Covert Communications in the RF Band of Primary Wireless Networks

By

Ghaith Shabsigh

Submitted to the Department of Electrical Engineering and Computer Science and the
Graduate Faculty of the University of Kansas
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy

Committee members

Victor S. Frost, Chairperson

Lingjia Liu

Erik Perrins

Shannon Blunt

Tyrone Duncan

Date defended:

The Dissertation Committee for Ghaith Shabsigh certifies
that this is the approved version of the following dissertation :

Covert Communications in the RF Band of Primary Wireless Networks

Victor S. Frost, Chairperson

Date approved:

Abstract

Covert systems are designed to operate at a low probability of detection (LPD) in order to provide system protection at the physical layer level. The classical approach to covert communications aims at hiding the covert signal in noise by lowering the power spectral density of the signal to a level that makes it indistinguishable from that of the noise. However, the increasing demand for modern covert systems that can provide better protection against intercept receivers (IRs) and provides higher data rates has shifted the focus to the design of Ad-Hoc covert networks (ACNs) that can hide their transmission in the RF spectrum of primary networks (PNs), like mobile networks. The early work on exploiting the RF band of other wireless systems has been promising; however, the difficulties in modeling such environments, analyzing the impact on/from the primary network, and deriving closed form expressions for the performance of the covert network have limited the work on this crucial subject.

In this work, we provide the first comprehensive analyses of a covert network that exploits the RF band of an OFDM-based primary network to achieve covertness. A spectrum access algorithm is presented which would allow the ACN to transmit in the RF spectrum of the PN with minimum interference. Next, we use stochastic geometry to model both the OFDM-based PN as well as the ACN. Using stochastic geometry would also allow us to derive closed-form expressions and provide a comprehensive analysis for two metrics, namely an *aggregate metric* and a *ratio metric*. These two metrics quantify the covertness and performance of the covert network from the perspective of the IR and the ACN, respectively. The two metrics are used to determine the detectability limits of an ACN by an IR.

The two metrics along with the proposed spectrum access algorithm will be used to provide a comprehensive discussion on how to design the ACN for a target covertness level, and analyze the effect of the PN parameters on the ACN expected performance. This work also addresses the question of trade-off between the ACN covertness and its achievable throughput. The overall discussion and results in this research work illustrate the strong potential for using man-made transmissions as a mask for covert communications. In addition, some of our results can be directly used for other applications such as device-to-device (D2D) and vehicle-to-everything (V2X) communications.

Acknowledgements

I would like to express my deepest gratitude to my advisor Dr. Victor S. Frost for his great support and guidance during my Ph.D. studies. Truly, one of the kindest advisors anyone can have. I am also very thankful to Dr. Lingjia Liu for the invaluable knowledge I have learned from him personally, and the courses he taught. I am very grateful to Dr. Liu for sharing with me his remarkable industry experience.

I would like to thank my parents for their encouragement and for raising me to value and seek knowledge. Also, my deep gratitude goes to all of my brothers and my loving sister for their great support, assistance, guidance, and everything I learned from them. Thanks to all of my family, especially my cousin Jontie, for everything. To my family, you are the best!

Many thanks goes to Dr. Swapan Chakrabarti, and my friend Arunabha Choudhury for the phenomenal work we have done on HTS which have resulted in a patent application.

I would like to thank Dr. Erik Perrins, Dr. Shannon Blunt, and all of the other professors in the Electrical Engineering and Computer Science (EECS) department for the knowledge I have learned from them. I would like to thank all of my friends here at KU, especially Hao Chen, for the great discussions and nice times. Many thanks also to my great friend Mashhood Syed.

Last but not least, I would like to thank everyone at the EECS department, and the Information and Telecommunications Technology Center (ITTC) for their help. Thanks for the National Science Foundation (NSF) for the financial support for this work.

Page intentionally left blank.

Contents

Page intentionally left blank.

List of Figures

List of Symbols

Φ_B	Poisson Point Process for PN base stations
y_k	Location of the kth ACN user
x_i	Location of the ith PN user
v	Location of the IR
ρ	PN load
$g_{\mathrm{v},k}$	Channel between kth ACN user and IR
$r_{\mathrm{v},k}$	Distance between kth ACN user and IR
$g_{1,i}$	Channel between ith PN user and IR
$r_{1,i}$	Distance between ith PN user and IR
$g_{0,i}$	Channel between ith PN user and ACN receiver
$g_{0,i}$	Distance between ith PN user and ACN receiver
Φ_P	Poisson Point Process for PN users
$g_{\mathrm{c},k}$	Channel between kth ACN user and ACN receiver
$r_{\mathrm{y},k}$	Distance between kth ACN user and ACN receiver
α	Pathloss exponent
P_min	PN user minimum transmission power
P_max	PN user maximum transmission power
P_t	PN user target power at its serving base station
G_A	Aggregate metric
G_R	Ratio metric
Φ_C	Poisson Point Process for ACN users

λ_{P}	Density of the primary network users
λ_{B}	Density of the primary network base stations
λ_{C}	Density of the ACN users
η_s	ACN sensing threshold
σ	Noise Power
P_{c}	ACN user transmission power

Page intentionally left blank.

Chapter 1

Introduction

1.1 Background

This dissertation covers the topics of spectrum access and covertness of modern covert systems that can exploit the RF band of OFDM-based mobile wireless networks. Such covert systems use the radio transmissions of the mobile network as a mask to hide their signal and achieve low probability of detection. The work in this dissertation relies heavily on stochastic geometry for the analysis and the derivation of the covert network performance. Thus, we provide an introduction to covert communications as well as a brief introduction to the main stochastic geometry concepts that will be used here.

1.1.1 Covert Communications

Covert communications allow two or more parties to exchange information without being detected by an interceptor. This type of communication aims at hiding the transmission per se because if it is revealed, the safety of the transmitter or the integrity of the data being transmitted could be compromised. In this regards, covert communication is fundamentally different from encryption. In encryption [1], algorithms are used to convert data messages into codes that can be interpreted by authorized users only. Here, encryption does not protect against interception, and an eavesdropper is usually assumed to know that a transmission is taking place; however, without knowing the exact key to decrypt the data under transmission, the eavesdropper will be unable to interpret the conveyed data. In contrast, the purpose of covert communications is to keep the eavesdropper unaware of the transmission when it is taking place. This approach adds another layer to data protection.

There are several methods to exploit available transmission mediums and achieve covert communications, of those are the following:

- **Steganography** [2]: it is defined as the practice of concealing messages or information within other non-secret messages or data. An example of such a method includes altering pixels of an ordinary image or video in accordance to the letters or words of the ‘secret’ message without making this change noticeable to the eye.

- **Covert Channels**: the US DoD defines the covert channel as a communication channel that can be exploited by a process to transfer information in a manner that violates the system’s security [3]. Usually, this refers to adding bits to packet headers or even altering unused packet bits of certain services.

- **Wireless Covert Communications**: a wireless system aims at hiding its radio transmissions in noise [4], [5] or interference to achieve a low probability of detection (LPD) by an intercept receiver (IR).

Wireless covert systems have been in use for several decades and many of the techniques that were developed to achieve LPD have found their way to commercial applications. Since the early days of wireless communications, several LPD techniques have been introduced to hide the transmission of information over wireless channels. Traditionally, covert systems have used spread spectrum [6] as the main method for hiding transmission over noisy channels. This method changes the transmission frequency and/or time in order to spread the power spectral density of the transmitted message and make it indistinguishable from the noise [4]. The three main spread spectrum techniques are [6]: frequency hopping, time hopping, and direct sequence. Another covert technique that is suggested to achieve covertness is presented in [7]. The authors showed that using a wavelet-like waveform makes the covert signal look like noise and, consequently, increases its LPD.

To counter these covert techniques, several detection methods have been proposed, and the decision to select one of them depends on how much information is known about the signal to be detected, i.e., carrier frequency, waveform, symbol rate. The most commonly used detection methods are:

- **Enegry Detectors** (ED): energy detection methods are considered the simplest methods to detect signals. An energy detector monitors a portion of the spectrum for a specific amount of time, and compares the received energy to a threshold to decide whether a signal is present or not. Energy detection methods do not utilize any prior knowledge of the signal to be detected, and various types of energy detectors are available [8] [6].

- **Matched filtering** (MF): this method is used when all or some of the signal parameters are known to the intercept receiver. This method is known as the optimum method [9] for signal detection as it gives the best performance even under relatively low SNR conditions.

- **Cyclostationary Detectors**: most modulated signals can be considered as cyclostationary signals for reasons such as, modulation, signal structure, or the insertion of cyclostationary pilots [10]. This means that some or all of the signal statistics are periodic. This periodicity can be exploited to detect the existence of signal transmission in a noisy environment [11], [12], and even classify it according to its modulation type [13]. The advantage of this detection method is that, contrary to MF, does not require an exact knowledge of all signal parameters, and contrary to ED, does not perform blind detection.

When detection is performed, metrics need to be used to quantify the covertness of the signal. In this regards, two metrics are widely used in traditional LPD systems: the intercept receiver's (IR) probability of detection, and its probability of false alarm. Regardless of the method to be used, the performance of the detection method relies on the time-bandwidth product of the IR as well as the signal-to-noise ratio of the covert signal.

The recent years have witnessed an increasing demand for new covert wireless systems that can achieve higher throughput, operate in more challenging environments, and can attain greater levels of covertness. Therefore, several covert systems that hide their signals in the RF transmission of other wireless systems have been suggested [14, 15]; however, very little theoretical work have been done on this subject.

OFDM-based wireless systems are good candidates for exploitation for covert communications. Those systems incorporate several innovative techniques such as Orthogonal Frequency Division Multiplexing (OFDM), Multiple Input Multiple Output (MIMO) antenna [16], higher order modulation, Hybrid Automatic Repeat Request (HARQ), and Automatic Modulation and Coding (AMC) to achieve high data rates and provide the flexibility to overcome channel variations and interference. These combined advantages make OFDM-based networks the preferred mobile wireless systems in most countries around the world for many years to come. However, these same advantages also open the door for researching the possibilities of exploiting these networks in the design of various ad-hoc networks (device-to-device (D2D) communications, covert systems [17], etc.).

This research work focuses on exploiting OFDM-based wireless systems for covert communications, and providing metrics to quantify the covertness and analyze the performance of the covert systems; an illustration of the covert network exploiting the RF band of an OFDM-based mobile network is provided in Figure 1.1. Here, an Ad-Hoc Covert Network (ACN) operates in the RF band of an OFDM-based primary network (PN). To minimize interference

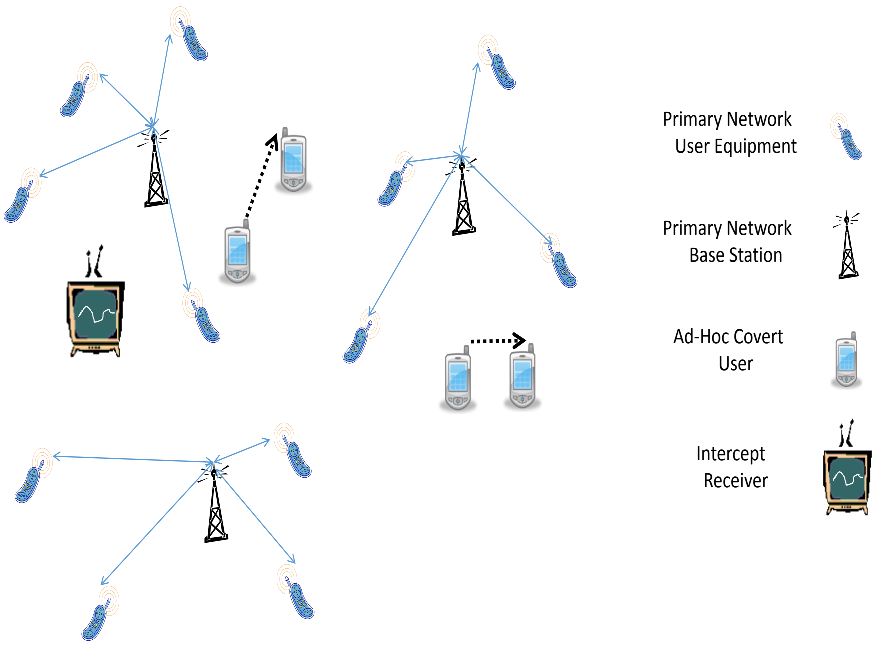

Figure 1.1: A covert network exploiting an OFDM-based multi user wireless network.

on/from the PN, the ACN users must opportunistically access the spectrum of the PN. An intercept receiver (IR) does not know if covert transmission is taking place; therefore, the IR must scan a wider bandwidth than the transmission bandwidth of an ACN user. In this research effort, we will use stochastic geometry to address the questions of the ACN achievable throughput as well as its covertness. Stochastic geometry has gained attention in the recent years because of the powerful tools it provides to model and analyze spatially distributed, multi-user, dynamic networks. Therefore stochastic geometry will be used as the main tool to build the system model and analyze the performance of the covert network.

1.1.2 Stochastic Geometry

Stochastic geometry [18] is a statistical method that provide models and methods to analyze the complicated geometrical patterns that occur in many areas of science such as physics, biology, and most recently wireless communications. Geometrical patterns can be frequently concerned with studying irregular patterns of collection of points in time and/or general, high dimensional spaces; therefore, the theory of point processes is a closely related and an integral part of the subject of stochastic geometry.

In order to mathematically define a point process, the following basic definitions are required:

- A set $\mathcal{X}$ is a collection of mathematical objects x_i that are taken from a suitable domain; that is $x_i \in \mathcal{X}$ for $i = 1, 2, \ldots$
- A σ-algebra is a system $\mathcal{X}$ of subsets of some set X and satisfy three conditions [18]:

$$\begin{aligned}&X \in \mathcal{X};\\&\text{if } A \in \mathcal{X}, \text{ then } A^{\mathrm{c}} \in \mathcal{X};\\&\text{if } A_1, A_2, \ldots \in \mathcal{X}, \text{ then } \bigcup_{k=1}^{\infty} A_k \in \mathcal{X}\end{aligned}$$

- The class of Borel sets $\mathcal{B}^{\mathrm{d}}$, is the smallerst σ-algebra on $\mathbb{R}^{\mathrm{d}}$ that contains all the open subsets of $\mathbb{R}^{\mathrm{d}}$.
- A function $f : X \longrightarrow \mathbb{R}$ is measurable if for each Borel set $B \in \mathcal{B}$, $f^{-1}(B) \in \mathcal{X}$

Formally, we can define a point process (PP) Φ as [18] a measurable mapping of a probability space $[\Omega, \mathcal{A}, \mathbb{P}]$ into a measurable space $[\mathbb{N}, \mathcal{N}]$:

$$\Phi : \Omega \longrightarrow \mathbb{N} \tag{1.1}$$

where $\mathbb{N}$ is the family of all sequences ϕ of points of $\mathbb{R}^{\mathrm{d}}$ [18], and $\mathcal{N}$ is its σ-algebra. Here, this mapping results in a distribution of the PP. Figure shows several examples of realizations of different types PPs in two dimensional space.

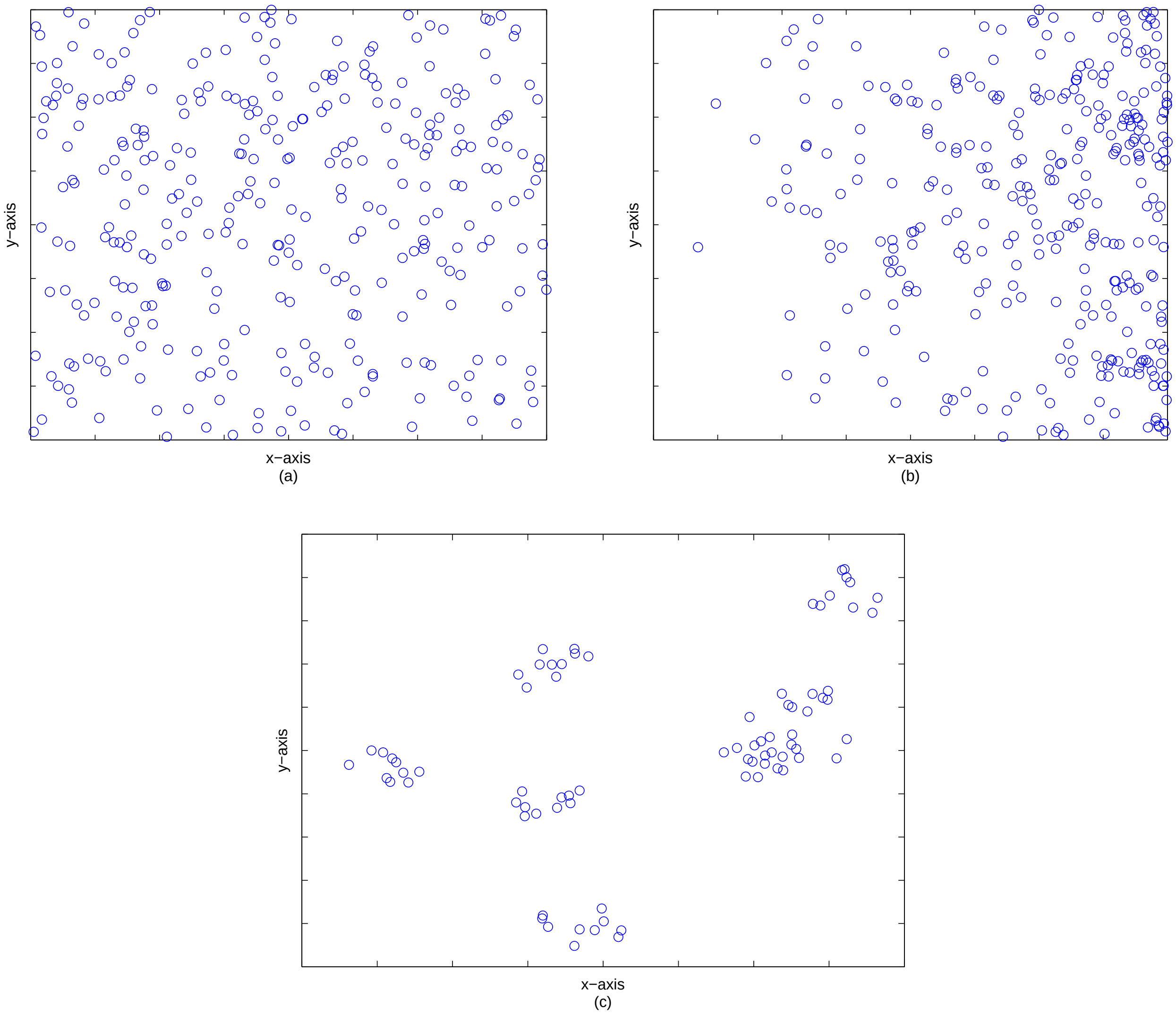

Figure 1.2: Examples of realizations of three types of point processes. (a) is an example of a Poisson point process, (b) shows an example of a point process with gradient in the horizontal direction, and (c) is an example of a Poisson cluster point process.

