INTERFERENCE ISSUES IN MODERN COMMUNICATIONS SYSTEMS

by

SONG LIU

A Dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Electrical and Computer Engineering

Written under the direction of

Professor Wade Trappe and Professor Larry Greenstein

and approved by

_____

_____

_____

_____

New Brunswick, New Jersey

October, 2010

ABSTRACT OF THE DISSERTATION

Interference Issues in Modern Communications Systems

By SONG LIU

Dissertation Directors:
Professor Wade Trappe and Professor Larry Greenstein

A critical component of a communication system's design is the analysis of potential electromagnetic interference from within the system and from outside sources. Through physical and mathematical modeling, we can quantify the impact of interference on key performance metrics of the system and pursue an optimal design based on certain interference constraints. In this dissertation, we investigate several interference related issues in three emerging technologies: Broadband over Power Line (BPL), Dynamic Spectrum Access (DSA), and Mobile Ad Hoc Networks (MANET).

In the BPL study, we analyze the radio interference from a BPL system operating between 2 MHz and several tens of MHz. An overhead medium-voltage power line is modeled as a 3-phase set of parallel wires above a lossy earth. Both a near-exact solution and a closed-form far-field approximation are presented. The maximum allowable excitation voltage vs. frequency is computed by assuming compliance with FCC field strength limits. These calibration results are used to study the interference to both terrestrial and airborne services, using noise floor increase as a metric of interference severity. We also quantify the relationship between BPL capacity and BPL interference.

In the DSA study, we propose a solution to spectrum policy enforcement in DSA networks involving the detection of unauthorized spectrum usage. We formulate the anomalous usage detection problem using statistical significance testing. The detection problem is investigated considering two cases, characterized by whether the authorized (primary) transmitter is mobile or fixed. We propose a detection scheme for each case, respectively, by exploiting the spatial pattern of received signal

energy across a network of sensors. Analytical models are formulated when the distribution of the energy measurements is given and we present an algorithm using machine learning techniques to solve the general case when the statistics of the energy measurements are unknown.

In the MANET study, we propose a two-phase interference classification framework in a CSMA/CA-based MANET. It classifies different jamming attacks in a 3-D metric space and distinguishes unintentional interference and interference-free conditions based on the consistency of ACK errors and received signal strength.

Acknowledgements

This thesis would not have been possible without the insightful guidance, generous help and great patience from people with whom I have been lucky to spend years of my Ph.D. study.

My deepest gratitude goes to my co-advisor, Professor Larry J. Greenstein. He not only guided me throughout the course of my study, but also shaped my attitude towards my career and life. His extensive knowledge, experience and exceptional precision were pivotal in my research. This work would not have been accomplished without his encouragement and patience.

I am deeply grateful to my co-advisor, Professor Wade Trappe, who not only gave me great freedom to define my research, but also offered me insightful and timely advice. His passion for research and innovation motivated me to complete this thesis.

I am indebted to Professor Yingying Chen of Stevens Institute of Technology, not only for serving on my Ph.D. dissertation committee, but also for her invaluable collaboration and generous financial support to my research publications.

I am appreciative to Professor Narayan Mandayam, as my Ph.D. dissertation committee member, for his dedication and valuable advice on this thesis. I am also thankful to Professor Yanyong Zhang for serving on my Ph.D. proposal exam committee. My better understanding of the thesis topic greatly benefited from their insightful comments. The informal but informative discussions with my fellow WINLAB colleagues have been indispensable to this work, and I would like to particularly acknowledge the help from Ruoheng Liu, Jing Lei, Liang Xiao, Xiaojun Tang, Lin Luo, Suli Zhao, Zhibin Wu, Xiangpeng Jing, Chandrasekharan Raman, Suhas Mathur, and Tingting Sun.

Last and most importantly, I am grateful to my wife, Yali Liu, for her love, understanding, patience and encouragement, and to my parents who have unconditionally supported and encouraged me to travel to the other side of the world to pursue my dreams.

Dedication

To Yali, and to my parents.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Motivation

A critical component of any communication system design is the analysis of potential electromagnetic interference from inside and outside sources. In the RF environment, interference generally limits the useable range of communication signals. Prior to deploying a new device, either an intentional RF transmitter or an unintentional emitter, an engineering analysis has to be performed regarding its impact on incumbent users and its vulnerability to the environment. Using a physical and mathematical description of interference, an optimal design can be pursued given the interference constraints. Recent years have witnessed technological advances of communications devices in terms of waveform adaptation, frequency agility, and mobility. New applications have been initiated for economic and efficient delivery of broadband signals. Consequently, higher demands for spectrum and greater density of RF devices have brought new challenges to the management of interference. In this thesis, we will investigate interference issues in three emerging technologies: Broadband over Power Line (BPL), Dynamic Spectrum Access (DSA), and Mobile Ad Hoc Networks (MANET).

1.1.1 Broadband over Power Line (BPL)

The emergence of BPL communications has attracted increasing attention in the past few years [2, 3]. Through its vast infrastructure and capability of interconnecting virtually every premise, the electric power distribution grid presents an economically attractive option for broadband signal delivery *in the last mile*. In the United States, BPL networks are categorized into two classes [4]:

(1) Access BPL, operating at frequencies between 1.705 MHz and 80 MHz over low- and medium-voltage power lines for interconnection between customer premises and the Internet; and (2) In-House BPL, using low-voltage wiring and electric power outlets for networking within a user's premises and/or connecting end premises to access BPL networks. As a medium designed for transmission of AC power at 60 Hz, power lines carrying broadband signals may cause perceptible interference to incumbent radio services by leaking in their operating frequency range, including Federal communications, shortwave and TV broadcasting, and amateur radios. The interference concerns regarding BPL have launched several field tests and analytical studies, e.g., [5] and [6]. Nevertheless, most existing results depend on specific configurations and a general consensus has been difficult to find. On the other hand, although several modulation and interference mitigation techniques have been proposed, the evaluation of BPL capacity has been rarely addressed under interference constraints, which is critical to the viability of BPL systems.

In this thesis, we investigate the electromagnetic (EM) emissions of an access BPL system on overhead medium-voltage (MV) wires, a configuration of particular interest for US deployments. We have chosen to focus on MV BPL instead of in-house networks because (a) its EM emissions are more likely to interfere with the public radio services due to its large physical dimension and near-street locations; (b) MV BPL has a simpler system structure that can possibly be abstracted into analytical models without loss of generality. Our work is aimed at providing an analytical framework for computing BPL-created electric fields with good accuracy and assessing the BPL interference in a general sense so that the results will not be confined to particular system configurations.

1.1.2 Dynamic Spectrum Access (DSA) Using Cognitive Radios

The increasingly scarce spectrum and its significant underutilization in today's wireless networks has prompted the development of a new communication paradigm to exploit existing spectrum resources dynamically. This new paradigm is referred to as Dynamic Spectrum Access (DSA) using Cognitive Radios (CR), or NeXt Generation (xG) Networks [7]. Among several forms of DSA, opportunistic spectrum access is perhaps the most appealing solution due to its flexibility and its compatibility with minimal interference to legacy systems. An opportunistic spectrum access network has a hierarchical access structure, where CR (secondary) users sense and make opportunistic

use of idle spectrum resources without causing harmful interference to incumbent (primary) users (e.g., TV services between 54 to 862 MHz [8]).

The openness of the lower-layer protocol stacks in cognitive radios, and their subsequent ability to adapt their waveforms, makes them an appealing solution to DSA. The open nature of their protocols will increase the flexibility of spectrum utilization and promote spectrally-efficient communication. Nevertheless, due to the exposure of the protocol stacks to the public for development, CR platforms can become a tempting target for adversaries or irresponsible secondary users [9]. A misuse of a CR can significantly compromise the benefits of DSA and threaten the privileges of incumbent users. For example, an improperly programmed CR may accidentally transmit in the operating band of a primary user, and fail to adhere to policies requiring it to vacate that spectrum. Therefore, having the ability to enforce spectrum etiquettes is critical to the effectiveness and correctness of a DSA system. In this thesis, we aim to provide a systematic solution to reliable DSA, including the network structure and policy enforcement. We will propose two detection schemes dedicated to a DSA environment according to the mobility of an authorized transmitter.

Identification of a malicious or reckless spectrum usage is an essential component of etiquette enforcement functions. This is basically a problem of distinguishing bad (unauthorized) transmissions from good (authorized) ones. While sophisticated signal processing techniques have been designed for detecting a desired signal from interference [10, 11], they are of little help in this new paradigm of spectrum access. In many DSA systems (e.g., spectrum leasing), there can be a heterogeneous collection of authorized users and it is impractical to enumerate all of their signal structures. Even if the authorized signal is known (e.g., TV signals in IEEE 802.22), unauthorized users can disguise themselves by emulating authorized signals [12]. Therefore, an effective detection mechanism should not rely on programmable features, such as signal patterns. Fortunately, there is one aspect of the problem that cannot be easily modified—the propagation channel. This motivates us to pursue a reliable detection approach by making use of the characteristics of radio propagation. Specifically, our detection will be based on the measurement of received signal energy at a group of collaborating sensors, and will incorporate propagation modeling to ascertain whether there is an anomalous transmission present.

1.1.3 Mobile Ad Hoc Network (MANET)

The communication protocols at different layers in a mobile ad hoc network (MANET) are designed under the assumption that all nodes obey the given specifications. However, a MANET is built upon a shared medium that makes it easy for selfish users to deviate from the underlying MAC protocol or for adversaries to launch jamming attacks. These attacks can be easily accomplished by emitting RF interference that prevents other nodes from accessing the network (i.e., denial-of-service (DoS) attacks [13]).

Ensuring resilience to DoS attacks is essential towards building a secure and dependable MANET. In general, a defense strategy consists of detection and appropriate countermeasures against network anomalies. Significant progress have been made in the literature to thwart jamming-based DoS threats through physical and MAC layer mechanisms. Many defense schemes are shown to be effective against certain types of jamming attacks. Such schemes include frame masking for protocol-aware reactive jammers [14], channel hopping for narrow band jammers [15], channel codings for low power jammers [16], and spatial retreats for powerful jammers [17]. However, existing detection methods can only tell whether a jamming attack is present but few are able to characterize the attack's behavior, which is the basis for choosing the corresponding defense schemes. The gap between the binary-answer (i.e., 'yes' or 'no') detection and dedicated countermeasure renders most of the existing defense proposals less effective when facing a sophisticated attacker, which can intelligently change its jamming strategies. Moreover, interference due to *hidden terminal problems* in a wireless network can cause throughput degradations similar to that caused by a jamming attack. Although such interference can be mitigated by MAC mechanisms, such as adaptive carrier sensing [18], without properly recognizing the cause of current network anomaly, we may over-react to a nonmalicious interference problem and may artificially introduce new threats to the network.

In this part of the thesis, we aim at classifying the interference behaviors in MANETs to bridge the gap between the existing detection solutions and effective countermeasures. Taking into account the dynamics of MANETs and the uncertainties of interference threats, we seek simple but robust metrics and generic classification methods.

1.2 Thesis Overview

1.2.1 Interference Evaluation of BPL Systems

To study the aforementioned interference issues in overhead MV BPL systems, we apply a bottom-up analytical method by modeling the electromagnetic fields from a 3-phase, arbitrarily long power lines over a lossy earth. The near-exact fields are presented in terms of Sommerfeld integrals and solved by direct numerical integration. For distances remote from the power line, moreover, a far-field closed-form solution is derived.

Using our field solutions, we first obtain a profile of BPL source voltage vs. frequency for attaining compliance with FCC field strength limits. Based on this profile, we evaluate BPL interference from the following three perspectives:

1. Interference impact from a single BPL on local terrestrial receivers is quantified in terms of a "critical distance" beyond which BPL interference is below ambient noise.

2. Aggregate radiation from a large BPL deployment could interfere with aeronautical radio services several kilometers above the earth and also with distant HF receivers. The interference impact to airborne receivers is quantified in terms of noise floor increase, and that to ionospheric radio applications is quantified in terms of the transmit power of an equivalent source.

3. Limiting the BPL transmission power can alleviate the BPL interference impact, but at the same time reduce the system capacity. Using the derived maximum allowable launch powers, we estimate system throughput bounds for two BPL bands, namely, a "lower band" from 2 to 30 MHz and an "upper band" from 32 to 60 MHz. In addition, we explore the possibility of trading the system capacity for less interference by adjusting the launch powers.

1.2.2 Interference Detection in DSA Networks

A robust and dependable design of an anomaly detection should not rely on a comprehensive description about anomalous behaviors, which is generally not attainable in practice. As a result, our detection method is based solely on energy measurements from authorized transmitters and we formulate the detection problem as a statistical significance test. Here, we define a normal usage

scenario as having no more than one transmitter–static or mobile–operating in each portion (e.g., channel) of the spectrum. Based on this assumption, our work is motivated by two properties of the spatial distribution of the received signal strength (RSS):

- The RSS (or received power in dB) from a single transmitter[1] decays approximately linearly with the logarithmic distance from the source, but it is no longer the case when the RSS is a sum of multiple transmitters at different locations.
- Transmitters at different locations will lead to different spatial distributions of the RSS. This spatial map, or *signalprint*, is an effective characterization of a transmitter.

By making use of these properties, we propose two detection methods according to the mobility of the authorized transmitter. Specifically, when the authorized transmitter is mobile, we exploit the property that dB path loss tends to increase linearly with log-distance. Unauthorized transmitters can then be detected by a significance test of the linearity of measured dB energy versus log-distance. For the case where the authorized transmitter is fixed, we use the notion of signalprints, i.e., the spatial pattern of RSS. Unauthorized transmitters can then be detected by a significance test by comparing the current pattern with a stored pattern of the authorized transmitter. In each case, we initially assume the sensor network knows the statistics of the detected energies, and thus it can set its decision region to obtain a specified false alarm rate. We also describe a machine-learning approach that can be used in the more general scenario when the statistics of the detected energies are *not* known.

1.2.3 Interference Classification in MANETs

The objective of this work is to understand the characteristics of network anomalies due to interference and, further, to devise a method to identify various interference scenarios. Being aware of a network anomaly, we want to know *what* and *where* the problem is. Such information is essential to the proper choice of countermeasures. A preferable solution would be a classifier that can distinguish among potential interference threats based on certain system measurements. Due to the dynamic topologies of MANETs, many vulnerabilities of MANETs arise due to unintentional

[1] Since the measuring circuit we use is commonly called an energy detector, we will use 'RSS' and 'energy' interchangeably in subsequent discussions.

interference and intentional jamming attacks. These vulnerabilities are highly dependent on the underlying technologies being used. As a result, our study has focused on a 802.11 CSMA/CA based MANET and we look into the problem from a packet sender's perspective. Specifically, by watching the statistics of the ACK (acknowledgment) from the receiver, the interference classification issue boils down to two fundamental questions:

- Is a data packet corrupted at the receiver?
- Is an ACK corrupted at the sender?

Correspondingly, a variety of interference scenarios can be classified into: (a) unintentional interference, (b) random jamming to the sender, (c) protocol-aware reactive jamming to the sender, (d) random or reactive jamming to the receiver, and (e) combined jamming targeting both the sender and receiver.

Based on the above problem definition, we propose three metrics that measure the reception of ACK's at the sender. The three metrics form a 3-dimensional space onto which all interference scenarios can be mapped. In addition, we utilize the consistency of the frame error rate and received signal strength to handle the case where a malicious jammer tries to emulate unintentional interference. The existing consistency model is extended so as to distinguish between low link quality (low SNR), unintentional interference, and malicious jamming. We note that the proposed classification scheme is carried out by the sender without the receiver's collaboration (except for sending ACK's). Such a non-cooperative scheme improves the robustness of the classifier against interference and thus is preferable in a dynamic MANET system.

1.3 Background Literature

1.3.1 Broadband Communications over Medium-Voltage Power Lines

Modeling the electromagnetic field from power lines in free-space above a homogenous conducting earth is a canonical problem in electromagnetics [19, 20]. The study was begun with an electric dipole radiating above a lossy half-space, published by Sommerfeld in 1909 [21]. The problem was treated by solving Maxwell's equations with the boundary conditions on the air-ground interface and the results were presented in terms of the Sommerfeld integrals [22, 23]. Since then, the problem

of a dipole has been extensively studied and numerous analytical approximations (e.g. [24–26]) have been proposed. For the problem of a horizontal line with finite electrical dimensions, several numerical techniques have been employed, such as the method of moments (MoM) [27] and the fast multipole method (FMM) [28]. Program packages are also available for this purpose, such as NEC-4 [29].

Meanwhile, a significant amount of effort has been expended on the transmission line characteristics above lossy ground. The first attempt was reported by Carson in 1926 [30]. In this classic paper, Carson presented the solutions for distribution parameter of a quasi-TEM transmission line, which is valid in the low-frequency range or for a highly conducting ground. A self-contained exact model was developed decades later by Wait, in his well known full-wave analysis [31], which generalizes Carson's approximation. Further studies discovered a new pole and a new branch cut of the modal equations in addition to the three known terms and identified the physical meanings and significance of all five spectral current components [32, 33]. Simple formulas of transmission line approximations were recently developed for multi-parallel line structures [34–37].

Following the push for commercialization, investigations have been carried out on various aspects of BPL systems, including the electromagnetic compatibility (EMC) [38], channel characteristics [39], modulation techniques [40] and capacity [41]. Among these research efforts, the potential electromagnetic interference from BPL to incumbent radio services has been recognized as the most essential issue. Since the first regulations for BPL emissions were published in 2004 [4], interference concerns have launched considerable field tests and analytical studies [3, 5, 6]. Nevertheless, some key aspects of the measurement and assessment of BPL emissions remain vague, such as the measurement height and the extrapolation factor (i.e., the dB/decade factor used to predict the field strength falloff with lateral distance) [42]. Thus, general agreement is hard to find among existing results. In addition, although several modulation and interference mitigation techniques have been proposed, the evaluation of BPL capacity has been rarely addressed under emission constraints, an issue which is critical to the viability of BPL systems.

1.3.2 Anomaly Detection in Wireless Networks

Spectrum usage enforcement is an emerging issue with the development of cognitive radios. The authors in [9] presented a trusted radio infrastructure dedicated to spectrum regulation in a DSA environment. The work formalized the spectrum policies and proposed a sensing architecture which is the system basis of our study. An unauthorized user in a DSA network can either be a reckless radio or a malicious attacker. The attack by emulating a primary user [43], is in fact a spoofing attack specially launched in DSA networks for illegal occupation of the spectrum. Detection methods based on location verification were proposed in [43] and [44]. Given the location of the primary transmitter, dedicated sensors collaboratively verify the source location of a received signal by its path loss fading rate, time difference of arrival, and location of the maximum received signal strength. All these methods are non-interactive and do not require modifying the incumbent system. However, they all assume the primary transmitter's location is known and far away from the sensing area where illegal users might reside. Otherwise, these methods may not work well due to the low accuracy of their location estimations.

Although few research efforts are dedicated to anomaly detection in DSA networks, there is a rich body of works addressing the detection of spoofing attacks in generic wireless networks. Received signal strength (RSS) based detection is one of the extensively studied methods due to its low implementation complexity and inherent correspondence to the propagation environments. The most related work to ours was published in [45]. In that work, two transmitters at different locations are distinguished by comparing their *signalprints*, which is a vector of RSS measured at multiple receivers. The proposed method shares the same principle as fingerprint-based localization [46]. Specifically, transmitters at different locations lead to different spatial distributions of RSS and thus an attacker can be detected by examining the difference between its signalprint and the authentic one. Without specifying the false alarm probability, the paper reported above 95% detection accuracy in a testbed experiment. However, since the method is not based on the statistics of RSS, it is impossible to choose a detection threshold according to a desired false alarm probability.

On the other hand, model-based detection methods are based on the stochastic characteristics of RSS, where the detection threshold can be analytically determined given the false alarm probability. In [47], the authors proposed a Gaussian Mixture Model (GMM) to characterize the distribution

of RSS, given the fact that commercial 802.11 radio devices generally have multiple antennas. The RSS from an authentic transmitter is profiled in terms of its GMM model parameters and attackers are detected using a likelihood-ratio test based on this profile. The method demonstrated superior performance to the method in [45]. However, it requires a constant transmission power at the authentic transmitter during detection, which limits its application in a more general system. A frequency domain fingerprint method was proposed in [48], where a profile of the channel response is built between the legitimate transmitter and a receiver. The method also assumed a constant transmission power of the authentic user in order to compare two measurements at different times.

1.3.3 Interference Detection and Countermeasures in MANETs

In general, interference related network anomalies can be characterized either as selfish misbehavior or as malicious jamming attacks, both of which can lead to DoS attacks in MANETs.

Detection of a selfish misbehavior is relatively easy because the selfish node is either an internal user of the network or an intruder who tries to maximize its own throughput. Such a misbehavior can be detected by preventive approaches via modifying the existing protocols. The authors in [49] addressed the MAC layer misbehavior detection by modifying a centralized 802.11 protocol. The main idea is to let the receiver assign and send back-off values to the sender in CTS and ACK frames and then use them to detect potential misbehavior. Based on the corrected MAC protocol, a rapid method of detecting selfish attacks through the access point (AP) is proposed. This mechanism has several limitations, such as the possible collusion between sender and receiver. The authors in [50] extended this idea by presenting an algorithm that ensures honest backoff selection among the sender and a receiver as long as one of the participants does not misbehave. While such approaches can detect some attacks, the modification of the protocol requires an update of the IEEE 802.11 installed base, making it difficult to deploy. The authors in [51] proposed to detect a selfish misbehavior through a system called DOMINO. Their detection scheme for backoff manipulation is based on comparing average values of the backoff to given thresholds. The authors in [50] improved the detection performance by proposing a new metric based on the entropy of the backoff process. These methods are based on monitoring internal users' behaviors and thus are not applicable for malicious attacks in the more general cases.

The anomalous behaviors that concern us are those resulting in a throughput decrease at some

or all users in the network. Hence, an effective DoS attack should be perceivable by monitoring the statistical changes with legitimate users' traffic, whether it is launched by a selfish user or a malicious attacker. In [52], a nonparametric detection mechanism is presented for CSMA/CA MAC layer DoS attacks that does not require any modification to the existing protocols. The authors proposed a metric called "explainability", which quantifies the probability of each collision during two successful transmissions and performs detection based on the M-truncated sequential Kolmogorov-Smirnov statistics. This metric is superior to the collision frequency based metric. However, the "explainability" must be calculated offline using an approximation method, which cannot adapt to the dynamic changes of the network.

Selfish misbehavior has been addressed mostly from a game theoretic perspective considering all nodes to be selfish. The goal in a game theoretic setting is to design distributed protocols that guarantee, for each node, the existence, uniqueness and convergence to a Nash equilibrium with an acceptable throughput. In order to obtain a desired Nash equilibrium, each node is assigned a cost for each time it accesses the channel. For example in [49], the authors consider the case of selfish users in Aloha who attempt to maximize their throughput and minimize the cost for accessing the channel (e.g. energy consumption). Another game theoretic scheme for CSMA/CA schemes is presented in [53]. It shows how a Nash equilibrium is achieved among selfish users when the cost for accessing the channel repeatedly is that the user is jammed by another node. A node jams anonymously any other node that achieves higher throughput than the average of everyone else (assuming nodes always have data to transmit, the throughput of every node should be fair).

Ensuring resilience to DoS attacks is essential towards building a secure and dependable MANET. In general, a defense strategy consist of detection and appropriate countermeasures against network anomalies. Significant progress has been made in the literature to thwart jamming based DoS threats through physical and MAC layer mechanisms. Many defense schemes are shown effective to certain types of jamming attacks, such as frame masking for protocol-aware reactive jammers [14], channel hoping for narrow band jammers [15,54], channel codings for low power jammers [16,55], incentive and punishment for selfish jammers [49, 56], and spatial retreats for powerful jammers [17, 57].

1.4 Contributions of the Thesis

The distinctive contributions of this thesis are outlined as follows with respect to the three communication technologies.

1.4.1 BPL

In the BPL study, we investigate the radio interference from BPL based on a near-exact electromagnetic model. Based on the numerical computations for the near emission field and the closed-form solution for the radiation far field, we show that:

1. BPL interference to local incumbent services can be discernible (out to a "critical distance" that can be as high as 85 meters) with high probability if the FCC limits are just met.

2. BPL interference to airborne receivers can be significant, depending on the ambient noise level in aircraft; thus, the excluded frequency bands specified in the FCC rules for aeronautical communications should remain.

3. The equivalent radiated transmit power of aggregate BPL deployments is far below that of a typical ham radio and so the interference threat to ionospheric radio services is negligible.

4. Practical BPL throughputs are attainable while meeting the FCC requirements.

5. If a simple power reduction scheme is adopted to mitigate the interference, the range of BPL interference can be reduced by 15 meters at the cost of 100 Mbps in capacity.

1.4.2 DSA

In the work involving the detection of interference in DSA networks, we first present a network structure and a spectrum access policy to guarantee authorized users will not interfere with each other. We then address the detection of anomalous spectrum usage through several statistical significance testing formulations. Based on this framework, we have done the following:

1. We propose two new interference detection algorithms, one for the case where the authorized transmitter is mobile and one that works better but only for the stationary case.

2. Provided the distribution of the authorized signal energy is known, we present analytical solutions to determining detection thresholds based on specified false alarm probabilities.

3. In the more general case where the analysis is not tractable, we propose to utilize a machine learning technique, Support Vector Machine, to derive empirical thresholds.

1.4.3 MANET

To classify interference in MANETs, we propose an interference classification framework, which distinguish between interference-free, unintentional interference, and jamming attacks. Our contributions include the following:

1. We remove the ambiguities in the existing consistency model of ACK errors and received signal strength and extend the function to classify unintentional interference and jamming attacks.

2. We introduce new metrics based on the statistics of ACK receptions, which are more reliable thanks to the short and fixed length of ACK.

3. The new metrics form a 3-D space and map three basic jamming models onto three orthogonal bases, which simplifies the representation of a more sophisticated attack.

1.5 Organization of the Thesis

The rest of the thesis is organized as follows. Chapter 2 presents the BPL study, including the modeling and evaluation of BPL interference. Chapter 3 describes a network structure for dynamic spectrum access and propose detection techniques to enforce the spectrum etiquette. Chapter 4 presents an interference classification framework for CSMA/CA based MANETs. Chapter 5 concludes the thesis and discusses possible future work.

Chapter 2

Interference Evaluation of Overhead Medium-Voltage Broadband Powerline Systems

2.1 Field Model for Medium-Voltage Lines over Lossy Ground

2.1.1 Preamble

This section, along with the Appendices, comprise the mathematically intensive part of the chapter. It sets forth the basic assumptions and formulas upon which our predictions of BPL electric field strength are built. The outcome is a general equation from which we obtain results for regions near the power line, and a simplification thereof, from which we compute the far (radiation) fields. Both solutions will find use in the system-related studies that follow.

