 2015. Available online: http://goo.gl/5nSiwt.

[51] 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. on Wireless Commun.*, vol. 12, no. 11, pp. 5740 – 5753, Nov. 2013.

[52] ——, "Fundamentals of throughput maximization with random arrivals for M2M communications," *IEEE Trans. on Commun.*, vol. 62, no. 11, pp. 4094 – 4109, Nov. 2014.

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

[54] 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., the 7th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, Oct. 2012, pp. 99–106.

[55] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys and Tutorials*, vol. 17, no. 2, pp. 757–789, Secondquarter 2015.

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

[57] S. Ulukus, A. Yener, E. Erkip, O. Simeone, M. Zorzi, P. Grover, and K. Huang, "Energy harvesting wireless communications: A review of recent advances," *IEEE Journal on Sel. Areas in Commun.*, vol. 33, no. 3, pp. 360 – 381, Mar. 2015.

[58] 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 and Tutorials*, vol. 15, no. 3, pp. 996 – 1019, 2013.

[59] S. Mukherjee, *Analytical Modeling of Heterogeneous Cellular Networks: Geometry, Coverage, and Capacity*. New York: Cambridge University Press, 2014.

[60] C. Zhong, X. Chen, Z. Zhang, and G. K. Karagiannidis, "Wireless-powered communications: Performance analysis and optimization," *IEEE Trans. on Commun.*, vol. 63, no. 12, pp. 5178–5190, Dec. 2015.

[61] K. Ganesan, P. Grover, and J. Rabaey, "The power cost of over-designing codes," *Proc., IEEE Workshop on Signal Processing Systems (SiPS)*, pp. 128–133, Oct. 2011.

[62] C. G. Blake and F. R. Kschischang, "Energy consumption of VLSI decoders," *IEEE Trans. on Info. Theory*, vol. 61, no. 6, pp. 3185–3198, June 2015.

[63] P. Grover, "Bounds on the tradeoff between decoding complexity and rate for sparse-graph codes," in *Proc., IEEE Info. Theory Workshop (ITW)*, Sept. 2007, pp. 196–201.

[64] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. on Commun.*, vol. 61, no. 11, pp. 4754–4767, Nov. 2013.

[65] S. Zhou, T. Chen, W. Chen, and Z. Niu, "Outage minimization for a fading wireless link with energy harvesting transmitter and receiver," *IEEE Journal on Sel. Areas in Commun.*, vol. 33, no. 3, pp. 496–511, Mar. 2015.

[66] 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. on Veh. Technology*, vol. 66, no. 3, pp. 2251–2275, March 2017.

[67] T. A. Khan, A. Alkhateeb, and R. W. Heath, "Millimeter wave energy harvesting," *IEEE Trans. on Wireless Commun.*, vol. 15, no. 9, pp. 6048–6062, Sept. 2016.

[68] M. M. Shaikh and M. C. Aguayo-Torres, "Joint uplink/downlink coverage and spectral efficiency in heterogeneous cellular network," *Wireless Personal Commun.*, pp. 1–12, Nov. 2016.

[69] K. Yang, P. Wang, X. Hong, and X. Zhang, "Joint downlink and uplink network performance analysis with CRE in heterogeneous wireless network," in *Proc., IEEE PIMRC*, Aug. 2015, pp. 1659–1663.

[70] S. Singh, X. Zhang, and J. G. Andrews, "Joint rate and SINR coverage analysis for decoupled uplink-downlink biased cell associations in HetNets," *IEEE Trans. on Wireless Commun.*, vol. 14, no. 10, pp. 5360–5373, Oct. 2015.

[71] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. on Commun.*, vol. 59, no. 11, pp. 3122–3134, Nov. 2011.

[72] M. Haenggi, "User point processes in cellular networks," *IEEE Wireless Commun. Letters*, vol. 6, no. 2, pp. 258–261, Apr. 2017.

[73] S. Weber, J. G. Andrews, and N. Jindal, "The effect of fading, channel inversion, and threshold scheduling on ad hoc networks," *IEEE Trans. on Info. Theory*, vol. 53, no. 11, pp. 4127–4149, Nov. 2007.

[74] P. Madhusudhanan, J. G. Restrepo, Y. Liu, T. X. Brown, and K. R. Baker, "Downlink performance analysis for a generalized shotgun cellular system," *IEEE Trans. on Wireless Commun.*, vol. 13, no. 12, pp. 6684–6696, Dec. 2014.

