PRIMARY USER AUTHENTICATION METHODS FOR MOBILE COGNITIVE RADIO NETWORKS

by

Swathi Chandrashekar

A Thesis Submitted to the Faculty of the

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

In Partial Fulfillment of the Requirements
For the Degree of

MASTERS OF SCIENCE

In the Graduate College

THE UNIVERSITY OF ARIZONA

2012

STATEMENT BY AUTHOR

This thesis has been submitted in partial fulfillment of requirements for an advanced degree at the University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the Library.

Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgment of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED: _____

Swathi Chandrashekar

APPROVAL BY THESIS DIRECTOR

This thesis has been approved on the date shown below:

_____ _____

Loukas Lazos
Assistant Professor

Date

ACKNOWLEDGEMENTS

It is my pleasure to thank the people who have made this thesis possible.

I would like to thank my academic advisor Dr. Loukas Lazos who has supported me throughout my thesis with his patience and knowledge whilst allowing me the room to work in my own way. His passion for his work encouraged me to pursue my own goals, while his attention to detail instilled in me a unique perspective with which to approach problems. I am deeply grateful to him for having been my mentor. Our academic work together has been a truly rewarding and enriching experience.

I would also like to thank the members of my thesis defense committee, Dr. Bane Vasić and Dr. Ivan B. Djordjevic, for both supporting my degree goals as well as being my instructors in classes that I have taken.

My time in Tucson was made enjoyable in large part due to my many friends and groups who became a large part of my life. I thank them for all the fun times and adventures which made my life away from home an excellent experience.

Last but not least, I would like to thank my family. To my boyfriend who has supported my ambitions from the very beginning, been with me through thick and thin, encouraging me to push my limits while doing all he can to help me along the way and giving me all the love. To my brother, who provides me with a lot of strength and encouragement. And to my loving mother who has been a constant pillar of support. And, thank you God for everything.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The current spectrum allocation policy adopted by communication agencies around the globe mandates for the static licensing of the available spectrum to various technologies and organizations. This non-overlapping partitioning of the spectrum reduces interference and guarantees exclusive spectrum use to licensed users. However, nearly all useful spectrum is now allocated to different entities, without provision for accommodating new wireless technologies. In addition, recent studies have shown that most spectrum frequency bands are heavily underutilized. To this end, new technologies have emerged that enable the dynamic usage of the spectrum by unlicensed users without interfering with licensed/primary users. One of such enabling technologies employs cognitive radios for sensing and utilizing periods of time that the spectrum remains idle.

An important rule mandated for the deployment of such systems is to develop solutions that do not require any changes to the existing primary user (PU) infrastructure. While this is necessary for reducing the deployment cost for the legacy infrastructure, it creates several security vulnerabilities for the secondary users that dynamically access the network. One of the most notable of these vulnerabilities is the launch of primary user emulation (PUE) attacks on the spectrum sensing process. In this attack, the adversary mimics PU behavior by modulating the characteristics of PU transmission in order to gain an unfair advantage in utilizing idle frequency bands.

In this thesis, we address the problem of authenticating the PU signals in order to mitigate PUE attacks. We propose a PU authentication system based on the deployment of "helper" nodes, fixed within the geographical area of the cognitive radio network. Our system relies on a combination of physical-layer signatures (link-signatures) and cryptographic mechanisms to reliably sense PU activity and relay information to the cognitive radio network. Our system can accommodate mobile secondary users and can be implemented with relatively low-power helper nodes. Our work also extends to suggest a reputation based framework for detecting compromised helper nodes.

CHAPTER 1

Introduction

1.1 Motivation and Scope

New wireless technologies are rapidly permeating all aspects of commercial and social life, thus ever increasing the demand for higher bandwidth availability under heavy traffic loads. These technologies must co-exist in the same RF spectrum in a non-interfering manner. The prevailing policy for managing this co-existence of multiple wireless technologies in the RF domain, is to statically allocate the available spectrum. A static allocation separates different RF services in frequency, for the purpose of alleviating interference and contention, while providing quality of service. As an example, Figure 1.1 shows the current spectrum allocation in the United States [2, 4]. From Figure 1.1, it is worth noting that almost all useful spectrum from $3kHz$ to $300GHz$ is already licensed for exclusive use to various entities (government, commercial and military) with only a very small portion of it left for unlicensed use. Because the spectrum is already allocated, new wireless technologies find it increasingly hard to operate in unlicensed bands, where they face significant contention and interference from other services. This situation is typically termed as *spectrum scarcity*, referring to the unavailability of any useful spectrum bands that can be allocated.

However, studies of the spectrum scarcity problem by various regulatory bodies around the globe, including the Federal Communication Commission (FCC) in the United States of America and OfCom in the United Kingdom have shown that this problem is the artifact of the spectrum management policy [2,4,5]. Further, these studies indicate the underutilization of the already allocated spectrum. In fact, according to the FCC [2], the temporal and geographical variations in the utilization of the assigned spectrum range from 15% to 85%. Figure 1.2 illustrates the signal strength distribution over a large portion of the wireless spectrum. We can see that most frequency bands are underutilized whereas some frequency

bands are under heavy use.

Hence, to address the spectrum underutilization and spectrum scarcity problems, regulatory bodies have suggested to allow unlicensed users to opportunistically access licensed bands when these bands are not occupied by their primary holders [3, 6–9]. In this architecture, licensed users are typically referred to as *Primary Users* (PUs) and the opportunistic users are typically referred to as *Secondary Users* (SUs). The FCC mandates that the licensed spectrum can be accessed by SUs only if it is not in use by PUs [10]. Essential to meeting this regulation is the ability of the SU devices in recognizing the portion of the spectrum that is idle. This operation termed as *spectrum sensing,* is realized by intelligent software defined radios, also known as *Cognitive Radios* (CRs), named due to their sensing and adaptability capabilities. According to [2], a CR is *a radio that can change its transmitter parameters based on interaction with the environment in which it operates.* By this definition, a CR should have the following capabilities [3, 11, 12].

Cognitive capability: This refers to the ability of the CR to sense and capture spectrum-related information such as the set of frequency bands that are not in use by the PUs. This capability requires sophisticated techniques which capture the temporal and spatial variations of the radio environment and typically involves (a) spectrum sensing, (b) spectrum analysis, (c) spectrum decision, and (d) spectrum sharing. During spectrum sensing, the CR monitors the available spectrum bands to detect if they are in use by the PU and hence detect free channels. Through spectrum analysis, the characteristics of the free channels that are detected through spectrum sensing are estimated and then a channel that best meets the SU's communication requirements is selected. In spectrum decision, once the CR determines the transmission mode, data rate, and bandwidth required for transmission, it determines the spectrum it will use for transmission. In spectrum sharing, the available channels are shared in a fair manner between all the SUs.

Reconfigurability: The CR must be reconfigurable depending on the conditions of the radio environment. Some of the reconfigurable parameters that need to be incorporated in a CR device are the operating frequency, modulation, and transmission power of the device [2].

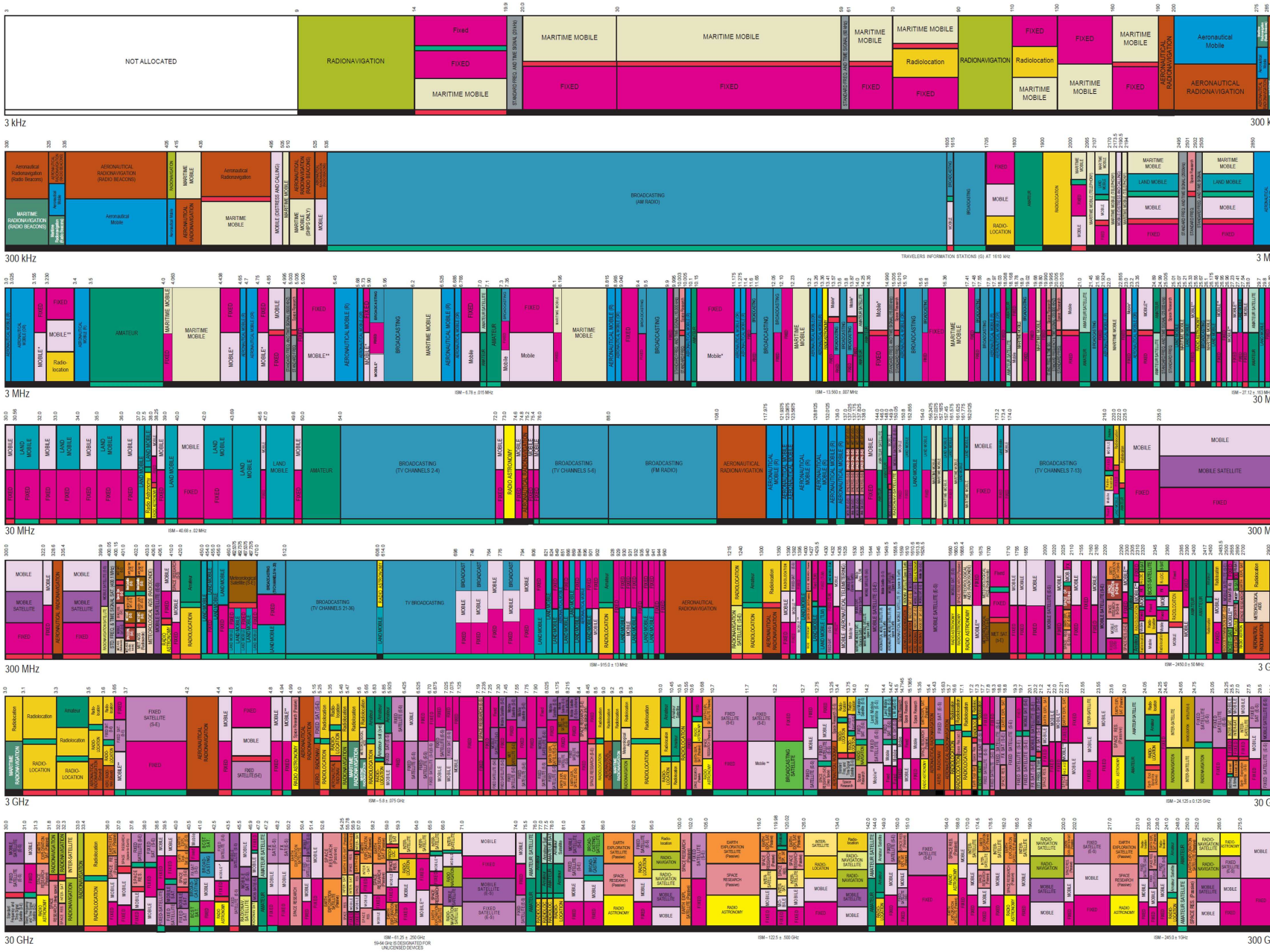

Figure 1.1: Current spectrum allocation in the United States of America [2].

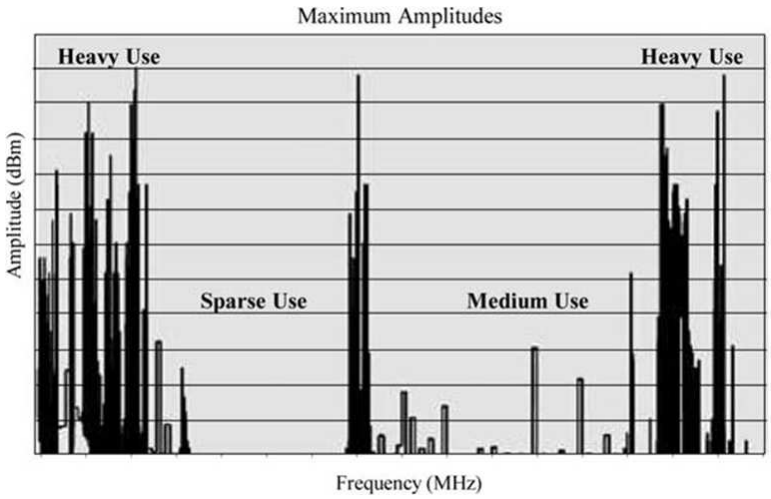

Figure 1.2: Signal strength distribution over the wireless spectrum [3].

The CR must be able to reconfigure each of these parameters adaptively to the user's requirements and channel conditions[1]. Moreover, in the event that a PU transmits in a channel currently used by a CR, the CR must have the capability of hopping to another free channel, without affecting its own transmission or causing interference to the PU transmission.

Enabling these functionalities requires designing of spectrum-aware communication protocols tailored to the dynamic nature of the available spectrum. Moreover, the harmonious co-existence of the PUs with the SUs must be achieved such that the PUs do not experience any performance degradation. In addition, since the legacy systems are already deployed infrastructures, no modifications should be made to these pre-existing systems. Hence, the SUs need to rely on self-sensing or cooperative sensing techniques to obtain spectrum information. Because modifications at the PUs are not possible, spectrum sensing must occur using unauthenticated physical layer methods such as energy detection, coherent signal detection and cyclostationary feature detection of the PU transmissions [6, 7, 13–16]. These requirements leave the spectrum sensing operation vulnerable to attacks from malicious entities (external adversaries or selfish SUs) that aim at distorting the spectrum availability.

An adversary equipped with a software defined radio can mimic the transmission characteristics of a PU in order to emulate PU activity on idle portions of the spectrum. He

[1]In the rest of this thesis, we use the term channel to refer to a frequency band.

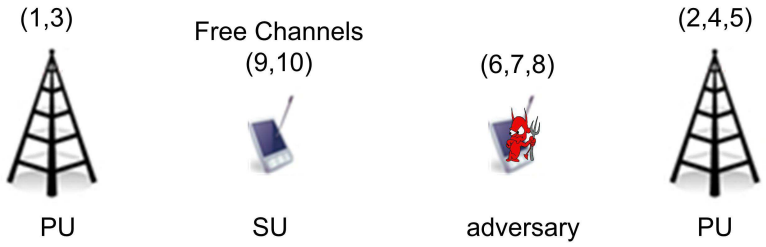

Figure 1.3: Primary user emulation attack scenario.

can record and replay a PU signal rendering the matched filter detector and cyclostationary feature detector inaccurate. The goal of this attack is to block legitimate SUs from utilizing the idle channels, thus reducing the available bandwidth and degrading the network performance. These types of attacks are known in literature as Primary User Emulation (PUE) attacks [1, 17–19].

As an example, Figure 1.3 shows an SU sensing the idle spectrum in the presence of an adversary. Assume that a total of 10 channels are available to the legacy system, and that channels $(1, 3)$ and $(2, 4, 5)$ are occupied by two PUs within the range of the SU. In a non-adversarial setting, the SU would have sensed channels $(6, 7, 8, 9, 10)$ as idle. However, in the presence of an adversary emulating PU activity on channels $(6, 7, 8)$, the set of idle channels sensed by the SU is limited to $(9, 10)$.