The access BPL system under study consists of three-phase aerial MV wires over lossy ground, and couplers located at utility poles where BPL signals are injected, repeated, or extracted from the wires, as depicted in Figure 2.1. This is intended to represent generic BPL systems in the United States. Given equivalent lumped impedances at each coupler, a segment of the wires between every two couplers can be modeled as horizontal parallel lines above the ground, as shown in Figure 2.2.

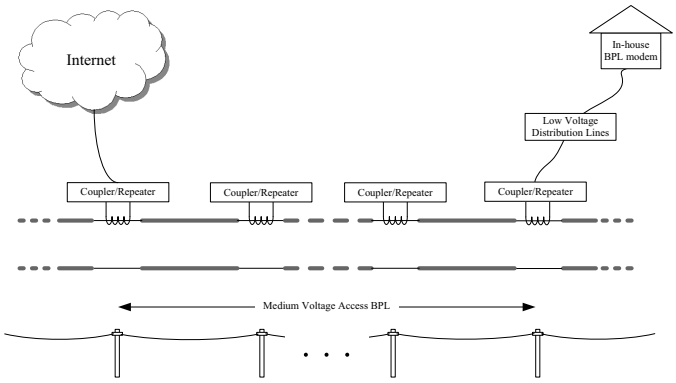
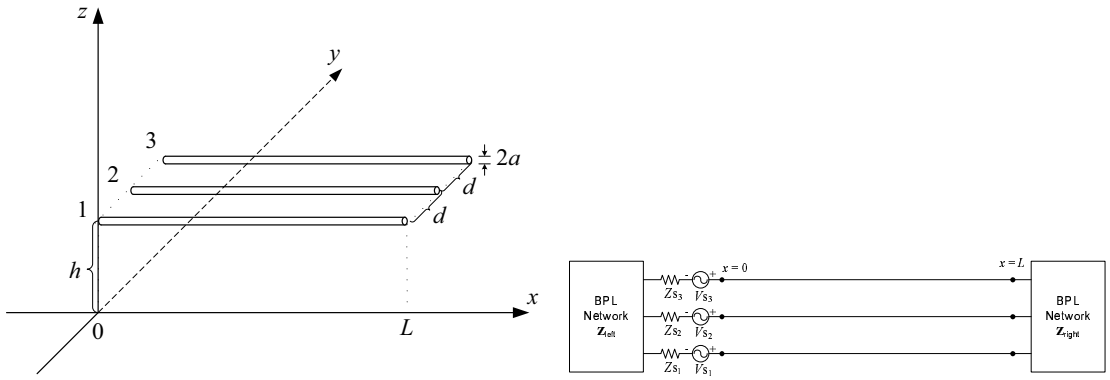


Figure 2.1: BPL system on medium-voltage overhead power lines.



(a) (b)

Figure 2.2: Single-segment model of a three-phase medium-voltage power line. (a) Physical structure of the three-phase line above ground. There is the possibility of a BPL coupler (not shown) on each line at $x = 0$. (b) Equivalent circuit of the BPL part. Regarding each coupler as a signal injector or repeater, it can be represented by an equivalent voltage source and series impedance at $x = 0$.

To facilitate a tractable analysis, in this study we ignore the effects of the insulation that might cover these lines and also the vertical sag caused by their weight. In Appendix A, we illustrate the validity of these simplifications for our assumed line geometry.

In this power line model, each line has a height h above ground, a spacing d from each other, a radius a, and a length L. With the assumption of a series excitation, an equivalent voltage source V_{Si}, and a source impedance Z_{Si}, connect to the i-th wire in series ($i = 1, 2, 3$ for the three-phase wires), representing the configuration of source couplers (i.e., injectors or repeaters). At both ends of the segment, attached networks are abstracted by equivalent lumped impedances. The ground is lossy with conductivity σ_g, permittivity ϵ_g, and permeability μ_0. Later, we will quantify our specific assumptions for the various geometric parameters, BPL sources, and line impedances.

2.1.2 Exact Field Solution

The procedure for modeling parallel lines of infinite length above a lossy ground is well described in [37]. That solution is to be extended here to the scenario of arbitrarily long lines (i.e., both finite and semi-infinite length).

First, consider a horizontal electric dipole located at the point $(x_0, 0, h)$, along the x-axis, and having the length Δl. The ground is lossy with conductivity σ_g, permittivity ϵ_g, and permeability μ_0. The Hertz potentials of the dipole at an observation position (x, y, z) above the ground (i.e.

$z > 0$) is given by [24]:

$$\overline{\mathbf{\Pi}} = \hat{\mathbf{x}}\Pi_x + \hat{\mathbf{z}}\Pi_z \quad \text{and} \quad \Pi_x = \Pi_{xd} + \Pi_{xr}^0 + \Pi_{xr}^1, \tag{2.1}$$

where

$$\begin{aligned}
&\Pi_{xd}(x,y,z) \\
&= -\frac{I(x_0)\Delta l}{8\pi^2\omega\epsilon_0}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{1}{k_{0z}}\exp\{-j[k_x(x-x_0)+k_y y+k_{0z}|z-h|]\}\,dk_x\,dk_y, &\text{(2.2a)}\\
&\Pi_{xr}^0(x,y,z) \\
&=\frac{I(x_0)\Delta l}{8\pi^2\omega\epsilon_0}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{1}{k_{0z}}\exp\{-j[k_x(x-x_0)+k_y y+k_{0z}(z+h)]\}\,dk_x\,dk_y, &\text{(2.2b)}\\
&\Pi_{xr}^1(x,y,z) \\
&= -\frac{I(x_0)\Delta l}{8\pi^2\omega\epsilon_0}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{2}{k_{0z}+k_{gz}}\exp\{-j[k_x(x-x_0)+k_y y+k_{0z}(z+h)]\}\,dk_x\,dk_y, &\text{(2.2c)}\\
&\Pi_z(x,y,z) \\
&= -\frac{I(x_0)\Delta l}{8\pi^2\omega\epsilon_0}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\frac{2k_x(k_{0z}-k_{gz})}{k_g^2k_{0z}+k_0^2k_{gz}}\exp\{-j[k_x(x-x_0)+k_y y+k_{0z}(z+h)]\}\,dk_x\,dk_y. &\text{(2.2d)}
\end{aligned}$$

The wavenumbers of free space and the ground are

$$k_0 = \omega\sqrt{\mu_0\epsilon_0}, \quad \text{and} \quad k_g = k_0\sqrt{\frac{\epsilon_g}{\epsilon_0} - \frac{j\sigma_g}{\omega\epsilon_0}}, \tag{2.3}$$

and ϵ_0 and μ_0 are free space permittivity and permeability, respectively. From the derivation, it can be shown that the integrating factors k_x and k_y represent the x- and y- components of the wavenumbers, respectively. In (2.6),

$$k_{0z}^2 = k_0^2 - k_x^2 - k_y^2, \quad \text{and} \quad k_{gz}^2 = k_g^2 - k_x^2 - k_y^2. \tag{2.4}$$

The polarities of k_{0z} and k_{gz} are chosen to satisfy the radiation constraints, meaning that

$$\text{Im}[k_{0z}] \leq 0 \quad \text{and} \quad \text{Im}[k_{gz}] \leq 0. \tag{2.5}$$

For a single horizontal line carrying a harmonic current $I(x_0) = I_0 e^{-\gamma x_0}$, the Hertzian potentials can be readily obtained by integrating (2.2a) over the entire length of the line (by letting $\Delta l = dx_0$). Expressing the electric and magnetic fields in terms of the Hertzian potential [58], we

have, for an arbitrarily long line,

$$E_x(x,y,z)$$
$$= jM\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} A(k_x)[(k_0^2-k_x^2)P(k_x,k_y)+(k_y^2+k_{0z}k_{gz})Q(k_x,k_y)]\,dk_x\,dk_y, \tag{2.6a}$$

$$E_y(x,y,z)$$
$$= -jM\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} A(k_x)k_xk_y[P(k_x,k_y)+Q(k_x,k_y)]\,dk_x\,dk_y, \tag{2.6b}$$

$$E_z(x,y,z)$$
$$= -jM\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} A(k_x)k_x[k_{0z}P(k_x,k_y)+k_{gz}Q(k_x,k_y)]\,dk_x\,dk_y, \tag{2.6c}$$

$$H_x(x,y,z)$$
$$= -\frac{1}{j\omega\mu_0}M\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} A(k_x)k_xk_y(k_{0z}-k_{gz})Q(k_x,k_y)\,dk_x\,dk_y, \tag{2.6d}$$

$$H_y(x,y,z)$$
$$= -\frac{1}{j\omega\mu_0}M\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} A(k_x)[k_0^2k_{0z}P(k_x,k_y)-(k_y^2k_{gz}-k_y^2k_{0z}-k_0^2k_{gz})Q(k_x,k_y)]\,dk_x\,dk_y, \tag{2.6e}$$

$$H_z(x,y,z)$$
$$= \frac{1}{j\omega\mu_0}M\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} A(k_x)k_yk_0^2[P(k_x,k_y)+\frac{k_g^2k_{0z}+k_{0k}^2k_{gz}}{k_0^2k_{0z}+k_0^2k_{gz}}Q(k_x,k_y)]\,dk_x\,dk_y, \tag{2.6f}$$

where

$$M=\frac{j\omega\mu_0}{8\pi^2k_0^2}I_0, \tag{2.7}$$

$$P(k_x,k_y)=\frac{1}{k_{0z}}[\pm e^{-jk_{0z}|z-h|}-e^{-jk_{0z}(z+h)}]e^{-j(k_xx+k_yy)}, \tag{2.8}$$

$$Q(k_x,k_y)=\frac{2k_0^2}{k_g^2k_{0z}+k_0^2k_{gz}}e^{-j[k_xx+k_yy+k_{0z}(z+h)]}, \tag{2.9}$$

and

$$A(k_x)=\frac{\sin[L(k_x+j\gamma)/2]}{(k_x+j\gamma)/2}e^{jL(k_x+j\gamma)/2}. \tag{2.10}$$

The minus sign in $P(\cdot)$ applies to E_z when $z<h$. Note that $P(\cdot)$ and $Q(\cdot)$ are also functions of (x,y,z). In the exact field solutions of (2.6), $A(k_x)$ is the only term affected by the dimension, L, of the line. For an infinitely long line (i.e., $-\infty<x<\infty$), one can easily recover the same solutions as those given by Wait's full-wave analysis [31]. For a finitely long line, by assuming $0\le x_0\le L$ in (2.2a), we have the L-dependent result in (2.10). In the following analysis, we will

model a semi-infinitely long BPL where L goes to infinity. By assuming a lossy line (i.e. γ has a positive real part, which is usually true in practice[1]), $A(k_x)$ then reduces to

$$A(k_x) = \frac{1}{\gamma - jk_x}. \tag{2.11}$$

We see from (2.6) that the fields consist of two part, where $P(\cdot)$ corresponds to the case of a perfect conducting ground and $Q(\cdot)$ represents the increment due to the lossy effects of the imperfect ground. This can be verified by letting the ground conductivity $\sigma_g \to \infty$. Then, k_g and thus u_g will tend towards infinite values, which eliminates the $Q(\cdot)$ terms in the field solutions. Also, the image part (second term) of $P(\cdot)$ is canceled by the lossy term $Q(\cdot)$ when $k_g = k_0$, and it then yields the solution of a single wire in the free space.

So far, we have presented an exact formula for the fields from an arbitrarily long, single power line over lossy ground, with current propagating in one direction (left to right). We now consider a set of N parallel lines at the same height, separated horizontally by d meters. In general, currents in transmission lines consist of forward and backward waves, so the current in the i-th line has the form

$$I_i(x) = \sum_{k=1}^{N} T_{i,k}(I^+_{m,k}e^{-\gamma_k x} - I^-_{m,k}e^{\gamma_k x}). \tag{2.12}$$

The index k denotes the mode in each line, and we assume as many modes as lines. In our case, $N = 3$. The propagation constant γ_k is the k-th diagonal element of the 3-by-3 diagonal matrix γ; the coefficient $T_{i,k}$ is the (i,k)-th element of the 3-by-3 transformation matrix $\mathbf{T}$. γ and $\mathbf{T}$ can be obtained by the following diagonalization [59]:

$$\gamma^2 = \mathbf{T}^{-1}\mathbf{YZT} = \mathrm{diag}\{\gamma_1^2, \gamma_2^2, \ldots, \gamma_n^2\}, \tag{2.13}$$

where $\mathbf{Z}$ and $\mathbf{Y}$ are the per-unit-length series impedance and shunt admittance, both of which are 3×3 matrices. They were derived in [35] for the condition of parallel lines over a lossy earth. The mode current $I^+_{m,k}$ ($I^-_{m,k}$) is the k-th forward (backward) mode current [60], whose particular solution is obtained in Section 2.1.4.

If we take the field solutions (2.6) to be functions of I_0 and γ (see (2.7) and (2.10)), as well as of x, y, and z, each of the E and H components can be obtained as a summation of the fields

[1]It is required that the integral contour of k_x is always on the real axis. This is the case in the following numerical computations.

generated by the forward and backward currents in all the lines. Thus,

$$E_{all,\xi}(x,y,z) = \sum_{i=1}^{N}\sum_{k=1}^{N} T_{i,k}[E_\xi(I^+_{m,k},\gamma_k,x,y-y_i,z) - E_\xi(I^-_{m,k},-\gamma_k,x,y-y_i,z)] \quad (2.14)$$

$$H_{all,\xi}(x,y,z) = \sum_{i=1}^{N}\sum_{k=1}^{N} T_{i,k}[H_\xi(I^+_{m,k},\gamma_k,x,y-y_i,z) - H_\xi(I^-_{m,k},-\gamma_k,x,y-y_i,z)] \quad (2.15)$$

where E_ξ and H_ξ are the fields having the form (2.6); ξ denotes x, y or z; and $y_i = (i-1)d$ is the y-coordinate of the i-th line, Figure 2.2.

2.1.3 Far-Field Approximation

Although closed-form evaluations have been extensively carried out for the Sommerfeld integrals in (2.6) in the near field, they are either limited by certain assumptions or are too complicated to provide tractable solutions [61]. Nonetheless, The radiation fields can be readily and accurately approximated by using a quick method of saddle-point approximation [62]. We now present that method.

It is easy to see that the total solutions (2.6) are Weyl-type integrals, by rewriting (2.8) and (2.9) as

$$P(k_x,k_y) = \pm F_d(k_x,k_y) - F_r(k_x,k_y) \quad (2.16)$$

and

$$Q(k_x,k_y) = \frac{2k_0^2 k_{0z}}{k_g^2 k_{0z} + k_0^2 k_{gz}} F_r(k_x,k_y), \quad (2.17)$$

where

$$\begin{aligned} F_d(k_x,k_y) &= \frac{1}{k_{0z}}\exp\{-jk_x x - jk_y y - jk_{0z}|z-h|\} := \frac{e^{-j\overrightarrow{\mathbf{k}}\,\overrightarrow{\mathbf{R}}}}{k_{0z}}, \\ F_r(k_x,k_y) &= \frac{1}{k_{0z}}\exp\{-jk_x x - jk_y y - jk_{0z}(z+h)\} := \frac{e^{-j\overrightarrow{\mathbf{k}}\,\overrightarrow{\mathbf{R}}}}{k_{0z}}, \end{aligned} \quad (2.18)$$

and $\overrightarrow{\mathbf{k}} = k_x\hat{x} + k_y\hat{y} + k_z\hat{z}$ is the propagation vector of plane wave components at the observation point and $\overrightarrow{\mathbf{R}}$ is the distance vector from the source point to the observation point. Now we can see the property of the far field. When $|\overrightarrow{\mathbf{R}}| \to \infty$, (2.18) will be rapidly oscillatory compared with other terms in the integrands of the field solution. According to the discussions in [63] and [62], most of the contributions to the integrals in (2.6) are from the vicinity of the saddle point (k_{x0}, k_{y0}), defined by

$$\frac{\partial}{\partial k_x}(\overrightarrow{\mathbf{k}}\,\overrightarrow{\mathbf{R}})\Big|_{k_{x0}} = 0, \quad \frac{\partial}{\partial k_y}(\overrightarrow{\mathbf{k}}\,\overrightarrow{\mathbf{R}})\Big|_{k_{y0}} = 0. \quad (2.19)$$

Thus

$$\frac{k_{x0}}{x} = \frac{k_{y0}}{y} = \frac{k_{z0}}{z}. \tag{2.20}$$

It is apparent that the saddle point corresponds to the plane wave component whose propagation vector points from the source to the observation point. Physically, this means the propagation direction (i.e. that of the Poynting vector) at that point. Therefore, we can take all terms in (2.6) out of the integrals, except $F_d(k_x, k_y)$ and $F_r(k_x, k_y)$, by setting

$$k_x = \frac{x}{R}k_0, \quad k_y = \frac{y}{R}k_0, \quad k_{0z} = \frac{|z \pm h|}{R}k_0, \tag{2.21}$$

where $R = \sqrt{x^2 + y^2 + (z \pm h)^2}$. Then, the remaining integrals are

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} F_{d,r}(k_x, k_y)\, dk_x\, dk_y = 2\pi j \frac{\exp(-jk_0R)}{R}. \tag{2.22}$$

The double integrals are now completely removed from the solution. The resulting far-field approximations to the E and H components are

$$\begin{aligned}
E_x(x,y,z) &= -2\pi k_0^2 M \left\{ A(k_{xd})(R_d^2 - x^2)\frac{\exp(-jk_0R_d)}{R_d^3} - A(k_{xr})(R_r^2 - x^2)\frac{\exp(-jk_0R_r)}{R_r^3} \right. \\
&\quad \left. + A(k_{xr})[y^2 + (z+h)u_g]Q_r\frac{\exp(-jk_0R_r)}{R_r^3} \right\}, \\
E_y(x,y,z) &= 2\pi k_0^2 Mxy \left\{ A(k_{xd})\frac{\exp(-jk_0R_d)}{R_d^3} - A(k_{xr})\frac{\exp(-jk_0R_r)}{R_r^3} \right. \\
&\quad \left. + A(k_{xr})Q_r\frac{\exp(-jk_0R_r)}{R_r^3} \right\}, \\
E_z(x,y,z) &= 2\pi k_0^2 Mx \left\{ A(k_{xd})(z-h)\frac{\exp(-jk_0R_d)}{R_d^3} - A(k_{xr})(z+h)\frac{\exp(-jk_0R_r)}{R_r^3} \right. \\
&\quad \left. + A(k_{xr})u_gQ_r\frac{\exp(-jk_0R_r)}{R_r^3} \right\}, \\
H_x(x,y,z) &= -2\pi j\frac{k_0^3}{j\omega\mu_0}MA(k_{xr})xy[(z+h) - u_g]Q_r\frac{\exp(-jk_0R_r)}{R_r^4}, \\
H_y(x,y,z) &= -2\pi j\frac{k_0^3}{j\omega\mu_0}M \left\{ A(k_{xd})(z-h)\frac{\exp(-jk_0R_d)}{R_d^2} - A(k_{xr})(z+h)\frac{\exp(-jk_0R_r)}{R_r^2} \right. \\
&\quad \left. - A(k_{xr})(y^2u_g - y^2(z+h) - u_g)Q_r\frac{\exp(-jk_0R_r)}{R_r^4} \right\}, \\
H_z(x,y,z) &= 2\pi j\frac{k_0^3}{j\omega\mu_0}My \left\{ A(k_{xd})\frac{\exp(-jk_0R_d)}{R_d^2} - A(k_{xr})\frac{\exp(-jk_0R_r)}{R_r^2} \right. \\
&\quad \left. + A(k_{xr})\frac{2(z+h)}{(z+h)+u_g}\frac{\exp(-jk_0R_r)}{R_r^2} \right\},
\end{aligned} \tag{2.23}$$

where $A(\cdot)$ is the same function defined in (2.6),

$$k_{xd} = \frac{x}{R_d} k_0, \quad k_{xr} = \frac{x}{R_r} k_0, \tag{2.24}$$

$$R_d = \sqrt{x^2 + y^2 + (z-h)^2}, \quad R_r = \sqrt{x^2 + y^2 + (z+h)^2}, \tag{2.25}$$

and

$$Q_r = \frac{2k_0^2(z+h)}{k_g^2(z+h) + k_0^2 u_g}, \quad u_g = \sqrt{\frac{k_g^2}{k_0^2} R_r^2 - (x^2+y^2)} \tag{2.26}$$

Note that the solutions given there are for a single current component propagating to the right, over an x-range from 0 to L. For the $N = 3$ parallel lines, each carrying three mode currents, and each of these with forward and backward components, each field component in (2.23) must be summed over 18 propagating current components, just as in (2.14).

The time-averaged radiation power per unit area at a receiving antenna can be readily obtained by the Poynting vector, which is

$$P_r = \frac{1}{2}\mathbf{E} \times \mathbf{H}^* = \frac{|\mathbf{E}|^2}{2\eta}, \tag{2.27}$$

where $\eta = 120\pi \approx 377\Omega$ is the characteristic impedance of free space.

2.1.4 Bidirectional BPL Line Model and Calculation of Line Currents

Due to line attenuation, a BPL signal may be regenerated one or more times before entering a subscriber's premise. At the same time, the attenuation can be sufficiently mild that several couplers are passed before regeneration is necessary. A BPL line structure showing several evenly-spaced couplers is shown in Figure 2.3, where the solid lines denote a multi-line (specifically, a 3-phase) system; the bold symbols denote matrices; and a coupler is represented as either a series impedance to a particular signal (no regeneration) or as a series impedance plus a voltage source (regeneration). We call the interval between couplers a *BPL section*, and we call the set of sections between regenerations a *BPL span*.

Here, we complete the solutions for the EM-fields in space, by making assumptions leading to formulas for the BPL mode currents, represented by the vectors $\mathbf{I}_{\mathrm{m}}^{+}$ and $\mathbf{I}_{\mathrm{m}}^{-}$. Using these solutions to compute the total E-field magnitude at $y = 30$ m ($y = 10$ m) for $f < 30$ MHz ($f > 30$ MHz), we will solve for the maximum allowable source voltage as a function of frequency.

Our assumptions are as follows:

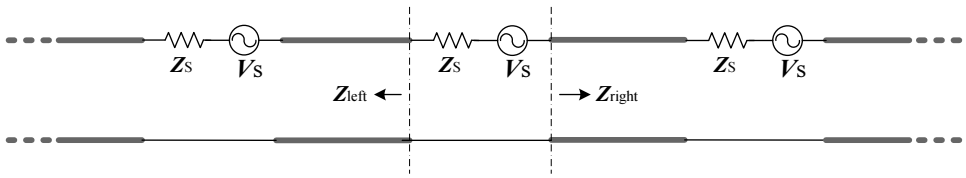


Figure 2.3: BPL line with evenly spaced couplers.

1. Signals are injected onto and extracted from the power line system via an inductive coupler associated with the outer conductor ($i = 1$ in Figure 2.2). That is, there are no source voltages or impedances for $i = 2, 3$. The coupler is essentially a transformer which reflects an equivalent series impedance onto the line from its secondary side and, when there is signal regeneration, also reflects an equivalent voltage source.

2. A BPL section is 100 m long and a BPL span is six sections (600 m) long [64].

3. All attachments to the line, both physical and inductive, lead to added signal attenuations that can amount to as much as 30 dB in 1 km [64]. We model this as 3 dB of attenuation at each coupler; more specifically, we treat it as a smooth, continuous excess attenuation—over and above the natural attenuation of the line—of 30 dB/km.

4. Subscribers are separated by means of frequency division multiple access (FDMA) among the OFDM tones transmitted over the line. Moreover, the FDMA subset for a given user at a given regenerator operates in the time-division mode between incoming and outgoing signals, so that regenerated signals will not be interfered with by the residue from the previous span.

5. By symmetry, the effective input impedances $\mathbf{Z}_{\rm left}$ and $\mathbf{Z}_{\rm right}$, Figure 2.3, should have the same statistical variations over time and sections. We exploit this to set $\mathbf{Z}_{\rm left} = \mathbf{Z}_{\rm right}$. We simplify matters even further by assuming the line is matched in both directions, so that $\mathbf{Z}_{\rm left} = \mathbf{Z}_{\rm right} = \mathbf{Z}_{\rm C}$, where $\mathbf{Z}_{\rm C}$ is the characteristic impedance matrix. The effect of this assumption is to drive $\mathbf{I}^-$ to 0.

6. For the above simplification to be even approximately valid, the impedance of the series coupler on the line should be a small fraction of the characteristic impedance. Our calculations for $\mathbf{Z}_{\rm C}$ show that the diagonal elements of this matrix (i.e., the self impedance of the power lines) are approximately resistant across BPL frequencies. Specifically, the diagonal elements of the

characteristic matrix range from $90 - j15$ ohms at 2 MHz, to $480 - j1.2$ ohms at 10 MHz, and to $487 + j1$ ohms at 80 MHz. Therefore, we postulate a series impedance matrix, $\mathbf{Z}_{\mathrm{S}}$, whose only non-zero term, namely, the $(1, 1)$ element, is resistant and equal to one-nineteenth of the resistance of $Z_{\mathrm{C},11}$. This is equivalent to coupling a very small series resistance onto one of the 3-phase lines. Appendix B show that, under this assumption, the power launched down the line to the right by the regenerator is 10 dB below the maximum launch power possible. This loss in power is an acceptable price to pay for keeping the line essentially transparent to the BPL couplers.

Based on the above assumptions, a BPL signal injected onto the lines will transmit power in both directions, under similar propagation conditions. Therefore, the BPL model in Figure 2.2 is now generalized into a bi-directional one, with semi-infinitely long lines on each side. Then, the only needed modification to the field solution (2.6) is

$$A(k_x) = \frac{1}{\gamma - jk_x} + \frac{1}{\gamma + jk_x} = \frac{2\gamma}{\gamma^2 + k_x^2}. \tag{2.28}$$

The above assumptions and simplifications can certainly be challenged, and they clearly represent the least rigorous part of our formulation. At the same time, they are practical and reasonable, and permit us to proceed numerically. Other assumptions, particularly about line matching, would lead us, under the FCC constraints, to essentially the same values of allowable BPL currents at $x = 0$, and *these values largely determine the maximum E-field along x for a given y*. For this reason, we believe the numerical results of this study are robust to any reasonable departures from the above simplifying assumptions. We can therefore proceed to set limits on source voltage, and to then quantify BPL interference.

