2009-10-22

Frequency Rendezvous and Physical Layer Network Coding for Distributed Wireless Networks

Di Pu
Worcester Polytechnic Institute

Frequency Rendezvous and Physical Layer Network Coding for Distributed Wireless Networks

by

Di Pu

A Thesis
Submitted to the Faculty
of the
WORCESTER POLYTECHNIC INSTITUTE
in partial fulfillment of the requirements for the
Degree of Master of Science
in
Electrical and Computer Engineering
by

October 20 2009

APPROVED:

Professor Alexander M. Wyglinski, Major Advisor

Professor Andrew G. Klein

Professor Weichao Wang

Abstract

In this thesis, a transmission frequency rendezvous approach for secondary users deployed in decentralized dynamic spectrum access networks is proposed. Frequency rendezvous is a critical step in bootstrapping a wireless network that does not possess centralized control. Current techniques for enabling frequency rendezvous in decentralized dynamic spectrum access networks either require pre-existing infrastructure or use one of several simplifying assumptions regarding the architecture, such as the use of regularly spaced frequency channels for communications. Our proposed approach is designed to be operated in a strictly decentralized wireless networking environment, where no centralized control is present and the spectrum does not possess pre-defined channels. In our proposed rendezvous algorithm, the most important step is pilot tone detection and receiver query. In order to realize a shortest search time for the target receiver, an efficient scanning rule should be employed. In this thesis, three scanning rules are proposed and evaluated, namely: frequency sequence scanning, pilot tone strength scanning, and cluster scanning. To validate our result, we test our scanning rules with actual paging band spectrum measurements.

Previous research on security of network coding focuses on the protection of data dissemination procedures and the detection of malicious activities such as pollusion attacks. The capabilities of network coding to detect other attacks has not been fully explored. In this thesis, a new mechanism based on physical layer network coding to detect wormhole attacks is proposed. When two signal sequences collide at the receiver, the difference between the two received sequences is determined by its distances to the senders. Therefore, by comparing the differences between the received sequences at two nodes, we can estimate the distance between them and detect those fake neighbor connections through wormholes. While the basic idea is clear, we design many schemes at both physical and network layers to turn the idea into a practical approach. Simulations using BPSK modulation at the physical layer show that the wireless nodes can effectively detect fake neighbor connections without the adoption of any special hardware on them.

Acknowledgements

First and foremost I would like to thank my advisor, Professor Alexander M. Wyglinski, for introducing me to the very interesting world of software defined radio, for encouraging me to pursue my research topic and for his guidance over the course of my time at the university. While giving his students a large degree of independence and flexibility to manage their time and projects, he is always available and willing to help in any way possible. Whether reviewing presentations, acquiring the necessary equipment or brainstorming about projects, his enthusiasm for new ideas and genuine interest in students work are admirable and deeply appreciated.

The financial support provided by The MathWorks, Natick, MA, USA and by Professor Wyglinski is duly acknowledged.

I would like to thank Professor Andrew G. Klein and Professor Weichao Wang, members of my M.S. committee, for their feedback and suggestions during the development phase of my Master Thesis. I would like to thank Mike McLernon from The MathWorks, for his great guidance on my internship at The MathWorks, as well as the contributions to our collaborated publication. I would also like to thank my current and former fellow colleagues at the Wireless Innovation Laboratory (WI Lab): Michael Leferman, Srikanth Pagadarai, Si Chen, Zhou Yuan, Kevin Bobrowski and Jingkai Su, for making my time in the lab such an enjoyable and memorable experience. Thanks to all of you for making my time at WPI special.

Last but certainly not the least, I'd especially like to thank my parents for taking interest in my work and encouraging me from my childhood days all the way through graduate school. Thanks for providing me with the tools I needed to succeed and for supporting me along the way. Thank you for everything.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Coordinating wireless devices in a decentralized communication network is a heavily researched problem. Whether it is an emergency/disaster relief situation [4–6], a military application [7–9], or a sensor network scenario [10–12], establishing a network without any form of centralized intelligence is difficult. Recently, *cognitive radios* (CRs) [13] have been proposed as a possible solution to improve spectrum utilization via opportunistic spectrum sharing. It is also a very promising technique for radios to find one another and bootstrap bidirectional communications. The process of two or more radios to search for one another and establish a link on a common frequency channel is called *frequency rendezvous*.

Network coding has attracted a significant attention in the research community since the concept was proposed. However, the security capabilities of physical layer network coding to detect malicious attacks have not been fully explored. For instance, it is possible that when signals collide at the receiver, we can potentially extract information about the network structure. This information can then be used to detect attacks on network topology. In this thesis, we conduct an initial investigation of this problem. Specifically, we propose a new mechanism to detect wormhole attacks.

1.2 Current State-of-the-Art

Currently, there are several techniques to realize frequency rendezvous in a cognitive radio network employing dynamic spectrum access. One approach for frequency-domain rendezvous was proposed in [14], where several frequencies are set aside for use as spectrum information channels. A link rendezvous protocol was proposed in [15] to minimize unintentional interference during the rendezvous process by using a very short duration, narrow bandwidth, low power attention signal. This approach avoids a dedicated signaling channel, only requiring radios to operate within a common band. Based on this link rendezvous protocol, an unaided sequence-based rendezvous was proposed in [16], which uses non-orthogonal sequences to determine the order in which radios visit potentially available channels.

With respect to network coding, when the intermediate nodes actively generate linear combinations of the received packets and forward the mixed results, we can improve network throughput for multicast traffic, reduce network congestion, and enhance network robustness with respect to packet loss. Investigators have proposed the concept of physical layer network coding [17, 18] for wireless networks to fully explore these advantages. The technique is especially valuable in wireless networks when we consider the limited bandwidth and power resources of the nodes. Since network coding may allow data errors and/or corrupted packets to propagate widely and ruin the data recovery procedure at the final destination, previous research into network coding security focused on the protection of data dissemination procedures and the detection of malicious activities such as pollution attacks [19, 20].

1.3 Thesis Contributions

Given the solutions currently available in the literature, several technical issues exist with current techniques for enabling rendezvous in decentralized wireless communications network, namely:

1. *Dedicated Control Channels*: While the use of a dedicated control channel simplifies

the initial step of determining in which frequency to look for neighbors, it may not be feasible to implement these control channels in several types of decentralized DSA network architecture.

2. *Regularly Spaced Frequency Channels*: The link rendezvous protocol needs to divide the spectrum into regularly spaced frequency channels, which may lack the flexibility required to perform dynamic spectrum access.

3. *Pre-defined Channel Visiting Order*: The sequence-based rendezvous algorithm makes an assumption of a pre-defined sequence by each radio to determine the visiting order to other potential channels. Consequently, this scheme is inflexible when wireless nodes enter or exit the network.

To resolve these issues, we propose a frequency rendezvous approach that enables ad hoc network formation. This approach employs a transmitter to scan the spectrum and visit all the receivers available at each frequency. If it is the target receiver, they can quickly handshake and start the data transmission. The benefits of such a scheme include[1]:

1. *No Control Channels*: In our framework, the transmitter (Tx) and each receiver (Rx) use pilot signals in order to identify their center frequency locations. All overhead information about the Tx and Rx is transferred within the data transmission bands. Moreover, a control channel is not employed since it would either require a dedicated frequency band assignment or it would be susceptible to interference if also employed in a secondary spectrum access approach.

2. *Flexible Frequency Channels*: Our technique views the spectrum as a whole, so the transmitter does not need to wait until a certain number of vacant channels are identified.

3. *No Pre-defined Channel Visiting Order*: Our algorithm makes no assumption about the channel center frequency locations. As a result, we can randomly search frequency ranges and focus on the portions of spectrum with greater possibility of finding the desired signal. This is the basis of our scanning rules.

[1]This is partially based on the work presented in [21] and [22].

Compared to previous approaches in physical layer network coding, our investigation has the following contributions[2]:

1. We make an attempt to explore the security capabilities of the physical layer network coding technique. The research will demonstrate that in addition to improving the bandwidth efficiency and data robustness in wireless networks, physical layer network coding can also be used to detect malicious attacks. This research provides a new incentive for further development of this technique.

2. The proposed wormhole detection mechanism does not require any special hardware or time synchronization in the wireless network. Therefore, existing systems can easily adopt the proposed approach without going through drastic structural and functional changes.

3. We carefully design schemes in both network layer and physical layer to make the approach practical. Impacts of different factors in the communication channel are studied through theoretic analysis and simulation.

1.4 Thesis Organization

The remainder of the thesis is organized as follows: In Chapter 2, the background of distributed wireless networks, a cognitive radio (*i.e.* an SDR), and how it relates to a dynamic spectum access network will be discussed. Also to be reviewed is work related to frequency rendezvous and network coding. In Section 2.4.3, we introduce the basic idea of the detection mechanism and the role of physical layer network coding in wormhole detection. Chapter 3 describes the network framework employing the frequency rendezvous algorithm and analyzes three different scanning rules mathematically. Simulation setup and performance results are presented at the end of this chapter. In Section 3.1, we describe the network framework employing the frequency rendezvous algorithm. Then, three different scanning rules proposed in [21] are provided. In Section 3.2, these three scanning rules are mathematically analyzed. Simulation setup and performance results, as well as

[2]This is partially based on the work presented in [23].

the comparison with the theoretical results are presented in Section 3.3. Chapter 4 elaborates on physical layer network coding in wormhole detection. Sections 4.1 and 4.2 design mechanisms in the network layer and in the physical layer to make the approach secure and practical. We perform both an analysis and simulations to investigate the impacts of different factors in the physical layer. In Section 4.3 we study the security and detection accuracy of the proposed approach. Finally, Chapter 5 concludes the thesis. It contains concluding remarks and the current and future work being done in relation to the progress of the frequency rendezvous and physical layer network coding described in this thesis.

Chapter 2

Overview of Distributed Wireless Networks and Applications

In this chapter, background is first given on distributed wireless network, since it is the environment where both frequency rendezvous and physical layer network coding are applied. Then, the basic characteristics of a cognitive radio and dynamic spectrum access, including its definition, function and model classification are reviewed. Finally, an overview of related work in the area of spectrum rendezvous and network coding will be presented.

2.1 Distributed Wireless Networks

With rapid progress in wireless communications, higher system capacity and higher data rates to a large number of users are needed to be provided. In conventional cellular system, because of the large distance to collocated antenna at base station and interference of nearby cells the users near cell boundaries have low performance. In recent years, there has been considerable interest in distributed wireless network due to its promising improvement in coverage, power efficiency and channel capacity [24, 25].

Distributed wireless network is a new architecture for a wireless access system with distributed antennas, distributed processors, and distributed controlling. With distributed antennas, system capacity can be expanded through dense frequency reuse, and transmission

power can be greatly decreased. With distributed processors controlling, the system works like a software or network radio, so different standards can coexist, and the system capacity can be increased by coprocessing of signals to and from multiple antennas.

In distributed wireless networks, the present cellular structure is removed and cells are substituted by virtual cell. Unlike traditional cell that is base-station-centered, a virtual cell is user-centered. In other words, the virtual cell is a set of distributed antennas that are within reach of a certain user. Each user has its own virtual cell, and it changes as the user moves or the environment changes. The processing layer selects a virtual cell for each user dynamically, and detects and optimizes for transmission jointly with the virtual cell.

In [24], the main features and advantages of distributed wireless networks are concluded as follows:

- Three distributed layers: Distributed antennas, distributed signal processing, and distributed high-layer control.
- No fast handoff problem: The virtual cell changes dynamically with the movement of the user, so no handoff is needed.
- Large capacity: With distributed antennas and distributed processing, the problem of increased interference in traditional cellular systems is overcome.
- Much lower power consumption: The transmission power can be greatly reduced.
- Seamless coverage: The antenna terminal is so cheap that the density of antennas can be very high.
- Suitable for nonuniformly distributed traffic: Simply by adjusting the density of antennas.
- Open structure: Existing and future standards and techniques can be realized on the platform of distributed wireless networks, and the resources of the wired system can be utilized sufficiently.
- Flexibility: The concept of software radio enables distributed wireless networks to accommodate different standards without hardware modification.

- Extendibility: The opened structure ensures that redeveloping and extension can easily be achieved on the same platform.
- Scalability: The scale of distributed wireless networks (including the number of antennas and processors) can be configured freely so that the cost of system devices can be minimized.

2.2 Cognitive Radio and Dynamic Spectrum Access

2.2.1 Cognitive Radio

Cognitive Radio (CR) was formally introduced to the radio community in 1999 by Joseph Mitola and Gerald Q. Maguire, Jr. in [13] as an extension of an SDR, which served to improve the overall performance of the radio in relation to its interaction with the spectrum using a cognition cycle, as shown in Figure 2.1. In [26], Mitola describes that a CR "is a goal-driven framework in which the radio autonomously observes the radio environment, infers context, assesses alternatives, generates plans, supervises multimedia services, and learns from its mistakes." While other definitions have been developed from research groups across the SDR community, the two components that are most often considered core features of the CR involve awareness of the RF environment and adaptation and/or learning algorithms to improve the performance of the radio.

A *Cognitive Radio* (CR) is an *Software Defined Radio* that additionally senses its environment, tracks changes, and reacts upon its findings. A CR is an autonomous unit in a communications environment that frequently exchanges information with the networks it is able to access as well as with other CRs. From our point of view, a CR is a refined SDR [27].

2.2.2 Why Dynamic Spectrum Access?

Today's wireless networks are regulated by a fixed spectrum assignment policy, *i.e.* the spectrum is regulated by governmental agencies and is assigned to license holders or services on a long term basis for large geographical regions. Although the fixed spectrum assignment

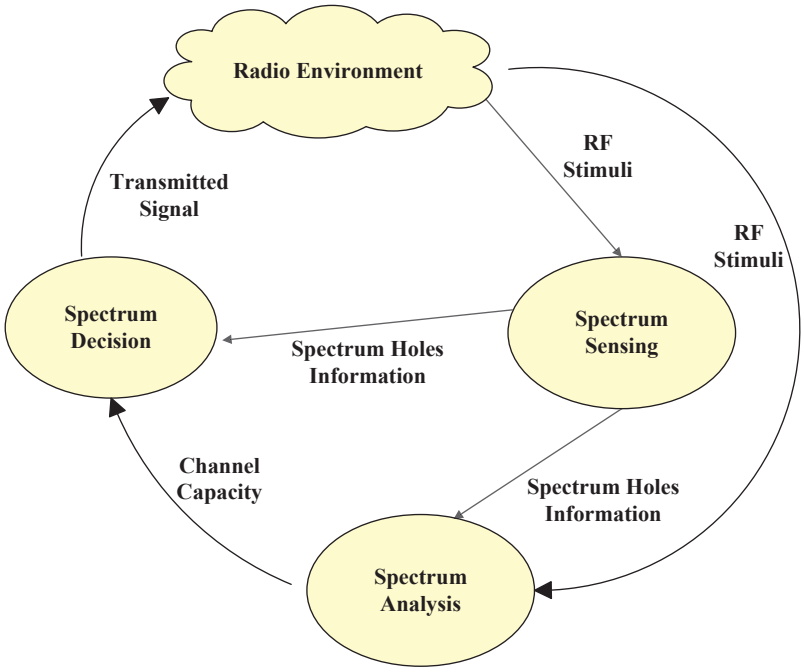


Figure 2.1: Cognitive cycle.(from [1])

policy has generally worked well in the past, there is a dramatic increase in the access to the limited spectrum for mobile services in recent years. Consequently, this increase is straining the effectiveness of the traditional spectrum policies [28].

It is commonly believed that there is a crisis of spectrum availability at frequencies that can be economically used for wireless communications. This misconception is strengthened by a look at the FCC frequency chart [29], which shows multiple allocations over all of the frequency bands; which is a situation essentially also true worldwide. This has resulted in fierce competition for use of spectra, especially in the bands below 3 GHz. On the other hand, a large portion of the assigned spectrum is used sporadically as illustrated in Figure 2.2, where the signal strength distribution over a large portion of the wireless spectrum is shown. The spectrum usage is concentrated on certain portions of the spectrum while a significant amount of the spectrum remains unutilized. This appears to be a contradiction to the concern of spectrum shortage since in fact we have an abundant amount of spectrum, and the spectrum shortage is partially an artifact of the regulatory and licensing process.

It is this discrepancy between FCC allocations and actual usage, which indicates that a

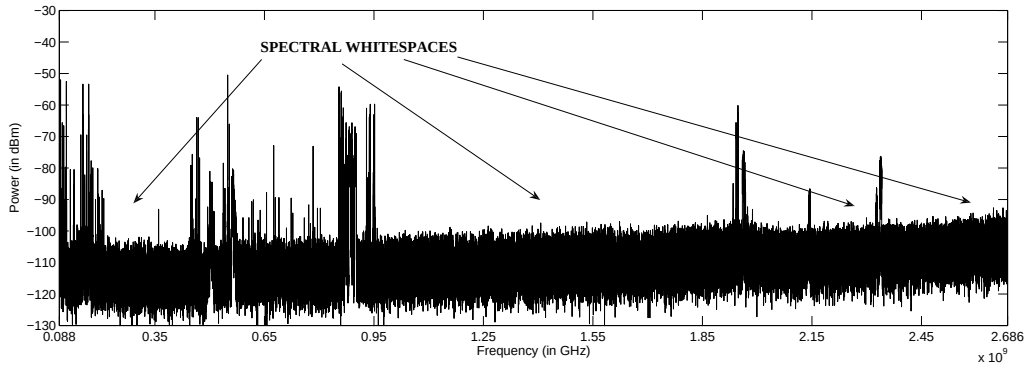


Figure 2.2: A snapshot of PSD from 88 MHz to 2686 MHz measured on July 11, 2008, in Worcester, Massachusetts (42°16′8″N, 71°48′14″W) (from [2]).

new approach to spectrum licensing is needed. This approach should provide the incentives and efficiency of unlicensed usage to other spectral bands, while accommodating the present users who have higher priority or legacy rights (*primary users*) and enabling future systems a more flexible spectrum access [30]. This new approach is called *dynamic spectrum access*.