For any PP $\Phi = \{x_i\}$, the notation $\Phi(B)$ refers to the number of points in the set B, while the notation $x_i \in \Phi$ means that a point at location x belongs to the PP Φ. In addition, any PP can have other properties which can be summarized as follows [18]:

- Stationary point process: a PP is said to be stationary if its characteristics are invariant under shift; that is, the characteristics of $\Phi = \{x_i\}$ and $\Phi = \{x_i + y\}$ are the same.
- Intensity measure: an intensity measure, $\Lambda(B)$, of a PP in a given set B is defined as the average number of points in the set B:

  $$\Lambda(B) \triangleq \mathbb{E}[\Phi(B)] \tag{1.2}$$

  where the expectation is with respect to the different realizations ϕ of the PP.
- Density of a PP: the density, or intensity as some might use, of a PP Φ over a set B is related to the intensity measure of the PP as follows:

  $$\Lambda(B) = \int_B \lambda(x)\, dx \tag{1.3}$$

  If the PP is stationary, then the density $\lambda(x)$ can be written as:

  $$\lambda = \Lambda(B)/v(B) \tag{1.4}$$

  where $v(B)$ is the d-dimensional volume of B.

There are numerous types of models that can be used to capture the randomness of a PP, such as Binomial PP (BPP), Poisson PP (PPP), Poisson cluster process (PCP), etc. Here, a short description of the main types of PPs is provided.

- Binomial PP (BPP): This PP can be considered as the simplest type. For a bounded region $B \subset \mathbb{R}^{\mathrm{d}}$, the number of point is a fixed number, and the points are randomly and uniformly distributed in the given region. Since the number of points in B is fixed, the number of points in disjoint subsets is dependent. The number of points in a subset A of B is a Binomial random variable that depends on the volume of both A and B. This property makes it difficult to analyze BPP and derive closed-form expressions.

- Poisson PP (PPP): As in the BPP, the location of the points in a bounded region B is randomly and uniformly distributed; however, in a PPP, the number of points in the region B is a random variable of a Poisson distribution with mean $\Lambda(B)$:

  $$\mathbb{P}[\Phi(B) = k] = \frac{\Lambda(B)^k}{k!} \exp(-\Lambda(B)) \tag{1.5}$$

  One of the most important properties of a PPP is that the number of points in disjoint regions are independent random variable. This property simplifies the analysis of the PP and can lead to easier derivation of closed-form expressions. If the PPP is stationary, then $\lambda = \Lambda(B)/|B|$, and the whole distribution of the PP can be determined once the value of λ is known [18]. Here, λ can be understood as the average number of points in unit d-dimensional volume. Figure 1.2(a) shows a realization of a stationary PPP of density $\lambda = 5 \times 10^{-6}$.

  If the PPP is conditioned to have a fixed number points in a region B, then the PPP is reduced to a BPP. A PPP has other important properties that will prove useful for modeling and analyzing covert systems. A thinning of a PP occurs when each point of the process is independently and randomly removed by a probability of ρ. In PPP, the thinning of a stationary PPP Φ of density λ, results in another PPP Φ_ρ of density ρ. Another important property is that the super position of two stationary PPP of densities λ_1 and λ_2 results in a new PPP of density $\lambda = \lambda_1 + \lambda_2$.

- Poisson Cluster Process (PCP): This type of PP starts with a PPP Φ_{p}, also called a *parent process*, of density λ_{p}. Then, each point $x_i \in \Phi_{\text{p}}$ gives rise to a finite set of points, *daugh-*

ter points, according to some distribution. Finally, all the *daughter points* forms a new point process which will be a PCP. A realization example of such process is illustrated in Figure 1.2(c).

There are also other types of point processes such as Cox PP, repulsive PP, etc.; however, this work only focuses on the PPP because of its close relation to the distribution of wireless transmitters. In addition, the use of stationary PPP makes it possible to obtain well compact expressions that can be used to analyze and have an in-depth understanding of the behavior and performance of wireless systems.

Stochastic geometry provides powerful tools to model the distribution of wireless transmitters, and analyze the performance of wireless networks in the presence of interference. In fact, stochastic geometry has been used to derived closed-form expressions for the signal-to-noise-and-interference ratio (SINR), outage capacity, and nearest neighbor of wireless users in the presence of interference [19]. In such system models, the intended receiver is considered as a point of the PP, while the remaining points are considered as interferers. In order to analyze the performance at a specific, i.e., typical, point of the PP, it is possible to use Palm distribution in order to condition the PP Φ to have a point at a specific location x; that is $\Phi \setminus \{x\}$. In case the effect of the point on itself needs to be ignored, the reduced Palm distribution is used. The analysis of interference at a specific point x of the PP is an example where the reduced Palm distribution becomes handy, because of the absence of self interference in most practical scenarios.

Although using Palm and reduced Palm distribution might appear at first to complicate the analysis of wireless systems, there are many cases where the analysis produces tractable results. For example, Palm and the reduced Palm distributions are easily applied to stationary PPPs. In this case, it has been shown, through Mecke-Slivnyak theorem [20] and other work, that the reduced Palm distribution reduces to a PPP which makes it possible to use all the PPP properties to study a specific point.

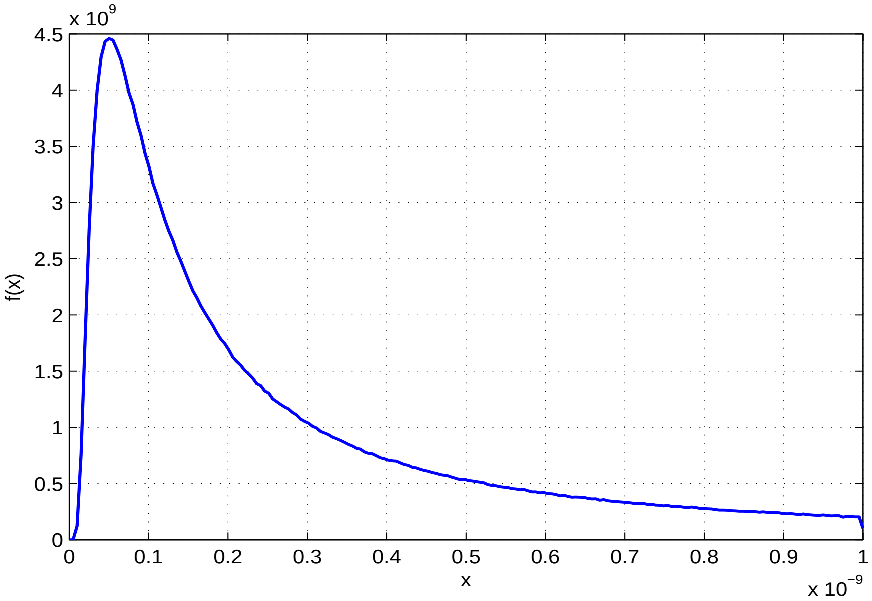

Figure 1.3: The probability density function (pdf) of interference from wireless transmitters that are distributed according to a PPP of density $\lambda = 5 \times 10^{-6}$. The signal from the wireless transmitters experiences small scale Rayleigh fading, i.e., exponential channel gain of unit mean, and large scale pathloss of parameter $\alpha = 4$. Clearly, the pdf cannot be approximated by a Gaussian distribution.

As previously mentioned, stochastic geometry has been successfully applied in the field of wireless communications to study interference. Two main observations are of particular importance. The first observation is that the interference coming from randomly distributed wireless transmitters, that experience Rayleigh fading and pathloss, can not be approximated by a Gaussian distribution [18]; as shown in Figure 1.3. The second observation is that interference from nearby transmitters contribute more than those at a farther distance. This important case gives rise to what is known as *local spectrum opportunities*. When a *local spectrum opportunity* is available, the interference is said to be below a specific threshold because either the interferers are located at a further distance from the typical user that is under analysis, or the channel gains between the interferes and the typical user are low. This allows the typical user to exploit the RF channel to transmit or receive data. This concept has been used in device-to-device (D2D) communications as well as cognitive radios.

1.2 Related Work

The problem of hiding a covert signal in noise to achieve LPD communication is a very well investigated subject [6], [21], [4]. Spread spectrum techniques, such as frequency hopping and direct sequence, were initially developed for LPD communications before they found their way to commercial applications. In the same context, various types of detection methods, and covert metrics have been developed to detect the covert transmission and determine the detection performance. Wideband energy detectors, such as channelized radiometers [6], scan a wide bandwidth for a period of time and measure the collected energy to determine the presence of covert transmission. In [22], the performance of energy detection is investigated when different assumptions on the noise variance are made. This work considers a case where the noise power spectral density is constant but unknown, and another case where the noise power is fluctuating.

The detectability of cooperative wireless communication networks is addressed in [23], where two metrics are used to evaluate the LPD performance. The first metric is the distance ratio between the transmitter and intended receiver and the minimum distance between all the interceptor and transmitter pairs. The second metric is the ratio between the average distance between all interceptor and transmitter pairs and the transmitter and intended receiver distance.

On the other hand, the detectability of covert signals using distributed sensors is investigated in [24]. Here, M intercept receivers try to detect the presence of the covert signal by taking N samples each and sent to a fusion center for processing. The processing center performs a GLRT detection on the received samples to make a decision on the presence of a signal. The performance of the detector was only studied for specific assumed locations for the intercept receivers, and no work was provided to address the random distribution of the receivers.

Although the probability of detection and probability of false alarm of an intercept receiver are widely used to quantify the LPD properties of covert systems, other metrics have also been proposed. The authors in [25] analyze the detection of communications signals by an energy detector and use the ratio of the distance from the transmitter to the radiometer and the intended receiver as a metric for quantifying the LPD characteristics of the system. Another metric is proposed in [26] that uses the ratio between the covert signal signal-to-noise ratio (SNR) at the intended receiver, and that at the intercept receiver. This metric takes into account several parameters such as the propagation loss, and the antenna gain of the covert transmitter, the covert receiver, and the intercept receiver. Similar to other work, a specific network topology was assumed in order to analyze the metric instead of deriving the performance for any random configuration.

Other existing work, such as [27–29] has focused on different aspects of covert communications in noisy channels. In [27], the theoretical limit of classical LPD methods, such as spread spectrum, is investigated. The authors main premise is that this theoretical limit has not been previously investigated; therefore, an information theoretic approach is used to find the amount of information that can be reliably transmitted over additive white Gaussian noise (AWGN) channels. In [27], the authors use mutual information between the covert transmitter and receiver, as well as between the covert transmitter and the eavesdropper in order to demonstrate that $o(\sqrt{n})$ bits can be exchanged between the covert transmitter and receiver during n channel uses while lower bounding $\alpha+\beta \geq 1-\epsilon$; where α and β are the IR probability of false alarm and missed detection, and ϵ is an arbitrary value [27]. The authors mention that their work can be related to a scenario where the LPD system operates in the presence of a primary network, in which, some of the users are eavesdroppers; however, they acknowledge that this is still an open area for research.

The work in [28] provides a conceptual analysis on some fundamental limits on the detectability of covert systems in noisy channels. This paper emphasizes the work done in [27], and provides a future vision on how to increase the LPD of a wireless covert system through the introduction of intentional jammers. Those jammers, as they suggested, would act as an additional source of AWGN noise at an IR; however, the analysis in [28] only focused on limits of covert rate in the presence of channel noise only, and no analysis is presented for the case where jammers are present. In contrast to [28], this work effort uses the radio transmission of the users of a primary network as a source of non-Gaussian interference to further hide the covert signal. Finally, [29] analyzes the detectability of a network of LPD users, and takes the SNR ratio of the covert signal at the covert receiver and that at the IR as a metric to quantify the covertness of the system. Due to the complexity of the proposed system model, only a numerical example is provided to illustrate the achievable covertness.

There are also a few papers that have touched on the subject of introducing artificial noise in the RF environment increase covertness. For example, in [30], it was shown that by having a node close to the intercept receiver which transmits artificial noise, a significant improvement in the throughput of the covert system can be achieved even without a close coordination between the transmitter and the interfering node. This work also takes into account the presence of multiple intercept receiver. However, the main drawback of this approach is the very concept of introducing intentional interferers to mask the covert signal. From an intercept receiver's perspective, knowing that noise sources are active could strongly indicate that a covert transmission is already talking place. Additionally, even if this method works for certain scenarios, it is infeasible for most realistic covert communication cases.

More recently, new covert techniques that exploit existing man-made transmissions have also been proposed. The authors in [14] provide a method to hide a covert transmission in the backscatter of radar pulses. In [31] and [32], the backscatter from radar pulses is shown to increase the interference at the IR with minimum impact on the radar operation as well as the covert system itself. The metric that was used to quantify covertness is the ratio between the signal-to-interference-plus-noise ratio (SINR) at the intended covert receiver and that at an IR.

Another approach that has been proposed to exploit the transmission of existing networks for covert communications is introduced in [17], [15], and [33]. The authors in [17] propose an Ad-Hoc covert network (ACN) that achieves LPD by accessing the spectrum of an OFDMA-based primary network (PN), like LTE. Here, the ACN transmits in the guardband of the RF spectrum of the PN to maintain minimum interference on the PN. At the same time, the transmission of the PN acts as an interference source at an IR and, consequently, decrease the detectability of the ACN. In [15], and [33], an analysis is presented on the impact of the ACN on an OFDM-based PN. The interference from the ACN on the PN bit error rate, frame error rate, as well as the different layers of the stack protocol is thoroughly analyzed.

1.3 Problem Statement

An examination of the most recent work on covert systems, it can be noticed that there is no existing work on quantifying neither the covertness nor the achievable throughput of similar ACNs. The reason for this is related to the difficulty of modeling such a scenario and deriving a closed-form expressions for corresponding suitable covert metrics [29]. In this work we will use stochastic geometry to address the questions of the ACN achievable throughput as well as its covertness.

The contributions in this research effort are summarized as follows:

- Present a spectrum sensing and power allocation algorithm that takes advantage of the OFDM nature of the PN signal that the ACN is exploiting for covert transmission. This algorithm takes into account the ACN transmission strategy to achieve covertness.

- Define a metric, namely the *aggregate metric*, to quantify the covertness of the ACN from the perspective of the IR. Then use stochastic geometry to derive a closed-form expression for this metric.

- Define a metric, namely the *ratio metric*, that quantifies the performance from the perspective of each ACN link. Using stochastic geometry, we derive a lower bound for this metric to take into account a worst case scenario from the perspective of the ACN.

- Provide an in-depth analysis of the ACN performance in terms of covertness and achievable throughput, and present a detailed description on how to design the ACN and select its main parameters.
- Develop a framework to analyze the trade-off between throughput and covertness for the ACN.

1.4 System Model

The system model is comprised of an OFDM-based primary network (PN) of multiple base stations and multiple mobile users, an Ad-Hoc covert network (ACN) that opportunistically exploits the RF spectrum of the PN to achieve LPD, and an intercept receiver that searches for the presence of the ACN by scanning the RF spectrum of the PN. An illustrative example of the system model is provided in Figure 1.4.

1.4.1 Wireless Primary Network

The PN is assumed to be a mobile wireless network with a number of base stations and a number of primary users that connect to the base stations on the PN uplink channel. The location distribution of the base stations is assumed to be a homogeneous Poisson point process (PPP) [18], $\Phi_{\mathrm{B}} = \{z_j \in \mathbb{R}^2; j = 1, 2, ...\}$, of intensity λ_{B}. The network spectrum is divided into a number of frequency resources, which we will refer to as Resource Blocks (RBs), and those resources are assigned to the PN users in a slotted manner for T seconds. The PN users belonging to the same base station communicate with their serving base station using orthogonal resources. The location distribution of the PN users is assumed to follow an independent PPP, $\Phi_{\mathrm{P}} = \{x_i \in \mathbb{R}^2; i = 1, 2, ...\}$, of intensity λ_{P}. We assume the PN users have a minimum and maximum transmission power, denoted as $P_{\min}$, and $P_{\max}$, respectively, and connect to their nearest base station, i.e., to the base station of the smallest pathloss. Unless the minimum or the max-

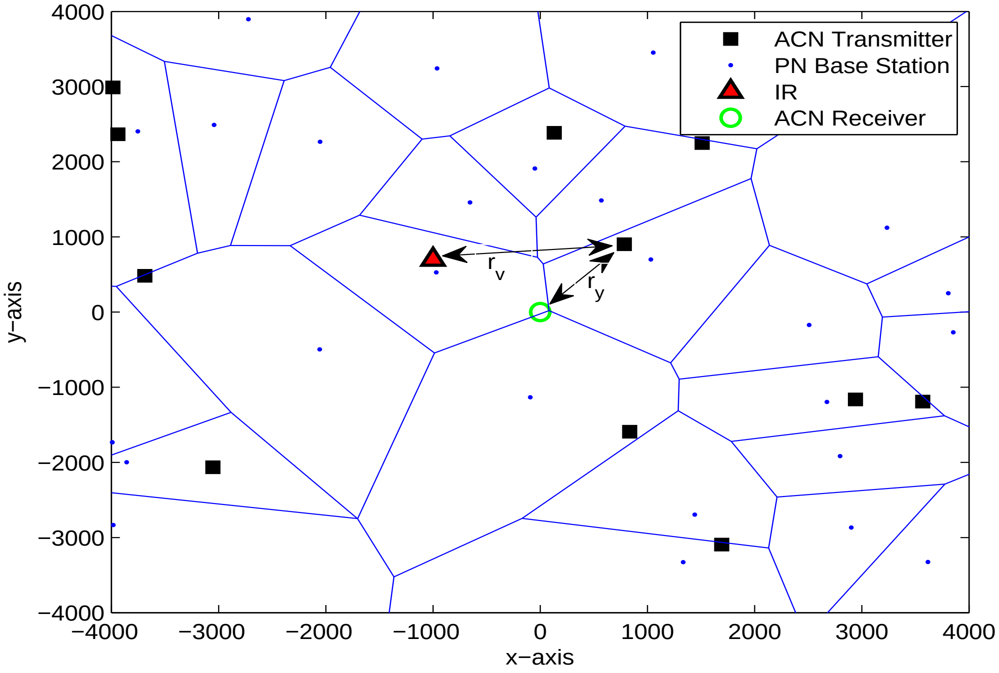

Figure 1.4: The figure shows a realization of a PPP of the distribution of the PN base stations and their Voronoi cells. It also shows a realization of the PPP of the ACN transmitters. The IR is randomly located in $\mathbb{R}^2$, and tries to detect if any covert activity is taking place.

imum transmission power is exceeded, each PU transmits at a power level that compensates for its pathloss to its serving base station and tries to achieve a target received power of P_{t}. Finally, due to channel variations and the scheduling algorithm of the PN, we assume that any PN base station's RB could be left unoccupied with a probability of $1-\rho$ could be occupied with a probability of ρ. Therefore, $\rho = 0$ means that all the PN RBs are always empty, which is equivalent to saying that there is no PN.