2.1.5 Summary

The E and H field components from a BPL segment of length L can be computed as double sums, (2.14), of double integrals, (2.6), and are totally determined by the matrices/vectors γ, $\mathbf{T}$, $\mathbf{I}^+$ and $\mathbf{I}^-$, which are introduced in Section 2.1.2. A simplification of the equations, valid for the far fields, is given in Section 2.1.3. The current vectors $\mathbf{I}^+$ and $\mathbf{I}^-$ must be made concrete for purposes of computation, and specific assumptions regarding the BPL line couplers (including their equivalent

impedance, Appendix B) lead to simplified solutions. These assumptions are enumerated in Section 2.1.4.

In the following section, the exact solutions of Section 2.1.2 are combined with numerical routines to compute the electric fields close to the power line, i.e., those too close to be regarded as far fields. For these computations, we make use of the numerical integration package CUBPACK [65].

2.2 Evaluation of BPL Interference

The parameters listed in Table 2.1 will be used for the numerical computations. They are chosen to reflect the prevailing MV line configurations in the United States and an "average" condition of earth [5, 38, 64].

Table 2.1: Parameters of the 3-Phase MV Transmission Line

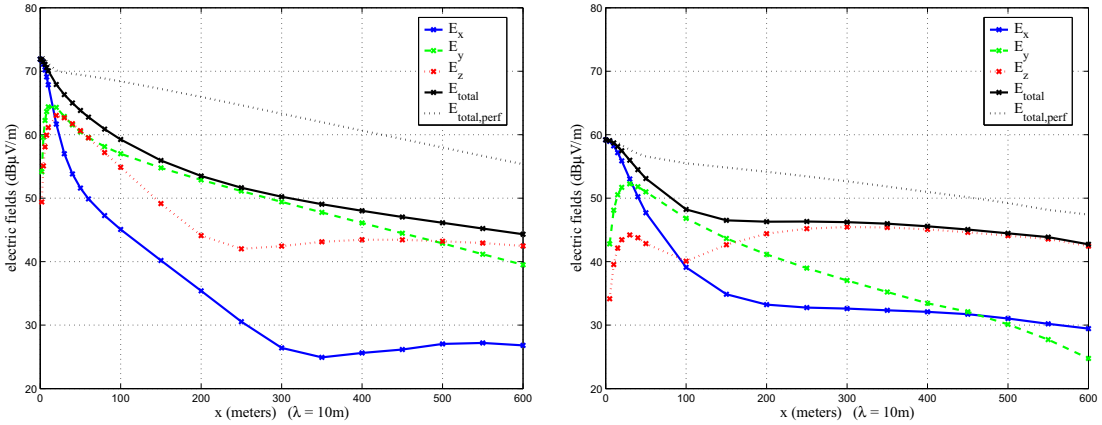
Line Topology	**Value**	**Line Conductor**	**Value**	**Ground**	**Value**
h	8.5 m	σ_w	5.8×10^7 S/m	σ_g	5 mS/m
a	5 mm	$\varepsilon_w/\varepsilon_0$	1	$\varepsilon_g/\varepsilon_0$	15
d	0.6 m				

2.2.1 Source Calibration — Setting Limits on the BPL Signal

The emissions from access BPL are subject to FCC Part 15 rules. These rules require the BPL system to comply with the limits for intentional radiators when operating below 30 MHz and those for unintentional radiators (Class A) when operating above 30 MHz [4]. The emission limits are summarized in Table 2.2. The limits and related bandwidths are based on measuring equipment using a CISPR quasi-peak detector. The measurement distance is specified as the horizontal distance between the measurement antenna and the closest point of the equipment under test. To ensure that the emissions from BPL meet the FCC limits, the maximum allowable excitation must be

Table 2.2: FCC Part 15 Electric Field limits for BPL on medium voltage lines [4].

Frequency (MHz)	**Field Strength (μV/m)**	**Measured Distance (m)**	**Measured Bandwidth (KHz)**
1.705 - 30	30	30	9
30 - 80	90	10	120



(a) $y = 10$ meters from the wires (b) $y = 30$ meters from the wires

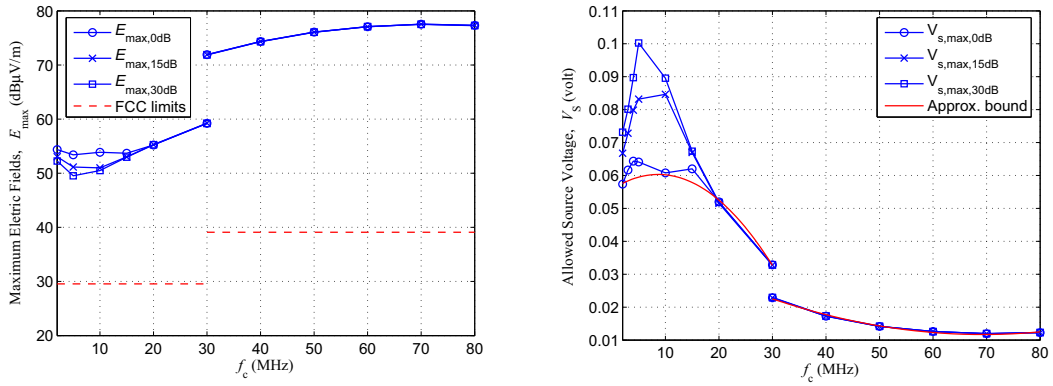
Figure 2.4: Electric fields from a BPL span carrying signals at 30 MHz, with $V_S = 1$ volt (In these plots, $x = 0$ corresponds to the point of BPL injection.)

determined. Since the limits are defined at distances close to the wires (i.e., at 10 m and 30 m), the following calibration results are based on the near-field solution.

According to FCC measurement guidelines [66], the field strength should be measured at distances of 0, 1/4, 1/2, 3/4, and 1 wavelength down the line from the BPL injection point. As a conservative test, we search for the maximum field down the line up to 600 meters, which is greater than the wavelength of the lowest BPL frequency (i.e. 1.7 MHz). A measurement height of 2 meters is used for all the results, to emulate the heights of widely used mobile antennas. Assuming a unity source voltage $V_S = 1$ volt, we obtain Figure 2.4, which depicts the electric field of a BPL section at 30 MHz[2]. The total field strength assuming a perfectly conducting ground is also presented. Following the assumptions of Section 2.1.4, these computations were made for an excess attenuation of 30 dB/km. The maximum electric field strength is seen to be ~ 72 dBμv/m at $y = 10$ m and ~ 60 dBμv/m at $y = 30$ m. The 12-dB difference is greater than that which would occur in a radiation for field ($20 \log_{10}(30/10) \sim 9.5$ dB), because the near field falls off more rapidly with distance, i.e., faster than y^{-1}.

The maximum electric field strength was computed across the BPL frequency band, as illustrated in Figure 2.5a. The electric field strength considered in our study is the root-mean-square (rms) magnitude of the total field. To take into account the coupler mismatching loss, results include an

[2]The BPL power propagates in both directions from its injection point. Under our assumptions, the field strength as a function of x is symmetrical about the injection point ($x = 0$ in Figure 2.4).



(a) (b)

Figure 2.5: Calibrating source voltage based on the maximum electric field strength from 2 to 80 MHz. (a) Maximum field strength for $V_S = 1$ volt at $y = 30$ m ($f < 30$ MHz) and $y = 10$ m ($f > 30$ MHz). (b) Limits on BPL source voltage and a curve-fitting approximation. Note that the ordinate is in rms volts within the relevant bandwidth.

excess attenuation of 0, 15, and 30 dB/km. For an excess attenuation of 30 dB/km, the maximum field strength is decreased by 4 dB or less for frequencies up to 15 MHz. Note that excess attenuation has little impact at frequencies above 15 MHz.

To satisfy emission requirements, the source voltage must be scaled down from 1 volt for every frequency so that its rms value within the relevant bandwidth (i.e., 9 kHz for $f < 30$ MHz and 120 kHz for $f > 30$ MHz) just meets the FCC limits. The results are presented in Figure 2.5b for the excess attenuations of 0 dB, 15 and 30 dB/km. Here, we choose to calibrate the source voltage using an excess attenuation of 0 dB; this leads to V_S values that are conservative, specifically, they are lower by ~ 4 dB at $f = 5$ MHz and by less at all other frequencies.

A convenient formula for the approximate voltage limit was devised by curve-fitting the following model to the result with 0-dB excess attenuation (i.e., the most conservative limit)

$$V_{\rm S} = \begin{cases} a_1 f_c^2 + b_1 f_c + c_1, & \text{if} \quad f_c \leq 30\text{MHz}, \\ a_2 f_c^2 + b_2 f_c + c_2, & \text{if} \quad f_c \geq 30\text{MHz}, \end{cases} \tag{2.29}$$

where f_c is the operating frequency in MHz and $V_{\rm S}$ is in rms volts within the relevant bandwidth. The coefficients are given in Table 2.3, and the result is shown by the solid curve in Figure 2.5b. We use this formula as our model for allowed BPL source voltage vs. frequency.

Table 2.3: Coefficients of Approximation Formula (2.29)

Coefficient	Value	Coefficient	Value
a_1	-6.076×10^{-5}	a_2	7.008×10^{-6}
b_1	1.054×10^{-3}	b_2	-9.718×10^{-4}
c_1	0.05574	c_2	0.04538

2.2.2 Interference to Terrestrial Services

To assess the potential interference from BPL into incumbent services, we need to translate electric field strength into the power level at the receiver of a local radio. For fixed-gain antennas, the received emission power is given by [5]

$$P_{\text{emit}} = 10\log_{10}\left(\frac{|E_r|^2}{2\eta}\right) + 10\log_{10}\left(\frac{\lambda^2}{4\pi}\right) + G_r + 10\log_{10}(\phi) + \delta, (\text{dBW}) \tag{2.30}$$

where E_r is the incident field strength in V/m, η is the characteristic impedance of free space, λ is the emission wavelength in meters, G_r is the receiver antenna gain in dBi, ϕ is the average duty cycle of the BPL signal, and δ is a compensation for differences between rms and measured quasi-peak values. In this evaluation, $G_r = 0$ dB and $\delta = -2$ dB; and $\phi = 50\%$ is used, which assumes moderate Internet utilization.

As a potential interferer to nearby radio services, a BPL system should emit as little power as possible, consistent with its purpose. Under the current emission limits, however, BPL emission power can be substantially higher than typical ambient noise, as shown in Figure 2.6. Here, the BPL power density is the received power given in (2.30) divided by 9 kHz (120 kHz) if $f < 30$ MHz ($f > 30$ MHz). We choose the noise levels in a "business environment" and a "quiet rural environment", which are the highest and the lowest levels, respectively, of man-made ambient noise as defined in [67]. We see that, at the specified measurement distances, the current FCC limits can lead to the BPL emission powers 20 to 35 dB higher than the noise.

It thus appears that BPL emission can be deleterious even if they meet FCC limits. To examine this prospect in a more complete way, we used our computation program for the near field to conduct the following experiment:

1. We define an interference condition as occurring at an incumbent receiver if the BPL power density there equals or exceeds that of the ambient noise. The ambient noise is chosen as

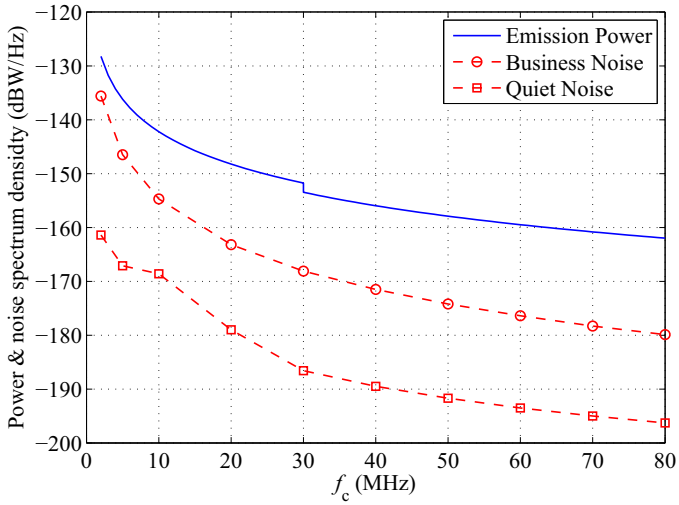


Figure 2.6: Maximum allowed emission power spectrum density from BPL at $y = 30$ m (for $f < 30$) MHz and at $y = 10$ m (for $f > 30$ MHz), compared with ambient noise level in a "business environment" and a "quiet rural environment".

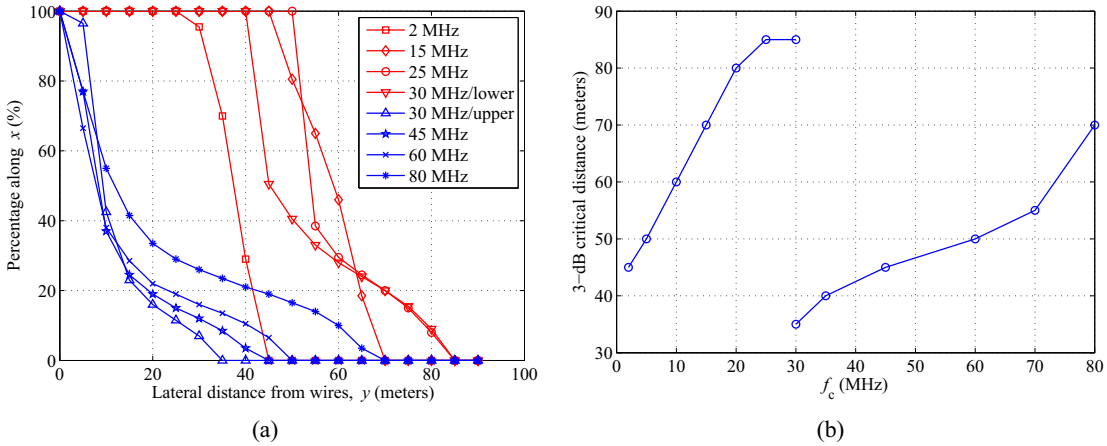
that in a "business environment". We define the *3-dB critical distance* as the smallest lateral distance from the power line for which no interference (as defined above) occurs.

2. We envision an incumbent receiver at a height $z = 2$ m; a lateral distance y of 0, 5, 10, 15, ..., 90 m; and a distance x along the transmission line within $L = 600$ m of the BPL source[3] (injection point).

3. For each y, we compute the percentage of x-positions between $x = 0$ and $x = L$ at which interference occurs, doing so for frequencies of 2, 15, 25, 30, 45, 60 and 80 MHz.

The results of this exercise are shown in Figure 2.7. For $f = 30$ MHz, we show two curves: One for the rules governing the lower band ($f < 30$ MHz), and one for the rules governing the upper band ($f > 30$ MHz). We see that the BPL interference impact is significantly greater for frequencies in the lower band. To completely avoid excess interference (meaning that the ordinate value is 0%), radio receivers have to be at a distance from the power lines of 45 to 85 m as f ranges from 2 MHz to 30 MHz. The corresponding distances for the upper band are from 35 to 70 m as f ranges from 30 MHz to 80 MHz.

[3]We assume the regenerator L meters to the right of $x = 0$ will generate the same field pattern, and so on down the line, leading to a periodic pattern of field strength $|E|$ vs. x, with period L. We can thus confine our attention to just one period.



(a) (b)

Figure 2.7: (a) Percentage of locations in longitudinal (x) direction where BPL interference is above the ambient noise. (b) 3-dB critical distance at various BPL frequencies.

To understand this difference, we note from Table 2.2 that the Part 15 requirement on E-field amplitude is 30 μV/m at $y = 30$ m, and 90 μV/m at $y = 10$ m. If these locations were in the far field, where $|E|$ is inversely proportional to y, these two requirements might seem commensurate. However, the near field is still dominant at these locations, so that $|E| \sim y^{-n}$, where n lies somewhere between 1 and 2. In this case, 90 μV/m at 10 m implies *less* than 30 μV/m at 30 m, i.e., it is a more stringent requirement. Moreover, these field strength limits are rms values within a specified bandwidth, namely, 9 kHz below 30 MHz and 120 kHz above 30 MHz. This amounts to a power spectrum density reduction of $\sim$ 11 dB for the allowed emissions above 30 MHz which, as Figure 2.7 shows, has major implications for the relative terrestrial interferences from these two bands. We will see similar differences between the two bands when we compare far-field interferences into airborne receivers and BPL throughputs.

2.2.3 Interference to Airborne Services

The FCC Part 15 Rules specify a set of bands at which to prohibit overhead MV BPL operation ([4], p. 148), as an additional measure to reduce harmful interference to aeronautical radio services. These excluded bands are currently used by federal aircraft stations in the 2 to 50 MHz frequency range and by commercial radionavigation services in the 74.8 to 75.2 MHz. In this section, we investigate the justification for such restrictions.

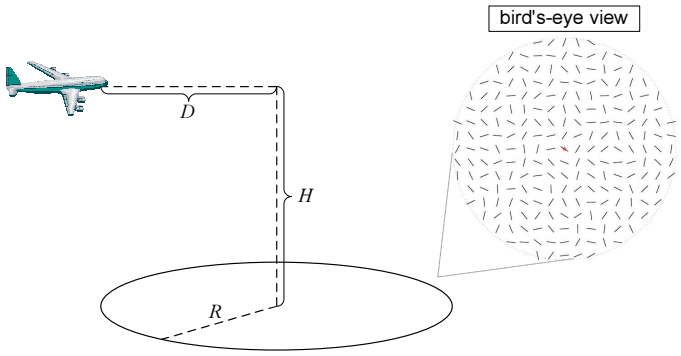


Figure 2.8: Interference to airborne radios from a mass BPL deployment on the ground with random directions.

We consider a circular area wherein BPL are placed with a fixed center-to-center spacings[4] and arbitrarily oriented. They form a grid structure as shown in Figure 2.8, where each short line indicates the orientation of a BPL span. Each numerical result is an average over 500 cases of random deployments where, for each deployment, the voltages from different BPL spans are assumed to add noncoherently.

We assume the BPL format is orthogonal frequency division multiplexing (OFDM); that, for concreteness, the tone spacing is 9 kHz; and that the transmit voltage per tone is chosen to just meet the FCC emission limits. The spectral density at a given frequency is then accurately estimated as the average received tone power at that frequency divided by the tone spacing.

We use the noise floor increase as a metric of the interference from the BPL aggregation, which is defined by [5]

$$\triangle N = 10 \log_{10}[(P_N + P_R)/P_N] \quad \text{(dB)}, \tag{2.31}$$

where P_N and P_R are the noise power and BPL radiation power, respectively. Hence, it represents the noise level increase, due to the BPL radiation, at the receiver of a victim radio service.

It is hard to predict the actual ambient noise level at an airborne receiver because of the complicated noise condition (e.g. engine, air flow, etc.). Therefore, we consider both the level in a "quiet rural environment" and that in a "business environment", to include a wide range of noise levels. BPL radiations were computed for both cases, from a BPL deployment[5] where $N = 221$ spans

[4]Although our BPL model is infinitely long, a signal is always attenuated to a negligible level within a certain distance. With the practical settings in Table 2.1, the effective propagation distance of a BPL signal is usually less than 1 km without regeneration.

[5]This results in a density of ~ 2.8 spans/km^2. If one BPL span carries broadband signals to 30 customers and 1

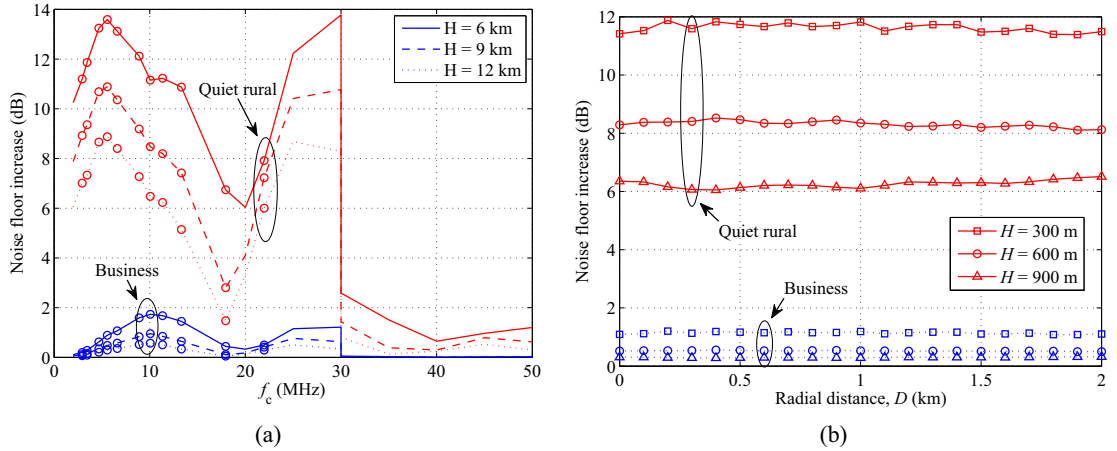


Figure 2.9: The noise floor increase from BPL interference at aircraft radio receivers. 221 BPL spans in a 5-km radius. (a) Federal aircraft stations in 2 to 50 MHz. The center frequencies at the excluded bands are indicated by small circles; (b) Radionavigation services at 75 MHz.

reside in a circular area with a radius of $R = 5$ km. Typical federal aircraft receivers in the 2 to 50 MHz frequency range operate at 18,000 to 40,000 feet (approximately 5.5 to 12 km) above ground and the radionavigation services at 75 MHz are used by aircrafts during climbing/landing from 0 to 3,000 feet (approximately 915 m) above ground. Therefore, heights of 6 km, 9 km and 12 km are considered in the 2 to 50 MHz frequency range, and heights of 300 m, 600 m and 900 m are considered at 75 MHz.

Figure 2.9 shows the noise floor increases at the center of the BPL deployment ($D = 0$ in Figure 2.8) in the 2 to 50 MHz frequency range, and those at various radial distances from the center of the deployment at 75 MHz. The results illustrate how much the noise level increase from the mass BPL deployment depends on the ambient noise levels at an aeronautical receiver. Assuming a less noisy environment (i.e., "quiet rural"), the tested deployment of BPL can cause up to a 14 dB increase in the noise level of a radio device traveling above it. On the other hand, a more noisy background (i.e., "business") can dominate this BPL interference. We also see that the BPL interference impact at frequencies above 30 MHz is mild, even for a quiet ambient environment. This is due to more stringent emission requirements set for this range of frequencies, as explained in Section 2.2.2.

We conclude from this exercise that due caution fully justifies the exclusion imposed by Part 15

---

of 4 urban households is a BPL customer, as predicted in [42], the deployment corresponds to a household density of $\sim 338/\text{km}^2$, which is far less than that in a major US city.

Rules on BPL usage at 75 MHz. The same applies to the exclusions at those frequencies in the 2-30 MHz band where federal aeronautical equipment operates.

2.2.4 Ionospheric Interference

We have shown that the direct radiation from a large BPL deployment can cause discernible interference to airborne receivers. Via ionospheric propagation, an aggregate radiation has the potential to raise noise levels at receivers hundreds of miles away. Ionosphere refraction is an important means of long-distance radio communication in the HF band (up to 30 MHz or up to 50 MHz depending on time-of-day, season, and sunspot cycle). Many government, military, amateur and commercial radio services reside in this frequency range, because of the ability to communicate over long distances. Since the HF band is also a major part of the BPL operating band, a large group of BPL spans operating at the same HF frequency may act like an effective HF transmitter and cause interference to incumbent receivers at a large distance.

This potential was investigated in Figure 2.10, where the total radiation power density from a large BPL deployment of 221 spans was computed for frequencies from 2 to 50 MHz. The BPL deployment setting is the same as that in Section 2.2.4. The result clearly shows that the aggregate radiation power for a large number of BPL spans at the same HF frequency is on the order of μW per KHz. This profile is very trivial compared to an amateur radio transmitter, which typically radiate 100 or 200 watts in a few KHz.

In one of our studies [68], we show that the aggregate radiation is proportional to the number of BPL spans. According to Figure 2.10, it would take an extremely large number of BPL spans (or equivalently, an extremely high density of BPL deployment) to achieve discernible interference at distant receivers. This large gap ensures that the BPL interference via ionospheric propagation is not an issue for amateur radios.

2.3 BPL Capacity Under Interference Constraint

The above study clearly shows that the BPL transmission power is bounded by its emission limit, which will further constrain the system capacity. Therefore, it is necessary for us to understand, (i) whether a viable BPL capacity can be achieved under current interference constraints; and (ii) the

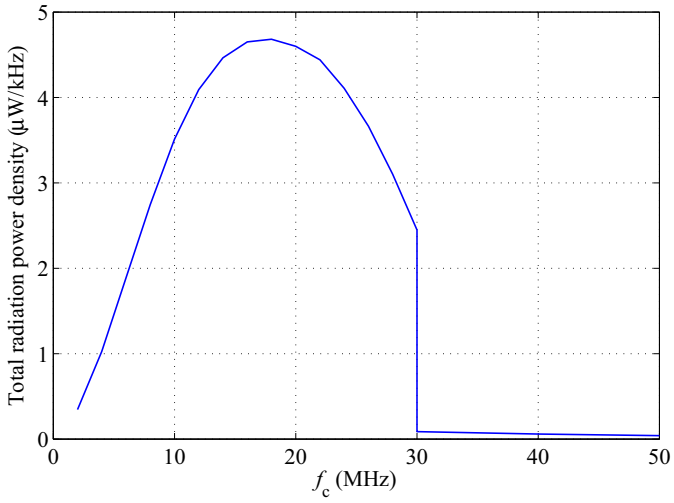


Figure 2.10: Total radiation power density from a large BPL deployment on the ground with random directions. $N = 221$ spans.

effectiveness of trading BPL capacity for less emission interference.

2.3.1 Capacity while Meeting FCC Rules

With knowledge of the maximum allowable BPL excitation, we can provide a rough estimate of the BPL capacity. Since allowable source voltage varies with frequency, attainable load power at the regenerators will also vary with frequency. Multicarrier modulation schemes such as OFDM are good choices for this condition, since frequency groups can be easily assigned different power levels, and also different modulations.

We will compute throughputs for two possible BPL systems, each occupying 28 MHz and using OFDM. One operates in a "lower band" from 2 to 30 MHz, and the other operates in an "upper band" from 32 to 60 MHz. Assuming additive flat Gaussian noise in each subcarrier channel, the Shannon capacity of a BPL system using OFDM with N subcarriers is given by

$$C = 0.5 \sum_{i=1}^{N} B_i \log_2 \left(1 + \frac{P_{L,i}}{N_{0,i} B_i} \right), \tag{2.32}$$

where the factor 0.5 accounts for the fact that time division is used at the regenerator to separate incoming (received) and outgoing (regenerated) OFDM packets. In addition:

1. $P_{L,i}$ is the power delivered by the i-th tone to the regenerator load, and it relates to the line current and regenerator impedance derived earlier. The current is the one associated with

Table 2.4: BPL throughputs (in Mbps) of two 28-MHz bands.