2.2.3 What is Dynamic Spectrum Access?

Dynamic spectrum access is the process of increasing spectrum efficiency via the real-time adjustment of radio resources, *i.e.* via a process of local spectrum sensing, probing, and the autonomous establishment of local wireless connections among cognitive nodes and networks. As originally proposed in [26], cognitive radio envisioned real time spectrum auctions among diverse constituencies, using for one purpose, such as cellular radio, spectrum allocated and in use for another purpose such as public safety, and conversely, in order to multiply both the number of radio access points for public safety and to more efficiency use public safety spectrum commercially during peak periods. Although that initial example has yet to be fully realized, the US FCC encouraged the application of that technology to the secondary use of underutilized television spectrum, such as in ad hoc, short range wireless local area network (WLAN) in spectrum that is allocated to another primary purpose such as broadcast television. In addition, the principles of cognitive radio for dynamic spectrum also apply to enhance the efficiency of use within and across each "lane in the road," such as via the intelligent selection among multiple alternative PHY-MAC layers (alternative lanes

in the spectrum road) by cognition across network, transport, and application layers of the protocol stack [31].

FCC endorsement of cognitive radio in secondary markets in the USA offered opportunities for improved spectrum utilization. In addition, the National Institute of Information and Communications Technology (NICT) Yokosuka, Japan have for characterized SDR and cognitive radio from technical [32, 33] and regulatory [34] perspectives. Ofcom, the regulatory body of the UK remains appropriately skeptical of the economics of dynamic spectrum [35]. On the other hand, the Commission for Communications Regulation (COMREG), Ireland, imposes constraints [36] but also encourages innovation such as by allocating over 100 MHz of spectrum for experiments and demonstrations during IEEE DySPAN 2007 in Dublin. Guatemala [37] employs Titulos de Usurfrucato de Frecuencias (TUF), specifying spectrum use parameters in great detail, which establishes a strong reference point for the liberalization of spectrum allocation towards dynamics [38]. In Europe, countries including Austria, Sweden, and the UK apparently have sanctioned de facto transfers of spectrum rights among spectrum licensees, while a recent EU Framework Directive empowers all EC countries to introduce secondary trading of spectrum usage rights [39].

2.2.4 Dynamic Spectrum Access Models

Standing for the opposite of the current static spectrum management policy, the term dynamic spectrum access has broad connotations that encompass various approaches to spectrum reform. The diverse ideas presented at the first IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN) suggest the extent of this term. As illustrated in Figure 2.3, dynamic spectrum access strategies can be broadly categorized under three models [3].

Dynamic Exclusive Use Model

This model maintains the basic structure of the current spectrum regulation policy: Spectrum bands are licensed to services for exclusive use. The main idea is to introduce flexibility to improve spectrum efficiency. Two approaches have been proposed under this model: Spectrum property rights and dynamic spectrum allocation. The former approach

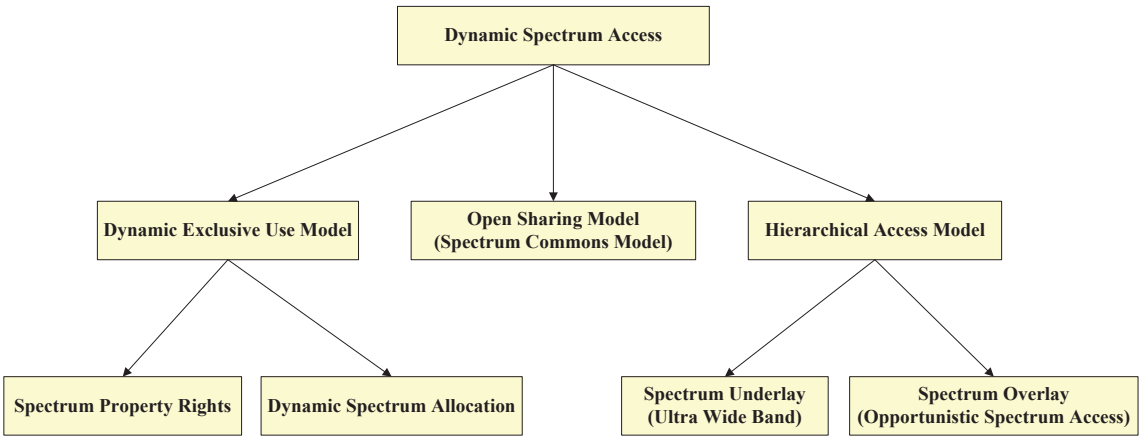


Figure 2.3: Three models of dynamic spectrum access strategies. (from [3])

allows licensees to sell and trade spectrum and to freely choose technology. Economy and market will thus play a more important role in driving toward the most profitable use of this limited resource. Note that even though licensees have the right to lease or share the spectrum for profit, such sharing is not mandated by the regulation policy.

The second approach, dynamic spectrum allocation, was brought forth by the European DRiVE project. It aims to improve spectrum efficiency through dynamic specturm assignment by exploiting the spatial and temporal traffic statistics of different services. In other words, in a given region and at a given time, spectrum is allocated to services for exclusive use. This allocation, however, varies at a much faster scale than the current policy.

Based on an exclusive use model, these approaches cannot eliminate white space in spectrum resulting from the bursty nature of wireless traffic.

Open Sharing Model

Also referred to as spectrum commons, this model employs open sharing among peer users as the basis for managing a spectral region. Advocates of this model draw support from the phenomenal success of wireless services operating in the unlicensed industrial, scientific, and medical (ISM) radio band (e.g., WiFi). Centralized and distributed spectrum sharing strategies have been initially investigated to address technological challenges under this spectrum management model.

Hierarchical Access Model

This model adopts a hierarchical access structure with primary and secondary users. The basic idea is to open licensed spectrum to secondary users while limiting the interference perceived by primary users (licensees). Two approaches to spectrum sharing between primary and secondary users have been considered: Spectrum underlay and spectrum overlay.

The underlay approach imposes severe constraints on the transmission power of secondary users so that they operate below the noise floor of primary users. By spreading transmitted signals over a wide frequency band (UWB), secondary users can potentially achieve short-range high data rate with extremely low transmission power. Based on a worst-case assumption that primary users transmit all the time, this approach does not rely on detection and exploitation of spectrum white space.

Spectrum overlay was first envisioned by Mitola under the term spectrum pooling and then investigated by the DARPA Next Generation (XG) program under the term opportunistic spectrum access. Differing from spectrum underlay, this approach does not necessarily impose severe restrictions on the transmission power of secondary users, but rather on when and where they may transmit. It directly targets at spatial and temporal spectrum white space by allowing secondary users to identify and exploit local and instantaneous spectrum availability in a nonintrusive manner.

Compared to the dynamic exclusive use and open sharing models, this hierarchical model is perhaps the most compatible with the current spectrum management policies and legacy wireless systems. Furthermore, the underlay and overlay approaches can be employed simultaneously to further improve spectrum efficiency.

2.3 Spectrum Rendezvous Protocols

Dynamic spectrum access (DSA) technology offers a solution to the current spectrum usage inefficiencies based on the ability to dynamically adapt operating frequencies and bandwidths to occupy spectrum white spaces. A number of significant challenges must be overcome before this solution can be realized. One of these key challenges is that of

frequency rendezvous. In traditional wireless communications networks, devices typically have a priori knowledge of the initial operating frequencies to be used. This means that upon commencing operation, nodes within the network may have a predetermined frequency, or list of frequencies which can searched in an attempt to established a wireless communications link with their peers. In a DSA network, the frequency of operation may not be known initially; establishing a common communications channel may be dependent on the available spectrum (*i.e.*, white space spectrum). The potential channel may therefore lie within a much greater frequency range and may also change during the operating lifetime of the network.

In addition, recent years have seen the untimely failure of first responder communication systems during disaster scenarios when they are most needed. These systems have failed due to a loss of critical infrastructure, incompatibility between the communication systems of responding agencies, inability to scale to meet the capacity demands of the crisis, and in some instances, difficulty in usability in the heat of the moment. As many researchers have noted, software defined radio (SDR), cognitive radio (CR), and dynamic spectrum access (DSA) are technologies especially suited to overcoming these problems [40].

Spectrum rendezvous is a critical step in bootstrapping a network. Since infrastructure is often lost or overwhelmed during a disaster scenario, the spectrum rendezvous should proceed unaided from any centralized coordination. Furthermore, it should exhibit a high probability of rendezvous, provided communication resources are within radio range. Finally, it should minimize the risk of interference with ongoing communications, as normal collaborative spectrum sensing is not practically accomplished until an initial link is established.

2.3.1 Approaches to Rendezvous

The process of rendezvous, also commonly referred to as neighbor discovery, has been the topic of a number of recent papers. In [41], McGlynn presents a set of neighbor discovery protocols which he calls "birthday protocols," coined after the probability of two or more people in a room having the same birthday. He describes a scenario where nodes and their link topology are static, as would be the case in a sensor network dispersed randomly

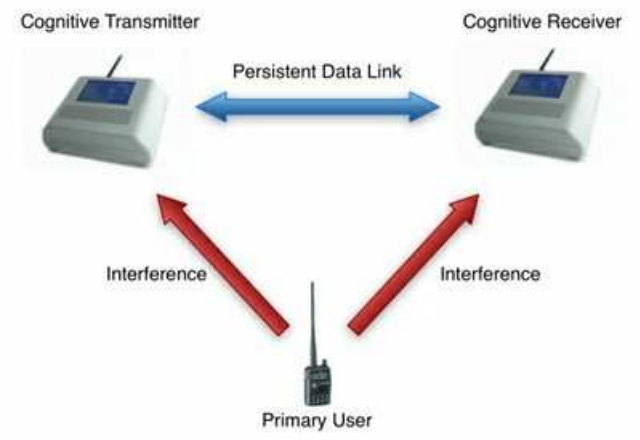


Figure 2.4: Schematic of a DSA network. Note that whenever the primary user transmits on a channel the cognitive network is occupying, the cognitive users rendezvous on another open primary channel to continue their communication.

throughout a region. Nodes are assumed to be in one of three statestransit, receive, or sleepin a given time slot, with fixed probabilities. He computes the fraction of the expected number of links that can be formed as a function of the number of nodes present, the number of time slots waited, and their state probabilities. Energy efficiency is obtained by varying the probability at which nodes sleep. This work forms a foundation for rendezvous analysis, but it is limited in that it assumes a single broadcast channel for rendezvous, and it assumes that time slots are fixed and synchronized across all nodes in the neighborhood.

We can broadly classify rendezvous mechanisms into *aided* (or infrastructure-based) and *unaided* (infrastructure-less).

Aided Rendezvous

Aided rendezvous is accomplished with help from a server, which periodically broadcasts information regarding available channels and may even serve as a clearinghouse for link establishment and the scheduling of transmissions, typically using a well-known control channel, where each transmitter can propagate information about which channel it is using.

For example, [14] introduces an aided rendezvous mechanism. It proposes an architecture in which some frequencies are set aside for use as spectrum information channels. Clients dedicate a wireless interface to scan these channels, where the base stations broad-

cast information regarding spectrum availability, interference conditions, etc. Clients can use those same control channels to request the use of dedicated spectrum to their traffic (or, alternatively, clients may directly proceed to the data channels that they now know to be available).

The rendezvous problem in the centralized CR network is addressed in [42]. In general, the spectrum environment in the CR network is highly dynamic. To establish the communication channel between BS and CR node, one has to manage the spectrum holes in an efficient manner. The authors propose a new channel classification method, which is more suitable for the volatile spectrum environment than conventional IEEE 802.22 method. They classify the spectrum environment into 4 cases as follows:

- Case 1: both up and down control channels available
- Case 2: up control channel unavailable, down control channel available
- Case 3: up control channel available, down control channel unavailable
- Case 4: neither up nor down channel available

The resource-aware rendezvous algorithm is proposed to enhance the performance of rendezvous algorithm. Unlike the conventional rendezvous algorithm as in IEEE 802.22, the proposed rendezvous algorithm can establish the down and up control channel by taking advantage of relay function in CR node. It is shown that the both down and up control channels can be acquired even both down or up channels cannot find the spectrum holes that are directly allocated. With proposed rendezvous algorithm, the CR network can runs in a stable condition in the dynamic spectrum environment.

Unaided Rendezvous

In aided rendezvous mechanism, the frequency of the dedicated control channel has to be known a priori by each radio connecting to the network, which generally means it is fixed. It also represents a single point of failure for the whole network and has scalability issues. A better and more flexible solution is to establish rendezvous without a control channel, which is known as unaided rendezvous.

In unaided rendezvous, each cognitive radio must find other nodes in the network on its own. Unaided rendezvous may also avail itself of a dedicated control channel, which all radios visit periodically to bootstrap their connectivity to other nodes in the network, or to set up links in new channels. There are two examples in this category:

First, Link Rendezvous Protocol for Cognitive Radio Networks. Dedicated channels are not needed in DSA based cognitive radio networks. CR networks can be designed so that nodes rendezvous with each other based upon the sensed spectral environment provided that the application can withstand some level of delay in initial network setup. This process is known as Link Rendezvous.

[15] proposes an approach to establish the first connection with a minimum risk of interference. A complete link rendezvous algorithm is described in this paper. This protocol relies on frequency domain decision statistics. Nodes wishing to join the network are emitting and scanning for a simple carrier with a small number of side tones. To validate this approach, the authors describe a series of experiments using the GNU Radio software defined radio toolkit.

This approach avoids a dedicated signaling channel, only requiring radios to operate within a common band. The concept tries to minimize unintentional interference during the rendezvous process by using a very short duration, narrow bandwidth, low power attention signal. The responding nodes begin coordinating the spectrum sensing by responding to the attention signal on a frequency which it interprets as being clear.

Second, Sequence-based Rendezvous for Dynamic Spectrum Access. In decentralized networks, each radio visiting potential channels in random fashion is called blind random rendezvous. In contrast to random rendezvous, [16] proposes the use of sequences that dictate the order in which two radios will visit a set of N channels of interest when attempting to rendezvous with each other. Through sequence-based rendezvous, it is possible to:

1. establish an upper bound to the time to rendezvous (TTR)
2. establish a priority order for channels in which rendezvous occurs
3. reduce the expected TTR as compared to random rendezvous

This paper derives a closed-form expression for expected time to rendezvous using sequences and show that it has an upper bound. The authors also derive expressions for the probability that rendezvous occurs in the best and worst channels, as well as the conditional expectation of TTR given that rendezvous occurs in each of those channels.

One limitation of this model is that it assumes CR nodes must be synchronized and rendezvous slots aligned in time.

2.3.2 Rendezvous Research Deficiencies

Reviewing related works in Section 2.3.1 highlights three areas in rendezvous protocol development which need additional research.

First, the foundational papers on rendezvous, such as McGlynn, focused only on the single channel instance. This highlights the need for more multi-channel analysis, particularly since most real world systems like Bluetooth, as well as upcoming cognitive radio systems, require operation on multiple channels.

Second, the large majority of rendezvous algorithms currently available require at least some degree of time synchronization between the nodes in the networks. In our opinion, this is a tenuous assumption that may be difficult or impossible to achieve in real systems. This is further evidenced by the fact that one of best well known and successful wireless networking systems, Bluetooth, is asynchronous.

Third, relatively few systems have analyzed or experimentally tested varying-width rendezvous slots. Most assume fixed slots of equal length, with the exception of Bluetooth.

2.4 Network Coding for Wormhole Detection

Several reasons lead us to choose wormhole attacks as the primary research topic for this investigation. First, wormhole attacks impose severe threats to the correct detection of the network topology, which is the foundation of various operations within wireless networks such as routing and data transmission. Second, a wormhole attack is a representation of stealth attacks on wireless networks, where traditional methods such as encryption and authentication cannot defend against such attacks. Therefore, a detection method based

on physical layer network coding will allow us to better understand this problem. Finally, previous approaches for detecting wormhole attacks are usually implemented at the network layer. Our proposed approach uses physical layer properties. At the same time, our approach does not require time synchronization among wireless nodes or depend on any special hardware.

2.4.1 Wormhole Detection

Location and Time Based Solutions This group of solutions try to restrict the transmission range of a packet by measuring the time and/or positions of the wireless nodes. For example, packet leash is proposed by Hu *et al.* [43] for wormhole prevention. The geographic leashes and temporal leashes use location information and signal propagation delay respectively to verify a neighbor relation. In SECTOR [44], the wireless nodes use a special hardware to respond to a one-bit challenge. The challenger measures the round trip time to estimate the distance between the nodes. Using directional antenna [45], the neighbor relation between two nodes can be verified based on the directions of the received signals. In LiteWorp [46], the wireless nodes use the short safe period after deployment to detect the real 1-hop and 2-hop neighbors. They will then monitor the packet forwarding actions to detect wormholes. The improved approach [47] for wormhole detection in mobile wireless networks requires the nodes to have GPS and loosely synchronized clocks. The EDWA [48] method also requires the wireless nodes to be equipped with GPS. In TrueLink [49], the wireless nodes strictly follow the 802.11 standard of the time interval between packets to restrict their transmission distances. It requires the wireless nodes to have very accurate clocks.

Graph Based Approaches Investigators have tried to detect wormholes based on their impacts on the network topology. MDS-VoW [50] is a centralized mechanism for wormhole detection in sensor networks. It reconstructs the layout of sensors using multi-dimensional scaling and detects wormholes by visualizing the anomalies introduced by the attacks. A decentralized approach for dynamic networks is proposed in [51]. In [52], the researchers analyze the geometric random graphs induced by the communication range constraint of

the nodes. They present a defense mechanism based on local broadcast keys. Maheshwari *et al.* [53] model the wormhole detection problem as a disk graph embedding task. They design a localized algorithm to locate the forbidden substructures in the connectivity graph.