1.4.2 Ad-Hoc Covert Network

The ACN is a covert network of a number of Ad-Hoc transmitters that exploit the uplink channel of the PN in order to hide their transmission. We assume the distribution of the ACN users follows a homogeneous PPP, $\Phi_{\mathrm{C}} = \{y_k \in \mathbb{R}^2; k = 1, 2, \ldots\}$ of intensity $\lambda_{\mathrm{C}} << \lambda_{\mathrm{P}}$, and each ACN user senses the RBs of the PN and decides to transmit at power P_{c} only when it finds an empty RBs; the ACN users could be communicating with each other or with a central unit located at the origin $o \in \mathbb{R}^2$; any discussion on MAC protocols is beyond the scope of this paper and is left for future work.

It is known that sensing is not accurate and depends on the chosen receiver operating characteristic (ROC) point; therefore, an ACN user will occasionally incorrectly transmit in a PN RB that is actually occupied by a PN user, which will cause interference on/from the PN users belonging to all the base stations that happened to be occupying the same RB; those PN users are represented by $\Phi_\delta \subset \Phi_\mathrm{P}$. We denote the probability of this event, i.e., sensing a RB is empty although it is occupied by a PN user, as $\pi_\mathrm{e} = (1 - \mathrm{P_d})\rho$; where $\mathrm{P_d}$ is the ACN probability of sensing a PN resource as occupied. We also denote the probability that the ACN correctly senses and transmits in a PN frequency resource as $\pi_\mathrm{s} = (1 - \mathrm{P_{fa}})(1 - \rho)$; where $\mathrm{P_{fa}}$ is the probability of false alarm of the ACN sensing method. It is important to keep in mind that $\pi_\mathrm{s} + \pi_\mathrm{e} \neq 1$ because we need to take into account that the ACN refrains from transmitting if it does not find empty PN RBs.

1.4.3 Intercept Receiver

The IR is located at $v \in \mathbb{R}^2$, and aims at detecting the presence of ACN transmission. However, because of the random behavior of the PN and the random position of the ACN users, IR cannot know *a priori* the frequency resources that the ACN plans to use, nor its transmission strategy, and therefore, we focus on the case where the IR must monitor the entire PN spectrum; extending this work to other cases is straight forward.

1.4.4 Channel Model

The channel between any transmitter and any receiver is subject to both small scale Rayleigh fading, i.e., exponential channel gain distribution of unit parameter, as well as large scale pathloss of pathloss exponent $\alpha > 2$. We denote the channel gain between the kth ACN user and the IR as $g_{\mathrm{v}k}$. We also donate the channel between the ith PU and the IR as g_{1i}, and between the ith PN user and the ACN receiver as g_{0i}.

Chapter 2

Exploiting the Spectrum of Primary Wireless Networks

2.1 Key Points of the Chapter

In this chapter, we discuss how an ACN user accesses the spectrum of the PN. In concept, the ACN user can either blindly transmit in the RF band of the PN or use sensing to determine which frequency resources are available at the time of its transmission. The former option introduces significant interference on/from the PN because the ACN user will very often transmit in PN resources that are being used by PN users. The later option is more suitable for the operation of the ACN because the ACN user needs to sense the PN resources and transmit only in those that will be found as empty. In this case the interference on the PN will be reduced.

2.2 Introduction

To address the question of the ACN achievable throughput, an ACN user is assumed to perform spectrum sensing to find potentially PN empty frequency resources. Then the ACN user will transmit in a subset of the empty resources at a certain power so that it maximizes its throughput and minimizes its interference on the PN. For this purpose, an ACN spectrum sensing and power allocation algorithm that takes advantage of the OFDM nature of the PN will be presented.

Spectrum sensing is a topic that has been very well investigated in the context of cognitive radios [34]. This available work mostly considers sensing a PN of a single or multiple bands where each band is occupied by a single PN transmitter. Those transmitters are assumed to transmit at a constant power for a long transmission period, which allows a cognitive radio to easily filter the PN signal and perform spectrum sensing in the time domain. However, because of the nature of the OFDM signal where the subcarriers have relatively narrow bandwidth, and different subcarriers are occupied by users that are transmitting at different power levels, time domain sensing of multiple subcarriers in a relatively short period of time is inefficient and computationally expensive. Also no work has been done on sensing the spectrum of PNs of multiple users and base stations. Therefore, for the covert communications model at hand, it is more practical to take advantage of the OFDM nature of the PN signal, where symbols are mapped onto orthogonal subcarriers, to perform sensing in the frequency domain.

The remainder of this chapter is organized as follows: Section 2.3 discusses how sensing in the frequency domain is more practical to determine which PN resources are empty. This section also discusses the three possible options to choose the ACN user sensing threshold. In Section 2.4, the performance of the sensing stage is discussed.

2.3 Spectrum Exploitation

If the ACN blindly transmits in the RF spectrum of the PN, excessive interference would be incurred on/from the PN. Therefore, an ACN that needs to operate in the RF band of a PN must choose *suitable* resource blocks for transmission. Since the ACN needs to stay covert as well as Ad-Hoc, no information on the empty RBs would be exchanged between the PN and the

ACN; therefore, the ACN users must perform spectrum sensing and transmit at a power level that guarantees minimum interference and detection.

As illustrated in Fig. 2.1, the PN resource grid is divided into resource blocks and each resource block is divided into P subcarriers in the frequency domain and multiple OFDM symbols in the time domain. We can take advantage of the subcarriers in a resource block for sensing if the sensing time, τ, is made equal to the duration of one, or an integer multiple of one, OFDM symbol. Lets assume the ACN user senses the PN spectrum by collecting L samples for the duration of one OFDM symbol, then using L-point discrete Fourier transform on the time-domain PN received signal, the vector of the PN received symbols, $\mathbf{Y}$, in the frequency domain is given as:

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{Y} = \mathbf{W}\,\mathbf{z} && = \mathbf{Z}, \\ \mathcal{H}_1 &: \mathbf{Y} = \mathbf{W}\left(\sum_{i=1}^{|\phi_{\mathrm{P}}|} \mathbf{s}_i + \mathbf{z}\right) && = \mathbf{S} + \mathbf{Z}, \end{aligned} \tag{2.1}$$

where small letter and capital letter symbols represent vectors of samples in the time and frequency domains, respectively. $\mathbf{W}$ is the $L \times L$ DFT matrix, and $\mathbf{z}$ is an $L \times 1$ vector of i.i.d. circularly symmetric complex Gaussian noise samples of known variance $\mathcal{CN}(0, \sigma^2)$, with real and imaginary parts of $\mathcal{N}(0, \sigma^2/2)$. ϕ_{P} is the realization of the point process Φ_{P} of the PN users who exist during the ACN sensing period, and $|\phi_{\mathrm{P}}|$ is its cardinality. $\mathbf{s}_i$ is an $L \times 1$ vector representing the received OFDM signal of the ith PN user. When DFT is performed on the received time-domain PN signal, the result is a vector of either noise $\mathbf{Z}$ or noise and PN symbols $\mathbf{S}$. It is known that only the PN users belonging to the same base station are scheduled on different RBs; therefore, any element S_l of the vector $\mathbf{S}$ will be the summation of the received symbols from all the PN users $x_i \in \phi_{\mathrm{P}}$ that belong to different PN base stations and happen to occupy the same OFDM subcarrier. That is $S_l = \sum_{k=1}^{|\phi_{\delta,l}|} S_{l,k}$, where $\phi_{\delta,l}$ is the point process realization of the PN users that are transmitting on the lth OFDM subcarrier.

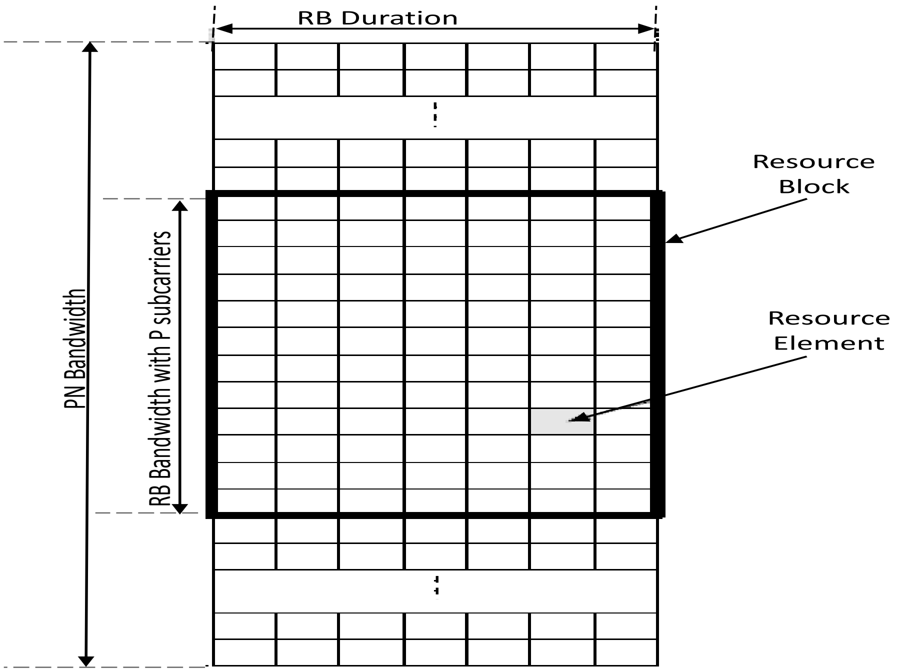

Figure 2.1: An illustration of one PN resource block (RB). The RB contains P subcarriers in the frequency domain and a number of OFDM symbols in the time domain.

Any PN user occupies P adjacent subcarriers that are grouped in a RB; therefore, an ACN user can use all the subcarriers in a RB for sensing. In this case, we can define the test statistic for the nth RB to be the summation of energy in all the subcarriers in that RB, that is:

$$V_n = \sum_{l=nP+1}^{P(n+1)} \left| \frac{Y_l}{\sigma} \right|^2 . \tag{2.2}$$

The ACN receiver compares this test statistic to a threshold η_s and determines whether the corresponding RB is occupied. All the available RBs, i.e., found as unoccupied, will then define a set $\mathcal{A} = \{n : V_n \leq \eta_s,\ n = 0, \ldots, N-1\}$ of RBs that can be used for transmission by the ACN network. The test statistics under analysis can now be formulated as a binary hypothesis testing problem for each RB:

$$\begin{aligned} \mathcal{H}_0 : V_n &= \sum_{l=nP+1}^{P(n+1)} \left| \frac{Z_l}{\sigma} \right|^2, \\ \mathcal{H}_1 : V_n &= \sum_{l=nP+1}^{P(n+1)} \left| \frac{S_l + Z_l}{\sigma} \right|^2, \end{aligned} \tag{2.3}$$

where S_l is the PN received symbol on the lth subcarrier. We notice that $|Z_l/\sigma|$ has a Rayleigh distribution with parameter $\sigma = 1$, while $|(S_l + Z_l)/\sigma|$ has a Rice distribution [35] with scale parameter $\sigma = 1$ and noncentrality parameter of $|S_l/\sigma|$. Under $\mathcal{H}_0$, the test statistic V_n has a Gamma distribution [36] with shape parameter P and scale parameter of 2, that is:

$$f(V_n \mid \mathcal{H}_0) \sim \Gamma(P, 2), \tag{2.4}$$

Under the alternative hypothesis $\mathcal{H}_1$, the test statistic is the sum of P Rice squared random variables which results in a non-central chi-squared distribution [36] with $2P$ degrees of freedom and noncentrality parameter λ_n, that is:

$$f(V_n \mid \mathcal{H}_1) \sim \chi^2_{2P}(\lambda_n), \tag{2.5}$$

Using the P available subcarriers in each RB, the non-centrality parameter can be written in terms of the PN signal-to-noise ratio on the nth RB, θ_n, as follows [36]:

$$\begin{aligned} \theta_n &= \frac{1}{P} \sum_{l=nP+1}^{P(n+1)} \frac{|S_l|^2}{\sigma^2} = \frac{\lambda_n}{P} \\ \Rightarrow \lambda_n &= P\theta_n \end{aligned} \tag{2.6}$$

The probability of false alarm, and the probability of correct sensing [36], at a target PN

SNR, on the nth RB becomes:

$$\begin{aligned} P_{fa}^{(n)} &= \int_{\eta_s}^{\infty} f(V_n \mid \mathcal{H}_0)\, dV_n = 1 - F_{V_n|\mathcal{H}_0}(\eta_s) \\ &= 1 - \frac{\gamma(P, \eta_s/2)}{\Gamma(P)}, \end{aligned} \tag{2.7}$$

$$\begin{aligned} P_{d}^{(n)} &= \int_{\eta_s}^{\infty} f(V_n \mid \mathcal{H}_1)\, dV_n \\ &= Q_P(\sqrt{\lambda_n}, \sqrt{\eta_s}) \end{aligned} \tag{2.8}$$

where $\gamma(.,.)$ is the lower incomplete Gamma function, and $Q_.(.,.)$ is the Marcum Q-function [37]. It should be noted that $P_d^{(n)}$ in (8) is for a specific realization of ϕ_p, i.e., specific PN SNR θ_n. Therefore, the average probability of correct sensing on the nth RB is found by averaging over the distribution of the PN SNR $f(\theta_n)$ as follows:

$$\hat{P}_d^{(n)} = \int_0^{\infty} Q_P(\sqrt{\lambda_n}, \sqrt{\eta_s}) f(\theta_n) d\theta_n \tag{2.9}$$

The integration in (2.9) cannot be expressed as a closed-form expression. The detection threshold can be set using the expression in (2.7), or the expression in (2.8) if a target θ_n is required, or even using the expression in (2.9) if an average probability of sensing is needed. In the rest of this paper, the value of the false alarm probability is used to set up the sensing threshold η_s to find the empty RBs. Choosing a high value for the false alarm probability will reduce the total throughput of the ACN, while choosing a small value for $P_{fa}^{(n)}$ will increase the interference on the PN. In order to extend the analysis to the case where k OFDM symbols are used for sensing, then the number of subcarriers per PN RB should be replaced by kP.

2.4 Exploitation Performance

In this section we first analyze the performance of the ACN frequency-domain sensing method. As discussed in the system model, the PN has a number of base stations and a number of users. The PN base stations and users are assumed to be distributed as a PPP of intensity $\lambda_{\mathrm{B}} = 10^{-5}\ \mathrm{BS}/m^2$, $\lambda_{\mathrm{P}} = 5 \times 10^{-5}\ \mathrm{PU}/m^2$, respectively. The PN spectrum is assumed to have a total bandwidth of 20MHz and is divided into sub-channels each of bandwidth 180KHz. Time is divided into slots of duration 10ms. Following the LTE standards [38], the PN user's minimum and maximum transmission power are chosen to be $P_{\min} = -40$dBm and $P_{\max} = 24$dBm, respectively. The ACN hides its transmission in the RF spectrum of the PN by choosing a sub-channel and a time slot for transmission. The sensing time and detection threshold are chosen so that $\mathrm{P}_{\mathrm{fa}} = 0.1$; this value will always be used unless otherwise specified.

Each RB is composed of $P = 12$ OFDM subcarriers in the frequency domain and seven OFDM symbols in the time domain. The time duration of the RBs is 0.5ms. In OFDM-based systems like LTE [38], each PN user is assigned 540KHz for the duration of $1ms$, i.e., a total of six RBs at each transmission cycle; however, the first three OFDM symbols cannot be used by the ACN for spectrum sensing as they are dedicated for transmitting PN control information. This leaves us with a total of $K = 11$ symbols for ACN sensing and transmission.

Now we can analyze the performance of the ACN sensing method. Figure 2.2 shows the performance of the proposed method when sensing is performed using one OFDM symbol out of the eleven available. We notice that the sensing method has a high performance even for low PN SNR values at the ACN. This property of the sensing method, i.e., high probability of detection at a low PN SNR value, is very important because it allows the ACN to find the empty RBs more accurately which reduces the interference on the PN.

Figure 2.3 shows the complementary cumulative distribution function (CCDF) of detecting N unoccupied RBs when only one OFDM symbol is used for sensing. The figure shows several curves representing different channel pathloss models. The target probability of false

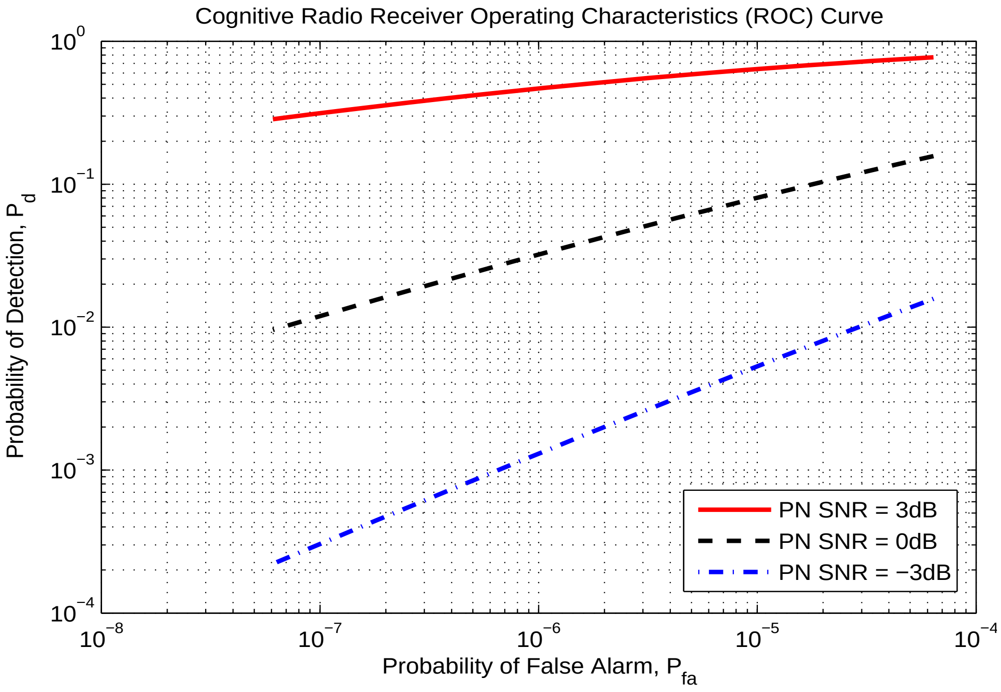

Figure 2.2: The probability of false alarm as a function of the ACN sensing threshold.

