AN ABSTRACT OF THE DISSERTATION OF

Nadia Adem for the degree of Doctor of Philosophy in Electrical and Computer Engineering presented on September 16, 2016.

Title: Jamming Attack Resiliency and Performance Analysis of Cognitive Radio Communication Networks

Abstract approved: _____

Bechir Hamdaoui

Cognitive radio technology emerges as a promising solution for overcoming shortage and inefficient use of spectrum resources. In cognitive radio networks, secondary users, which are users equipped with cognitive radios, can opportunistically access spectrum assigned to primary users, the spectrum license holders. Although it improves spectrum utilization efficiency, this opportunistic spectrum access incurs undesired delays that can degrade the quality of service (QoS) of delay-sensitive applications substantially. It is therefore important to understand, model, and characterize these delays, as well as their dependency on primary user behaviors. Moreover, the lack of access priority leads to significant performance degradation when the network is under jamming attacks. It turns out that addressing jamming attacks while maintaining a desired QoS is very challenging. In this thesis, we characterize the properties of the random process that describes the availability of the opportunistic resources, and analytically model and analyze cognitive network average delays. Furthermore, we propose and study new techniques that mitigate jamming attacks in mobile cognitive radio networks. More specifically, this thesis consists of the following three complimentary frameworks:

1. *Stochastic Resource Availability Modeling and Delay Analysis.* In this framework, we define and characterize the properties of the random process that describes the availability of the opportunistic network resources. We apply the mean residual service time concept to derive an analytical solution for the cognitive network queueing delay. We model the service mechanism, and determine the manner in which it depends on spectrum availability. We show that the delay becomes unbounded if spectrum dynamics are not carefully considered in network design.

2. *Mitigating Jamming through Pseudorandom Time Hopping.* In this framework, we propose and evaluate jamming countermeasure approaches for mobile cognitive users. We propose two time-based techniques which, unlike other existing frequency-based techniques, do not assume accessibility to multiple channels and hence do not rely on spectrum handoff to countermeasure jamming. In these two techniques, we allocate data over time based on cryptographic and estimation methods. We derive analytical expressions of the jamming, switching and error probabilities. Our findings show that our proposed technique outperforms other existing frequency-based techniques.

3. *Optimally Controlled Time-Hopping Anti-Jamming Technique.* In this framework, we propose a jamming and environment aware resource allocation method for mobile cognitive users. We propose to mitigate jamming based on an optimal allocation of data over time. In addition, we optimally control network mobility to meet a desired QoS. Our findings show that our proposed technique achieves better QoS than those achieved by existing cryptographic methods while not compromising jamming resiliency.

Jamming Attack Resiliency and Performance Analysis of Cognitive Radio Communication Networks

by

Nadia Adem

A DISSERTATION

submitted to

Oregon State University

in partial fulfillment of
the requirements for the
degree of

Doctor of Philosophy

Presented September 16, 2016
Commencement June 2017

Doctor of Philosophy dissertation of Nadia Adem presented on September 16, 2016.

APPROVED:

Major Professor, representing Electrical and Computer Engineering

---

Director of the School of Electrical Engineering and Computer Science

---

Dean of the Graduate School

I understand that my dissertation will become part of the permanent collection of Oregon State University libraries. My signature below authorizes release of my dissertation to any reader upon request.

Nadia Adem, Author

ACKNOWLEDGEMENTS

I am grateful for all the knowledge and research as well as life experience I have gained through out my PhD journey. All praise is due to my Lord for the uncountable favors and blessings He has bestowed upon me. With out the patience and trust He has given me, this journey has not been completed. I am, then, thankful for the support of many people, mentors, family, friends, and colleagues. First, my gratitude goes to my adviser Professor Bechir Hamdaoui for his guidance, and continuous support.

I also thank my committee members, Professors Arun Natarajan, Rakesh Bobba, Attila Yavuz and to the GCR representatives Professor Maggie Niess for their helpful discussions. Special thank goes to Professor Attila Yavuz for his cooperation in one of our research projects. I also thank Professor Thinh Nguyen for some helpful discussions we had with him during early stage of my PhD. I am thankful to our papers'-anonymous reviewers for their feedback that lead to improvements of our papers. I also thank my current and former colleagues for their collaboration, feedback, and good company.

I am also grateful to the Libyan government and Libyan society in general for funding my PhD completely.

I am grateful to my parents for their unlimited trust, unconditional love, prayers, patience and continuous encouragement. I am also tankful for all my siblings, my grandmother, my nephews and niece, and all my relatives for their unconditional love. I thank all my friends every where for their support.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

LIST OF FIGURES (Continued)

LIST OF TABLES

LIST OF ALGORITHMS

Chapter 1: Introduction

The drastic increase in demand for wireless devices, services, and applications is causing a shortage in the radio spectrum resource supply [1]. This spectrum shortage problem is, however, shown to be due not to the scarcity of the wireless spectrum resource, but rather to the current static assignment schemes used to allocate this spectrum resource among spectrum users [2]. Indeed, studies have shown that the licensed radio spectrum is under-utilized, and only a small fraction of it is being actually exploited by licensed users, commonly referred to as primary users. This problem has therefore prompted spectrum regulatory bodies (e.g., FCC) as well as industry and academic researchers to think of new ways that can utilize the available spectrum more effectively.

The use of cognitive radios [3] has therefore emerged as a potential solution that can overcome this shortage problem by enabling dynamic (or opportunistic) spectrum access (DSA) [4]. The main idea behind DSA, enabled via the cognitive radio technology, is to allow unlicensed users (also referred to as secondary or cognitive users) to exploit and utilize unused licensed spectrum whenever primary users are not using it. Through cognitive capabilities, cognitive users can then adjust their operating parameters, such as power and frequency, to avoid interfering with primary users. Generally speaking, in order to be able to dynamically access the spectrum, cognitive users need to undergo a four-phase cycle [3, 5, 6]: (i) **Observation or sensing phase**, during which cognitive radio users perform real-time spectrum sensing to locate and determine spectrum access opportunities. This requires the reliance on signal detection techniques designed for spectrum sensing. (ii) **Reasoning phase**, during which cognitive radio users analyze the observation data acquired through the sensing phase to decide on the best strategy to

use to allocate spectrum and share it among other users. (iii) **Adaptation phase**, during which cognitive radio users switch to the best available spectrum opportunity, and tune their parameters (operating frequency, transmission power, modulation scheme, etc.) accordingly. During this phase, users might be required to handoff from one frequency channel to another, and every time they do so they need to adjust their parameters to match the new channel. (iv) **Acting phase**, during which cognitive users carry out their communications according to the adapted parameters.

Due its great potential in improving spectrum utilization efficiency and addressing next-generation wireless spectrum challenges, DSA communication and networking have received significant research attraction ranging from distributed spectrum resource sharing [7–11] and power resource allocation [12–14] to performance analysis [15–19] and protocol design [20,21]. Although DSA enabled through cognitive radios has great potential for overcoming the spectrum supply shortage problem, the lack of access priority to spectrum incurs undesired delays and possible network outages. This can degrade the quality of service (QoS) of delay-sensitive applications substantially. Moreover, having cognitive users go over the aforementioned cycle incurs overhead in terms of energy consumption, delay, and control traffic, which in turns leads to QoS degradation. For example, the spectrum sensing process is needed to locate spectrum opportunities, but not without consuming energy, causing delay, and incurring extra traffic overhead. Furthermore, the nature of the cognitive radio access makes it more subject and vulnerable to security threats than what conventional wireless networks are.

In the rest of this section, we first highlight the impact of the opportunistic spectrum access on some performance and security aspects of cognitive radio networks and review some of the related works. We then present a summary of the contributions made in this thesis.

1.1 Performance of Cognitive Radio Networks

Due to the opportunistic access and sharing nature of spectrum, the performance assessment metrics in cognitive radio networks differ from those used in conventional wireless networks. As mentioned earlier, a cognitive user is susceptible to experiencing some delay when trying to locate and use spectrum opportunities. The main cause of such delays is due to the random and sporadic availability of the licensed spectrum whose primary users have the right to access and leave their licensed frequency bands at any time. Upon the return of a primary user to its channel, cognitive users must immediately vacate the channel, which may result in halting the ongoing communication for some time until a new available channel is found, thereby causing undesired delays that can be problematic especially if the applications are time-sensitive. What makes this delay problem even more problematic is the fact that these events are unpredictable and look very random to cognitive users. It is therefore important to model, characterize, and analyze these delays by capturing and studying the impact of spectrum availability randomness on them. Delay performance modeling and analysis can then help in providing guidelines for designing protocols and techniques for cognitive radio networks.

For a given primary user activity, cognitive users might not be able to meet a certain performance criterion, and such an activity could result in excessive packet drops or queue instability through the network. Hence, modifications need to be introduced to network settings to make sure desired QoS is maintained. To the best of our knowledge, little to no work has been done in the literature to derive comprehensive delay models for cognitive radio networks. Hence, more thorough investigations need to be done in this area. We now review some of the existing delay analysis works. In [22], the authors present a queuing analysis to study delay in cognitive networks. They derive the solution of the queue average length for cognitive users that content to access primary user channels. The authors in [23] analyze the stationary queue distribution

for a constant cognitive users arrival process. They derive a closed-form expression for the stationary queue distribution for the case of two channels, and upper and lower bounds for an arbitrary number of channels. In [24], the authors analyze the delay for a clustered cognitive radio network by approximating the average length of queue size. The authors in [25] consider cooperation among secondary and primary users to enhance the delay performance. In [26], the authors analyze the cognitive network transmission delay by considering the distribution of time through which some opportunistic resources are available. In [27], the authors propose centralized and distributed spectrum access schemes for cognitive users with different priority classes. The authors also study the performance of cognitive radio networks by analyzing the blocking probability and average switching delay of cognitive users. The authors in [28] develop an admission control technique that meets the QoS requirements in terms of packet queueing delay. In [29], the authors study the impact of guard bands on the cognitive radio performance by deriving the termination and blocking probabilities of cognitive users under various spectrum assignment schemes. In our work [15, 30] (Chapter 2), we capture and study the volatile nature of spectrum availability in cognitive radio networks while considering Markovian primary user activities, and assess its impact on network outage statistics, spectrum handoff (or switching) statistics, queueing delay, and service delay.

1.2 Security in Cognitive Radio Networks

Cognitive radio systems are vulnerable to numerous security threats. The lack of access priority of cognitive users to spectrum makes their communications subject to a set of security attacks that conventional wireless networks are not subject to. Security threat models and countermeasure solution techniques have already been investigated for cognitive networks [31]. There is, for example, a spectrum sensing threat called primary user emulation attack, where an adversary

transmits signals whose characteristics emulate those of primary user signals. This type of attack interferes with the spectrum sensing process, leading to significant reduction in spectrum access opportunities [32–35]. There are also user privacy attacks that again result from the access flexibility nature of cognitive radio communication. For example, cognitive users can be involved in a cooperative spectrum sensing task to identify spectrum access availability, and when it is the case, they end up exchanging sensing reports with one another. The correction between the data in the sensing reports and their corresponding user location results in leakage of the location privacy information of cognitive users [36–41]. Cognitive radio networks are also vulnerable to jamming attacks, which can significantly impact the network performance by degrading the spectrum utilization efficiency. It is therefore important to address such jamming attacks so as to maintain a desired QoS. Jamming attacks are known to be more detrimental than other types of attacks [42]. Though attempts to address jamming in the context of cognitive radio networks have been made, most existing jamming countermeasures proposed so far assume accessibility to multiple channels, and hence consider frequency-hopping (spectrum handoff) based approaches to mitigate jamming. For instance, in [43], the authors assume that cognitive users hop among multiple channels and randomly allocate power to defend against jammers. They model interactions between jammers and secondary users as a Colonel Blotto game, and derive hopping patterns by relying on Markov decisions processes and learning techniques. Similarly, the authors in [44] propose frequency-hopping based countermeasure methods by modeling the anti-jamming problem as a game. Unlike [43], in [44], hopping patterns are derived based on prospect theory. The work in [45] is similar to that in [43]. However, while transmission power is allocated randomly in [43], the authors in [45] use learning algorithms instead to allocate power optimally. In [46], the authors assume that jammers and legitimate users compete sequentially, and model their interaction as a game using Stackelberg model. Their scheme allocates power to secondary users based on estimated jamming power. The authors in [47] model spectrum

availability and access as a partially observed Markov process. They assume that users learn to retreat from jammers through, similar to the other works, spectral surfing. They derive their retreating strategy using a multiple-armed bandit problem with the assumption that secondary users and jammers have the same knowledge about spectrum availability. In [48], the authors also consider spectral surfing as a jamming countermeasure with the assumption that secondary users use pre-shared secret keys for channel selections.

In our work [49], unlike most existing techniques, we propose a cryptography time-based countermeasure solution approach. Through pseudorandom allocation of data over time, we achieve jamming resiliency without making any assumptions about the number of accessible channels. More details about our proposed anti-jamming techniques are given in Chapters 3 and 4. In the following section, we present the thesis contributions.

1.3 Dissertation Contributions and Organization

The contributions of this dissertation are summarized as follows.

- We model and characterize, in Chapter 2, the properties of the random process that describes the opportunistically available spectrum resources. Our characterization of these properties allow us to analytically derive handoff and network outage performances that cognitive users experience. In this Chapter, we also apply the mean residual service time concept [50] to derive the queueing delay for single as well as batch packet arrivals. In addition, inspired by the slotted-Aloha system [51], we statistically characterize the packet service time distribution, and hence the average service delay for single as well as multi-cluster networks.

- We propose, in Chapter 3, time-based techniques which, unlike other existing techniques,

provide jamming resiliency without making any assumptions about the number of accessible channels. Our techniques do not rely on spectrum handoff and hence avoid any associated communication overhead. With the use of a shared private key, users allocate data securely over time. In addition, unlike existing works, our work considers user mobility and does assume that users are stationary. We also derive closed-form expressions for a number of performance metrics, including jamming probability, switching probability, and error probability.

- In Chapter 4, we propose a mathematical framework for modeling a decision process that uses reinforcement learning to allocate data over time and control mobility of cognitive radio users. Our proposed framework does so while accounting for spectrum resource volatility, channel gain variations over both time and space, and jamming attacks.

Chapter 2: The Impact of Stochastic Resource Availability on Cognitive Network Performance: Modeling and Analysis

The dynamical spectrum availability makes secondary user (SU) packet average delay one of the most important performance measures of a cognitive network. It is important to understand the nature of delay, as well as its dependence on primary user (PU) behaviors. In this chapter, we analytically model and analyze spectrum dynamics and their impact on delay, where the cognitive network is modeled as a discrete-time queueing system and the PU channel occupancy is modeled as a two-state Markov chain. The contribution of this chapter is characterizing the random process that describes the opportunistic availability of spectrum. In addition, we apply the mean residual service time concept to achieve an analytical solution for the queueing delay. Moreover, inspired by the slotted-Aloha system, we model the packet service process, and derive the packet service delay accordingly. Depending on PU behaviors, we show that the delay can become unbounded, thereby demonstrating the importance of considering PU behaviors in network design.

2.1 Introduction

The rapid and continuous growth of new wireless devices and applications increases the demand for spectrum resources. The development of cognitive radios is a promising framework to get the best of the limited radio spectrum and keeping up with the growth of wireless technologies. However, in case cognitive users are not allowed to simultaneously transmit with primary users,

their activities become restricted. In other words, unless there is a spectrum hole (spectrum not utilized by primary users), cognitive users are required to be inactive. They are also required to vacate a spectrum whenever a primary user reclaims the right to use it. These requirements, in turn, can cause huge cognitive network delay and as a consequence, instability issues. It is therefore important to quantify PU activities and determine the impact of that on cognitive network performance in general, and most importantly on delay.