Statistical Analysis Methods In [54], the investigators study the impacts of wormholes on multi-path routing protocols. They try to locate the hot links that are contained in a majority of the obtained routes. In NNT and ADT [55], the researchers try to detect increases in the node degrees and decreases in the shortest paths caused by the wormholes.

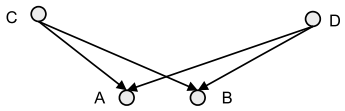
2.4.2 Physical Layer Network Coding

Physical layer network coding (PNC) tries to turn the broadcast property of wireless networks to a capacity boosting advantage. It uses the additive nature of the electromagnetic waves to serve as the coding procedure. The PNC technique under QPSK modulation is studied in [18]. The researchers investigate the general modulation-demodulation principles and analyze the performance penalty of different factors. In [17], the authors try to decode the interfered signals under MSK modulation. The mechanism can recover the colliding sequences under phase shift and the lack of synchronization. After these pioneering papers, research on PNC focuses on improving the decoding accuracy. In [56], the authors compare the amplify-and-forward and decode-and-forward techniques. Zhang *et al.* investigate the decoding techniques of PNC over finite and infinite fields in [57]. In [58], the authors propose to dynamically adjust the coefficients to increase the 'distances' among different codes. Investigators also proposed to adopt Tomlinson-Harashima precoding to improve the data recovery accuracy [59]. The determination of threshold values for decoding in two-way relay channels is studied in [60].

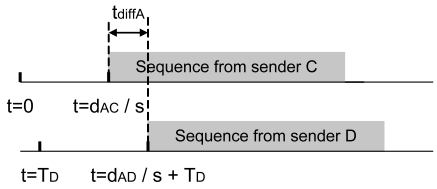
2.4.3 The Basic Idea

In this part, we introduce the basic idea of using physical layer network coding to detect wormhole attacks. We assume that two wireless nodes are neighbors if and only if the distance between them is shorter than r. However, this assumption does not restrict wireless nodes from transmitting signals at a higher power level in order to reach a longer

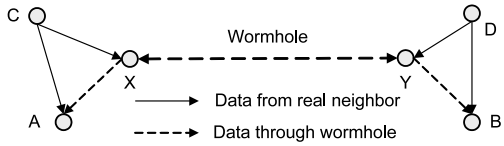
distance. We assume the attackers are not capable of compromising any wireless nodes within the network. However, they can deploy their own nodes to eavesdrop on the traffic, tunnel the packets, and retransmit the data. In the following analysis, we use d_{MN} to represent the physical distance between two nodes M and N. We use T to represent a specific moment and t to represent a time duration. If the radio signal propagates at the speed of light s, the transmission delay between two nodes M and N will be $\frac{d_{MN}}{s}$. In the following analysis, we describe the time difference between the received sequences. We are not using the system clocks to directly measure the actual time. On the contrary, we can pinpoint the starting bit in the sequence that the collision starts. Then we can translate this information into a time difference. This topic is discussed further in Section 4.3.1.



(a) Sequences from C and D collide at A and B.



(b) t_{diffA}: difference b/w arriving time of two sequences at A.



(c) Two colliding sequences are tunneled through the wormhole.

Figure 2.5: Two colliding sequences and the impacts of the wormhole.

Figure 2.5.(a) illustrates an example of using physical layer network coding to verify the neighbor relationship. We assume that nodes A and B in the network can hear each other and they want to verify the neighbor relationship. They jointly choose two other nodes, C and D, in the network that can both hear from. C and D will then generate and send out long random sequences that will collide at A and B. Without losing generality, we assume that node C will send out its sequence first. We assume that C starts sending at $T_C = 0$

and D starts sending at $T_D \geq 0$.

Based on these assumptions, we can derive that A will receive the signals from C at the time $\frac{d_{AC}}{s}$, and the signals from D at $(T_D + \frac{d_{AD}}{s})$. Therefore, the difference between the arriving time of the two sequences at node A is $t_{diffA} = (T_D + \frac{d_{AD}-d_{AC}}{s})$, as illustrated in Figure 2.5.(b). In other words, A will first receive the sequence from C for t_{diffA} seconds, then the two sequences will collide at the node. If $t_{diffA} < 0$, the sequence from D will arrive first at A. Similarly, we can derive the difference between the arriving time at node B as $t_{diffB} = (T_D + \frac{d_{BD}-d_{BC}}{s})$.

Now let us look at the difference between t_{diffA} and t_{diffB}:

$$\begin{aligned} & t_{diffB} - t_{diffA} \\ = \; & (T_D + \frac{d_{BD} - d_{BC}}{s}) - (T_D + \frac{d_{AD} - d_{AC}}{s}) \\ = \; & \frac{(d_{BD} - d_{AD}) + (d_{AC} - d_{BC})}{s} \end{aligned} \tag{2.1}$$

For the three nodes A, B, and D, they either form a triangle or stay on the same line. Either way, we must have $||(d_{BD} - d_{AD})|| \leq ||d_{AB}||$. Similarly, we have $||(d_{AC} - d_{BC})|| \leq ||d_{AB}||$. Therefore, we must have:

$$\begin{aligned} & ||(t_{diffB} - t_{diffA})|| \\ = \; & \frac{||(d_{BD} - d_{AD}) + (d_{AC} - d_{BC})||}{s} \\ \leq \; & \frac{||d_{BD} - d_{AD}||}{s} + \frac{||d_{AC} - d_{BC}||}{s} \\ \leq \; & \frac{||d_{AB}||}{s} + \frac{||d_{AB}||}{s} \\ = \; & \frac{2 \times d_{AB}}{s} \leq \frac{2r}{s} \end{aligned} \tag{2.2}$$

The last part of the equation holds since when A and B are real neighbors, the distance between them is smaller than or equal to r. From Equation (2.2), we can see that the difference between t_{diffA} and t_{diffB} is restricted by the physical distance between nodes A and B. In this way, the two nodes can compare the time differences between the received colliding sequences to verify their neighbor relationship.

Below we will study the case when A and B are not real neighbors and they have to communicate through a wormhole. Here we adopt a simplified model of attackers and

assume that the two attackers X and Y can send and receive radio signals at the same time. More realistic scenarios will be discussed in Section 4.1. Since the malicious nodes possess total control over the tunneling procedure, in the following analysis we assume that X and Y will introduce extra delay $t_{\overrightarrow{XY}}$ and $t_{\overrightarrow{YX}}$ for the traffic transmitted in different directions. This scenario is illustrated in Figure 2.5.(c).

Following the previous assumptions, we can derive that A will receive the sequence from C at time $\frac{d_{AC}}{s}$, and the sequence from D at time $(T_D + \frac{d_{DY}+d_{XY}+d_{AX}}{s} + t_{\overrightarrow{YX}})$. Similarly, B will receive the sequence from C at time $(t_{\overrightarrow{XY}} + \frac{d_{CX}+d_{XY}+d_{BY}}{s})$, and the sequence from D at time $(T_D + \frac{d_{BD}}{s})$. Therefore, we have:

$$t_{diffA} - t_{diffB} = t_{\overrightarrow{XY}} + t_{\overrightarrow{YX}} + \frac{(d_{DY} + d_{BY} - d_{BD})}{s} + \frac{(d_{AX} + d_{CX} - d_{AC})}{s} + 2 \times \frac{d_{XY}}{s} \quad (2.3)$$

Since the three nodes A, C, and X either form a triangle or are on the same line, we must have $(d_{AX} + d_{CX} - d_{AC}) \geq 0$. Similarly, we have $(d_{DY} + d_{BY} - d_{BD}) \geq 0$. The extra transmission delay $t_{\overrightarrow{XY}}$ and $t_{\overrightarrow{YX}}$ introduced by the malicious nodes cannot be smaller than 0. Therefore, we have:

$$||t_{diffA} - t_{diffB}|| \geq (2 \times \frac{d_{XY}}{s}) \quad (2.4)$$

When the length of the wormhole d_{XY} is longer than the radio transmission range r, we have $||t_{diffA} - t_{diffB}|| > \frac{2r}{s}$. Combining the results in Equations (2.2) and (2.4), we find that two nodes in the wireless network can verify their neighbor relationship by comparing the differences between the starting points of collision in the received sequences.

The proposed approach has several highly desirable properties. First, since the mechanism uses only the starting points of the collision between the sequences to detect wormholes, we do not need the senders or receivers to synchronize their clocks. As illustrated in Equations (2.2) and (2.4), the parameter T_D has been canceled out. Second, in Equation (2.2) the physical distances between the senders and the receivers have also been canceled out. The difference is determined only by the physical distance between the nodes that want to verify their neighbor relationship. This implies that we can choose the senders from a larger area in the network, and they do not need to be direct neighbors of A and B. Third, the proposed mechanism does not require the wireless nodes to be equipped with any special hardware which will result in a lower node cost. The capabilities of the nodes to recover

colliding sequences will be discussed in Section 4.2. Finally, the proposed approach works in a distributed manner and does not require a centralized controller. Nodes A and B can determine their senders and exchange t_{diffA} and t_{diffB} to detect wormholes. With these desirable properties, the approach can be easily adopted by existing networks.

2.5 Summary

In this chapter, the background of distributed wireless networks, cognitive radio (*i.e.* an SDR), and how it relates to a dynamic spectum access network has been discussed. An overview of related work in the area of spectrum rendezvous and network coding has been presented. In particular, we introduce the basic idea of the detection mechanism and the role of physical layer network coding in wormhole detection.

Chapter 3

Proposed Link Rendezvous Framework for Dynamic Spectrum Access Network[1]

In this chapter, we propose an analysis of frequency rendezvous techniques employing three different scanning rules by combining analytical results with computer simulations. Our approach is designed to be operated in a purely decentralized wireless networking environment, where no centralized control is present and the spectrum does not possess pre-defined channels. This is accomplished via a combination of receiver pilot tones, a tone scanning protocol, and transmitter/receiver handshaking process. In order to realize a shortest search time for the target receiver, an efficient scanning rule should be employed. In this chapter, three scanning rules, namely: frequency sequence scanning, pilot tone strength scanning, and cluster scanning, are analyzed using mathematical derivations. To validate our theoretical result, we test the three scanning rules with computer simulations.

[1]This chapter is partially based on the work presented in [21] and [22].

3.1 Frequency Rendezvous Framework

The network framework proposed in [21] that is employed in this work operates as follows: There are N radios in the network and each of them has multiple transceivers. One radio is designated as the transmitter, which we refer to as TX_1. The other radios are all defined as receivers, namely RX_1, RX_2, $\cdots$, and RX_{N-1}. All radios within the vicinity are transmitting their own unmodulated pilot tones at different center frequencies in order to signal their frequency locations to other wireless nodes, *i.e.*, the pilot tones serve as beacons to a potential transmitter. There is no centralized control in this network. Thus, the transmitter is responsible for locating a target receiver and sending data to it. In order to realize this function, the following frequency rendezvous algorithm is employed.

3.1.1 Frequency Rendezvous Algorithm

Without loss in generality, our algorithm assumes a single transmitter, and potentially multiple receivers within transmission range. Based on a *priori* determination about frequency occupancy and a temporary transmission frequency assignment, all of the receivers and the transmitter are broadcasting pilot tones at unoccupied frequencies within a wireless spectral range designated for DSA. Besides, these frequencies are selected completely randomly. In our proposed framework, the downlink channel is at a frequency just below the pilot tone while the uplink channel is at a frequency just above the pilot tone. The transmitter attempts to find one or several target receivers to form a network and exchange data, but it does not know at which frequencies these receivers are located.

Figure 3.1 provides a flow diagram of the frequency rendezvous algorithm used in this work. First of all, since the center frequencies of all the receivers are completely unknown to the transmitter, the algorithm is initialized by having the transmitter sweep the wireless spectrum in order to determine the frequency locations of pilot tones corresponding to potential receivers. The transmitter searches for the target receivers across a frequency band of interest. Frequency locations of all active receivers are denoted by a pilot tone per device. Consequently, the transmitter proceeds to poll each receiver by looking into the

identified pilot tones[2].

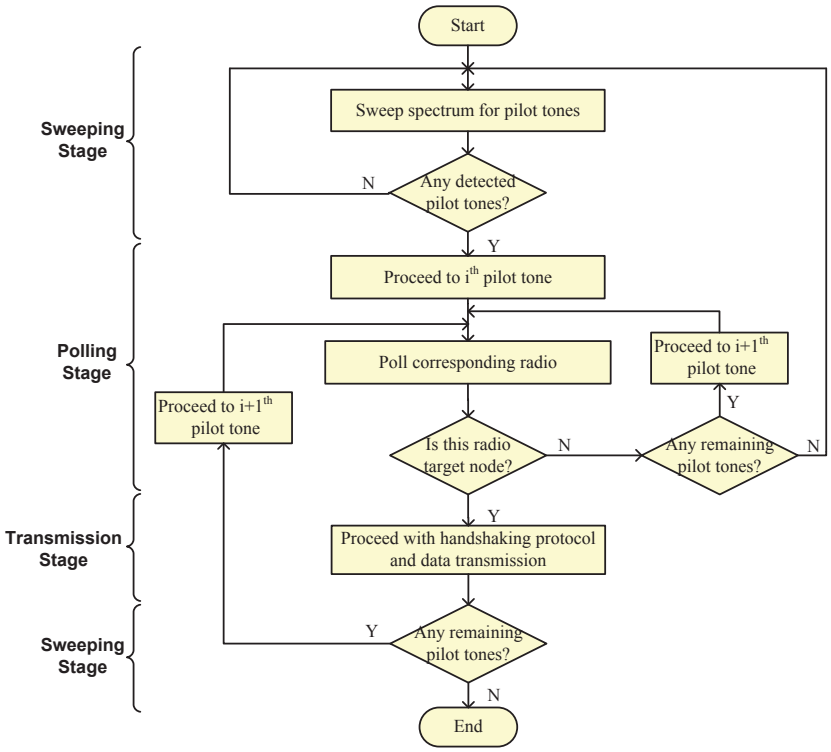


Figure 3.1: Frequency rendezvous algorithm employing pilot tones, which enables several radios to meet and establish a link on a common channel.

Once a pilot tone has been identified, the transmitter begins its attempt to connect to the receiver associated with the detected pilot tone and establish a network connection. Figure 3.2 describes the process of rendezvous between the transmitter and the target receiver. To start with, the transmitter broadcasts its own pilot tone towards the detected receiver for T seconds. Since this protocol is used in DSA network, it means there exist the primary users. At the initial state of frequency rendezvous, the transmitter does not have much knowledge about the real condition of the network, so its unmodulated pilot tone needs to be low power and short in duration in order to minimize unintentional interference with primary users, which is referred to as polling pattern. Meanwhile, all the receivers are periodically

[2]Unlike a wired network where frames can flow to every station, in a wireless LAN environment it is possible for obstructions to hide one station to be communicating with another while a third station listens to the channel and, thinking it is available, begins to transmit. This is referred to as the *hidden node problem* [61].

monitoring their adjacent spectrum for this polling pattern. When a particular receiver is exposed to this pattern, it will send out a signal in response. Upon receiving this signal, the transmitter will make a decision based on its knowledge about the spectrum occupancy and the signal strength of the incoming signal, along with other channel statistics it may have gathered. If the responding node is considered as a target radio, it will continue to the next communication step with the transmitter. Otherwise, the transmitter will leave this node and proceed to the next flagged pilot tone.

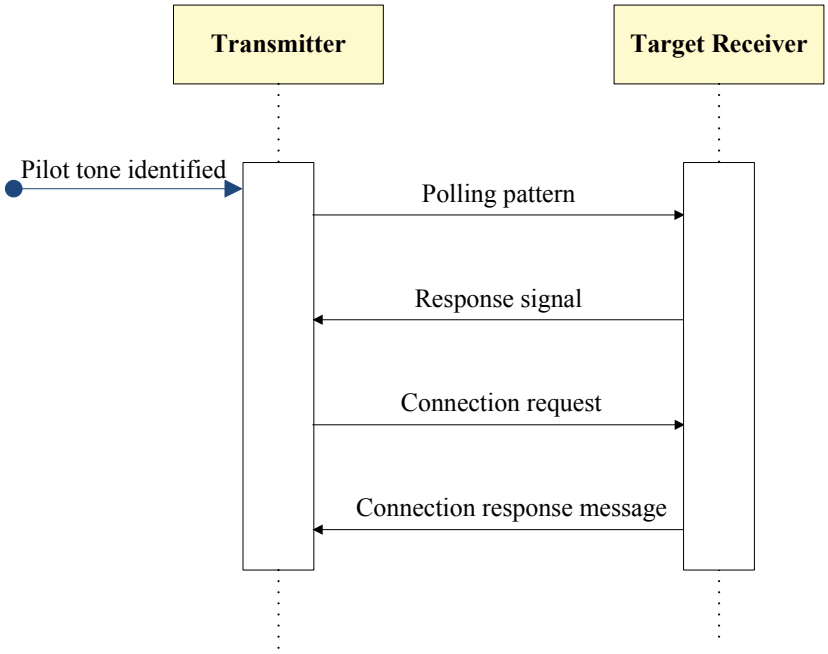


Figure 3.2: The process of rendezvous between the transmitter and the target receiver, which starts with transmitter broadcasting its polling pattern and ends with target receiver transmitting a connection response message directly to the transmitter.

When a target receiver radio is detected, the transmitter is finally ready to establish a connection, so it sends a connection request to the target receiver. At the same time, after transmitting the reply signal to the transmitter in the previous step, the idle receiver enters a listen mode for a connection request. Upon detecting a connection request, the receiver transmits a connection response message directly to the transmitter. This message is the first unicast message and can include information about the node such as the services it can provide and connection parameter preferences, which technically finishes the rendezvous

process. Since both the transmitter and receiver have already reserved a channel for data transmission beforehand, there will be no interference or congestion during this process. If there is no pilot tone available on the whole spectrum, the transmitter will sweep the spectrum again and repeat the process of searching for the potential target receivers.