1.1.1 Thesis Problem and Main Contributions

In this thesis, we address the problem of preventing PUE attacks in mobile cognitive radio networks (CRNs). We propose a PU authentication system that securely and reliably delivers PU activity information to SUs. Our system does not require any modifications to the legacy system, as mandated by the FCC [10]. Provision of robust sensing information is facilitated by the deployment of a set of "helper" nodes. These helper nodes are responsible for authenticating the PUs and providing channel status information to the CRs. We suggest a two-way authentication system, where, the helper nodes authenticate PU activity and transmit channel availability information to the SUs. The helper nodes authenticate the PU using a link signature [20] which is a channel property between two nodes. The

SUs authenticate the helper nodes by verifying their cryptographic signatures. Helpers are deployed within the area of the PU network, independent of the location of the PUs, and can be relatively cheap low-power devices. Moreover, the location of the PUs need not be known. We also make use of a reputation-based system to detect compromised helpers that provide erroneous spectrum information.

1.2 Thesis Organization

In Chapter 2, we present related work, our system and threat model assumptions. In Chapter 3 we present the proposed PU authentication system. We analyze the security of our system and also provide a mathematical analysis in Chapter 4. In Chapter 5 we develop a reputation-based framework for detecting compromised helper nodes. In Chapter 6, we present simulation results and finally conclude in Chapter 7.

CHAPTER 2

Related Work, System Model, and Assumptions

The implementation of robust spectrum sensing mechanisms is pivotal to the co-existence of SUs with legacy systems. Before we discuss work related to PUE attacks, it is important to understand the spectrum sensing mechanisms that lead to inherent vulnerabilities in the spectrum sensing process.

2.1 Spectrum Sensing

Existing spectrum sensing methods can be classified into non-cooperative and cooperative sensing. Non-cooperative methods exploit the physical layer characteristics of PU transmissions such as energy, spectral density modulation, and cyclostationary features [6, 7, 13–16, 21–23]. Cooperative methods improve upon non-cooperative methods by allowing the exchange of spectrum sensing information between neighbors. In the following subsections, we discuss the above spectrum sensing methods in more detail.

2.1.1 Non-cooperative Spectrum Sensing Methods

Each CR should be able to distinguish between used and free spectrum bands/channels by determining if a particular signal is a PU transmission. Existing spectrum sensing methods rely on physical-layer characteristics of PU transmissions such as energy, spectral power density, modulation, cyclostationary features and pilot information [6, 7, 13–16]. The basic hypothesis model for transmitter detection is defined as given below [24]

$$x(t) = \begin{cases} n(t) & H_0, \\ hs(t) + n(t) & H_1, \end{cases} \tag{2.1}$$

where $x(t)$ is the received signal at the CR, $s(t)$ is the transmitted signal, $n(t)$ is the channel noise modeled as Additive White Gaussian Noise (AWGN) and h is the amplitude gain of the channel. In this hypothesis, H_0 is the null hypothesis that no PU is transmitting in the given channel or band, whereas, H_1 is the alternative hypothesis which indicates the existence of a PU signal in that channel. Sahai et al. [14] mention three schemes for transmitter detection according to the hypothesis model mentioned above. We briefly explain them below.

Matched filter detection: A matched filter is obtained by correlating a known signal with an unknown signal. The advantages of a matched filter are that, (a) it is analyzed to be the optimal detector[1] in the presence of additive stochastic noise [14] and (b) it requires little time to achieve high processing gain. However, it requires a priori knowledge of transmitted signals to work effectively. Several systems today employ preambles to this end. In the context of CRN's, we would require knowledge of PU signal characteristics such as the modulation type, packet format and the pulse shape at the CR.

Energy detection: In an energy detector, the energy of a received signal is compared to a threshold λ to decide whether a licensed user is present or not [25]. From this, it is evident that an energy detector is easy to design and implement. Hence, energy detection is the most widely adopted approach for spectrum sensing in recent works [7, 14, 26]. However, the performance of the energy detector is susceptible to uncertainty in noise power. If the noise power levels are high, the energy detector can raise a false alarm about PU existence. On the other hand, shadowing and multipath fading also affect the accuracy of the energy detector, causing misdetection of PU activity [24].

Cyclostationary feature detection: PU presence can also be detected by using a cyclostationary feature detector [7, 13, 21–23]. In this method, the periodicity of the signal is detected. Generally, a modulated signal is coupled with sine wave carriers, pulse trains, hopping sequence, etc. These are characterized as cyclostationary as their mean and autocorrelation exhibit periodicity. The detector looks for such periodicity in detecting a PU signal. The advantage of this method over energy detection is that it differentiates the noise

[1] one that maximizes the SNR.

signal from a modulated signal. Tang et al. show that this detector performs better than an energy detector [22]. However, it is computationally complex and requires a long observation time since the cyclostationary feature of a signal needs to be learnt and then used for detection.

2.1.2 Cooperative Spectrum Sensing Methods

Non-cooperative methods may become erroneous due to factors like shadowing and fading. Also, if the CR is located extremely far from the PU, it may not be in a position to decide the spectrum status [27, 28]. Cooperative spectrum sensing refers to sensing methods where information from multiple CRs is incorporated for PU detection. Theoretically, cooperative detection is more accurate since uncertainty in a single user's detection can be minimized as the influence of shadowing and multi-path fading factors can be minimized [24].

Cooperative detection can be implemented in either a centralized or distributed manner [26,29]. In the centralized approach, a base station collects all the spectrum information from different CRs and detects spectrum holes. In the distributed approach, the CRs exchange spectrum information amongst themselves and collectively decide on the spectrum holes.

The final decision about the channel occupancy is computed based on either an OR rule or a majority rule. According to the OR rule, even if one of the CRs reports the channel to be busy, the combined decision about the channel status is busy. In a majority scheme, a channel is decided to be busy if the majority of CRs report it as busy and idle if the majority of CRs do not sense activity on the channel.

2.1.3 Authenticated Spectrum Sensing

Several researchers have described and studied the feasibility of PUE attacks for both non-cooperative and cooperative sensing mechanisms [1, 17–19]. In a PUE attack, an attacker emulates the characteristics of a PU signal, thereby causing legitimate SUs to erroneously detect a channel to be busy, and, therefore deter from its use. An attacker may modify its transmission to mimic a PU signal's characteristics, thereby causing legitimate SUs to

erroneously identify the attacker as a PU. The problem of PU signal authentication has received attention only recently [1, 17, 18, 30]. The attacker may be emulating the PU for selfish or malicious reasons. The end result of this attack is, a legitimate SU will not be able to transmit in a channel even when its free. This results in an unfair distribution of the set of idle channels.

Current spectrum sensing methods do not provide authentication. An adversary may transmit a signal with high energy, emulating a PU, thereby rendering an energy detector inaccurate. An adversary may also emulate the cyclostationary features of a PU signal by replaying them, rendering a cyclostationary feature detector inaccurate. The successful deployment of the CRN depends on the security mechanisms which will resist the misuse of the system. The key to addressing this problem is to be able to distinguish between a PU transmission and an attacker signal in a robust fashion. Fundamentally, the problem can be modeled as a two-party authentication problem where SUs must be capable of authenticating PU activity. These types of problems have been addressed in literature using cryptographic methods [31]. However, such methods require modification on the legacy system side, thus not meeting the FCC mandates [10]. As a result, several systems have been demonstrated that do not require cryptographic methods. We outline the most relevant ones below.

Chen et al. proposed an authentication method based on a network of monitoring nodes which verify the origin of PU signals using received signal strength (RSS) measurements [17,32]. They estimate the distances from the PU using RSS values. If the estimated location of a PU deviates from the known PU location by a threshold, the signal is assumed to be emulated. However, location distinction methods based on RSS can be circumvented if the adversary employs antenna arrays [20]. If an adversary is capable of positioning itself close to the PU, it can regulate its transmission to emulate a PU. Moreover, RSS measurements are notoriously unreliable leading to high probabilities of false alarm.

Liu et al. proposed a PU authentication system assisted by helper nodes deployed in close proximity to the PUs [1]. The authors employed a combination of cryptographic and RF signatures to authenticate PU activity. The helpers are physically bound to PUs which may be TV towers with thousands of watts of transmission power, covering an area of tens

of square miles [8]. These helper nodes verify the PU presence by using the amplitude ratio r of the amplitude of the first to the second multipath component for the received signal. This ratio r is compared with a threshold w, and if $r > w$, then the received signal is marked as a PU signal. Next, helper nodes transmit in all the channels which the SUs listen to with the same power as the PU. This is a training phase in which the SUs build a history of the helper signals [20], called link signatures. Later, when an actual PU transmission occurs, the signal is compared to the stored history at the SU. If they match, the signal is considered to be of a PU. If they fail to match, then a PUE is reported. Although the helper nodes need not transmit all the time, the overall energy usage is significant as their energy level should be the same as that of the PU. Secondly, a training phase is required before a SU can robustly sense PU activity. This SU training process will need to occur every time a new SU joins the network or if the present SUs move to a new location.

Anard et al. proposed an analytical model for detecting primary user emulation attacks [30]. In their system model, malicious devices emulating the PU signal are deployed at fixed locations, at least R_0 units away from any SU. Using simplified propagation models, they compute the probability of a successful PU emulation. In this work, the authors assume that the location of a malicious node is very close to the benign node.

Chen et al. modeled the PU emulation problem as an estimation theory problem [18]. In their work, they divide the secondary users as attackers and defenders. n samples of the received signals are collected and the mean and variance of the signal is calculated. Then, the variance is compared with a threshold factor k to determine whether the signal is from a PU or an attacker. This work is based on the fact that the variance is very different for the signals of a PU and an attacker, as they will be at different locations, considering path loss and log-normal shadowing. Their work assumes that with high probability the attacker and the unbiased SU will be closer to each other than the PU. Also, the authors only consider stationary SUs.

Tan et al. propose a method that allows PUs to add a cryptographic link signature to their signal so that spectrum usage by PUs can be authenticated [19]. The authors propose two schemes for adding a cryptographic signature, one based on modifying the underlying

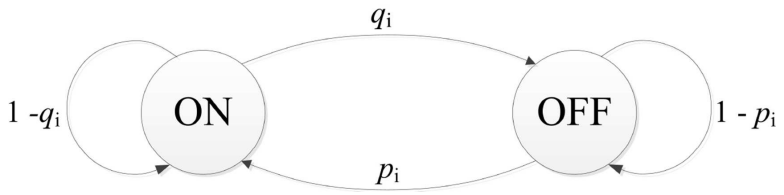

Figure 2.1: The semi-Markov PU activity model for a channel i.

modulation and one based on modifying error correction codes. This cryptographic signature is an authentication tag which the PU needs to generate using hashing. A particular hash value is valid only for some duration. This tag is included in the modulation scheme or to the error coding module at the physical layer. The tags are added in a transparent way as noise so that all PU receivers continue to function normally while the CR devices can authenticate the PU. In the modulation scheme, the noise tolerance in the constellation is exploited to insert the tag information while in the coding scheme, a pre-determined position is overwritten with the tag information. This scheme, however, proposes to modify the architecture of legacy systems and thus violates one of the rules mandated by the FCC [2].

2.2 System Model

For clarity purposes, we define a few notations that will be used in the rest of this thesis.

Table 2.1: Notations

$\mathcal{M}$	Set of channels licensed to a PRN
p_{md}	Probability of mis-detecting the state of an occupied channel by the CR
p_{fa}	Probability of false alarm in sensing an idle channel by the CR
p_{busy}	Probability that the channel is occupied
p_{idle}	Probability that the channel is idle
$\hat{p}_{busy}$	Probability that the channel is sensed as busy by the helper node
$\hat{p}_{idle}$	Probability that the channel is sensed as idle by the helper node
p_{rej}	Probability that the CR thinks there is an attack while there is none
p_{acc}	Probability of the CR incorrectly detects the presence of PUE when there is none
ε	Threshold to decide the rejection or acceptance of an occupancy vector
p_k	Probability that k out of m available channels are busy

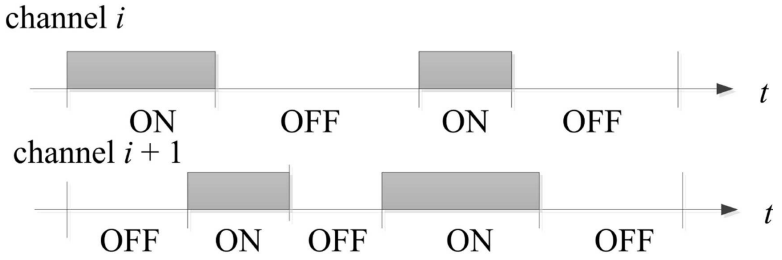

Figure 2.2: PU activity modeled as semi-Markov ON/OFF model for channels i and $i+1$.

Our system consists of a set of PUs, co-existing with a CRN. PUs are licensed to use a fixed spectrum, which can be divided to a set $\mathcal{M} = \{1, 2, \ldots, m\}$ of m orthogonal frequency bands, referred to as *channels*. The PU traffic is modelled after a semi-Markov ON-OFF process in which the channel state alternates between busy/ON and idle/OFF periods as shown in Figure 2.1. We assume that the channels are licensed to independently operating PUs and hence the state of a channel i is independent of the state of other channels. It has been verified that PU networks follow a semi-Markov model in a variety of scenarios [33,34]. We assume that the length of ON-OFF periods follow a geometric distribution with a transition from ON to OFF state occurring with probability q_i and a transition from OFF to ON state occurring with probability p_i. Figure 2.2 shows the PU activity at two channels, i and $i+1$ when the semi-Markov model is used. These assumptions have been extensively adopted in analyses of CRN performance in [35–37]. Hence, the probability that a channel is idle is given by

$$p_{idle} = \frac{q_i}{q_i + p_i}. \tag{2.2}$$

Let N be the random variable denoting the number of idle channels in the system. Also, assume that all the channels have the same traffic characteristics. Therefore, the probability mass function for N can be written as,

$$\Pr[N = k] = \binom{m}{k} p_{idle}^{k} (1 - p_{idle})^{m-k}. \tag{2.3}$$

Each channel i is assumed to be busy with a probability p_{busy} and idle with a probability

of p_{idle}. The PUs are assumed to be stationary (e.g., TV or cellular towers). The SUs are allowed to opportunistically use the set of channels $\mathcal{M}$, if they do not cause interference on PU communications. For this purpose, SUs are fitted with cognitive radio capabilities that can sense the spectrum using methods such as energy detection, cyclostationary feature extraction, and pilot signals [3, 6–8]. The SUs are assumed to be mobile. To provide PU signal authentication, we introduce a set of stationary helper nodes H, also equipped with cognitive radio capabilities. Helpers cover the geographical area where SUs are deployed. To securely communicate with SUs, helpers are initialized with public/private keys and certificates from a trusted authority. We assume that a dedicated common control channel is available in order for helper nodes to communicate with the SUs. Existence of a control channel is assumed in the majority of cooperative sensing protocols [26, 32] and CRN MAC designs [27, 38]. This channel is used for the purpose of communicating spectrum sensing information. Finally, helpers are assumed to be loosely synchronized.