Δ_{L} (dB)	0	6	12	18	24
C	125	97	70	45	25
TP	88	62	38	19	8

(a) Lower band, [2, 30] MHz

Δ_{L} (dB)	0	6	12	18	24
C	72	46	24	9.3	2.8
TP	38	18	6.4	1.8	0.4

(b) Upper band, [32, 60] MHz

using the maximum allowable source voltage, V_S, and includes the effect of the assumed excess attenuation of 30 dB/km.

2. The noise spectrum density $N_{0,i}$ is the ambient noise level at the i-th tone frequency, as given in [69][6].

3. The noise bandwidth B_i is assumed here to be 9 kHz, corresponding to about 3111 tones in each 28-MHz band. Since V_S, as modeled by (2.29), is the rms voltage in a 9-kHz (120-kHz) bandwidth for the lower (upper) band, we can use (2.29) directly to get the source voltage in the lower band, and must scale (2.29) by $\sqrt{9/120}$ to get the source voltage in the upper band.

Clearly, (2.32) represents an upper bound on the throughput than can be achieved in a given BPL system. A practical lower bound on the throughput, based on the use of uncoded adaptive modulation, can be shown to be [71]

$$TP = 0.5 \sum_{i=1}^{N} B_i \log_2 \left(1 + \frac{P_{L,i}}{6.4 \times N_{0,i} B_i} \right). \tag{2.33}$$

We have computed results for both throughput measures, (2.32) and (2.33). We consider five different spacings of the regenerators, remembering that our default assumption is 600 m. Specifically, we consider excess losses (Δ_{L}) between regenerators of 0, 6, 12, 18 and 24 dB, corresponding to spacings (still assuming 30 dB/km excess attenuation) of 0, 200, 400, 600, and 800 meters. The results are given in Table 2.4 for both 28-MHz bands.

In these tables, C represents an upper bound on the total attainable throughput. We note that the numbers are a lot smaller than the 600-Mbps figure reported in [41]. To see why, we enumerate the major differences in assumptions between that study and this one:

[6]The referenced paper reports the noise level up to 25 MHz. Since there is generally less noise at higher frequencies [70], the noise density above 25 MHz is conservatively set to -120 dBm/Hz.

1. The earlier analysis omits the factor of 0.5 that we have assumed to reflect time division between reception and regeneration.

2. The earlier analysis assumes a total launch power of 10 mW, apportioned via water-filling among subcarriers spanning [2, 50] MHz. Assuming BPL voltages that satisfy Part 15 limits, we obtain a launch power that is lower by ~ 6 dB for the same band and is even lower for the smaller bandwidth (28 MHz) used in the present analysis.

3. In the earlier analysis, the estimate of 600-Mbps capacity pertains to a simple network with few junctions and no excess loss. The present analysis treats excess loss as a study parameter, starting at 0 dB.

If we adjust our calculations to match the transmit power, bandwidth and excess loss of the analysis in [41], with the power distributed uniformly *and* the time division factor of 0.5 omitted, we obtain a capacity $C \sim 560$ Mbps. The two analyses are thus reconciled.

In Table 2.4, TP is the total attainable throughput when the modulation for each subcarrier is uncoded *BPSK* or uncoded *M-QAM*, with the specific modulation (i.e., constellation size) chosen according to the received SNR for that subcarrier. For span lengths of 600-1000 m (excess loss of 18-24 dB), the throughputs in the lower band are in the range predicted in [64], i.e., ~ 10 Mbps or more. The results for both C and TP are decidedly lower for the upper band, a consequence of the tighter restrictions on BPL emissions in that band. This suggests that operators might choose the lower band for downlink (operator-to-subscriber) transmissions and the upper band for uplink (subscriber-to-operator) transmissions.

2.3.2 Tradeoff between Capacity and Interference

The most effective and reliable way to mitigate the BPL interference is to reduce the source power, although this will correspondingly degrade the throughput. Considering the desire for more stringent emission regulations [6], it is worth understanding the relationship between capacity and BPL interference potential.

Assuming the signal-to-noise ratio at the load receiver is large, we can approximate the capacity

of a BPL system by

$$\begin{aligned} C &= \int \log_2(1+\alpha_L(f)\alpha_M SNR(f))df \\ &\approx \int \log_2(\alpha_L(f)\alpha_M SNR(f))df \\ &= \int \log_2(\alpha_L(f)SNR(f))df + BW\log_2(\alpha_M), \end{aligned} \tag{2.34}$$

where $SNR(f)$ is the received signal-to-noise ratio in a narrow band channel, centered at f and with the source power just meeting the emission limits at each BPL frequency; $\alpha_L(f)$ accounts for the frequency-dependent loss due to any imperfect transmission conditions (e.g, multipath); α_M denotes the mitigation ratio of the source power, which we assume to be constant across the BPL frequency range. The first term of the approximation accounts for the capacity without power reduction (i.e., $\alpha_M = 1$). If, for example, $\alpha_L(f) = 1$, $SNR(f) = 1000$ (30 dB) and the BPL frequency range is from 2 to 80 MHz, the first term will be ~ 780 Mbps. The second term of the approximation is the reduction in capacity due to reducing α_M. If, for example, $\alpha_M = 0.5$ (a 3-dB reduction in transmit power), the capacity decrease will be ~ 78 Mbps.

Assuming an infinitely long BPL span[7], Figure 2.11 illustrates the tradeoff between BPL interference and BPL capacity by assuming a sufficiently large capacity (i.e., the first term of the approximation is greater than 800 Mbps). The interference is quantified in terms of the 3-dB critical distance (defined in Section 2.2.2), assuming "Business" ambient noise. The critical distance is approximately linear with capacity decrease up to 400 Mbps, where the critical distance is very short. The exchange rate is about 15 m/100 Mbps for most frequencies. Note that this slope is independent of the definition of the critical distance. It is in fact a function of the decay rate of the electric field in the lateral direction. Fox example, assume we define the critical distance as the lateral distance at which the noise increase is X dB. It can be shown that the distance-capacity slope is ~ 15 m/100 Mbps independent of X.

[7]That is, the lines span from $-\infty$ to ∞. This model simplifies the field computation by ignoring the longitudinal variations of the emission fields. The results should approximate the lateral variations of the fields in the vicinity of a long BPL span.

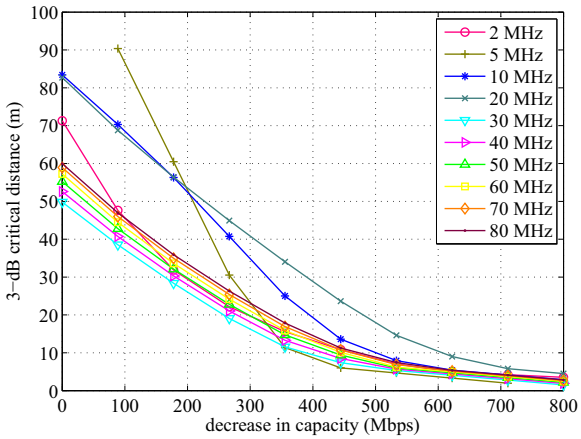


Figure 2.11: Relationship between interference (measured by the 3-dB critical distance) and capacity reduction. The ambient noise level is for a "business environment".

2.4 Summary

We have modeled the electromagnetic fields from a medium-voltage 3-phase power line mounted above a lossy earth and carrying BPL signals to and from Internet customers. Beginning with an exact formulation for the fields, we have made a number of practical assumptions and approximations to facilitate reductions to numerical results. This includes the use of the saddle point method to simply and accurately estimate the radiation far field. For computing near fields, corresponding to locations close to the power lines, we have resorted to the numerical computation of near-infinite double integrals. The methodology used here can be applied for various alternative assumptions about the power line dimensions and impedances, the BPL couplers and placements, and other parameters.

The near-field computation program developed from this effort was used to obtain a profile of BPL source voltage vs. frequency for attaining compliance with FCC field strength limits. This profile was used to determine BPL interference impact on local terrestrial receivers in terms of the percentage of the area where the BPL emission was perceptible. The far-field approximation was then used to assess the potential of aggregate interference to airborne receivers and HF radios via ionospheric propagation. Finally, we explored the tradeoff between BPL capacity and interference potential, and used the profiles of allowed source voltage vs. frequency to quantify system throughput bounds for two BPL bands, namely, a "lower band" from 2 to 30 MHz and an "upper band" from 32 to 60 MHz.

The numerical results show that: (i) BPL interference to local incumbent services can be discernible with high probability if the FCC limits are just met. (ii) BPL interference to airborne receivers can be significant, depending on the ambient noise level in aircraft; thus, the exclusive frequency bands specified for aeronautical communications should remain. (iii) The equivalent radiated transmit power of aggregate BPL deployments is far below that of a typical amateur radio and so the interference threat to ionospheric radio services is negligible. (iv) Reasonable throughputs can be achieved with launch powers for which the resulting E-fields meet FCC Part 15 rules. (v) By lowering the launch powers, one can reduce the interference range by roughly 15 meters for every 100-Mbps decrease in system capacity.

Chapter 3

Anomaly Detection in Dynamic Spectrum Access Networks

Dynamic spectrum access has been proposed as a means to share scarce radio resources, and requires devices to follow protocols that access spectrum resources in a proper, disciplined manner. For a cognitive radio network to achieve this goal, spectrum policies and the ability to enforce them are necessary. Detection of an unauthorized (anomalous) usage is one of the critical issues in spectrum etiquette enforcement. In this chapter, we first present a network structure for dynamic spectrum access and then formulate the anomalous usage detection problem using statistical significance testing. The detection problem is investigated considering two cases, namely, the authorized (primary) transmitter is (i) mobile and (ii) fixed. We propose a detection scheme for each case, respectively, by exploiting the spatial pattern of received signal energy across a network of sensors. Analytical models are formulated when the distribution of the energy measurements is given and, due to the intractability of the general problem, we present an algorithm using machine learning techniques to solve the general case when the statistics of the energy measurements are unknown.

3.1 A System Model of Dynamic Spectrum Access

3.1.1 DSA Network Structure

We consider a DSA network as illustrated in Figure 3.1, where licensed (i.e., primary) and unlicensed (i.e., secondary) transmitters are scattered in an area filled with auxiliary spectrum sensors. In the paradigm of DSA, secondary users make use of idle spectrum resources by opportunistically accessing the network in these idle bands, which will not result in interference to incumbent users. However, such a spectrum efficiency can be easily undermined by a reckless user or an attacker who disguises itself as the primary transmitter in an attempt to convince other secondary users that a primary users has returned to use that spectrum band. Thus, a spectrum access policy is necessary

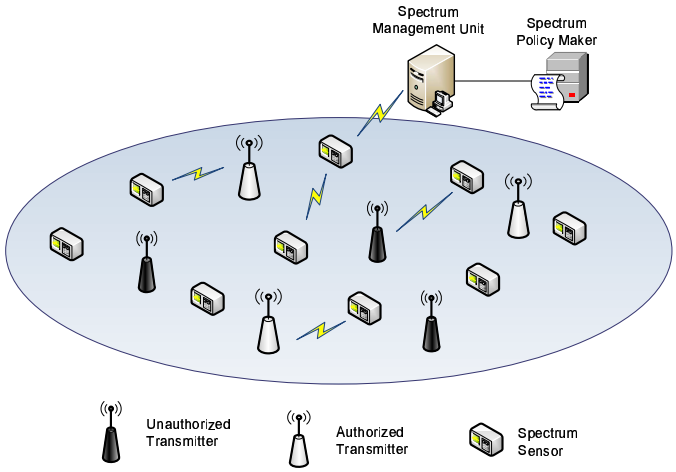


Figure 3.1: A DSA environment, with primary and unauthorized transmitters within an area populated with spectrum sensors. Spectrum sensors cooperatively detect the presence of the unauthorized transmitters via the local exchange of energy measurements.

as such a policy explicitly states the conditions for when a secondary user can and cannot use spectrum. The policies are defined by spectrum policy makers and are broadcast by a management unit, which can be either a stand alone central processor or a part of the primary transmitter's functions. For spectrum agility, the policies can change dynamically and users should be able to interpret them without human intervention. Interpreted languages, such as XG Policy Language (XGPL), have been proposed to formalize the policies [9]. To enforce spectrum policies, a trusted spectrum sensor network is responsible for collecting spectrum usage data and reporting them to the spectrum management unit. The management unit applies appropriate detection rules to identify anomalous usage and performs localization to locate anomalous transmitters.

To minimize the interference, we assume there should be no more than one authorized transmitter in a certain spectrum band at any time. In addition, since an interference signal may use the same signal structure as a primary signal, the proposed detection algorithms will be based on received signal energy.

3.1.2 Energy Detection Model at A Sensor

We consider a time-domain energy detector consisting of a band-pass filter (BPF), Nyquist sampling A/D converter, square-law device and integrator, as depicted in Figure 3.2. At the n-th sensor, the

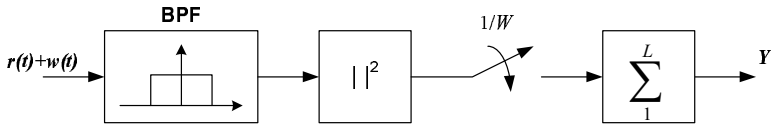


Figure 3.2: The signal processing of the assumed energy detector. The square-law envelope detector produces the squared envelope of the BPF output, which is then sampled at uniform intervals. W is the bandwidth of the BPF. The energy is estimated as the sum of L such samples.

output of an energy detector can be expressed as

$$y_n = \sum_{l=1}^{L} |r_n(l) + w_n(l)|^2 \tag{3.1}$$

where $r_n(l)$ is the complex received signal at the n-th sensor, and $w_n(l)$ is the complex Gaussian noise with zero mean and variance σ_w^2 at each phase. $w_n(l)$ is i.i.d. over the L temporal energy samples. Previous work has shown that y_n/σ_w^2 has a noncentral chi square distribution [72]. In this section, we will show that its distribution can be approximated to lognormal for two extreme cases. The results here will be utilized to develop our detection algorithms.

Let $\mu_{r,n}(l)\cos\theta_n(l)$ and $\mu_{r,n}(l)\sin\theta_n(l)$ be the real and imaginary part of $r_n(l)$, respectively, where θ_n is an arbitrary phase value. Then the total received signal envelop $|r_n(l)+w_n(l)|$ is Ricean distributed with the parameter

$$K_n(l) = \frac{\mu_{r,n}^2(l)}{2\sigma_w^2}. \tag{3.2}$$

It is easy to see that $K_n(l)$ is the instantaneous SNR at the n-th sensor. By approximating a Ricean distribution as Nakagami ([73], p. 79), $p_n = |r_n(l) + w_n(l)|^2$ has a gamma distribution with the PDF

$$f(p_n) = \frac{p_n^{m_{n,l}-1}}{\Gamma(m_{n,l})a_n^{m_{n,l}}} \exp\left(-\frac{p_n}{a_n}\right), \tag{3.3}$$

where

$$a_n = \frac{E[p_n]}{m_{n,l}} \tag{3.4}$$

and

$$m_{n,l} = \frac{(K_n(l)+1)^2}{2K_n(l)+1}. \tag{3.5}$$

In the following two asymptotic cases, we show that the sum of L energy samples are also Gamma distributed.

1) Asymptotic distribution of y_n for very large SNR:

When $\mu_{r,n}^2(l) \gg 2\sigma_w^2$, $K_n(l) \gg 1$ and

$$a_n = \frac{E[p_n]}{m_{n,l}} = \frac{\mu_{r,n}^2(l) + 2\sigma_w^2}{m_{n,l}} = \frac{(2K_n(l)+1)2\sigma_w^2}{(K_n(l)+1)} \approx 4\sigma_w^2. \tag{3.6}$$

Then, the scale a_n is a constant over the sample index l and thus y_n is also gamma distributed with the scale a_n and the shape

$$m_n = \sum_{l=1}^{L} m_{n,l} = \sum_{l=1}^{L} \frac{(K_n(l)+1)^2}{2K_n(l)+1} \approx \frac{1}{2}\sum_{l=1}^{L}(K_n(l)+1) = \frac{L}{2} + \frac{1}{4\sigma_w^2}\sum_{l=1}^{L}\mu_{r,n}^2(l) = \frac{L}{2}(1+\bar{\gamma}_n), \tag{3.7}$$

where

$$\bar{\gamma}_n = \frac{\sum_{l=1}^{L}\mu_{r,n}^2(l)}{2\sigma_w^2 L} \tag{3.8}$$

is the average received SNR within one measurement. When $\bar{\gamma}_n$ is sufficiently large, m_n in (3.7) can be further simplified by neglecting $L/2$. Following Appendix C, $Y_n = 10\log_{10}(y_n)$ is approximately Gaussian distributed.

2) Asymptotic distribution of y_n for very small SNR:

When $\mu_{r,n}^2(l) \ll 2\sigma_w^2$, $K_n(l) \approx 0$, $m_{n,l} \approx 1$, and

$$a_n = \frac{E[p_r]}{m_{n,l}} = \frac{(2K_n(l)+1)2\sigma_w^2}{(K_n(l)+1)} \approx 2\sigma_w^2. \tag{3.9}$$

Again, the scale a_n is a constant over the sample index l and thus y_n is also gamma distributed with the scale a_n and the shape

$$m_n = \sum_{l=1}^{L} m_{n,l} \approx L. \tag{3.10}$$

Similarly, Y_n is Gaussian distributed when L is large. In addition, the signal power is negligible in this case and thus the energy measurement only includes the noise.

Therefore, for both of the above asymptotic distributions, $Y_n \sim \mathcal{N}(\mu_{Y,n}, \sigma_{Y,n}^2)$ with the mean

$$\mu_{Y,n} = 10\log_{10}(a_n m_n) \tag{3.11}$$

and the variance

$$\sigma_{Y,n}^2 = \left(\frac{10}{\ln 10}\right)^2 \psi'(m_n). \tag{3.12}$$

The parameters a_n and m_n are given by (3.6) and (3.7) or (3.9) and (3.10), depending on the approximations. A special treatment to $\mu_{Y,n}$ in the large-SNR approximation is that, we neglect the term, $L/2$, in (3.7), that is, $m_n = \bar{\gamma}_n L/2$. The reason will be clear as follows.

In the detection analysis, we will approximate an energy measurement to either of these two asymptotic solutions, depending on the received SNR. It is then necessary to find an optimal SNR threshold to minimize the approximation error. From (3.7) we see that, when the average SNR $\bar{\gamma}_n = 1$, two asymptotic approximations will give the same $\mu_{Y,n}$ and $\sigma^2_{Y,n}$. Therefore, in the proposed analytical solutions, we will use the large SNR approximation when the average SNR is greater than 0 dB, and use the small SNR approximation otherwise.

3.1.3 Energy Detection Model Over Multiple Sensors

In the case of a large SNR, by neglecting the term $L/2$ in (3.7),

$$\mu_{Y,n} = 10\log_{10}\left(\sum_{l=1}^{L}\mu^2_{r,n}(l)\right). \tag{3.13}$$

Noting that Y_n is Gaussian distributed conditional on the received signal energy $\sum_{l=1}^{L}\mu^2_{r,n}(l)$ within one measurement, we rewrite the energy detector output as

$$Y_n = Y_{0,n} + Y_{S,n} + Y_{W,n}, \tag{3.14}$$

where $Y_{0,n} + Y_{S,n} = \mu_{Y,n}$ and $Y_{W,n} \sim \mathcal{N}(0, \sigma^2_{Y,n})$ accounts for the randomness due to the noise.

We use $Y_{0,n}$ to quantify the measured energy due only to the deterministic path loss fading, and it is generally given by

$$Y_{0,n} = Y_0 - 10\gamma\log_{10}(d_n/d_0), \tag{3.15}$$

where Y_0 is the signal strength measured at the reference distance d_0, d_n is the distance between the transmitter and the n-th sensor, and γ is the path loss exponent[1].

Further, $Y_{S,n}$ accounts for the multipath and shadow fading at different locations, and we model $Y_{S,n}$ as a spatial Gaussian process[2], $Y_{S,n} \sim \mathcal{N}(0, \sigma^2_{S,n})$. Taking into account the spatial correlation of channel fading, we assume $\mathbf{Y}_S = (Y_{S,1}, Y_{S,2}, \ldots, Y_{S,N})$ are jointly Gaussian, $Y_S \sim \mathcal{N}(0, \Sigma_S)$.

---

[1]Here we do not specify the direction of a propagation link, as depicted in the model (3.15). Therefore, the authorized transmitter is assumed to use an omnidirectional antenna.

[2]The shadow fading is widely modeled as lognormal over space [74]. The multipath fading can be modeled as a Nakagami distribution and thus its gain (in the linear ratio) is also Gamma distributed. Again by Appendix C, it approximates to lognormal. However, this approximation is not always accurate as the parameter m in (C.1) may be small.

Since the randomness due to the noise (quantified by $Y_{W,n}$) and that due to the channel fading (quantified by $Y_{S,n}$) are independent, Y_n is Gaussian distributed over space, that is,

$$Y_n \sim \mathcal{N}(Y_{0,n}, \sigma^2_{Y,n} + \sigma^2_{S,n}). \tag{3.16}$$

In addition, the measurements from all the N sensors, $\mathbf{Y} = (Y_1, Y_2, \ldots, Y_N)$, are also jointly Gaussian with the covariance matrix

$$\Sigma_Y = \Lambda_Y + \Sigma_S, \tag{3.17}$$

where Λ_Y is a diagonal matrix where the n-th diagonal element is $\sigma^2_{Y,n}$.

In the case of a very small SNR, from (3.9) and (3.10), we virtually neglect the signal strength, and thus the energy measurement Y_n is i.i.d. Gaussian across sensors.

In the following, we devise our detection algorithms based on the above models.

3.2 Modeling Anomalous Detection Using Significance Testing

In general, we only have the information in the normal situation and thus the detection of anomalous usage can be formulated as a statistical significance testing problem. The received signal at each sensor is defined as:

$$\mathcal{H}_0 : r(t) + w(t), \qquad \text{normal usage}, \tag{3.18a}$$

$$\mathcal{H}_1 : r(t) + u(t) + w(t), \qquad \text{anomalous usage}. \tag{3.18b}$$

where $r(t)$ is the signal from an authorized transmitters complying with the spectrum policy, $u(t)$ is an unknown unauthorized signal, and $w(t)$ is noise that we assume to be additive and white Gaussian with zero mean. The normal spectrum usage is defined as the null hypothesis $\mathcal{H}_0$.

A significance testing problem consists of the following key components:

- Test statistic $\mathbf{v}$: a measure of the observed data.
- Acceptance region Ω: if $\mathbf{v} \in \Omega$, we accept the null hypothesis $\mathcal{H}_0$.
- Significance level α: the probability of incorrectly rejecting the null hypothesis, i.e., the probability of false alarm.

In our detection problem, the observed data is a series of energy measurements, $\mathbf{Y} = (Y_1, Y_2, \ldots, Y_N)$, where Y_n is given by Section 3.1.2 and 3.1.3. For different statistics of $\mathbf{Y}$ in what follows, we will define $\mathbf{v}$ and Ω so that, for a specified false alarm probability α, $Prob(\mathbf{v} \notin \Omega|\mathcal{H}_0) \leq \alpha$, where $\mathbf{v}$ not in Ω declares the presence of the anomalous behaviors in the network.

3.3 Detecting Unauthorized Spectrum Usage in DSA Networks

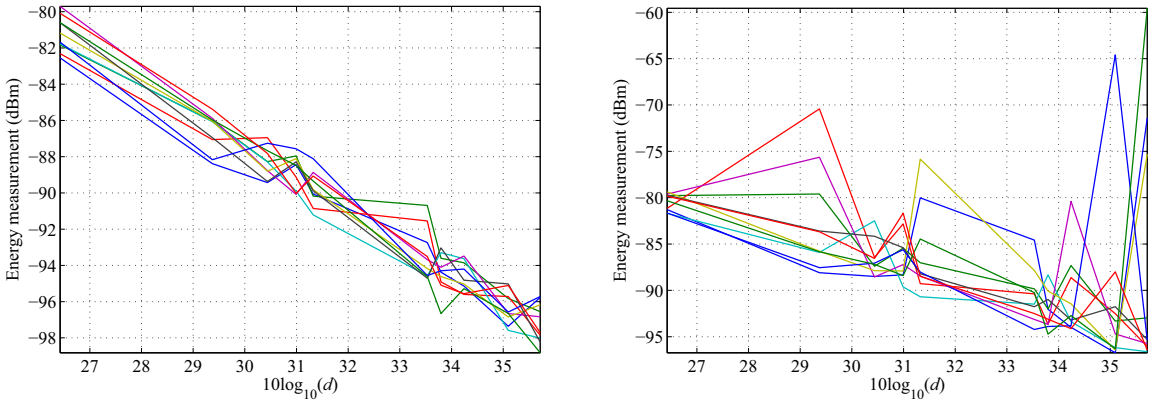
Unlike the conventional energy detection problems where a signal is detected from noise based on the noise power level [72,75], it is generally impractical to apply a threshold based on the authorized signal strength to detect interference. The authorized signal strength can be time-variant because of several effects, such as power control and transmitter mobility. This power variation can render the energy estimation useless. In this section, we propose two detection algorithms, one for the case where the authorized transmitter is mobile and one that works better but only for the stationary case. Provided the distribution of the authorized signal energy is known, we present analytical solutions to determining detection thresholds. In the more general case where it is hard to obtain such information, we propose to utilize a machine learning technique to derive empirical thresholds.