Note that in this scheme, the network does not possess any form of centralized control. For example, the determination of which receivers can communicate with the transmitter and on which frequency the communications will take place are made dynamically based on the network situation. This is in contrast to wired networks in which routers perform the task of routing. It is also in contrast to managed (infrastructure) wireless networks, in which a special node known as a base station manages communication among other nodes.

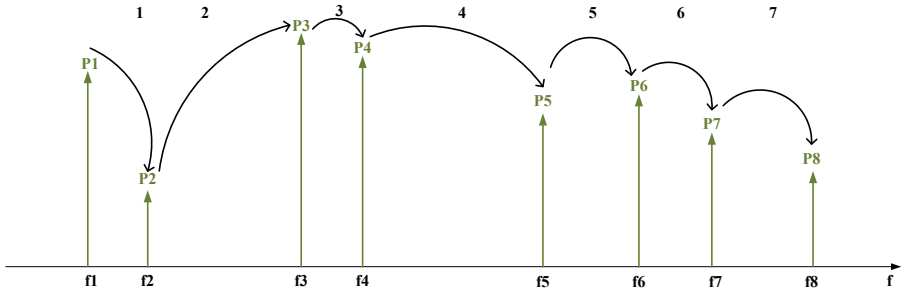
3.1.2 Frequency Scanning Rules

In the previous rendezvous algorithm, one important step for the transmitter is the detection of pilot tones. However, the order in which we scan and poll receivers may affect how long it takes to find the desired receiver. We propose three different scanning rules, that are used by the transmitter to decide the visiting order to all the detected pilot tones. These three scanning rules are:

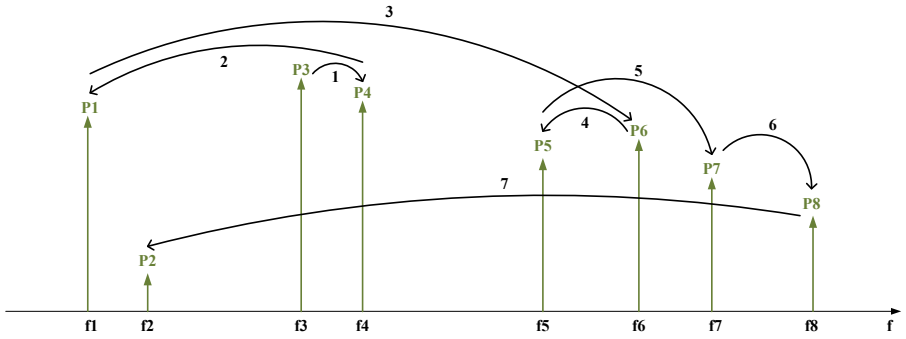
- *Frequency Sequence Scanning* The receiver who has a lowest center frequency will be scanned first, as shown in Figure 3.3(a). In this situation, the transmitter will visit the pilot tones in the order f_1, f_2, f_3, ..., f_8.

- *Pilot Tone Strength Scanning* The receiver which has the highest power from transmitter's viewpoint will be scanned first, as shown in Figure 3.3(b). In this situation, just taking these eight pilot tones into account, the transmitter will visit the them in the order f_3, f_4, f_1, f_6, f_5, f_7, f_8, f_2.

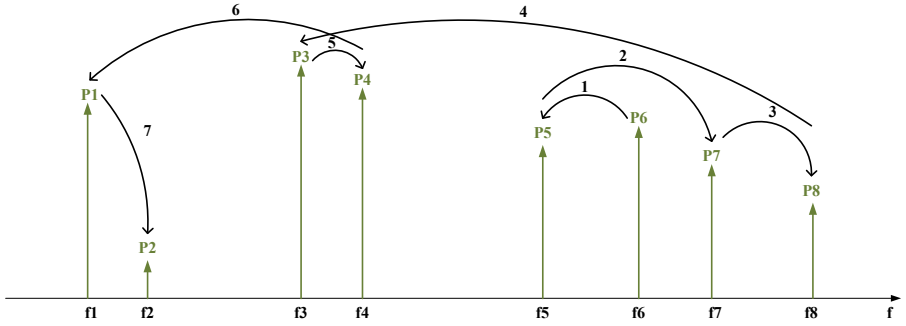
- *Cluster Scanning* The transmitter will first scan the populated receiver locations, as shown in Figure 3.3(c). In this situation, there are three clusters. f_1 and f_2 form the first cluster, f_3 and f_4 form the second one, while f_5 to f_8 form the third cluster, so the transmitter will first visit the cluster with the most number of receivers.



(a) Frequency sequence scanning rule.



(b) Pilot tone strength scanning rule.



(c) Cluster scanning rule.

Figure 3.3: Three proposed scanning rules. Suppose there are eight receivers with their detected pilot tones (f_1, f_2, f_3, ..., f_8), which are in frequency sequence. The pilot tones' amplitudes (P_1, P_2, P_3, ..., P_8) display the tones' strength.

Although we only analyze the situation of four receivers here, it is very straightforward to generalize to N receivers.

For a certain scenario and a certain number of receivers, the transmitter usually needs to poll k radios before it eventually find the target radio. The scanning time for one execution is proportional to this k. If we apply the same receiver distribution, *i.e.*, uniform or Gaussian, but generate N different frequencies, we can get a different scanning time. When repeating this process a large number of times, we can get a steady average scanning time for a certain number of receivers and therefore, define it as the metric for scanning rules.

Since we set the number of the receivers as a variable N, we can change this number and see how the scanning rules work when the number of receivers changes.

3.2 Mathematical Analysis

For the mathematical derivations in this section, we always assume that it does not take any time for the transmitter to move from one receiver to another. Consequently, scanning time only refers to the polling time the transmitter spends on the receivers and this polling time is considered to be the same for each receiver. For simplicity, we designate this polling time to be 1 for each receiver. The definition of the variables in this section are shown in Table 3.1.

3.2.1 Frequency Sequence Scanning

The receiver who has a lowest center frequency will be scanned first. Assume the desired receiver is the kth receiver, the transmitter needs to scan k receivers before it finally reaches the target. Based on *law of total expectation* [62], the average scanning time is:

$$E(X) = \sum_{i=1}^{M} X_i P(X = X_i) \tag{3.1}$$

where E$(\cdot)$ is the expectation of scanning time, and P$(\cdot)$ is the probability that the ith receiver is the target receiver.

Table 3.1: Definition of the variables in Section 3.2

Variable	Description
M	The total number of receivers
X	The random variable for scanning time
X_i	The actual scanning time when the target is the ith receiver*
P_i	The probability that the ith receiver will be scanned
p_i	The power of the ith receiver from transmitters viewpoint
p_{min}	The lowest power from transmitters viewpoint
N	The total number of clusters
Y_n	The number of receivers in the nth cluster
X_n	The actual scanning time when the target receiver appears in the nth cluster
P_n	The probability that the nth cluster will be scanned

* When doing mathematical analysis and computer simulations, our purpose is to compare the performance of three scanning rules, so we have to assume a target receiver in order to get quantitative results. This target receiver can be any receiver in the network (we use a random number i to express this target receiver here), so it is not a fixed and particular radio.

Since the target receiver is generated on a equal probability basis, we can express P(X=X_i) as:

$$P(X = X_i) = \frac{1}{M}, \quad i = 1, 2, 3, \ldots, M. \tag{3.2}$$

Therefore, using the formula of arithmetic series summation, we can expand the expression in Eq. (3.1) to be equal to:

$$E(X) = \frac{1}{M} \times \sum_{i=1}^{M} X_i = \frac{1}{M} \times \frac{(1+M) \times M}{2} = \frac{M+1}{2}. \tag{3.3}$$

From this result, it can be observed that the average scanning time for frequency sequence scanning rule does not depend on the distribution of center frequencies, and that it is located around $M/2$.

3.2.2 Pilot Tone Strength Scanning

As for the second scanning rule, the receiver which has the highest power from transmitters viewpoint will be scanned first. In this situation, we solve the problem from another

point of view.

Since the receiver with the highest power will be scanned first, we can come to the conclusion that the higher the power is, the larger probability it will be scanned. Actually, we can assume that the probability a receiver will be scanned is proportional to p_i–p_{min}. On the other hand, the total probability of all the receivers being scanned is 1 [62], namely:

$$\sum_{i=1}^{M} P_i = 1 \tag{3.4}$$

Hence, we can normalize the probability of each receiver to be scanned as:

$$P_i = \frac{p_i - p_{min}}{\sum_{i=1}^{M}(p_i - p_{min})}, \quad i = 1, 2, 3, \ldots, M. \tag{3.5}$$

As mentioned at the beginning of this section, we do not count the time for the transmitter to move from one receiver to another, so the layout of the receivers does not affect the scanning time. In order to do the calculation more intuitively, we can reorder the receivers according to their power amplitude. The receiver with the highest power will be labeled as the 1st receiver while the receiver with the lowest power will be labeled as the Mth receiver. Therefore, the scanning time is i if the ith receiver is the target, namely X_i=i.

Similar to the first scanning rule, based on *law of total expectation* [62], the average scanning time is:

$$\begin{aligned} E(X) &= \sum_{i=1}^{M} X_i P_i = \sum_{i=1}^{M} i \times \frac{p_i - p_{min}}{\sum_{i=1}^{M}(p_i - p_{min})} \\ &= \frac{\sum_{i=1}^{M} i \times (p_i - p_{min})}{\sum_{i=1}^{M}(p_i - p_{min})}. \end{aligned} \tag{3.6}$$

When there are a few receivers, which means the sample space for the random variable p_i is large enough, we can use the average power value $\overline{p}$ to approximate the random variable p_i. As a result, we can express Eq. (3.6) as:

$$E(X) = \frac{(1 + 2 + 3 + \cdots + M) \times (\overline{p} - p_{min})}{M \times (\overline{p} - p_{min})} = \frac{M + 1}{2} \tag{3.7}$$

From this result, we can see that the average scanning time for pilot tone strength scanning rule does not depend on the distribution of center frequencies either and is approximately around $M/2$.

3.2.3 Cluster Scanning

As for the third scanning rule, the transmitter will first scan the frequency locations of highest receiver density. Given a receiver distribution in Figure 3.3(c), the transmitter will scan the third cluster first, then either the first cluster or the second one, because they two have the same number of receivers.

In this part, we are not trying to get a numerical result regarding the exact average scanning time for this scanning rule. Our purpose is to show that cluster scanning rule has a shorter scanning time compared with the previous two. We solve the problem from the cluster's viewpoint.

Suppose there are N clusters, the number of receivers in each cluster is Y_1, Y_2, Y_3,...,Y_N and $\mathrm{Y}_1 > \mathrm{Y}_2 > \mathrm{Y}_3 > \ldots > \mathrm{Y}_N$.

Since the transmitter will first scan the locations of highest receiver density, we can come to the conclusion that the more receivers a cluster has, the larger probability this cluster will be scanned. Actually, we can assume that the probability a cluster will be scanned is proportional to its number of receivers. At the same time, the total probability of all the clusters being scanned is 1 [62], namely:

$$\sum_{i=1}^{N} P_n = 1 \tag{3.8}$$

Hence, we can normalize the probability of each cluster to be scanned as:

$$P_n = \frac{Y_n}{\sum_{i=1}^{N} Y_n}, \quad n = 1, 2, 3, \ldots, N \tag{3.9}$$

which can be rewritten using:

$$\sum_{n=1}^{N} Y_n = M \tag{3.10}$$

to obtain the expression:

$$P_n = \frac{Y_n}{M}, \quad n = 1, 2, 3, \ldots, N. \tag{3.11}$$

The cluster in which the target receiver is located at is called target cluster. Since the majority of scanning time is spent on searching for the target cluster, we assume as long as the target cluster is found, the target receiver will be immediately found. In the other word, the time used for searching the target receiver inside the target cluster is neglected[3].

Similarly, based on *law of total expectation* [62], the average scanning time is:

$$\begin{aligned} E(X|Y_n) &= \sum_{n=1}^{N} X_n P_n \\ &= 1 \times \frac{Y_1}{M} + (1+Y_1) \times \frac{Y_2}{M} + \cdots + \\ &\quad (1+Y_1+Y_2+\cdots+Y_{N-1}) \times \frac{Y_N}{M} \\ &= \frac{1}{M} \times [M + \sum_{\substack{p,q=1 \\ p \neq q}} Y_p Y_q]. \end{aligned} \tag{3.12}$$

In this equation, when $n = 2$, X_2=1+Y_1. $n = 2$ means that the target receiver appears in the second cluster. Since it is cluster-based scanning, the transmitter must scan the first cluster before it reaches the second one. As defined at the beginning of this section, Y_n is the number of receivers in the nth cluster, so this is where Y_1 comes from. In addition, we assume that as long as the transmitter reaches the target cluster, it only requires 1 scanning time to locate the target receiver. The value 1 means when the transmitter reaches the second cluster, it only takes 1 scanning time to locate the target receiver.

Since the square of the sum can be expanded as:

$$(Y_1 + \cdots + Y_N)^2 = Y_1^2 + \cdots + Y_N^2 + 2 \sum_{\substack{p,q=1 \\ p \neq q}} Y_p Y_q \tag{3.13}$$

and the sum of squared numbers is much larger than zero:

$$Y_1^2 + \cdots + Y_N^2 >> 0 \tag{3.14}$$

So the last item in Eq. (3.13) can be expressed as:

$$\sum_{\substack{p,q=1 \\ p \neq q}} Y_p Y_q << \frac{1}{2}(Y_1 + \cdots + Y_N)^2 = \frac{1}{2} M^2 \tag{3.15}$$

[3]This assumption provides a trackable and closed-form solution, which is also an optimistic result. The inclusion of the per cluster scanning time will be studied in the future work.

Therefore, the average scanning time for cluster scanning rule is within the range:

$$E(X) << \frac{1}{M} \times (M + \frac{1}{2}M^2) = \frac{1}{2}M + 1 \tag{3.16}$$

From this result, we can see that the average scanning time for cluster scanning rule is much less than $M/2$. Since the average scanning time for frequency sequence scanning and pilot tone strength scannning are both around $M/2$, cluster scanning definitely has a better performance on this.

3.3 Performance Results

3.3.1 Network Setup

In this work, our computer simulations employ three scenarios for 1 transmitter and N receivers. In Scenario 1 and 2, all the radios are randomly positioned inside a square with a diagonal of 20 meters. The only difference is that in Scenario 1, the center frequencies are generated using uniform distribution, ranging between 2.35GHz and 2.45GHz, as shown in Figure 3.4. In Scenario 2, the center frequencies are generated using Gaussian distribution, with the mean of 2.4GHz and the standard deviation of 0.01GHz, as shown in Figure 3.5.

In Scenario 3, we employ the actual spectrum measurement data of paging band signals located in Worcester, MA. We made the measurement on the frequency range of 928MHz to 948MHz, and the power spectrum is shown in Figure 3.6. By applying Otsu's method [63] and inspection, we set the threshold power at -100dBm, which means all the signals stronger than -100dBm are considered being used by primary users, and the other signals are classified to be noise. Our receivers, as the secondary users, can be allocated to unoccupied frequencies, labeled as Rx01 to Rx05 in Figure 3.7.

Due to the distance between the transmitter and the receivers, the energy of the pilot tones will attenuate on its path and the attenuations seen by the transmitter will vary according to the spatial distribution of the receivers. We can quantitatively express it using a log-distance path loss model [64]:

$$\overline{PL}(\text{dB}) = \overline{PL}(d_0) + 10n \log \frac{d}{d_0} \tag{3.17}$$

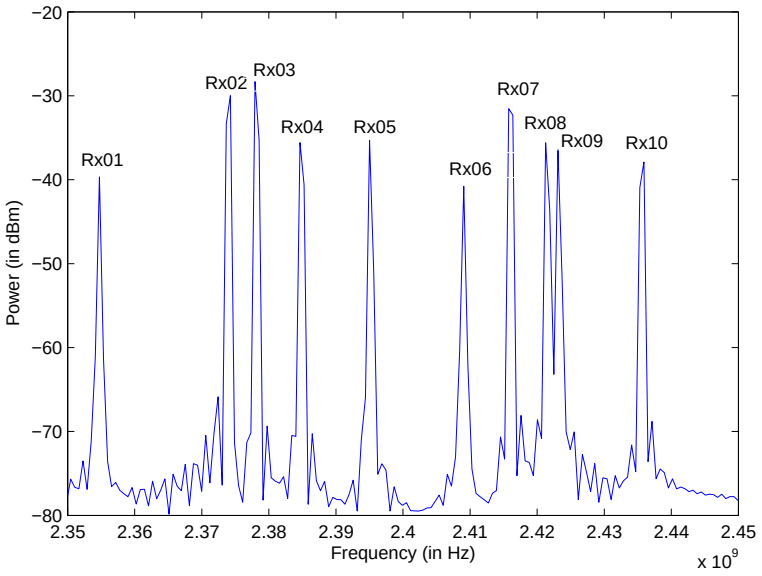


Figure 3.4: The amplitude spectrum of 10 receivers, whose center frequencies are uniformly distributed between 2.35GHz and 2.45GHz.

where n is the path loss exponent which indicates the rate at which the path loss increases with distance. Since we assume all the nodes are in wireless environment, we specify n as 3.5.

Before the simulation starts, all the receivers are numbered from 1 to N according to their center frequencies, starting from the lowest. Then, we generate a random integer between 1 and N to designate the target receiver radio. Consequently, the transmitter implements the proposed frequency rendezvous algorithm and tries to find that receiver.