In this chapter we analyze the performance of clustered cognitive networks, where a set of nodes along with a cluster head, equipped with a cognitive radio, form a cluster. This model can very well apply to a cognitive radio sensor network, where the sensor nodes send their data to a sink, the cluster head in our model, that accesses to channels opportunistically. Sensor applications usually generate data in small rates and hence there is no need for acquiring a licensed band, and having opportunistic spectrum access can be enough to achieve a desired QoS.

2.1.1 Summary of Contributions

The availability of spectrum varies over time depending on PU behaviors. It turns out that different important cognitive network characteristics, e.g., handoff process parameters, are modeled analytically by establishing the model of the process that describes this availability. To the best of our knowledge, this research has never been addressed.

In addition, the adaption of cognitive user's operation parameters to spectrum dynamics results in different delay components. A SU experiences a delay while identifying and exploiting spectrum access opportunities. To the best of our knowledge, none of the existing works comprehensively address all of these delays. There is also no much work done about modeling SU's packets service mechanism, in spite of its importance in delay performance analysis. Hence,

more investigations in this area need to be developed. The complexity of analyzing cognitive networks delay performance and the broad aspects of such analysis seem to be the reason behind the area being not well investigated.

In this chapter, we analyze the performance of clustered cognitive radio network modeled as a discrete-time queueing system where the data queues up at the cluster head. We consider the case where there is only one cluster, and extend it to the case where there are multiple clusters content for spectrum resources. The channel occupancy is modeled as a Markov chain. The contributions of this chapter ([15, 30]) are summarized as follows.

- We characterize the properties of the random process that describes spectrum dynamics. Based on this process, we analytically characterize the handoff (also refereed to as switching) performed and the outage experienced by cognitive users.
- We develop an analytical model for the SUs' packet waiting delay. We also model the service time distribution and hence derive the average service delay formula. The derived closed-form expression captures the dependence of this delay on the PU behaviors.
- Trough providing some numerical results, we show the importance of our analytical analysis in maintaining network stability.

2.2 Related Work

Due to its great potentials in addressing the spectrum shortage problem, the cognitive radio network paradigm has attracted significant research focus over the past decade, addressing various different aspects, such as protocol design [4, 52–56], spectrum sensing [41, 57–59], resource allocation and management [60–67], performance modeling and analysis [18, 19, 21, 68–71], and spectrum trading and auction [72–74], just to name a few. Delay performance analysis has also

received some attention, but not as much [22–28]. As a way to study network delay, the authors in [22], determined the queue average length for SUs that content to access spectrum. The authors in [23], however, analyzed queue distribution. They obtained analytical solutions for case of two channels, and upper and lower bounds for an arbitrary number of channels. They assumed constant packet arrival processes. In this chapter, however, we are not concerned about the queue statistics, but rather about the impact of spectrum dynamics on delay for given traffic parameters. In [24], the authors analyzed the delay for a clustered cognitive network. They also ended up analyzing the delay through approximating the queue size average length. In [26], a delay analysis was done by considering the distribution of time through which some opportunistic spectrum resources are available. In our chapter, however, we characterize the properties of the process that describe the evolution of the resource availability over time. We use this process not only to understand the nature of delay, but also to obtain the analytical characterization of network outage and switching mechanism. To enhance delay experience, the authors in [25] assumed SUs and PUs cooperate for spectrum access. In [27], for different priority classes, the authors proposed different spectrum access methods. They analyzed blocking probability and average spectrum handoff delay. The authors in [28] developed an admission control technique that guarantee a QoS requirements in terms of queueing delay. The authors assumed the availability of channels holds over a slot duration. In [75], the authors suggested a pricing strategy for reusing cellular networks spectrum. The cellular primary usage in [75] is modeled as a Poisson process. In this chapter, we model the primary users behavior similarly. In [76], the authors used fluid flow models to analyze the queueing system in a cognitive network. Aside from congnitive networking, [50] presented the residual service time concept and applied it for continuous systems queueing analysis. The residual service time concept, for the best of our knowledge, has not been considered for evaluating the performance of discrete-time systems. In this chapter, inspired with [50], we determine the mean residual service time for the discrete systems and use

it to analyze the delay performance in cognitive radio networks. The authors in [51] characterized the service time mechanism of a slotted-Aloha system with either finite or infinite user population where each user has finite or infinite buffer capacity. We consider the analysis in [51] to determine the service time distribution in cognitive networks.

2.3 Network Model

The cognitive radio network (CRN) has access to N channels licensed to some PUs. The occupancy of each channel is modeled as a two-state Markov chain. We are considering a clustered network, where M nodes along with a cluster head, which equips cognitive radio, form a cluster. There are L clusters, each contend with probability P_c to access the spectrum. Each cluster is modeled as a discrete-time queueing system where the data queues up at the cluster head buffer. Fig. 2.1 illustrates a single cluster network.

The cognitive radio system works as follows:

- The system is time slotted.
- The traffic arrives to the cluster head follows a Bernoulli process. The arrivals are independent of each other. Packets arrive in a batch within each slot. The average number of arrived packets per slot is λ, which can be viewed of as the arrival rate per slot.
- Over any available channel, the cluster head sends the data on a first-in first-serve basis. It switches from a spectrum to another whenever the last assigned becomes unavailable.
- The service times are assumed to be independent and identically distributed with an unspecified general distribution. The service process is assumed to be independent from the arrival process.

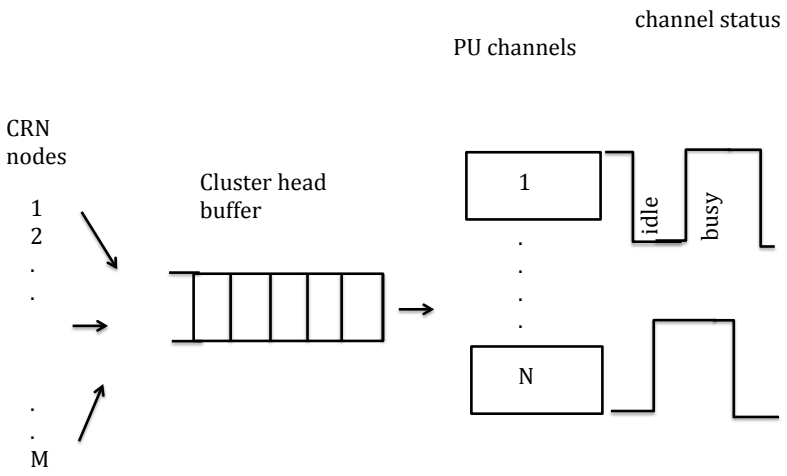

Figure 2.1: A single cluster cognitive network

The slotted system assumption is a reasonable widely-used assumption, e.g. [22], [24], and [28], and many others consider a similar assumption. In addition to dedicating a part of the slot for packets transmission, another part is usually assumed to be dedicated to spectrum sensing and opportunities detection.

The Bernoulli arrival process assumption is more realistic than the Poisson process in our setting. Unless some sort of reservations is assumed, which might not be possible to achieve, assuming a Poisson arrivals for multi-packet messages is not reasonable.

In addition, our PU model applies to the users in cellular networks. It is popular to model the calls arrival as a Poisson process (i.e., exponentially distributed interarrival times), and the call durations probability distributions as exponential [75]. Successive interarrival times and call durations are independent of each other in this model.

The SUs' packet arrival process is independent from the service process. As we will explain in Section 2.5, the service process depends mainly on the size of packets, contention methodol-

ogy and the dynamics of the spectrum availability.

As the cluster head plays the role of identifying spectrum opportunities, we are not concerned with the delay that might result from sensing errors, as it remains low. This error is usually ignored when there is a central point involved in detecting spectrum opportunities (that is the case in [28] and [76] for example). Our work can serve as the basis for achieving other analytical delay models that include this delay.

Our model applies to cognitive radio sensor networks, where sensor nodes send their data to a sink, the cluster head in our model. The sensors send their data over unlicensed channel in a triggered based. In other words, once an event is sensed, sensors report to the cluster head. Sensor applications usually require large number of sensors to be implemented, each generates data in small rate. Hence, a scheduled access scheme might not be suitable and it suffices for nodes to randomly access the channel shared among them. Within each slot λ packets arrive the cluster head on average. Through reusing cellular bands, L number of clusters within the network transmit data, received from the nodes associated with them, to backbone network.

2.4 Resource Availability Process

The availability of the opportunistic resources vary over time depending on the primary users activity and their spectrum usage pattern. In this section, we model and derive a number of statistics that describe the random availability of the resources. We model a number of random processes that are used to define the resource availability process and characterize its properties.

Single-Channel Availability Model The evolution of the availability of a channel i over time is a random process CH_i. This process is a family of random variables $\{CH_i(t) : t \geq 0\}$, where each random variable takes a value zero if the channel is idle and one otherwise. By assumption,

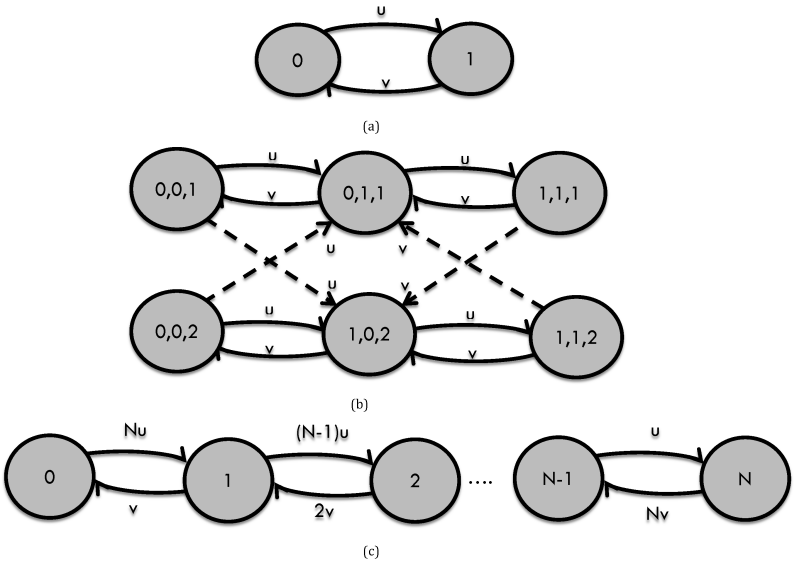

Figure 2.2: (a) Single channel Markov chain. (b) Extended model of the two-channel availability. (c)Simultaneously occupied channels model.

this process is modeled as a continuous-time Markov Chain with two states, labeled 0 and 1. The states 0 and 1 represent the idle and busy events, respectively. The transition time of the CH_i states, denoted by T_{CH_i}, is exponentially distributed with parameters u for the zero state and v otherwise. The state-transition diagram a channel occupancy appears in Fig 2.2(a). All the channels are assumed to be independent of each other and identical.. The analysis can be developed similarly if the channels are unidentical. Through out our analysis we are assuming the transition rates u and v are known. In practice, if they are not known, they can be estimated by observing the PUs behavior.

Multi-Channels Availability Model Studying the process corresponding to the joint channels availability is important for our subsequent analysis. The joint availability process CH_{joint} is a family of vectors of random variables $\{(CH_1(t), \ldots, CH_N(t)) : t \geq 0\}$. Since at any time

instant, the realization of CH_i, $\forall i \in \{1,..,N\}$, is either zero or one, the state space of CH_{joint} has a size of 2^N states. The transition time between the states is denoted by $T_{CH_{joint}}$.

Lemma 1. *The joint availability process is Markov.*

Proof. The state transition time for a given state $\{(CH_1 = ch_1,..,CH_N = ch_N)\}$, where $ch_i \in \{0,1\}$ $\forall i \in \{1,..,N\}$, is given by $T_{CH_{joint}} = min\{T_{CH_1},\ldots,T_{CH_N}\}$. Since T_{CH_i}, for $\forall i \in \{1,..,N\}$, is exponentially distributed with parameter $u^{1-ch_i}v^{ch_i}$, $T_{CH_{joint}}$ has also exponential distribution with parameter equals $\sum_{i=1}^{N} u^{1-ch_i}v^{ch_i}$ [77].

□

2.4.1 Resource Availability Process Model

The resource availability process is basically a process that describes if there are any resources can be accessed by the cognitive network at any given time. Modeling this process is required for achieving the analytical analysis for some performance measures.

Definition 1. *The resource availability process for N-channel system ($N \geq 2$) is a process $CH = \{CH(t) : t \geq 0\}$ such that:*

$CH(t) = CH_1(t)CH_2(t)\ldots CH_N(t)$.

At any instant of time, the value of $CH \in \{0,1\}$. When CH equals zero, it means that there are some resources can be used by cognitive users. In other words, there is at least one PU channel idle. However, when CH equals one, that indicates all the channels are simultaneously busy and the cognitive network is going through an outage.

The process CH is not Markovian. The state zero in the state space corresponds to all states in the CH_{joint} state space except the state representing the event of all busy channels, i.e., the

state with $CH_i = 1, \forall i \in \{1, .., N\}$. Hence, the transition time of the state zero, denoted by T_0, is a random sum of the transition times of the corresponding CH_{joint} states. As proven in Lemma 1, the probability distribution of the transition time of each CH_{joint} state is exponential, hence T_0 can not be exponential.

2.4.2 Resource Availability Process Statistics

The previously described models are used to derive some of the process statistics, which are important in making decisions concerning the applications that are admissible by the cognitive network. The cognitive users rate of switching, the cognitive network probability of outage, and the rate of outage, are important performance measures. It is of interest to obtain the analytical relationship between those statistics and the dynamics of the spectrum availability.

Switching Model To find the rate of switching, denoted by r_{sw}, we extend the CH_{joint} chain such that each state is represented by $(CH_1, CH_2, \ldots, CH_N, n)$ where $n \in \{1, .., N\}$ indicates the last channel the cluster head was assigned to. For a two-channel system, we show in Fig. 2.2(b) the state-transition diagram for this extended Markov chain. The dashed arrows in the figure represent transitions that involve channel switching. By analyzing the chain for N-channel, we get

$$r_{sw} = \frac{u}{(u/v + 1)^2} + \frac{(N-1)v}{(v/u + 1)^N} \tag{2.1}$$

Where u is a channel idle-to-busy transition rate and v is a channel busy-to-idle transition rate.

Outage Model The cognitive radio network outage rate, the outage probability, and the average outage time formulas can be derived by modeling the number of channels that are simultaneously busy. The evolution of the number of occupied channels over time is a random process $\{i(t) : t \geq 0\}$ where $i \in \{0, 1, \ldots, N\}$. This process is modeled as a Markov chain with $N + 1$ states labeled 0 to N. The state label indicates the number of simultaneously occupied channels. The i^{th} state transition time distribution is exponential with parameter $iv + (N - i)u$ (the proof follows from the proof of Lemma 1). Fig. 2.2(c) shows the state-transition diagram for this chain.

The outage rate, denoted by r_{outage}, is defined as the rate at which all channels become simultaneously busy. It can be obtained by determining the rate at which the state N is visited. By analyzing the chain we obtain

$$r_{outage} = Nv/(1 + v/u)^N \tag{2.2}$$

The outage probability, denoted by P_{outage}, is defined as the percentage of time during which no resources are available. That is the probability that the system is in the state N. It can be expressed as follows

$$P_{outage} = 1/(1 + v/u)^N \tag{2.3}$$

The average outage time, denoted by $\overline{T}_{outage}$, is the average time spent in the state N. It is given by

$$\overline{T}_{outage} = 1/(Nv) \tag{2.4}$$

2.5 Delay Modeling and Characterization

In this section we are interested in analytically characterizing the average time required to deliver a packet within the cognitive radio network. We are considering two delay components, waiting and service delay.