2.3 Sensing Model

We assume an imperfect sensing model for the spectrum sensing process performed by any of the system participants. In this model, the status of a channel i is subject to erroneous state determination due to misdetection or false alarm. In particular, due to the phenomena of multipath and shadowing of the PU signal [39, 40], the probability that an idle channel is sensed busy (false alarm) is p_{fa} and the probability that an occupied channel is sensed idle (misdetection) is p_{md}. For simplicity, we assume that p_{fa} and p_{md} have the same value for every channel i. Further, we also assume that errors in the determination of the channel state occur independently at every channel and at every CR. These assumptions have been shown to be truthful since the received signal decorrelates fast in space and frequency [41].

Huang et al. analyze the misdetetction and false alarm models using the hypothesis in equation (2.1). Here, the probability of misdetection (p_{md}) can be written as

$$p_{md} = P_r\{Y < \gamma | H_1\}, \tag{2.4}$$

where Y is the energy of the received signal at a frequency band of interest and measured over the sensing period, and γ is a pre-specified energy threshold that indicates the presence or absence of PU activity. The probability that an idle channel is falsely estimated to be busy can be written as

$$p_{fa} = P_r\{Y > \gamma | H_0\}, \tag{2.5}$$

where H_0 is the hypothesis that no PU activity is present.

2.4 Threat Model

The goal of the adversary is to mislead the SUs regarding the available spectrum opportunities, thus preventing them from utilizing idle channels. To achieve his goal, the adversary is capable of emulating the primary radio signal characteristics. This can be easily achieved if the adversary is equipped with a software defined radio, or is capable of recording and replaying primary radio signals. While the adversary can be present at any location within the deployment area, we assume that he cannot place a transceiver in close proximity (within a few feet) to a PU. We assume that the PUs are physically secure, as mandated by the FCC. We further assume that some of the helpers deployed for PU signal authentication purposes can be compromised, thus providing false spectrum sensing information.

CHAPTER 3

Primary User Authentication System

3.1 System Architecture

The problem of authenticating the PU signal at the SU can be modelled as a two-party authentication problem. The latter is well studied in the literature and can be addressed using known cryptographic primitives such as public key, or symmetric key cryptography [31]. The technical challenge in applying such methods for PU signal authentication, however, is that, according to the FCC regulations [10], no modifications are allowed at the PU network.

Alternatively, SUs may authenticate PU signals by exploiting the unique characteristics of the RF channel. It has been shown that *link signatures* can be used to distinguish RF sources positioned at distinct locations [20,42,43]. For an SU sensing the spectrum, as long as the location of a PU remains static, the RF characteristics of the PU's transmission can serve as a unique signature for PU authentication. This is achieved by sampling the RF channel during a training period and extracting unique features of the RF channel such as the impulse response [20, 42, 43]. However, the RF signature between a PU and an SU changes if the SU is mobile, leading to frequent repetition of the training process. This requirement poses additional challenges that have to be addressed. First, the training period for extracting the RF signal has to be kept short so that the sensing process remains within the mandated period of two seconds [10]. A fast moving SU would have to devote a significant amount of time in obtaining the received RF signature in order to authenticate its sensing results. Second, SUs must have a mechanism for authenticating the PU training signals, every time their location changes.

To overcome the aforementioned challenges, we propose a PU authentication system that relies on the deployment of stationary helper nodes. These nodes are responsible for, (a) authenticating the PU signal and, (b) broadcasting spectrum status information. Initially,

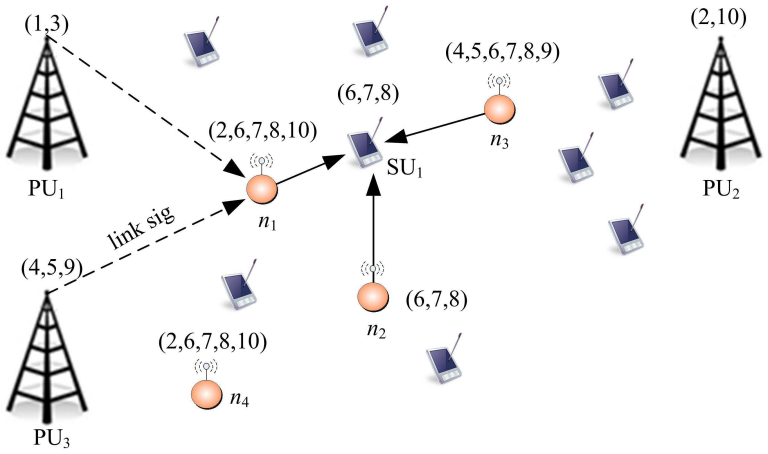

Figure 3.1: System architecture.

the helpers authenticate the PU signal using link signatures. Since both the helpers and the PUs are stationary, there is no need for frequent repetition of the training process after the initial training is completed. In the second phase, the helpers convey spectrum availability information to the SUs via a secure broadcast operation. This design can accommodate mobile SUs that do not need to be trained with every location change. An example of the proposed system architecture is shown in Figure 3.1. Helper nodes, n_1, n_2, n_3, and n_4 sense the activity of three PUs. The helper nodes authenticate the PU signals using link signatures and sense the channels to determine their status. As shown in Figure 3.1, n_1 senses that channels $(2, 6, 7, 8, 10)$ are free, n_2 senses that channels $(6, 7, 8)$ are free, n_3 senses that channels $(4, 5, 6, 7, 8, 9)$ are free, and n_4 senses that channels $(2, 6, 7, 8, 10)$. This spectrum information is conveyed to the SUs, who compute the idle portion of the spectrum. Based on the received information from helpers n_1, n_2, and n_3, SU_1 determines that channels $6, 7$, and 8 are idle.

We now give some preliminary information on link signatures which are used for validating PU signals, before we discuss the details of the PU authentication mechanism.

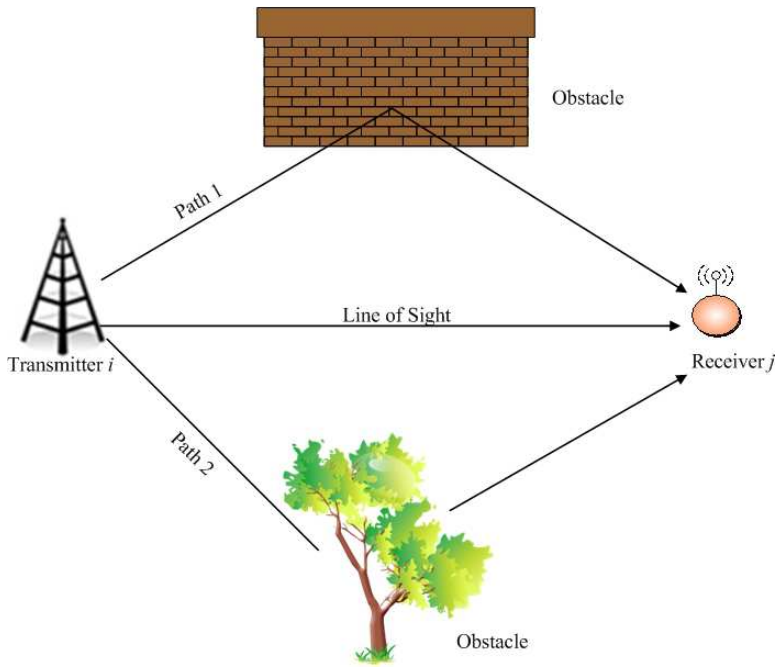

Figure 3.2: Multipath effect in a transmission between two nodes.

3.2 Location Distinction using Link Signatures

When a radio signal is transmitted over the air, it propagates in multiple paths due to reflection, scattering and diffraction. Hence, multiple copies of the transmitted signal are received at the receiver [20]. Figure 3.2 shows the multipath effect between a transmitting node i and receiving node j. Node j receives the signal transmitted by node i via three different paths. Each signal follows a path of different length, thus taking a different amount of time to reach the receiver. Moreover, each signal undergoes a different attenuation and phase shift per path. At the receiver, multiple copies of the transmitted signal are received, each copy arriving at a different time and with different amplitude and phase. Hence, the received signal is a linear combination of the transmitted signal. For the channel between transmitter i and receiver j, the channel impulse response [44, 45] is given by,

$$h_{ij}(t) = \sum_{l=1}^{L} a_l e^{j\phi_l} \delta(t - t_l), \tag{3.1}$$

where L is the total number of paths, $\delta(t)$ is the Dirac delta function, and a_l, ϕ_l and t_l are the channel gain, phase delay, and time delay for the l^{th} multipath component respectively. Hence, the channel impulse response is the superposition of many impulses, each one representing a single path in the multiple paths of a link. The received signal $r(t)$ can be expressed as the convolution of the transmitted signal $s(t)$ and the channel impulse response $h_{ij}(t)$,

$$r(t) = h_{ij}(t) \star s(t),$$

where " $\star$ " denotes the convolution operation. To obtain the desired impulse response, operations in the frequency domain yield,

$$H_{ij}(f) = \frac{1}{P_s} S^*(f) R(f), \tag{3.2}$$

where P_s denotes the transmission power at the sender, and $X(f), X^*(f)$ denote the Fourier transform and the complex conjugate of the Fourier transform of a signal $x(t)$ respectively. The link signature of the n^{th} packet is given by

$$h_{ij}^n(t) = \frac{1}{P_s} F^{-1}\{S^*(f) R(f)\}, \tag{3.3}$$

where F^{-1} denotes the inverse Fourier transform. It is important to note that to construct a link signature, the transmitted signal must be known at the helper.

Patwari et al. suggested an algorithm using the link signatures defined above for location distinction [20]. The algorithm has two phases, a training phase and a verification phase. During the training phase, the receiver j computes a sampled version of the link signature

denoted by

$$h_{ij}^{(n)} = [h_{ij}^{(n)}(0), h_{ij}^{(n)}(T_r), h_{ij}^{(n)}(2T_r), ..., h_{ij}^{(n)}(kT_r)]. \tag{3.4}$$

where T_r denotes the sampling rate of the receiver and this signature contains $k+1$ samples. The receiver stores a history of $(N-1)$ such link signatures for $(N-1)$ different packet transmissions. This history for the link between i and j is represented by

$$\mathcal{H}_{ij} = [h_{ij}^{1}, h_{ij}^{2}, ..., h_{ij}^{(N-1)}]. \tag{3.5}$$

During the verification phase, for a newly measured link signature h^N, the receiver computes its distance from the historical average of $\mathcal{H}_{ij}$ as follows

$$l_{ij} = \frac{1}{\beta_{i,j}} \min_{h \in \mathcal{H}_{ij}} ||h - h^N||, \tag{3.6}$$

where l_{ij} is the normalized minimum Euclidean distance between the new measurement and the set of vectors in the history and $\beta_{i,j}$ denotes the average distance between pairs of vectors in the history. If l_{ij} is above a predetermined threshold, a location change is detected. If not, the new measurement also represents a signature of the link between i and j and is added to the history of signatures. The oldest one can be discarded if there is a space constraint. Authors in [20] experimentally prove that the link signature between a pair of nodes fails to pass the verification test if one of the nodes changes its position by more than 3 m. Hence, even a small change in location can be detected. We use the same idea to check whether a signal has originated from a PU at a known location or from an adversary at a different location.

3.3 Authentication Mechanism

In this section, we describe the two phases of our spectrum authentication mechanism, i.e., the authentication of the PU signal at the helpers and the secure broadcasting of spectrum status information from the helpers to the SUs.

3.3.1 Phase I: PU Signal Authentication at the Helpers

To authenticate PU signals, a location distinction mechanism using multipath-based link signatures is employed. During Phase I, helpers sample PU activity on every channel of the PU network in order to create a link signature for each channel. The helpers utilize known pilot signals typically transmitted by the PUs for synchronization purposes. For instance, digital TV transmissions consist of a sequence of segments. For every 313 segments, a Data Field Sync segment of one known 511-bit PN sequence, and three known 63-bit PN sequences is used for synchronization [46]. Given that the frequency response $S_i(f)$ of a PN sequence is approximately flat within the transmitted frequency band, the channel frequency response $H_{ij}(f)$ can be computed based on equation (3.2).

To obtain the impulse response, the helper samples the PU signal during the transmission of the known sequence and stores the necessary samples to robustly "fingerprint" the fixed RF channel. During this training phase, which needs to be performed only once, it is assumed that no adversary is present to emulate PU activity (the training is performed during a supervised system deployment phase that is assumed to be secure and free of adversaries). Once a link signature for a given PU has been constructed, the helper can authenticate subsequent transmissions by comparing their characteristics to the stored link signature.

The helper continues to sample the RF channel for keeping an up-to-date history of the channel's multipath components and their temporal variations. The history $\mathcal{H}_{ij}$ is updated each time PU activity is sensed. Once the comparison with the threshold value validates that the channel is being occupied by a PU, $h_{ij}^{(N)}(t)$ is considered the new, valid link signature. The oldest $h_{ij}(t)$ vector which is stored in $\mathcal{H}_{ij}$ is discarded and the new vector is added. Though the algorithm in [20] is used for location distinction, we extend it to our work to validate whether a signal is from a PU which is stationary.

Using link signatures, a helper i constructs an occupancy vector V_i indicating the set of channels where legitimate PUs are active. V_i is an m-bit vector (m is the number of channels of the legacy system), with $V_i(j) = 1$ if $\mathcal{M}(j)$ is occupied by a PU, and zero otherwise. For instance, in a system with $m = 10$ channels, an occupancy vector $V = [1001010000]$ indicates

that channels 1,4 and 6 are occupied by legitimate PUs.

It has been mandated by FCC that if a PU starts transmission on a channel, the SU occupying that channel should vacate it within two seconds [10]. Therefore, the helper nodes continuously sense the channels for detecting a valid PU signal. In case the helper node senses PU activity on a free channel, or senses a previously occupied channel to become idle, it updates its occupancy vector to all the neighboring SUs.

3.3.2 Phase II: Secure Distribution of Spectrum Information to the SUs

In this phase, the helpers distribute spectrum information to the SUs. Contrary to the work in [1], in our design, this is achieved using solely cryptographic methods. This is preferred to avoid the need for frequent SU training due to mobility. To update the spectrum state to nearby SUs, a helper transmits the following information.

$$g_i : m_i || sig_{sk_i}(m_i), \quad m_i : V_i || L_i || SN_i. \tag{3.7}$$

In (3.7), V_i is the occupancy vector of helper i, $L_i = (X_i, Y_i)$ is the location of helper i, SN_i is the transmission sequence number used for verifying the freshness of V_i, and $sig_{sk_i}(m_i)$ is the signature of i on m_i using $i's$ private key sk_i. To avoid the frequent broadcast of spectrum information, the helpers update the SUs if, (a) a change in PU activity has been sensed, or (b) an SU moving to a new location has requested for an update. Note that for PUs such as TV stations, the dynamics of PU activity is expected to be low (in the order of hours). Therefore, while the helpers continuously monitor the spectrum status, a frequent update of the SUs may not be necessary. On the other hand, for other types of PU networks such as cellular networks, PU activity can be more dynamic.

Once an SU node j has obtained the occupancy vectors V_i from nearby helpers, it executes the Spectrum Authentication (SA) algorithm shown in Algorithm 1. Here, we assume that the network of helpers is loosely synchronized to the same transmission sequence number. The SA algorithm includes several cryptographic and topology consistency checks to ensure that the spectrum information obtained by SUs is authentic and fresh.