3.3.2 Analytical Results

In the simulation, the three scanning rules are tested in three different scenarios. For each scenario and each receiver number N, we run the scanning rule for 100 times and obtain an average. Figure 3.8 is the result for Scenario 1 (uniformly distributed wireless nodes), Figure 3.9 is the result for Scenario 2 (Gaussian distributed wireless nodes) and Figure 3.10 is the result for Scenario 3 (actual paging band spectrum measurements). We have added lines of best fit using least squares for each group of data.

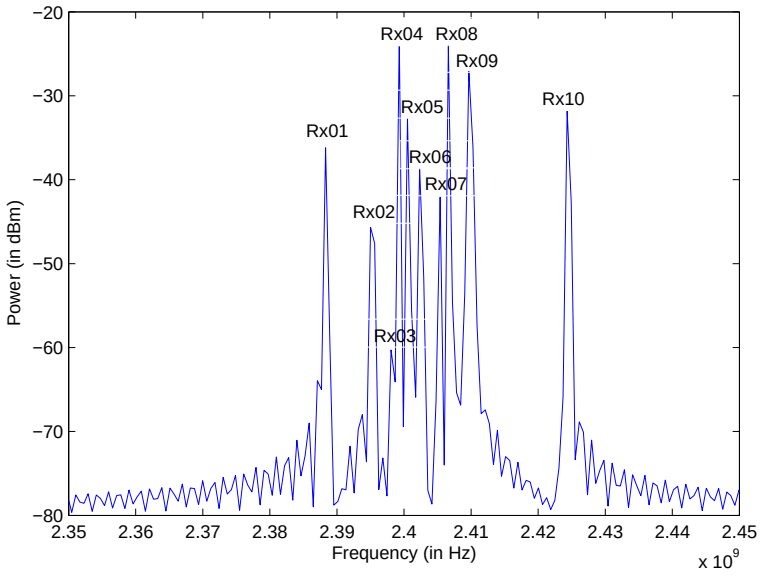


Figure 3.5: The amplitude spectrum of 10 receivers, whose center frequencies are Gaussian distributed with the mean of 2.4GHz.

As for uniform distribution and Gaussian distribution, the performance of Scanning Rules 1 and 2 is comparable, while the Scanning Rule 3 has a better performance with a uniform distribution. We can see that the two fitted lines in Figure 3.8 are parallel, while the two fitted lines in Figure 3.9 trend toward converging when N increases. This is due to the Gaussian distribution, where receivers are concentrated around the mean value, which is already a kind of cluster. Hence, the cluster algorithm in scanning rule will not significantly improve performance.

As for actual paging band spectrum measurements, since most of the free spectrum is located at (930MHz, 936MHz) and (940MHz, 948MHz), which is 14MHz in total. It is much narrower than the spectrum of the first two scenarios, which is from 2.35GHz to 2.45GHz (100MHz). Therefore, we cannot put as many receivers here; otherwise, the interference between the channels would be unacceptably high. As a result, for the first two scenarios, N is set from 20 to 150, while for Scenario 3, N is set from 20 to 60. Based on this, we can find that the peak density of the receivers in Scenario 3 (3 receivers/MHz) is much lower than that in the first two scenarios (7.5 receivers/MHz).

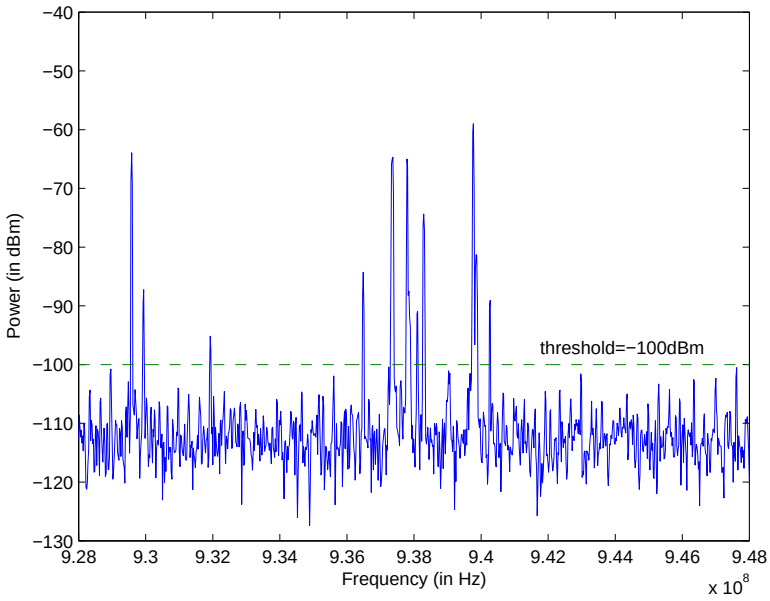


Figure 3.6: Spectrum measurement of 928MHz-948MHz paging band signals in Worcester, MA (42°16′8″N, 71°48′14″W), taken at 17:00 in 13 January 2009.

The cluster algorithm used here is the k-means algorithm [65]. It is an algorithm to cluster n objects based on attributes into k partitions. In the application here, we are trying to cluster N center frequencies into $\lfloor 0.1(N-1) \rfloor + 1$ partitions based on their distance with each other, hoping that the frequencies in each cluster are close together.

As for actual paging band data, we can see that the two lines of best fit in Figure 3.10 diverge as N increases, which means the performance of Scanning Rule 3 is especially good in this situation. As mentioned before, compared to Scenarios 1 and 2, the receiver density of Scenarios 3 is lower. In this situation, the cluster algorithm in scanning rule will really take effect in clustering the distributed receivers into groups and increase the search efficiency of the transmitter.

Based on these three figures, we can find out some common characteristics of the average scanning time:

- *Linear Character*: The average scanning time for all the three scanning rules are proportional to the number of receivers. The more receivers there are, the more scanning time it requires. We can put a best fitting line for each of the scanning rules,

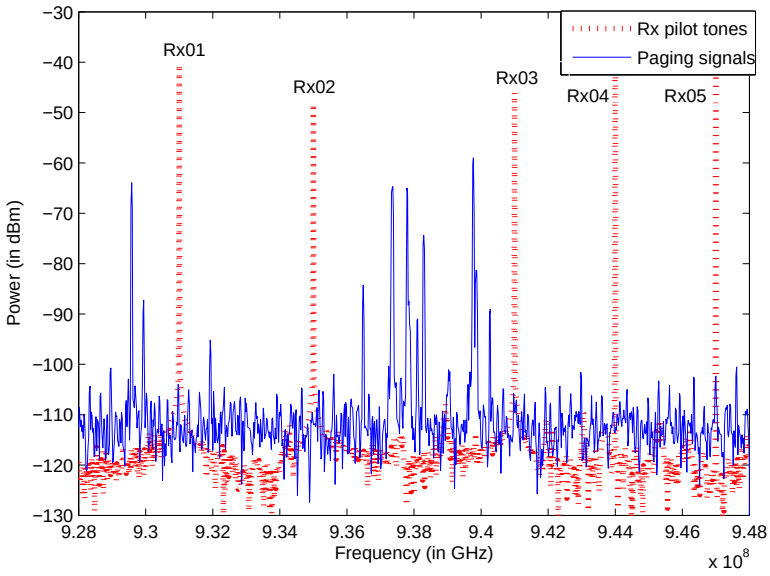


Figure 3.7: The power spectrum of 5 receivers, which are secondary users in paging band.

and the data are distributed around this line.

- *Similar Scanning Times*: Scanning Rule 1 (in frequency sequence) and Scanning Rule 2 (in pilot tone strength sequence), have quite close average scanning time, although sometimes, one is a little better than the other. We can use the same best fitting line for both of them, and the Y-axis of this line is just half of the number of the receivers N. This is consistent with the mathematical derivations in Section 3.2.1 and 3.2.2.

- *Relative Scanning Performance*: In general, Scanning Rule 3 (*i.e.*, the cluster sequence) achieves the smallest average scanning time in Figures 3.8, 3.9, and 3.10, which is consistent with the analytical results in Section 3.2.3, although there are several exceptions when the number N is very large. Compared to Scanning Rules 1 and 2, the cluster-based scanning is relatively more complicated to implement, thus resulting in a trade-off between complexity and efficiency.

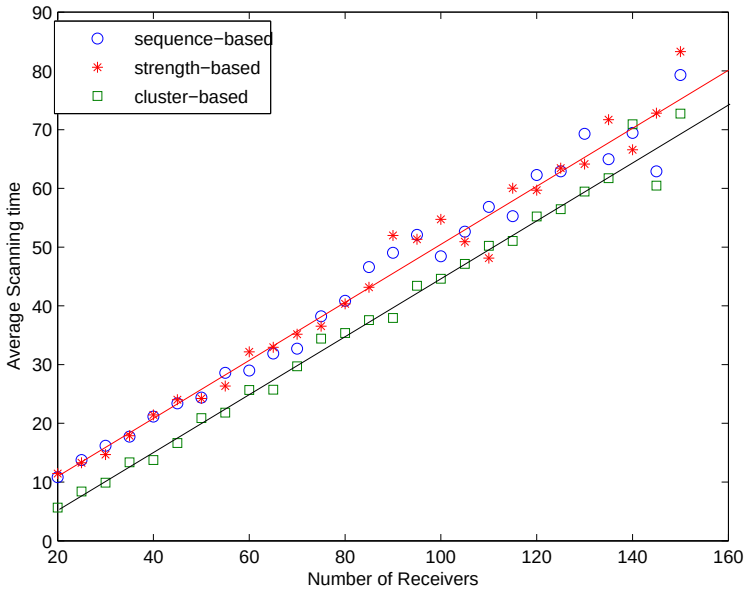


Figure 3.8: Comparison between three different scanning rules for uniformly distributed center frequencies. The blue circles, red asterisks and green squares represent the average scanning times for sequence-based scanning rule, strength-based scanning rule, and cluster-based scanning rule, respectively. The red straight line is the line of best fit for the first two scanning rules, which also corresponds to half of the number of receivers.

3.4 Summary

The efficiency of the proposed frequency rendezvous approach depends heavily on the scanning rule. The mathematical analysis of three different scanning rules has been presented. They have also been applied to uniform, Gaussian and practical paging band spectrum in computer simulation to validate the analysis. The results of these two methods are perfectly consistent with each other. Generally speaking, scanning in frequency sequence and in pilot tone strength sequence takes almost the same time, while scanning in cluster requires less time.

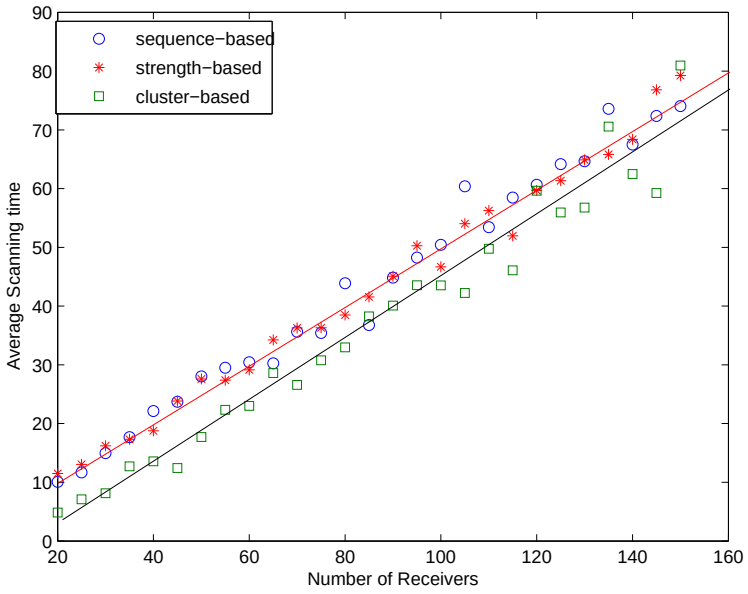


Figure 3.9: Comparison between three different scanning rules for Gaussian distributed center frequencies. The blue circles, red asterisks and green squares represent the average scanning times for sequence-based scanning rule, strength-based scanning rule, and cluster-based scanning rule, respectively. The red straight line is the line of best fit for the first two scanning rules, which also corresponds to half of the number of receivers.

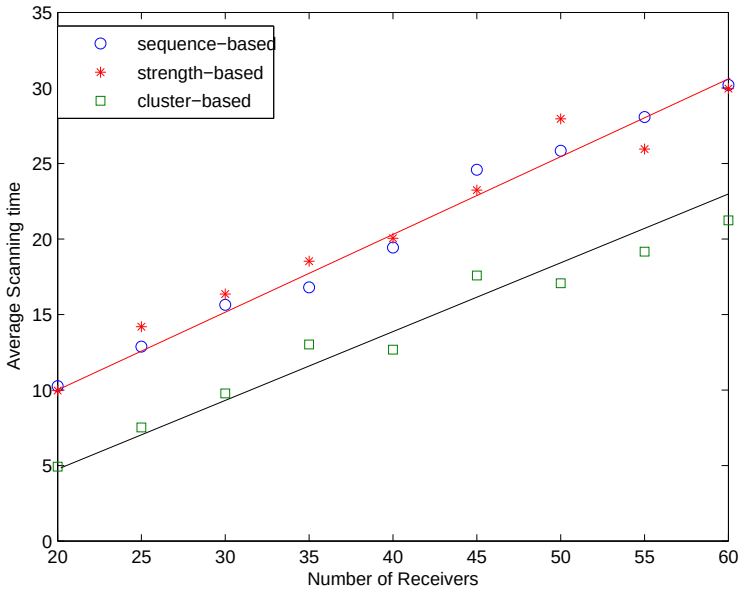


Figure 3.10: Comparison between three different scanning rules for real paging band spectrum. The blue circles, red asterisks and green squares represent the average scanning times for sequence-based scanning rule, strength-based scanning rule, and cluster-based scanning rule, respectively. The red straight line is the line of best fit for the first two scanning rules, which also corresponds to half of the number of receivers.

Chapter 4

Detecting Wormhole Attacks with Physical Layer Network Coding[1]

In Section 2.4.3, we introduce the basic idea of using physical layer network coding to detect wormhole attacks. However, several issues need to be solved before the idea can be turned into a viable solution. In this chapter, mechanisms are designed on the network layer and the physical layer to make the approach secure and practical. We perform both an analysis and simulations to investigate the impacts of different factors in the physical layer. In the end, we study the security and detection accuracy of the proposed approach.

4.1 Network Layer Framework

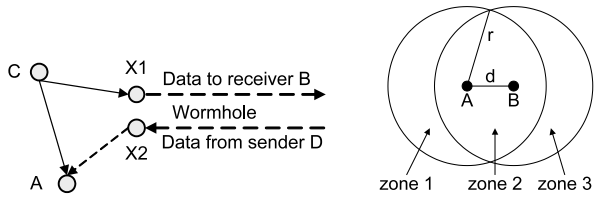
In this section we focus on the issues in the network layer. The physical layer issues will be handled in the next section.

4.1.1 Assumptions and Model of Attackers

We assume that the links among wireless nodes are bidirectional and the two neighboring nodes can always send packets to each other. We adopt the unit disk graph model in this work and assume that two wireless nodes are neighbors when the distance between them is

[1]This chapter is partially based on the work presented in [23].

shorter than r, where r is defined as the communication range. We assume that the wireless nodes can adjust the transmission power such that the signal range can be increased, e.s. $2r$. We assume that each node is equipped with an omni-directional antenna. We also assume that the communication channel is half duplex and a node cannot transmit and receive signals at the same time. The wireless nodes will periodically broadcast neighbor discovery beacons such that changes in neighbor lists can be detected.



(a) (b)

Figure 4.1: Practical issues in the network layer. (a) a more realistic node model of the attackers for the half-duplex channel. (b) the zones that the senders can be chosen from.

We assume that the wireless nodes share a secure, light-weight pseudo random bit generator (PRBG) [66]. The senders will use this generator to determine the sequences. By exchanging only the seeds for the PRBG, the receivers can regenerate the sequences and determine whether or not they have successfully recovered the sequences. Since we assume that the malicious nodes are all external attackers, the wireless nodes will employ encryption to protect the data communication amongst them. They can use either group keys or pair wise keys. Note that the generation and maintenance of the keys is beyond the scope of this thesis.

For the attackers, we assume that they cannot compromise the legitimate nodes in the wireless networks. At the same time, they cannot break the secret keys amongst the legitimate nodes by passively listening to the communication channel. The attackers can deploy their own nodes in the network to form wormholes. We assume that the attackers can communicate with each other through a real-time, long-range, out-of-band channel.

The assumption of the half-duplex channel has some impacts on the analysis of data collision through the wormhole. As illustrated in Figure 2.5.(c), the malicious node X cannot simultaneously listen to the sequence from C and forward data to A. It has to be decoupled into two nodes, X_1 and X_2, in order to accomplish these tasks. As illustrated in

Figure 4.1.(a), X_1 can get a copy of the data that X_2 is transmitting through the out-of-band channel. Therefore, X_1 will be able to decode the sequence from C in the presence of interference. Decoupling the node X into two nodes will introduce some changes to Equation (2.4). However, these changes can be hidden in the transmission delay of the wormhole and will not subvert our approach.

4.1.2 Selection of Senders

In this part we study two problems: first, how to choose the senders in a real network environment; second, the relationship between the wormhole detection probability and the number of rounds of verification. Answers to these questions will allow us to better understand the advantages and limitations of the proposed approach.

Selection of Senders

The analysis in Section 2.4.3 showed that the detection of wormholes will not be impacted by the distances among the senders and receivers. However, in a real wireless network, several reasons restrict us from choosing a sender that is multiple hops away from the receiver. First, if the sender is far away from the receivers, it has to transmit the signal at a high power level. This will not only consume the limited battery power of the sender but it will also cause interference in a large area. Second, if we choose a sender that is multiple hops away, this path has a higher probability to contain a wormhole. The malicious nodes can then manipulate the arriving time of the sequences and compromise the detection mechanism. Therefore, we propose to choose the senders from the union of the neighbor lists of the receivers.