The waiting delay is the time a packet spends at the queue until it starts being served. If a packet arrives to the system while there is a packet under service, the remaining of this service time is included in its waiting time. In addition, if a packet arrives while the queue is not empty, then the waiting time also includes the service time of all the packets ahead of it in the queue. In this section, we achieve the analytical solution for the expected waiting delay and show the way it is related to the service delay and hence to the opportunistically available resources.

The service delay is defined as the time between the instant the packet reaches the head of the queue to the instant it successfully departs the queue. If the cognitive network has access priority, it takes only one slot to serve a packet. The service time of any packet starts and ends at the slot boundaries. However, since the cluster head has only an opportunistic access to the channel, it takes integral (random) multiple of the slot duration to successfully transmit a packet. In this section, we determine the service time distribution and obtain analytically the manner in which the expected service time depends on the dynamics of the spectrum availability.

2.5.1 Residual Service Time

We derive the average waiting delay for our system using the service residual time concept. The concept of the mean residual service time has been considered for evaluating the performance of some continuous-time queueing systems [50]. However, to the best of our knowledge, it has not been considered for evaluating the performance of discrete-time systems. The analysis made for

continuous-time systems can not be readily applied to discrete-time systems. In this section, we determine the mean residual service time for the discrete systems and use it to analyze the delay performance.

2.5.1.1 Residual Service Time Concept

An arrival to the system may experience some delay resulting from the residual service time of one of the packets arrived ahead of it. Let R_i denotes the residual service time seen by the i^{th} arrival. If the j^{th} packet is being served when the i^{th} packet arrives, then R_i corresponds to the remaining time until packet j completes its service. When packet i arrives while the system is empty, then R_i equals zero.

Fig. 2.3 illustrates by example the concept of residual time. In this figure we draw the number of arrivals and departures over time and show the residual service time corresponding to each arrival. X_i denotes the service time of the i^{th} arrival. t_i represents the time at which the i^{th} arrival arrives, and $t_i^{'}$ represents the time at which the i^{th} arrival leaves the system. The residual time can take a non zero value only at the instants at which an arrival occurs.

2.5.1.2 Residual Service Time in Discrete Systems

The evolution of the residual time over time is random, we showed a sample path for a simple example in Fig. 2.3. In continuous systems, the residual time can take a non zero value at any instants since an arrival can occur at any time. However, in discrete systems, the residual time can take a non zero value only at the slot boundaries. Also, since a service time is integral multiples of slot duration and it starts and ends at the slot boundaries, the remaining of a service time as seen by an arrival can only equal integral multiples of the slot duration.

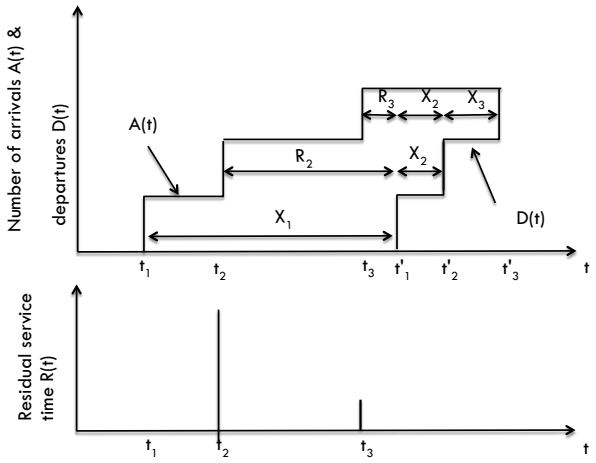

Figure 2.3: The concept of residual service time

Let the service time of the i^{th} arrival starts at the beginning of the k^{th} slot. Assume this service lasts for X_i slots. Let's refer to the residual time at the end of a slot k by r_k, where r_k is measured in slots. The residual times corresponding to the arrivals arrive during the service of the i^{th} arrival are denoted by $r_k, r_{k+1}, \ldots, r_{k+X_i-1}$. Their values are $X_i - 1, X_i - 2, \ldots, 1, 0$ slots, respectively. At the end of the first slot of the service time, the residual time is $X_i - 1$ slots, and its value decreases by one slot at the end of the next slot, and keeps doing so until the service time completes. It equals zero at the end of the last slot of the service time. See Fig. 2.4 for illustration.

For an outside observer, any service corresponds to an arrival arrives right prior to the start of the service. The service that starts at the k^{th} slot corresponds to an arrival arrives at the begining of that slot. Since one packet at most can arrive at any given time slot, no other arrivals can arrive at this particular arrival instant. The residual times at the beginning of any slot at which a service starts is zero. See Fig. 2.4 for illustration.

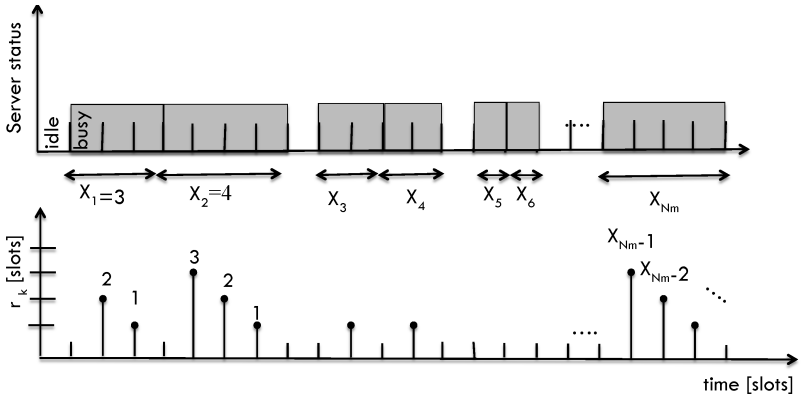

Figure 2.4: A sample path of a server status and the corresponding residual service time.

2.5.1.3 Mean Residual Service Time

According to [50] , the mean residual time as seen by an arrival is equal to the mean residual time seen by an outside observer at a random time. This is valid for any arrivals satisfying the Poisson Arrivals See Time Averages (PASTA) property, which is the case for the queueing systems with Poisson arrival process. The question arises here is what about the Bernoulli arrivals system. Since the Bernoulli Arrivals See Time Averages (BASTA) property for those systems is analogous to the PASTA property in continuous-time systems, we can also define the mean residual time as seen by an arrival (denoted by $\overline{R}$) to be the mean residual time seen by an outside observer at a random time. We use a graphical argument to obtain $\overline{R}$. The analysis we make applies for single and batch arrivals. The residual time of an arrival depends on the arrival instant and not on the number of arrivals arrive at that instant.

The cluster head status over time is random. During any time slot, it could be either busy serving a packet or idle. When a packet i starts to be served, the cluster head stays busy for X_i slots. In Fig. 2.4, we plot a sample path of the cluster head status. We also plot the corresponding

residual service time sample path, which we use to obtain the time average of the residual service time. Consider the time interval [0,τ], where τ is the time instant corresponding to the end of the m^{th} slot. We are assuming that up to the m^{th} slot, N_m packets have already been served. The time average of the residual time (measured in slots) in this interval is given by $E_m = \frac{1}{m}\sum_{k=1}^{m} r_k$.

Since we know the values of r_k's during the service time of each packet (as we explained earlier), the sum of the r_k over the m slots can be determined by summing the r_k's corresponding to the service times. The average time of the residual time can then be rewritten as

$$E_m = \frac{1}{2}\frac{N_m}{m}\left(\frac{\sum_{i=1}^{N_m} {X_i}^2}{N_m} - \frac{\sum_{i=1}^{N_m} X_i}{N_m}\right)$$

Taking the limit as $m \to \infty$, assuming it exists, we obtain

$$\lim_{m\to\infty} E_m = \frac{1}{2}\lim_{m\to\infty}\frac{N_m}{m}\lim_{m\to\infty}\left(\frac{\sum_{i=1}^{N_m} {X_i}^2}{N_m} - \frac{\sum_{i=1}^{N_m} X_i}{N_m}\right)$$

The left-hand side limit is the time average of the residual time. The limits on the right-hand side are the departure rate (which equals the arrival rate), the service time second and first moments respectively. Assuming that the time averages can be replaced by the ensemble averages, the average residual time can then be expressed as

$$\overline{R} = \frac{1}{2}\lambda(\overline{X^2} - \overline{X}) \tag{2.5}$$

where $\overline{X}$ and $\overline{X^2}$ denote the service time first and second moment respectively.

2.5.2 Waiting Delay

We derive the average waiting delay for our system in terms of the average service residual time.

2.5.2.1 Single Arrival Systems

The per-packet average waiting time $\overline{W}$ can be expressed in terms of the average residual time as $\overline{W} = \overline{R}/(1-\rho)$, where $\rho = \lambda\overline{X}$ is the utilization factor [50]. ρ should be less than unity for a stable system [78] and λ is the arrival rate per slot. Replacing $\overline{R}$ with its expression presented in Equation (2.5) yields

$$\overline{W} = \frac{1}{2}\frac{\lambda(\overline{X^2} - \overline{X})}{(1-\rho)} \tag{2.6}$$

2.5.2.2 Batch Arrival Systems

The average waiting time of an arbitrary chosen packet in batch arrival systems is consisting of two independent components. One is the average waiting time of the batch that the packet belongs to, $\overline{W_b}$. The other is the average waiting time within the batch $\overline{W_w}$. The average waiting time $\overline{W_b}$ is the same as the average waiting time of the first packet in the batch. $\overline{W_b}$ equals average residual time of the first packet arrive in the bach plus the average service time of all the packets ahead of the batch in the queue. $\overline{W_b}$ can be expressed as

$$\overline{W_b} = \frac{\overline{R} + \rho\overline{W_w}}{(1-\rho)} \tag{2.7}$$

Denote by A the batch size. The first moment and second moment of A are denote by λ, and $\overline{\lambda^2}$ respectively. For a fixed batch size a, the average waiting of a packet within a batch is given

by $\overline{X}\frac{(a^2-a)}{2a}$. The probability that an arbitrary chosen packet is in a batch of size a is expressed as aP_a/λ, where P_a is the probability that a batch has a size a. Therefore, $\overline{W_w}$ for an arbitrary packet is expressed as

$$\overline{W_w} = \frac{1}{2}\overline{X}(\overline{\lambda^2} - \lambda) \tag{2.8}$$

From Equation (2.7) and (2.8), the per-packet mean waiting time of a batch arrival system can be written as

$$\overline{W} = \frac{\lambda^2(\overline{X^2} - \overline{X}) + \overline{X}(\overline{\lambda^2} - \lambda)}{2\lambda(1-\rho)} \tag{2.9}$$

2.5.3 Service Delay

The service time distribution is a prerequisite for analyzing the delay performance. The analytic solution of the expected waiting delay given in Equations (2.6) and (2.9) involves both the first and second moments of the service time. Delay analysis can still be made if the service time distribution is not realized. However, the exact analysis appears to be very difficult. Depending on the model of the system under consideration, the service time can turn out to be not following any standard distribution. Let's assume that a channel needs to be available for an S amount of time continuously so that a packet can be transmitted. Let's also assume that the cluster head starts to serve packets whenever there is a channel available. It is possible that a cluster head starts to serve a packet and then before it completes its transmission, the channel gets occupied by a PU. This could happen many times in a random manner. This causes the service time to be random and not following any standard distribution.

Inspired by the slotted-Aloha system presented in [50] and [51], we make the following

arguments. Let S denotes the slot duration. Corresponding to our model, at any given slot the cluster head transmits a packet ready for service if there is idle channel. Given that the availability of spectrum is time-variant with some probability channel remains available over the entire slot duration and transmission succeeds. If transmission failed, cluster head retransmits (with probability P_c in case there are number of clusters contend for channels) the packet in the successive slot until transmission succeeds. Denote by μ the probability that the time spent in serving a packet is one slot only. μ can be viewed as the service rate per slot. The service time (measured in slots) needed by the cluster head to successfully transmit a packet is geometric random variable with parameter μ. We derive the expression of μ for the single and multi-cluster systems.

2.5.3.1 Single Cluster Systems

A packet transmission is successful within a time slot if there is at least one channel available during at least the slot duration. The probability of transmission success can be written as $\mu = Pr\{no\ outage\}Pr\{channel\ idle\ time > S\}$.

Using Equation (2.3) which gives the probability of no cognitive network outage and considering the exponential distribution of channel idle time, we obtain

$$\mu = (1 - \frac{1}{(1 + v/u)^N})e^{-uS} \tag{2.10}$$

The packet average delay (denoted by $\overline{T}$) consists of the average waiting delay and the service time average delay. From Equation (2.6), $\overline{T}$ for the single arrival system can be written as

$$\overline{T} = \overline{X} + \frac{1}{2}\frac{\lambda(\overline{X^2} - \overline{X})}{(1 - \lambda\overline{X})} \tag{2.11}$$

2.5.3.2 Multi-cluster Systems

Clusters contend with probability P_c to access primary user channels in multi-cluster system. We illustrate in Fig. 2.5 arrivals state transition diagram for single-arrival multi-cluster system. At any given slot, a packet at cluster head queue waits (i.e., it is in the state labeled WAITING in Fig. 2.5) for service with probability ρ, which is the probability that the cluster head is loaded. When the packet reaches the head of queue (i.e., it makes transition to state ACQUIRING), with probability P_n the cluster head acquires an idle channel. P_n is the probability that there is no outage. The cluster head contends over the acquired channel with probability P_c. The cluster transmits the packet with probability P_nP_c (makes transition to state TRANSMITTING). With probability P_t the transmission succeed and the packet leaves the system. P_t is the probability that no collision occurred over the acquired channel and no primary user reclaims the channel usage right. The average service time $\overline{X}$ corresponds to the average time spent in ACQUIRING and TRANSMITTING states. $\overline{X}$ is given by $1/\mu$. Denote the number of clusters by L. μ can be expressed as

$$\mu = e^{-uS}\Big(\frac{u/v}{1+u/v}\Big)^N (1-P_c)^L \sum_{l=1}^{L}\binom{L-1}{l}\Big(\frac{P_c}{1-P_c}\Big)^l \sum_{i=1}^{N}\binom{N}{i}(u/v)^i\Big(\frac{i-1}{i}\Big)^{l-1} \tag{2.12}$$

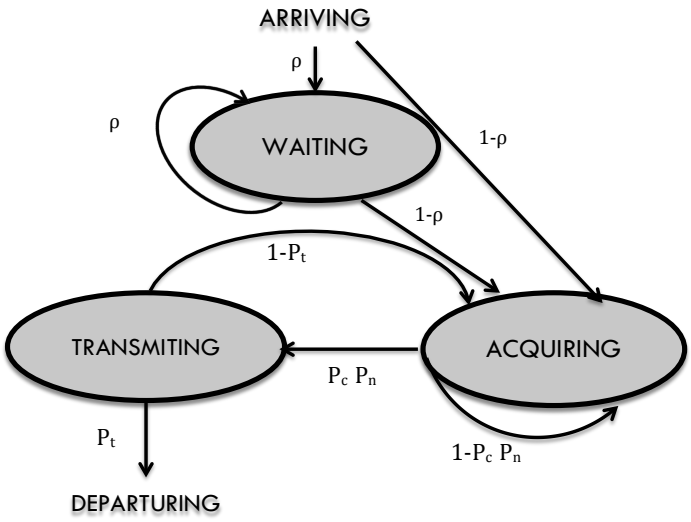

Figure 2.5: Arrivals state transition diagram

2.6 Performance Evaluation and Analysis

In this section, we numerically analyze the impact of the PU behaviors on the statistics of the resource availability process. We also measure the delay performance and study its dependence on the dynamics of the spectrum availability. For convenience, a reference of used network parameters and their descriptions is given in Table 2.1.