3.3.1 Linearity Check for A Mobile Authorized Transmitter

Following the discussion in Section 3.1.1, there should be only one authorized transmitter at any time in the spectrum under surveillance. Thus, the detection problem becomes distinguishing between single and multiple transmissions in the same spectral resource. To do this, we need a decision statistic that captures the characteristics of the radiation power in the case of a single transmission. Provided a single radio source, we rewrite the energy detector output in (3.14) as

$$Y_n = Y_0 - 10\gamma \log_{10}(d_n/d_0) + Y_{R,n}, \tag{3.19}$$

where $Y_{R,n} = Y_{S,n} + Y_{W,n} \sim \mathcal{N}(0, \sigma^2_{Y,n} + \sigma^2_{S,n})$. (3.19) shows that, when the received SNR is large, the energy measurement (in log scale) is a linear function of the log-distance (i.e., $\log_{10}(d)$) plus a random Gaussian term, $Y_{R,n}$, across the sensors. On the other hand, this linearity breaks when the measurement consists of signal strengths from multiple transmitters. As depicted in Figure 3.3, where we measure the received signal energy at 10 sensors for 10 independent trials, the energy from a single transmitter shows distinct linear decay with the log-distance, whereas the RSS from



(a) $\mathcal{H}_0$ (b) $\mathcal{H}_1$

Figure 3.3: Energy measurement vs. logarithmic distance between an authorized transmitter and $N = 10$ sensors. In an 100-meter$\times$100-meter area, the sensors are uniformly located. Path loss exponent $\gamma = 3.5$ and $\sigma_{S,n} = 1$ dB in (3.14). The noise power is neglected. The authorized transmitter is located at the center. In the $\mathcal{H}_1$ case, one unauthorized transmitter is randomly located. Detailed simulation settings are given in Section 3.4.1.

two transmitters does not present the similar pattern. Thus, by examining the linearity of the energy measurements with log-distance, we may distinguish the case of a single transmission (i.e., normal usage) from the case of multiple overlapped transmissions (i.e., anomalous usage). It is worth noting that, as shown in (3.14), this method relies on the linear property of the channel fading, and thus the detection is performed only based on the energy measurements where the received SNR is greater than 0 dB (i.e., the large SNR approximation is acceptable). With a slight abuse of notations, N in the following denotes the number of energy measurements we actually use, which is less or equal to the number of all the sensors.

Further, the distance d_n between the transmitter and a sensor can be obtained in two ways: (a) the authorized transmitter periodically announces its location, using a signal format that is decodable at the sensors; or (b) the sensors cooperatively estimate the transmitter location based on measured RSS. In either case, a sensor knows its own location.

Given the distance d_n, the remaining unknown parameters are the mean Y_0 and the path loss exponent γ. In general, it is hard to obtain their accurate values, so we use linear least squares to estimate them.

Suppose $\mathbf{Y} = (Y_1, \ldots, Y_N)^T$ is the vector of N energy measurements, and

$$\mathbf{A} = \begin{bmatrix} 1 & -10\log_{10}(d_1/d_0) \\ \vdots & \vdots \\ 1 & -10\log_{10}(d_N/d_0) \end{bmatrix}. \tag{3.20}$$

Note that $\mathbf{A}$ has a rank of 2 as long as there are at least two sensors with difference distances from the transmitter. Then, the least square estimation of Y_0 and γ gives

$$\begin{aligned} \begin{bmatrix} \hat{Y}_0 \\ \hat{\gamma} \end{bmatrix} &= (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{Y} \\ &= (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T(\mathbf{A}\begin{bmatrix} Y_0 \\ \gamma \end{bmatrix} + \mathbf{Y}_R) \\ &= \begin{bmatrix} Y_0 \\ \gamma \end{bmatrix} + (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{Y}_R, \end{aligned} \tag{3.21}$$

where $\mathbf{Y}_R = (Y_{R,1}, Y_{R,2}, \ldots, Y_{R,N})^T \sim \mathcal{N}(0, \Sigma_Y)$ as defined in (3.17). Further, we define the vector of the estimation error (residuals) $\hat{\mathbf{e}}$ as

$$\begin{aligned} \hat{\mathbf{e}} &= \mathbf{Y} - \hat{\mathbf{Y}} \\ &= \mathbf{A}\begin{bmatrix} Y_0 \\ \gamma \end{bmatrix} + \mathbf{Y}_R - \mathbf{A}\begin{bmatrix} \hat{Y}_0 \\ \hat{\gamma} \end{bmatrix} \\ &= \mathbf{Y}_R - \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{Y}_R \\ &= (\mathbf{I} - \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T)\mathbf{Y}_R. \end{aligned} \tag{3.22}$$

When the distance matrix $\mathbf{A}$ is exactly known, the residuals are independent of the transmission power. Based on the linearity of the propagation model, we infer that the distribution of the residuals in the normal usage case should differ from that of the anomalous case. Then, the residuals $\hat{\mathbf{e}}$ can be a measure of linearity. However, its distribution is not always explicit. As (3.27) below shows, the matrix $\mathbf{D} = (\mathbf{I} - \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T)$ in (3.22) is singular, so $\hat{\mathbf{e}}$ is no longer a multivariate Gaussian even though $\mathbf{Y}_R$ is. To facilitate the analysis, we seek a new measure of the linearity, which not only has a known distribution but also retains as much information from $\hat{\mathbf{e}}$ as possible. Given that the $N \times N$ matrix $\mathbf{D}$ has two zero eigenvalues (see (3.27)), $\hat{\mathbf{e}}$ only has $N - 2$ independent bases

from $\mathbf{Y}_R$. Therefore, we can construct a new statistic $\hat{\mathbf{e}}_u$ whose distribution can be derived in the normal usage case, using the following theorem:

Theorem 1 *Given a multivariate Gaussian* $\mathbf{Y}_R \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_Y)$ *and a* $N \times 2$ *matrix* $\mathbf{A}$ *with rank of 2, we define* $\hat{\mathbf{e}}_u = \mathbf{U}_2^T \hat{\mathbf{e}}$*, where* $\mathbf{U}_2$ *is an* $N \times (N-2)$ *matrix consisting of* $(N-2)$ *eigenvectors of* $\mathbf{A}\mathbf{A}^T$ *that correspond to the* $(N-2)$ *zero eigenvalues. Then*

$$\hat{\mathbf{e}}_u \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_\mathbf{e}), \tag{3.23}$$

where $\mathbf{\Sigma}_\mathbf{e} = \mathbf{U}_2^T \mathbf{\Sigma}_Y \mathbf{U}_2$.

Proof 1 *Given that* $\mathbf{A}$ *in (3.20) is a* $N \times 2$ *matrix, using the singular value decomposition (SVD), we have*

$$\mathbf{A} = \mathbf{U}\mathbf{\Lambda}\mathbf{V}^T, \tag{3.24}$$

where $\mathbf{U}$ *is a* $N \times N$ *orthogonal matrix,* $\mathbf{V}$ *is a* 2×2 *orthogonal matrix.* $\mathbf{\Lambda}$ *is a* $N \times 2$ *diagonal matrix with two nonzero singular values (i.e., assuming there are at least two sensors that have different distances from the transmitter):*

$$\mathbf{\Lambda}_{N\times 2} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} \tilde{\mathbf{\Lambda}}_{2\times 2} \\ 0 \end{bmatrix}. \tag{3.25}$$

Then we have

$$\begin{aligned} \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T &= \mathbf{U}\mathbf{\Lambda}\mathbf{V}^T(\mathbf{V}\mathbf{\Lambda}^T\mathbf{U}^T\mathbf{U}\mathbf{\Lambda}\mathbf{V}^T)^{-1}\mathbf{V}\mathbf{\Lambda}^T\mathbf{U}^T \\ &= \mathbf{U}\mathbf{\Lambda}(\mathbf{\Lambda}^T\mathbf{\Lambda})^{-1}\mathbf{\Lambda}^T\mathbf{U}^T \\ &= \mathbf{U}\begin{bmatrix} \tilde{\mathbf{\Lambda}} \\ 0 \end{bmatrix}(\tilde{\mathbf{\Lambda}}\tilde{\mathbf{\Lambda}})^{-1}\begin{bmatrix} \tilde{\mathbf{\Lambda}} & 0 \end{bmatrix}\mathbf{U}^T \\ &= \mathbf{U}\begin{bmatrix} \mathbf{I} \\ 0 \end{bmatrix}\begin{bmatrix} \mathbf{I} & 0 \end{bmatrix}\mathbf{U}^T \\ &= \mathbf{U}\begin{bmatrix} \mathbf{I}_{2\times 2} & 0 \\ 0 & 0 \end{bmatrix}\mathbf{U}^T \end{aligned} \tag{3.26}$$

Therefore,

$$\mathbf{D} = \mathbf{I} - \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T = \mathbf{U}(\mathbf{I}_{N\times N} - \begin{bmatrix} \mathbf{I}_{2\times 2} & 0 \\ 0 & 0 \end{bmatrix})\mathbf{U}^T = \mathbf{U}\begin{bmatrix} 0 & 0 \\ 0 & \mathbf{I}_{(N-2)\times(N-2)} \end{bmatrix}\mathbf{U}^T. \tag{3.27}$$

There are 2 *zero singular values in the matrix* $\mathbf{D}$ *and thus it is not invertible.*

Now let $\mathbf{U} = [\mathbf{U}_1, \mathbf{U}_2]$*, where* $\mathbf{U}_1$ *is* $N \times 2$ *and* $\mathbf{U}_2$ *is* $N \times (N-2)$*. Since*

$$\begin{aligned} \mathbf{A}\mathbf{A}^T &= \mathbf{U}\mathbf{\Lambda}\mathbf{\Lambda}^T\mathbf{U}^T \\ &= [\mathbf{U}_1, \mathbf{U}_2]\begin{bmatrix} \tilde{\mathbf{\Lambda}}^2 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} \mathbf{U}_1^T \\ \mathbf{U}_2^T \end{bmatrix}, \end{aligned} \tag{3.28}$$

$\mathbf{U}_2$ *consists of* $(N-2)$ *eigenvectors of* $\mathbf{A}\mathbf{A}^T$ *corresponding to the* $(N-2)$ *zero eigenvalues.*

Multiplying the residues $\hat{\mathbf{e}}$ *by* $\mathbf{U}_2^T$*, we have*

$$\begin{aligned} \hat{\mathbf{e}}_u &= \mathbf{U}_2^T\hat{\mathbf{e}} \\ &= \mathbf{U}_2^T\mathbf{D}\mathbf{Y}_R \\ &= \mathbf{U}_2^T\mathbf{U}\begin{bmatrix} 0 & 0 \\ 0 & \mathbf{I}_{(N-2)\times(N-2)} \end{bmatrix}\mathbf{U}^T\mathbf{Y}_R \\ &= \mathbf{U}_2^T\mathbf{U}_2\mathbf{U}_2^T\mathbf{Y}_R \\ &= \mathbf{U}_2^T\mathbf{Y}_R. \end{aligned} \tag{3.29}$$

Given $\mathbf{Y}_R \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_Y)$*, it is known that* $\hat{\mathbf{e}}_u \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}_\mathbf{e})$*, where*

$$\mathbf{\Sigma}_\mathbf{e} = E[\hat{\mathbf{e}}_u\hat{\mathbf{e}}_u^T] = \mathbf{U}_2^T\mathbf{\Sigma}_Y\mathbf{U}_2. \tag{3.30}$$

Similar to the significance test in [76], we can define a likelihood-based acceptance region for $\hat{\mathbf{e}}_u$ as

$$\Omega = \{\hat{\mathbf{e}}_u : f(\hat{\mathbf{e}}_u) \geq f_T\}, \tag{3.31}$$

where the probability density function is

$$f(\hat{\mathbf{e}}_u) = (2\pi)^{-N/2}|\mathbf{\Sigma}_e|^{-1/2}\exp\left(-\frac{1}{2}\hat{\mathbf{e}}_u^T\mathbf{\Sigma}_e^{-1}\hat{\mathbf{e}}_u\right).$$

Then, Ω in (3.31) can also be expressed as

$$\Omega = \{\hat{\mathbf{e}}_u : \hat{\mathbf{e}}_u^T \boldsymbol{\Sigma}_e^{-1} \hat{\mathbf{e}}_u < T_e\}. \tag{3.32}$$

Therefore, we obtain the test statistic $\hat{\mathbf{e}}_{LCM} = \hat{\mathbf{e}}_u^T \boldsymbol{\Sigma}_e^{-1} \hat{\mathbf{e}}_u$. It can be shown that $\hat{\mathbf{e}}_{LCM}$ follows a chi-square distribution with $N-2$ degrees (e.g., see Section V-C in [76]). Thus, the false alarm probability is given by

$$P_F = \frac{\Gamma((N-2)/2, T_e/2)}{\Gamma((N-2)/2)}, \tag{3.33}$$

where $\Gamma(k, x)$ is the upper incomplete gamma function.

This probability is accurate only when the distance matrix $\mathbf{A}$ (or equivalently, the location of the authorized transmitter) is exactly known and the distribution of the energy measurements across sensors is lognormal. These two conditions are not often met in practice, which will result in an unknown distribution for the test statistic $\hat{\mathbf{e}}_{LCM}$ and distort the expected false alarm rate (i.e., P_F in (3.33)), as we shall see in Section 3.4.2. To extend our algorithm to a more general scenario, we propose the application of One-class SVM (Support Vector Machines), proposed in [77], to find an acceptance region.

One-class SVM is a kernel based machine learning technique for data classification, which involves a training phase and a testing phase. Each data instance, either in the training set or in the testing set, is represented by one or multiple attributes. As the name of One-class SVM implies, all training data are from a class of interest and the goal is to empirically generate a model that can predict whether a data instance from the testing set belongs to this class. One-class SVM finds its use in the anomalous or outlier detection problems where the anomalous case cannot be accurately described using training data and thus the classification can only be formulated as a significance test (see Section 3.2). Therefore, the data attributes are the test statistics in our significance test model.

Since the SVM method can handle data with an unknown distribution, there can be many choices of data attributes in our anomalous detection problem. An obvious option is $\hat{\mathbf{e}}_{LCM}$ derived in the analytical solution. However, it will result in a similar[3] detection performance to that of the analytical one in terms of the receiver operating characteristic (ROC). Since we are actually interested

[3]Note that the ROCs of the analytical solution and SVM are not necessarily the same even if they both use $\hat{\mathbf{e}}_{LCM}$ as the test statistic, because they have different acceptance regions. Specifically, the analytical solution has a single-sided acceptance region as defined in (3.32) but the SVM has a double-sided acceptance region as given by (D.4).

in the estimation residues $\hat{\mathbf{e}}$ given in (3.22), we use it directly in the SVM. $\hat{\mathbf{e}}$ is also more reliable compared to $\hat{\mathbf{e}}_{LCM}$ as it involves less matrix manipulations, which are based on the assumption of the Gaussian distribution. Note that it is not necessary to assume the received SNR > 0 dB in the SVM solution. Hence $\hat{\mathbf{e}}$ utilizes energy measurements from all the sensors regardless of the received SNR.

Provided the training data are sufficiently sampled from an underlying probability distribution (i.e., in the normal class), we apply One-class SVM to estimate a subset, Ω, (i.e., a fraction of the training data), so that, any testing data from the same distribution will lie outside of Ω with a probability equal to a specified value, $\nu \in (0, 1)$. Apparently ν corresponds to the false alarm probability and Ω is the acceptance region in the significance test. In summary, given the energy measurements (thus $\hat{\mathbf{e}}$) that are well-sampled in the normal usage case, we use One-class SVM to find an empirical acceptance region corresponding to a specified false alarm probability, P_F. See Appendix D for the mathematical description of One-class SVM.

3.3.2 Signalprint Check for A Stationary Authorized Transmitter

Provided the authorized transmitter is stationary, we can further improve the performance of unauthorized signal detection by exploiting a more reliable metric, the signalprint. In this section, we present a fingerprint based method analogous to the fingerprint based localization [46]. Specifically, transmitters at different locations lead to different spatial distribution of RSS. Thus, an interference signal can be detected by examining the difference between its signalprint (i.e., the vector of energy measurements $\mathbf{Y}$) and the authorized one. The authorized signalprint can be obtained (i) if the authorized transmitter periodically broadcasts an "identity" signal that is decodable at the sensors; or (ii) by using a previous measurement that is known from the authorized signal.

Denote the known authorized signal energy by Y_n and the currently measured energy by $\tilde{Y}_n$ at the n-th sensor, respectively. For measurements with large SNR, since the channel is stationary, the shadowing and multipath fading $Y_{S,n}$ in (3.14) is constant over time. Thus,

$$\begin{aligned}
\tilde{Y}_n - Y_n &= \tilde{Y}_{0,n} - Y_{0,n} + \tilde{Y}_{W,n} - Y_{W,n} \\
&= \tilde{Y}_0 - Y_0 + \tilde{Y}_{W,n} - Y_{W,n} \\
&= \tilde{Y}_0 - Y_0 + dY_{W,n}. \qquad (3.34)
\end{aligned}$$

Since $Y_{W,n}$ and $\tilde{Y}_{W,n}$ are due to noise, they are independent of each other and $dY_{W,n} = \tilde{Y}_{W,n} - Y_{W,n}$ is also Gaussian distributed, that is, $dY_{W,n} \sim \mathcal{N}(0, \sigma^2_{\tilde{Y},n} + \sigma^2_{Y,n})$, where $\tilde{Y}_{W,n} \sim \mathcal{N}(0, \sigma^2_{\tilde{Y},n})$. The reference energy Y_0 can be time variant, because (i) the authorized transmission power may change over time (e.g., by power control), and (2) the signal strength $|r(t)|$ may change over time (e.g., an OFDM signal with many subcarriers). For measurements with small SNR, we neglect the signal strength (see Section 3.1.2) and thus $Y_0 = \tilde{Y}_0$. Combining the two approximations, we have[4]

$$\tilde{Y}_n - Y_n = \begin{cases} C + dY_{W,n} & \text{if } \bar{\gamma}_n \geq 0 \text{ dB}, \quad (3.35a) \\ dY_{W,n} & \text{if } \bar{\gamma}_n < 0 \text{ dB}, \quad (3.35b) \end{cases}$$

where the signal strength shift $C = \tilde{Y}_0 - Y_0$ is a constant across all the sensors. Denote $\mathbf{Y} = [Y_1, Y_2, \ldots, Y_N]^T$ and $\tilde{\mathbf{Y}} = [\tilde{Y}_1, \tilde{Y}_2, \ldots, \tilde{Y}_N]^T$. We estimate C using a simple linear regression model,

$$\hat{C} = \begin{cases} \hat{C} = \frac{1}{N_r} \mathbf{e}_r^T (\tilde{\mathbf{Y}} - \mathbf{Y}) = \frac{1}{N_r} \sum_{n=1}^{N_r} (\tilde{Y}_n - Y_n), & N_r > 0, \quad (3.36a) \\ 0, & N_r = 0, \quad (3.36b) \end{cases}$$

where $\mathbf{e}_r$ is a $N \times 1$ vector with the n-th element

$$e_{r,n} = \begin{cases} 1 & \text{if } \bar{\gamma}_n \geq 0 \text{ dB}, \quad (3.37a) \\ 0 & \text{if } \bar{\gamma}_n < 0 \text{ dB}. \quad (3.37b) \end{cases}$$

N_r is the number of 1's in $\mathbf{e}_r$. Without loss of generality, we assume the energy measurements from all the N sensors are arranged so that the first N_r measurements have SNR ≥ 0 dB and thus the first N_r elements of $\mathbf{e}_r$ are 1 and the rest of them are 0.

Then, the residue of the estimation is

$$\begin{aligned} \hat{\mathbf{e}} &= \tilde{\mathbf{Y}} - \mathbf{Y} - \hat{C}\mathbf{e}_r \\ &= \tilde{\mathbf{Y}} - \mathbf{Y} - \frac{1}{N_r} \mathbf{e}_r \mathbf{e}_r^T (\tilde{\mathbf{Y}} - \mathbf{Y}), \quad \text{for } N_r > 0, \\ &= (I - E_r)(\tilde{\mathbf{Y}} - \mathbf{Y}), \end{aligned} \quad (3.38)$$

where E_r is a $N \times N$ matrix where all elements in the top left $N_r \times N_r$ block are $1/N_r$ and others are zeros.

[4]This method requires the same asymptotic approximation (either for large- or small-SNR) for both measurements Y_n and $\tilde{Y}_n$. For a good approximation in practice, we will only use the measurements where Y_n and $\tilde{Y}_n$ both have SNR greater or less than zero.

The mean of the estimate residue is

$$\mathbb{E}[\hat{\mathbf{e}}] = (I - E_r)\mathbb{E}[\tilde{\mathbf{Y}} - \mathbf{Y}]. \tag{3.39}$$

From (3.35), $\mathbb{E}[\tilde{\mathbf{Y}} - \mathbf{Y}]$ gives a $N \times 1$ vector whose first N_r elements are C and the remaining elements are zeros. Then $\hat{\mathbf{e}}$ has zero mean.

Since E_r has the rank of 1, $(I - E_r)$ is a singular matrix with rank of $(N-1)$. As a result, the joint distribution of the N elements in $\hat{\mathbf{e}}$ is not easy to obtain. Similar to Theorem 1, we construct a $N \times (N-1)$ matrix, Q_2, whose columns are the $N-1$ eigenvectors of E_r corresponding to its $N-1$ zero eigenvalues. Then, we have $E_r Q_2 = 0$ and

$$\hat{\mathbf{e}}_{sub} = Q_2^T \hat{\mathbf{e}} = Q_2^T(\tilde{\mathbf{Y}} - \mathbf{Y}). \tag{3.40}$$

Since Q_2 has a full rank (i.e., $N-1$), the $N-1$ elements of $\hat{\mathbf{e}}_{sub}$ are jointly Gaussian distributed. Also $\hat{\mathbf{e}}_{sub}$ has a zero mean because of (3.39).

From (3.35), we have

$$\mathbb{E}[(\tilde{Y}_i - Y_i)(\tilde{Y}_i - Y_i)] = \begin{cases} C^2 + \sigma^2_{\tilde{Y},i} + \sigma^2_{Y,i}, & \text{if } \bar{\gamma}_i \geq 0 \text{ dB}, \quad (3.41a) \\ \sigma^2_{\tilde{Y},i} + \sigma^2_{Y,i}, & \text{if } \bar{\gamma}_i < 0 \text{ dB}. \quad (3.41b) \end{cases}$$

and

$$\mathbb{E}[(\tilde{Y}_i - Y_i)(\tilde{Y}_j - Y_j)] = \begin{cases} C^2, & \text{if } \bar{\gamma}_i \geq 0 \text{ dB and } \bar{\gamma}_j \geq 0 \text{ dB}, \quad (3.42a) \\ 0, & \text{if } \bar{\gamma}_i < 0 \text{ dB and } \bar{\gamma}_j < 0 \text{ dB}. \quad (3.42b) \end{cases}$$

Then,

$$\mathbb{E}[(\tilde{\mathbf{Y}} - \mathbf{Y})(\tilde{\mathbf{Y}} - \mathbf{Y})^T] = \Lambda_{\tilde{Y}} + \Lambda_Y + C^2 N_r E_r, \tag{3.43}$$

where $\Lambda_{\tilde{Y}}$ and Λ_Y are covariance matrix for $\tilde{Y}_W$ and Y_W, respectively, as defined in (3.17).

Then the variance of $\hat{\mathbf{e}}_{sub}$ is given by

$$\begin{aligned} \Sigma_e &= \mathbb{E}[\hat{\mathbf{e}}_{sub}\hat{\mathbf{e}}_{sub}^T] \\ &= Q_2^T \mathbb{E}[(\tilde{\mathbf{Y}} - \mathbf{Y})(\tilde{\mathbf{Y}} - \mathbf{Y})^T] Q_2 \\ &= Q_2^T(\Lambda_{\tilde{Y}} + \Lambda_Y)Q_2 + C^2 N_r Q_2^T E_r Q_2 \\ &= Q_2^T(\Lambda_{\tilde{Y}} + \Lambda_Y)Q_2. \end{aligned} \tag{3.44}$$

Similar to (3.32), the likelihood-based acceptance region for $\hat{\mathbf{e}}_{sub}$ is

$$\Omega = \{\hat{\mathbf{e}}_{sub} : \hat{\mathbf{e}}_{SCS} = \hat{\mathbf{e}}_{sub}^T \Sigma_e^{-1} \hat{\mathbf{e}}_{sub} < T_e\}. \tag{3.45}$$

Therefore, the false alarm probability is

$$P_F = \frac{\Gamma((N-1)/2, T_e/2)}{\Gamma((N-1)/2)}. \tag{3.46}$$

Since this analytical solution is derived based on the asymptotic approximations in Section 3.1.2, we will see from Section 3.4.2 that, it is only accurate when the received SNR is either very large or very small. Therefore, for a general scenario where the approximations are no longer acceptable, we will apply the SVM method to obtain an empirical detection threshold. Similarly, we will use the residues, $\hat{\mathbf{e}}$, from (3.38) as the test statistics of the SVM.

3.4 Simulation Evaluation

3.4.1 Simulation settings

In this section we evaluate the performance of our proposed methods, which we call LCM (Linearity-Check-for-Mobile Transmitter, Section 3.3.1) and SCS (Signalprint-Check-for-Stationary-Transmitter, Section 3.3.2). Their performance were tested in a 100-meter$\times$100-meter square area, where N sensors are randomly placed with a uniform probability distribution. Both authorized transmitter and unauthorized transmitters are randomly located in the area. Each result is an average over 20000 independent trials (i.e., independent transmitter and sensor locations and independent random channel fadings). Unless otherwise noted, in these numerical studies we assume that, (a) there is only one unauthorized transmitter and it uses the same transmission power as the authorized user; (b) $N = 50$ for LCM and $N = 10$ for SCS; (c) the path loss, $\gamma = 3.5$, and the standard deviation of the fading, $\sigma_{S,n} = 4$ dB, which are typical values in an urban microcell environment with a very mild random fading; (d) the variation of the channel fading across all sensors is i.i.d., that is, Σ_S in (3.17) is a diagonal matrix; (e) the number of samples in each energy measurement, $L = 16$.