Figure 4.1.(b) shows the areas that the senders can be chosen from. As an example, nodes A and B want to verify their neighbor relationship. They jointly choose the senders C and D such that C is a direct neighbor of A and D is a direct neighbor of B. Since A and B are neighbors, the senders must be within the distance $2r$ to both of the receivers. In this way, the senders can adjust their sending power to make sure that the signals can be received by both of the receivers.

This scheme will greatly increase the pool of senders that we can choose from. As shown

in Figure 4.1.(b), if we require the senders to be direct neighbors of both receivers, we can choose senders only from zone 2. Now we can choose from zones 1 and 3 as well. If the distance between A and B is d where $(d \leq r)$, the size of zone 2 is:

$$Area_{zone2} = 2r^2 \arccos(\frac{d}{2r}) - d\sqrt{r^2 - (\frac{d}{2})^2}$$

and the size of zone 1 is $\pi r^2 - Area_{zone2}$. Therefore, if the distance between A and B has a uniform distribution on the interval $[0, r]$, we can calculate the average size of zone 2. We find that on average the ratio between the total size of zones 1, 2 and 3 and the size of zone 2 ≈ 1.9. This implies that our approach has a much larger pool of senders to conduct wormhole detection.

Determining Number of Verification Rounds

In Figure 2.5.(c), we show one possible scenario of sender selections in which C and D are at different sides of the wormhole. Since the wireless nodes cannot distinguish a real neighbor from a fake neighbor through the wormhole, there is a chance that both senders are located at the same side of the wormhole. At the same time, the existence of multiple wormholes in the network can also create more complicated scenarios. In Figure 4.2, we illustrate two such cases. In both scenarios, the sequences from C and D will go through a wormhole to reach B. Therefore, the malicious nodes can manipulate the difference between the arriving time of the two sequences to compromise the proposed approach. To mitigate such attacks, we propose to conduct multiple rounds of verification with different senders to improve the odds of countering the malicious nodes.

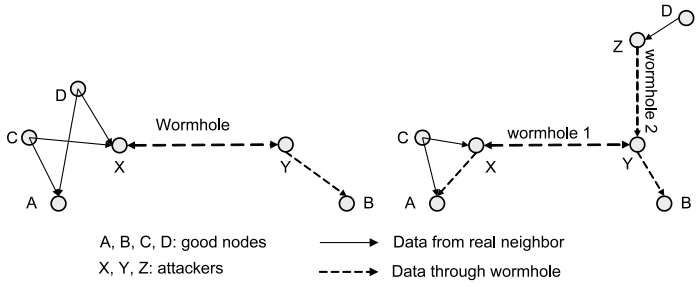


Figure 4.2: Neighbor selection scenarios that can avoid detection.

We assume that nodes A and B are connected through a wormhole and they want to verify their neighbor relationship. We assume that the number of real neighbors of A and B are RN_A and RN_B, respectively. Similarly, the number of fake neighbors of the two nodes through the wormhole are FN_A and FN_B. Therefore, the probability that we choose one real neighbor for each receiver in order to form the senders within p rounds is:

$$1 - (1 - \frac{RN_A}{RN_A + FN_A} \cdot \frac{RN_B}{RN_B + FN_B})^p \tag{4.1}$$

Based on this equation, we can see that the malicious nodes can reduce the probability of being detected by introducing a large number of fake neighbors via wormholes. However, in real wireless networks there are several reasons that will restrict the attackers from doing this. First, when the attackers deploy a large number of malicious nodes to create numerous wormholes, it will become fairly difficult for them to maintain a web of real-time, out-of-band communication channels across all of these nodes. Second, the legitimate nodes possess a good estimate of the node density and the average number of neighbors in the network. Previous research efforts [67, 68] have shown that the node degrees in MANETs follow some distributions. Therefore, if the wormholes make the node degrees abnormally large, the legitimate nodes will become suspicious and adopt other mechanisms to detect the wormholes. If the node degrees follow some distributions such as binomial [68], the wireless nodes can easily figure out the corresponding parameters to achieve a certain detection probability.

4.1.3 Generation of Sending Sequences

The sequences that the senders transmit should satisfy two requirements: First, the receivers should be able to verify the authenticity of the sequences to make sure that they are generated by the senders. Second, the sequences should be kept as a secret from the attackers before they are sent out. The first requirement will guarantee that the attackers cannot generate some random sequence to deceive the receiver. As illustrated in Figure 2.5.(c), if the receivers cannot verify the authenticity of the sequences, the malicious nodes X and Y can generate some random sequences to send to A and B. In this way, they can easily control the difference between the arriving time of the two sequences and compromise

the proposed approach. The second requirement can prevent the man-in-the-middle attack. If the attackers know the sequences before they are sent by C and D, they can impersonate the senders and control the starting point of the collision of the sequences at the receivers.

To satisfy these requirements, the wireless nodes can use the following procedure to generate the sequences. We assume that every node is equipped with the same pseudo random bit generator (PRBG). They also have a secure channel to exchange information and the attackers cannot gain access to the data. Therefore, the two senders and two receivers can jointly determine two random numbers. These numbers will be used by the two senders as the seeds for the PRBG. Since the receivers also know the seeds, they can easily verify the received sequences. At the same time, the seeds will be kept as a secret from the attackers.

4.1.4 Neighbor Verification Procedure

Given the building blocks at the network layer, the following neighbor relation verification algorithm is employed.

1. When two nodes A and B want to verify their neighbor relationship, each of them will choose one neighbor from their neighbor lists, namely C and D, to be the senders. C and D should be within $2r$ to both A and B.

2. The four nodes will jointly choose two seeds r_C and r_D for the PRBG at C and D to generate the sequences. A and B will also have a copy of the seeds.

3. A uses (r_C *xor* r_D) as the seed for the PRBG to generate a series of pilot bits. A will broadcast the pilot bits at the power level such that B, C, and D will all receive the data to learn that the verification procedure starts.

4. C and D will verify the pilot bits from A. Each of them will then choose a random delay to make sure that A and B are ready to receive. Then, the two nodes will send out the sequences generated by the PRBG based on the seeds r_C and r_D. They will send the sequences with a sufficiently high power level such that both A and B can receive them. The two sequences will be long enough such that a large part of the sequences will collide at the receivers.

5. A and B will use the algorithm in Section 4.2 to separate the sequences and verify them. The two nodes will exchange the starting points of the collisions and use the method described in Section 2.4.3 to verify their neighbor relationship.

6. Steps 1 to 5 will repeat until A and B find that they are connected through a wormhole or they are convinced that they are real neighbors after p rounds.

4.2 Proposed Physical Layer Approach

To turn the proposed approach into a practical solution, the physical layer needs to accomplish the following tasks. First, the physical layer needs to successfully separate the two combined sequences. It also needs to locate the starting point of the collision so that the information can be used to detect wormholes. Second, we need to assess the impacts of different factors in the physical layer on the proposed approach. In the following subsections, we will determine the parameters for signal transmission, design the receiver algorithm to separate the colliding sequences, and evaluate the approach under different parameters through theoretical analysis and simulation.

4.2.1 Modulation of Signals

When the two senders generate their sequences using the PRBG, the data bits need to be modulated and demodulated in order to achieve over-the-air transmission. Thus, we need to decide on a proper modulation/demodulation scheme on both ends.

Binary Phase Shift Keying (BPSK)

Phase-shift keying (PSK) is a digital modulation scheme that conveys data by modulating the phase of the carrier wave. Since any digital modulation scheme uses a finite number of distinct signals to represent digital data, PSK uses a finite number of phases that are each assigned with a unique pattern of binary bits. The demodulator, which is designed specifically for the symbol set used by the modulator, determines the phase of the received signal and maps it back to the symbol it represents, thus recovering the original binary

data. This requires the receiver to be able to compare the phase of the received signal to a reference signal.

Binary Phase Shift Keying (BPSK) is the simplest form of PSK. It uses two phases which are often separated by π. Using BPSK, a symbol can be expressed by the following formula:

$$s_i(t) = \cos(2\pi\omega_c t + \theta_i),\ i = 1, 2$$

where θ_i is the phase of the symbol and $|\theta_1 - \theta_2| = \pi$. It does not particularly matter exactly where the constellation points are positioned so long as their phase difference is sufficiently large, e.g., π.

When we consider that there are two senders in the proposed mechanism, the jth output symbol of sender i can be expressed as:

$$s_{ij}(t) = \cos(2\pi\omega_c t + \theta_{ij}),\ i = 1, 2,\ j = 1, 2$$

where θ_{ij} is the phase, and $\theta_{11} = \theta_1$, $\theta_{12} = \theta_1 + \pi$, $\theta_{21} = \theta_2$, $\theta_{22} = \theta_2 + \pi$.

Why BPSK?

Several reasons lead us to choose BPSK as the modulation scheme for the proposed mechanism. First, BPSK is a very robust modulation scheme. Compared to the other PSK schemes, the constellation points of BPSK are the farthest away from each other, which means it takes a substantial amount of noise or distortion to make the demodulator reach an incorrect decision. This property is especially important when we consider that the receiver must verify the authenticity of the received sequences to avoid attacks on the proposed approach.

This modulation scheme will also help the receiver separate the two sequences. Using BPSK, the largest phase difference among the four modulated symbols is $\pi/2$. When the two input sequences are orthogonal to each other, it is straightforward for the receiver to distinguish between those two sequences from their collision. Furthermore, the structure of the receiver is much simpler compared to the other modulation schemes, resulting in lower implementation costs of the proposed approach.

4.2.2 Data Recovery Algorithms

Data recovery is the most important task that the receiver needs to implement. Below we will describe in detail the sequence detection and separation algorithms. For simplicity, we do not consider frequency jitter and power amplitude in this subsection, although they will be discussed later in this section.

Packet Reception

When we are designing the physical layer mechanisms, the first question we need to answer is how the receiver can detect the arrival of a data packet. This is a standard problem in digital communication. Since the received signal demonstrates a much higher energy level than that of the white noise, the receiver can look at the incoming energy level to detect the reception of data packets.

Next, since our approach does not require the wireless nodes to maintain synchronized clocks, there is a good chance that the sequence from one sender will arrive at the receiver first. Therefore, the receiver must be able to locate the starting point of the collision. Before this point, the receiver runs standard BPSK decoding. After this point, the receiver will treat the data as a packet corrupted by interference. It will then execute the interference decoding algorithm described below. To answer this question, the receiver will measure the variance in the energy level of the incoming signals. Since BPSK encodes the bits in the phase, the energy of a non-interfered BPSK signal is nearly constant. When two signals collide at the receiver, the variance will become much larger. Therefore, we can set up a threshold, and when the variance is larger than the pre-determined value, the sequence separation algorithm will be executed.

Data Recovery

As described in Section 4.2.1, one of the key advantages of using two BPSK signals is to simplify the structure of the receiver. Given the modulation scheme in Section 4.2.1, the receiver only needs a low pass filter and an oscillator, which generates the cosine wave of the same phase offset as one of the sequences. Without loss of generality, we assume its

phase offset to be the same as sequence 1. Therefore, the receiver can be expressed as:

$$r(t) = \cos(2\pi\omega_c t + \theta_1)$$

where ω_c is the carrier frequency of the receiver and θ_1 is the phase of sequence 1.

If the received signal is from sequence 1, for example s_{11}, using trigonometric identities, the output of the oscillator will be:

$$\begin{aligned} r_1(t) &= s_{11}(t) \cdot r(t) = \cos(2\pi\omega_c t + \theta_1) \cdot \cos(2\pi\omega_c t + \theta_1) \\ &= \frac{1}{2}[1 + cos(4\pi\omega_c t + 2\theta_1)] \end{aligned} \tag{4.2}$$

Similarly, if the received signal is from sequence 2, for example s_{21}, the output of the oscillator will be:

$$\begin{aligned} r_2(t) &= s_{21}(t) \cdot r(t) = \cos(2\pi\omega_c t + \theta_2) \cdot \cos(2\pi\omega_c t + \theta_1) \\ &= \frac{1}{2}[cos(\theta_1 - \theta_2) + cos(4\pi\omega_c t + \theta_1 + \theta_2)] \end{aligned} \tag{4.3}$$

Since we attach a low pass filter after the oscillator at the receiver, the $4\pi\omega_c t$ term in Equations (4.2) and (4.3) will be eliminated. Since the two sequences collide at the receiver, the final output of the filter will be:

$$\tilde{r}(t) = \tilde{r}_1(t) + \tilde{r}_2(t) = \frac{1}{2} + \frac{1}{2}cos(\theta_1 - \theta_2) \tag{4.4}$$

Since $cos(\theta_1 - \theta_2) \leq 1$, $\tilde{r}_1(t) \geq \tilde{r}_2(t)$, the demodulation is actually determined by $\tilde{r}_1(t)$ such that the final output of the receiver is the recovered sequence 1. In particular, when $\theta_1 - \theta_2 = \pi/2$, $cos(\theta_1 - \theta_2) = 0$ so that $\tilde{r}(t) = \tilde{r}_1(t)$, there is not any interference from sequence 2, resulting in the recovered sequence 1 being the most accurate. This is the orthogonal case mentioned in Section 4.2.1. When the phase difference between the two signals is not $\pi/2$, we propose to adopt the phase equalization method to compensate for this error. The details of the method will be described in Section 4.2.2. When the recovered sequence 1 is obtained, it can be subtracted from the combined signal to yield sequence 2. The receiver will then execute the decoding algorithm to recover the second sequence.

Sequence Verification As we discussed in Section 4.1, the receiver must verify the authenticity of the recovered sequences to defend against attacks from malicious nodes.

Since the receiver has a copy of the seeds of the PRBG, it can regenerate the sequences. It will then compare the calculated sequences to the recovered ones. To distinguish a correct sequence from a random one, the similarity between the calculated sequence and the recovered one should be non-negligibly larger than 0.5. This threshold value shows that the proposed mechanism is very robust against bit errors in recovered sequences.

Improvement on the Algorithm

Based on the discussion above, it is obvious that in order to achieve the highest recovery accuracy, we need to ensure that the phase offset of the receiver is consistent with the phase offset of sequence 1 and that the phase difference between the two senders ($|\theta_1 - \theta_2|$) is around $\pi/2$. However, in reality, the phase is actually a time-varying variable that depends on many factors. Consequently, we introduce pre-equalization here to compensate for this error.

Pre-equalization is a function applied at the transmitter that counteracts the phase degradation caused by the transmission channel. Equalization is implemented in two steps, namely, channel training and data transmission. In the first step, each of the two senders will send out some pilot bits to train the channel. The receiver will figure out how the channel influences the phases by comparing the received signals. Then, before the second step starts, the senders will adjust their phases based on the feedback from the receiver. Since we assume this communication system is in a pseudo-stationary state within a period of time, the channel condition in Step 2 is almost the same as in Step 1. Thus, these adjustments will lead to orthogonality in Step 2.

4.2.3 Impacts of Various Factors on BER

As discussed in Section 4, the receiver must verify the authenticity of the recovered sequences. Otherwise, an attacker can send out some random sequence and the receiver cannot distinguish it from the real sequence. In this subsection, we plan to investigate the impacts of various factors in the physical layer on the bit error rate (BER), which is defined

as:

$$\text{BER} = \frac{\text{number of incorrectly recovered bits}}{\text{total number of transmitted bits}}$$

Phase Difference

In Section 4.2.2, the final output of the filter is:

$$\tilde{r}(t) = \tilde{r}_1(t) + \tilde{r}_2(t) = \frac{1}{2} + \frac{1}{2}cos(\theta_1 - \theta_2)$$

When $\theta_1 - \theta_2 = \pi/2$ such that $cos(\theta_1 - \theta_2) = 0$, the two signals are orthogonal to each other and they have the least interference. When $\theta_1 - \theta_2 = 0$ such that $cos(\theta_1 - \theta_2) = 1$, then $\tilde{r}_1(t) = \tilde{r}_2(t)$, which means the interference from sequence 2 is as strong as sequence 1 itself. Therefore, the recovered sequence 1 will be the least accurate. Using probability theory, we can calculate the BER value in this case. There are four possible combinations of sequence 1 and sequence 2, namely {(0,0),(0,1),(1,0),(1,1)}. When the transmitted bits are (0,0) or (1,1), there will be no problem, since the interference of sequence 2 will not change the decision on sequence 1. However, when the transmitted bits are (0,1) or (1,0), the resulting signal is around 0, which means there is a probability of 0.5 that the recovered bit is wrong. Therefore, the BER here can be expressed as a conditional probability:

$$BER = P[E|(0,1) \cup (1,0)] \times P[(0,1) \cup (1,0)] = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4} \tag{4.5}$$

where E is the event that a bit is incorrectly recovered.

When $\theta_1 - \theta_2 \in (0, \pi/2)$ such that $cos(\theta_1 - \theta_2) \in (0, 1)$. Since the cosine function is monotonically decreasing in the range $(0, \pi/2)$, we can expect that the interference from sequence 2 decreases as $\theta_1 - \theta_2$ increases, which means the BER is a monotonically decreasing function within the range $[0, \frac{1}{4}]$ concerning phase difference. Note that the receiver can still successfully verify the recovered sequences with the 25% BER rate.

Frequency Jitter

In our previous analysis, the carrier frequencies of sequence 1, sequence 2, and the oscillator are assumed to be the same. However, similar to the behavior of the phase, the carrier frequency is also a time-varying variable. In this subsection, we will explore how the

frequency jitter affects the BER performance. When taking frequency jitter into account, the symbol can be expressed as:

$$s_i(t) = A\cos(2\pi(\omega_c + \omega_{\Delta i})t + \theta_i)$$

where $\omega_{\Delta i}$ is the frequency jitter of the ith carrier frequency. The frequency jitter of the oscillator is assumed to be $\omega_{\Delta 3}$.