2.6.1 Resource Availability Process Statistics Analysis

In Fig. 2.6, we plot the probability of outage (Equation (2.3)) versus the ratio between the average channel idle time to the busy time. Here we refer to the average channel idle and busy interval by $\overline{T}_{idle}$ (which equals $1/u$, where u is the PU idle to busy transition rate) and $\overline{T}_{busy}$ (which equals $1/v$, where v is the PU busy to idle transition rate) respectively.

Table 2.1: Descriptions of Frequently Used Symbols

Parameter	Description
u	A channel idle-to-busy transition rate
v	A channel busy-to-idle transition rate
N	Number of channels
r_{outage}	Outage rate
$\overline{T}_{idle}$	Average channel idle interval
$\overline{T}_{busy}$	Average channel busy interval
λ	Arrival rate per slot
S	Time slot duration

As the ratio $\overline{T}_{idle}/\overline{T}_{busy}$ increases, the outage probability decreases. When this ratio is much less than one, the outage probability can be close to one. Also, as the number of channels N increases, the outage probability decreases. Increasing the number of channels gives the cognitive network more chances to find an idle one. However, as $\overline{T}_{idle}/\overline{T}_{busy}$ increases, the outage occurs with less probability and the effect of having more channels on this probability becomes less. This is an important observation to consider when it comes to making decision about the number of channels a cluster head needs to be able to access to.

Fig. 2.7 plots the effect of the PUs activity on the outage rate, as expressed by Equation (2.2). The observation we make here is when $\overline{T}_{idle}$ is low ($1/u < 1$) and $\overline{T}_{idle}$ is less than $\overline{T}_{busy}$ (i.e., $v < u$), as the value of $\overline{T}_{busy}$ decreases, so does the outage rate r_{outage}. However, for large $\overline{T}_{idle}$, as the $\overline{T}_{busy}$ increases, the r_{outage} decreases. One thinks that the lower the value of the $\overline{T}_{busy}$ is, the better the performance. For example, if the PUs are a cellular network users, one thinks the smaller the average call duration, the better the SUs performance. However, Fig. 2.7 indicates for a large call interarrival time, the longer the call duration, the less the outage rate. The trend for the outage probability change is different though, as shown Fig. 2.6. In other words, as the calls durations increases, the outage probability decreases. That should make sense since the outage rate illustrates how often the network goes through outage, but does not tell how long

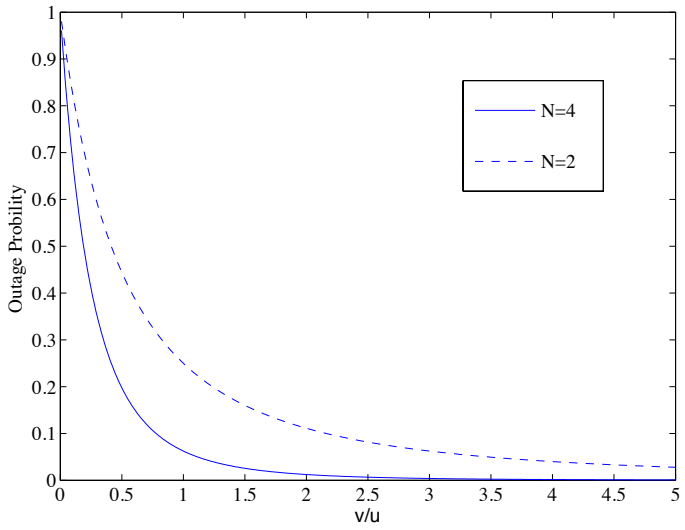

Figure 2.6: Outage probability vs $\overline{T}_{idle}/\overline{T}_{busy}$

the outage is or what its probability is. The different changing trends shows the importance of considering all the different resource availability statistics if one desires to determine if an application is admissible by the cognitive network.

The switching rate is also an important parameter to consider when it comes to designing a multi-channel cognitive network. In practice, there is a communication overhead and energy consumption associated with switching. The graph of switching rate behavior, as described by Equation (2.1), versus $\overline{T}_{idle}$ is shown in Fig. 2.8. An important conclusion we point out from this figure is that the impact of the number of channel on the performance varies depending on the value of $\overline{T}_{idle}$. For a given v value (i.e., $\overline{T}_{busy}$), when $u > 1$ ($\overline{T}_{idle}$ is small) and $\overline{T}_{idle}$ is less than $\overline{T}_{busy}$ (i.e., $v < u$), the larger the number channels N, the higher the switching rate. This is because when the time in which a channel remains idle gets smaller on average, the cluster head needs to switch across the channels more often. As $\overline{T}_{busy}$ increases, the switching rate decreases.

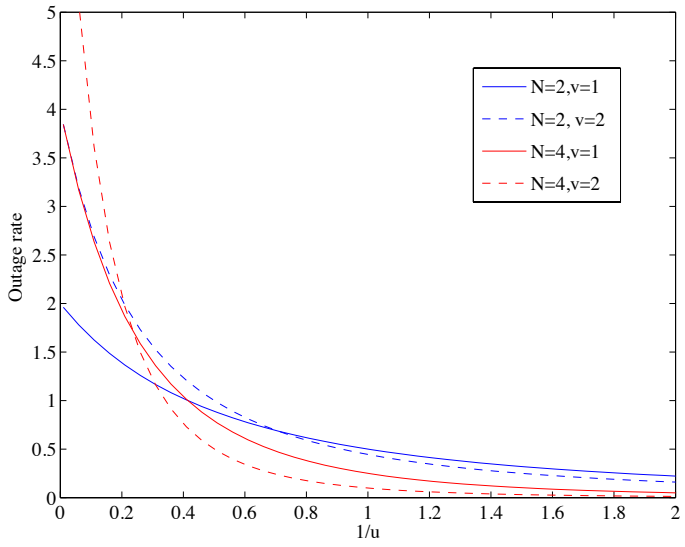

Figure 2.7: Outage rate vs $\overline{T}_{idle}$

It might seem appealing to decrease the switching rate, however, as v and N decrease, the outage probability increases. In fact, the increase in the outage probability is the reason behind the decrease in the switching rate as no switching occurs during the outage. Similar to the observation we made about the outage rate, the trend of switching rate change is different than that for the outage probability. This confirms our conclusion about the importance of considering all these statistics for making designing decisions concerning the cognitive network.

2.6.2 Delay Analysis

For a given SUs' and PUs' traffic parameter, we plot in Fig. 2.9 the delay performance for the single-arrival single-cluster system (Equation (2.11)) versus number of channels. The average delay decreases as number of channels increases, which is intuitive. However, how fast delay decreases and what value the delay converges to depend on the slot duration, the SUs' packet

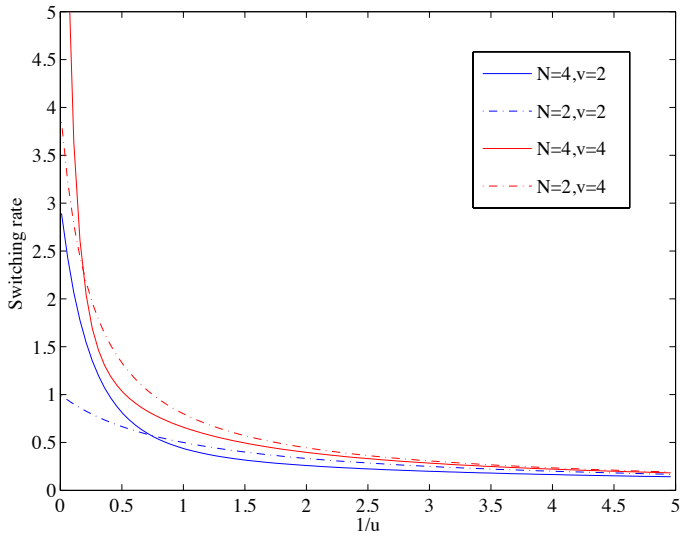

Figure 2.8: Switching rate vs $\overline{T}_{idle}$

arrival rate, and the PUs usage of the channels reflected via the rate at which a channel make transition from idle to busy (u) and from busy to idle (v).

As we explained earlier, as u increases, the outage probability increases. Also, the probability that a channel remains idle for an entire slot duration S decreases. Hence, the average service rate decreases. Since the cluster head uses only one channel at any given time to send data, having more channels while u is large does not improve the performance considerably.

Note that in this and all the subsequent figures, if the results are not shown for a range of values within the horizontal axis, this implies that the delay is unbounded. For a given network setting, if the cluster head can not keep up with the arrival rate, in other words service rate is less than the arrival rate, the network becomes unstable and the delay increases without bounds.

Fig. 2.10 illustrates how Equation (2.11) behaves when $\overline{T}_{idle}$ changes. As $\overline{T}_{idle}$ increases, the performance improves. However, the significance of the improvement depends on some other

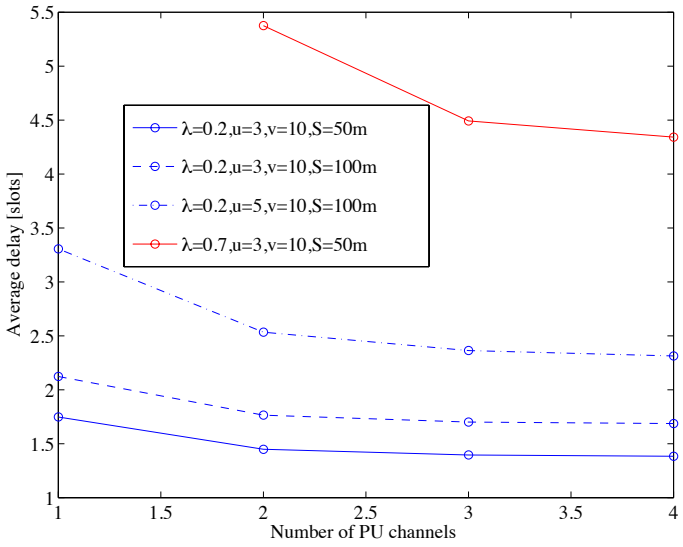

Figure 2.9: Average delay vs. number of PU channels

network settings. We observe from this figure that increasing the number of channels for highly loaded network has more impact on the delay performance than the lightly loaded. Similarly, the impact of increasing the slot duration becomes more severe as the value of λ increases. Increasing the slot duration decreases the probability that a channel can remains idle over the slot duration. Hence, the average service time increases, and so consequently does the average waiting time, especially for large values of λ. The range of $\overline{T}_{idle}$ through which the system is unstable varies depending on the primary and cognitive network settings. In order to maintain the network stability, it is necessary to design the cognitive network such that the traffic arrival rate does not exceed the service rate, which is as expressed in Equation (2.10) is a function of primary users' traffic parameter.

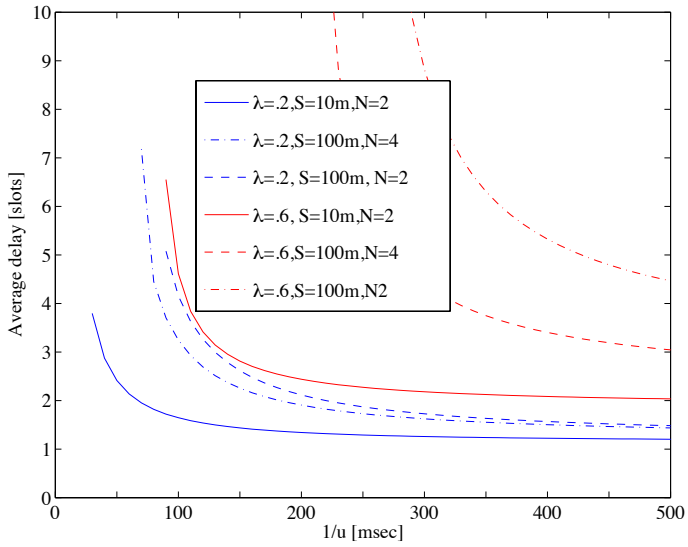

Figure 2.10: Average delay vs average of channel availability time ($\overline{T}_{idle}$)

2.7 Conclusion and Future Work

In this chapter, we have analyzed the dynamics of the spectrum availability and studied the delay performance of a clustered cognitive network. We have introduced the concept of the resource availability process and characterized its properties as a way to measure the network performance. We have also obtained the analytical characterization of the relationship between the packets delay and the dynamics of the spectrum availability. The opportunistically available resources need to be carefully considered in making design decisions regarding the cognitive network to maintain its stability. We plan to study the gain of the multiple-interface transmission on the performance of both discrete-time and continuous-time systems.

Chapter 3: Mitigating Jamming Attacks in Mobile Cognitive Networks Through Pseudorandom Time Hopping

5G wireless networks are expected to support massive connectivity and require lots of spectrum resources, mainly due to device-to-device communications and the high bandwidth demand of next-generation wireless services and applications. An enabling technology for device-to-device links is the dynamical spectrum access, where the devices, to be equipped with cognitive radios, are to be allowed to reuse spectrum occupied by cellular links in opportunistically. However, security threats can severely affect spectrum utilization of these emerging cognitive networks. Jamming attacks for example can disrupt cognitive network communications completely. One potential solution to address these attacks is rely on traditional cryptographic schemes. In this chapter ([49]), we focus on the study and modeling of cognitive radio networks under jamming attacks. Specifically, we model and characterise the impact of the spectrum dynamics on the performance of jammed cognitive networks. While existing anti-jamming mechanisms assume stationary users, in this chapter we propose and evaluate countermeasure solutions for cognitive radio networks whose users are mobile. Unlike existing countermeasure methods, our techniques are not frequency-based and hence do not assume accessibility to multiple channels. In this framework, we derive analytic solutions that capture cognitive mobile network performances terms of their jamming, switching and error capabilities. Our findings show that our techniques outperform their existing frequency-based counterparts.

3.1 Introduction

5G wireless networks are projected to support 1,000-fold gains in capacity and support 100 billion devices in the very near future [79]. Deployment of networks with such a massive capacity and connectivity poses many challenges, among which radio resource management is the most significant. The challenge is even more acute when security concerns are taken into account. Cognitive users can be self-managed as they are capable of observing, learning, and adapting to environment changes. The self-management is a desirable capability when it comes to deploying networks with large number of devices. However, the lack of access priority makes communication between cognitive users more vulnerable to security attacks, and therefore, mechanisms that handle security threats and take into account the volatility of resources need to be designed. Jammers can utilize their transmission capabilities over the limited resources accessible by cognitive users and completely disrupt the communications between them. As mobility of users makes communication channels in both frequency and time dispersive, the challenge of maintaining a desired QoS is even more acute when users are mobile. The focus of this chapter is then on proposing and studying anti-jamming schemes for mobile cognitive users.

3.1.1 Related Work

Jamming attacks in cognitive networks have attracted research attention as they are more detrimental than other types of attacks. Most existing countermeasure approaches (e.g., [43–47]) are based on spectrum handoff. Such countermeasures are only applicable in case multiple channels are accessible. In [43], the authors proposed to randomly allocate the power among multiple channels to anti-jamming. The interactions between jammers and cognitive users were modeled as a Colonel Blotto game. Similarly, the authors in [44] proposed frequency hopping based

countermeasure and modeled the anti-jamming scheme as a game. They applied prospect theory to derive the hopping patterns. As in [43, 44] , the authors in [45] proposed a frequency-based countermeasures. However, while the transmission power is allocated randomly in [43], the authors in [45] proposed to allocate power optimally based on some learning techniques. In [46], the authors assumed that jammers and legitimate users compete sequentially. They modeled their interaction as a game using Stackelberg model. Power is allocated, in their techniques, based on estimated jamming power. [47] modeled spectrum dynamics as partially observed Markov process. The authors in [47] assumed that users learn to retreat from jammers through, similar to the other works, spectral surfing. They applied multiple-armed bandit method to derive their countermeasure. In [48], the authors also considered spectral surfing as a jamming countermeasure with the assumption that secondary users use pre-shared secret keys for channels selection.