Algorithm 1 Spectrum Authentication (SA) Algorithm

for all $i \in N_i$ **do**
  if $sig_{sk_i}(m_i) = false$ **then**
    discard V_i
  end if
end for
for all $i \in V_j$ **do**
  if $SN_i \leq SN_{stored}$ **then**
    discard V_i
  end if
end for
for all $a, b \in V_i$ **do**
  if $|L_a - L_b| \leq 2r_h$ **then**
    $V_j = \bigcup_{i \in N_i} V_i$
  end if
end for

Step 1: Let $N_i = \{j | d_{ij} \leq r_h\}$ denote the set of helpers within the communication range of an SU i. In step 1, SU i collects all $g_j, j \in N_i$.

Step 2: For each $j \in N_i$, the SU i verifies the authenticity and integrity of m_j using $sig_{sk_j}(m_j)$. Messages m_j that fail to be authenticated are discarded.

Step 3: For each $j \in N_i$, the SU i verifies that $SN_j > SN_{stored}$ and $SN_j = SN_k, j, k \in N_i, j \neq k$. Since the helpers are assumed to be loosely synchronized, they must use the same sequence number. All $g_j's$ that do not meet the freshness requirement are rejected.

Step 4: SU j performs a location consistency test by verifying that

$$\mid L_j - L_k \mid \leqslant 2r_h, \forall j, k \in N_i. \tag{3.8}$$

Step 5: If the location consistency check is consistent, the SU determines the occupancy vector V_i using the OR operator.

$$V_i = \bigcup_{j \in N_i} V_j \tag{3.9}$$

Step 6: If the location consistency check fails, the helper resolution algorithm is invoked.

This algorithm identifies legitimate helpers from emulated ones (see Chapter 4).

Step 7: Once all emulated messages are discarded, the occupancy vector V_i is computed as in Step 5.

An application of the SA algorithm is explained on the topology of Figure 3.1. SU_1 listens to the helpers, n_1, n_2 and n_3 and their occupancy vectors, m_1, m_2 and m_3. According to Step 2, SU_1 verifies the signature on each of the occupancy vectors and discards the vectors when the signature check fails. Assume that the signature check on m_1 fails. Hence, m_1 is discarded. SU_1 considers only m_2 and m_3 for further checks. According to Step 3, the sequence number on m_2 and m_3 is checked. If SN_2 and SN_3 are both greater than the previously stored sequence number, then both m_2 and m_3 are accepted. In Step 4, SU_1 verifies that $\mid L_2 - L_3 \mid \leqslant 2r_h$. In step 5, SU_1 performs an OR operation between m_2 and m_3 to resort to occupancy vector $V_1 = [1111100011]$ (here, channels 6,7 and 8 are free). If the location consistency check fails, further checks are done as explained in later algorithms.

CHAPTER 4

Security and Theoretical Analysis

In this chapter, we show that the proposed PU authentication system is robust to various possible security threats.

4.1 PU emulation attack

We first show that our method is immune to direct PUE attacks. In a direct PUE attack, the goal of the adversary is to impersonate the features of a PU signal on the idle portion of the spectrum. This can be achieved by mimicking features of PU transmissions such as power, modulation type, synchronization sequences etc., or by recording and replaying PU transmissions [1, 17]. In this attack, the adversary must convince helpers that the emulated signal originates from an authentic PU.

Consider an adversary who is emulating a PU signal. The helper node will perform link signature verification on the emulated signal, as described in Chapter 3. In particular, the helper node calculates the channel impulse response of the newly obtained signal as explained in equation (3.4). The newly obtained impulse response is $h^{(new)}$. The helper calculates the minimum distance between the history of signatures $\mathcal{H}_{ij}$ and $h^{(new)}$ as follows.

$$l_{ij} = \frac{1}{\beta_{i,j}} \min_{h \in \mathcal{H}_{ij}} ||h - h^{new}||, \tag{4.1}$$

If l_{ij} exceeds a pre-determined threshold, then the helper decides that the measured link signature is from a different link and hence not indicative of PU activity.

In order for a PUE attack to be successful, the difference between the link signatures must be less than the threshold value. Though the adversary has emulated the characteristics of a PU transmission, the channel between the helper node and the adversary is different from the channel between the PU and the helper node. Because we assume that PUs such as TV

towers, cellular towers etc. are physically protected, as recommended by FCC regulations, it would not be possible to place an emulation transmitter close to a PU. Therefore, in this case, $h_{ij}^{(new)}$ fails the link signature validation. Therefore, the occupancy vectors constructed by the helpers accurately reflect the PU activity.

4.2 Helper Impersonation Attacks

The adversary may attempt to impersonate a helper in order to provide false occupancy vectors to the SU. The use of cryptographic signatures for authenticating the broadcast of the messages m_i containing the occupancy vectors, prevent the adversary from fabricating false spectrum information.

Consider a message g_i transmitted by helper i containing vector V_i. Message g_i contains m_i and signature, $sig_{sk_i}(m_i)$. If the adversary modifies the occupancy vector V_i to $V_i^{'}$, the signature verification test would fail since the message m_i is used as input to the signature generation and verification algorithms. The adversary must possess the secret key sk_i of the helper node in order to generate a valid signature.

Without the opportunity of fabricating authentic messages, the adversary may choose to replay old ones that were recorded during earlier broadcasts. These replays will pass the signature verification test at the SUs since they originated from legitimate helpers and contain valid signatures. To avoid such replay attacks, the transmission sequence number SN_i is included with each broadcast message m_i. Assuming that an SU under attack hears at least one legitimate helper, the SN of the legitimate helper will be different (larger) than the SN of the replays. Here, we exploit the fact that the network of helpers is loosely synchronized to the same SN. If an SU receives m_is with older SN_is, it discards them as old replays.

If the SUs are not guaranteed to be within range of at least one legitimate helper at all times, it is possible that replay attacks are successful. To deal with cases of SUs isolated from legitimate helpers, a stronger condition of synchronization between the helpers and the SUs is required. The helpers timestamp messages m_i to prevent stale information from

being replayed. Using the timestamp, SUs can reject replays even if fresh broadcasts from legitimate helpers are not available.

This can be done as follows. The message transmitted by a helper g_i becomes

$$g_i : m_i||sig_{sk_i}(m_i), \quad m_i : V_i||L_i||t_i, \tag{4.2}$$

where t_i is the timestamp generated by helper i before the message is transmitted. An SU j receiving the transmitted message at time $t_i^{'}$ checks if

$$t_i^{'} - t_i \leq \gamma_t, \quad \gamma_t = t_{tr} + t_p + t_\delta. \tag{4.3}$$

where t_{tr} denotes the transmission delay for g_i, t_p denotes the propagation delay which is upper bounded by r_h/c sec, where r_h is the helper range and c is the propagation speed of electromagnetic waves over the air (e.g. $c \approx 3 \times 10^8 m/sec$ in vacuum), and t_δ is the processing delay for the time a packet is timestamped at the helper, until its reception is recorded at the receiver, plus the upper bound of the synchronization accuracy of the entire system. Note here that an adversary replaying older messages from legitimate helpers will fail to authenticate the replay messages, if it is subjected to the same processing delays as SU nodes.

Finally, for a loosely synchronized network of helpers, the adversary may replay spectrum authentication messages via a wormhole tunnel between two (or more) parts of the network [47]. This attack is depicted in Figure 4.1. The adversary deploys a fast link (wired or long-range wireless) between two parts of the network A and B. He then records broadcasted information on one end, transmits it via the wormhole tunnel to the other end, and replays it. Because messages m_i transmitted by the helpers are only *loosely* synchronized to the same SN value, a fast tunnelling and replay may contain m_is with up-to-date SN_is.

Wormhole attacks are detected by the location consistency check of the SA algorithm. A broadcast received by an SU must originate from helpers located within a radius r_h from the SU's location. Therefore, the pairwise distance between two helpers a, b heard at the

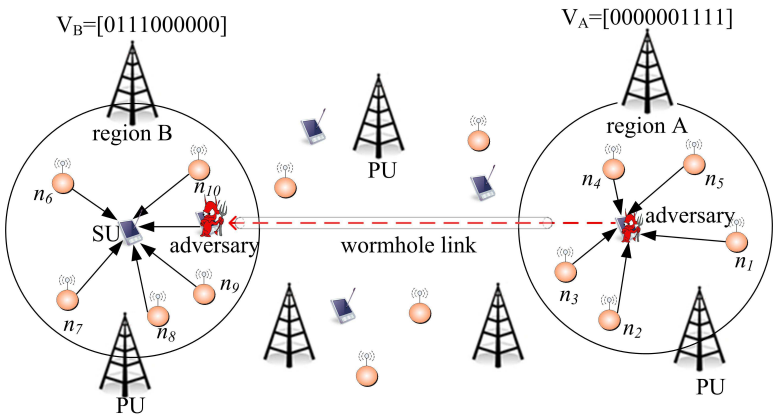

Figure 4.1: Replay of helper broadcasts via a wormhole tunnel. Scenario 1: V_A = [0000001111], V_B = [0111000000], V^* = [0111000000]. Scenario 2: Adversary emulates PU signal in channels 7,8,9 and 10 so that V^* = [0111001111].

same SU, cannot be longer than $2r_h$. The SU uses the location consistency check to verify that the set of helpers it hears is consistent. If spectrum authentication messages from part A are replayed via a wormhole tunnel to part B, the helpers' locations included in each m_i will fail the location consistency test and reveal the wormhole attack.

If the adversary chooses the wormhole origin location A to be too close to the destination location B in order to pass the location consistency check, this attack is expected to have a very limited effect since helpers at both areas A and B will sense similar PU activity. The adversary can record but not change what is being sensed by the helpers. Note that in our location consistency check method, SUs are not required to be aware of their own location (no GPS is necessary at the SUs). The location information of the helpers is sufficient to perform the test. However, without their own location information, the SU cannot distinguish the set of helpers located nearby from the ones replayed. To resolve this ambiguity, the SU utilizes the Helper Resolution (HR) algorithm.

We first analyze the scenario where, the adversary simply replays information from far away helpers. An SU that receives information from an inconsistent group of helpers G_i, creates two groups, G_A, G_B that correspond to consistent subgroups of helpers[1]. G_A and

[1]Our method can be easily extended to more than two groups.

G_B are formed such that a helper node $a \in G_A$ and helper node $b \in G_B$ are found to be in locations that satisfy $|L_a - L_b| > 2r_h$. A node $k \in G_i$ is assigned to G_A if $|L_a - L_k| \leq 2r_h$ and assigned to G_B if $|L_b - L_k| \leq 2r_h$. Note that a node k can simultaneously belong to two groups if it satisfies both conditions. Let V_A be the vector resulting from performing an OR operation on all vectors in G_A and V_B be the corresponding occupancy vector for G_B. Also let V^* be the occupancy vector when the SU senses the spectrum on its own.

Given the spatial variation of PU activity, occupancy vectors V_A and V_B, corresponding to G_A and G_B are likely to be different, with the occupancy vector corresponding to helpers nearby the SU being similar to V^*. On the other hand, the occupancy vector corresponding to replayed information likely indicates idle channels as occupied. To exploit this inconsistency, for each of the two vectors V_A and V_B, the SU computes counters c_A and c_B that indicate the number of channels that were sensed idle in V^*, but were marked occupied in V_A and V_B respectively. For example, counter c_A is increased by one if, for the i^{th} channel, $V^*(i) = 0$ and $V_A(i) = 1$. If any of the counters, c_A, c_B increases more than a threshold value ε, the corresponding occupancy vector is rejected as a replay. The justification for considering only flips from 0 to 1 when comparing V^* with a vector V_X of a consistent group of helpers G_X is the fact that the adversary cannot easily eliminate the presence of PU activity[2]. That is, if a PU were to be active on a channel i, that channel would be sensed busy by the SU making the corresponding value $V^*(i) = 1$. This outcome cannot be influenced by any malicious activity. On the other hand, a bit flip from $V^*(i) = 1$ to $V_X(i) = 0$ (i.e., a channel i to be sensed occupied by the SU under attack, but idle by the set of helpers G_X) could be the outcome of a successful wormhole attack. This is because the adversary can relay a signal from a helper that senses an active PU on channel i via the wormhole, and replay it to the SU. Since the SU does not use link signatures to authenticate activity recorded by G_X, this PUE attack will be successful. Therefore, flips from 1 to 0 are not taken into consideration when computing counters c_X for each consistent helper group G_X.

Step 1: Let G_i denote the group of helpers heard by an SU i. In step 1, SU i collects all

[2]Eliminating the presence of a signal requires the transmission of a cancelling signal for the SU under attack. Derivation of the cancelling signal requires perfect channel information (i.e. channel gain and phase) at the receiver's location which is not possible due to the randomness of the multipath components.

$g_j, j \in G_i$.

Step 2: The SU initializes two groups G_A and G_B by placing two helpers, $a, b \in G_i$ to each group respectively with $|L_a - L_b| > 2r_h$. Then, $G_A = \{j \mid |L_a - L_j| \leq 2r_h, j \in G_i\}$ and $G_B = \{j \mid |L_b - L_j| \leq 2r_h, j \in G_i\}$.

Step 3: The SU performs an OR operation between the occupancy vectors of each subgroup to obtain $V_A = \bigcup_{i \in G_A} V_i$ and $V_B = \bigcup_{i \in G_B} V_i$

Step 4: The SU senses occupancy vector V^*

Step 5: $\forall i \in \mathcal{M}$ if $V_{G_A}(i) = 1$ and $V^*(i) = 0$, then increase counter c_A by one unit. Similarly, $\forall i \in \mathcal{M}$ if $V_{G_B}(i) = 1$ and $V^*(i) = 0$, then increase counter c_B by one unit.

Step 6: Both counters c_A and c_B are compared with the predetermined threshold ε. If $c_A > \varepsilon$, discard V_A as a replay. If $c_B > \varepsilon$, discard V_B as a replay.

Step 7: If no occupancy vector is accepted, use a timing based method to determine the valid group of helpers.

The pseudo-code for the HR algorithm is given in Algorithm 2. An application of the HR algorithm for the topology of Figure 4.1 is explained as follows. The SU has identified that $|L_1 - L_6| > 2r_h$. Based on the distances of all helpers from L_1 and L_6, the SU creates subgroups $G_A = \{n_1, n_2, n_3, n_4, n_5\}$ and $G_B = \{n_6, n_7, n_8, n_9, n_{10}\}$. The corresponding occupancy vectors are $V_A = \cup_{i=1}^{5} V_i = [0000001111]$ and $V_B = \cup_{i=6}^{10} V_i = [0111000000]$. Moreover, $V^* = [0111000000]$, since the SU is located in region B. The detection threshold value is set to $\varepsilon = 2$. The counter for G_A is $c_A = 4 > \varepsilon$ while the counter for G_B is $c_B = 0 < \varepsilon$. Therefore, V_A is discarded and the SU accepts V_B as the valid occupancy vector. We now show that the adversary can launch a more elaborate attack described in the following section.