[75] J. Schloemann, H. S. Dhillon, and R. M. Buehrer, "Toward a tractable analysis of localization fundamentals in cellular networks," *IEEE Trans. on Wireless Commun.*, vol. 15, no. 3, pp. 1768–1782, March 2016.

[76] T. Bhandari, H. S. Dhillon, and R. M. Buehrer, "The impact of proximate base station measurements on localizability in cellular systems," in *Proc., IEEE SPAWC*, July 2016.

[77] V. V. Chetlur and H. S. Dhillon, "Downlink coverage probability in a finite network of unmanned aerial vehicle (UAV) base stations," in *Proc., IEEE SPAWC*, July 2016.

[78] ——, "Downlink coverage analysis for a finite 3-D wireless network of unmanned aerial vehicles," *IEEE Transactions on Communications*, vol. 65, no. 10, pp. 4543–4558, Oct. 2017.

[79] D. Moltchanov, "Distance distributions in random networks," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1146–1166, 2012.

[80] C. Saha, M. Afshang, and H. S. Dhillon, "Enriched K-tier HetNet model to enable the analysis of user-centric small cell deployments," *IEEE Trans. on Wireless Commun.*, vol. 16, no. 3, pp. 1593–1608, Mar. 2017.

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

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

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

[84] J. Xiong, K. K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Commun. Letters*, vol. 16, no. 9, pp. 1496–1499, Sept. 2012.

[85] H. Sun, M. Wildemeersch, M. Sheng, and T. Q. S. Quek, "D2D enhanced heterogeneous cellular networks with dynamic TDD," *IEEE Trans. on Wireless Commun.*, vol. 14, no. 8, pp. 4204–4218, Aug. 2015.

[86] M. Afshang, H. S. Dhillon, and P. H. J. Chong, "Modeling and performance analysis of clustered device-to-device networks," *IEEE Trans. on Wireless Commun.*, vol. 15, no. 7, pp. 4957–4972, July 2016.

[87] 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. on Commun.*, vol. 62, no. 6, pp. 2006–2021, 2014.

[88] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[89] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for gaussian block-fading channels," *IEEE Trans. on Info. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[90] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Letters*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

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

[92] 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 Intl. Conf. on Acoustics, Speech, and Sig. Proc. (ICASSP)*, May 2014, pp. 1596–1600.

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

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

[95] 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. on Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, 2014.

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

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

[98] 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. on Information Forensics and Security*, vol. 9, no. 10, pp. 1617–1628, Oct. 2014.

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

[100] M. A. Kishk and H. S. Dhillon, "Stochastic geometry-based comparison of secrecy enhancement techniques in d2d networks," *IEEE Wireless Communications Letters*, vol. 6, no. 3, pp. 394–397, June 2017.

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

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

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

[104] 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. on Wireless Commun.*, vol. 11, no. 11, pp. 3980–3991, Nov. 2012.

[105] 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. on Information Forensics and Security*, vol. 8, no. 5, pp. 717–732, May 2013.

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

[107] 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 Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7178–7194, Aug. 2017.

[108] 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. on Wireless Commun.*, vol. 14, no. 1, pp. 410–420, Jan. 2015.

[109] 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.

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

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

[112] Y. Ren, T. Lv, H. Gao, and Y. Li, "Secure wireless information and power transfer in heterogeneous networks," 2017, *IEEE Access*, to appear.

[113] 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 Processing Letters*, vol. 21, no. 7, pp. 804–808, July 2014.

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

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

[116] C. h. Lee and M. Haenggi, "Interference and outage in Poisson cognitive networks," *IEEE Trans. on Wireless Commun.*, vol. 11, no. 4, pp. 1392–1401, April 2012.

[117] W. H. Sandholm, *Population games and evolutionary dynamics*. MIT press, 2010.

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

[119] E. Barron, R. Goebel, and R. Jensen, "Best response dynamics for continuous games," *Proceedings of the American Mathematical Society*, vol. 138, no. 3, pp. 1069–1083, 2010.

[120] H. ElSawy, E. Hossain, and M.-S. Alouini, "Analytical modeling of mode selection and power control for underlay D2D communication in cellular networks," *IEEE Trans. on Wireless Commun.*, vol. 62, no. 11, pp. 4147–4161, Nov 2014.