3.1.2 Summary of Contributions

Most jamming countermeasures exist in literature are based on frequency hopping. They mainly differ in the strategies used to derive hopping patterns. Due to volatile access opportunities, frequency-based countermeasures are not the best choices in cognitive networks. Since secondary users lack spectrum-access priority, whenever a primary user claims the right to use a channel, they have to vacate it and switch to some other idle one. Mitigating jamming through spectral surfing leads to a higher switching rate. Hence, more energy consumption, delay, and communication overhead in general. In addition, high primary users activity reduces the number of channels accessible by secondary users. Hence, frequency hopping techniques become less effective as primary users become more and more active. More importantly, these techniques work only if multiple channels are accessible. None of them addresses jamming attacks when there is only one channel accessible by legitimate users. To avoid these limitations, we propose to

mitigate jamming through time-based techniques. In the following we summarize the properties of our proposed countermeasures and point out their differences from existing schemes.

- We propose two time-based techniques that work with arbitrary number of channels. They can be as few as one. Existing jamming countermeasures, however, assume accessibility to multiple channels.
- Our techniques do not rely on switching and hence avoid any associated overhead.
- While existing schemes assume stationary users, we assume mobile users. One of our proposed schemes is designed to mitigate jamming and mobility effects as well (see section 3.3.2 for details).
- We obtain closed-form formulas to a number of performance metrics including jamming probability, switching probability, and error probability.
- Our findings show our proposed techniques outperform other existing frequency-based techniques.

3.2 Preliminaries and Models

Notations. Operator $||$ denotes the concatenation. $\lceil x \rceil$ denotes the ceiling of x. $\lfloor x \rfloor$ denotes the floor of x.

Definitions.

1. key derivation function (KDF) is a function with which an input key and other input data are used to generate keying material that can be employed by cryptographic algorithms.

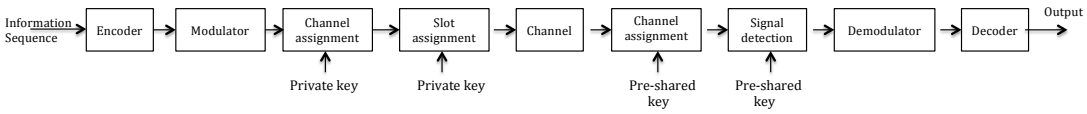

Figure 3.1: Pseudorandom time hopping system block diagram

2. Pseudorandom number generators (PRNG) is a deterministic algorithm used to generate a sequence of bits which looks like random sequence, given as input a short random sequence (the input seed).

Channels Model. Cognitive users have access to N channels licensed to some primary users. Cognitive users opportunistically utilize the spectrum. The occupancy of each channel is modeled as a two-state Markov chain. The average channel idle and busy interval are independent and exponentially distributed with parameters u and v respectively. All channels are assumed to be independent of each other and identical. Channels are both frequency and time dispersive. The frequency dispersion is caused by the relative motion between the two communicating entities. We consider the mobile-to-mobile channel model described in [80]. The model of primary users applies to users in cellular networks. It is popular to model arrival of calls as a Poisson process (i.e., exponentially distributed interarrival times), and the probability distributions of call durations as exponential [81]. Successive interarrival times and call durations are independent of each other in this model.

Secondary Users Model. We assume that there are n connections within the cognitive network at most. Each connection is established between a pair of secondary users which access spectrum opportunistically. Each user accesses no more than one channel at a time. Users operate in a time-slotted mode. They are required to sense the spectrum periodically to avoid interfering with primary users. They also need to vacate a channel if it is detected to be occupied. More

details about how users get assigned to spectrum each transmission period is given in section 4.3.

Jamming Model. We assume that there is jammer in the cognitive network with transmission capabilities similar to secondary users. In other words, jammer is able to identify and exploit spectrum access opportunities. It intentionally disrupts the communication between secondary users. Jammer activities are required to be transparent to licensed users. This assumption is reasonable and widely-used, e.g. [48, 82], and many others consider a similar assumption. To ensure transparency, jammer, similar to legitimate users, is required to perform periodic channel sensing. In fact, we are not concerned about primary users security. We are only addressing jamming attacks in cognitive networks. Back to the model, jammer periodically sense the spectrum to identify the unoccupied channels and pick one of them randomly to launch a jamming attack. Jammer exploits its limited energy to degrade legitimate users performance either by performing partial-time or continuous-time jamming. It aims to make legitimate users switch between channels by making jammed channels unaccessible. However, our main goal is to make legitimate users avoid jamming without having them switch between channels.

3.3 Proposed Schemes and their Analysis

To mitigate jamming, we propose to spread a legitimate user data over time. More specifically, instead of transmitting legitimate user data continuously over time, a user transmits some data over some time, holds for some other random amount time, and then transmits again and so on. The idea is to make the transmission instants look random to jammer. In this way, we impose jammer to jam in a discontinuous way, otherwise, it wastes its limited power (more details about possible jammer interactions and their effects on performance are to discussed). This idea, which we refer to as *time hopping*, is simple yet outperform frequency hopping technique. It is also

used to achieve multiple access. To apply time hopping we propose the two following schemes.

3.3.1 Private Key Based Time Hopping (PKTH)

In PKTH, we consider the capacity of a channel to be subdivided into n portions, where n is the maximum number of connections can be established between secondary users. A user is constrained to use only one portion for data transmission. The allocation is done by dividing the time axis into frames. Each frame is divided into n slots of fixed length (e.g., one bit or one packet long). According to a pairwise shared key, a user allocates one slot per a frame. A block diagram of time hopping transmitter and receiver system is shown in Fig. 3.1. In any signaling interval, time hopping pattern (slots to be occupied by the transmitted signal over time) and channel selections are determined as described in Algorithm 2. As we do not assume multiple channels accessibility, we only consider *time evasion* as a countermeasure in PKTH. However, in case there is more than a channel accessible by the cognitive network, users take the advantage of their pre-shared keys for spectrum access. Spectral surfing is performed to avoid interfering with primary users. To ensure security seeds used for time hopping pattern derivation are different from the ones used for spectrum access. The transmitter pre-shares the key and seeds with the receiver, which in turn removes the pseudorandomness introduced to allocate transmitted signal over time and frequency. We give a high level description of Algorithm 2 below, and discuss its complexity.

Initialization. A trusted third party, which is in our model the primary users network base station, distributes private keys among pairs of users. Keys are generated such that similarities between patterns derived from different pairs are minimal such that multiple access can be achieved [83]. Cellular network base station also assigns an identification number to each legitimate user.

Algorithm 1 Time Hopping Pattern Derivation and Channel Selection Algorithm

Initialization: Executed once after the network deployment.

1: Cellular network base station assigns a private key to each pair of users.

2: Users $\mathcal{X}$ and $\mathcal{Y}$ both determine the slot g ($decision_{TH}$) and channel k ($decision_{CS}$) to be used for transmission. They set a to be $\lceil \log_2 n \rceil$, b to be $\lceil \log_2 N \rceil$, C_{CS}, C_{TH},A ,B all to be one. $Seed_{CS}$ ($Seed_{TH}$) denotes seed used for channel selection (time hopping). s denotes session ID. l denotes the size of users $\mathcal{X}$ and $\mathcal{Y}$ private key K.

Pseudorandom Numbers Generation: Executed by both $\mathcal{X}$ and $\mathcal{Y}$ each session.

3: $Seed_{CS} \leftarrow KDF_K(ID_x \parallel ID_y \parallel s)$.

4: $PRSeq_{CS} \leftarrow PRNG_K(Seed_{CS})$. Denote the binary string $PRSeq_{CS}$ by $\{x_i\}_{i=1}^{l}$.

5: **if** $B = 0$ **then** $B \leftarrow 1$, $C_{CS} \leftarrow 1$, go to 12

6: $Seed_{TH} \leftarrow KDF_K(ID_y \parallel s \parallel ID_x)$.

7: $PRSeq_{TH} \leftarrow PRNG_K(Seed_{TH})$. Denote the $PRSeq_{TH}$ binary string by $\{y_i\}_{i=1}^{l}$.

8: **if** $A = 0$ **then** $A \leftarrow 1$, $C_{TH} \leftarrow 1$, go to 20

Hopping Pattern Derivation: Executed every time frame by both $\mathcal{X}$ and $\mathcal{Y}$.

9: **if** the last assigned channel is idle **then** $decision_{CS} \leftarrow$ no switching.

10: **else**

11: **if** $C_{CS} \leq \left\lfloor \frac{l}{b} \right\rfloor$ **then**

12: $k \leftarrow (\sum_{j=C_{CS}}^{C_{CS}+b-1} x_j 2^j) \mod N$.

13: $C_{CS} \leftarrow C_{CS} + 1$

14: **if** k^{th} channel is idle **then** $decision_{CS} \leftarrow$ switch to k^{th} channel.

15: **else**

16: go to 11

17: **else**

18: $B \leftarrow 0$, update s, go to 3

19: **if** $C_{TH} \leq \left\lfloor \frac{l}{a} \right\rfloor$ **then**

20: $g \leftarrow (\sum_{i=C_{TH}}^{C_{TH}+a-1} y_i 2^i) \mod n$. $decision_{TH} \leftarrow$ allocate g^{th} slot.

21: $C_{TH} \leftarrow C_{TH} + 1$

22: **else**

23: $A \leftarrow 0$, update s, go to 6

Pseudorandom Numbers Generation. Using the private key along with seeds (generated by KDF using session, transmitter and receiver IDs) transmitter and receiver run PRNG to generate pseudorandom sequence of bits used for time hopping pattern derivation (denoted by $PRSeq_{TH}$) and sequence used for channel selection (denoted by $PRSeq_{CS}$).

Hopping Pattern Derivation. The generated pseudorandom sequences $PRSeq_{TH}$ and $PRSeq_{CS}$ are truncated into chunks of $\lceil \log_2 n \rceil$ and $\lceil \log_2 N \rceil$ bits long respectively. The modulo n and modulo N of the decimal numbers corresponding to resulted chunks are used to indicate the allocated slot and channel.

Algorithm complexity The number of accessible channels, the chance of their occupancy, the required level of security required by Algorithm 2 are all factors determine its computational complexity. The type of the employed key derivation function, KDF, and the length of the seed it generates play an important role in determining the running time of the algorithm. We assume that BLAKE hash [84] based key derivation function is applied and analyze the complexity accordingly. In BLAKE based key derivation functions, users hash some secret information (in our case a private key, their id's, and session id) using BLAKE hash function. BLAKE is one of hash functions in the final of National Institute of Standards and Technology (NIST) 2007-2012 Competition for developing cryptographic hash algorithms [85]. There are two main instances of BLAKE, BLAKE-256 and BLAKE-512. They respectively produce 256- and 512-bit digests and run with complexity $\mathcal{O}(256^{1.3})$ and $\mathcal{O}(512^{1.225})$ [84].

The complexity of the pseudorandom number generators, PRNG, algorithm is also affected by the output of the KDF (the input for the PRNG algorithm). The goal of the PRNG algorithm is to generate a number that has a pseudo-random distribution such that no efficient procedure can distinguish it from uniform distribution. The complexity of the PRNG algorithm depends on the type of procedure the generator is secure aganist. In case efficient procedures are associated

with (probabilistic) polynomial time algorithm, the PRNG complexity is a polynomial time (in terms of its input, the seed) [86]. I.e., the PRNG runs in $\mathcal{O}(l_s^L)$ where l_s is the seed length, and L is an integer greater than one. Hence, the complexity of the KDF and PRNG in Algorithm 2 is $\mathcal{O}(l_s^L)$ where l_s equals either 256 or 512 depending on the used hash function. For any given session, executing lines 6-7 is enough for allocating time slot for $\lfloor l/a \rfloor$ time frames. Similarly, lines 3-4 results in allocating a channel for (at most) $\lfloor l/b \rfloor$ time frames. However, since with a probability p_{busy} a channel is occupied by a primary user, it takes $\lceil 1/p_{busy} \rceil$ operations as much, in average, to allocate a channel. The overall computational complexity of the algorithm, hence, is $\mathcal{O}(N_S N_T \left\lceil \frac{1/p_{busy}}{\lfloor l/b \rfloor} \right\rceil l_s^L)$, where N_S is the number of sessions, N_T is the number of time frame within each session assuming, without loss of generality, all sessions have the same number of frames.

To analyze the anti-jamming capabilities of the time hopping system, we assume users employ orthogonal frequency division multiplexing (OFDM) with N_c subcarriers where each subcarrier employs either coherent binary phase shift keying (BPSK) or differential phase shift keying (DPSK) modulation depending on the fading environment.

We further analyze a number of performance measures to evaluate this technique. We analyze the jamming probability and investigate its dependence on primary user behaviors. We also derive the expression of the switching and bit error probability in the presence of jamming attack.

3.3.1.1 Jamming Probability

The dynamical spectrum availability makes cognitive users more vulnerable to jamming. It is important to understand the nature of jamming probability and its dependence on primary user behaviors. The jamming probability has its consequence on the delay performance, error

probability and hence on the network design.

Jamming probability is the probability that a jammer hits both the channel and slot assigned to a legitimate user. At least one channel needs to be idle for a jammer to be able to jam cognitive users communication. A channel idle time and busy time are exponentially distributed with parameters u and v respectively. The average idle and busy intervals are denoted by $\overline{T}_{idle}$ and $\overline{T}_{busy}$ respectively. The probability that a channel is idle, as a result of this model, is given by $\frac{v}{(u+v)}$. Considering that there are N identical and independent channels, the probability that there are exactly i idle channels out of the N accessible channels is given by $\frac{1}{(v/u+1)^{N-i}}\frac{1}{(u/v+1)^{i}}$. A jammer chooses to jam a fraction ρ of each time frame. Jammer sets the value ρ to countermeasure the time hopping technique, as we will see in section 3.3.1.3 and 3.3.2. Conditioning on the availability of i channels, the probability of jamming a channel in a given time frame is $\frac{\rho}{i}$. Recalling that the probability of the availability of i is given by $\frac{1}{(v/u+1)^{N-i}}\frac{1}{(u/v+1)^{i}}$, and considering that there are $\binom{N}{i}$ possible combinations for i idle channels out of the N channels, the jamming probability, denoted by P_j, is expressed as

$$P_j = \sum_{i=1}^{N} \binom{N}{i} \frac{\rho}{i} \frac{1}{(v/u+1)^{N-i}} \frac{1}{(u/v+1)^{i}} \tag{3.1}$$

The graph of this equation for different primary user behaviors and continuous time jamming ($\rho = 1$) is shown in Fig. 3.2. It is observed that P_j changes drastically as primary user activities change. The jammer is gaining from the volatile availability of spectrum. For high levels of primary user activities (i.e., the ratio between u and v is high which means that $\overline{T}_{busy}$/ $\overline{T}_{idle}$ is high), the average number of unoccupied channels can be much less than the total number of channels, which in turn gives jammer a higher chance to disrupt the communication of legitimate users. Another observation we can make is that P_j can be low when there are few channels and u/v is relatively high. The reason is that the resources are lacking for both legitimate users

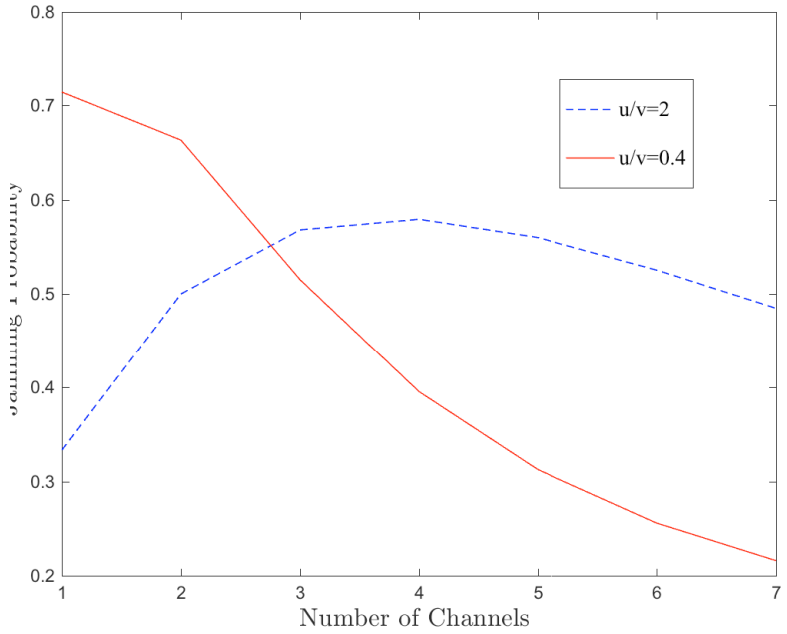

Figure 3.2: Jamming probability vs number of primary user channels

and attacker. In other words, jammer is not able to jam because of lack of access opportunities. Low P_j might seem appealing, but the lack of access opportunities leads to higher transmission delay [30].