4.2.1 Combination of PUE attacks with wormhole attacks

In this attack scenario, the adversary combines a wormhole attack with a PUE attack. The goal of the PUE attack is to distort the occupancy vector V^* sensed by the SU. This is possible because the PU signal is not authenticated using link signatures at the SU. This scenario is illustrated with the assistance of Figure 4.1. The adversary replays spectrum

Algorithm 2 Helper Resolution (HR) Algorithm

Initialize
G_i: set of helpers heard by SU_i
V^*: Occupancy vector sensed by SU_i
$c_A = 0, c_B = 0$
find $a, b \in G_i$, s.t. $|L_a - L_b| > 2r_h$
$G_A = \{j | d_{aj} \leq 2r_h, j \in G_i\}$
$G_B = \{j | d_{bj} \leq 2r_h, j \in G_i\}$
$V_{G_A} = \bigcup_{i \in G_A} V_i$ and $V_{G_B} = \bigcup_{i \in G_B} V_i$ and V^*
for $i = 1 \rightarrow m$ **do**
  if $V_{G_A}(i) = 1$ and $V^*(i) = 0$ **then**
    $c_A = c_A + 1$
  end if
  if $V_{G_B}(i) = 1$ and $V^*(i) = 0$ **then**
    $c_B = c_B + 1$
  end if
end for
if $c_A > \varepsilon$ **then**
  discard V_{G_A}
end if
if $c_B > \varepsilon$ **then**
  discard V_{G_B}
end if

authentication messages from region A to region B. However, in order to avoid the rejection of V_A based on the counter c_A, the adversary emulates PU activity close to the SU, at occupied channels in region A. Therefore, the occupancy vector at the SU becomes similar to V^*. In this case, both counters c_A and c_B remain below ε for both groups G_A and G_B. For instance, in the example of 4.1, the adversary emulates PU activity on the channels $7, 8, 9, 10$ so that $V^* = [0111001111]$ and $c_A = 0$. To resolve this ambiguity, timing-based methods can be employed to identify which of the conflicting group of helpers is close to the SU [48]. C̃apkun et al. suggested a commitment scheme to securely determine a lower bound on the distance between two nodes [48]. The distance bounding scheme presented in [48] makes sure that any node u cannot claim to be located at a distance closer than the physical distance between u and v. The pseudocode for the distance bounding protocol in [48] is in

Table 4.1. If the SU performs this algorithm, one helper from each group, it can select the closest group of helpers as the valid one and compute the corresponding occupancy vector.

In our system, the SU is the verifier and the helper node is the claimant. Therefore, the helper node's position is tested using the commitment scheme. In the first step of this protocol, the claimant (helper node) u commits to a random value n_u. Here, $commitment(c, d) = commitment(n_u)$, where c, d are the commitment and decommitment values, respectively. The value c is sent to SU v. The verifier v replies with a challenge nonce n_v which is sent to u in the reverse bit order. This is done so that u can reply to this message only once all the bits from v are received. Once v transmits all the n_v bits out, it starts a timer, t_v. The helper node responds immediately with the value $n_u \oplus n_v$ upon receiving the challenge from v. The SU stops the timer with reception of $n_u \oplus n_v$ and calculates the distance between itself and the helper node. In the final step of the protocol, u authenticates itself to v by revealing the decommitment value. In the final step, u sends $n_u, n_v, d, sig_{sk_u}(u, n_u, n_v, d)$ to v. Then v can verify n_u, which is obtained by opening the commitment value pair. The SU can verify the authenticity of the message sent by the helper node u by checking the included signature.

Table 4.1: Protocol to calculate distance between SU and helper node

Helper Node	: Generate random nonce, n_u
	: Commitment(c,d) = Commitment(n_u)
Helper Node $\rightarrow$ SU	: c
SU	: Generate random nonce n_v
SU$\rightarrow$Helper node	: n_v (The bits are sent in the reverse order, MSB to LSB), Start timer
Helper node $\rightarrow$ SU	: $n_v \oplus n_u$ (bits sent in normal order LSB to MSB)
SU	: Measure time t between sending and receiving
Helper node $\rightarrow$ SU	: $n_u, n_v, d, sig_{sk_v}(u, n_u, n_v, d)$
SU	: Find $n_u = open(c, d)$ and verify the signature

We emphasize that this challenge-response mechanism is not necessary if the SU has information about its location. By comparing the distance between itself and the helpers it overhears, it can easily reject helper information replayed from distant parts of the network.

4.3 Probabilistic Security Analysis

In this section, we present a probabilistic analysis on rejecting PUE attacks in the light of imperfect sensing. Specifically, we compute the following quantities[3].

- Probability of rejection p_{rej}: The probability that an SU i will erroneously reject the correct occupancy vector V_X, derived from the group $G_X = N_i$ of neighboring helpers.

- Probability of false acceptance p_{acc}: The probability that an SU i will erroneously accept an incorrect occupancy vector V_X, derived from a group of helpers $G_X \neq N_i$.

We now establish several preliminary results before we derive the probabilities of rejection and acceptance.

Proposition 1. *An SU i within the range of a set of neighboring helpers N_i, sets a channel $V_{N_i}(j)$ of its occupancy vector V_{N_i} to one (busy) with probability*

$$\hat{p}_{busy} \quad = \quad p_{busy}((1-p_{fa})^{|N_i|} - p_{md}^{|N_i|}) + (1-(1-p_{fa})^{|N_i|}). \tag{4.4}$$

where p_{busy} is the probability that a PU is active on a given channel j and p_{md}/p_{fa} are the probabilities of misdetection/false alarm due to imperfect sensing.

Proof. The proof follows in a straightforward manner due to the independence of the sensing process at each helper. Channel j is marked as busy by an SU if (a) a PU is active on channel j and at least one helper detects its activity, or, (b) there is no PU activity on channel j but at least one helper has a false alarm. These conditions are a consequence of the adoption of an OR rule for computing the occupancy vector at the SU. Because misdetection at each helper is an independent event (due to the fast signal decorrelation in space), condition (a) occurs with probability

[3]Here, we avoid the more intuitive terminologies of false alarm and misdetection in order to differentiate from the terms used to characterize the imperfect sensing process.

$$p_{busy}(1 - \prod_{N_i} p_{md}) = p_{busy}(1 - p_{md}^{|N_i|}). \tag{4.5}$$

In equation (4.5) the event that at least one of the helpers correctly detects a busy channel is complementary to the event that all helpers misdetect the state of the channel. The latter occurs with the probability $p_{md}^{|N_i|}$. Multiplying the probability of the complementary event with the probability p_{busy} that a PU occupies channel j yields equation (4.5).

Similarly, condition (b) occurs with probability

$$p_{idle}(1 - \prod_{N_i}(1 - p_{fa})) = p_{idle}(1 - (1 - p_{fa})^{|N_i|}). \tag{4.6}$$

Adding the probabilities of the two conditions yields Proposition 1.

$$\begin{aligned} \hat{p}_{busy} &= p_{busy}(1 - p_{md}^{|N_i|}) + p_{idle}(1 - (1 - p_{fa})^{|N_i|}) \\ &= p_{busy}(1 - p_{md}^{|N_i|}) + (1 - p_{busy})(1 - (1 - p_{fa})^{|N_i|}) \\ &= p_{busy}((1 - p_{fa})^{|N_i|} - p_{md}^{|N_i|}) + (1 - (1 - p_{fa})^{|N_i|}). \end{aligned} \tag{4.7}$$

□

Using Proposition 1, we can compute $\hat{p}_{idle}$ to be $(1 - \hat{p}_{busy})$ since sensing the medium as idle is the complementary event to sensing it as busy.

We are now interested in computing the probability that the jth bit of the occupancy vector V^* sensed by an SU is equal to $V^*(j) = 0$ when the equivalent bit in the occupancy vector V_{N_i} derived based on the helpers in neighbor set N_i is equal to 1. This event indicates a flip from zero to one when V^* is compared with V_{N_i} and increases the counter c_{N_i} by one unit. The probability of this event is given in the following proposition.

Proposition 2. *The probability that $V^*(j) = 0$ while $V_{N_i}(j) = 1$ is given by*

$$p_R = p_{busy}\big((1 - p_{md}^{|N_i|})p_{md} - (1 - p_{fa})(1 - (1 - p_{fa})^{|N_i|})\big) + (1 - p_{fa}(1 - (1 - p_{fa})^{|N_i|}).$$

Proof. In order for $V^*(j) = 0$ and $V_{N_i}(j) = 1$, the following conditions must be met: (a) the PU is active on channel j and at least one of the helpers detects its activity while the SU misdetects the PU activity, (b) the PU is idle on channel j and one of the helpers has a false alarm while the SU detects no activity.

Misdetection at each helper and the SU are independent events due to the fast decorrelation of the signal in space. Condition (a) occurs with probability

$$p_{busy}(1 - \prod_{N_i} p_{md})p_{md} = p_{busy}(1 - p_{md}^{|N_i|})p_{md}. \tag{4.8}$$

In equation (4.8) the event that at least one helper correctly detects the channel status is complementary to the event that all the helpers misdetect the status of the channel. The latter occurs with a probability $p_{md}^{|N_i|}$. Multiplying this event with the probability p_{busy} that a PU occupies the channel j and the probability p_{md} that the channel is sensed idle by the SU yields our result.

Similarly, condition (b) occurs with probability

$$p_{idle}(1 - p_{fa})(1 - \prod_{N_i}(1 - p_{fa})) = p_{idle}(1 - p_{fa})(1 - (1 - p_{fa})^{|N_i|}). \tag{4.9}$$

Adding the probabilities of these two conditions yields Proposition 2.

$$\begin{aligned} p_R &= p_{busy}(1 - p_{md}^{|N_i|})p_{md} + p_{idle}(1 - p_{fa})(1 - (1 - p_{fa})^{|N_i|}) \\ &= p_{busy}(1 - p_{md}^{|N_i|})p_{md} + (1 - p_{busy})(1 - p_{fa})(1 - (1 - p_{fa})^{|N_i|}) \\ &= p_{busy}\big((1 - p_{md}^{|N_i|})p_{md} - (1 - p_{fa})(1 - (1 - p_{fa})^{|N_i|})\big) + (1 - p_{fa}(1 - (1 - p_{fa})^{|N_i|}). \end{aligned}$$

□

Proposition 3. *An SU rejects a legitimate occupancy vector V_{N_i} due to the imperfection in*

channel sensing process with probability

$$p_{rej} = \sum_{k=\varepsilon}^{m} \Big(\sum_{j=\varepsilon}^{k} \binom{k}{j} p_R^j (1-p_R)^{k-j} \Big) p_k, \quad p_k = \binom{m}{k} p_{busy}^k (1-p_{busy}^{m-k}),$$

where m denotes the total number of channels, p_R denotes the probability of $V^*(j) = 0$ while $V_{N_i}(j) = 1$, ε denotes the threshold value for the counter c_{N_i} in order to detect a PUE attack, and p_k denotes the binomial probability of k out of m channels being occupied during the computation of the occupancy vector at the SU.

Proof. Let K denote a random variable that represents the number of channels that are occupied by PUs with $p_k = \Pr[K = k]$. To falsely detect a PUE, a flip from $V_{N_i}(j) = 1$ to $V^*(j) = 0$ must occur at least ε times on any j of the m available channels. Using the law of total probability by conditioning on the number of occupied channels i, we have

$$\begin{aligned} p_{rej} &= \sum_{k=\varepsilon}^{m} \Pr[c_{N_i} \geq \varepsilon | K = k] P_r[K = k] \\ &= \sum_{k=\varepsilon}^{m} \Big(\sum_{j=\varepsilon}^{k} \binom{k}{j} p_R^j (1-p_R)^{k-j} \Big) p_k, \end{aligned} \tag{4.10}$$

where, p_R is the probability given by Proposition 2. In equation (4.10), we have considered all possible values for the number of occupied channels k. In equation (4.10), we have utilized the fact that a flip from 0 to 1 on each channel independently occurs with probability p_R, and those flips on at least ε channels lead to the rejection of a correct vector. □

We now analyze the event that an SU fails to reject an occupancy vector that is replayed to the SU via a wormhole link, due to the imperfection in the channel sensing process.

Proposition 4. *An SU fails to reject an occupancy vector replayed via a wormhole link with probability*

$$p_{acc} = 1 - \Big(\sum_{k=\varepsilon}^{m} \Big(\sum_{j=\varepsilon}^{i} \binom{k}{j} p_C^j (1-p_C)^{k-j} \Big) p_k \Big),$$

where

$$p_k = \binom{m}{k} p_{busy}^{k}(1 - p_{busy}^{m-k}),$$

and

$$p_C = \hat{p}_{busy}(p_{busy}p_{md} + p_{idle}(1 - p_{fa})).$$

Proof. Let X denote the set of helpers whose broadcasts are recorded at the origin of the wormhole link. In order for an SU under a wormhole attack to accept replayed information originating from X, less that ε bit flips must occur between V^* and V_X. Given the independence in observations made by the SU and the helpers in X, we can write probability of accepting V_X as

$$\begin{aligned} p_{acc} &= 1 - p_{rej} \\ p_{acc} &= 1 - \Big(\sum_{k=\varepsilon}^{m} \Big(\sum_{j=\varepsilon}^{k} \binom{k}{j} p_C^{j}(1 - p_C)^{k-j}\Big) p_k\Big), \end{aligned}$$

where p_C is the probability that a channel is sensed busy by the group of helpers X at the origin of the wormhole link while the same channel is sensed idle at the region where SU performs sensing. This can be written as

$$\begin{aligned} p_C &= [(p_{busy}(1 - p_{md}^{|X|}) + p_{idle}(1 - (1 - p_{fa})^{|X|})][p_{busy}p_{md} + p_{idle}(1 - p_{fa})] \\ &= \hat{p}_{busy}(p_{busy}p_{md} + p_{idle}(1 - p_{fa})). \end{aligned} \tag{4.11}$$

□

CHAPTER 5

Reputation-Based Framework for Compromised Helpers

Until now we have assumed that the helper nodes are always honest. In this chapter, we consider the scenario where a helper node can be compromised by an adversary and broadcast false occupancy vectors.

Since our PU authentication method employs an OR operation in order to compute the authentic PU activity, a compromised helper can prove detrimental in obtaining spectrum opportunities. Consider an adversary trying to utilize a particular channel or a set of channels at all times. If the adversary can succeed in compromising one of the helpers, it can make the helper node modify the occupancy vector to its liking. In this case, SUs can be easily misled into accepting false channel information.

To address the problem of helper compromise, we adopt a reputation-based system, where helper nodes maintain reputation values of other helpers that is used to evaluate the trustworthiness of the information they provide. We design our framework to work in two phases. In the first phase, we assume that all helpers are honest and compute the list of commonly sensed channels between every pair of neighboring helpers. In the second phase, we assume that helper nodes can be compromised and use the channel lists created during the first phase to detect compromised helpers. To achieve this, we maintain helper reputation values based on the similarity of the occupancy vectors transmitted by neighboring helpers. In our work, we focus our attention on evaluating the truthfulness in a transmission of a helper and not on the reputation management aspect. Many reputation management systems have been proposed in the literature [49–53] and can be used in conjunction with our evaluation method. We now discuss the details of each of these steps.