3.4.2 Detection Performance

Figure 3.4 shows the complementary receiver operating characteristic (C-ROC) curves by LCM and SCS methods under various SNR conditions. The expected false alarm probabilities are both from 0.002 to 0.2, set by (3.33) and (3.46), respectively. The ROC curves are shown for different SNR levels of energy measurements, represented by the median of received SNR among all the sensors,

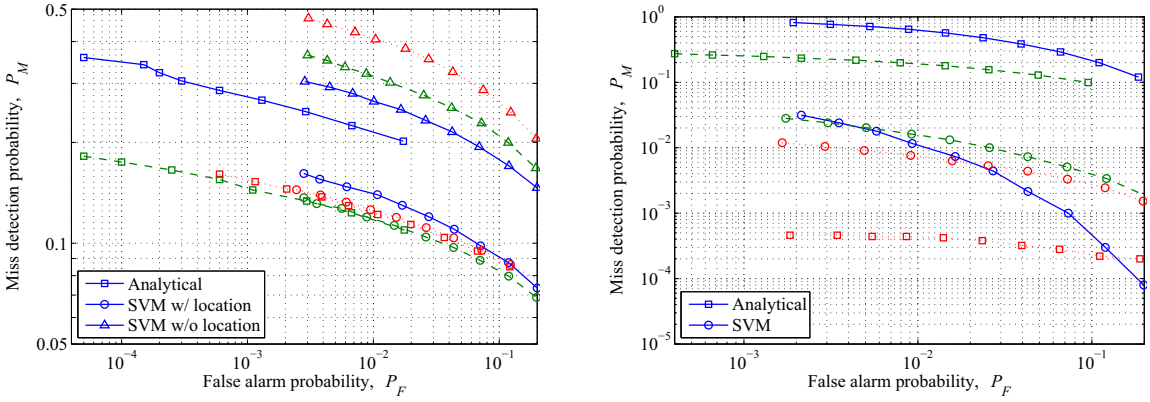


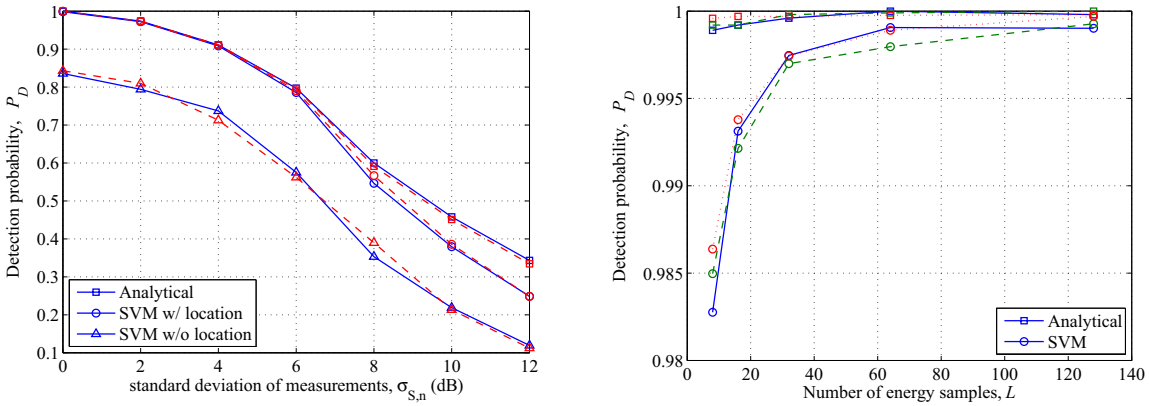
Figure 3.4: Complementary ROC by (a) LCM and (b) SCS. The expected false alarm probabilities are $[0.002, 0.2]$. In LCM, the median of the received SNR among all the sensors is 0 dB (solid), 10 dB (dashed), and 20 dB (dotted), respectively. In SCS, the median of the received SNR among all the sensors is -20 dB (solid), 0 dB (dashed), and 20 dB (dotted), respectively.

$\bar{\gamma}_{med}$. For the SVM method in LCM where the location of the authorized transmitter is unknown (i.e., "SVM w/o location"), we estimate it by the weighted centroid as

$$[x, y] = \frac{\sum_{i=1}^{N_C} p_i [x_i, y_i]}{\sum_{i=1}^{N_C} p_i}, \tag{3.47}$$

where p_i is the i-th largest signal strength (in linear scale) from all the sensors and (x_i, y_i) is the location of the corresponding sensor. It has been shown in [78] that an unbalanced distribution of sensors (with respect to the transmitter to be localized) can degrade the accuracy of a centroid based algorithm. To mitigate the impact due to the unbalanced network topology, we choose $N_C = 10$ sensors with the strongest energy measurement to perform the localization. An advantage of the SVM solutions seen from the results is that the actual P_F is close to the designated one regardless of the SNR level. On the contrary, the analytical solution fails to predict the correct false alarm probability under certain SNR conditions. Specifically, in LCM, the actual and analytical false alarm probabilities match each other only for large $\bar{\gamma}_{med}$ (e.g., $>$ 20 dB), because the analytical solution is based on the large SNR approximation. In SCS, the analytical false alarm probability is accurate when the absolute dB value of $\bar{\gamma}_{med}$ is large (e.g., $\pm$20 dB), because the method makes use of data in both asymptotic conditions.

Regarding the detection performance, given a large SNR (e.g., $\bar{\gamma}_{med} = 20$ dB), both schemes achieve detection rate above 90% for a false alarm rate of 10%. Moreover, SCS achieves much



(a) (b)

Figure 3.5: The effects of energy measurement variation on the detection probability, P_D, for the actual false alarm rate of 0.1. $\bar{\gamma}_{med} = 20$ dB. (a) P_D vs. $\sigma_{S,n}$ for LCM. $L = 8$ (solid) and $L = 128$ (dashed); (b) P_D vs. L for SCS. $\sigma_{S,n} = 0$ dB (solid), 6 dB (dashed), and 12 dB (dotted).

higher detection probability using far fewer sensors than LCM, thanks to the more reliable metric based on signalprints. However, SCS can only be used in the case where the authorized transmitter is fixed while LCM does not have this constraint. In addition, the results show the effects of using the estimation residues, $\hat{\mathbf{e}}$, as the test statistics. In LCM, we observe that, given the location of the authorized transmitter, the analytical and SVM solutions have similar ROCs although they use different test statistics. In SCS, the detection rate by the SVM solution is more stable against SNR than that of the analytical solution. Particularly, the SVM solution is superior to the analytical one when the SNR of energy measurements is small (i.e. $\bar{\gamma}_{med} \leq 0$ dB).

In the following results, we fix the false alarm rate at $P_F = 0.1$ and investigate the effects of different system parameters on the detection probability of the proposed methods.

The variation of energy measurements are mostly caused by the random channel fading and noise, as we have seen from (3.14). Their effects are illustrated in Figure 3.5. From (3.19), we see that the variation of measurements mostly results from the random channel fading, $\sigma_{S,n}$. The noise, averaged by L samples, has little impact on LCM. On the other hand, from (3.34), the variation of measurements is caused solely by the noise. Thus, with more samples in a measurement, the detection rate of SCS is higher.

Figure 3.6 shows the detection probability for different values of interference-to-signal ratio

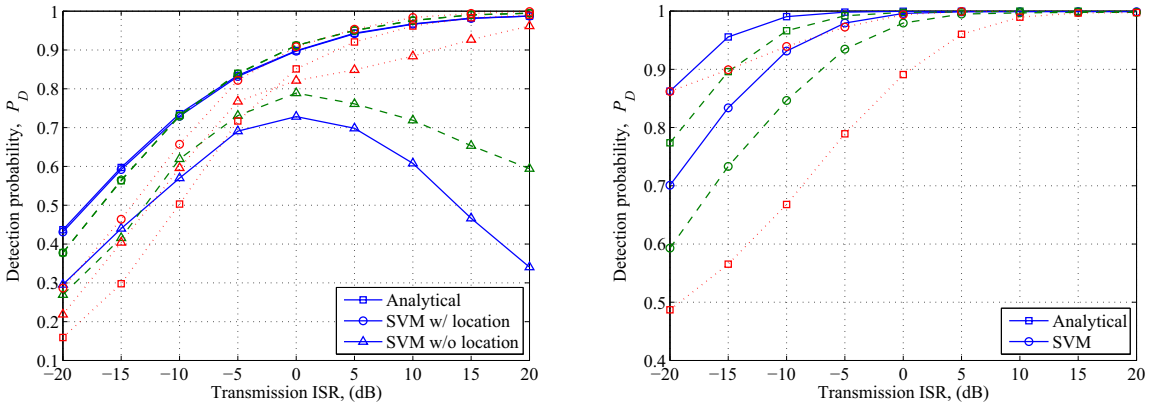


Figure 3.6: Detection probability vs. transmission ISR by (a) LCM and (b) SCS, where $\bar{\gamma}_{med}$ is 20 dB (solid), 10 dB (dashed) and 0 dB (dotted). The actual $P_F = 0.1$.

(ISR), which is defined by the ratio of transmission power from unauthorized and authorized transmitter. For both methods, the detection rates monotonically increase with the interference power, except for the LCM's SVM solution where the unauthorized transmitter location is unknown (i.e., curves with triangle markers). For these cases, and when the noise power is negligible (e.g., $\bar{\gamma}_{med} = 20$ dB), the machine learning based solution treats the signal strengths from both transmitters equally and it only tries to tell whether there are simultaneous transmissions. Thus, the detection probabilities appear approximately symmetric with respect to the ISR of 0 dB, where the highest accuracy is usually obtained. When the noise power is significant (e.g., $\bar{\gamma}_{med} = 0$ dB), the estimation residues, $\hat{\mathbf{e}}$, are mostly contributed by noise in the normal case. When the interference power is significant (i.e., ISR > 0 dB), its impact on $\hat{\mathbf{e}}$ increases and it deviates the residues from those in the normal (large noise) case. Therefore, when ISR > 0 dB, the detection probability increases as the SNR decreases.

We now consider the case of multiple unauthorized transmitters. The transmitters are assumed non-colluding and independent, so that their powers add noncoherently at each sensor. Intuitively, more unauthorized radios should lead to better detection because the total amount of transmitted power (and the resulting interference power at each sensor) increases. We thus address a more interesting scenario, where the total transmission powers from all unauthorized radios is fixed. Figure 3.7 shows the detection probabilities of LCM and SCS schemes for different numbers of unauthorized

transmitters. The unauthorized transmitters have equal transmission powers and are randomly located in the test area with a uniform distribution. In addition, the total transmission power from all the unauthorized radios is equal to the authorized one. We observe that more unauthorized radios leads to higher detection rates for both schemes, even if the aggregate interference power remains constant.

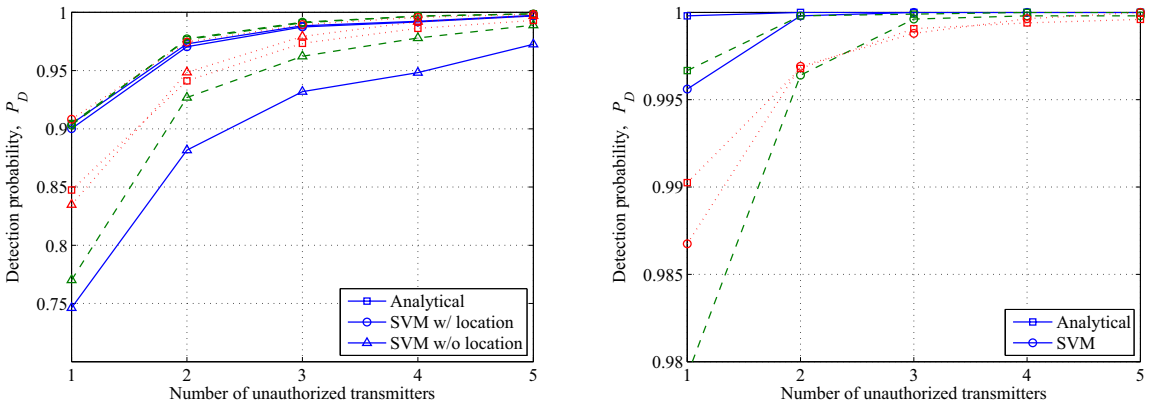


Figure 3.7: Detection probability vs. the number of independent authorized transmitters, for (a) LCM and (b) SCS, where $\bar{\gamma}_{med}$ is 20 dB (solid), 10 dB (dashed), and 5 dB (dotted). The total transmission power of the unauthorized radios equals the authorized transmission power (i.e., ISR = 0 dB). The actual $P_F = 0.1$.

3.5 Summary

In this chapter, we investigated the problem of detecting unauthorized spectrum usage in a dynamic spectrum access network. Assuming there is only one authorized user in each spectrum channel, we formulated the detection of anomalous spectrum usage as several statistical significance testing problems. With respect to the mobility of the authorized transmitter, we propose two detection algorithms. For the mobile case, we present a Linearity-Check-for-Mobile-Transmitter (LCM) method to examine the linear relation between log-scale RSS and logarithmic link distance. For the stationary case, we present a Signalprint-Check-for-Stationary-Transmitter (SCS) method to compare the current RSS pattern with a stored pattern of the authorized transmitter. Provided the distribution of the energy measurements is known, we derive analytical models for the significance test statistics. In the general case where the distribution is unknown, we introduce a machine-learning approach to provide empirical solutions.

The simulation results show that, the false alarm probabilities predicted by the analytical solutions are sensitive to the SNR of energy measurements across the sensor network. The accuracy of (3.33) increases with the SNR and the accuracy of (3.46) increases as the SNR changes away from 0 dB. Given the authorized transmitter location in LCM, the SVM based empirical solution and analytical solution have very similar detection probabilities. On the other hand, the empirical solution of SCS is more stable against noise than the analytical solution in terms of the detection performance. Furthermore, the random variation of measurements has different effects on the detection performance of two proposed schemes. Specifically, the random channel fading significantly deteriorates the detection rate of LCM but has little impact on SCS. In contrast, the number of samples in each measurement, indicating how well the noise can be averaged, is the only factor that determines the variance of measurements in SCS. Provided a large SNR and a single unauthorized radio, both LCM and SCS schemes achieve the detection probability above 0.9 while keeping the false alarm rate less than 0.1. The detection probabilities are even higher when there are multiple unauthorized radios, for the same total interference power. Moreover, SCS is always superior to LCM in that it achieves much higher detection probability using far fewer sensors, thanks to the more reliable metric based on signalprints.

Chapter 4

Interference Classification in Mobile Ad Hoc Networks

4.1 Preamble

Wireless communications are very susceptible to interference and poor communication performance. Communication protocols (particularly at the link layer) have been designed to deal with a variety of causes for poor link performance. For example, power control techniques might increase the transmission power when a receiver is not able to receive a strong enough version of a communication signal. Or, in the presence of congestion, a medium access control protocol might commence a back off procedure to wait for the channel utilization to improve. Even in more malicious settings, such as jamming, link layer adaptation whereby a transmitter and receiver pair coordinate a switch in operating channels is possible. Unfortunately, the solution for one type of poor performance might not be the proper response for another cause of poor performance. Consequently, identifying and classifying the cause for poor communication performance is an essential first step in network repair, in defending the network from potential adversaries and, even, in taking appropriate offensive countermeasures.

The fact that the wireless medium is a shared and open medium makes easy for other entities, intentionally or otherwise, to cause interference. For example, a selfish node may deviate from an underlying MAC protocol by aggressively using a shorter back off time (or even disregarding back off entirely) in order to gain a larger fraction of channel access time, or an adversarial entity may launch a jamming attack targeted at ensuring that a receiver cannot successfully decode a packet. Merely identifying the presence of interference, however, is not sufficient for deciding how to respond. Network congestion can look very similar to an adversarial jammer bypasses MAC-layer back off and emits valid protocol packets. Consequently, being able to identify the cause of poor performance also requires being able to identify whether the interference is adversarial or due to a more benign reason, identifying the strategy that an adversarial source of interference may be

employing, and understanding the likelihood associated with different potential explanations for a perceived radio scenario.

Ensuring resilience to interference and denial of service attacks is an essential step towards building a secure and dependable MANET. In general, a defense strategy consists of detection and appropriate countermeasures against network anomalies. Significant progress have been made in the literature to thwart jamming-based DoS threats through physical and MAC layer mechanisms. Many defense schemes are shown to be effective against certain types of jamming attacks. Such schemes include frame masking for protocol-aware reactive jammers [14], channel hopping for narrow band jammers [15, 54], channel codings for low power jammers [16, 55], incentive and punishment for selfish jammers [49, 56], and spatial retreats for powerful jammers [17, 57]. Nevertheless, existing detection methods (e.g. [50, 51, 79]) can only tell whether a jamming attack is present but few are able to characterize the attack's behavior, which is the basis of choosing the corresponding defense schemes. The gap between the binary-answer (i.e., 'yes' or 'no') detection and dedicated countermeasure renders most of the existing defense proposals less effective facing a sophisticated attacker, which can intelligently change its jamming strategies. Moreover, we will show in this chapter that, interference due to *hidden terminal problems* in a wireless network can cause throughput degradations similar to that by a jamming attack. Although such interference can be mitigated by MAC mechanisms such as adaptive carrier sensing [18, 80], without properly recognizing the cause of current network anomaly, we may over-react to a nonmalicious interference problem and may artificially introduce new threats to the network. In this chapter, we address the issue of classifying unintentional and intentional (i.e., jamming) interference in a 802.11 based MANET and we seek the answers to the following two important questions:

- When a packet is received with error, is it due to unintentional interference, malicious jamming, or just poor link quality with a low SNR?
- When an expected ACK is missing, is the data packet lost at the receiver or the ACK is corrupted at the sender?

4.2 Vulnerabilities in MANET

A fundamental vulnerability of wireless networks arises from the open nature of the wireless medium and, when one considers MANETs, further vulnerabilities arise from the open peer-to-peer architecture. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, securing wireless networks and MANETs can be very challenging as the attacks can easily come from anywhere within the network as well as from outside the network. A quick survey of the literature for securing wireless networks reveals a categorization of many vulnerabilities. Loosely speaking, these threats can be broadly categorized into: confidentiality threats (e.g. adversaries inferring the meaning of communications), integrity threats (e.g. threats that arise from attacks on the identity of participants or from manipulation of messages), and availability threats (e.g. denial of service attacks that might exploit medium-access protocols) [81]. For this thesis, our interest will focus on issues related to availability of communications in wireless/MANET scenarios. Specifically, we will focus on the following three physical layer vulnerabilities of a 802.11 based MANET, which can be easily taken advantage of by jamming attacks. It is worth noting that, although the discussion here is specific for the 802.11 protocol, similar issues also apply to other wireless MAC protocols in general.

4.2.1 Carrier sensing

Carrier sensing is a fundamental mechanism in the 802.11 CSMA/CA protocol [1]. Each user senses the channel before a transmission and defers the transmission if it senses a busy channel to reduce the collision. This mechanism consists of physical carrier sensing and virtual carrier sensing. In the physical carrier sensing, the channel is determined busy if the sensed signal power is larger than a carrier sensing threshold, or idle otherwise. In the virtual carrier sensing, each user regards the channel busy during the period indicated in the MAC header of the MAC frames. An example of such virtual carrier sensing is the use of RTS (ready to send), CTS (clear to send), DATA, and ACK as defined in the IEEE 802.11 protocol.

The virtual carrier sensing mechanism can only notify the nodes in the transmission range of the sender that the medium is occupied or not, and hence whether a transmission can be decoded

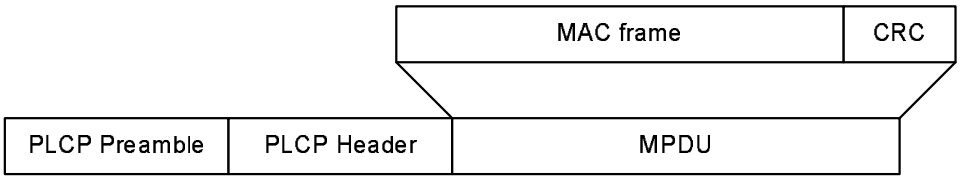


Figure 4.1: 802.11 DSSS-PHY frame format [1].

correctly assuming that the ambient background interference level is small enough. Transmissions outside of the transmission range can introduce enough interference to corrupt the reception [82]. In addition, some ongoing transmissions may not be decoded correctly due to other transmissions nearby, resulting in the failure of the virtual carrier sensing. Hence virtual carrier sensing cannot rule out collisions from inside of the transmission range and is incapable of prevent interference from outside of the transmission range.

Physical carrier sensing range, in which a transmission is heard but may not be decoded correctly, can be much larger than the transmission range and hence it can be more effective than the virtual carrier sensing in avoiding the interference. However, large carrier sensing range reduces spatial reuse and thus the network capacity. An adaptive carrier sensing range is often pursued based on the network topology, reception power, and data rate [18, 80].

The fact that carrier sensing is not sufficient to avoid interference can be exploited by malicious jamming attacks that: (i) transmit a low power signal to emulate outside-of-range interference, and (ii) misguide the network to make wrong decisions (e.g., an improperly large sensing range).

4.2.2 Packet reception

We use the 802.11 DSSS (Direct Sequence Spread Spectrum) PHY as our underlying physical layer while studying the process of packet reception in 802.11. Figure 4.1 illustrates an 802.11 DSSS PHY frame, which consists of a 144-bit PLCP (Physical Layer Convergence Procedure) preamble, a 48-bit PLCP header, and a MPDU (MAC payload tailed by a 32-bit CRC). To correctly receive a packet, the receiver must go through three phases without error: preamble detection, PLCP header reception, and a MAC-layer CRC check.

The preamble carries a pseudorandom number (PN) sequence that is the same for all frames. In the preamble detection phase, the receiver tries to synchronize its timing with the PN sequence of an

incoming packet when the signal strength of the preamble is greater than a hardware-set threshold, known as the carrier sensing threshold (CS_THRESHOLD). After the receiver successfully synchronizes with the preamble, the receiver recognizes the start of a valid 802.11 frame transmission and searches for a PLCP header after the preamble. The PLCP header contains the information about the modulation/coding bitrate (e.g., 1 Mb/s DBPSK or 2 Mb/s DQPSK), the frame length (16 bits) and a frame check sequence (16-bit CRC). If the PLCP header reception passes the CRC check, the receiver enters the *receive state* and starts to receive the MAC header, data payload, and the MAC CRC. The packet is successfully received after the MAC CRC checksum is deemed to be correct. We note that the preamble detection and PLCP header reception are independent of the MAC header information. Thus, the receiver can lock onto a packet and go into a receive state even when a packet is being transmitted with a different node intended as the destination.

The above reception process exposes a 802.11 receiver to three common forms of interference/DoS attacks: (i) scrambling the preamble synchronization and preventing the victim node from entering the receive state; (ii) corrupting the MAC frame by introducing errors in the CRC checksum; and (iii) forcing the victim node into a receive state by continuously transmitting random packets.

4.2.3 Capture effect

The capture effect is a physical layer mechanism that provides some ability to cope with interference or collisions in wireless networks. When multiple nodes transmit simultaneously in the same channel, interference occurs but does not necessarily result in packet collisions. An incoming packet can be correctly received if the received SINR exceeds a certain threshold [83, 84]. This phenomenon is known as the capture effect. Recent experiments show that the SINR threshold that a packet can be captured at (i.e., the capture threshold) is highly dependent on the arrival timing of the contending packets [85]. For the Atheros 802.11a chipset under their test, the receiver can capture the first incoming packet with the SINR of ~ 4 dB but can only capture the secondly arrived packet when its SINR is above ~ 11 dB. Therefore, a DoS attacker can send a jamming packet with a relatively low power and prevent the victim receiver from locking onto its destined packet as long as the jamming packet arrives the first.

4.3 Interference Classification Using ACK

To facilitate the design of an interference resilient MANET, we propose an interference classification scheme based solely on the statistics of the ACK reception. Our choice of ACK as the only measure of interference is motivated by the following considerations:

- The classification should be performed at the sender without cooperation from the receiver (except for sending an ACK for every received packet). Communications between the sender and receiver are the target of jamming attacks, and hence it is precisely the sender who would be most interested in understanding the cause for poor communications en route to its receivers.

- The receiver has a passive role in a communication because it often does not know who is a potential sender and/or when a packet is coming. Therefore, the receiver's perception about interference is less accurate and it can be easily fooled by an attacker. On the contrary, the sender initializes a communication and knows when an ACK should come (i.e., within a certain timeout after sending out a packet). Hence, it not only has a more accurate observation on the network condition, but also is more agile to react to anomalies.

- An ACK packet is usually short (i.e., 14 Byte long in 802.11) and thus less vulnerable to interference.

- An ACK packet has a fixed length in most MAC protocols (except for piggybacked ACK) and thus its statistics are more stable compared to variable length packets.

We do not consider authentication based attacks (e.g., fake ACKs) in this work and note that there have been many security enhancements that have been proposed to address authentication threats against communications [86, 87].

4.3.1 Jamming Attack Models

Although a radio jammer can apply many strategies to interfere with a target communication, they boil down to several basic cases and their combinations from a sender's perspective:

- A random on-off jammer that only interferes with the sender. The jammer alternatively switches between sleeping for t_s units of time and jamming for t_j units of time. t_s and t_j can be either random or fixed. During the jamming phase, the jammer constantly sends jamming packets with a variable length[1]. We define the *attack strength* as the average ratio of the jamming duration and total time. Specifically, there is no jamming when the attack strength is 0 and the jammer launches a constant attack when the strength is 1. Since this type of jammer only interferes with the sender, the ACKs from the receiver will occasionally be corrupted even if all data packets can be successfully delivered (assuming a good link condition). Note that this model does not take into account attacks that prevent the sender from sending out a packet. Detection of such attacks is beyond the scope of our interference classification.

- A reactive on-off jammer that only corrupts the ACK reception at the sender. This jammer is more intelligent compared to the above random jammer, as it can eavesdrop on data packets from the sender and predict the transmission time of ACKs. The jammer only turns on during the ACK transmission phase and tries to corrupt the sender's reception of an ACK. Similarly, we define the attack strength as the probability that the jammer turns on in an ACK transmission duration. The reactive jammer is more stealthy in that, (i) it will not appear in an idle channel; (ii) it can deliberately corrupt the preamble synchronization for an ACK packet to prevent the sender entering the receive state. Consequently, the sender may not even know whether the receiver sends the ACK.

- A jammer that only interferes with the receiver. It can be either random or reactive. A random jammer is irrespectively blocking the receiver. A reactive jamming attack dedicated to a receiver may be difficult to implement in general because it is not easy to know the destination node of a packet before it is completed received and decoded. In practice, a reactive jammer can turn on whenever it detects an incoming packet (by synchronizing the preamble). These two jamming models result in the same impact from the sender's view—data packets are corrupted. Therefore, we do not distinguish them in this work.

- Combination attacks that are any combinations of the above three basic strategies can be

[1] Similar attacks can be launched by simply sending a radio waveform or a sequence of random bits. Their differences will be discussed in Section 4.4.

employed by an adversary so as to be more difficult to recognize or classify.

4.3.2 Classification Metrics

The direct consequence of interference is packet corruption. Hence the packet error rate is an ideal measure of the interference level and its effectiveness has been recognized in previous works [79]. However, a malicious jammer can try to disguise itself by preventing a node from starting the receive state, as discussed in Section 4.2. As a result, the sender may not even notice an incoming packet, and hence it cannot detect that there was a packet error. A merit of our ACK based classification scheme is that, the sender knows that an anomaly happens if it fails to receive an expected ACK, and is thus not dependent on whether a receiver noticed that there was a start of a packet. Therefore, we believe that detection at the source is an essential component to classifying interference and thus propose the following metrics based on the statistics associated with the ACK reception event.

ACK Error Rate (AER):

$$AER = \frac{N_e}{N_c + N_e}, \tag{4.1}$$

where N_c is the number of correctly received ACKs and N_e is the number of ACKs received with error. We count a failed reception as an erroneous ACK as long as the sender enters its receive state. The incoming packet can be an interference packet other than the true ACK that never comes (e.g., the receiver does not receive the data packet so it does not send the ACK). As a result, the AER is an overestimate of the true ACK error. However, it does disclose an anomalous case that should not happen if there is no interference. Therefore it is a reliable measure of the SINR level at the sender end.