3.3.1.2 Switching Probability

In the time hopping systems no switching is performed due to the presence of a jammer. In other words, if a jammer gets to access the same channel that a legitimate user uses, the legitimate user is not required to switch to another channel.

Channels availability and user's offered load β, which is defined as the ratio between the

arrival probability and service probability, determine if a channel handoff needs to be performed within a particular time frame. For stability conditions β is assumed to be less than unity. The arrival probability λ is the probability that a user generates a data packet within a frame duration. The service probability μ is the probability that a cognitive user gets a channel access opportunity for at least slot duration T_s. The service probability, derived in [30], is the probability that at least a channel is idle (which is given by $(1-\frac{1}{(1+v/u)^N})$) multiplied by the probability that the channel is idle for at least a time frame (which is, considering our channel model, given by e^{-uT_s}). In other words, the service probability is expressed as [30]

$$\mu = (1 - \frac{1}{(1+v/u)^N})e^{-uT_s} \tag{3.2}$$

The probability that a user switches between channels at any frame is the probability that the last assigned channel is busy during that frame while there is another channel idle and offered load is greater than zero. The switching probability is written as

$$P_{sw} = \beta \sum_{i=1}^{N-1} \binom{N-1}{i} \frac{1}{(v/u+1)^{N-i}} \frac{1}{(u/v+1)^i} \tag{3.3}$$

The justification behind this equation is similar to that made for Equation(3.1). In Equation(3.3), however, the limit of the sum does not exceed $N-1$. That is intuitive since, excluding the channel a user is currently assigned to, the user can only switch to one of $N-1$ channels at most. In Fig. 3.3, we plot the switching probability for time hopping system along with the corresponding probability in frequency hopping system where legitimate users are required to vacate a channel whenever it is jammed. [47, 48] and some other existing works assume that successful channel jamming leads to switching. We set $u = 2$, $v = 1$, and slot duration $T_s = 100$ msec. It is observed that switching probability for the time hopping system is relatively low. Because of high jamming probability, the switching probability of frequency hopping system is much higher than

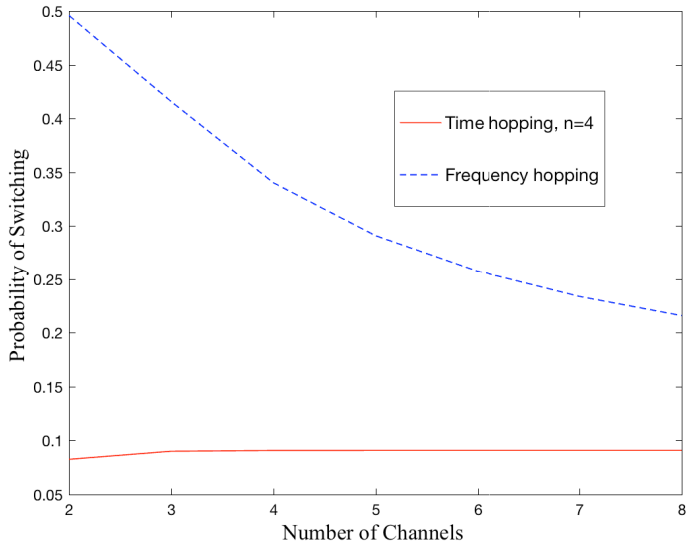

Figure 3.3: Switching probability vs number of primary user channels

that for the time hopping, especially with few channels.

3.3.1.3 Error Probability

We investigate the probability of error for the additive white Gaussian noise (AWGN) channels and mobile-to-mobile fading channels. The jamming signal is modeled as a Gaussian random process with zero mean. Similar jamming signal model is commonly considered in the literature (e.g., [48, 87, 88]).

Error Probability in AWGN Channel The jammer jams ρ fraction of the total frame time. If the jamming power per frame is J, then the received jamming-signal variance per slot is ρJ. Assuming that the jamming power dominates the noise, the probability of error is given by

$$P_e = \sum_{i=1}^{N} \binom{N}{i} \frac{\rho}{i} \frac{1}{(v/u+1)^{N-i}} \frac{1}{(u/v+1)^{i}} Q\Big(\sqrt{\frac{2\rho E_s}{J}}\Big) \tag{3.4}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt$ and E_s is the average symbol energy. Equation (3.4) follows from Equation (3.1) and the BPSK error probability [88].

Attacker sets ρ to countermeasure legitimate user anti-jamming techniques. The jammer selects ρ that causes the worst legitimate users performance. In Fig. 3.4, for several values of E_s/J we plot the probability of error versus jamming fraction time ρ. As legitimate-to-attacker power ratio increases, the attacker can make legitimate users performance worse by focusing its power over smaller fraction time. Otherwise, the attacker wastes its power without degrading the performance of legitimate user significantly. That is to say that by making legitimate user discontinuously transmit its data and randomly allocate data over time, we impose jammer to follow the same strategy (i.e., jam discontinuously), which is turn reduces the probability of jamming.

Error Probability in Mobile-to-Mobile Fading Channel Within each OFDM subcarrier the channel is assumed to be non-selective Rayleigh fading with zero mean Gaussian channel gain. The cross correlation between l^{th} subcarrier channel gain at time $t + \tau$ ($\alpha_l(t + \tau)$) and the and k^{th} subcarrier channel gain at time t ($\alpha_k(t)$) can be factorized into two factors $R_t(\tau)$ and $R_f(\tau)$. While $R_t(\tau)$ represents the temporal correlation of the channel gain, $R_f(\tau)$ represents the correlation across subcarriers. We consider the mobile-to-mobile model described in [80] to characterize our channel. $R_t(\tau)$ in this model is expressed as $2J_0(2\pi f_{m1}\tau)J_0(2\pi f_{m2}\tau)$. Where $J_0(.)$ is the zero order Bessel function. In this model the communicating users both can be in motion. f_{m1}, and f_{m2} are the maximum Doppler frequency due to the motion of the transmitter

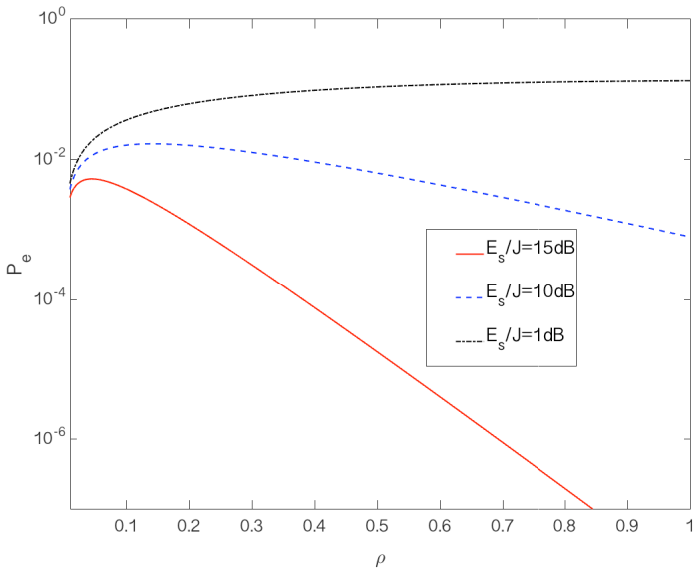

Figure 3.4: Error probability vs jamming fraction

and receiver respectively. Without loss of generality, f_{m2} can be represented in terms of f_{m1} as af_{m1}, where $0 \leq a \leq 1$. The power spectral density $PSD(f)$ corresponding to $R_t(\tau)$ is given in [89] and expressed in Equation(3.3.1.3). The multipath power intensity profile which describes the frequency selectivity of channels is modeled as an exponential.

$$PSD(f) = \frac{1}{\pi^2 f_{m1}\sqrt{a}} \begin{cases} \frac{1}{x}K(\frac{1}{x}) & \text{if } |f| \leq (1-a)f_{m1} \\ K(x) & \text{if } (1-a)f_{m1} < |f| \leq (1+a)f_{m1} \\ 0 & \text{if } |f| > (1+a)f_{m1} \end{cases}$$

where $x \triangleq \frac{1+a}{2\sqrt{a}}\sqrt{1-(\frac{f}{(1+a)f_{m1}})^2}$ and $K(x) \triangleq \int_0^{\pi/2} \frac{dt}{\sqrt{1-x^2 sin^2 t}} dt$ is the complete elliptical integral of the first kind. Due to the mobility of users, all OFDM subchannels experience frequency dispersion, leading to intercarrier interference. The OFDM baseband signal trans-

mitted over the channel is expressed as $s(t) = \frac{1}{\sqrt{T_s}} \sum_{i=0}^{N_{sc}-1} s_i e^{j2\pi i/T_s t}$, where $0 \leq t \leq T_s$, N_{sc} is the number of subcarriers. s_i, $i \in \{1, .., N_{sc}\}$, represents the BPSK symbol at the i^{th} subcarrier. The subcarrier symbols are assumed to be independent and identically distributed, each with zero mean and average energy E_s. The received baseband signal is expressed as $s_r(t) = \frac{1}{\sqrt{T_s}} \sum_{i=0}^{N_{sc}-1} \alpha_i(t) s_i e^{j2\pi i/T_s t} + j(t)$, where $j(t)$ is the jammer signal. The l^{th} subchannel-gain variations over time $\alpha_l(t)$ can be expressed as $\alpha_l(T_s/2) + \acute{\alpha_l}(t - T_s/2)$, $0 \leq t \leq T_s$, where $\acute{\alpha_l}$ is the l^{th} subchannel-gain first derivative [90]. To detect the l^{th} symbol, the received signal is passed through a correlator tuned to the l^{th} frequency. The received l^{th} symbol $\hat{s}_l$ is expressed (as in [88]) as $\frac{1}{\sqrt{T_s}} \int_0^{T_s} s_r(t) e^{-j2\pi f_l t} dt$. Where f_l is the l^{th} carrier frequency. As a result, $\hat{s}_l$ is expressed as

$$\hat{s}_l = \alpha_l(T_s/2) s_l + \frac{T_s}{2j\pi} \sum_{\substack{i=0 \\ i \neq l}}^{N_{sc}-1} \frac{\acute{\alpha_l}(T_s/2) s_l}{(i-l)} + j_l \tag{3.5}$$

Where j_l is the jamming signal at the l^th subcarrier. Due to the mobility of users, subchannels interfere with the l^{th} subcarrier (second term in Equation(3.5)). Considering the power spectral density of the channel, the average power of intercarrier interference at the l^{th} subchannel I_l is expressed as

$$I_l = \frac{4E_s T_s^2}{\pi^2 f_{m1} \sqrt{a}} \sum_{\substack{i=0 \\ i \neq l}}^{N_{sc}-1} \frac{1}{(l-i)^2} \Bigg[\int_0^{(1-a)f_{m1}} f^2 \frac{1}{x} K(\frac{1}{x}) df + \int_{(1-a)f_{m1}}^{(1+a)f_{m1}} f^2 K(x) df \Bigg] \tag{3.6}$$

The probability of error, corresponding to detecting the symbol at the l^{th} subcarrier, is defined only if there exists at least one idle primary user channel. The lack of a channel access

opportunity causes a service delay [30]. The error probability conditioned on the subchannel gain is given by

$$P_{e|\alpha_l} = \sum_{i=1}^{N} \binom{N}{i} \frac{1}{(v/u+1)^{N-i}} \frac{1}{(u/v+1)^{i}} \left[\frac{\rho}{i} Q\left(\sqrt{\frac{2E_s|\alpha_l|^2}{\rho J + I_l}}\right) + \left(1 - \frac{\rho}{i}\right) Q\left(\sqrt{\frac{2E_s|\alpha_l|^2}{I_l}}\right) \right] \tag{3.7}$$

Equation (3.7) can be derived from Equation (3.1) and (3.4). By averaging over the distribution of the subchannel gain we obtain the unconditional error probability which can be expressed as

$$P_e = \frac{1}{2} \sum_{i=1}^{N} \binom{N}{i} \frac{1}{(v/u+1)^{N-i}} \frac{1}{(u/v+1)^{i}} \left[\frac{\rho}{i} \left(1 - \sqrt{\frac{\gamma_1}{1+\gamma_1}}\right) + \left(1 - \frac{\rho}{i}\right) \left(1 - \sqrt{\frac{\gamma_2}{1+\gamma_2}}\right) \right] \tag{3.8}$$

where $\gamma_1 = \frac{2E_s E[|\alpha_l|^2]}{\rho J / + I_l}$, and $\gamma_2 = \frac{2E_s E[|\alpha_l|^2]}{I_l}$. $E[|\alpha_l|^2]$, which is normalized to unity, denotes the average value of $|\alpha_l|^2$. Note that for a deterministic number c, the random variable $c|\alpha_l|^2$ has a chi-square probability distribution given by $c^{-1} exp(-c^{-1}|\alpha_l|^2)$.