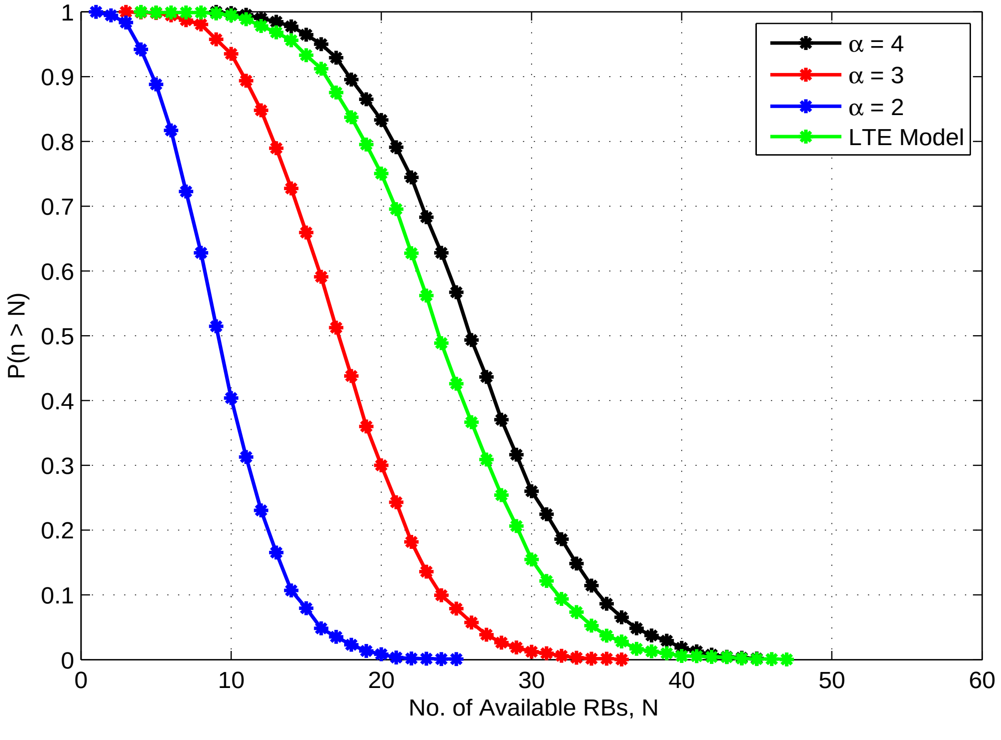

Figure 2.3: The complimentary distribution function of the number of PN RBs that can be found empty by the ACN and can be used for covert transmission. The curve related to the channel model provided by LTE standards is close to the curve of $\alpha = 4$.

alarm is set at 10^{-3}. Figure 2.3 shows the probability of available RBs when the ACN-RX is randomly located at a spatial location in the coverage area of the PN. Clearly, as the value of the pathloss exponent, α, increases, the number of RBs that are sensed as available by the ACN increases as well. This is because the amount of energy received from the PN users at the ACN becomes lower due to higher pathloss. In this figure, we use for comparison the channel pathloss model that is used in the LTE standards [18]. We notice that the corresponding CCDF curve is very close to the curve where $\alpha = 4$; which is the value we used throughout this paper for our analysis. This means that our work and the derived metrics are applicable for practical implementation.

Chapter 3

Quantifying Covertness and Performance of the ACN

3.1 Key Points of the Chapter

In this chapter, we use stochastic geometry to develope and provide a comprehensive analysis for two metrics. The *aggregate metric* is used to quantify the covertness of the ACN from the perspective of the IR, while the *ratio metric* quantifies the covertness and performance from the perspective of the ACN users. The metrics are used to determine the detectability limits of the ACN by an IR, and the advantages of using interference, instead of noise, to increase covertness will be demonstrated. The performance of the *ratio metric* will be discussed under three different cases: noise-limited, interference-limited with perfect sensing of the environment, and interference-limited with imperfect sensing.

3.2 Introduction

To address the question of covertness of a network of Ad-Hoc users, we define and analyze two metrics that quantifies the covertness of the ACN from two different perspectives: the ACN, and the IR perspectives. In this context, we notice that regardless of the specific characteristics of the PN, and the detection method being used by an IR, a low SINR for the covert signal at the IR is a main factor in limiting the performance of the IR. Therefore, a question in the design of an ACN is how low the ACN SINR can be maintained at a desired distance for a given covert configuration and operating requirements. Two perspectives need to be considered in regards to the covertness of an ACN of multiple users. From the perspective of the IR, determining whether an ACN is active or a covert transmission is taking place is needed before attempting to localize the ACN transmitter; therefore, it can be said that covertness is achieved if the aggregate SINR, from all the ACN users exploiting a certain RF band, remains below some threshold. From the perspective of the ACN, the goal is to know whether each transmitter can achieve a target SINR at its intended receiver while maintaining a lower SINR at an IR that could be located at some distance away from the ACN transmitter. This discussion shows that the SINR from the collective ACN users is a suitable metric to quantify covertness at an IR; here, we define this metric as the aggregate metric. On the other hand, the ratio of ACN SINR at the intended ACN receiver to that at an IR is a useful metric to quantify covertness from the perspective of individual ACN users; we define this metric as the ratio metric. In this paper, we derive a closed-form formula for the aggregate metric and a lower bound on the ratio metric.

3.3 Covertness of a Network of Covert Users

As illustrated in Fig. 3.1, the first step for an IR is to determine if a covert transmission is taking place. Next it can try to localize one of the transmitters. The probability that the IR detect the ACN depends on various factors such as the detection method being used, the detection threshold, the time-bandwidth product of the IR, and the ACN SINR at the IR. Of these parameters, the ACN can can try to control its SINR to remain covert. In this sense, the communication of the ACN is considered covert if the IR fails to detect its presence with a certain probability, i.e., $\mathrm{P}_{\mathrm{det}} \leq \eta_1$, which is equivalent to saying that the aggregate SINR of the ACN users remains below a certain threshold with a certain probability, i.e., $\mathbb{P}[\mathrm{SINR}_{\mathrm{R}} \leq \eta]$. Since interference from the PN users is dominant in the RF environment, noise can be ignored. The *aggregate metric* is defined here as follows:

$$\mathrm{G}_{\mathrm{A}} = \frac{\sum_{y_k \in \Phi_{\mathrm{c}}} P_c \, g_{\mathrm{v}k} \, r_{\mathrm{v}k}^{-\alpha}}{\sum_{x_i \in \Phi_{\mathrm{p}}} P_i \, g_{1i} \, r_{1i}^{-\alpha}}, \tag{3.1}$$

where P_c is each ACN user's total transmitted power, $r_{\mathrm{v}k} = ||y_k - v||$ and $r_{\mathrm{v}i} = ||x_i - v||$ are the distance between the kth ACN user and the IR and between the ith PN user and the IR, respectively. This metric represents the total received power from all the ACN users to the total interference from all the PN users falling in the time-bandwidth product of the IR. Note that the lower the value of this metric, the better the covertness of the ACN. In fact, this metric is a random variable due to the variations in channel gains and the randomness in the location of both the ACN transmitters and the PN users. The following theorem finds the probability of this metric being less than an SINR threshold η.

The following corollary will prove helpful in the derivation of the CDF of the aggregate metric.

Corollary I: *The expected value of a typical PN user's transmitted power, given the transmission policy discussed in Chapter I, is obtained as follows:*

$$\mathbb{E}\left[P^{\frac{2}{\alpha}}\right] = P_{\mathrm{t}}^{\frac{2}{\alpha}} \left\{\beta_1^2 + \frac{1}{\pi\lambda_{\mathrm{B}}}\left(e^{-\pi\lambda_{\mathrm{B}}\beta_1^2} - e^{-\pi\lambda_{\mathrm{B}}\beta_1^2}\right)\right\}. \tag{3.2}$$

where

$$\beta_1^2 = \left(\frac{P_{\min}}{P_{\mathrm{t}}}\right)^{1/2}, \qquad \beta_2^2 = \left(\frac{P_{\max}}{P_{\mathrm{t}}}\right)^{1/2}. \tag{3.3}$$

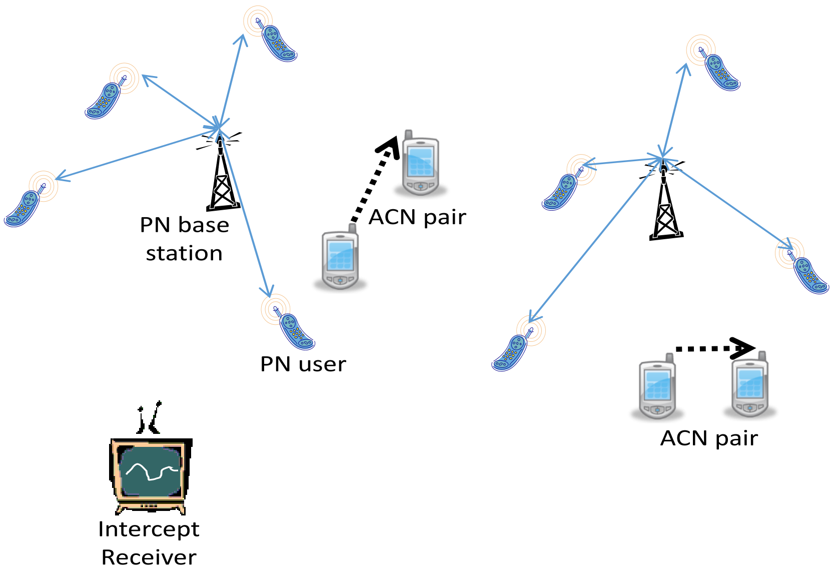

Figure 3.1: The first step for an IR is to determine if covert transmission is taking place. Next it can try to localize one of its transmitters.

Proof: The expected value of the PN transmitted power, given the transmission policy for each PN user as discussed in Chapter I, is obtained as follows:

$$\begin{aligned}\mathbb{E}\left[P^{\frac{2}{\alpha}}\right] &= 2\pi\lambda_{\mathrm{B}}\left\{\int_0^{\beta_1} P_{\min}^{\frac{2}{\alpha}}\, r\, e^{-\pi\lambda_{\mathrm{B}} r^2}\, dr\right. \\ &\qquad \left. + \int_{\beta_1}^{\beta_2} P_{\mathrm{t}}^{\frac{2}{\alpha}}\, r^3\, e^{-\pi\lambda_{\mathrm{B}} r^2}\, dr + \int_{\beta_2}^{\infty} P_{\max}^{\frac{2}{\alpha}}\, r\, e^{-\pi\lambda_{\mathrm{B}} r^2}\, dr\right\} \qquad (3.4) \\ &= P_{\mathrm{t}}^{\frac{2}{\alpha}}\left\{\beta_1^2 + \frac{1}{\pi\lambda_{\mathrm{B}}}\left(e^{-\pi\lambda_{\mathrm{B}}\beta_1^2} - e^{-\pi\lambda_{\mathrm{B}}\beta_1^2}\right)\right\}.\end{aligned}$$

The variables β_1 and β_2 are given in (3.3). ■

Now Corollary I can be used to derive the CDF of the *aggregate metric* as presented in the next theorem.

Theorem II: *The cumulative distribution function (CDF) of the aggregate covert metric is given by:*

$$\mathbb{P}[\mathrm{G_A} \leq \eta] = \frac{2}{\pi}\tan^{-1}\left(\sqrt{\frac{\eta}{P_\mathrm{c}}}\frac{K}{M}\right), \tag{3.5}$$

where

$$K = 1.57\pi\sqrt{P_\mathrm{t}}\rho\lambda_\mathrm{P}\left(\beta_1^2 + \frac{1}{\pi\lambda_\mathrm{B}}\left[e^{-\pi\lambda_\mathrm{B}\beta_1^2} - e^{-\pi\lambda_\mathrm{B}\beta_2^2}\right]\right), \tag{3.6}$$

$$M = 1.57\pi\rho\lambda_\mathrm{C}. \tag{3.7}$$

Proof: The direct approach to prove the theorem is to first find the pdf of the interference at the IR and the pdf of the aggregate ACN received power. Following the general approach of [19], the pdf of the interference $\mathcal{I}$ is obtained in this case as follows:

$$\begin{aligned}
\mathbb{E}\left[e^{-s\mathcal{I}}\right] =& \mathbb{E}\left[\exp(-s\sum_{x_i\in\Phi_\mathrm{P}} P_i\, g_{1i}\, r_{1i}^{-\alpha})\right] \\
\overset{(a)}{=}& \mathbb{E}\left[\prod_{x_i\in\Phi_\mathrm{P}} \exp(-sP_i\, g_{1i}\, r_{1i}^{-\alpha})\right] \\
\overset{(b)}{=}& \exp\left\{\mathbb{E}\left[\int_{\mathbb{R}^2}\{\exp\left(-sPg_1\, r_1^{-\alpha}\right) - 1\}\Lambda(dx)\right]\right\} \\
\overset{(c)}{=}& \exp\left\{-\frac{2\pi\rho\lambda_\mathrm{P}}{\alpha}\mathbb{E}\left[(sPg_1)^{\frac{2}{\alpha}}\right]\right. \\
&\left. \times\int_0^\infty (1-e^{-r_1})\, r_1^{-\frac{2}{\alpha}-1}dr_1\right\} \\
\overset{(d)}{=}& \exp\left\{-P_\mathrm{t}^{\frac{2}{\alpha}}\frac{2\pi\rho\lambda_\mathrm{P}}{\alpha}\,\Gamma\left(1+\frac{2}{\alpha}\right)\left(\beta_1^2 + \frac{1}{\pi\lambda_\mathrm{B}}\right.\right. \\
&\left.\left.\times\left[e^{-\pi\lambda_\mathrm{B}\beta_1^2} - e^{-\pi\lambda_\mathrm{B}\beta_2^2}\right]\right)\Gamma\left(1-\frac{2}{\alpha}\right)\, s^{2/\alpha}\right\}.
\end{aligned} \tag{3.8}$$

In (a), the summation is taken outside the exponential function and became a multiplication. (b) is obtained by applying the probability generating functional (PGFL) [20], and $\Lambda(.)$ is the measurable function [19]. In (c), the location x is represented in polar coordinates. In (d), the expected value of the channel gain [19] is: $\mathbb{E}[g_1^{2/\alpha}] = \Gamma(1 + \frac{2}{\alpha})$, and the expected value of the transmitted power is derived in Corollary I.

Now, the pdf of $\mathcal{I}$ can be found by taking the inverse Laplace transform [39] of the final expression in (3.8). This expression has an inverse [19] for $\alpha = 4$, and is given as:

$$f_{\mathcal{I}}(\xi) = \frac{K}{2\sqrt{\pi}}\, \xi^{-1.5} e^{\frac{-K^2}{4\xi}}, \tag{3.9}$$

where the parameter K is given in (3.6). Similarly, the aggregate ACN received power will have the same pdf if we replace the pdf parameter K with M that is given in (3.7); where in this case $\mathbb{E}[P^{2/\alpha}] = \sqrt{P_\mathrm{c}}$. Consequently, the CDF of the *aggregate metric* can be derived as follows:

$$\begin{aligned}
\mathbb{P}[\mathrm{G_A} \leq \eta] &\overset{(a)}{=} \mathbb{E}\left[\mathbb{1}\left\{\frac{\sum_{y_k \in \Phi_\mathrm{c}} P_\mathrm{c}\, g_{\mathrm{v}k}\, r_{\mathrm{v}k}^{-\alpha}}{\sum_{x_i \in \Phi_\delta} P_i\, g_{1i}\, r_{1i}^{-\alpha}} \leq \eta\right\}\right] \\
&\overset{(b)}{=} \mathbb{E}\left[\mathbb{1}\left\{\sum_{y_k \in \Phi_\mathrm{c}} g_{\mathrm{v}k}\, r_{\mathrm{v}k}^{-\alpha} \leq \eta\, \mathcal{I} \mid \mathcal{I}\right]\right\} \\
&\overset{(c)}{=} \mathbb{E}\left[\operatorname{erfc}\left(\sqrt{\frac{P_\mathrm{c}}{\eta\, \mathcal{I}}\frac{M}{2}}\right)\right] \\
&\overset{(d)}{=} \frac{2}{\pi} \tan^{-1}\left(\sqrt{\frac{\eta}{P_\mathrm{c}}\frac{K}{M}}\right),
\end{aligned} \tag{3.10}$$

where (a) is the definition of probability in terms of expected value over the indicator function $\mathbb{1}\{.\}$ of the events $\mathcal{A} = \{\mathrm{SINR_R} \leq \eta\}$. ($b$) is just a rearrangement of the terms and conditioning on the value of the interference. In (c), the CDF of the ACN aggregate received power is calculated using the derived pdf. In (d), the CDF is averaged over the pdf of interference. ■

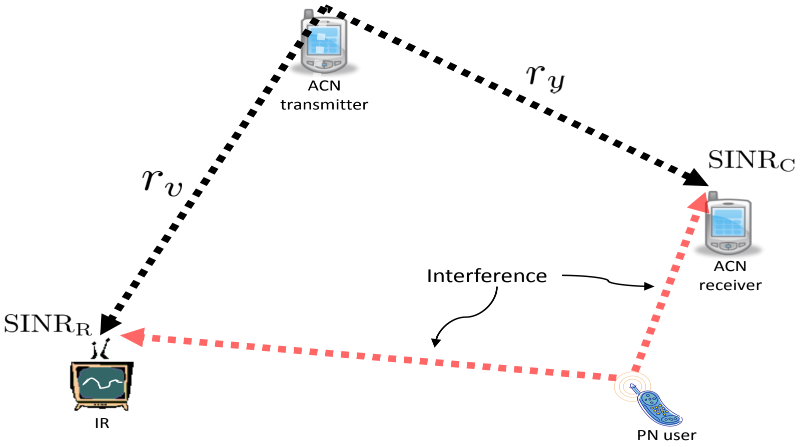

Figure 3.2: The ACN transmitter needs to achieve high throughput, i.e, high SINR, at the ACN receiver, but also minimize its SINR at an IR. In this case there will be a trade-off between the ACN throughput and its covertness.