ACK Block Rate (ABR):

$$ABR = \frac{N_{mh}}{N_t}, \tag{4.2}$$

where N_t is the total number of data packets successfully sent, or equivalently, the total number of expected ACKs. N_{mh} is the number of missing ACKs when the sender does not go into the receive state but the carrier sensing power is above CS_THRESHOLD (i.e., the preamble power threshold which triggers the receive state). This situation occurs when (i) the expected ACK does not come but there is a strong interference packet, or (ii) the expected ACK comes but the sender fails to synchronize with its preamble due to interference. In either case, the ABR reflects the interference

level at the sender that blocks or may block the reception of ACKs.

ACK Missing Rate (AMR):

$$AMR = \frac{N_{ml}}{N_t}, \tag{4.3}$$

where N_{ml} is the number of missing ACKs when the sender does not go into the receive state and the carrier sensing power is below CS_THRESHOLD. It accounts for the case where the receiver does not actually send an ACK and indicates that the receiver either fails to receive the data packet or is kept from sending the ACK. In either case, the receiver is not at a good point to maintain a reliable communication. Note that N_{ml} is not an inclusive counter for the receiver-side interference and a part of the missing ACKs can be counted in N_{mh} if the sender is being interfered with at the same time. Consequently, it may underestimate the interference level at the receiver end when the interference is severe at the sender.

AER-RSS consistency: As we will see, although the AER is an effective measure of the received ACK errors, it cannot tell whether a weak reception is caused by an intentional jamming, an unintentional interference, or merely by poor link quality. Therefore, we introduce another metric, the AER–RSS consistency, similar to the PDR–RSS consistency proposed in [79]. Here the RSS is the signal strength of the received ACK. Given a specific modulation and coding scheme, AER is a monotonically decreasing function of SINR, which can be expressed by

$$AER = f\left(\frac{P}{I+N}\right) = f\left(\frac{RSS}{I+N} - 1\right), \tag{4.4}$$

where P, I, N is the power of the ACK signal, interference signal, and noise, respectively. Then, the interference power is uniquely determined by AER and RSS for a certain noise level:

$$I = \frac{RSS}{f^{-1}(AER) + 1} - N. \tag{4.5}$$

A vanishing I implies that the ACK errors are caused by a low link quality (i.e., a low SNR) and otherwise by interference. In addition, Section 4.2 shows that the unintentional interference in a properly operating network is always from outside of the carrier sensing range and thus its strength must be limited within a certain level. When an estimate I is above this level, we can claim that the interference is from a malicious attacker.

4.3.3 Machine learning based classification model

A general model for our interference classification work can be expressed by,

$$\begin{aligned} \mathcal{H}_0 &: \{y_1, \ldots, y_K\} \in \Omega_0, \quad \text{interference free,} \\ \mathcal{H}_1 &: \{y_1, \ldots, y_K\} \in \Omega_1, \quad \text{interference type 1,} \\ &\vdots \\ \mathcal{H}_M &: \{y_1, \ldots, y_K\} \in \Omega_M, \quad \text{interference type M,} \end{aligned} \tag{4.6}$$

where a case of interest is classified into one of M interference scenarios based on K metrics, $\{y_1, \ldots, y_K\}$, or classified as an interference free scenario. These statistics can be any combination of the above metrics (i.e., AER, ABR, AMR, and RSS) depending on the actual problems that we discuss below. An acceptance region, Ω_m, $m = 0, \ldots, M$, is a subset of a K-dimensional vector space that accounts for the network behaviors under interference of type-m.

Due to the dynamics of a wireless network (e.g. our motivating scenario of a MANET), the wide range of specifications for the hardware of senders and receivers, and the potential uncertainties that arise from often unforseen threats, it is impractical to analytically quantify the above statistic metrics in a real network. Fortunately, machine learning techniques provide us powerful tools that can empirically describe the acceptance regions, Ω_m, in a statistically stationary environment. Specifically, we use a Support Vector Machine (SVM) method proposed in [88], C-SVC , to perform the classification in this work. Note that the classification model in (4.6) is independent of the method to quantify Ω_m and many other statistical tools, including other SVM based methods, can serve the purpose of our classification.

4.4 Case Studies

4.4.1 Simulation in QualNet

We investigate the performance of the proposed classification metrics in several typical interference scenarios and, in the process, seek to arrive at a comprehensive classifier design that can handle all possible interference threats in a MANET. A MANET with 802.11b MAC and PHY protocols was built in the QualNet network simulator [89]. To maximize the impact of interference, we set an infinite number of data packets in all senders' queues to keep the channel saturated. In addition, we

implemented a MAC protocol that can perform both random and reactive jamming attacks with an adjustable probability, as defined in Section 4.3.1. Unless otherwise specified, the jammer uses the same transmission power as that of a legitimate node. Since the official QualNet does not implement a SINR-based preamble detection function or the capture effect, which play important roles in the interference analysis, we have incorporated the implementation from [85] into our simulations. Table 4.1 summarizes the key parameters in the simulation. In the following results, all the statistic metrics defined in Section 4.3.2 are estimated over a 20 second window.

Table 4.1: MANET Simulation Parameters in QualNet

Parameter	**Value**
PHY data rate	2 Mbps
RTS/CTS	disabled
TX power	15 dBm
Noise power	-103 dBm
CS_THRESHOLD	-93 dBm
Preamble detection threshold	[1, 5] dB
Capture threshold	8 dB
Data packet length	512 Bytes
Jamming MAC packet length	16 Bytes
Path loss exponent, γ	4
Shadow fading	none

4.4.2 Unintentional Interference versus Jamming

As discussed in Section 4.2, carrier sensing mechanisms in 802.11 CSMA/CA cannot rule out all unintentional interference cases in a wireless network. Figure 4.2 depicts such a scenario, where the node 3 and 4 are moving from the inside to the outside of the carrier sensing range of the node 1 and 2. Specifically, the horizontal distance (which we call *interference distance*) between the interfering nodes, d, increases from 300 to 900 meters. We see from Figure 4.3 that, when all the nodes are within the carrier sensing range of each other, the two communication pairs will equally share the medium. However, when they move out of the carrier sensing range, the nodes can no longer detect a busy channel but the transmission at the remote nodes (say, 3 and 4) still increases the background noise level and thus corrupts packets at a local receiver (say, node 2). Therefore, the throughput of

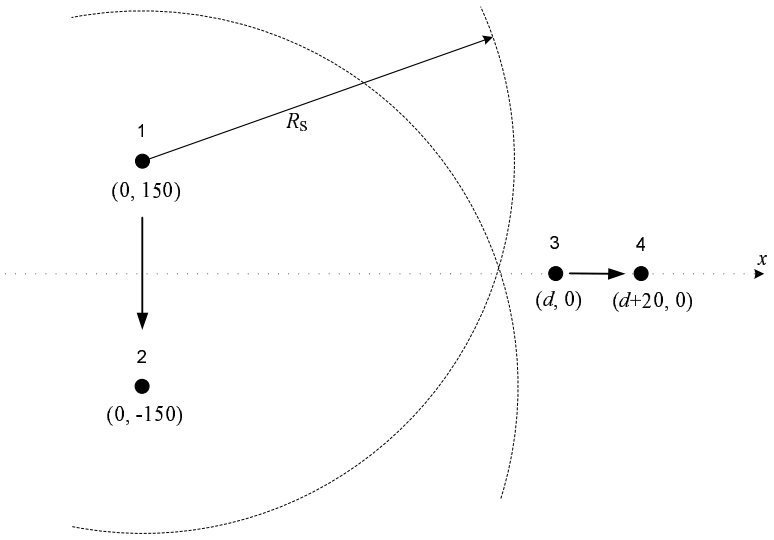
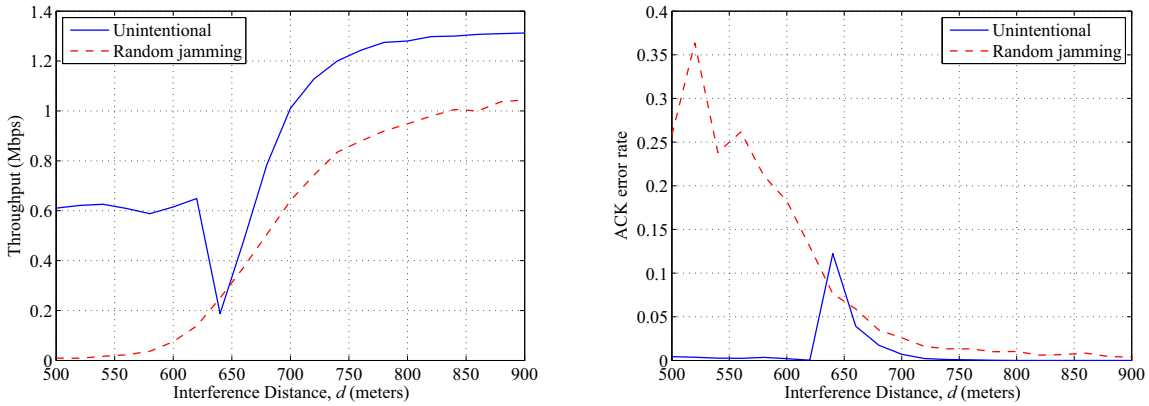


Figure 4.2: A MANET that unintentional interference occurs. Node 1 and 3 keep sending packets to node 2 and 4, respectively. R_S is the radius of the carrier sensing range (denoted by dashed arcs). (x, y) denote the coordinates of each node.

the node 1 shows a sudden drop when the interference nodes are ~ 640 meters away from each other (which implies the carrier sensing range) and gradually increases to a saturation point (i.e., $d > 900$ meters) where the medium is totally interference free and each pair of the nodes exclusively occupy the channel.

As we have known, jamming attackers can take advantage of this vulnerability and launch a low power jamming attack to emulate the unintentional out-of-range interference. We replace the node 3 with a random jammer and similarly move it between 500 to 900 meters away from the node 1 and 2. The random jammer sends jamming packets at a probability of 0.3. The jamming probability is chosen so that the effect of jamming is similar to that of the unintentional interference at the interference distance $\sim$ 640 m, where the unintentional interference is the strongest.) By Comparing the throughput and ACK errors between the jammer and unintentional interference in Figure 4.3, we see that the threat of the random jammer is only significant when it goes into the carrier sensing range of the victim node, or equivalently, increases its jamming power above the maximal level of an unintentional interference. This provides us an opportunity to distinguish the jamming attack from unintentional interference using the consistency between AER and RSS.

For different link distances between the node 1 and 2, Figure 4.4 shows the *footprints* of AER and RSS measured at the node 1 for the above two interference scenarios and the one without



(a) (b)

Figure 4.3: Unintentional interference versus random jamming in terms of (a) the throughput and (b) AER at the node 1. The interference distance is the horizontal distance between the node 1 and 3 (or the jammer). The jamming probability is 0.3.

interference. It clearly shows that the unintentional interference power is upper bounded and from the above analysis, we know this maximal power is achieved at the edge of the carrier sensing range. Only an intentional jamming attack can go beyond this limit. Hence this AER–RSS boundary is where we distinguish the jamming from unintentional interference. On the other hand, the lower bound for the unintentional interference is achieved when the interference distance increases to the infinity and the interference power diminishes. Using the AER and RSS as the input metrics to the SVM classifier in Section 4.3.3, we can obtain the empirical acceptance regions (i.e., Ω_m in (4.6) as the three shaded areas in Figure 4.4.

4.4.3 Random Jammer versus Reactive Jammer

A reactive protocol-aware jammer can prevent the sender (waiting for an ACK) from going into the receive state by corrupting the preamble synchronization of the incoming ACK. As a result, the sender may not correctly perceive the collision and AER alone is no longer a reliable indicator of the interference level. Hence we have introduced another two metrics, ABR and AMR, to account for the more stealthy interference attacks as described in Section 4.3.1.

For the three basic jamming attack models, including random sender jammer, reactive sender jammer, and receiver jammer, Figure 4.5 shows the discriminating capability of the proposed classification metrics. A very interesting observation is that, for each basic attack model, there is only one

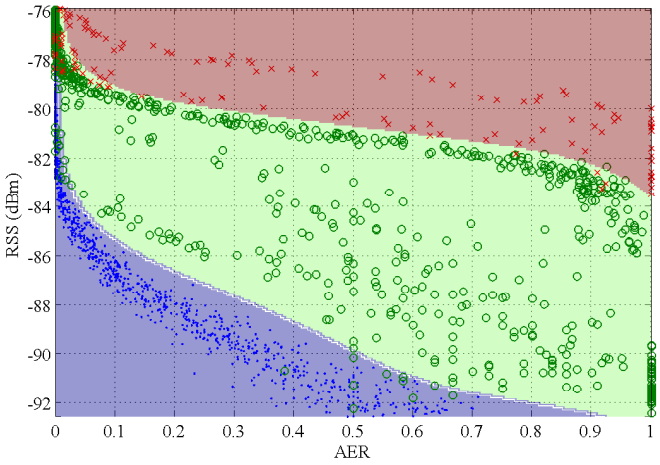
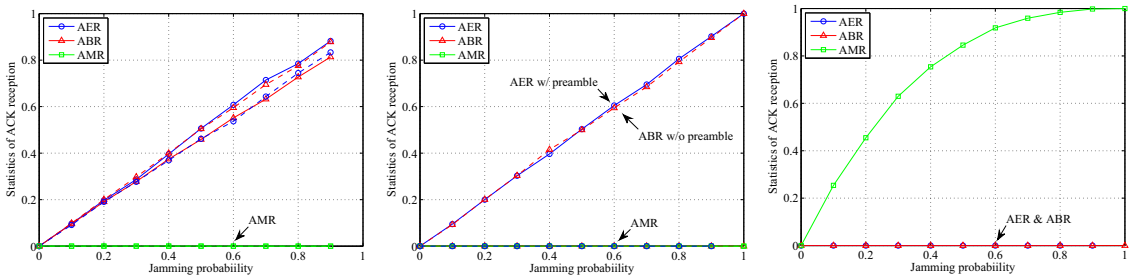


Figure 4.4: AER–RSS consistency for the cases of no interference (dots), unintentional interference (circles), and random jamming (crosses). The shaded areas are the three acceptance regions derived using C-SVC corresponding to the three interference scenarios.



(a) (b) (c)

Figure 4.5: Statistics of the ACK reception by (a) random sender jammer, (b) reactive sender jammer, (c) receiver jammer.

statistic metric with nontrivial values. If we lay out all the three metrics in a 3-dimensional space as depicted in Figure 4.6, the three basic attack models are neatly mapped onto three orthogonal bases. We also test two combined jamming attacks. For the combined random receiver jamming and reactive sender jamming ($\mathrm{Jam}_{\mathrm{combo}}$), the 3-tuple metrics fall onto the ABR–AMR plane, that is, the resulted AER is 0. For the combined random receiver and sender jamming ($\mathrm{Rand}_{\mathrm{both}}$), the 3-tuple values fall across all three dimensions. We note that the results from the interference-free case reside in the AER–AMR plane, which can be emulated by an attacker that switch between receiver jamming and random sender jamming. However, such an emulation attack can be detected using the above consistency check.

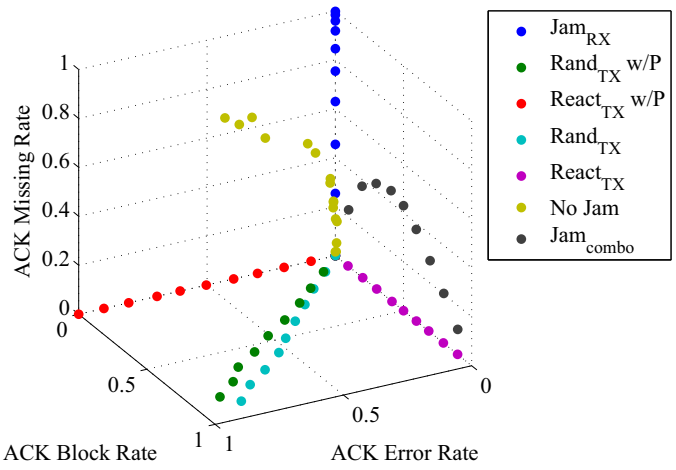


Figure 4.6: 3-d metric space to classify the receiver jamming ($\mathrm{Jam_{RX}}$), random sender jamming ($\mathrm{Rand_{TX}}$), reactive sender jamming ($\mathrm{React_{TX}}$), interference-free (No Jam), combined random receiver jamming and reactive sender jamming ($\mathrm{Jam_{combo}}$), and combined random receiver and sender jamming ($\mathrm{Rand_{both}}$).

4.5 Summary

To classify interference in an 802.11 based wireless network, or more specifically a MANET, we have proposed an interference classification framework, which distinguish between interference-free, unintentional interference, and jamming attacks. From the sender's perspective, we first categorize the potential interference scenarios into (a) unintentional interference, (b) random jamming to the sender, (c) protocol-aware reactive jamming to the sender, (d) random or reactive jamming to the receiver, and (e) combined jamming to both the sender and receiver. Given these interference models, we have introduced new classification metrics based on the statistics of ACK receptions. Specifically, we have proposed the AER, ABR, and AMR metrics, which correspond to ACK error rates, blocking rates, and missing rates measured at the sender. The three metrics form a 3-dimensional space onto which all interference scenarios can be mapped. In addition, we utilized the consistency of the frame error rate and received signal strength to handle the case where a malicious jammer tries to emulate unintentional interference. The existing consistency model has been extended so as to distinguish between low link quality (low SNR), unintentional interference, and malicious jamming. Further, we reiterate that the proposed classification scheme is carried out by the sender without the receiver's collaboration (except for sending ACKs).

Chapter 5

Conclusion and Future Work

In this thesis, we have investigated three interference related issues that are critical to the success of three emerging communication systems, including evaluation of HF interference from Broadband over Power Line (BPL) systems, detection of interference in Dynamic Spectrum Access (DSA) networks, and classification of interference in Mobile Ad Hoc Network (MANET).

First, we model the electromagnetic fields from a medium-voltage 3-phase power line mounted above a lossy earth and carrying broadband signals to and from Internet customers. We present both an exact solution for the near fields and a closed-form approximation for the far field from arbitrarily long lines. BPL emissions are computed by considering a semi-infinitely long BPL section and the maximum allowable excitation voltage versus frequency is computed by assuming compliance with FCC field strength limits. We show, based on our power line model, that (i) terrestrial interference can be significant under FCC compliance, (ii) interference into airborne receivers is potentially significant, and so current rules prohibiting BPL use at selected frequencies in the 2-50 MHz band and at 75 MHz are appropriate, (iii) there is no threat from BPL deployments to high frequency (HF) and very high frequency (VHF) ionospheric channels, (iv) Reasonable throughputs (up to 125 Mbps for a 28-MHz band) can be achieved with launch powers for which the resulting E-fields meet FCC Part 15 rules, and (v) By lowering the launch powers, one can reduce the interference range by roughly 15 meters for every 100-Mbps decrease in system capacity.

Then we study the problem of detecting unauthorized spectrum usage in a DSA network. Assuming there is only one authorized user in each spectrum channel, we propose two detection algorithms. For the mobile case, we present a Linearity-Check-for-Mobile-Transmitter (LCM) method to examine the linear relation between log-scale RSS and logarithmic link distance. For the stationary case, we present a Signalprint-Check-for-Stationary-Transmitter (SCS) method to compare the current RSS pattern with a stored pattern of the authorized transmitter. Our study shows that both

schemes achieve a detection probability above 0.9 while keeping the false alarm rate less than 0.1, given that the received SNR is large. The detection probabilities are even higher when there are multiple unauthorized radios, for the same total interference power.

Finally, we propose an interference classification framework to classify interference in a 802.11 based MANET, which distinguishes between interference-free, unintentional interference, and jamming attacks. Given the proposed interference models, we introduce new classification metrics based on the statistics of ACK receptions, including ACK error rate (AER), ACK block rate (ABR), and ACK missing rate (AMR). The three metrics form a 3-dimensional space onto which all interference scenarios can be mapped. In addition, we utilize the consistency of the frame error rate and received signal strength to handle the case where a malicious jammer tries to emulate unintentional interference. The existing consistency model is extended so as to distinguish between low link quality (low SNR), unintentional interference, and malicious jamming. We note that the proposed classification scheme is carried out by the sender without the receiver's collaboration (except for sending ACK's). It eliminates the interference threats to the classification scheme and thus is preferable in a dynamic MANET system.

Throughout the study, we have identified several issues that are worth further attention.

Our current BPL interference analysis is based on a 3-phase overhead parallel line model. In practice, HF interference from a BPL system is not only from medium-voltage power lines, but also from couplers, neutral lines, and low-voltage distribution lines [5]. It is computationally prohibitive to take into account all these factors in the analysis and thus a comprehensive study based on field measurements would be a highly useful next step. Although the FCC Part 15 rules specify the peak emission strength from BPL, the measurement guidelines to locate this peak strength remains vague. For example, the rules do not specify the measurement antenna height and the recommended distance extrapolation factors have been shown to be inconsistent with real tests [90]. Appropriate measurement schemes should be further investigated to identify the maximal BPL emissions at the minimum cost.

For the interference detection in DSA networks, we have seen that our LCM scheme for the mobile transmitter case is very sensitive to noise and random channel fadings. To improve the robustness of the proposed method, promising solutions include: (i) Incorporating other estimated

parameters, such as the path loss exponent, $\hat{\gamma}$, in (3.21) into the test statistics; and (ii) including measurement samples from the anomalous case in the machine learning process. Existing algorithms, such as [91], can make use of undersampled anomalous training data to refine the acceptance region of the detection. It is also worth carrying out experiments to confirm our theoretical analysis.

We have presented a framework to classify interference in MANET. However, the current solution only addresses several typical interference models. A comprehensive classifier design is not yet available to handle all potential interference threats. It would be useful to understand the characteristics of some more advanced jamming attacks in our proposed 3-d metric space, further define different regions in this space that correspond to different interference scenarios, and evaluate other powerful classification metrics to complement our classifier design.

Appendix A

Effects of Insulation and Line Sags

To facilitate a tractable analysis, the proposed model of BPL interference does not take into account the effects of insulation and conductor sags. Nonetheless, we examine the validity of such assumptions through simulations in 4nec2, a popular electromagnetics modeling program based on the Numerical Electromagnetics Code [92]. Figure A.1 illustrates the maximal E-field strength from a 3-phase BPL section (i.e., between two poles) under various assumptions on line insulation and line sag. For the case of line insulation, we assume polyethylene material with a thickness of 2.3 mm [93]. For the case of line sag, we use the parabolic approximation (26) in [94], and a piecewise line structure is built to emulate the resulting catenary section. For a 100-meter long and 10-meter high power line, we estimate a sag of 2 meters.

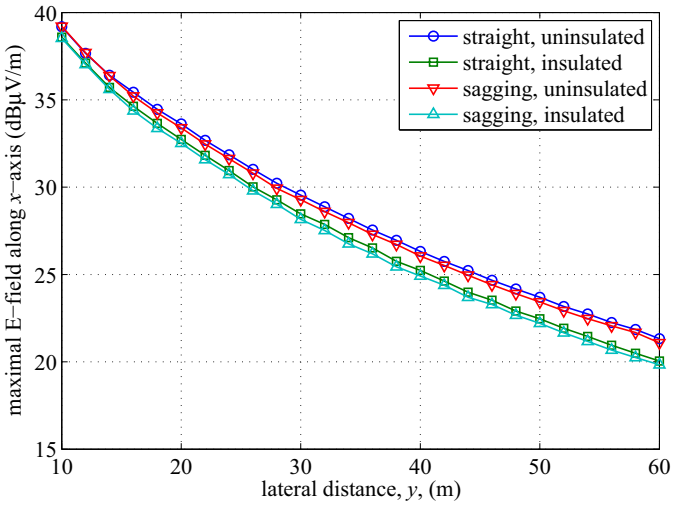


Figure A.1: Maximal E-field strength from a 3-phase BPL section with various configurations at 30 MHz. The maximal value is taken along the BPL propagation direction (i.e., x-axis) and at a height of 2 meters above ground. Each BPL section is 100 meters long, 10 meters above the lossy ground. Insulated power lines are covered by polyethylene with the thickness of 2.3 mm, with a permittivity of $2.4\varepsilon_0$. The line sag is 2 meters at the lowest point (i.e., mid-span). All four configurations have the same source voltage.

The computations for all four configurations (Figure A.1) were made for the same BPL source voltage. We observe that, for the assumed geometry, (i) the effect of ignoring line sag is negligible, and (ii) the effect of ignoring line insulation is minor ($\sim$ 1 dB at all lateral distances) and on the conservative side. Moreover, a feature of our study is that the BPL source voltage is always calibrated to just meet the FCC limits. Thus, a scale-factor change in the predicted emission field due to ignoring the insulation is compensated by a corresponding change in the assumed source voltage. We conclude that our analytical model, in its simplifications regarding insulation and sag, provides accurate estimates of BPL interference.

Appendix B

The Source Impedance of A BPL Coupler

Using an approximate analysis, we will first calculate the source impedance for a single phase wire and then show that the result can be extended to the three-phase BPL scenario with minor adjustment. The choice of the source coupler impedance is a tradeoff between the competing goals of high power delivery efficiency and low transmission loss: A larger coupler impedance can extract more power from the BPL transmissions, while it also results in greater attenuation of those signals along the line. Based on a discussion of this subject in [38], we believe a useful rule-of-thumb for BPL engineering is to satisfy the condition,

$$P_{\text{launch}} = \frac{1}{10} P_{\text{avail}} \tag{B.1}$$

where the power launched onto the wires, P_{launch}, is given by

$$\begin{aligned} P_{\text{launch}} &= \frac{1}{2}\text{Re}\left[Z_{\text{right}} \left| \frac{V_S}{Z_S + Z_{\text{left}} + Z_{\text{right}}} \right|^2 \right] \\ &= \frac{1}{2}\text{Re}\left[Z_{\text{in}} \left| \frac{V_S}{Z_S + Z_{\text{in}} + Z_{\text{in}}} \right|^2 \right] \\ &\approx \frac{1}{2}\text{Re}\left[Z_{\text{C}} \left| \frac{V_S}{Z_S + 2Z_{\text{C}}} \right|^2 \right]. \end{aligned} \tag{B.2}$$

The last two lines are based on assumptions in Section 2.1.4.