In Fig. 3.5, we plot the error probability for the subcarrier in the middle of a channel ($l = 128$). We set the number of primary user channels to four ($N = 4$), number of subcarriers to 256, ρ to 0.1, average busy to idle time to unity ($u/v = 1$), receiver to transmitter speed ratio to be 0.5 ($a = 0.5$), and the product of maximum Doppler frequency and slot duration ($T_s f_{m1}$) to 0.05. We observe from the figure that the probability of error reaches a limit such that any increase in E_s/J no longer improves the performance. In other words, increasing legitimate-to-jammer

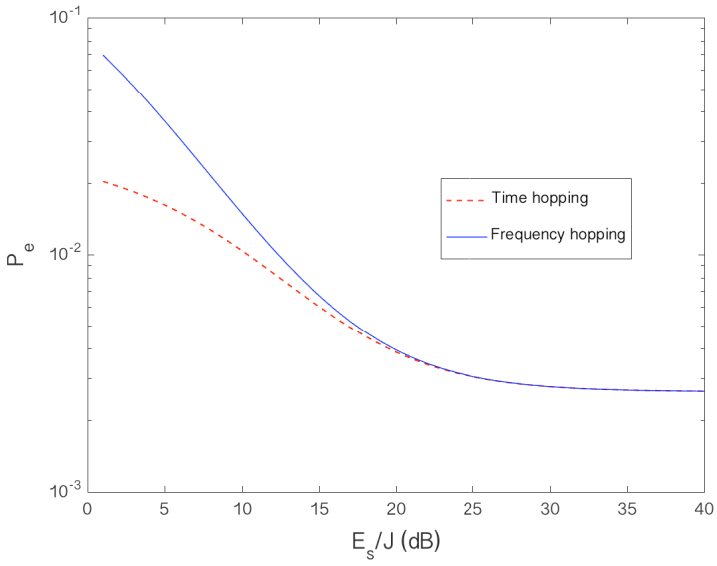

Figure 3.5: Error probability vs legitimate-to-attacker power ratio

power ratio makes no difference after a certain threshold as mobility effects starts to dominate jamming effect. This limit, which can be derived by taking the limit of Equation (3.8) as E_s/J goes to infinity, is referred to as irreducible error probability [91]. For a given transmitter and receiver speed, if a higher quality of service is desired, an adjustment in the slot duration needs to be made (to reduce the value of $T_s f_{m1}$) so that the effect of mobility is mitigated. Also we can observe that for low legitimate-to-attacker power ratio, the pseudorandom time hopping system outperforms the frequency hopping system. In other words, when jamming power is relatively high, our system achieves with less power the same level of performance that frequency hopping systems achieve. That is because, in the time hopping system we enforced jammer to discontinuously jam. One might think that we are not utilizing our resources, as we only allocate one slot for a legitimate user within each frame. However, our system is a multiusers system where each slot can be allocated to a different user. As legitimate-to-attacker power

ratio increases, the intercarrier interference domains the jamming effect and time and frequency hopping systems perform similarly.

To overcome the performance improvement limitations and mitigate the fading channel effects, we propose another time hopping technique.

3.3.2 Selective Diversity Based Time Hopping (SDTH)

SDTH anti-jamming technique is similar to PKTH, however, in this scheme we consider the channel quality in the hopping pattern derivation. The time axis is divided into frames. The time frame is subdivided into s subframes, which are in turn divided into n_s slots. In any signaling interval, based on a shared key, a user selects a subframe. Within the selected subframe, slot to be allocated with user's transmitted signal is determined based on channel quality. Channel envelope-crossing rate, which is the rate at which the transmitted signal envelope crosses a specified level, can be a criteria for channel quality determination. Duration of fades defined as average time during which signal envelope remains below a certain level is another channel quality measure. Mobile-to-mobile channel statistical properties that can be used to determine channel quality over time are analytically characterized in [92]. In SDTH, best channel gain is our criteria for subrames slot allocation. Best gain in the sense that the allocated slot has the maximum channel gain among the subframe slots. The estimation method presented in [93] can be used to determine the channel with the best quality. Channel coherence time, which characterizes the time varying of the frequency dispersiveness caused due to mobility of users, is an important SDTH design parameter that needs to be considered in determination of slot and frame durations. The slot duration should be small (smaller than channel coherence time) so that channel variations within the slot are small. Also, since coherence time quantifies the correlation of channel gain at different times, to ensure security, frame duration should be larger than the

coherence time. In other words, frame durantion should be set such that channel responses for different frames are uncorrelated.

We further analyze analytically the scheme error probability and compare it with the corresponding probability of PKTH. We will show, in different fading environments, SDTH improves the probability of error considerably over PKTH and hence over frequency hopping.

There is a correlation between channel gains at different slots in the subframes, in general. Using the probability joint distribution of channel gains at different slots to obtain the error probability is complicated and does not lead to a closed form solution. The correlation between the channel gains can be described by their joint characteristic function [94]. Considering the correlation between the n_s subframe slots, the error probability of an allocated slot is expressed as [94]

$$P_e = \int_{-\infty}^{\infty} .. \int_{-\infty}^{\infty} CF(x_1, .., x_{n_s}) f(x_1, .., x_{n_s}) dx_1 .. dx_{n_s} \tag{3.9}$$

$CF(x_1, .., x_{n_s})$ is the characteristic function which is defined as $E[e^{j(x_1 r_1 + .. + x_{n_s} r_{n_s})}]$. Where $r_i \triangleq |\alpha_{s_i}|^2$, and α_{s_i} is the i^{th} slot channel gain $\forall\ i \in \{1, .., n_s\}$. r_i is distributed as chi-squared with two degrees of freedom. $CF(x_1, .., x_{n_s})$ is expressed as $det(\mathbf{A})^{-1}$. where $\mathbf{A}(l, l) = 1 - j x_l E[r_l]$, and $\mathbf{A}(l, k) = \sqrt{c V_{r_l} V_{r_k}}\ \forall\ l, k \in \{1, .., n_s\}$. c is the correlation coefficient between r_l and r_k, V_{r_l} is the variance of the random variable r_l. $f(x_1, .., x_{n_s})$ is given by

$$f(x_1, .., x_{n_s}) = \frac{1}{(2\pi)^{n_s}} \int_0^{\infty} P_{e|r} h(r, x_1, .., x_{n_s}) dr \tag{3.10}$$

Where r is the maximum of $r_1, .., r_{n_s}$ and $h(r, x_1, .., x_{n_s})$ is given by

$$h(r, x_1, .., x_{n_s}) = \prod_{l=1}^{n_s} \Bigg[\sum_{k=1}^{n_s} (-1)^{k+1} \sum_{b_1+..+b_{n_s}} \frac{j(b_1 x_1 + .. + b_{n_s})}{exp(jr((b_1 x_1 + .. + b_{n_s})))} \Bigg] \tag{3.11}$$

Depending on the fading environment, it can be difficult for coherent systems such as phase shift keying to maintain coherence over a single pulse duration. With out loss of generality, we consider differential phase shift keying modulation to express P_e. The error probability conditioned on the availability of at least one channel for a fixed r is given by

$$\begin{aligned} P_{e|r} = \frac{\rho}{2} \sum_{i=1}^{N} \binom{N}{i} \frac{1}{i\,(v/u+1)^{N-i}} \frac{1}{(u/v+1)^{i}} \times \\ \Big(exp\Big(-\frac{E_s r}{(J/\rho + I)}\Big) - exp\Big(-\frac{E_s r}{I}\Big) \Big) \\ + \frac{1}{2}\Big(1 - \frac{1}{(v/u+1)^{N}}\Big) exp\Big(-\frac{E_s r}{I}\Big) \end{aligned}$$

Considering the error probability of DPSK [88], Equation (3.12) can be derived similar to Equation (3.4). By plugging Equation (3.12) and (3.11) into equation (3.10) which in turns plugged into (3.9) gives the closed form of the error probability for any fading environment, jamming strategy, and primary user activities level. For mathematical tractability, we evaluate SDTH error probability when number of slots within a subframe n_s is two. In this case, P_e is expressed as follows

$$P_e = \frac{2\rho}{(4\pi)^2}\Bigg[\sum_{i=1}^{N}\binom{N}{i}\frac{1}{i\,(v/u+1)^{N-i}}\frac{1}{(u/v+1)^{i}} \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\Big(f_1(x_1,x_2)-f_2(x_1,x_2)\Big)dx_1dx_2 + \Big(1-\frac{1}{(v/u+1)^{N}}\Big)\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_2(x_1,x_2)dx_1dx_2\Bigg]$$

Where $f_i(x_1, x_2)$ for $i \in \{1, 2\}$ is given by

$$f_i(x_1,x_2) = \frac{1}{(x_1E[r_1]+j)(x_2E[r_2]+j)}\times \frac{(x_1+x_2-2j\gamma_i)}{(x_1-j\gamma_i)(x_2-j\gamma_i)(x_1+x_2-j\gamma_i)} \tag{3.12}$$

Where $\gamma_1 = \frac{E_sE[r]}{J/\rho+I}$, and $\gamma_2 = \frac{E_sE[r]}{I}$.

In Fig. 3.6, we plot SDTH error probability vs legitimate-to-attacker power ratio for various values of correlation coefficient. We consider both the cases when there is no correlation between slots (c=0) and the correlation coefficient is 0.7. We assume that there are two identical primary user channels. The probability that a channel is idle is half. The fraction of jammed frame time ρ is half. The product of maximum Doppler frequency and slot duration is 0.05, the receiver-to-transmitter speed ratio is 0.5. $E[r_1]$ and $E[r_2]$ are normalized with respect to $E[r]$ each equals $4/3$, the variance of both r_1 and r_2 equal four.

Fig. 3.6 shows that SDTH technique reduces error probability significantly over PKTH scheme. The reduction becomes more significant as the intecarrier interference dominates jamming (i.e., as legitimate-to-attacker power ratio increases). Furthermore, we observe that a correlation between slots leads to more performance improvements. The number of slots within a

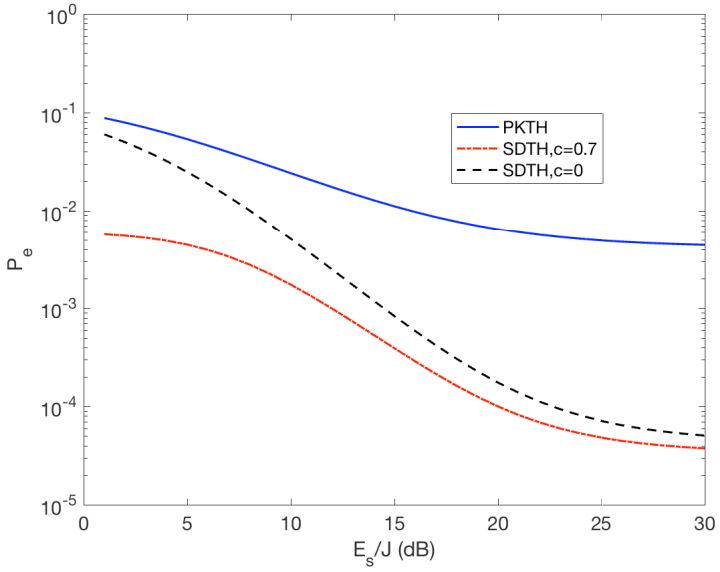

Figure 3.6: Error probability vs legitimate-to-attacker power ratio

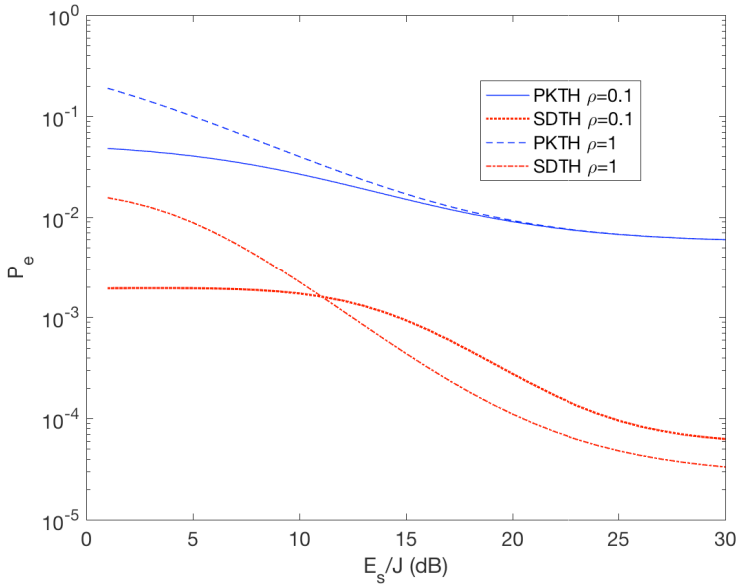

Figure 3.7: Error probability vs legitimate-to-attacker power ratio

frame, number of subframes, and the duration of time slots can all be designed such that slots within a subframe are correlated to maintain a desired error performance.

In Fig. 3.7, for correlation coefficient equals 0.7 and various values of jamming fraction time ρ, we plot the error probability for both PKTH and SDTH. The figure shows that in case of SDTH, when the jammer power is relatively high (i.e, E_s/J is low) as the percentage of time jammed increases, legitimate user performance can be degraded significantly. In other words, if the power of jammer is high, it can contentiously jam ($\rho = 1$) and hence the performance of legitimate user becomes worse than that if it jams partially ($\rho < 1$). However, as jammer-to-legitimate power ratio decreases, the lower the jamming fraction time, the worse the performance it can be. These observations agree with those made from Fig. 3.4 in the sense that jammer can lead to worst case performance depending on its power and percentage of jammed time.

3.4 Conclusion

In this chapter, we have proposed two time based jamming countermeasures. While taking into account jamming attacks, mobility of users, and spectrum availability dynamics, we obtained the analytical solutions of jamming, switching, and error probabilities. We showed that our anti-jamming methods outperform the frequency hopping anti-jamming schemes.

Chapter 4: Optimally Controlled Time-Hopping Anti-Jamming Technique for Mobile Cognitive Radio Networks

We proposed in Chapter 3 cryptographic time-based jamming countermeasures that outperform other existing frequency-based schemes. The techniques proposed in chapter 3 require a secret key to be shared between cognitive users. In this chapter, however, we propose to mitigate jamming through optimal control by controlling the mobility of cognitive users so that desired QoS levels are met. Our proposed approach mitigates jamming while avoiding the overhead associated with secret key sharing. Our approach does so while also achieving better QoS levels and without compromising jamming resiliency.

4.1 Introduction

The availability of resources in cognitive networks varies over time and space depending on primary user behaviors. The process of identifying and exploiting spectrum access opportunities causes performance degradation as we showed in Chapter 2. In addition, jamming the limited resources accessible by cognitive users results in achieving poor QoS levels. Since mobility of cognitive users makes spectrum access opportunities even more stochastic, the performance can be degraded even more when considering mobile users. In this chapter, we propose a time-based framework that is robust against jamming while improving the quality of communication. Our framework introduces randomness over time and controls mobility based on how spectrum access opportunities and channel gains vary over space.

4.1.1 Summary of Contributions

This chapter is an extension of our work presented in chapter 3. We use the idea of time hopping as a way to retreat the jammer. However, the methodology of the data allocation and objectives of the allocation in this chapter are completely different. In the following, we highlight what distinguishes the countermeasure technique proposed in this chapter from existing ones.

- Does not assume, similar to the countermeasure approaches proposed in chapter 3, accessibility to multiple channels. Existing jamming countermeasure approaches, however, assume accessibility to multiple channels.
- Unlike our previously proposed countermeasures, does not require secret keys for data communication.
- Considers cognitive user mobility, where mobility is defined in terms of an agent moving through users. We optimally control the agent mobility to achieve a better quality of service.
- Allocates data optimally by learning the variations of channel gain, spectrum access opportunities, and jammer's strategy over time.

4.2 System and Adversary Models

System Model. We consider cognitive network where each legitimate user is associated to one out of M clusters. Users opportunistically utilize a spectrum, licensed to some primary users. Cognitive users operate in a time-slotted mode, and are required to sense the spectrum periodically to avoid interfering with primary users. The users communicate with a central unit, a cluster head, which moves through the M clusters. This model applies to a cognitive radio

sensor network, where the sensor nodes send their data to a sink, the cluster head in our model, that moves through them and accesses to channels opportunistically. Sensor applications usually generate data in small rates, and hence, there is no need for acquiring a licensed band. The cluster head coordinates spectrum usage through a control channel, and clusters are defined based on the stochastics of spectrum availability and channel variations models (as we will explain later).

Adversary Model. We assume that the cognitive network is subject to random jamming in the sense the jammer alternates, due to energy limitations, between sleeping and jamming modes. In other words, the jammer jams for some random time, and enters sleep mode for some other random time. During the transmission mode, it emits random signal. If legitimate user and adversary happen to transmit signals at the same time, a collision occurs. If no ACK is received, legitimate user detects that a packet is jammed. The jammer is assumed to be reactive as it learns about the success of previously launched attacks and use that to decide about future attacks. Deciding about the success of jamming attacks can be determined by listing to ACK intervals. This type of jamming attack is widely used as it is proven to be effective [95]. Jammer activities are also required to be transparent to licensed users. This assumption is reasonable and widely-used, e.g. [48, 82], and many others consider a similar assumption. To ensure transparency, the jammer is required to perform periodic channel sensing. We also assume that all clusters are subject to a similar jamming, and jammers over different clusters are assumed to apply a similar jamming strategy.