3.4 Performance of a Single Covert Link

From the perspective of the ACN, covertness for individual users is crucial. As shown in Fig. 3.2, any ACN transmitter needs to achieve a high SINR at its intended receiver while still minimizing its SINR at the IR. In other words, the SINR at an IR, $\mathrm{SINR_R}$, located at some distance, r_v, from an ACN transmitter should be sufficiently lower than the SINR at an intended covert receiver, i.e., $\mathrm{SINR_C}$, that is located at a distance r_y. This case raises a trade-off between the ACN possible throughput and its covertness; therefore, we can define the *ratio metric* as the ratio of $\mathrm{SINR_C}$ to $\mathrm{SINR_R}$.

For this metric, the covert signal received by the ACN receiver will be corrupted by both noise and interference with a probability π_e (erroneous transmission) or noise only with probability of π_s if there are no nearby local interferes. Assume the ACN transmission bandwidth is B_c, and the IR detection bandwidth is $B_\mathrm{r} = \kappa\, B_\mathrm{c}$. Let the noise be i.i.d., zero-mean AWGN of power spectral density N_0 W/Hz, then the noise power at the ACN and IR receivers become, $\sigma^2 = B_\mathrm{c}\, N_0$ and $\sigma_\mathrm{r}^2 = B_\mathrm{r}\, N_0 = \kappa\, N$, respectively. The SINR at the ACN receiver, $\mathrm{SINR_C}$, can be written as follows:

$$\mathrm{SINR_C} = \pi_{\mathrm{s}} \frac{P_{\mathrm{c}}\, g_{\mathrm{c}}\, r_y^{-\alpha}}{\sigma^2} + \pi_{\mathrm{e}} \frac{P_{\mathrm{c}}\, g_{\mathrm{c}}\, r_y^{-\alpha}}{\sigma^2 + \sum\limits_{x_j \in \Phi_\delta} P_j\, g_{0j}\, r_j^{-\alpha}}, \tag{3.11}$$

where $r_y = ||y||$, and $r_j = ||x_j||$ are the distances of the ACN transmitter and the jth PU to the ACN receiver (which is located at the origin), respectively.

On the other hand, the IR does not know the frequency or the transmission strategy of the ACN; therefore, the SINR of the covert signal at the IR will always be corrupted by interference of all the PUs in the network as well as the noise. Hence, the instantaneous SINR at the IR, $\mathrm{SINR_R}$, is given as:

$$\mathrm{SINR_R} = (\pi_{\mathrm{s}} + \pi_{\mathrm{e}}) \frac{P_{\mathrm{c}}\, g_{\mathrm{v}}\, r_{\mathrm{v}}^{-\alpha}}{\sigma_{\mathrm{r}}^2 + \sum\limits_{x_i \in \Phi_{\mathrm{P}}} P_i\, g_{1i}\, r_i^{-\alpha}}, \tag{3.12}$$

where $r_v = ||y - \mathrm{v}||$, and $r_i = ||x_i - \mathrm{v}||$ are the distances of the ACN transmitter, and the ith PN user to the IR, respectively. Now, we can formally define the *ratio metric*, $\mathrm{G_R}$, as follows:

$$\mathrm{G_R} = \frac{\mathrm{SINR_C}}{\mathrm{SINR_R}} = \frac{g_{\mathrm{c}}}{g_{\mathrm{v}}} \frac{r_y^{-\alpha}}{r_{\mathrm{v}}^{-\alpha}} \frac{\sigma_{\mathrm{r}}^2 + \mathcal{I}_1}{\pi_{\mathrm{e}} + \pi_{\mathrm{s}}} \left(\frac{\pi_{\mathrm{s}}}{N} + \frac{\pi_{\mathrm{e}}}{\sigma^2 + \mathcal{I}_0} \right). \tag{3.13}$$

where $\mathcal{I}_0 = \sum\limits_{x_j \in \Phi_\delta} P_j\, g_{0j}\, r_j^{-\alpha}$ and $\mathcal{I}_1 = \sum\limits_{x_i \in \Phi_{\mathrm{P}}} P_i\, g_{1i}\, r_i^{-\alpha}$. From the perspective of the ACN, the larger this metric, the higher the covertness of each ACN user. Note that this metric is also a random variable due to variations in parameters such as channel gains, the location of the PN users. Therefore, a suitable way to characterize the system covert performance is to analyze the complimentary cumulative distribution function (CCDF) of the metric, i.e., $\mathbb{P}[\mathrm{G_R} > \mu]$.

Also note that $\mathrm{G_R}$ does not depend on the transmission power of the ACN. This is because we are analyzing the probability that the SINR at the ACN receiver being greater than the SINR at the IR by a factor of μ; regardless of the transmission power of the ACN. In this case, if the ACN choses to transmit at a power level P_{c} to achieve a target $\mathrm{SINR_C}$, then the metric guarantees that the covert SINR at the IR, i.e., $\mathrm{SINR_R}$, will be smaller by a factor of μ with a probability of $\mathbb{P}[\mathrm{G_R} > \mu]$. A lower bound on the CCDF of the *ratio metric* $\mathrm{G_R}$ is presented in the theorem below.

Theorem III: *For an ACN user with imperfect sensing, the CCDF of* $\mathrm{G_R}$ *has a lower bound given by:*

$$\mathbb{P}[\mathrm{G_R} > \mu] \geq \frac{1}{1+A}\left\{1 - \frac{\pi_\mathrm{e}\, A}{((\pi_\mathrm{e}+\pi_\mathrm{s})\,A+\pi_\mathrm{s})}\;\frac{2}{1+\sqrt{1+\frac{2}{\upsilon^2}(1-(1-\frac{2}{\pi})\;e^{-\upsilon f(\upsilon)})}}\right\}, \tag{3.14}$$

where

$$\begin{aligned}
A &= \frac{\mu}{\kappa}\frac{r_\mathrm{v}^{-\alpha}}{r_y^{-\alpha}}\left(1-\frac{2}{1+\sqrt{1+\frac{2}{\varepsilon^2}(1-(1-\frac{2}{\pi})\;e^{-\varepsilon f(\varepsilon)})}}\right),\\
K_1 &= 1.57\pi\sqrt{P_t}\rho\lambda_\mathrm{P}\left(\beta_1^2+\frac{1}{\pi\lambda_B}\left[e^{-\pi\lambda_B\beta_1^2}-e^{-\pi\lambda_B\beta_2^2}\right]\right),\\
f(\varepsilon) &= 0.8577(1-0.024\varepsilon^2(1-0.8577\varepsilon/\pi^2)),\\
\upsilon &= \sqrt{\frac{\gamma_t(A+\pi_s)}{A+\pi_e+\pi_s}\frac{K_2}{2}}, \qquad \varepsilon = \sqrt{\frac{\gamma_t}{\kappa}\frac{K_1}{2}},\\
K_2 &= \frac{\lambda_\mathrm{B}}{\lambda_\mathrm{P}}K_1, \qquad \gamma_t = \frac{P_t}{\sigma^2}.
\end{aligned} \tag{3.15}$$

Proof: The CCDF of $\mathrm{G_R}$ has the lower bound that is given in:

$$\mathbb{P}[\mathrm{G_R} > \eta] \geq \mathbb{E}\left[\frac{1}{1+\eta\frac{r_\mathrm{v}^{-\alpha}}{r_\mathrm{y}^{-\alpha}}\mathbb{E}\left[\frac{\pi_\mathrm{e}+\pi_\mathrm{s}}{\sigma_\mathrm{r}^2+\mathcal{I}_1}\left(\frac{\pi_\mathrm{s}}{\sigma^2}+\frac{\pi_\mathrm{e}}{\sigma^2+\mathcal{I}_0}\right)^{-1}\right]}\right]. \tag{3.16}$$

The terms $\mathcal{I}_1$, and $\mathcal{I}_0$ are dependent because $\Phi_\delta \subset \Phi_\mathrm{P}$. Consequently, we can think of the interference measured at the IR, i.e., $\mathcal{I}_1$, as comprised of two terms: the first term, $\mathcal{I}_{10}$, which represents the interference from the PUs that also interfere with the ACN when it mistakenly transmit in the same RF resources. The second term, $\mathcal{I}_{11}$, represents the rest of the interferers which falls in the detection bandwidth of the IR. $\mathcal{I}_{10}$ can be ignored in comparison with $\mathcal{I}_{11}$ because the ACN achieves covertness by transmitting in a small percentage of the PN spectrum. With this assumption, $\mathcal{I}_0$ and $\mathcal{I}_1$ can be assumed independent without making any significant compromises. Therefore:

$$\mathbb{P}[\mathrm{G}_\mathrm{R} > \mu] \geq \mathbb{E}\left[\frac{1}{1 + \frac{\eta r_\mathrm{v}^{-\alpha}}{\kappa r_\mathrm{y}^{-\alpha}} \frac{\pi_\mathrm{s}+\pi_\mathrm{e}}{\pi_\mathrm{s}+\frac{\pi_\mathrm{e}}{1+\gamma_t \mathcal{I}_0}} \mathbb{E}\left[\frac{1}{1+\frac{\gamma_t}{\kappa}\mathcal{I}_1}\right]}\right]. \tag{3.17}$$

The outer and inner expectations are with respect to the terms of $\mathcal{I}_0$ and $\mathcal{I}_1$, respectively. Following the approach presented in Appendix C, the pdf of $\mathcal{I}_0$ and $\mathcal{I}_1$ can be easily found to be similar to (3.9) with parameters K_1 and K_2 given in (3.15), respectively; which are given in (3.15). The expectation term in the denominator is then found as follows:

$$\begin{aligned}
\mathbb{E}\left[\frac{1}{1+\frac{\mathcal{I}_1}{\kappa\sigma^2}}\right] &= \int_0^\infty \frac{M}{2\sqrt{\pi}} \frac{1}{1+\frac{\gamma_t}{\kappa}\,\xi}\, \xi^{-1.5} e^{\frac{-M^2}{4\xi}}\, d\xi \\
&\overset{(a)}{=} 1 - \sqrt{\frac{\gamma_t \pi}{\kappa}} \frac{M}{2}\, e^{\frac{\gamma_t M^2}{4\kappa}} \operatorname{erfc}\left(\sqrt{\frac{\gamma_t}{\kappa}} \frac{M}{2}\right) \qquad (3.18) \\
&\overset{(b)}{=} 1 - \frac{2}{1+\sqrt{1+2\varepsilon^{-2}(1-(1-2/\pi)\exp(-\varepsilon f(\varepsilon)))}}
\end{aligned}$$

where $f(\varepsilon)$, ε, and γ_t are all given in (3.15). The expression in (a) multiplies a very large number, i.e., the exponential term, by a very small number, i.e., the complimentary error function. This might lead to inaccurate answers when evaluated in digital systems. Therefore, we use the alternative expression in (b) which has been shown to be a good approximation [40]. Finally, we can calculate the outer expectation in (3.17) using the pdf of $\mathcal{I}_0$ and then simplify the result to prove the theorem. ■

This theorem provides valuable insights for several special cases. The first special case is when we assume there is no interference. In the absence of interference, noise becomes the main factor in achieving covertness in the noise-limited regime (NL). Therefore, this case represents the classical approach of hiding signals in noise, such as spread spectrum. By ignoring the interference terms in (3.13), the covert metric for a NL regime is calculated as follows:

$$\mathbb{P}[\mathrm{G_R} > \mu] = \frac{1}{1 + \frac{\mu}{\kappa}\frac{r_z^{-\alpha}}{r_y^{-\alpha}}} \tag{3.19}$$

It can be noticed that the result in (3.19) reinforces the idea that the covertness of an ACS system is directly related to both its processing gain w.r.t. to the IR, and its relative distance to the IR. Later, we will use this case as a benchmark to see if hiding the ACN signal the RF spectrum provides any additional covertness.

The second special case is when we set $\pi_e = 0$. This is equivalent to saying that the ACN does not make any sensing mistakes and perfectly accesses the spectrum of the PN, i.e., interference-limited perfect sensing (ILPS); this could be possible if the ACN has prior knowledge about the local availability of certain PN RBs. In this case, (3.14) is reduced to the following expression:

$$\mathbb{P}[\mathrm{G_R} > \mu] \geq \frac{1}{1 + A}. \tag{3.20}$$

It can be noticed that this represent the first term in (3.14), which makes the remaining term equivalent to covertness loss due to the imperfect sensing and exploitation of the PN spectrum.

3.5 Performance Analysis

In this section, we validate the derived expressions for both the aggregate and ratio metrics. The PN has a number of base stations and a number of users. The PN base stations and users are assumed to be distributed as a PPP of intensity $\lambda_{\mathrm{B}} = 10^{-5}$ BS$/m^2$. Following the LTE standards [38], the PN user's minimum and maximum transmission power are chosen to be $P_{\min} = -40$dBm and $P_{\max} = 24$dBm, respectively. The ACN hides its transmission in the RF spectrum of the PN by choosing a sub-channel and a time slot for transmission. The ACN uses the frequency-domain sensing method, that was previously discussed, to sense the PN spectrum for empty resources; the sensing time and detection threshold are chosen so that $\mathrm{P}_{\mathrm{fa}} = 0.1$; this value will always be used unless otherwise specified.

Fig. 3.3 shows the CDF of the *aggregate metric* for different λ_{C} values. The simulated curves were obtained by running 50,000 iterations and averaging over the random locations of both the PN and ACN users. It can be noticed that the simulation results match the theoretical prediction. By looking at individual curves, it can be observed that when the value of λ_{C} is small in comparison with the given value of λ_{P}, i.e., low number of ACN users, the CDF curve of the metric rapidly approaches 1, even for low SINR values, η. Since these curves represent the aggregate ACN SINR values when averaged over the locations of the ACN users, it can be said that on average the SINR of the ACN is guaranteed to remain low, and a covert communication is possible. Moreover, when we compare different CDF curves of the metric, we notice that the covertness of the ACN, i.e., the probability that the ACN maintains a specific value for η, rapidly decreases as the intensity (the number) of the ACN users increases. So, for example, we can choose $\eta = 10$ and notice that $\mathbb{P}[\mathrm{G}_{\mathrm{A}} \leq \eta]$ decreases by 20%, i.e., from 0.98 to 0.79, when the intensity of the ACN users increases ten folds from $\lambda_{\mathrm{C}} = 10^{-7}$ to $\lambda_{\mathrm{C}} = 10^{-6}$; however, $\mathbb{P}[\mathrm{G}_{\mathrm{A}} \leq \eta]$ decreases by almost 50%, i.e., from 0.79 to 0.4 when λ_C only increases four folds from 10^{-6} to 4×10^{-6}.

In Fig. 3.4, we choose $\eta = 1$ and graph the maximum intensity of the ACN transmitters

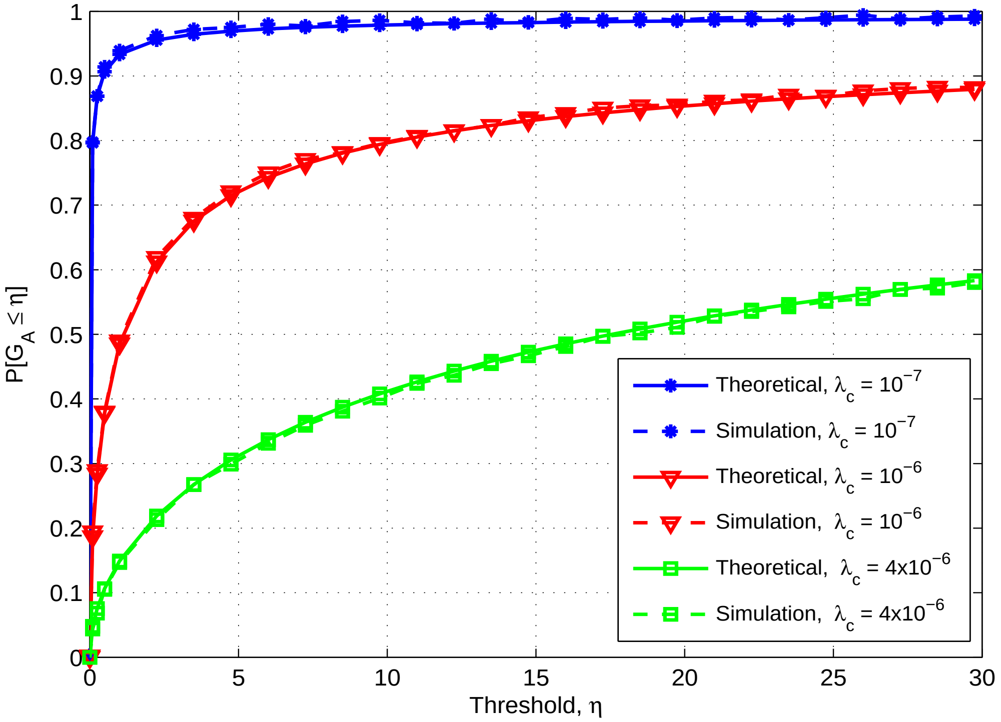

Figure 3.3: The complimentary distribution function for the aggregate metric $\mathrm{G_A}$ for $\lambda_\mathrm{P} = 15 \times 10^{-5}$.

that can maintain a desired $\mathbb{P}[\mathrm{G_A} \leq 1]$. Each curve shows that the ACN intensity must be decreased if the ACN is to be designed to achieve a higher $\mathrm{G_A}$ CDF value. On the other hand, the different curves in Fig. 3.4 demonstrate that it is possible for more ACN transmitters to operate in the same region and maintain the same $\mathbb{P}[\mathrm{G_A} \leq \eta]$ if the intensity of the PN users increases. This result should in fact be expected because as the number of the PN users increases in the operation area of the ACN, the ability of the IR to detect the presence of the covert transmission decreases.