The maximum available power at the load, P_{avail}, is achieved when the load impedance equals the source impedance, that is, $\hat{Z}_{\text{in}} = Z_S/2$ (because the power is launched in both directions). Hence,

$$P_{\text{avail}} = \frac{1}{2}\text{Re}\left[\hat{Z}_{\text{in}} \left| \frac{V_S}{Z_S + 2\hat{Z}_{\text{in}}} \right|^2 \right] = \frac{1}{16}\text{Re}\left[\frac{|V_S|^2}{Z_S} \right]. \tag{B.3}$$

Combining (B.1)-(B.3), we have

$$\frac{1}{2}\text{Re}\left[Z_{\text{C}} \left| \frac{V_S}{Z_S + 2Z_{\text{C}}} \right|^2 \right] = \frac{1}{160}\text{Re}\left[\frac{|V_S|^2}{Z_S} \right]. \tag{B.4}$$

If we further assume that Z_S and $Z_{\rm in}$ are both resistances (a fair approximation), we obtain $Z_S \approx \frac{1}{19} Z_{\rm C}$. For $Z_{\rm C} \approx 500$ ohms, $Z_S = 26$ ohms.

For the three-phase power lines, we assume that the BPL signal is launched only into the first wire, with ground return, so $\mathbf{Z}_S$ has the form

$$\mathbf{Z}_S = \begin{pmatrix} Z_{S1} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \tag{B.5}$$

and $\mathbf{V}_S = [V_{S1}, 0, 0]^T$. Then the expression for $P_{\rm avail}$ remains unchanged and

$$P_{\rm launch} = \frac{1}{2} {\rm Re} \left[\mathbf{I}(0)^* \mathbf{Z}_{\rm in}(0) \mathbf{I}(0) \right], \tag{B.6}$$

where

$$\mathbf{I}(0) = [\mathbf{Z}_S + 2\mathbf{Z}_{\rm in}(0)]^{-1} \mathbf{V}_S. \tag{B.7}$$

Consider now a weak coupling system, that is, where the diagonal elements of $\mathbf{Z}_{\rm in}(0)$ dominate[1]. Then

$$\mathbf{I}(0) \approx \left[\frac{V_{S1}}{(Z_{S1} + Z_{\rm in,11})}, 0, 0 \right]^T \tag{B.8}$$

and $P_{\rm launch}$ has the same form as that in the single phase wire. Thus the impedance solution is again

$$Z_{S1} \approx \frac{1}{19} Z_{\rm in,11} \approx \frac{1}{19} Z_{\rm C,11}, \tag{B.9}$$

where $Z_{\rm in,11}$ and $Z_{\rm C,11}$ are the first-row and first-column element of $\mathbf{Z}_{\rm in}(0)$ and $\mathbf{Z}_{\rm C}$, respectively. Here we also assume that Z_{S1} and $Z_{\rm in,11}$ can be approximated as resistances.

[1]This is a very bold assumption. The actual characteristic matrix $\mathbf{Z}_{\rm in}(0) = \mathbf{Z}_C$ is nearly full for the BPL configurations in this problem. However, our numerical tests show that the resulted ratio, $P_{\rm launch}/P_{\rm avail} \approx 0.12$ at $f_c \geq 5$ MHz and is much smaller at $f_c < 5$ MHz. Thus, the impedance choice (B.9) can provide a ballpark estimate based on the expected transmission loss in (B.1).

Appendix C

Approximating A Gamma Distribution Using A Lognormal Distribution

For a Gamma distributed random variable y whose PDF is given by

$$f(y) = \frac{y^{m-1}}{\Gamma(m)a^m} \exp\left(-\frac{y}{a}\right), \quad a = \frac{E[y]}{m}, \tag{C.1}$$

$Y = \ln(y)$ can be approximated by a normal distribution $\mathcal{N}(\mu_Y, \sigma_Y^2)$ given m is large [95], where

$$\mu_Y = \ln(a) + \psi(m) \tag{C.2}$$

and

$$\sigma_Y = \sqrt{\psi'(m)}. \tag{C.3}$$

$\psi(m) = \frac{d}{dm} \ln \Gamma(m)$ is the digamma function and $\psi'(m) = \frac{d^2}{dm^2} \ln \Gamma(m)$ is the trigamma function. In addition, $\psi(m) \approx \ln(m)$ for a large m. We denote a lognormally distributed random variable $y \sim$ Log-N(μ_Y, σ_Y^2).

Appendix D

Mathematical Model of One-class SVM

One-class SVM is defined by the following optimization problem [77],

$$\begin{aligned} \min_{\rho\in\mathbb{R},\xi\in\mathbb{R}^l,c} \quad & \rho^2 + \frac{1}{\nu l}\sum_{i=1}^{l}\xi_i \\ \text{subject to} \quad & \|\Phi(\mathbf{v}_i) - c\|^2 \le \rho^2 + \xi_i, \\ & \xi_i \ge 0, \quad i = 1,\ldots,l. \end{aligned} \tag{D.1}$$

where the data instance (i.e., the test statistics), $\mathbf{v}_i$, is the estimate residues in our anomaly detection work, given in (3.22) and (3.38), respectively. Hence $\mathbf{v}_i$ is a N-dimensional energy measurements. k is the number of attributes in each data instance. Hence k equals to N, the total number of spectrum sensors. l is the number of data instances in the training set, that is, the number of trials in the training phase. $\xi = (\xi_1,\ldots,\xi_l)$ are slack variables, which allow a fraction of training data to be excluded from the hypersphere in the constraint. $\Phi(\mathbf{v}_i)$ is a mapping function that maps the measurements, $\mathbf{v}_i$, into a feature space where an inner product can be computed by a kernel function defined as $K_\Phi(\mathbf{v}_i,\mathbf{v}_j) = \Phi(\mathbf{v}_i)^T\Phi(\mathbf{v}_j)$. We use the radial basis function (RBF) as the kernel function in our study:

$$K_\Phi(\mathbf{v}_i,\mathbf{v}_j) = \exp(-\frac{1}{k}\|\mathbf{v}_i - \mathbf{v}_j\|^2), \quad \gamma > 0. \tag{D.2}$$

The anomaly detection problem can be viewed as minimizing the radius ρ of a hypersphere, centered at c, that encloses a subset of the training data (i.e., the acceptance region, Ω).

The optimization problem (D.1) is solved by the dual problem,

$$\begin{aligned} \min_{\alpha} \quad & \sum_i\sum_j \alpha_i\alpha_j K_\Phi(\mathbf{v}_i,\mathbf{v}_j) - \sum_i \alpha_i K_\Phi(\mathbf{v}_i,\mathbf{v}_j) \\ \text{subject to} \quad & 0 \le \alpha_i \le \frac{1}{\nu l}, \quad \sum_i \alpha_i = 1. \end{aligned} \tag{D.3}$$

Each data instance from the testing set, $\mathbf{u}$, is then classified using the decision function,

$$\mathcal{H}_0 : \quad \sum_i \sum_j \alpha_i \alpha_j K_\Phi(\mathbf{v}_i, \mathbf{v}_j) - 2 \sum_i \alpha_i K_\Phi(\mathbf{v}_i, \mathbf{u}) + K_\Phi(\mathbf{u}, \mathbf{u}) \leq R^2. \tag{D.4}$$

Note that we do not need to know the explicit form of $\Phi(\mathbf{v}_i)$ to solve the dual problem.

References

[1] *ISO/IEC Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (Includes IEEE Std 802.11, 1999 Edition; IEEE Std 802.11A.-1999; IEEE Std 802.11B.-1999; IEEE Std 802.11B.-1999/Cor 1-2001; and IEEE Std 802.11D.-2001)*, Std., 2005.

[2] *IEEE J. Sel. Areas Commun., Special Issue on Power Line Communications*, vol. 24, no. 7, Jul. 2006.

[3] ISPLC. [Online]. Available: http://www.isplc.org/

[4] "Radio frequency devices," Title 47 of the Code of Federal Regulations, Part 15, FCC, Jul. 2008.

[5] D. Evans and M. D. Gallagher, "Potential interference from broadband over power line (BPL) systems to federal government radiocommnunications at 1.7 - 80 mhz – phase I study," National Telecommunications and Information Administration (NTIA), U.S. Dept. of Commerce, NTIA Report 04-413, Apr. 2004.

[6] E. Hare. Calculated impact of plc on stations operating in the amateur radio service. The American Radio Relay League (ARRL). [Online]. Available: http://www.arrl.org/tis/info/HTML/plc/interference.html

[7] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, May 2006.

[8] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar, "Ieee 802.22: the first worldwide wireless standard based on cognitive radios," in *Proc. IEEE DySPAN 2005*, Nov. 2005, pp. 328–337.

[9] W. Xu, P. Kamat, and W. Trappe, "TRIESTE: A trusted radio infrastructure for enforcing spectrum etiquettes," in *Proc. Networking Technologies for Software Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop on*, Sep. 2006, pp. 101–109.

[10] S. Verdú, *Multiuser detection*. New York: Cambridge University Press, 1998.

[11] H. L. V. Trees, *Detection, estimation, and modulation theory*. New York: Wiley, 2001.

[12] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[13] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *Wireless Communications, IEEE*, vol. 11, no. 1, pp. 38–47, Feb. 2004.

[14] A. D. Wood, J. A. Stankovic, and Z. Gang, "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," in *SECON'07. 4th Annual IEEE Communications Society Conference on*, Jun. 2007, pp. 60–69.

[15] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *Proc. INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, May 2007, pp. 2526–2530.

[16] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, no. 3, pp. 29–30, Jul. 2003.

[17] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *Network, IEEE*, vol. 20, no. 3, pp. 41–47, May 2006.

[18] J. Zhu, X. Guo, L. L. Yang, W. S. Conner, S. Roy, and M. M. Hazra, "Adapting physical carrier sensing to maximize spatial reuse in 802.11 mesh networks: Research articles," *Wirel. Commun. Mob. Comput.*, vol. 4, no. 8, pp. 933–946, Dec. 2004.

[19] F. Rachidi, C. A. Nucci, M. Ianoz, and C. Mazzetti, "Influence of a lossy ground on lightning-induced voltages on overhead lines," *IEEE Trans. Electromagn. Compat.*, vol. 38, no. 3, pp. 250–264, Aug. 1996.

[20] R. G. Olsen, J. L. Young, and D. C. Chang, "Electromagnetic wave propagation on a thin wire above earth," *IEEE Trans. Antennas Propag.*, vol. 48, no. 9, pp. 1413–1419, Sep. 2000.

[21] A. Sommerfeld, "Über die ausbreitung der wellen in der drahtlosen telegraphie," *Ann. Physik*, vol. 28, p. 665C736, 1909.

[22] R. W. P. King, *The theory of linear antennas, with charts and tables for practical applications*. Cambridge, MA: Harvard University Press, 1956.

[23] A. Baños, *Dipole radiation in the presence of a conducting half space*, 1st ed. New York: Pergamon Press, 1966.

[24] K. A. Norton, "The propagation of radio waves over the surface of the earth and in the upper atmosphere," *Proc. Inst. Radio Eng.*, vol. 25, no. 9, pp. 1203–1236, Sep. 1937.

[25] P. Parhami, Y. Rahmat-Samii, and R. Mittra, "An efficient approach for evaluating sommerfeld integrals encountered in the problem of a current element radiating over lossy ground," *IEEE Trans. Antennas Propag.*, vol. 28, no. 1, pp. 100–104, Jan. 1980.

[26] R. W. P. King, "Electromagnetic field of a vertical electric dipole over an imperfectly conducting half-space," *Radio Sci.*, vol. 25, pp. 149–160, Mar./Apr. 1990.

[27] R. F. Harrington, "Matrix methods for field problems," *Proceedings of the IEEE*, vol. 55, no. 2, pp. 136–149, Feb. 1967.

[28] R. Coifman, V. Rokhlin, and S. Wandzura, "The fast multipole method for the wave equation: a pedestrian prescription," *IEEE Antennas Propag. Mag.*, vol. 35, no. 3, pp. 7–12, Jun. 1993.

[29] Numerical Electromagnetics Code (NEC) – method of moments. Lawrence Livermore Laboratory. [Online]. Available: http://www.llnl.gov/ipandc/technology/software/softwaretitles/nec.php

[30] J. R. Carson, “Wave propagation in overhead wires with ground return,” *Bell Syst. Tech. J*, vol. 5, pp. 539–554, Oct. 1926.

[31] J. R. Wait, “Theory of wave propagation along a thin wire parallel to an interface,” *Radio Sci.*, vol. 7, pp. 675–679, Jun. 1972.

[32] E. Kuester, D. Chang, and R. Olsen, “Model theory of long horizontal wire structure above the earth, 1, excitation,” *Radio Sci.*, vol. 13, pp. 605–613, Jul./Aug. 1978.

[33] R. Olsen, E. Kuester, and D. Chang, “Model theory of long horizontal wire structure above the earth, 2, properties of discrete modes,” *Radio Sci.*, vol. 13, pp. 615–623, Jul./Aug. 1978.

[34] M. D’Amore and M. S. Sarto, “Simulation models of a dissipative transmission line above a lossy ground for a wide-frequency range. I. single conductor configuration,” *IEEE Trans. Electromagn. Compat.*, vol. 38, no. 2, pp. 127–138, May 1996.

[35] ——, “Simulation models of a dissipative transmission line above a lossy ground for a wide-frequency range. II. multiconductor configuration,” *IEEE Trans. Electromagn. Compat.*, vol. 38, no. 2, pp. 139–149, May 1996.

[36] ——, “A new formulation of lossy ground return parameters for transient analysis of multiconductor dissipative lines,” *IEEE Trans. Power Del.*, vol. 12, no. 1, pp. 303–314, Jan. 1997.

[37] ——, “Electromagnetic field radiated from broadband signal transmission on power line carrier channels,” *IEEE Trans. Power Del.*, vol. 12, no. 2, pp. 624–631, Apr. 1997.

[38] P. S. Henry, “Interference characteristics of broadband power line communication systems using aerial medium voltage wires,” *IEEE Commun. Mag.*, vol. 43, no. 4, pp. 92–98, Apr. 2005.

[39] M. Zimmermann and K. Dostert, “A multipath model for the powerline channel,” *IEEE Trans. Commun.*, vol. 50, no. 4, pp. 553–559, Apr. 2002.

[40] E. Biglieri, “Coding and modulation for a horrible channel,” *IEEE Commun. Mag.*, vol. 41, no. 5, pp. 92–98, May 2003.

[41] P. Amirshahi and M. Kavehrad, “High-frequency characteristics of overhead multiconductor power lines for broadband communications,” *IEEE J. Sel. Areas Commun.*, vol. 24, no. 7, pp. 1292–1303, Jul. 2006.

[42] J. C. Richards and J. V. Williams, “Potential interference from broadband over power line (BPL) systems to federal government radiocommnunications at 1.7 - 80 mhz – phase II study,” National Telecommunications and Information Administration (NTIA), U.S. Dept. of Commerce, NTIA Report 08-450, Oct. 2007.

[43] R. Chen and J.-M. Park, “Ensuring trustworthy spectrum sensing in cognitive radio networks,” in *Proc. Networking Technologies for Software Defined Radio Networks, 2006. SDR ’06.1st IEEE Workshop on*, Sep. 2006, pp. 110–119.

[44] R. Chen, J.-M. Park, and J. H. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” *Selected Areas in Communications, IEEE Journal on*, vol. 26, no. 1, pp. 25–37, 2008.

[45] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proc. Proceedings of the 5th ACM workshop on Wireless security*, Los Angeles, CA, Sep. 2006, pp. 43–52.

[46] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building rf-based user location and tracking system," in *Proc. INFOCOM 2000*, Mar. 2000, pp. 775–784.

[47] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 mac layer spoofing using received signal strength," in *Proc. INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, Apr. 2008, pp. 1768–1776.

[48] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *Wireless Communications, IEEE Transactions on*, vol. 7, pp. 2571–2579, Jul. 2008.

[49] P. Kyasanur and N. H. Vaidya, "Selfish mac layer misbehavior in wireless networks," *Mobile Computing, IEEE Transactions on*, vol. 4, no. 5, pp. 502–516, Sep. 2005.

[50] A. C. Alvaro, S. Radosavac, and J. S. Baras, "Detection and prevention of mac layer misbehavior in ad hoc networks," in *Proc. the 2nd ACM workshop on Security of ad hoc and sensor networks*. Washington DC, USA: ACM, 2004, pp. 17 – 22.

[51] M. Raya, J.-P. Hubaux, and I. Aad, "DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots," in *Proc. the 2nd international conference on Mobile systems, applications, and services*. Boston, MA: ACM, 2004, pp. 84 – 97.

[52] A. L. Toledo and X. Wang, "Robust detection of mac layer denial-of-service attacks in csma/ca wireless networks," *Information Forensics and Security, IEEE Transactions on*, vol. 3, no. 3, pp. 347–358, Jun. 2008.

[53] M. Cagalj, S. Ganeriwal, I. Aad, and J. P. Hubaux, "On selfish behavior in CSMA/CA networks," in *Proc. INFOCOM 2005. IEEE*, Mar. 2005, pp. 2513–2524.

[54] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: defending wireless sensor networks from interference," in *Proc. Proceedings of the 6th international conference on Information processing in sensor networks*. Cambridge, Massachusetts, USA: ACM, 2007, pp. 499 – 508.

[55] J. T. Chiang and Y.-C. Hu, "Cross-layer jamming detection and mitigation in wireless broadcast networks," in *Proc. the 13th annual ACM international conference on Mobile computing and networking*. ACM, 2007, pp. 346 – 349.

[56] J. Konorski, "A game-theoretic study of CSMA/CA under a backoff attack," *Networking, IEEE/ACM Transactions on*, vol. 14, no. 6, pp. 1167–1178, Dec. 2006.

[57] A. D. Wood, J. A. Stankovic, and S. H. Son, "Jam: a jammed-area mapping service for sensor networks," in *Proc. Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE*, Dec. 2003, pp. 286–297.

[58] J. R. Wait, *Electromagnetic Radiation from Cylindrical Structures*. New York: Pergamon Press, 1959.

[59] L. M. Wedepohl, "Application of matrix methods to the solution of travelling-wave phenomena in polyphase systems," *Electrical Engineers, Proceedings of the Institution of*, vol. 110, no. 12, pp. 2200–2212, Dec. 1963.

[60] C. R. Paul, *Analysis of multiconductor transmission lines*, ser. Wiley series in microwave and optical engineering. New York: John Wiley & Sons Inc, 1994.

[61] K. A. Michalski, J. R. Mosig, and M. I. Aksun, "Enhancing the robustness of the discrete complex image method for planar multilayered media," in *Proc. Microwave Conference, 2007. APMC 2007. Asia-Pacific*, Dec. 2007, pp. 1–4.

[62] W. C. Chew, "A quick way to approximate a sommerfeld-weyl-type integral," *IEEE Trans. Antennas Propag.*, vol. 36, no. 11, pp. 1654–1657, Nov. 1988.

[63] R. W. P. King, *The theory of linear antennas, with charts and tables for practical applications*. Cambridge, MA: Harvard University Press, 1956, ch. VII.6.

[64] R. Olsen, "Technical considerations for broadband powerline (BPL) communication," in *Proc. Zurich Symposium on EMC*, Zurich, Switzerland, Feb. 2005.

[65] R. Cools and A. Haegemans, "Algorithm 824: CUBPACK: A package for automatic cubature; framework description," *ACM Trans. Math. Software*, vol. 29, no. 3, pp. 287–296, 2003.

[66] "Amendment of part 15 regarding new requirements and measurements guidelines for access broadband over power line systems and carrier current systems including broadband over power line systems," FCC, Report and Order 04-245, Oct. 2004.

[67] *Radio Noise*, ITU-R Std. P.372-8, 2003.

[68] S. Liu and L. J. Greenstein, "Radiation characteristics and interference of large broadband power line (BPL) deployments," in *Proc. Communications, 2008. ICC'08. IEEE International Conference on*, Beijing, China, May 2008, pp. 2071–2075.

[69] J. Lee, S. Choi, H. Oh, W. Lee, K. Kim, and D. Lee, "Measurements of the communications environment in medium voltage power distribution lines for wide-band power line communications," in *Proc. the 8th International Symposium on Power-line Communications and its Applications (ISPLC 2004)*, Zaragoza, Spain, Mar. 2004, pp. 69–74.

[70] D. Liu, E. Flint, B. Gaucher, and Y. Kwark, "Wide band AC power line characterization," *IEEE Trans. Consum. Electron.*, vol. 45, no. 4, pp. 1087–1097, Nov. 1999.

[71] S. Catreux, P. F. Driessen, and L. J. Greenstein, "Simulation results for an interference-limited multiple-input multiple-output cellular system," *IEEE Commun. Lett.*, vol. 4, no. 11, pp. 334–336, Nov. 2000.

[72] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, Apr. 1967.

[73] A. Goldsmith, *Wireless Communications*. New York, NY: Cambridge University Press., 2005.

[74] M. Gudmundson, "Correlation model for shadow fading in mobile radio systems," *Electronics Letters*, vol. 27, no. 23, pp. 2145–2146, Nov. 1991.

[75] F. F. Digham, M. S. Alouini, and M. K. Simon, "On the energy detection of unknown signals over fading channels," in *Proc. Communications, 2003. ICC '03. IEEE International Conference on*, May 2003, pp. 3575–3579.

[76] Y. Chen, W. Trappe, and R. P. Martin, "Attack detection in wireless localization," in *Proc. INFOCOM 2007. 26th IEEE International Conference on Computer Communications*, Anchorage, AK, May 2007, pp. 1964–1972.

[77] B. Schölkopf, J. C. Platt, J. C. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Neural Comput.*, vol. 13, no. 7, pp. 1443–1471, Jul. 2001.

[78] L. Xiao, L. Greenstein, and N. Mandayam, "Sensor-assisted localization in cellular systems," *IEEE Trans. Wireless Commun.*, vol. 6, no. 12, pp. 4244–4248, Dec. 2007.

[79] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. the 6th ACM international symposium on Mobile ad hoc networking and computing*. Urbana-Champaign, IL, USA: ACM, 2005, pp. 46–57.

[80] H. Zhai and Y. Fang, "Physical carrier sensing and spatial reuse in multirate and multihop wireless ad hoc networks," in *Proc. INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, 2006, pp. 1–12.

[81] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in *Proc. the 12th conference on USENIX Security Symposium - Volume 12*. Washington, DC: USENIX Association, Aug. 2003.

[82] K. Xu, M. Gerla, and S. Bae, "How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks?" in *Proc. Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE*, 2002, pp. 72–76.

[83] A. Kochut, A. Vasan, A. U. Shankar, and A. Agrawala, "Sniffing out the correct physical layer capture model in 802.11b," in *Proc. Network Protocols, 2004. ICNP 2004. Proceedings of the 12th IEEE International Conference on*, Oct. 2004, pp. 252–261.

[84] J. Lee, W. Kim, S.-J. Lee, D. Jo, J. Ryu, T. Kwon, and Y. Choi, "An experimental study on the capture effect in 802.11a networks," in *Proc. Proceedings of the second ACM international workshop on Wireless network testbeds, experimental evaluation and characterization*. Montreal, Quebec, Canada: ACM, 2007, pp. 19–26.

[85] J. Lee, J. Ryu, S.-J. Lee, and T. T. Kwon, "Improved modeling of ieee 802.11a phy through fine-grained measurements," *Computer Networks*, vol. 54, no. 4, pp. 641–657, Mar. 2010.

[86] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *Network, IEEE*, vol. 13, no. 6, pp. 24–30, Nov. 1999.

[87] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion detection techniques in mobile ad hoc and wireless sensor networks," *Wireless Communications, IEEE*, vol. 14, no. 5, pp. 56–63, Oct. 2007.

[88] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, Sep. 1995.

[89] Qualnet simulator. [Online]. Available: http://www.scalable-networks.com/

[90] E. Hare, "Electric and magnetic fields near physically large radiators," ARRL, Exhibit D to ARRL Comments, Jul. 2003.

[91] D. M. J. Tax and R. P. W. Duin, “Support vector data description,” *Machine Learning*, vol. 54, no. 1, pp. 45–66, Jan. 2004.

[92] A. Voors. 4nec2 – NEC based antenna modeler and optimizer. [Online]. Available: http://home.ict.nl/~arivoors/

[93] G. M. Hashmi, M. Lehtonen, and M. Nordman, “Modeling and experimental verification of on-line pd detection in mv covered-conductor overhead networks,” *Dielectrics and Electrical Insulation, IEEE Transactions on*, vol. 17, no. 1, pp. 167–180, Feb. 2010.

[94] A. V. Mamishev, R. D. Nevels, and B. D. Russell, “Effects of conductor sag on spatial distribution of power line magnetic field,” *IEEE Trans. Power Del.*, vol. 11, no. 3, pp. 1571–1576, Jul. 1996.

[95] R. L. Prentice, “A log gamma model and its maximum likelihood estimation,” *Biometrika*, vol. 61, no. 3, pp. 539–544, 1974.

Curriculum Vita

Song Liu

2010 Ph.D. in Electrical Engineering, Rutgers University, USA
2003 M.E. in Electronic Engineering, Tsinghua University, China
2000 B.E. in Electronic Engineering, Tsinghua University, China

2004-2010 Graduate Assistant, WINLAB, Rutgers University, USA
2006 Graduate Intern, Intel Corporation, USA
2000-2003 Research Assistant, Network Theory Laboratory, Tsinghua University, China

Publications

[1] S. Liu, and L. J. Greenstein, ”Interference Evaluation of Overhead Medium-Voltage Broadband Power Line (BPL) Systems,” to appear in IEEE Transactions on Electromagnetic Compatibility.

[2] S. Liu, Y. Chen, W. Trappe, L. J. Greenstein, ”ALDO: An Anomaly Detection Framework for Dynamic Spectrum Access Networks,” in Proc. IEEE International Conference on Computer Communications (INFOCOM) 2009, pp. 675-683.

[3] S. Liu, Y. Chen, W. Trappe, L. J. Greenstein, ”Non-interactive Localization of Cognitive Radios Based on Dynamic Signal Strength Mapping,” in Proc. IEEE International Conference on Wireless On-demand Network Systems and Services (WONS) 2009, pp. 85-92. (*Best Paper Award*)

[4] S. Liu and L. J. Greenstein, ”Emission Characteristics and Interference Constraint of Overhead Medium-Voltage Broadband Power Line Systems,” in Proc. IEEE Global Telecommunications Conference (Globecom) 2008. pp. 1-5.

[5] S. Liu and L. J. Greenstein, ”Radiation Characteristics and Interference of Large Broadband Power Line (BPL) Deployments,” in Proc. IEEE International Conference on Communications (ICC) 2008, pp. 2071-2075.

[6] S. Liu and L. J. Greenstein, ”Modeling and Interference Evaluation of Overhead Medium-Voltage Broadband Power Line (BPL) Systems,” in Proc. IEEE Global Telecommunications Conference (Globecom) 2007, pp. 134-139.