[121] M. Afshang and H. S. Dhillon, "Spatial modeling of device-to-device networks: Poisson cluster process meets Poisson hole process," in *Proc. Asilomar*, Nov. 2015, pp. 317–321.

[122] N. Deng, W. Zhou, and M. Haenggi, "Heterogeneous cellular network models with dependence," *IEEE Journal on Sel. Areas in Commun.*, vol. 33, no. 10, pp. 2167–2181, Oct. 2015.

[123] C.-H. Lee and C. Y. Shih, "Coverage analysis of cognitive femtocell networks," *IEEE Wireless Commun. Letters*, vol. 3, no. 2, pp. 177–180, April 2014.

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

[125] R. K. Ganti and M. Haenggi, "Regularity in sensor networks," in *Proc., Intl. Zurich Seminar on Commun.*, 2006, pp. 186–189.

[126] Z. Yazdanshenasan, H. S. Dhillon, and P. H. J. Chong, "Serving distance and coverage in a closed access PHP-based heterogeneous cellular network," in *Proc., Biennial Symposium on Commun.*, June 2016.

[127] M. A. Kishk and H. S. Dhillon, "Joint uplink and downlink coverage analysis of cellular-based RF-powered IoT network," *IEEE Trans. on Green Commun. and Networking*, vol. 2, no. 2, pp. 446–459, June 2018.

[128] ——, "Coexistence of RF-powered IoT and a primary wireless network with secrecy guard zones," *IEEE Trans. on Wireless Commun.*, vol. 17, no. 3, pp. 1460–1473, March 2018.

[129] ——, "Modeling and analysis of ambient RF energy harvesting in networks with secrecy guard zones," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, March 2017, pp. 1–6.

[130] A. M. Hunter, J. G. Andrews, and S. Weber, "Transmission capacity of ad hoc networks with spatial diversity," *IEEE Trans. on Wireless Commun.*, vol. 7, no. 12, pp. 5058–5071, Dec. 2008.

[131] G. Lee, W. Saad, M. Bennis, A. Mehbodniya, and F. Adachi, "Online ski rental for ON/OFF scheduling of energy harvesting base stations," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 2976–2990, May 2017.

[132] N. Abuzainab, W. Saad, and B. Maham, "Robust bayesian learning for wireless RF energy harvesting networks," in *2017 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, May 2017, pp. 1–8.

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

[134] M. Franceschetti, L. Booth, M. Cook, R. Meester, and J. Bruck, "Percolation in multi-hop wireless networks," 2003.

[135] O. Dousse, F. Baccelli, and P. Thiran, "Impact of interferences on connectivity in ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 13, no. 2, pp. 425–436, 2005.

[136] M. Franceschetti, O. Dousse, D. N. C. Tse, and P. Thiran, "Closing the gap in the capacity of wireless networks via percolation theory," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 1009–1018, March 2007.

[137] T. Gebele, "Site percolation threshold for square lattice," *Journal of Physics A: Mathematical and General*, vol. 17, no. 2, p. L51, 1984.

[138] S. Zhang, N. Zhang, S. Zhou, J. Gong, Z. Niu, and X. Shen, "Energy-aware traffic offloading for green heterogeneous networks," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 5, pp. 1116–1129, May 2016.

[139] P. S. Yu, J. Lee, T. Q. S. Quek, and Y. W. P. Hong, "Traffic offloading in heterogeneous networks with energy harvesting personal cells-network throughput and energy efficiency," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1146–1161, Feb. 2016.

[140] G. Qiao, S. Leng, K. Zhang, and K. Yang, "Joint deployment and mobility management of energy harvesting small cells in heterogeneous networks," *IEEE Access*, vol. 5, pp. 183–196, 2017.

[141] G. Fayolle and R. Iasnogorodski, "Two coupled processors: the reduction to a riemann-hilbert problem," *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, vol. 47, no. 3, pp. 325–351, 1979.

[142] S. Krishnan and H. S. Dhillon, "Spatio-temporal interference correlation and joint coverage in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 5659–5672, Sept. 2017.

[143] M. A. Kishk and H. S. Dhillon, "Tight lower bounds on the contact distance distribution in Poisson hole process," *IEEE Wireless Commun. Letters*, to appear.