5.1 Phase I: Derivation of Commonly Sensed Channels

To evaluate the trustworthiness of nearby helpers, we consider how the individual evaluations of each helper match the ongoing PU activity. Every helper is responsible for monitoring the activity of his neighbors. Consider helper i, monitoring the activity of helper j. In phase I, helper i builds the list of channels that are sensed both by i and j based on overheard occupancy vectors. In this phase, all helpers are assumed to be honest (system initialization). To generate the list VC_{ij} of commonly sensed channels between i and j, helper i records all occupancy vectors V_j broadcasted by j over a period of time T_0. If $V_i(e) = V_j(e) = 1$, then channel e is added to VC_{ij}. That is, if both helpers i and j report channel e to be busy, they must both be capable of sensing e and therefore e is added to VC_{ij}. Note here that channels for which $V_i(e) = V_j(e) = 0$ are not taken into account since it is possible that j cannot sense PU activity on channel e, thus always reporting a zero value at $V_j(e)$.

At the end of this phase, helper i maintains the list $VC_{ij} \subseteq V_i$ for each helper j within its communication range. The list VC_{ij} can be amended after period T_0, if a busy state is reported by helper j for any other channel. The list VC_{ij} is utilized in phase II for evaluating the reputation of the neighboring helpers.

5.2 Phase II: Helper Trustworthiness Evaluation

In this phase, every helper evaluates its neighbors based on the similarity of their occupancy vectors. This is done based on the outcome of a hypothesis test. We first provide a relevant definition.

Definition 1. Vector dissimilarity $d_{ij}(V_i, V_j)$**:** *The dissimilarity* d_{ij} *between the occupancy vectors* V_i, V_j *of two helpers* i, j *with a common list of channels* VC_{ij} *is denoted as the Hamming distance between* V_i *and* V_j *on the channels indicated by* VC_{ij}*. The vector dissimilarity is a measure of the disagreement of two neighboring helpers with respect to the channel state due to PU activity. Such a disagreement can be an aftermath of imperfect sensing or of a deliberate false occupancy vector reported by a compromised helper.*

The helper trustworthiness can be viewed as a choice between two events H_0 and H_1, H_0 being the hypothesis that helper j is honest and H_1 being the hypothesis that helper j is compromised.

$$\begin{aligned} H_0 &: \hat{d}_{ij} \leq \mu \quad (j \text{ is honest}) \\ H_1 &: \hat{d}_{ij} > \mu \quad (j \text{ is compromised}) \end{aligned} \tag{5.1}$$

where, μ is the mean of the Hamming distance distribution when helpers are honest and $\hat{d}_{ij}$ is the sample mean of d_{ij}. We now set the test statistic for our hypothesis. We know that for values of n ($n > 20$), we can approximate a binomial distribution to a normal distribution. Therefore, the test statistic can be written as

$$Z = (\hat{d}_{ij} - \mu)/(\sigma/\sqrt{n}) \tag{5.2}$$

where, μ is the mean of the distribution, $\hat{d}_{ij}$ is the sample mean, σ is the variance of the distribution and n is the number of samples over which $\hat{d}_{ij}$ is averaged.

We first calculate the value of μ mathematically. During system initialization, $d_{ij}(V_i, V_j)$ for two helpers i and j depends on imperfect sensing of the channels due to events of false alarm and misdetection.

Consider two helpers i, j. A channel is sensed as busy by i and idle by j or vice-versa with following probability

$$p_{busy}(1 - p_{md})p_{md} + p_{idle}p_{fa}(1 - p_{fa}). \tag{5.3}$$

Since either scenario leads to an increase in the Hamming distance d_{ij}, the probability for $V_i(e) \neq V_j(e)$ is given by

$$p_{diff} = 2(p_{busy}(1 - p_{md})p_{md}) + 2(p_{idle}(1 - p_{fa})p_{fa}). \tag{5.4}$$

Next, we find the probability that any k channels in the list VC_{ij} are different. This probability can be viewed as obtaining k success in a binomial distribution that has a total of $|VC_{ij}|$ trials.

$$\Pr[d_{ij} = k] \quad = \quad \binom{|VC_{ij}|}{k} p_{diff}^{k} (1 - p_{diff})^{|VC_{ij}|-k} \tag{5.5}$$

This is due to the fact that the events of false alarm and misdetection are assumed to occur independently at each channel. From the binomial distribution it follows that $\mu = |VC_{ij}|p_{diff}$ and $\sigma = |VC_{ij}|p_{diff}(1 - p_{diff})$.

We next calculate the Hamming distance experimentally between any two occupancy vectors over a period of time. Every time there is a change in the occupancy of the channels, helper nodes transmit an occupancy vector. A monitoring helper i computes the Hamming distance between its occupancy vector and the vector transmitted by j. After the collection of n such samples, we compute the sample mean $\hat{d}_{ij}$.

The sample mean $\hat{d}_{ij}$ is used in our test statistic in equation 5.2 for hypothesis testing as follows. Let α be the critical value for rejecting hypothesis H_0. If $Z > \alpha$ then, the hypothesis H_0 is rejected. This rejection means that the helper node is compromised. Using the outcome of this hypothesis testing, the monitoring helper can submit its recommendation to the reputation manage and adjust the reputation of neighbors accordingly.

CHAPTER 6

Simulations

In this chapter, we evaluate the performance of our PU authentication method under static and mobile SU network scenarios. In our evaluation, we employ the following metrics:

Helper Communication Overhead O_h: The average rate O_h that helpers need to update SUs with PU activity information.

Helper transmission power ratio: The average power that helpers need to transmit in order to enable PU authentication.

Probability of rejection p_{rej}: The probability of rejecting the occupancy vector obtained by a valid set of helpers.

Probability of acceptance p_{acc}: The probability of accepting an occupancy vector that is replayed via a wormhole link.

6.1 Simulation setup

In our evaluation, we consider the co-existence of a Cognitive Radio Network (CRN), a Primary Radio Network (PRN) and a Helper Node Network (HNN). The three co-existing networks are set up as follows:

Cellular PRN Setup: We consider the PRN to be a cellular network consisting of sixteen cells covering an area of 7 km x 7 km, as shown in Figure 6.1. We prefer the use of a cellular network over the recently opened TV white spaces due to the high dynamics of PU activity expected under a cellular scenario. To avoid interference between PUs, a separate set of frequency bands is assigned on adjacent cells. This assignment is performed according to the four color theorem [54], which guarantees that any planar map can be colored with at most four colors such that no two adjacent regions have the same color. For the network considered in our simulations, three colors suffice. The assignment of the various sets of

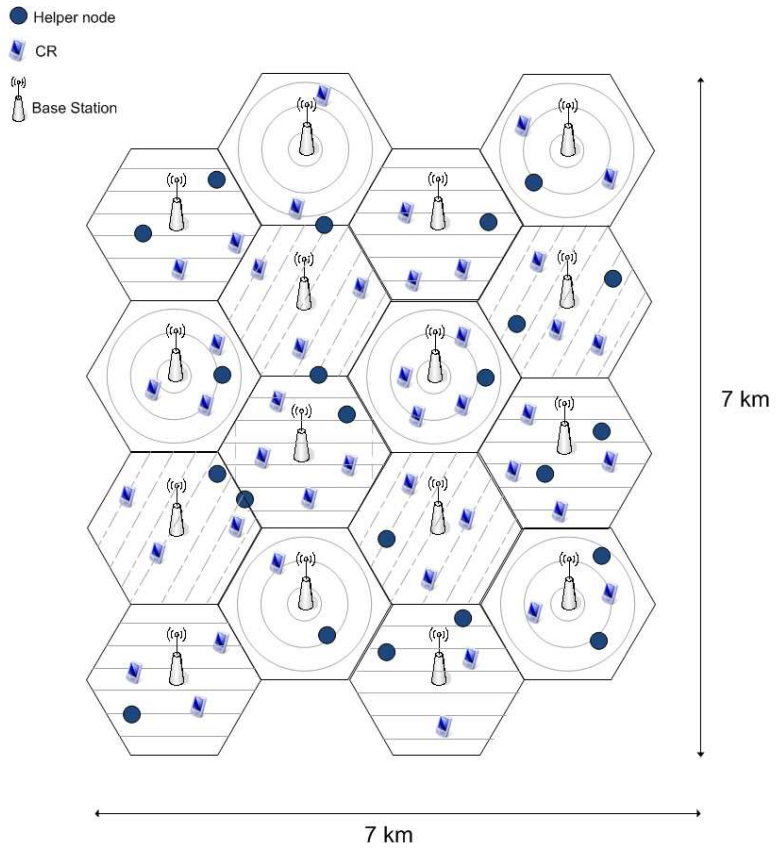

Figure 6.1: Evaluation set-up consisting of a cellular PRN, CRN and HNN. 10 channels are assigned per channel. Adjacent cells do not share any channels

frequency bands per cell according to the four color theorem is shown in Figure 6.1, where different shading patterns are used on various cells to indicate the corresponding frequency channel assignments. Each cell is assigned 10 frequency bands, summing to a total of 30 bands for the entire PRN. The PU transmission radius is set to 1.5 km (transmission radius for cell towers is known to vary anywhere from 1 km to 30 km [55]). Calls arrive at each cell tower following a Poisson process with an average rate of λ calls/min. Each call lasts a fixed period of time equal to $\mu = 5$ min.

CRN Setup: The CRN is randomly deployed within the PRN area. The communication range of each SU is set to 400 m. This is a typical range for CR devices [56, 57]. We consider both static and mobile CRNs. Mobile CRs are free to move within the PRN deployment

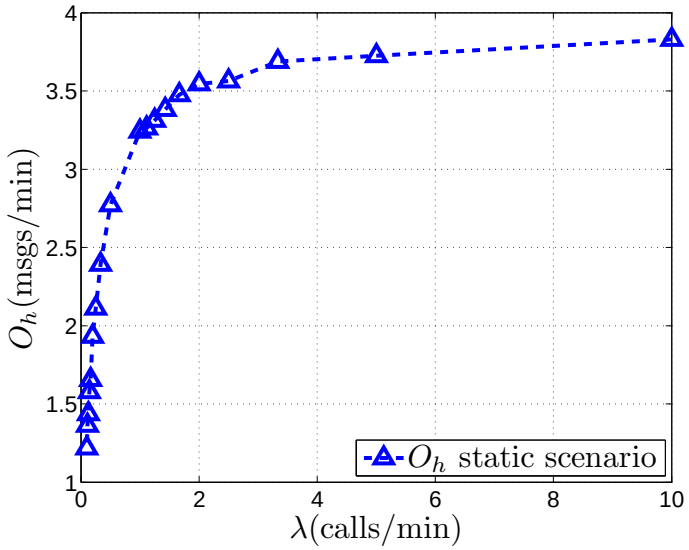

Figure 6.2: Communication overhead (helper rate) as a function of the call arrival rate at each PU

area according to the random waypoint model [58, 59].

HNN Setup: Helper nodes are placed within the deployment area such that they cover all locations of the SUs and sense all PU activity. Since the SUs are randomly deployed, we select a systematic grid deployment in order to reduce the number of helpers needed to achieve 1-coverage. Helpers are placed at the vertices of a triangular grid with side length equal to 200 m. The helper communication range is set to 400 m (helpers are also assumed to be CR devices). The set of helpers is assumed to be static. Every helper records the PU activity of the cell that it belongs to.

6.2 Helper Communication Overhead in Static CRN

We first evaluated the communication overhead introduced by helpers when broadcasting occupancy vectors to SUs when SUs were assumed to be static. In this case, helper nodes broadcast an occupancy vector only if they sense a change in the status of any channel.

Figure 6.2 shows the average rate O_h of transmitting occupancy vector messages as a function of the traffic arrival rate λ at each PU. We observe that the overhead rate increases

rapidly at smaller values of λ. This is due to the fact that most channels are idle for low arrival rates triggering several overhead messages. However, this trend flattens out as the available frequency bands saturate after $\lambda = 3$ calls/min, leading to a constant rate of change in the occupancy. As an extreme case, for the arrival rate of $\lambda = 10$ calls/min, several calls are blocked due to the high service rate ($\mu = 5$ min). These dropped calls do not contribute to the dynamics of the PU activity and thus O_h remains fairly constant.

6.3 Communication Overhead in Mobile CRNs

In the second set of experiments, we considered a mobile CRN. SUs were assumed to move around the deployment area according to the random waypoint model [58, 59]. In particular, at every minute, an SU i picks a random direction $\theta_i \in [0, 2\pi)$ for the following variants: (a) the number of SUs are increased at every step keeping the velocity fixed at some value v_0 for the entire simulation, and (b)the velocity v_i is increased in the range of [1 m/sec, 10 m/sec]. The lower end of the velocity values simulate a walking person, while the higher values simulate slow-moving traffic.

For the mobile scenario, the helpers broadcast PU activity information if their sensed occupancy vector has changed, or if an SU has requested an update. SUs request for PU activity update every time they come within the range of at least one new helper in an on-demand fashion. This is required even if the SU is moving within an area in which the helpers sense the same PUs as there could be inaccuracies in helper sensing. However, no message needs to be sent if the SU is moving within the range of the same helper(s).

Figure 6.3 represents O_h as a function of the number of SUs when the velocity of an SU is fixed at 2 m/sec, while the direction is randomly selected every minute. Therefore, after every minute, if the SU comes within the vicinity of a new helper, it requests the current channel status from that helper. This causes the increase in O_h with the growth in the number of SUs. The solid line represents O_h for this scenario. The dashed line represents O_h due to the change in channel status alone. Observe that the dashed line is nearly invariant with respect to the number of SUs as it is only a function of the number of helpers and the

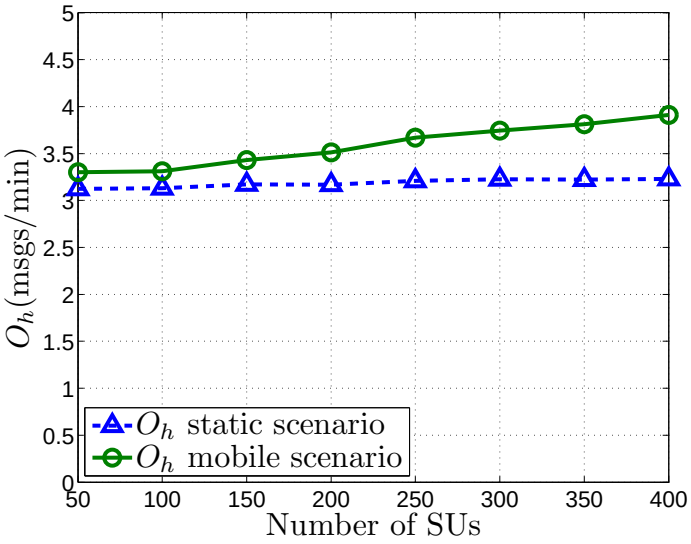

Figure 6.3: Communication overhead (helper rate) as a function of the number of SUs

PU activity both of which are constant in this experiment.