To validate the derived expression of the *ratio metric*, we can assume a case where an ACN user is equally located from both the ACN receiver and the IR, i.e., $r_y = r_\mathrm{v} = 100$. In Fig. 3.5, we graph the simulated and theoretical curves of the *ratio metric* for three scenarios: noise-limited (NL), interference-limited with perfect sensing (ILPS) $\pi_e = 0$, and interference-limited with imperfect sensing (ILIS)$\pi_e = 1$. Here, the case $\pi_e = 0$ means that the ACN perfectly senses and accesses the PN spectrum without any errors. Therefore, the ACN will to be able

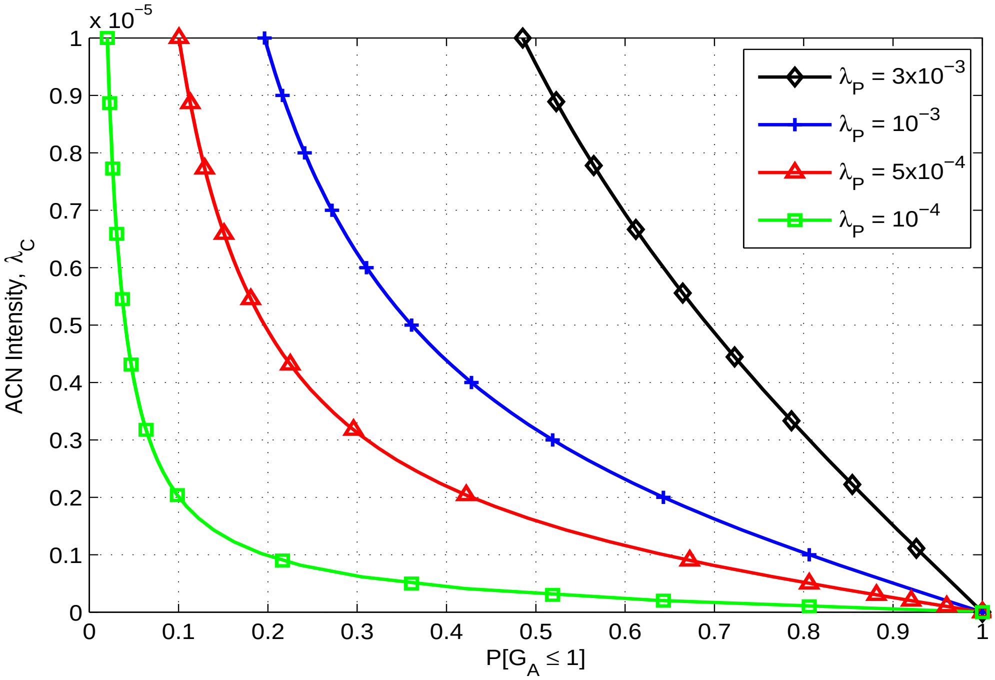

Figure 3.4: The maximum ACN transmitter density as a function of the CDF of G_A, for $\eta = 1$. The different curves represent different intensity values for the PN users.

to operate with minimum transmission power and achieve the highest covertness because it will experience the lowest interference from the PN. On the other hand, the noise-only curve represents the case where there is no PN that the ACN can exploit to increase covertness. This case is equivalent to the traditional scenario of hiding signals in noise; therefore, it can be considered as the worst case scenario for hiding the ACN signal. It is clear from Fig. 3.5 that the ACN achieves higher covertness if it hides its signal in the radio transmissions of another network rather than in noise only, and this covertness increases as the ACN sensing accuracy of the PN RBs increases. For example, in $\pi_e = 0$ case, the figure shows that with 95% probability, the SINR of the covert signal at the ACN receiver will be $\mu = 20$ times greater than at the IR. In comparison, for the $\pi_e = 1$ case, the ACN SINR has only 56% probability to be 20 times higher at the ACN receiver than at the IR, and only 32% for the noise-only case. This means that if the ACN must achieve a target SINR of (10dB) at its receiver, then it is guaranteed with 95% probability that the covert SINR at the IR is at or below (-10dB) for $\pi_e = 0$ case.

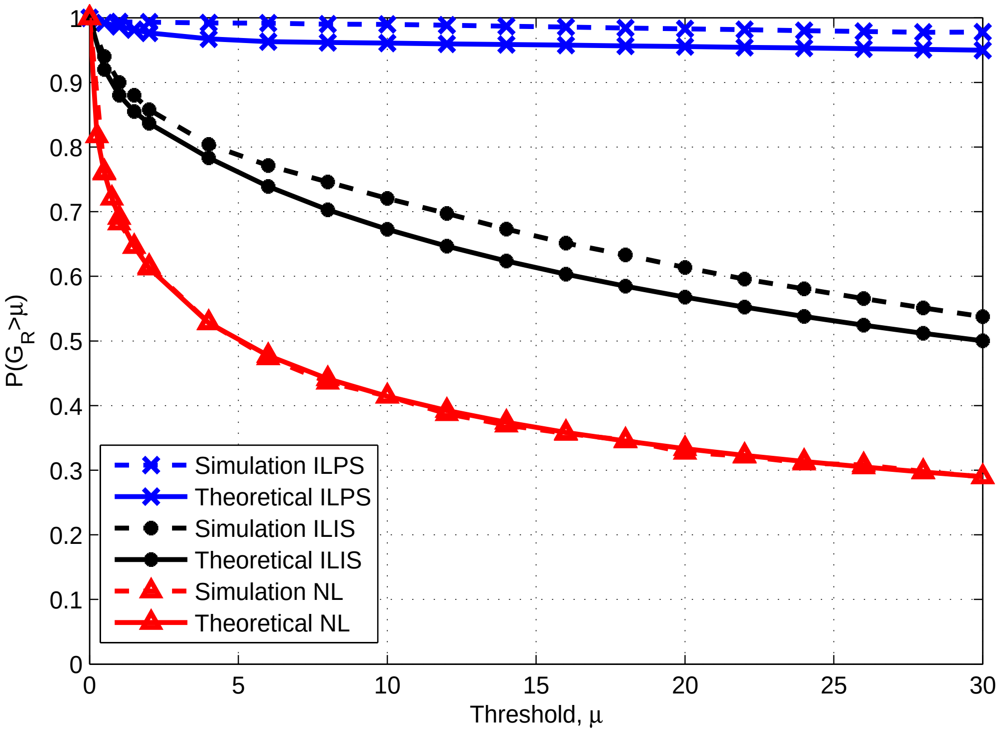

Figure 3.5: The complimentary distribution function of the ratio metric GR for $\lambda_{\mathrm{p}} = 15 \times 10^{-5}$. The blue and black curves represent the upper and lower bounds on the performance of the ACN in the presence of a PN, while the red curve at the bottom represents the covertness of the ACN in the absence of a PN.

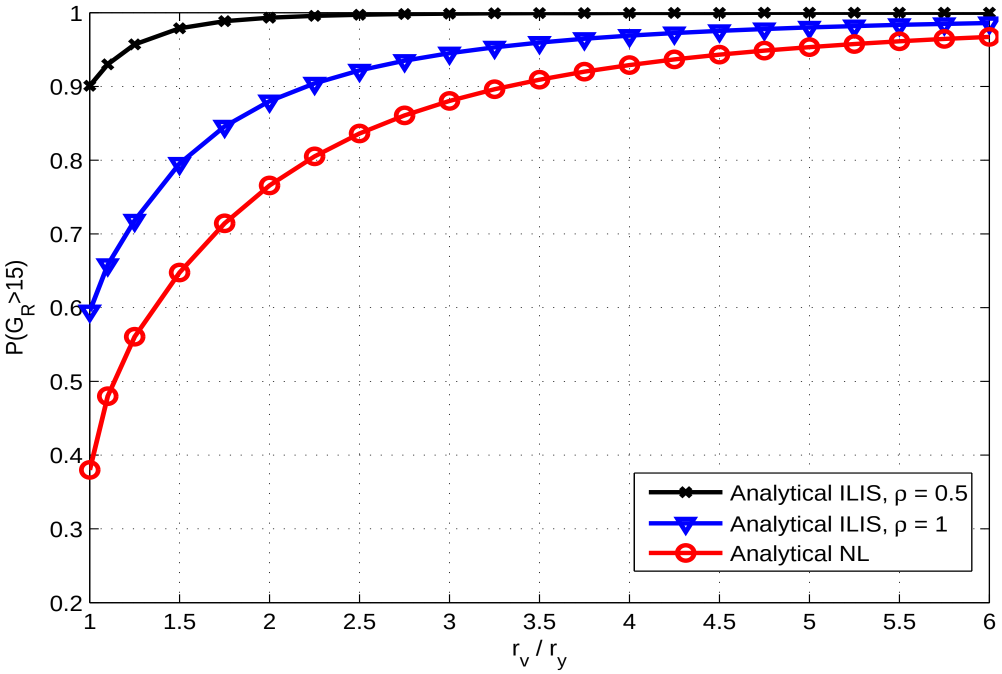

Figure 3.6: The CCDF of the ratio metric when the distance between the ACN transmitter and the IR is increased relative to the ACN transmitter-receiver distance. The ACN covertness rapidly increases as the ratio increases; $\mu = 15$.

In Fig. 3.6, we set $\eta = 15$, and graph the theoretical curves for the covert metric when we increase the distance of the IR with respect to the ACN transmitter. It is shown that the covertness of the ACN increases as the distance between the IR and the ACN increases. It can also be noticed that the covertness rapidly increases for the NL case as well as for high PN load.

Finally, Fig. 3.7 shows the theoretical curves of the CCDF of the covert metric as a function of the PU density λ_P as well as the network load ρ; for $\mu = 15$. When the density decreases to zero, the metric value converges to the NL scenario. As the density increases, the CCDF of the metric increases and seems to converge to an upper value that depends on system parameters. On the other hand, the CCDF of the covert metric increases as the PN traffic load increases before decreasing. This behavior occurs because for low and moderate PN load, the ACN can still find unoccupied PN resources for transmission which increases its covertness; however, as the PN load continues to increase and reaches full capacity, the ACN starts to transmit more in

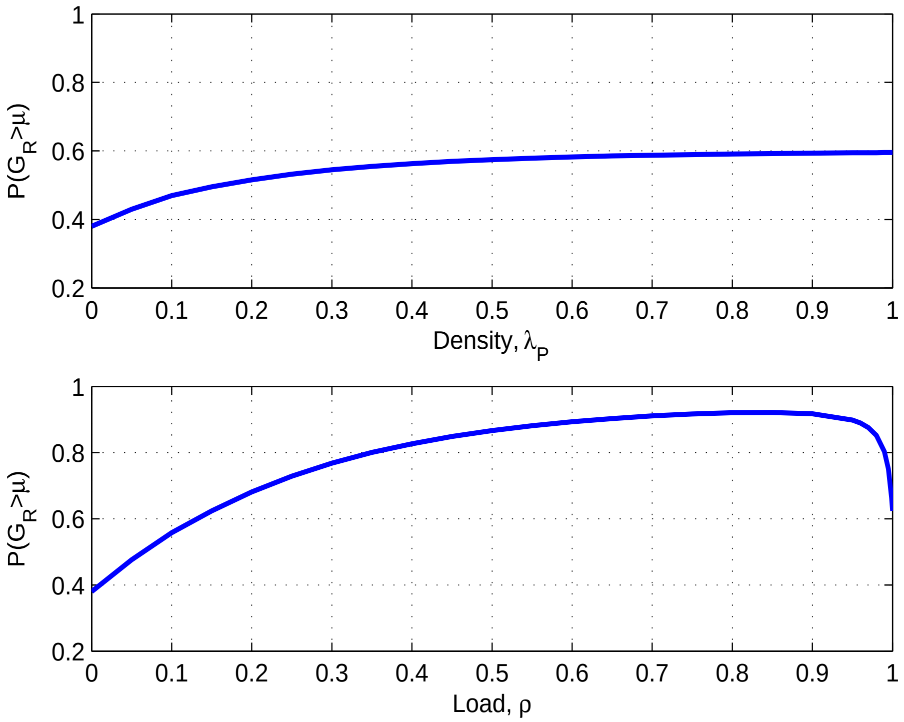

Figure 3.7: The figure shows the CCDF of the covert metric as a function of the PU density (top) and the PN load (bottom); $\mu = 15$.

resources occupied by the PN than in empty resources which decreases its corresponding SINR and, consequently, decreases the ability to maintain covertness. Figure 3.6 clearly demonstrates that the ACN can perform better when the PN has empty resources, i.e., the PN is not fully loaded.

In the next chapter, we analyze the trade-off between the ACN achievable throughput and covertness.

Chapter 4

ACN Covertness-Throughput Tradeoff and System Design

4.1 Key Points of the Chapter

In this chapter, we discuss the case where the ACN user exploit multiple PN resources. In this case there would be a trade-off between the ACN achievable throughput and its covertness. This chapter we also discuss some of the factors that affect the design of the ACN, and also present design case. This chapter is organized as follows: Section 4.2 describe how the ACN user can exploit multiple PN resources to achieve higher throughput. Section 4.3 discusses important covertness characteristics and design aspects for the ACN.

4.2 Introduction

A comprehensive analysis of the ACN performance is presented in this chapter. The derivation of the two covert metrics assumes that the ACN user senses the PN spectrum and transmit in an empty PN resource. However, allowing the ACN user to transmit in multiple resources could increase its throughput, but might decrease its covertness as well. Therefore, there is a trade-off between the ACN achievable throughput and its covertness. One of the questions that needs to be addressed is whether the ACN should use all the PN resources it finds for transmission or just choose a subset. Another question is how to allocate power to the empty PN resources. Another important question is whether the aggregate metric and the ratio metrics can be used to answer key design and system tradeoff factors that would affect the performance of the ACN. These questions will be answered in the following sections. To be specific, we look at how the ACN will allocate its power to the available PN resources. Also we discuss how the PN configuration affects the achievable throughput of the ACN. We also use our analysis of the two metrics to design the ACN and draw conclusions on its expected performance. This chapter can be considered as the first work to provide the first comprehensive analysis of an Ad-Hoc covert system that exploits the RF spectrum of a PN, and would open the door for future work on this subject.

4.3 Covertness-Throughput Tradeoff Analysis

When spectrum sensing is complete using the algorithm previously discussed, the ACN chooses to exploit all or a limited number of the PN RBs in the set $\mathcal{A}$. For a certain level of required covertness, the ACN user can occupy either part or the whole RB bandwidth. Therefore, the instantaneous throughput the ACN can achieve when a RB is found available, given it was actually available, is given by:

$$C_0^{(n)} = \rho_s \, \log_2\left(1 + \frac{P_{\mathrm{c},n}\, g_{\mathrm{c},n}\, r_y^{-\alpha}}{\sigma^2}\right), \tag{4.1}$$

where $P_{\mathrm{c},n}$ is the ACN power allocated to the nth RB, σ^2 is the noise power, $g_{\mathrm{c},n}$ is the channel gain between the ACN transmitter and receiver, and $\rho_s \in [0, 1]$ is the percentage of the available RB bandwidth that will be occupied by the ACN, and its value affect the value of κ in the *ratio* and *aggregate* metrics. Since noise and channel fading are present, spectrum sensing becomes imperfect, and a false alarm can occur. In such a case, the ACN will mistakenly transmit in an unoccupied RB unaware of the presence of the PN signal. The achievable capacity in this case becomes:

$$C_1^{(n)} = \rho_s \ \log_2\left(1 + \frac{P_{\mathrm{c},n}\ g_{\mathrm{c},n}\ r_y^{-\alpha}}{\sum\limits_{x_i \in \Phi_{\delta,n}} P_i\ g_{0i}\ r_{0i}^{-\alpha} + \sigma^2}\right), \tag{4.2}$$

where P_i is the transmission power of the ith PN user that is in the transmitting in the nth RB, g_{0i} is the channel gain between the ith PN user and the ACN receive, and $r_i = ||x_i||$ is the distance of the ith PU and the ACN receiver. On the other hand, if the ACN detects the presence of the PN, it will not transmit on that RB; this includes the case of detecting the PN when in fact it is not present. The achievable throughput of the ACN network over all available RBs is then given as:

$$\begin{aligned} C = \rho_s \left(\frac{T-\tau}{T}\right) \sum_{n \in \mathcal{A}} \Big(& (1-\rho)(1-\mathrm{P}_{\mathrm{fa}})C_0^{(n)} \\ & + \rho(1-\mathrm{P}_{\mathrm{d}})C_1^{(n)} \Big), \end{aligned} \tag{4.3}$$

In order to maximize its throughput, the ACN transmitter has to allocate a total power of P_{c} to the available RBs, and, at the same time, must protect the PN from undesired interference. These two constraints on the ACN network can be described respectively as:

$$\sum_{n \in \mathcal{A}} P_{\mathrm{c},n} \leq P_{\mathrm{c}}, \tag{4.4}$$

$$\sum_{n \in \mathcal{A}} g_{\mathrm{cp},n}\ P_{\mathrm{c},n}\ r_{\mathrm{cp}}^{-\alpha} \leq I_{\mathrm{max}}, \tag{4.5}$$

where $g_{\mathrm{cp},n}$ and r_{cp} are the channel gain and distance between the ACN transmitter and PN receiver, respectively. Therefore, the ACN must solve the following optimization problem at the beginning of each transmission cycle:

Prob. 1: $$\max_{\{\tau, P_{\mathrm{c},n}\}} C$$

$$s.t. (4.4), (4.5), P_{\mathrm{c},n} \geq 0, 0 \leq \tau \leq T$$

The objective of this optimization problem is to find an optimum transmission power in each RB, as well as the optimum sensing time that maximizes the total ACN throughput. This optimization problem is not convex; Therefore, we will first fix the sensing time and solve the power allocation sub-problem for the chosen RBs. Later we will show that there is no need to optimize the sensing time if the previously discussed frequency domain spectrum sensing is used. In addition, the ACN can set up its maximum transmission power based on the maximum allowed interference and the average estimated channel gain over all the available RBs [41]. Since the ACN is trying to maintain a low probability of detection by transmitting at lower power and using frequency hopping, the condition in (4.5) can be neglected as long as (4.4) in maintained.

Therefore, the optimization problem **Prob1** can now be re-written as:

Prob2:

$$\begin{aligned} \max_{P_{\mathrm{c},n}} \quad & \rho_s \left(\frac{T-\tau}{T}\right) \sum_{n\in\mathcal{A}} \left[(1-\rho)(1-\mathrm{P}_{\mathrm{fa}})C_0^{(n)} + \rho(1-\mathrm{P}_{\mathrm{d}})C_1^{(n)}\right] \\ s.t. \quad & \sum_{n\in\mathcal{A}} P_{\mathrm{c},n} \leq P_{\mathrm{c}}, \\ & P_{\mathrm{c},n} \geq 0 \end{aligned} \tag{4.6}$$

The following theorem solves the previous optimization problem and provides the transmission power needed for each available PN resources.