As for sequence 1, whose frequency jitter is $\omega_{\Delta 1}$, its output of the oscillator will be:

$$\begin{aligned} r_1(t) &= s_1(t) \cdot r(t) \\ &= \cos[2\pi(\omega_c + \omega_{\Delta 1})t + \theta_1] \cdot \cos[2\pi(\omega_c + \omega_{\Delta 3})t + \theta_1] \\ &= \frac{1}{2}\{cos[2\pi(\omega_{\Delta 1} - \omega_{\Delta 3})t] \\ &+ cos[4\pi\omega_c t + 2\pi(\omega_{\Delta 1} + \omega_{\Delta 3})t + 2\theta_1]\} \end{aligned} \tag{4.6}$$

Due to the low pass filter, the final output of the filter will be:

$$\tilde{r}_1(t) = \frac{1}{2}cos[2\pi(\omega_{\Delta 1} - \omega_{\Delta 3})t] \tag{4.7}$$

Similarly, as for sequence 2, whose frequency jitter is $\omega_{\Delta 2}$, its output of the low pass filter will be:

$$\tilde{r}_2(t) = \frac{1}{2}cos[2\pi(\omega_{\Delta 2} - \omega_{\Delta 3})t + (\theta_2 - \theta_1)] \tag{4.8}$$

Considering the orthogonal case, where $\theta_2 - \theta_1 = \pi/2$, Equation (4.8) becomes:

$$\tilde{r}_2(t) = \frac{1}{2}cos[2\pi(\omega_{\Delta 2} - \omega_{\Delta 3})t + \pi/2] = \frac{1}{2}sin[2\pi(\omega_{\Delta 2} - \omega_{\Delta 3})t] \tag{4.9}$$

In order to get an accurate recovery of sequence 1, the $\tilde{r}_1(t)$ should be as large as possible, while $\tilde{r}_2(t)$ should be as small as possible. Therefore, we would like $\omega_{\Delta 1} - \omega_{\Delta 3} = 0$ and $\omega_{\Delta 2} - \omega_{\Delta 3} = 0$. In other words, if the carriers have the same frequency jitter, it will have no effect on BER. Otherwise, it will result in an increased number of bit errors.

4.2.4 Simulation Results

In this subsection, we use computer simulators implemented in Simulink to explore the impacts of various factors on BER and compare them with the theoretical analysis results derived in Section 4.2.3.

Phase Difference and SNR

In real wireless networks, all the signals will pass through a noisy channel prior to arriving at the receiver. In wireless communication, an additive white Gaussian noise (AWGN) channel is the most widely used model and the signal-to-noise power ratio (SNR) is a key metric of the transmission performance across this channel. Intuitively, a high noise level will result in a high BER rate.

In this part, the relationship between the BER and phase difference, as well as BER and SNR, are studied. SNR values of 0 dB, 3 dB and 5 dB are examined. The phase difference ranges from 0 to $\pi/2$. The resulting plot is shown in Figure 4.3.

There are several important observations about the results shown in Figure 4.3:

1. All the three curves are monotonically decreasing functions.

2. When the phase difference is equal to zero, BER$\approx$ 0.25 in all three cases.

3. Given the same phase difference, the BER is larger when there is a higher noise level.

All of these observations match the analysis results in Section 4.2.3.

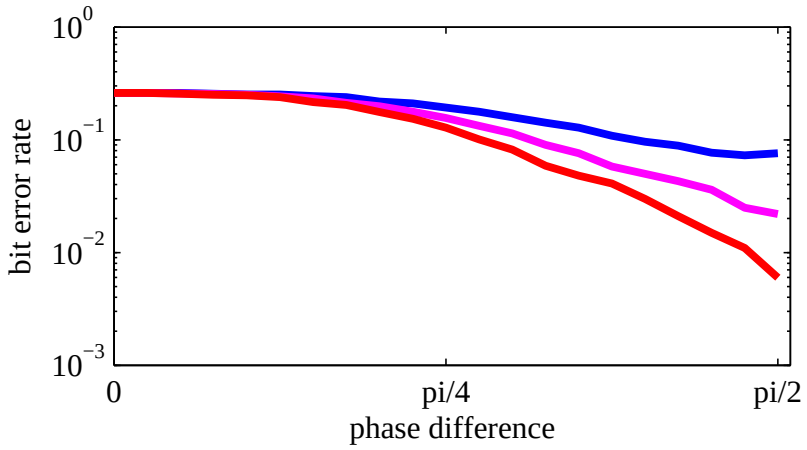


Figure 4.3: The BER values with respect to phase difference and SNR. The blue curve is obtained when SNR=0 dB, the pink curve corresponds to SNR=3 dB, and the red curve is for SNR=5 dB.

Power Amplitude

In our previous discussions, we have not taken power amplitude into account. However, in an actual communication system, the power of a signal will gradually deteriorate on its way to the destination. Even when the two signals are transmitted using the same power, the received power will not be the same. Therefore, the resulting output of the filter should be rewritten as:

$$\tilde{r}(t) = A_1\tilde{r}_1(t) + A_2\tilde{r}_2(t) = \frac{1}{2}A_1 + \frac{1}{2}A_2 cos(\theta_1 - \theta_2) \tag{4.10}$$

where A_1 and A_2 are amplitude of the received sequence 1 and received sequence 2, which are different.

In order to recover sequence 1 correctly, we want the interference from sequence 2 to be as low as possible. This is a relative comparison between the two sequences, such that we can use a fraction to express their relationship:

$$\frac{P_1}{P_2} = \frac{A_1}{A_2 cos(\theta_1 - \theta_2)}$$

Given $\theta_1 - \theta_2$ is kept constant, if A_1 becomes larger or A_2 becomes smaller, the interference from sequence 2 becomes weaker such that the recovered sequence 1 is more accurate.

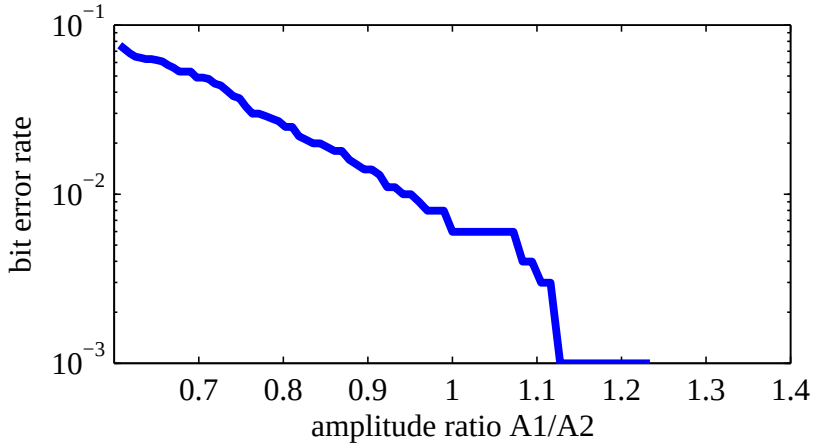


Figure 4.4: The BER value with respect to amplitude. The x-axis is the ratio of amplitude between two sequences.

In the following simulation, we set phase difference between two signals to be $\pi/2$ and the SNR to be 5 dB. We also assume that the receiver has the same phase offset as sequence

1. The amplitude of sequence 1 is increased from -5 dB to 5 dB, while the amplitude of sequence 2 is decreased from 5 dB to -5 dB. Therefore, the ratio is monotonically increasing. The BER plot is shown in Figure 4.4.

Based on Figure 4.4, it is obvious that the power amplitude has an impact on BER. When A_2 is much larger than A_1, the BER can be as high as 0.08. However, when A_1 becomes larger than A_2 ($\frac{A_1}{A_2} > 1$), the BER value falls below 0.5%, which introduces a very low bit error rate.

The simulation results provide us some insight into the data recovery algorithm. When the senders send out the pilot bits to train the channel for phase equalization, the receiver can also provide feedback to them for their transmission power. Based on the signal deterioration model, we can control the power ratio between the received signals to achieve a balance between the recovery rates of the two sequences.

Frequency Jitter

In this subsection, the relationship between the BER and frequency jitter is studied. We set the phase difference of the two signals to be $\pi/2$, the amplitude of the two sequences to be the same, and the SNR value to be 5 dB. We change the carrier frequency of the receiver. Since the carrier frequency can be either smaller or larger than the normal one, we use frequency offset as the x-axis and the corresponding BER plot is shown in Figure 4.5.

Based on Figure 4.5, it is obvious that the frequency jitter also has an impact on the BER. As predicted in Section 4.2.3, when there is no frequency jitter, which means the two senders and the receiver have the same carrier frequency, the BER is the lowest. Consequently, the more jitter presents in the system, the higher the BER will be. However, when the frequency jitter is within a range, we have a relatively low BER rate and the overall performance will not be severely hurt.

Having studied Figures 4.3, 4.4 and 4.5, we can conclude that phase difference has the largest impact on the BER rate. We can adopt different methods to compensate for the errors so that the detection capabilities of the proposed approach will not be severely impacted by these factors.

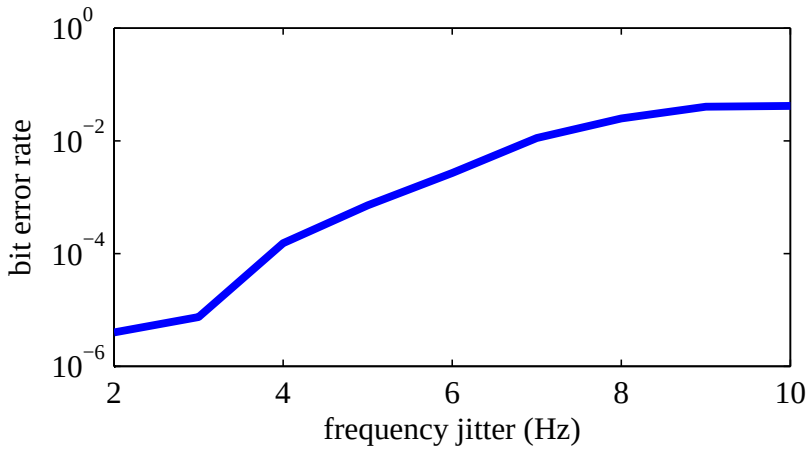


Figure 4.5: The BER value with respect to frequency jitter. The x-axis is the carrier frequency offset of the receiver.

4.3 Discussion

4.3.1 Why Depend on PNC to Measure Time Difference

As shown in Section 2.4.3, the proposed approach measures the starting point of interference of two colliding sequences to estimate the distance between the receivers. Here we have to answer one question: why do not we directly use system clocks to measure the difference between the arriving time of two sequences? In that way, we can let the two senders send out their packets alternatively and still allow the receivers to estimate their distance.

Unfortunately, previous research [69, 70] has shown that wireless nodes have a maximum clock drift rate at microsecond level (10^{-6} second). At the same time, the deviations of clock drift rates are also at the microsecond level. Equation (2.2) in Section 2.4.3 shows that when the two receivers are real neighbors, the difference between t_{diffA} and t_{diffB} is restricted by $\frac{2r}{s}$. If we assume that the radio range r is 250 meters and the signal propagates at the speed of light, the difference is roughly 500 $m \div$ 300,000 $km/s \approx 1.67 \times 10^{-6} sec$. We can see that the measured duration and the clock drift are at the same level. Therefore, directly using the system clock to measure the time difference will introduce a large number of false alarms.

Physical layer network coding provides a solution to this problem. As the analysis in [17] shows, the wireless nodes can locate the bit from which the interference of two colliding sequences starts. If the wireless nodes are transmitting at the bit rate of 11 Mb/s, 1.67 μsec equals to the difference of 18 bits in the received sequences. With the continuous increase in the bit-rate of wireless networks, the difference will become larger and larger. Therefore, physical layer network coding allows us to more accurately measure the difference and detect fake neighbor connections.

4.3.2 Security of the Proposed Approach

In Section 4.1 we discuss the authenticity of the received sequences and the prevention of man-in-the-middle attack. In this part, we study other security aspects of the approach.

When node A uses (r_C *xor* r_D) as the seed to generate the pilot bits, it is very difficult for the attackers to counterfeit this information. If we assume that the seeds r_C and r_D have the length of k and the pilot bits have the length of h, the probability that an attacker can correctly regenerate the pilot bits without the information of r_C and r_D equals to $\max(\frac{1}{2^h}, \frac{1}{2^k})$. We can adjust the values of k and h to prevent the attackers from fabricating the starting signal and conducting man-in-the-middle attack on the mechanism.

Since the attackers have a total control over the tunneling procedure, they can block the verification procedure by discarding the packets going through the wormhole. This operation, however, will allow the legitimate nodes to derive more information about the wormholes. If node A fails to get a sequence from a sender and it is not because of the low quality of the communication channel, we conclude that there is a wormhole between A and the sender. This can be proven by contradiction. If there is no wormhole between A and the sender, we know that the distance between them is shorter than $2r$. Therefore, the sender will send out the sequence when it receives the pilot bits and A would have received the sequence. When node B fails to receive a sequence, it will exchange information with node A. If A gets that sequence, B concludes that there is a wormhole between the sender and B. It can draw this conclusion since node A confirms that the sender actually sends out the sequence. Therefore, if there is no wormhole between B and the sender, it would have received it. Based on the analysis, we can see that the attackers will expose more

wormholes when they try to avoid detection by discarding packets.

Except for discarding packets, the attackers can also intentionally add noise to the packets when they tunnel them through the wormhole. This operation may lead to one of the two results. If the introduced noises are not strong and the receivers can still verify the authenticity of the sequences, the neighbor verification procedure will not be impacted. On the contrary, if the bit error rate becomes very large and the receiver can no longer verify the authenticity of the sequence, it will treat the packet as a lost one. The receiver can then follow the description in the previous paragraph and treat the connection as a wormhole. This decision can be justified as follows: treating a very error-prone connection as a wormhole and avoiding it during the routing procedure will not significantly deteriorate the network performance.

4.3.3 False Alarms of the Proposed Approach

False positive and false negative alarms are important parameters to evaluate a detection mechanism. In Section 4.1.2, we propose to adopt multiple rounds of verification to reduce false negative alarms. In this part, we focus on the investigation of false positive alarms.

When nodes A and B are real neighbors and the proposed approach identifies that they are connected through a wormhole, we have a false positive alarm. If both of the senders C and D are real neighbors to at least one of the receivers, we can derive that the two senders are within $2r$ to the two receivers. In this way, both the pilot bits and the transmitted sequences will reach their targets and the verification procedure will complete successfully. Therefore, to cause a false positive alarm, we must have at least one sender connecting to both receivers through wormholes. Without losing generality, we assume that the sender is node C.

If the two receivers A and B get the sequence from C through the same sending operation of the wormhole, the attackers will not be able to manipulate the difference between t_{diffA} and t_{diffB} since this operation has the same effect as node C is at the position of the wormhole node. The attacker can keep the sequence in the wormhole for a period of time. This operation, however, has the same effect as node C adjusts its transmission time. Previous analysis has shown that this parameter will be removed from the final calculation

result.

With this analysis, we find that the attackers need to deliver the sequence from C to the two receivers through two different sending operations so that they can control the difference between their arriving time. This goal can be achieved through maintaining two separate wormholes to the receivers, or transmitting the sequences through different directional antennas. Both schemes will increase the deployment difficulty and the hardware costs of the attackers. At the same time, the following simulation will show that the false positive alarms have limited impacts on the average path length in the network.

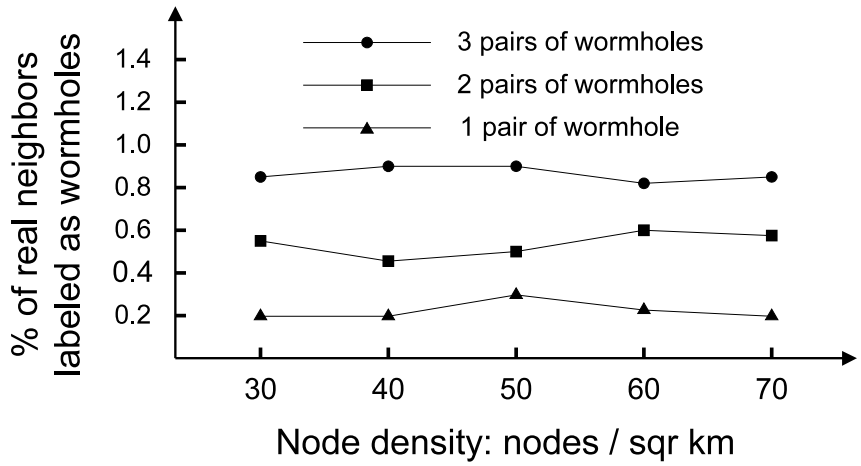


Figure 4.6: Percent of real neighbors labeled as wormholes (false positive alarm).

In this simulation, we assume that the legitimate nodes are deployed randomly and uniformly in a 2 $km \times 2$ km area. The transmission range r is 250 m. Two legitimate nodes A and B are real neighbors. When they want to verify the neighbor relationship, the attackers will transmit the sequences to them through two malicious nodes X and X' respectively. Here X is only a neighbor of A and X' is only a neighbor of B. Since A and B are real neighbors, the physical distance between X and X' is in the interval $[0, 3r]$. Under these assumptions, we study the relationship among the number of false positive alarms, the node density, and the number of wormholes in the network.

Figure 4.6 shows the simulation results. We can see that the node density does not have a large impact on the ratio between the number of false positive alarms and the total number of neighbor relations in the network. At the same time, when there are fewer than 3 pairs

of wormholes, there are less than 1% of real neighbor relations that are wrongly labeled as wormholes. Previous research [50] shows that when the false positive alarm rate is smaller than 1%, its impacts on the average path length among legitimate nodes are very limited. Therefore, we conclude that when there are not many pairs of wormholes in the network, the false positive alarms will not significantly deteriorate the network performance.