Figure 6.4 shows O_h as a function of SU velocity. After every minute, if the mobile SU is in the vicinity of a new helper, an on-demand occupancy vector is sent to the SU. We can see that with an increase in the speed of the SU, it traverses an increasing number of new helpers (new areas) neighborhoods. This gives a slight raise to the growth in the number of occupancy vectors (due to the on-demand messages) as evidenced in Figure 6.4.

6.4 Comparative Performance Analysis with the Scheme in [1]

In this section, we compare the communication overhead and power requirement of our method with the one presented in [1]. Recall that the work in [1] also employs a stationary network of helpers for authenticating PU activity.

In our model, we only need to send out an occupancy vector when an SU is in the vicinity of a new helper. Our method does not need SU training, and hence results in just one message per helper node upon movement. Also, in our scheme, if the SU is moving within the range of the same set of helper nodes, no extra occupancy messages need to be

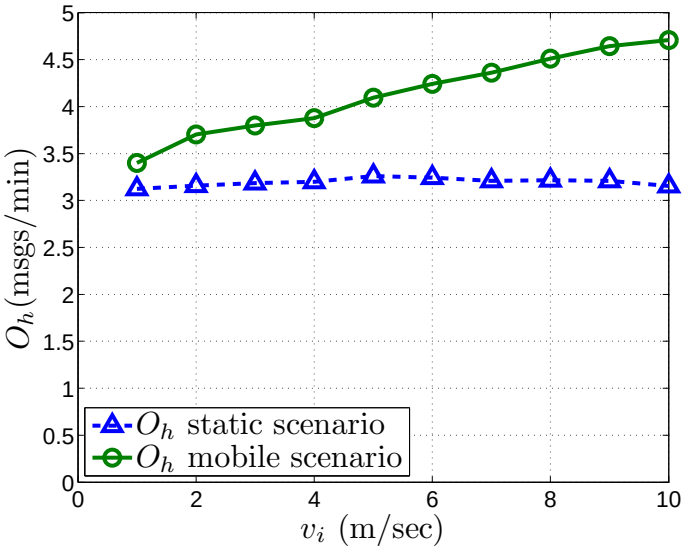

Figure 6.4: Communication overhead (helper rate) as a function of the velocity of SUs

sent.

In [1], every SU movement requires re-training of the SU. Further any mobility of the SUs results in a re-training of the SU. This is true even in the case of the SU moving within the vicinity of a given helper node since their scheme is tightly coupled with the channel between the helper and the SU. In particular, any movement of an SU by more than 3 m will result in 5 training packets per channel [20]. For a PU that uses 10 channels and an SU that is moving at 3 m/s, their scheme would require a total of 50 messages/helper every second. This would result in 3000 messages per minute for each helper node. This shows that their model is not very suitable for mobile SUs. In summary, we see that in our model, the messaging overhead is significantly lower than the training overhead involved in [1].

Power Comparison: We next compare the power required by both the models. In the model suggested by [1] where the helper node is in close proximity to the PU, it will have to transmit with the same power as that of the PU. This is required since the SU needs to be trained with similar signal characteristics as that of the PU for link signature verification.

Before we compare our model to theirs, we observe that according to the Rayleigh fading channel, the received power is inversely proportional to the α^{th} power of the distance between

the transmitter and the receiver [45]. The value of α varies with the environment and typically ranges between 2 to 6 [60, 61]. In an urban setting, fading can be considerable and hence α can be as large as 5. In a rural setting, the value of $\alpha \approx 2.5$.

To compare the transmission power required in the two models, we fix the received power P_r to be the same for an SU in either setting. Let P_t denote the transmitted power of the helper in their model while P_t' denote the power required in our model.

We have,

$$P_t \propto P_r d^\alpha \text{ , where } d \text{ is the transmission radius of the PU.}$$
$$P_t' \propto P_r d'^\alpha \text{ , where } d' \text{ is the transmission radius of helper node}$$

Thus we have,

$$\frac{P_t}{d^\alpha} = \frac{P_t'}{d'^\alpha}$$

The transmission range of the helper in their model is the same as that of the $PU = 1.5$ km. In our model, the helper transmission range is 400m. In the worst case, when the SU is on the circumference of the disc in either setting, we have

$$\frac{P_t}{P_t'} = (\frac{1500}{400})^\alpha$$

In Figure 6.5 we vary the transmission range of the helper node in the model in [1] from 1.5 km to 30 km while keeping our helper transmission range fixed at 400m. We plot the power ratio for each of these transmission ranges on a log scale. Each curve represents a particular α value. For instance, when α is 2, and the distance that the helper needs to transmit is 1.5 km, the model in [1] requires 10 times more power per helper than our model. This is the best case scenario for their model. As α increases, the power ratio increases exponentially as shown by Figure 6.5. Since our scheme requires a significantly lower power expenditure, we employ more helper nodes than theirs. The helpers in our model are CR's and thus expected to be inexpensive.

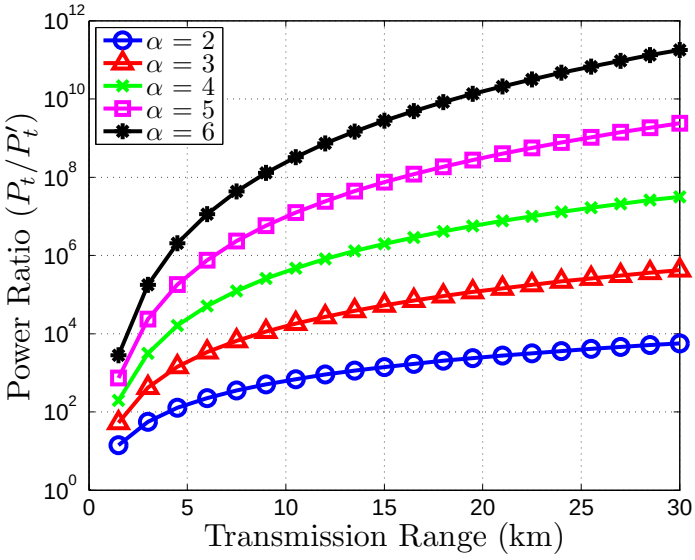

Figure 6.5: Helper power ratio as a function of the distance of coverage

6.5 Probability of Rejection and Probability of Acceptance

In the previous chapter, we discussed possible attack scenarios and we considered a threshold ε above which an SU rejects the occupancy vector. We outlined the rejection and acceptance criteria on a channel in Chapter 4. We now analyze p_{rej} and p_{acc} by varying the parameter values and plotting them.

Figure 6.6 shows the probability of rejecting a valid occupancy vector p_{rej} as a function of the probability of a channel being busy p_{busy} for different values of p_{fa}. We fix p_{md} to be 0.1 and ε to be 3. We observe that for low values of p_{fa} there is a very low probability of p_{rej}. This is because when p_{fa} is low, chances of a helper hearing a 1 while an SU hearing is 0 are low. This increases with higher values of p_{fa} and hence p_{rej} increases. The trend of each curve with an increase in p_{busy} is explained as follows. Beyond a certain $p_{busy} \approx 0.6$, the chances of rejection starts dropping since the channel is actually busy.

In Figure 6.7, we plot the probability of rejecting a valid occupancy vector p_{rej} as a function of the probability of a channel being busy p_{busy} for different values of p_{md}. We fix the value of p_{fa} to be 0.1 and ε to be 3. We obtain very low values for p_{rej} for low p_{md} values

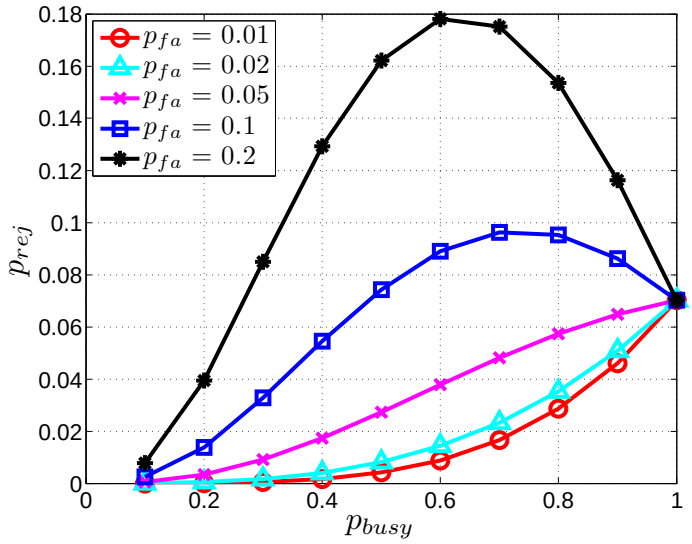

Figure 6.6: Probability of rejection as a function of probability of channel being busy for different false alarm probabilities.

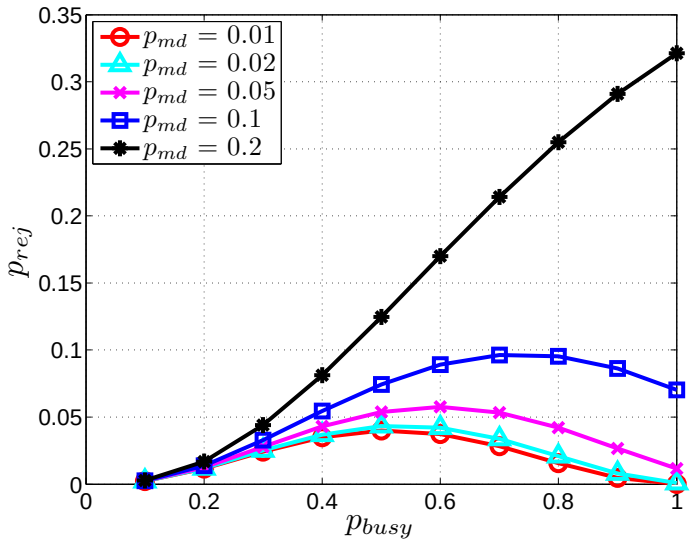

Figure 6.7: Probability of rejection as a function of probability of channel being busy for different misdetection probabilities.

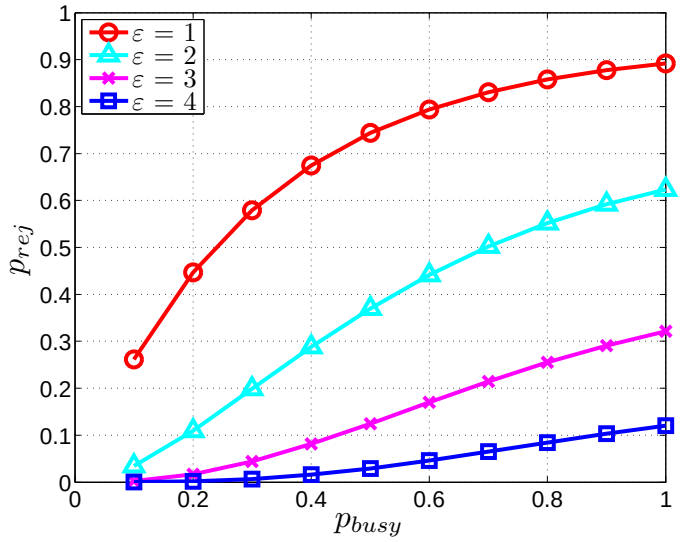

Figure 6.8: Probability of rejection as a function of probability of channel being busy for different ε values.

since SU's do not misdetect channel activity. For high values of p_{md} such as 0.2, the channels are likely to be misdetected by the SU. However, since the helper outputs are ORed, there are high chances of at least one helper detecting PU activity in spite of high p_{md}. This leads to an increase in the number of 1 to 0 discrepancies observed at the SU which contribute to the increase in the probability of rejection p_{rej}.

Figure 6.8 shows the probability of rejecting a valid occupancy vector p_{rej} as a function of the probability of a channel being busy, p_{busy} for different values of ε. We fix the values of both p_{md} and p_{fa} to be 0.1. At high values of ε, we see that p_{rej} is low as the threshold for the rejection of a vector is never reached. At low values of ε, the threshold is reached more often and hence the vector is rejected. p_{rej} depends directly on p_{busy} since other parameters are fixed. Thus, an increase in p_{busy} leads to an increase in p_{rej}.

Figure 6.9 shows the probability of accepting an invalid occupancy vector p_{acc} as a function of the probability of a channel being busy p_{busy} for different values of probability of false alarm p_{fa}. We set p_{md} to be 0.1 and ε to be 3. We see that p_{acc} is high at low channel activity. This is because the vectors at the wormhole origin and the SU location are identical

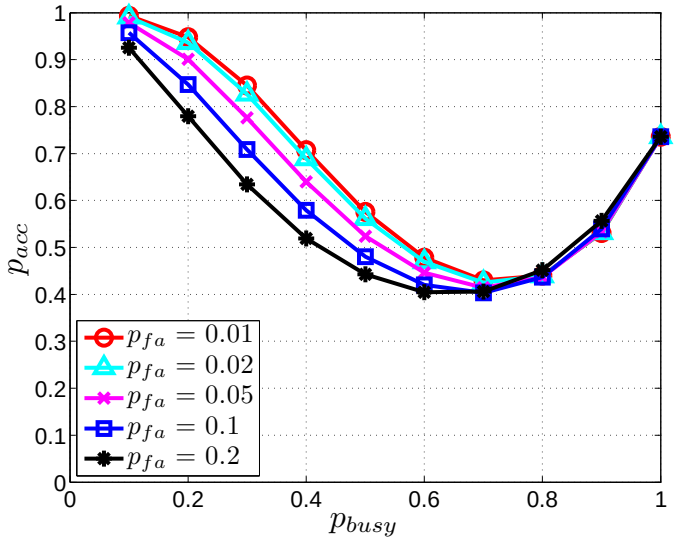

Figure 6.9: Probability of acceptance as a function of probability of channel being busy for different false alarm values.

and there are not enough 1 to 0 flips which would increase the threshold. As p_{busy} increases, there is a decrease in p_{acc} because the occupancy vectors are reaching the threshold for a 1 to 0 flip. At very high p_{busy} values, most of the channels at both the wormhole origin and the SU location are likely to be busy. This again leads to the threshold for rejection of a vector at the SU not being reached and hence an increase in p_{acc}.

Figure 6.10 shows the probability of accepting an invalid occupancy vector p_{acc} as a function of the probability of a channel being busy p_{busy} for different values of probability of misdetection p_{md}. We set the value of p_{fa} to be 0.1 and ε to be 3. We observe that p_{acc} is high at low channel activity. This is because most of the channels are idle at both the wormhole origin and the current SU location, thereby making the vectors nearly identical. When p_{busy} takes values around 0.6, there is more of a 1 to 0 flip between the wormhole region and the SU region, and hence, p_{acc} is low. When p_{busy} is high, both regions again have similar vectors and hence a high p_{acc}.