Theorem I: *For the optimization problem in* **Prob. 1**, *the ACN optimal power allocation* *for the available PN resources is:*

$$P_{\mathrm{c},n}^{*} = \left[\frac{1}{|\mathcal{A}|} \left(P_{\mathrm{c}} + \sum_{n\in\mathcal{A}} \left(\frac{\mathcal{I}_{\mathrm{P},n} + \sigma^2}{g_{\mathrm{c},n}} \right) \right) - \frac{\mathcal{I}_{\mathrm{P},n} + \sigma^2}{g_{\mathrm{c},n}} \right]^{+}, \tag{4.7}$$

where

$$\mathcal{I}_{\mathrm{P},n} = \sum_{x_i \in \Phi_{\delta,n}} P_i \, g_{0i} \, r_{0i}^{-\alpha}, \tag{4.8}$$

is the received power from the PN users on the nth RB, and $\left[P_{\mathrm{c},n}^{*}\right]^{+} = max(P_{\mathrm{c},n}^{*}, 0)$ *is used to guarantee a positive transmission power value for every RB.*

Proof: The optimization problem in **Prob. 2** is convex and can be solved using Lagrange Multipliers technique [42]:

$$\mathcal{L} = \rho_s \left(\frac{T-\tau}{T} \right) \sum_{n\in\mathcal{A}} \left[(1-\rho)\left(1-P_{fa}\right) C_0^{(n)} + \rho(1-P_d) C_1^{(n)} \right] - \lambda \left(\sum_{n\in\mathcal{A}} P_{\mathrm{c},n} - P_{\mathrm{c}} \right). \tag{4.9}$$

The optimal solution $\left(P_{\mathrm{c},n}^{*}, \lambda^{*}\right)$ is found by letting the derivative of (4.9) with respect to $P_{\mathrm{c},n}$ equal zero:

$$-\rho_s \left(\frac{T-\tau}{T} \right) \left[\left(g_{\mathrm{c},n}/\sigma^2 \right) \frac{a}{1 + P_{\mathrm{c},n} \, g_{\mathrm{c},n}/\sigma^2} + b \frac{g_{\mathrm{c},n}/\left(\mathcal{I}_{\mathrm{P},n} + \sigma^2\right)}{1 + P_{\mathrm{c},n} \, g_{\mathrm{c},n}/\left(\mathcal{I}_{\mathrm{P},n} + \sigma^2\right)} \right] + \lambda = 0, \tag{4.10}$$

where $a = (1-\rho)\left(1-P_{fa}\right)$, $b = \rho\left(1-P_{fa}\right)$. The following Karush-Kuhn-Tucker (KKT) conditions [42] must hold for the optimal solution:

$$\sum_{n\in\mathcal{A}} P_{\mathrm{c},n}^{*} \leq P_{\mathrm{c}}, \tag{4.11}$$

$$\left(\sum_{n\in\mathcal{A}} P_{\mathrm{P},n}^{*} - P_{\mathrm{c}} \right) \lambda^{*} = 0, \tag{4.12}$$

$$\lambda^{*} \geq 0. \tag{4.13}$$

Examining the KKT condition in (4.12) shows that either $\lambda^* = 0$, or $\sum_{n\in\mathcal{A}} P^*_{\mathrm{c},n} = P_c$. However, if $\lambda^* = 0$, then (4.10) implies that $P^*_{\mathrm{c},n} \leq 0$, which is invalid; therefore, $\sum_{n\in\mathcal{A}} P^*_{\mathrm{c},n} = P_\mathrm{c}$, i.e., replace the inequality sign in (4.11) with equality. We know that, for a given detection threshold, the ACN falsely decides that a RB is available if either the channel gain to the PN is low, or the noise power is high, i.e., low PN SNR. Therefore, the gradient of the Lagrange Multiplier in (4.10) can be shown to equal:

$$P_{\mathrm{c},n} \approx \frac{\rho_s\ (T-\tau)(a+b)}{T\lambda} - \frac{\mathcal{I}_{\mathrm{P},n}+\sigma^2}{g_{\mathrm{c},n}} \tag{4.14}$$

Substituting in (4.12), the optimal value of the constant λ is:

$$\lambda^* = \frac{2\rho_s\ (T-\tau)\, b\, \sigma^2/T}{P_\mathrm{c} + \sum_{n\in\mathcal{A}} \left(\mathcal{I}_{\mathrm{P},n}+\sigma^2\right)/g_{\mathrm{c},n}}, \tag{4.15}$$

which clearly satisfies (4.13). The optimal power allocated to each available RB can now be calculated as in (4.7). ■

An important observation is that the power allocation in (4.7) does not depend on the processing gain of the ACN which means the power allocation is independent of the waveform of the ACN.

As previously discussed, the duration of one OFDM symbol, i.e., the minimum possible time, is used for spectrum sensing in order to simplify the optimization problem **Prob1**. Now we can show that the optimum sensing time that yields the highest throughput is achieved when only one OFDM symbol is used for sensing. Equations (2.7) and (2,8) allow the sensing time to be an integer multiple of the duration of one OFDM symbol, i.e., replacing P by kP. For this purpose, we assume that the PN base stations are distributed as a PPP of intensity $\lambda_\mathrm{B} = 10^{-5}$ BS$/m^2$. Following the LTE standards [38], the PN user's minimum and maximum transmission power are chosen to be $P_\mathrm{min} = -40$dBm and $P_\mathrm{max} = 24$dBm, respectively. The

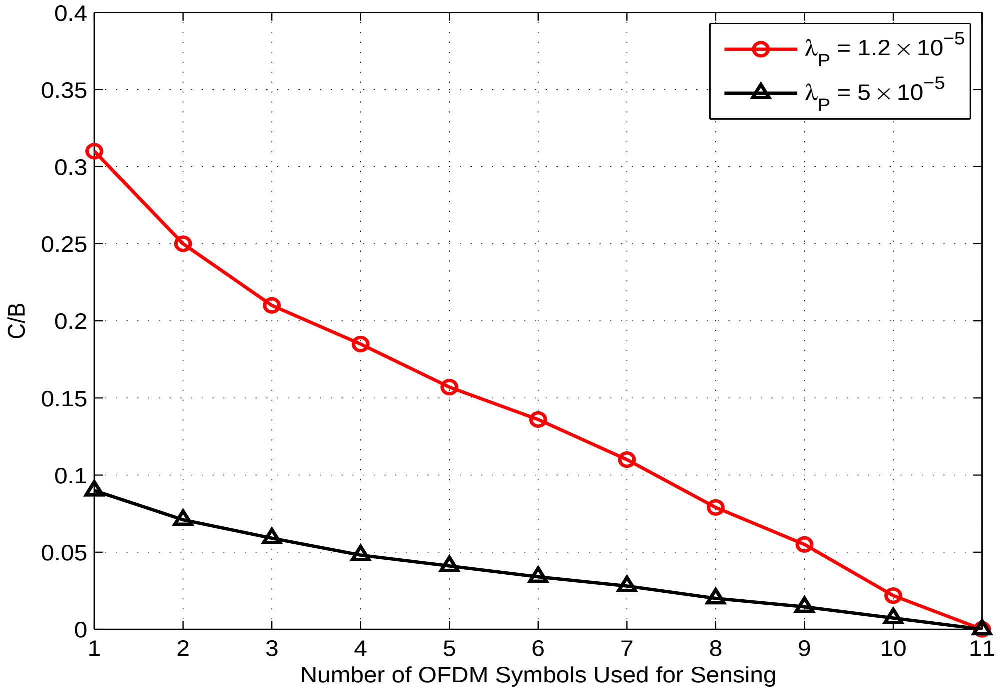

Figure 4.1: Average ACN throughput versus the number of OFDM symbols used for spectrum sensing. The figure shows the throughput for two different PN user densities. It can be noticed that the throughput decreases as the number of symbols used for sensing increases.

ACN sensing threshold is chosen so that $P_{fa} = 0.1$.

In Figure 4.1, we graph the ACN average information theoretic throughput, scaled by the PN bandwidth, as a function of the number of OFDM symbols used for sensing. Each curve represents a different density of PN users, and the power allocation algorithm is used without any consideration to the ACN covertness. The figure shows that the ACN capacity decreases when more OFDM symbols are used for spectrum sensing; therefore, for a covert system that has a limited time for sensing and transmitting, our assumption in **Prob2**, that the optimization of the sensing time equals to one OFDM symbol is valid. It should be noted that in practical systems, additional time is needed for synchronizing the ACN receiver to the ACN transmitter and for other hardware limitations; therefore, the scaled information theoretic throughput, C/B, is the ideal limit which only provides a reference for initial system designs and illustrates how much room there is for improvement.

At this stage, it is possible to use the power allocation expression along with CCDF of the ratio metric to provide a system level tradeoff between the ACN achievable throughput and expected covertness. However, in order to derive a closed-form expression for the ratio metric in (3.14), we made an assumption that the ACN must only transmit in a *small percentage* of the PN RBs; without clearly defining what a small percentage is. On the other hand the spectrum access algorithm could allow the ACN user to access a large number of PN RBs. In this case, the accuracy of the expression of the ratio metric could be compromised. Therefore, it is very important to find out the maximum number of PN RBs that the ACN can exploit before the derived expression of the ratio metric is no longer accurate. Once this value is determined, the ACN user must not use for its transmission more PN RBs than that value.

In order to address this point, we compare our derived expression of the *ratio metric*, where we used this approximation, with a simulation of the actual metric value had we not used this approximation. Figure 4.2, shows three pairs of curves where each pair represents the CCDF of the ratio metric with and without the approximation. The figure shows that as the ACN transmits in more PN RBs, the approximation becomes less valid. We can also notice that both the actual curve and the approximated one closely match or are very close if the ACN uses less than 12% of the PN RBs. Therefore, the ACN should only use less than 12% of the PN RBs, which is a reasonable assumption when a system wants to achieve covertness.

Now, it is possible to combine the spectrum sensing approach that was discussed in Chapter 2 with the power allocation method to create a complete spectrum access algorithm. Here, the ACN needs to implement this algorithm at the beginning of each transmission cycle. The complete algorithm is presented in Algorithm 1.

Using the throughput analysis and the derived two metrics, we can now look at the ACN system throughput and covertness trade-off. The main question in this type of trade-off analysis is that if an ACN user needs to maintain, with a certain probability, a specific SINR advantage over the IR, then what would be the maximum throughput that this ACN user can achieve?

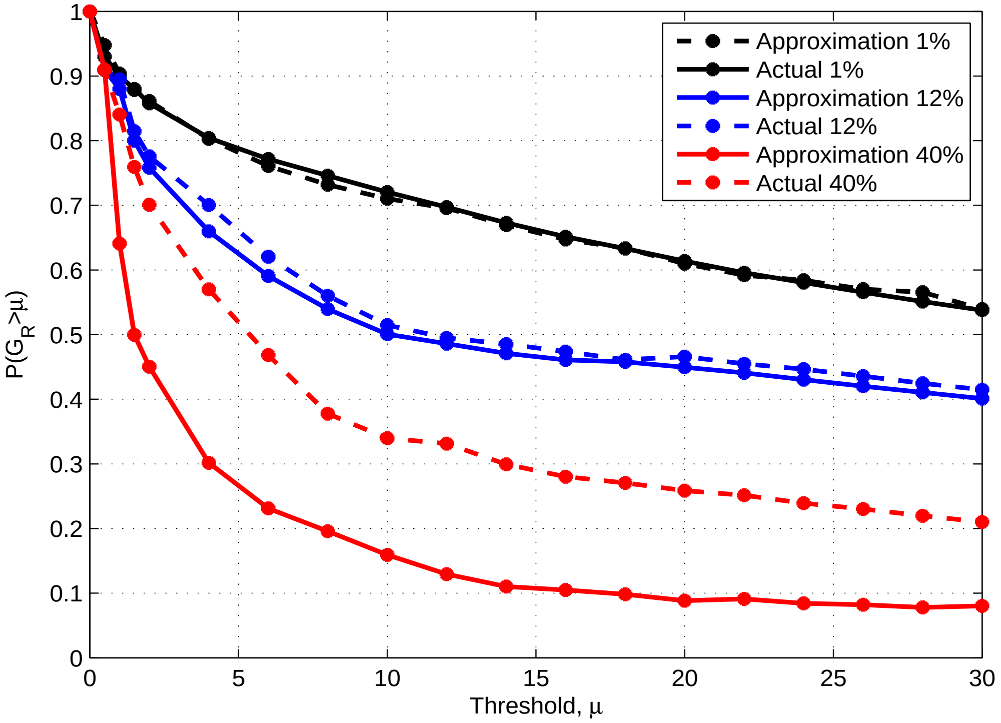

Figure 4.2: The figure shows a comparison between the approximation of $\mathbb{P}[\mathrm{G}_{\mathrm{R}} \geq \eta]$ derived lower bound and its actual value. We notice that the approximation holds as long as the ACN does not use more than approximately 12% of the PN RBs, which is a very valid assumption.

Algorithm 1 : ACN Spectrum Access

```
Initialize: $(\pi_0, P_{fa}, P_{max}, \eta)$
for $n : 1 \longrightarrow N$ do
    Calculate $V_n$ as in (2.2)
    if $V_n \leq \eta_s$ then
        $\mathcal{A} \leftarrow n$
    end if
end for
Choose up to $|\mathcal{A}|$ empty resources
Calculate $P_n^*$ as in (4.7)
End of Algorithm
```

In Fig. 4.3, we graph the ACN user information theoretic throughput C, scaled by the total bandwidth of the PN $B = 20$MHz, as a function of a given covertness requirement; in this case $\mathbb{P}[\mathrm{G_A} \geq 14]$. In this figure, different throughput and covertness values have been obtained by changing the ACN sensing threshold. It can be noticed that when the PN user density is high, the ACN throughput is very low and does not significantly vary. This observation is expected because when the PN has a high density in a certain geographical area, the number of PN RBs that can be sensed as available by the ACN and used for covert transmission becomes very scarce. When the density of the PN users is low, we notice that the ACN throughput increases at the expense of lowering its covertness. In this case, the PN has low number of users per square area which makes the received energy from those users at the ACN very low. As a result, the ACN would have the opportunity to transmit in more RBs and achieve a higher throughput. The downside for the low density of the PN users is that the IR would be more capable of detecting the presence of the ACN user. One important observation in Fig. 4.3 is shown when the density of the PN users is medium. Here, the ACN throughput increases then converges as the covertness decreases. In this type of scenarios it would be infeasible for the ACN to decrease its covertness in pursuit of higher throughput. In this scenario much of the ACN potential throughput can be achieved without sacrificing much of its covertness.

Another aspect that can affect the ACN is the effect of the density of the PN users on the ACN performance. In this regards, Fig. 4.4 shows the ACN scaled throughput as a function of the PN density. Notice that the ACN throughput rapidly decreases when the PN density increases. Therefore, knowing the density of the PN at which the ACN will be deployed have an impact on the performance of the ACN.

4.4 Designing the Covert Network

The metrics discussed in the previous sections can be used to design the ACN. The *ratio metric* can be used to determine the distance between a typical ACN-TX and the ACN-RX, r_y, relative

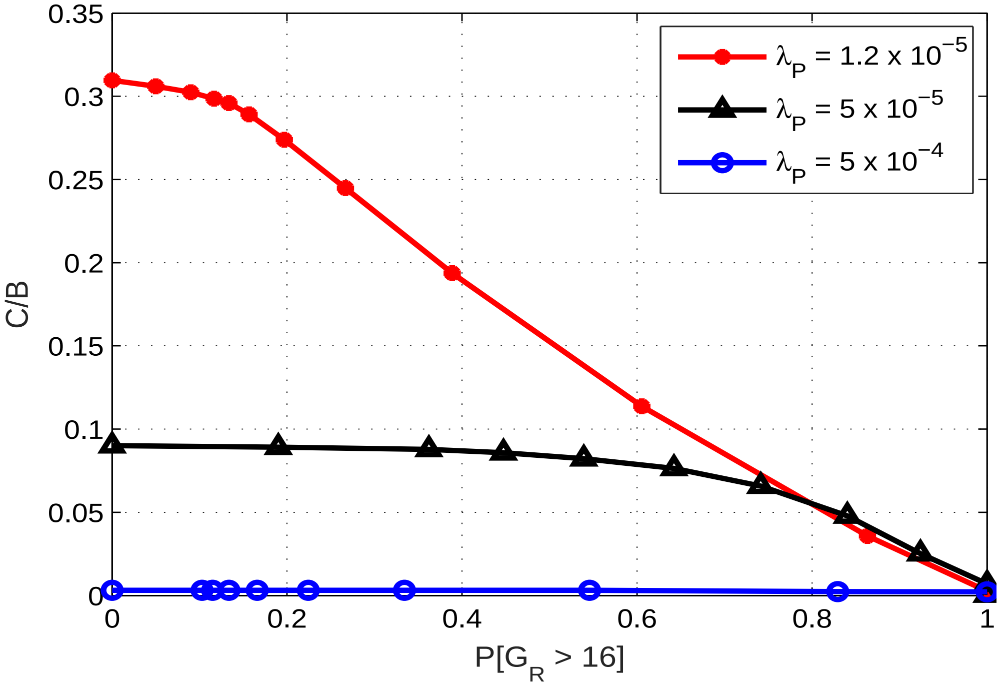

Figure 4.3: The ACN throughput, scaled by its transmission bandwidth, as a function of the probability of a target covertness level. Different curves represents different densities of the PN users. The figure shows that sacrificing the ACN covertness for higher throughput is not always possible, and it only depends on the density of the PN users.