4.4 Summary

In this chapter, we propose a wormhole detection mechanism for wireless networks based on physical layer network coding. When the sequences from two senders collide at the receiver, the starting point of collision is determined by the distances from the senders to the receiver. Two wireless nodes can then compare their starting points of collision to estimate the distance between them and verify the neighbor relationship. To turn this mechanism into a practical approach, we study various problems in the network layer and the physical layer. We also analyze the safety of the proposed approach and investigate the false alarm rate.

Chapter 5

Conclusion

5.1 Research Achievements

In this thesis, a number of contributions have been made in the area of frequency rendezvous and physical layer network coding. The research achievements of this thesis are the following[1]:

- A frequency rendezvous algorithm that does not require a control channel, makes no assumption about the frequency locations and views the spectrum as a whole. It can be successfully applied to uniform, Gaussian and practical paging band spectrum.
- Mathematical analysis of three different scanning rules, which reveals that scanning in frequency sequence and in pilot tone strength sequence takes almost the same time, while scanning in cluster requires less time.
- Applying three different scanning rules to uniform, Gaussian and practical paging band spectrum in computer simulation. The results of computer simulation are perfectly consistent with the mathematical analysis.
- A wormhole detection mechanism for wireless networks based on physical layer network coding, which can be used by two wireless nodes to estimate the distance between them and verify the neighbor relationship.

[1]Some of the achievements have been presented in [21], [22] and [23].

- A network layer framework and a physical layer approach to turn this detection mechanism into a practical one, along with various problems and factors on both layers.

5.2 Future Work

Immediate extensions to our approach consist of the following aspects. First, we will implement the proposed approach in software defined radio and test it in real network environments. Second, we will improve the efficiency of the detection mechanism by allowing multiple pairs of neighbors to share the same pair of senders. Finally, we will investigate using physical layer network coding to detect other stealth attacks on wireless network topology.

Initial design, implementation, and evaluation of the proposed distributed wireless network architecture have been conducted via computer simulation. However, given the existing software-defined radio (SDR) research facility and expertise available at The Wireless Innovation Laboratory (WI Lab) [71], it is expected that the final network architecture will be quickly prototyped and evaluated in hardware. Specifically, we will be employing the Universal Software-Defined Radio Peripheral 2 (USRP2) by Ettus Research LLC as the development platform of choice for the proposed network architecture. The platform provides a powerful development environment accessible to research groups too small to develop their own wireless network prototyping solutions. The USRP2 is a highly configurable hardware platform providing both RF data capturing and arbitrary waveform generation.

Leveraging existing software and support available from existing collaborations with The MathWorks, new wireless designs, algorithms, and architectures can be readily developed and tested under real world and reproducible conditions. Streaming-based software solutions such as Simulink [72] are ideal for debugging the radios in simulation and then running the radios in real time using the USRP2. Our current solution for interfacing Simulink to the USRP2 hardware platform is shown in Figure 5.1. Interfacing these radios to the USRP2 will accelerate research and development for the cognitive radio field. With Simulink being a graphical and user-friendly software environment, this readily lends itself to being an excellent teaching tool. Since many communications texts use block diagrams to explain

the flow of communication systems, Simulink will add the functionality behind these blocks and bridge the gap between the learning environment and development. Consequently, providing this robust tool for this project will enable rapid prototyping and evaluation of new ideas.

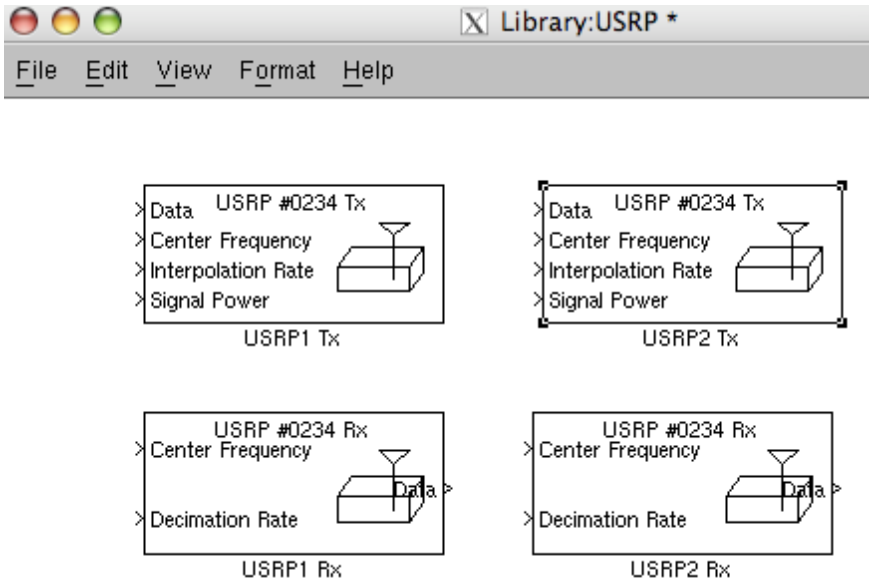


Figure 5.1: Simulink blocks for interfacing with the USRP2 platforms.

Bibliography

[1] Simon Haykin. Cognitive radio: brain empowered wireless communications. *IEEE Journal on Selected Areas in Communications*, pages 201–220, February 2005.

[2] Srikanth Pagadarai, Rakesh Rajbanshi, and Alexander M. Wyglinski. *Cognitive Radio Communications and Networks: Principles and Practice*, chapter Agile Transmission Techniques. Elsevier, 2009 [in preparation].

[3] Qing Zhao and Brian M. Sadler. A Survey of Dynamic Spectrum Access. *IEEE Signal Processing Magazine*, May 2007.

[4] Fulu Li and Kui Wu. Reliable, distributed and energy-efficient broadcasting in multi-hop mobile ad hoc networks. In *Proceedings of the 27th Annual IEEE Conference on Local Computer Networks*, Tampa, FL, November 2002.

[5] Roberto Aldunate, Sergio F. Ochoa, Feniosky Pea-Mora, and Miguel Nussbaum. Robust mobile ad hoc space for collaboration to support disaster relief efforts involving critical physical infrastructure. *Journal of Computing in Civil Engineering*, 2006.

[6] Qilian Liang. Ad hoc wireless network trafficself-similarity and forecasting. *IEEE Communications Letters*, 6, July 2002.

[7] Kitti Wongthavarawat and Aura Ganz. IEEE 802.16 based last mile broadband wireless military networks with quality of service support. In *Proceedings of the IEEE Military Communications Conference*, volume 2, pages 779–784, October 2003.

[8] Kamal Jain, Jitendra Padhye, Venkata N. Padmanabhan, and Lili Qiu. Impact of interference on multi-hop wireless network performance. *Wireless Networks*, 2005.

[9] Matthew J. Zieniewicz, Douglas C, Douglas C. Wong, and John D. Flatt. The evolution of army wearable computers. *IEEE Pervasive Computing*, October-December 2002.

[10] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. Wireless sensor networks: a survey. *Computer Networks*, 38:393–422, March 2002.

[11] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, pages 102–114, August 2002.

[12] Chee-Yee Chong and Srikanta P. Kumar. Sensor networks: Evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8), August 2003.

[13] J. Mitola III and G. Q. Maguire. Cognitive radio: making software radios more personal. *Personal Communications, IEEE*, 6(4):13–18, 1999.

[14] Milind M. Buddhikot, Paul Kolodzy, Scott Miller, Kevin Ryan, and Jason Evans. Dimsumnet: New directions in wireless networking using coordinated dynamic spectrum access. In *Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, June 2005.

[15] Brent Horine and Damla Turgut. Link rendezvous protocol for cognitive radio networks. In *Proceedings of the IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Dublin, Ireland, April 2007.

[16] Luiz A. DaSilva and Igor Guerreiro. Sequence-based rendezvous for dynamic spectrum access. In *Proceedings of the IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Chicago, IL, October 2008.

[17] Sachin Katti, Shyamnath Gollakota, and Dina Katabi. Embracing wireless interference: analog network coding. In *Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communications (SigComm)*, pages 397–408, 2007.

[18] Shengli Zhang, Soung Chang Liew, and Patrick P. Lam. Hot topic: physical-layer network coding. In *Proceedings of the annual international conference on Mobile computing and networking (MobiCom)*, pages 358–365, 2006.

[19] Denis Charles, Kamal Jain, and Kristin Lauter. Signatures for network coding. *Int. J. Inf. Coding Theory*, 1(1):3–14, 2009.

[20] Jing Dong, Reza Curtmola, and Cristina Nita-Rotaru. Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks. In *Proceedings of the ACM conference on Wireless network security (WiSec)*, pages 111–122, 2009.

[21] Di Pu, Alexander M. Wyglinski, and Mike McLernon. A frequency rendezvous approach for decentralized dynamic spectrum access networks. In *Proceedings of the IEEE International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, Hannover, Germany, June 2009.

[22] Di Pu, Alexander M. Wyglinski, and Mike McLernon. An analysis of frequency rendezvous for decentralized dynamic spectrum access. *Submitted to IEEE Transactions on Vehicular Technology - Special Issue on "Achievements and the Road Ahead: The First Decade of Cognitive Radio"*, May 2009.

[23] Weichao Wang, Di Pu, and Alexander M. Wyglinski. Forced collision: Detecting wormhole attacks with physical layer network coding. In *Submitted to Proceedings of the ACM Conference on Wireless Network Security*, Hoboken, NJ, USA, March 2010.

[24] S. Zhou, M. Zhao, X. Xu, and J. Wang. Distributed wireless communication system: a new architecture for future public wireless access communications. *IEEE Commun. Magazine*, 41:108–113, 2003.

[25] J. Wang, Y. Yao, M. Zhao, S. Zhou, Y. Wang, and X. S. Conceptual platform of distributed wireless communication system. In *Proceedings of IEEE Vehicular Technology*, volume 2, pages 593–597, 2002.

[26] Joseph Mitola III. *Cognitive Radio*. Licentiate dissertation, The Royal Institute of Technology, Stockholm, Sweden, September 1999.

[27] Friedrich K. Jondral. Software-defined radio-basics and evolution to cognitive radio. *EURASIP Journal on Wireless Communications and Networking*, 3:275–283, 2005.

[28] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Elsevier Computer Networks*, 50:2127–2159, 2006.

[29] Federal Communications Commission (FCC). Spectrum Inventory Table 137 MHz to 100 GHz. [Online]: http://www.fcc.gov/oet/info/database/spectrum/.

[30] D. Cabric, S.M. Mishra, D. Willkomm, R. Brodersen, and A. Wolisz. A cognitive radio approach for usage of virtual unlicensed spectrum. In *Proceedings of the 14th IST Mobile and Wireless Communications Summit*, June 2005.

[31] B. S. Manoj, Michele Zorzi, and Ramesh Rao. A new paradigm for cognitive networking. In *Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2007.

[32] Hiroshi Harada. Software defined radio prototype toward cognitive radio communication systems. In *Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2005.

[33] Hiroshi Harada. Regulatory perspective of japan. In *Proceedings of the VCE Regulatory Workshop*, London, UK, April 2007.

[34] Hiroshi Harada. Advances in flexible radio technology to support cognitive radio. In *Proceedings of the VCE International Research Workshop on Intelligent Spectrum Usage for Personal Communications*, London, UK, April 2007.

[35] William Webb. IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks 2007 keynote presentation.

[36] Keith E. Nolan, Eamonn Ambrose, and Donal O'Mahony. Cognitive radio: Value creation and value migration. In *Proceedings of the SDR Forum Technical Conference 2006*, 2006.

[37] International Telecommunication Union. Radio-spectrum management for a converging world. [online]: http://www.itu.int/osg/spu/ni/spectrum/.

[38] Roberto Ercole. Innovation, spectrum regulation, and dyspan technologies access to markets. In *Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2005.

[39] L. Kovacs and A. Vidacs. Spectrum auction and pricing in dynamic spectrum allocation networks. In *Proceedings of the IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2007.

[40] Brent Horine and Damla Turgut. Performance analysis of link rendezvous protocol for cognitive radio networks. In *Proceedings of International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, August 2007.

[41] M. J. McGlynn and S. A. Borbash. Birthday protocols for low energy deployment and flexible neighbor discovery in ad hoc wireless networks. In *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Long Beach, CA, 2001.

[42] Pil Jung Jeong and Myungsik Yoo. Resource-aware rendezvous algorithm for cognitive radio networks. In *Proceedings of the 9th International Conference on Advanced Communication Technology*, Feb 2007.

[43] Y. Hu, A. Perrig, and D. Johnson. Wormhole attacks in wireless networks. *IEEE J. Sel. Areas Commun*, pages 370–380, 2006.

[44] Srdjan Čapkun, Levente Buttyán, and Jean-Pierre Hubaux. Sector: secure tracking of node encounters in multi-hop wireless networks. In *Proceedings of ACM workshop on Security of ad hoc and sensor networks*, pages 21–32, 2003.

[45] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In *Proceedings of Network and Distributed System Security Symposium*, 2004.

[46] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff. Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks. *Comput. Netw.*, 51(13):3750–3772, 2007.

[47] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff. Mobiworp: Mitigation of the wormhole attack in mobile multihop wireless networks. *Ad Hoc Netw.*, 6(3):344–362, 2008.

[48] X. Wang and J. Wong. An end-to-end detection of wormhole attack in wireless ad-hoc networks. In *Annual International Computer Software and Applications Conference*, pages 39–48, 2007.

[49] J. Eriksson, S. Krishnamurthy, and M. Faloutsos. Truelink: A practical countermeasure to the wormhole attack in wireless networks. In *Proceedings of IEEE International Conference on Network Protocols*, pages 75–84, 2006.

[50] W. Wang and B. Bhargava. Visualization of wormholes in sensor networks. In *Proceedings of ACM Workshop on Wireless Security (WiSe)*, pages 51–60, 2004.

[51] Weichao Wang, Jiejun Kong, Bharat Bhargava, and Mario Gerla. Visualisation of wormholes in underwater sensor networks: a distributed approach. *Int. J. Secur. Netw.*, 3(1):10–23, 2008.

[52] Radha Poovendran and Loukas Lazos. A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wirel. Netw.*, 13(1):27–59, 2007.

[53] R Maheshwari, Jie Gao, and S.R. Das. Detecting wormhole attacks in wireless networks using connectivity information. In *INFOCOM*, pages 107–115, 2007.

[54] L. Qian, N. Song, and X. Li. Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach. *Journal of Network and Computer Applications*, 30(1):308–330, 2007.

[55] L. Buttyan, L. Dora, and I. Vajda. Statistical wormhole detection in sensor networks. In *European workshop on Security and Privacy in Ad-hoc and Sensor Networks*, pages 128–141, 2005.

[56] V. Stankovic, L. Fagoonee, A. Moinian, and S. Cheng. Wireless full-duplex communications based on network coding. In *Proc. of Annual Allerton Conference on Communications, Control and Computing*, 2007.

[57] Shengli Zhang, Soung Chang Liew, and Lu Lu. Physical layer network coding schemes over finite and infinite fields. In *IEEE GLOBECOM*, pages 1–6, 2008.

[58] Wei Pu, Chong Luo, Binxing Jiao, and Feng Wu. Natural network coding in multi-hop wireless networks. In *IEEE ICC*, pages 2388–2392, 2008.

[59] Yonggang Hao, Dennis Goeckel, Zhiguo Ding, Don Towsley, and Kin K. Leung. Achievable rates for network coding on the exchange channel. In *IEEE Milcom*, pages 1–7, 2007.

[60] Tao Cui, Tracey Ho, and J. Kliewer. Some results on relay strategies for memoryless two-way relay channels. In *Information Theory and Applications Workshop*, pages 158–164, 2008.

[61] Gilbert Held. *Building a Wireless Office*. CRC Press, 1st edition, 2002.

[62] Athanasios Papoulis and S. Unnikrishna Pillai. *Probability, Random Variables and Stochastic Processes*. McGraw-Hill, New York, NY, 4th edition, 2002.

[63] N.Otsu. Threshold selection method from gray level histogram. *IEEE Transactions on System, Man and Cybernetics*, 9(1):62–67, 1979.

[64] Theodore S. Rappaport. *Wireless Communications: Principles and Practice*. Prentice Hall, Upper Saddle River, NJ, USA, 2nd edition, December 2001.

[65] William H. Press, Saul A. Teukolsky, William T. Vetterling, and Brian P. Flannery. *Numerical Recipes: The Art of Scientific Computing*. Cambridge University Press, Cambridge, United Kingdom, 3rd edition, 2007.

[66] Rabia Latif and Mukhtar Hussain. Hardware-based random number generation in wireless sensor networks(wsns). In *Proceedings of the International Conference and Workshops on Advances in Information Security and Assurance*, pages 732–740, 2009.

[67] Hoai-Nam Nguyen and Yoichi Shinoda. A node's number of neighbors in wireless mobile ad hoc networks: A statistical view. In *Proceedings of International Conference on Networks*, pages 52–60, 2009.

[68] C.-C. TSENG, H.-T. CHEN, and K.-C. CHEN. Distribution of the node degree for wireless ad hoc networks in shadow fading environments. *IEICE Transactions on Communications*, E90-B(8):2155–2158, 2007.

[69] K. Römer. Time synchronization in ad hoc networks. In *ACM MOBIHOC*, pages 173–182, 2001.

[70] Hui Song, Sencun Zhu, and Guohong Cao. Attack-resilient time synchronization for wireless sensor networks. In *Proc. of IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, 2005.

[71] Alexander M. Wyglinski. WI Lab: Wireless Innovation Laboratory. [Online]: http://www.wireless.wpi.edu/index.html.

[72] The MathWorks. Simulink Simulation and Model Based Design. [Online]: http://www.mathworks.com/products/simulink/.