Figure 6.11 shows the probability of accepting a valid occupancy vector p_{acc} as a function of the probability of a channel being busy p_{busy} for different values of ε. We fix the values

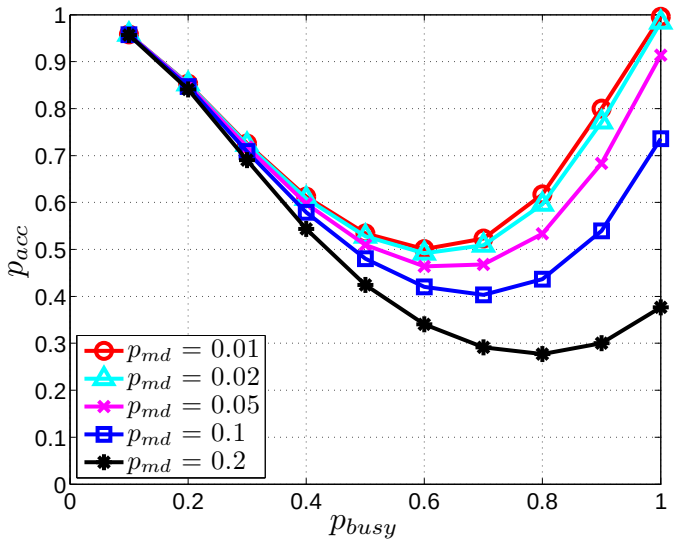

Figure 6.10: Probability of acceptance as a function of probability of channel being busy for different misdetection values.

of both p_{fa} and p_{md} to be 0.1. At higher thresholds, most of the vectors are accepted as the threshold value is not reached. For low values of ε, the vectors are rejected more often thus leading to low p_{acc}. The variation in p_{acc} for $\varepsilon = 2$ can be explained as follows. At high and low values of p_{busy}, the channel characteristics at both the regions are similar, leading to the vectors being identical and hence acceptance at the SU. When $p_{busy} = 0.5$, the channels at the two regions are not identical, thereby rejecting a few vectors and decreasing p_{acc}.

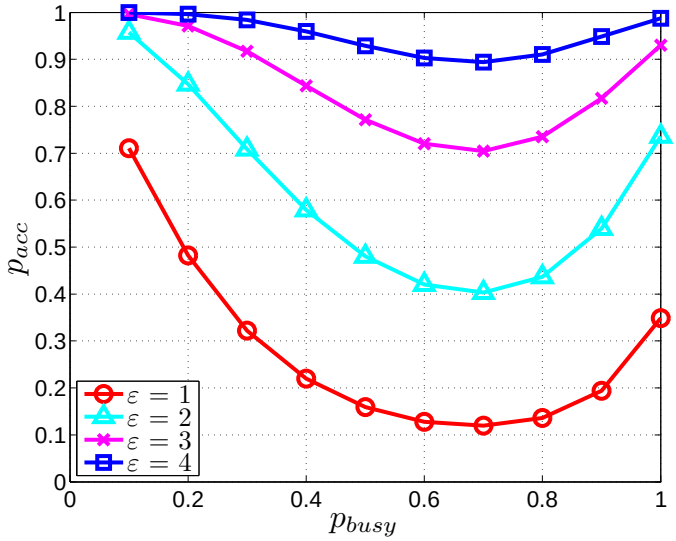

Figure 6.11: Probability of acceptance as a function of probability of channel being busy for different ε values.

CHAPTER 7

Conclusions

Wireless communications rely on a shared medium and thus require wireless technologies to cooperate and share the spectrum in a non-interfering manner for useful communication. With an increase in the number of wireless technologies, there is a growing problem of spectrum scarcity. The Federal Communications Commission (FCC) has decided to allow the usage of spectrum belonging to licensed users by secondary users employing CRs when the licensed users are not using the spectrum. Cognitive radio networks (CRNs) exploit the idle portion of the licensed spectrum to establish network communications. Essential to the co-existence of this technology with legacy systems, is the reliable sensing of spectrum opportunities. However, existing spectrum sensing techniques are vulnerable to adversaries that mimic the characteristics of Primary User (PU) transmissions in order to reduce the bandwidth availability for the CRN.

In this thesis, we address the problem of preventing PUE attacks in mobile CRNs. We propose a PU authentication system that securely and reliably delivers PU activity information to SUs. Our PU authentication system relies on the deployment of a network of static helper nodes for verifying the availability of idle spectrum. These helper nodes are deployed within the area of PU network. We have taken care to satisfy the FCC requirement not to modify the existing legacy systems as mandated by FCC.

In our system, the helper nodes authenticate the PU using link signatures which is a channel property between any two nodes. A link signature can determine a change in position of a transmitter since the channel is different when the position changes [20]. We use this idea in our system to see whether a PU signal has been transmitted from the known PU location or some other location. The helper nodes are trained to recognize this PU signal and validate it. The SU does not do any sensing in our system except when it hears more than one helper group and neither of the vectors get discarded.

As the helpers and the PU are stationary, the helpers need to be trained just once. Though our system requires the helper nodes to continuously sense the spectrum to transmit spectrum information, the training overhead is less in contrast to the previous work as repeated training is not needed. Also, our system supports mobility with very little extra overhead. No re-training is required even in this case as the SUs just need to request for the current channel status upon changing its location.

The network of helpers is limited to the deployment area of the SUs and is decoupled from the PUs' locations. Our security analysis showed that our authentication system can withstand impersonation attacks of the PUs as well as of the helpers nodes. Since we do not provide any physical security to the helper node network, we also suggest a reputation-based system to detect compromised helper nodes.

BIBLIOGRAPHY

[1] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, 2010, pp. 286–301.

[2] E. D. N. FCC, "03-222," *Notice of Proposed Rule Making and Order*, 2003.

[3] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[4] I. Atakli, H. Hu, Y. Chen, W. Ku, and Z. Su, "Malicious node detection in wireless sensor networks using weighted trust evaluation," in *Proceedings of the 2008 Spring simulation multiconference*. Society for Computer Simulation International, 2008, pp. 836–843.

[5] M. McHenry, "Spectrum white space measurements. presented to new america foundation broadband forum, june 2003."

[6] Q. Yuan, P. Tao, W. Wenbo, and Q. Rongrong, "Cyclostationarity-based spectrum sensing for wideband cognitive radio," in *Proceedings of the WRI International Conference on Communications and Mobile Computing*, vol. 1, 2009.

[7] H. Kim and K. Shin, "In-band spectrum sensing in cognitive radio networks: energy detection or feature detection?" in *Proceedings of MOBICOM*, 2008, pp. 14–25.

[8] B. Wild and K. Ramchandran, "Detecting primary receivers for cognitive radio applications," in *Proceedings of IEEE DySPAN*, 2005, pp. 124–130.

[9] Y. Gao and Y. Jiang, "Performance analysis of a cognitive radio network with imperfect spectrum sensing," in *INFOCOM IEEE Conference on Computer Communications Workshops, 2010*. IEEE, 2010, pp. 1–6.

[10] FCC, "Second report and order and memorandum opinion and order, FCC-08-260," 2008.

[11] S. Haykin, "Cognitive radio: brain-empowered wireless communications," vol. 23, no. 2. IEEE, 2005, pp. 201–220.

[12] R. Thomas, L. DaSilva, and A. MacKenzie, "Cognitive networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on.* Ieee, 2005, pp. 352–360.

[13] L. Goh, Z. Lei, and F. Chin, "Dvb detector for cognitive radio," in *Communications, 2007. ICC'07. IEEE International Conference on.* IEEE, 2007, pp. 6460–6465.

[14] A. Sahai, N. Hoven, and R. Tandra, "Some fundamental limits on cognitive radio," in *Allerton Conference on Communication, Control, and Computing*, 2004, pp. 1662–1671.

[15] S. Shellhammer, R. Tandra, J. Tomcik *et al.*, "Performance of power detector sensors of dtv signals in ieee 802.22 wrans," in *Proceedings of the first international workshop on Technology and policy for accessing spectrum.* ACM, 2006, p. 4.

[16] W. Xia, S. Wang, W. Liu, and W. Cheng, "Correlation-based spectrum sensing in cognitive radio," in *Proceedings of the 2009 ACM workshop on Cognitive radio networks.* ACM, 2009, pp. 67–72.

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

[18] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Raez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *Proceedings of the 28th IEEE International Performance Computing and Communications Conference (IPCCC)*, 2009, pp. 208–215.

[19] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic link signatures for spectrum usage authentication in cognitive radio," in *Proceedings of the fourth ACM conference on Wireless network security.* ACM, 2011, pp. 79–90.

[20] N. Patwari and S. Kasera, "Robust location distinction using temporal link signatures," in *Proceedings of MOBICOM*, 2007, p. 122.

[21] D. Cabric, S. Mishra, and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*, vol. 1. Ieee, 2004, pp. 772–776.

[22] H. Tang, "Some physical layer issues of wide-band cognitive radio systems," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on.* IEEE, 2005, pp. 151–159.

[23] A. Fehske, J. Gaeddert, and J. Reed, "A new approach to signal classification using spectral correlation and neural networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on.* Ieee, 2005, pp. 144–150.

[24] A. Ghasemi and E. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on.* Ieee, 2005, pp. 131–136.

[25] F. Digham, M. Alouini, and M. Simon, "On the energy detection of unknown signals over fading channels," in *Communications, 2003. ICC'03. IEEE International Conference on*, vol. 5. Ieee, 2003, pp. 3575–3579.

[26] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on.* IEEE, 2005, pp. 137–143.

[27] Q. Zhao, L. Tong, and A. Swami, "Decentralized cognitive mac for dynamic spectrum access," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on.* IEEE, 2005, pp. 224–232.

[28] H. Zheng and L. Cao, "Device-centric spectrum management," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on.* IEEE, 2005, pp. 56–65.

[29] J. Zhao, H. Zheng, and G. Yang, "Distributed coordination in dynamic spectrum allocation networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on.* IEEE, 2005, pp. 259–268.

[30] S. Anand, Z. Jin, and K. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," in *Proceedings of IEEE DySPAN*, 2008, pp. 1–6.

[31] D. Stinson, *Cryptography: theory and practice.* CRC press, 2006.

[32] R. Chen and J. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in *Networking Technologies for Software Defined Radio Networks, 2006. SDR'06.1 st IEEE Workshop on.* IEEE, 2006, pp. 110–119.

[33] S. Geirhofer, L. Tong, and B. Sadler, "A measurement-based model for dynamic spectrum access in wlan channels," in *Proc. IEEE MILCOM.* Citeseer, 2006.

[34] A. Motamedi and A. Bahai, "Mac protocol design for spectrum-agile wireless networks: Stochastic control approach," in *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on.* Ieee, 2007, pp. 448–451.

[35] Q. Zhao, L. Tong, A. Swami, and Y. Chen, "Decentralized cognitive mac for opportunistic spectrum access in ad hoc networks: A pomdp framework," *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 3, pp. 589–600, 2007.

[36] L. Yang, L. Cao, and H. Zheng, "Proactive channel access in dynamic spectrum networks," *Physical Communication*, vol. 1, no. 2, pp. 103–111, 2008.

[37] H. Kim and K. Shin, "Efficient discovery of spectrum opportunities with mac-layer sensing in cognitive radio networks," *IEEE Transactions on Mobile Computing*, pp. 533–545, 2008.

[38] C. Cormio and K. Chowdhury, "A survey on mac protocols for cognitive radio networks," vol. 7, no. 7. Elsevier, 2009, pp. 1315–1329.

[39] X. Huang, N. Han, G. Zheng, S. Sohn, and J. Kim, "Weighted-collaborative spectrum sensing in cognitive radio," in *Communications and Networking in China, 2007. CHINACOM'07. Second International Conference on*. IEEE, 2007, pp. 110–114.

[40] L. Luo, C. Ghosh, and S. Roy, "Joint optimization of spectrum sensing for cognitive radio networks," in *GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference*. IEEE, 2010, pp. 1–5.

[41] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Proceedings of IEEE ICC*, 2007, pp. 4646–4651.

[42] J. Zhang, M. Firooz, N. Patwari, and S. Kasera, "Advancing wireless link signatures for location distinction," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 2008, pp. 26–37.

[43] N. Patwari and S. Kasera, "Temporal link signature measurements for location distinction," vol. 10, no. 3. IEEE, 2011, pp. 449–462.

[44] H. Hashemi, "The indoor radio propagation channel," *Proceedings of the IEEE*, vol. 81, no. 7, pp. 943–968, 1993.

[45] R. T. S., *Wireless Communications: Principles and practice*. Prentice hall, 2001.

[46] A. T. S. Committee, "ATSC digital television standard (a/53) revision e, with amendments no. 1 and 2,," http://www.atsc.org/cms/, 2006.

[47] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proceedings of INFOCOM*, 2003, pp. 1976–1986.

[48] S. Capkun and J. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[49] S. Buchegger and J. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," *Communications Magazine, IEEE*, vol. 43, no. 7, pp. 101–107, 2005.

[50] S. Ganeriwal, L. Balzano, and M. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no. 3, p. 15, 2008.

[51] W. Kozma and L. Lazos, "React: resource-efficient accountability for nodemisbehavior in ad hoc networks based on random audits," in *Proceedings of the second ACM conference on Wireless network security*. ACM, 2009, pp. 103–110.

[52] Y. Liu and Y. Yang, "Reputation propagation and agreement in mobile ad-hoc networks," in *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, vol. 3. IEEE, 2003, pp. 1510–1515.

[53] A. Selcuk, E. Uzun, and M. Pariente, "A reputation-based trust management system for p2p networks," in *Cluster Computing and the Grid, 2004. CCGrid 2004. IEEE International Symposium on*. Ieee, 2004, pp. 251–258.

[54] N. Robertson, D. Sanders, P. Seymour, and R. Thomas, "The four-colour theorem," *Journal of Combinatorial Theory, Series B*, vol. 70, no. 1, pp. 2–44, 1997.

[55] J. Flood, "Telecommunication networks," *Institution of Electrical Engineers, London*, 1997.

[56] Q. Liu, Z. Zhou, C. Yang, and Y. Ye, "The coverage analysis of cognitive radio network," in *Networking and Mobile Computing, 2008*.

[57] K. Jain, J. Padhye, V. Padmanabhan, and L. Qiu, "Impact of interference on multi-hop wireless network performance," *Wireless networks*, vol. 11, no. 4, pp. 471–487, 2005.

[58] C. Bettstetter, H. Hartenstein, and X. Pérez-Costa, "Stochastic properties of the random waypoint mobility model," *Wireless Networks*, vol. 10, no. 5, pp. 555–567, 2004.

[59] W. Navidi and T. Camp, "Stationary distributions for the random waypoint mobility model," *Mobile Computing, IEEE Transactions on*, vol. 3, no. 1, pp. 99–108, 2004.

[60] T. Chrysikos and S. Kotsopoulos, "Impact of channel-dependent variation of path loss exponent on wireless information-theoretic security," in *Wireless Telecommunications Symposium, 2009. WTS 2009*. IEEE, 2009, pp. 1–7.

[61] J. Seybold, *Introduction to RF propagation*. Wiley Online Library, 2005.