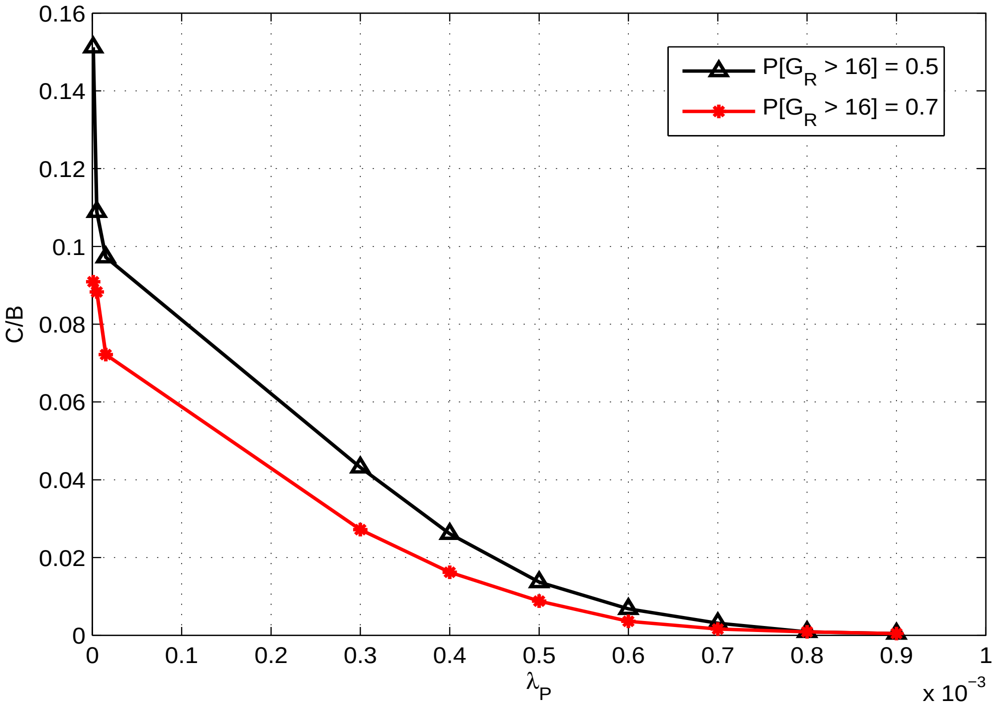

Figure 4.4: The ACN scaled throughput as a function of the density of the PN users for different target covertness levels. The ACN throughput rapidly decreases as the density of the PN users increases.

to that of the ACN-TX and the IR, r_v, to achieve certain covertness level. In Fig. 4.5, we choose $\mu = 15$, and graph r_y/r_v versus the CCDF of the *ratio metric*. For the top curve where $\pi_s = 1$, the ACN user always transmits in empty PN resources, and, therefore, experiences the highest SINR; or the highest SNR in this case. In contrast, the bottom curve where $\pi_e = 1$ represents the lowest ACN SINR because the ACN user always incorrectly transmits in RF resources that are occupied by PN users and, therefore, always experiences interference from the PN. The figure shows that, for the same $\mathbb{P}[\mathrm{G_R} > \mu]$, the communication distance between the ACN transmitter and receiver is larger for the case of $\pi_s = 1$, and smaller for the case of $\pi_e = 1$ because the absence of interference allows the ACN to have the same received signal quality at a longer distance. In addition, each curve shows that the maximum possible distance between the ACN transmitter and receiver must be decreased to maintain a high $\mathbb{P}[\mathrm{G_R} > \mu]$. For example, Fig. 4.5 shows that it is impossible to design an ACN for which the probability of $\mathrm{G_R} = \frac{\mathrm{SINR_C}}{\mathrm{SINR_R}} > \mu$

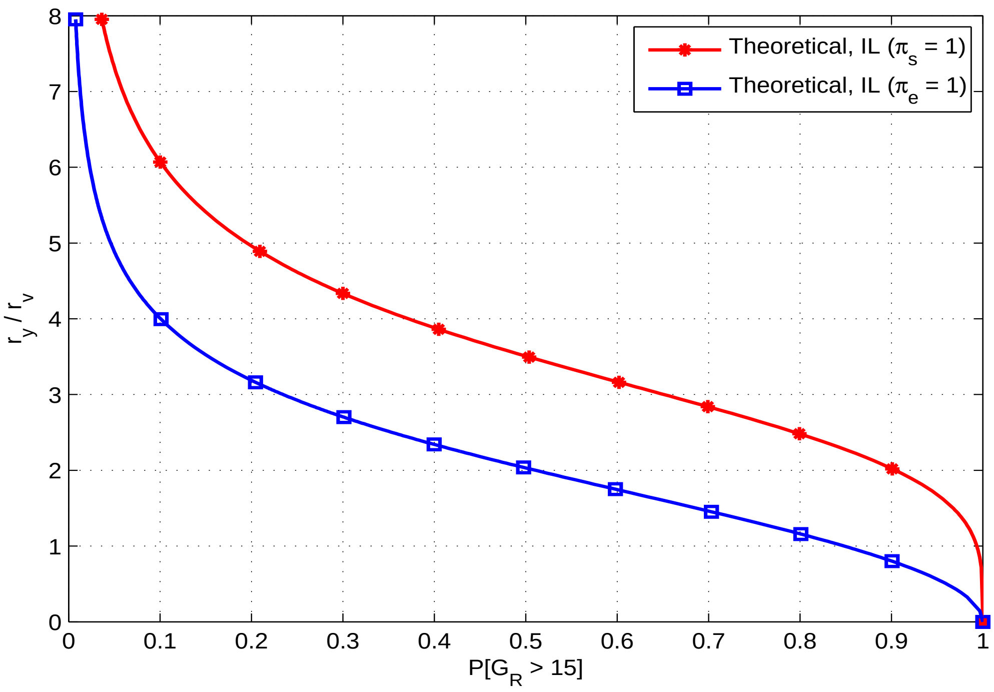

Figure 4.5: The average ACN transmitter-receiver distance (scaled by the distance between the IR and the ACN transmitter) versus $\mathbb{P}[\mathrm{G_R} \geq 15]$. For the top curve, the ACN always transmits in empty PN resources. For the bottom curve, the ACN always incorrectly transmits in PN resources occupied by PN users. The curve for any other case falls in between these two curves.

is 1 because $\mathbb{P}[\mathrm{G_R} > \mu] = 1$ means that the ACN must not be detected by the IR; which can only happen if either the ACN transmitter-receiver distance is set to zero, i.e., $r_y = 0$, or if the IR is located at an infinite distance from the ACN transmitter, i.e., $r_z \to \infty$.

If multiple ACN users needs to operate in the same spatial area, our results can be used to calculate their maximum number that is permitted under a target level of covertness. In this regards, consider the *ratio metric* for the ACN transmitter that is closest to the IR; assume r_z represents the average distance between the IR and this nearest ACN user. According to [43], the distribution of the distance to the nearest neighbor from an arbitrarily chosen point is given as: $f(\xi) = 2\pi\lambda_{\mathrm{C}}\xi e^{-\pi\lambda_{\mathrm{C}}\xi^2}$, with a mean of $\mathbb{E}[\xi] = 1/(2\sqrt{\lambda_{\mathrm{C}}})$. In designing the ACN, $\mathbb{E}[\xi]$ can be thought of as the mean of the distance between the IR and its nearest ACN transmitter, that is, $r_z \triangleq \mathbb{E}[\xi]$. Therefore, for a given set of system parameters and a desired $\mathbb{P}[\mathrm{G_R} > \mu]$, the distance

r_z can be calculated using the lower bound expression of *ratio metric*. Then, r_z is substituted in the expression of the mean of the nearest distance distribution to find a bound on the intensity of the ACN users. Consequently, it becomes possible to quantify the covertness of the ACN from the perspective of the *aggregate metric*. For example, if $r_y = 750$m, and the ACN is to be designed to have $\mathbb{P}[\mathrm{G_R} > 15] = 0.96$ for $\pi_\mathrm{e} = 1$, then Fig. 4.5 shows that $r_y/r_z = 0.5$. Now r_z can be calculated and substituted in the expression of the nearest neighbor to find the ACN maximum intensity as $\lambda_\mathrm{C} = 10^{-7}$. Now it is possible to graph the CDF curve of the *aggregate metric* for the calculated intensity and evaluate the ACN covertness from the perspective of the IR; in our example, $\lambda_\mathrm{C} = 10^{-7}$ represents the top curve in Fig. 3.3.

By looking at the bigger picture, we notice that our two covert metrics, along with the resource allocation algorithm, can be used for the purpose of designing the ACN. After choosing the geographical area in which the ACN will be operating, the designer of the ACN begins by setting the PN main parameters, such as the density of the PN users in that area. This information allows the designer to use Fig. 4.5 to find out how far the ACN transmitter can be from the location of the IR (if that location is known), or what type of precautions need to be taken to maintain that distance (if the IR location is not exactly known). Next, it would be possible to use Fig. 4.3 to make tradeoff choices regarding the target covertness. An example to illustrate this process is as follows: let the PN users' density be $\lambda_\mathrm{P} = 1.2 \times 10^{-5}$, then the steps of the example in the previous paragraph can be used to estimate the maximum possible density of the ACN users; in that case $\lambda_\mathrm{C} = 5.1 \times 10^{-7}$. Next, the ratio metric curve is generated and a desired $\mathbb{P}[\mathrm{G_R} > \mu]$ is chosen; $\mathbb{P}[\mathrm{G_R} > 16]$ for example. Finally, Fig. 4.3 shows the possible throughput-covertness trade off. So, if the ACN needs to achieve $\mathbb{P}[\mathrm{G_R} > 16] = 0.8$, the figure shows that the ACN expected scaled information theoretic throughput is about 1.8Mbps.

Chapter 5

Conclusions

Covert wireless systems that use the radio transmissions of other wireless networks to hide their signals have been suggested as a mean to increase covertness; however, to the best of our knowledge, no detailed work has been done to model and analyze such covert systems. In this paper, we have presented a spectrum access method that would allow an Ad-Hoc covert network (ACN) to opportunistically access and use the spectrum of an OFDM-based wireless network for covert communications. We also defined and derived expressions for two metrics that quantifies the covertness of the ACN from the perspective of an intercept receiver (IR) as well as an ACN user. Additionally, it has been shown that the covert metrics can be used to design an ACN to get a specific level of covertness and throughput. This work can be considered as a foundation for future research on covert systems that can exploit radio transmissions of other networks to achieve higher covertness.

5.1 Contributions

1. Present and discuss a spectrum access algorithm that allows an ACN user to opportunistically accesses the spectrum of an OFDM-based, multi user, wireless network. The sensing stage takes advantage of the OFDM nature of the PN signal to perform sensing in the fre-

quency domain by using the OFDM subcarriers in each PN resource to determine its vacancy. The ACN user then chooses a subset of the empty PN resources for covert transmission.

2. The covertness of the ACN can be determined by the probability that it can be detected by an intercept receiver. This probability of detection is related to the IR parameters as well as the ACN SIR. Therefore, the ACN needs to maintain a lower SIR at the IR in order to achieve higher covertness. Thus, in order to quantify the covertness of the ACN from the perspective of an intercept receiver, the ACN SIR is used as a suitable first covert metric; and the metric is called the *aggregate metric*. Stochastic geometry is used to derive a closed-form expression for the CDF of the metric, and it has been shown how to use this metric to estimate the expected covertness of the ACN.

3. A second metric has been presented and analyzed which captures the performance of a single ACN user. The second metric, namely the *ratio metric*, is defined as the ratio between the SINR of the ACN signal at the intended receiver to that at the IR. When an ACN user covertly communicate with another user, it tries to achieve the highest data rate, i.e., highest SINR, at the intended receiver, while minimizing its SINR at the IR. This trade-off between achieving the highest SINR at the intended receiver and achieving the lowest SINR at the IR makes the ratio metric very suitable. A lower bound on the CCDF of this metric is derived using stochastic geometry, and the corresponding performance is analyzed.

4. Finally, we used both metrics to present a comprehensive analysis of the ACN performance and provided a guideline to design the ACN and choose its key parameters based on the configuration of the OFDM-based PN. We also showed that the spectrum access algorithm, along with the ratio metric, can be used to understand the trade-off between the ACN covertness and its expected covertness.

5.2 Areas of Future Work

We consider the work presented in here as a foundation for future study on covert wireless systems that use the radio transmissions of other wireless networks to hide their signals and achieve covertness. Therefore, there are several promising research directions that can be followed. One particular area that requires further investigation in a future work is the covertness of the ACN in the presence of multiple intercept receivers. This area has been very well studied for covert systems that hide their signals in noise; however, to the best of our knowledge, there is no existing work for systems that exploit the RF band of other wireless networks to achieve covertness.

Another area for possible research is the coexistence between multiple ACN users. In the future, it is expected that multiple sensors, multiple IoT devices, or other security devices will be deployed and some might be required to protect its transmission at the physical layer level. If those systems are designed to share the spectrum with other existing wireless networks, MAC protocols need to be designed to allow the covert devices exploit local spectrum opportunities and share it with minimum inter and intra interference.

Other potential research directions include studying the effect of the mobility of the primary network and ACN users on the achievable covertness and performance. Also, work is possible to study the potential benefits and challenges that a covert system can face if the primary network users are equipped with Multiple Input Multiple Output (MIMO) antennas. When MIMO beamforming is used by the primary network users, one would expect that more local spectral opportunities could become available because of the concentration of the radiated energy from each antenna; however, this potential benefit might decrease the covertness of the ACN.

Page intentionally left blank.

References

[1] J. Katz and Y. Lindell. Introduction to Modern Cryptography, 2nd Ed. *CRC Press*, 2015.

[2] E. Cole. Hiding in Plain Sight: Steganography and the Art of Covert Communication. *Wiley Press*, 2002.

[3] NCSC. Trusted Computer System Evaluation Criteria. *National Computer Security Center Tech.*, 1985.

[4] D. Nicholson. Spread Spectrum Signal Design LPE and AJ Systems. In *Computer Science Press Inc.*, 1988.

[5] R.A. Dillard. Detectability of Spread-Spectrum Signals. *Aerospace and Electronic Systems, IEEE Transactions on*, 1979.

[6] Don Torrieri. Principles of Spread-Spectrum Communication Systems: Edition 3. *Springer Press*, 2015.

[7] R. Orr, C. Pike, M. Bates, M. Tzannes, and S. Sandberg. Covert Communications Employing Wavelet Technology. In *Con. on Signals, Systems and Computers, 1993.*, page vol.1, 1993.

[8] S. Kay. Fundamentals of Statisitcal Signal Processing, Detection Theorey. *Pearson*, 1998.

[9] John Proakis and Masoud Salehi. Digital communications, 4th edition. *McGraw Hill*, 2001.

[10] W. A. Gardner. Exploitation of spectral redundancy in cyclostationary signals. *Signal Processing Magazine, IEEE*, 8(2):14–36, 1991.

[11] A. V. Dandawate and G. B. Giannakis. Statistical tests for presence of cyclostationarity. *IEEE Transactions on Signal Processing*, 42, Sep 1994.

[12] G. Huang and J. K. Tugnait. On cyclic autocorrelation based spectrum sensing for cognitive radio systems in gaussian noise. In *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on*, Sept 2011.

[13] W. Gardner. Cyclostationarity in Communications and Signal Processing. In *IEEE Press*, 1994.

[14] S.D. Blunt, P. Yatham, and J. Stiles. Intrapulse Radar-Embedded Communications. *Aerospace and Electronic Systems, IEEE Transactions on*, 46(3):1185–1200, July 2010.

[15] Z. Hijaz and V.S. Frost. A Method for Analyzing the Impact of Interference on a Wireless Link with AMC, HARQ, and Finite Queue. In *Wireless Personal Multimedia Communications, Symposium on*, 2014.

[16] J. R. Hampton. Introduction to MIMO ommunications. In *Cambridge University Press*, 2005.

[17] Zaid Hijaz and Victor S Frost. Exploiting OFDM systems for covert communication. In *IEEE Military Communications Conference*, 2010.

[18] S. Chiu, D. Stoyan, and W. Kendall. Stochastic Geometry and its Applications, Third Ed. *Wiley*, 2013.

[19] M. Haenggi. Stochastic Geometry for Wireless Networks. *Wiley*, 2012.

[20] F. Baccelli and B. Blaszczyszyn. Stochastic Geometry and Wireless Networks, Volume I-Theory. *Inria*, 2009.

[21] Rodger E. Ziemer. Fundamentals of Spread Spectrum Modulation. *Morgan and Claypool*, 207.

[22] L. K. Nguyen, M. A. Blanco, and L. J. Sparace. On the sensitivity of wideband radiometric detection for low probability of intercept and probability of detection (lpi/lpd) in frequency hopped systems. In *MILCOM 2013 - 2013 IEEE Military Communications Conference*, Nov 2013.

[23] Y. R. Zheng and L. L. Fan. Performance metrics for low probability of detection in cooperative communication networks. In *OCEANS 2016 - Shanghai*, April 2016.

[24] N. Vankayalapati and S. Kay. Asymptotically optimal detection of low probability of intercept signals using distributed sensors. *IEEE Transactions on Aerospace and Electronic Systems*, 48(1), Jan 2012.

[25] G.D. Weeks, J.K. Townsend, and J.A. Freebersyer. A Method and Metric for Quantitatively Defining Low Probability of Detection. In *Military Communications Conference, 1998*.

[26] R. F. Mills and G. E. Prescott. Detectability models for multiple access low-probability-of-intercept networks. *IEEE Transactions on Aerospace and Electronic Systems*, 36(3), Jul 2000.

[27] B. A. Bash, D. Goeckel, and D. Towsley. Limits of reliable communication with low probability of detection on awgn channels. *IEEE Journal on Selected Areas in Communications*, 31, September 2013.

[28] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha. Hiding information in noise: fundamental limits of covert wireless communication. *IEEE Communications Magazine*, 53, Dec 2015.

[29] R.F. Mills and G.E. Prescott. Waveform Design and Analysis of Frequency Hopping LPI Networks. In *IEEE Military Communications Conference, 1995.*, volume 2, Nov 1995.

[30] R. Soltani, B. Bash, D. Goeckel, S. Guha, and D. Towsley. Covert single-hop communication in a wireless network with distributed artificial noise generation. In *Communication, Control, and Computing (Allerton), 2014 52nd Annual Allerton Conference on*, Sept 2014.

[31] S. D. Blunt, J. G. Metcalf, C. R. Biggs, and E. Perrins. Performance Characteristics and Metrics for Intra-Pulse Radar-Embedded Communication. *IEEE Journal on Selected Areas in Communications*, (10), Dec. 2011.

[32] J. G. Metcalf, C. Sahin, S. D. Blunt, and M. Rangaswamy. Analysis of Symbol Design Strategies for Inrapulse Radar-Embedded Communications. *IEEE Trans. Aerospace and Electronic Systems*, (4), Oct. 2015.

[33] Z. Hijaz and V.S. Frost. The Impact of Interference from a Covert Link on a Data Link UsingAMC, and Hybrid ARQ. In *Performance Computing and Communications Conference, IEEE International*, 2013.

[34] T. Yucek and H. Arslan. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Communications Surveys Tutorials*, 11(1):116–130, 2009.

[35] F. F. Digham, M. S. Alouini, and Marvin K. Simon. On the energy detection of unknown signals over fading channels. In *Communications, 2003. ICC '03. IEEE International Conference on*, volume 5, pages 3575–3579 vol.5, 2003.

[36] H. Urkowitz. Energy detection of unknown deterministic signals. *Proceedings of the IEEE*, 55(4):523–531, April 1967.

[37] A.P.S. Pillai. Probability, Random Variables and Stochastic Processes, 4th Ed. *Mc Graw Hill*, 2002.

[38] 3GPP. E-UTRA UE Radio Transmission and Reception. *3GPP TS 36.101*, v1.0.0.

[39] A. Papoulis and S. Pillai. Probability, Random Variables and Stochastic Processes, 4th Ed. *Wiley*, 2010.

[40] K. B. Oldham. Approximation for the x exp(x2) erfc(x) Function. *Mathematics of Computaion*, 22, 1968.

[41] 3GPP. TS 36.211 Evolved Universal Terresttial Radio Access Physical Channels and Modulation. *3GPP*, 2008.

[42] D.L.Y. Ye. Linear and nonlinear programming, 3rd edition. *Wiley*, 2008.

[43] D. Moltchanov. Distance distributions in random networks. In *Ad-Hoc Networks*, volume 10, Aug. 2012.