4.3 Problem Formulation and Optimal Solutions

The anti-jamming technique to be proposed needs to achieve the following goals.

- Cluster head needs to adapt its transmission statistics and location to environment variations.

- Cluster head needs to introduce some sort of randomness to maximize the cognitive network throughput while mitigating jamming.

To achieve the above, we adapt our idea of spreading the legitimate user data over time [49]. Instead of transmitting legitimate user data continuously over time, a user transmits some data over some time, holds for some other random amount time, and then transmits again and so on. This way, transmission instants look random to jammer, and as a consequence, jammer is imposed to jam in a discontinuous way, otherwise, it wastes its limited energy [49]. We referred to this technique as time hopping. How to allocate data over time is what distinguishes this work from our previous one. In [49], we assumed users are sharing secret keys which in turn are used to determine transmission instants. In this work, however, no keys are assumed to be shared. The allocation is done by dividing the time axis into frames (or stages), where each frame is divided into N slots of fixed length (one packet long). At any given stage, the cluster head uses the knowledge it has acquired about channel variations and jamming experience to decide about the number packets to be transmitted (or equivalently the number of slots to be occupied). It also uses that to control its mobility. Some rewards are received for each decision the cluster head takes. The goal of the decision process is to determine the optimal actions for a given system state and to use that to coordinate the use and sharing of spectrum among users. Details about system states, system dynamics, accessible actions, and possible rewards are given below. These quantities are used to derive the optimal decisions for any given system state.

4.3.1 System States

At any given frame k, the system state S_k is

$$S_k = A_k, G_k, C_k, N_{k-1}, J_{k-1} \tag{4.1}$$

where k is the discrete time or frame index, $k \in \{1, 2, .., K\}$. A system state at the k^{th} stage S_k is a random variable represents joint of the random variables corresponds to channel accessibility A_k, channel gain G_k, the location of cluster head at that stage C_k, and jamming experience in stage $k-1$ represented by the N_{k-1} and J_{k-1}. The state at first stage is initialized as $A_1, G_1, C_1, 0, 0$.

4.3.1.1 Channel availability

The random variable $A_k \in \{0, 1\}$ expresses the channel availability at stage k. While $A_k = 0$ indicates channel is idle, $A_k = 1$ indicates channel is occupied by a primary user. A_k follows a discrete Markov chain distribution with statistics vary over space. In other words, different clusters observe different primary users activity. The probability that $A_k = i$ given that $A_{k-1} = j$ for a given cluster $C_k = c$, P$\{A_k = i | A_{k-1} = j, C_k = c\}$, is denoted by p_c^{ij} for all $i, j \in \{0, 1\}$.

4.3.1.2 Channel gain

The random variable G_k represents the channel gain. It is modeled, based on [96], as a finite-state Markov process. States correspond to partitioning channel gain amplitude into L nonoverlapping regions $\left[0, v_c^1\right)$, $\left[v_c^1, v_c^2\right)$, ..., $\left[v_c^{L-1}, \infty\right)$, where the v_c^l denotes the l^{th} fading amplitude partition threshold within the c^{th} cluster for all $l \in \{1, 2, .., L-1\}$. Fading amplitude within the c^{th} cluster is assumed to follow Rayleigh distribution with fading channel gain variance σ_c^2. v_c^l is expressed in [96] as

$$v_c^l = \sqrt{-\sigma_c^2 \ln(1 - \frac{l}{L})} \tag{4.2}$$

The transition probabilities between state i and j within the c^{th} cluster, denoted by q_c^{ij}, for i and $j \in \{1, 2, .., L-1\}$ and $i \neq j$ can be written, based on [96], as

$$v_c^l = \sqrt{-\sigma_c^2 \ln(1 - \frac{l}{L})} \tag{4.3}$$

The transition probabilities between state i and j within the c^{th} cluster, denoted by q_c^{ij}, for i and $j \in \{1, 2, .., L-1\}$ and $i \neq j$ can be written, based on [96], as

$$q_c^{ij} \approx \begin{cases} \sqrt{2\pi} L \frac{v_c^l}{\sigma_c} f_D T_f \exp\left(-\frac{(v_c^l)^2}{\sigma_c^2}\right) & \text{if } |i-j| = 1, \\ 0 & \text{otherwise .} \end{cases}$$

Where $l = \max(i, j)$, f_D denotes the Doppler frequency and T_f is the time frame duration. $q_c^{ii} = 1 - q_c^{ii+1} - q_c^{ii-1}\ \forall i \in \{2, .., L-2\}$. The probability of revisiting state 1 & $L-1$ is given by $1 - q_c^{12}$ and $1 - q_c^{L-1L-2}$ respectively.

4.3.1.3 Jamming experience

Adversary tends to increase the chance of jamming data by introducing randomness to its transmission timing. Jammer transmits J_k random number of packets within the frame k, which in turn, results in N_k random number of jammed packets. The randomness introduced is done based on the success of jamming in frame $k-1$. More details about adversary's strategy is given in section 4.3.2.

4.3.1.4 Cluster head mobility

The variable C_k indicates cluster head location at time frame k. To model mobility, we adapt the random waypoint model, origionally proposed in [97]. If at a given time stage k cluster head decides to move to a certain cluster c', it selects a destination point (referred to as waypoint) uniformly distributed in the destination cluster c'. It then moves at a fixed velocity v along the line connecting its current waypoint to the newly selected waypoint. This process repeats at each waypoint. We assume cluster head moves only to neighboring clusters.

To limit the system state space, we do not keep track of the exact physical location of cluster head. Instead, we use C_k to identify the cluster. $C_k = c$ indicates that the cluster head is at c^{th} cluster at the k^{th} decision interval. We assume through out the chapter, without loss of generality, that there are M clusters and they all have same shape and occupy same area. The mobility of cluster head is to be optimally controlled as we explain in section 4.3.3.

4.3.2 System Dynamics

In this subsection we explain how we model system state transitions. Assume that, at the k^{th} ($k > 1$) time frame, the system is at state $s = a, g, c, n, j$ (s is the realization of S_k, a, g, c, n, and j are the realizations of A_k, G_k, C_k, N_{k-1}, and J_{k-1} respectively) and the cluster head decides to transmit d_t^s packets within this frame and moves to the d_m^s clusters. The probability the system evolves, in the following time frame, to a state $s' = a', g', c', n', j'$ (s' is the realization of S_{k+1}, a', g', c', n', and j' are the realizations of $A_{k+1}, G_{k+1}, C_{k+1}, N_k$, and J_k respectively) is given by the state transition probability $T(S_{k+1} = a', g', c', n', j' | S_k = a, g, c, n, j, d_t^s, d_m^s)$. This probability can be written as $P(A_{k+1} = a', G_{k+1} = g', N_k = n', J_k = j' | S_k = a, g, c, n, j, C_{k+1} = c', d_t^s, d_m^s)\ P(C_{k+1} = c' | S_k = a, g, c, n, j, d_t^s, d_m^s)$. The probability cluster head moves to cluster c' conditioned on current location c and a mobility decision d_m^s is independent from other random variables. Current location c and a mobility decision d_m^s are sufficient statistics for determining the chance of c' (this will become more clear as we explain how the decision process works). In other words, the probability $P(C_{k+1} = c' | S_k = a, g, c, n, j, d_t^s, d_m^s)$, denoted as p_c, can be written as $P(C_{k+1} = c' | C_k = c, d_m^s)$. Based on our cluster head mobility model, p_c equals one if c' equals c and zero otherwise. The probability $P(A_{k+1} = a', G_{k+1} = g', N_k = n', J_k = j' | S_k = a, g, c, n, j, C_{k+1} = c', d_t^s, d_m^s)$ can be written as $P(A_{k+1} = a', G_{k+1} = g' | S_k = a, g, c, n, j, C_{k+1} = c', N_k = n', J_k = j', d_t^s, d_m^s)\ P(N_k = n', J_k = j' | S_k = a, g, c, n, j, C_{k+1} = c', d_t^s, d_m^s)$. The channel gain variations are, conditioning on the current gain, independent of the actions of cluster head, jammer and primary users activity. Also, since primary users have priority to access spectrum, their activity (hence channel availability) is independent from the cognitive network activity. In other words, the probability $P(A_{k+1} = a', G_{k+1} = g' | S_k = a, g, c, n, j, C_{k+1} = c', N_k = n', J_k = j', d_t^s, d_m^s)$, denoted by p_{ag}, based on the channel gain and channel availability model, can be expressed as

$$p_{ag} = \begin{cases} p_c^{a'a} q_c^{g'g} & if \text{ c=c'}, \\ \dfrac{p_c^{a'}}{L} & \text{otherwise.} \end{cases}$$

Where $p_c^{a'}$ is the probability the channel is in state a' conditioned in cluster c. $p_c^{a'}$ can be determined easily by solving the channel availability model Markov chain. L is the number of channel gain amplitude partitions. $p_c^{a'a}$ and $q_c^{g'g}$ are respectively defined in section 4.3.1.1 and 4.3.1.2.

The last term determines the state transition probability is $P(N_k = n', J_k = j' | S_k = a, g, c, n, j, C_{k+1} = c', d_t^s, d_m^s)$. We denote this probability by P_j. This probability represents how jammer actions and the number of jammed packets evolve over time. P_j does not depend on the mobility decisions and channel gain by assumption. It, however, depends on channel availability as follows

$$P_j = \begin{cases} 1 & if \text{ a=1 \& n'=j'=0}, \\ P_{j_a} & if \text{ a=0} \\ 0 & \text{otherwise.} \end{cases}$$

That is to say that jammer does not jam unless channel is idle. P_{j_a} equals $P(N_{k+1} = n', J_{k+1} = j' | N_k = n, J_k = j, d_t^s)$ which in turns equals $P(N_{k+1} = n' | N_k = n, J_k = j, J_{k+1} = j', d_t^s) P(J_{k+1} = j' | N_k = n, J_k = j, d_t^s)$. We assume that the j' packets , transmitted by the jammer, are randomly allocated over N possible frame slots. The same assumption holds for the d_t^s packets transmitted by the cluster head. Hence, $P(N_{k+1} = n' | N_k = n, J_k = j, J_{k+1} = j', d_t^s)$, denoted by $P_{n'}$, depends only on jammer and cluster head actions. $P_{n'}$ is expressed as

$$P_{n'} = \begin{cases} \frac{\binom{j'}{n'}\binom{N-j'}{d_t^s-n'}}{\binom{N}{d_t^s}} & \text{if } \max\left(0, d^t - n' + j'\right) \leq n', \\ & \text{\& if } n' \leq \min\left(d_t^s, j'\right). \\ 0 & \text{otherwise .} \end{cases}$$

$P(J_{k+1} = j' | N_k = n, J_k = j, d_t^s)$, denoted by $P_{j'}$, by assumption is given by

$$P_{j'} = \begin{cases} r\binom{N+h}{j'+h} 0.5^{(N+h)} & \text{if } (-1)^{\mathbb{1}(h,p)}\left(j' - j\right) \leq 0. \\ 0 & \text{otherwise .} \end{cases}$$

Where r is a normalization factor, ρ is a random variable equals zero with probability p and one otherwise. h and $\mathbb{1}\left(h, \rho\right)$ are given respectively by

$$h = \begin{cases} -j & \text{if } n \leq 0.5j \text{\& } \rho = 0. \\ 0 & \text{otherwise .} \end{cases}$$

$$\mathbb{1}\left(h, p\right) = \begin{cases} 1 & \text{if } h = -j \text{or } \rho = 1 \text{\& } j' < j. \\ 0 & \text{otherwise .} \end{cases}$$

The intuition behind this jamming strategy is to introduce as much randomness as possible while taking energy limitations into consideration. Equations (4.3.2 to 4.3.2) indicate that if jammer successfully jammed less than fifty percent of what has been transmitted in frame k, it (probabilistically, with probability $1 - p$) transmits J_{k+1} random number of packets, J_{k+1} takes value less than N and greater than j. However, with the same probability, $1 - p$, if successfully jammed more than fifty percent, it jams for less than what has been jammed in time frame k. In other words, J_{k+1} takes value less than j. To avoid predictable actions, with probability p,

jammer jams for J_{k+1} random number of packets with $J_{k+1} \in \{0, 1, .., N\}$ in spite of the previously taken actions. In all cases J_{k+1} is distributed as Binomial(0.5,n), where n, as mentioned, depends on the probability p and the last frame jamming success. In the following subsection we show how to optimally allocate the resources in the presence of such a jammer.

4.3.3 Anti-jamming Scheme

At each stage k, cluster head decides about number of slots d_t^s, to be occupied for data transmission within the stage. $d_t^s \in \{0, 1, .., N\}$ if the channel is idle, d_t^s equals zero otherwise. The set of the admissible decisions for a state s is denoted by D_t^s. Cluster head also decides which cluster to move to d_m^s. Depending on the network model, cluster head speed, time frame duration, and the cluster head location at stage k, cluster head may be, at stage $k+1$, able only to access to one of a limited number of clusters. The set of all admissible mobility decisions for a given state is denoted by D_m^s. A cluster head action results in a reward given by a reward function denoted by $R(S_k, d^s, S_{k+1})$, where d^s denotes the joint of d_m^s and d_t^s $\forall d_m^s \in D_m^s$ and $d_t^s \in D_t^s$. d^s is the decision variable (or control) selected from the control space D^s, where D^s denotes the joint of the two sets D_m^s and D_t^s. S_k and S_{k+1} are the random variables corresponding to current and future states respectively. Assuming that the reward function is additive, the total cost incurred over the horizon, K, is given by

$$\sum_{k=1}^{K} \gamma^k R(S_k, d_,^s S_{k+1}) \tag{4.4}$$

Where γ takes value between 0 and 1. The rewards are discounted (by the factor γ) to indicate that rewards come later in time are less desirable than the current rewards. This can covers the case when jamming threat discontinues.

Considering that the goal of cluster head is to achieve a high data rate while counter-measuring jamming, we choose the reward function to be the *effective throughput*. For s being the current state $s = (a, g, c, n, j)$ (the realization of S_k), and s' being the future state $s' = (a', g', c', n', j')$ (the realization of S_{k+1}), and $d^s = (d^s_m, d^s_t)$ we define the effective throughput as

$$R(s, d^s, s') = \begin{cases} g\left(1 - \dfrac{n'}{d^s_t}\right) if a = 0, \& d^s_t \neq 0. \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad otherwise. \end{cases}$$

The reward function in Equation (4.3.3) captures the effect of channel gain g, channel availability a, as well as jamming effects (in terms of fraction of unjammed packets), motivating cluster head to transmit more while avoiding jammer, and move to clusters where the channel is more accessible and has a higher gain. Hence achieving a better communication quality while mitigating jamming.

The goal of legitimate user is to select the decision d^s such that the total overall reward given by equation (4.4) is maximized. Since the reward function involves number of random variables, it cannot be meaningfully optimized. We therefore formulate the problem as an optimization of the expected cost

$$E\{\sum_{k=1}^{K} \gamma^k R(S_k, d^s_, S_{k+1})\} \tag{4.5}$$

where the expectation is with respect to the transition probability $T(S_{k+1} = s' | S_k = s, d^s)$, derived in section 4.3.2. The optimization is over the control space.

The solution of the problem is to find a policy that specify the optimal control, for each state s, $d^s \in D^s$. At each time frame, our discrete time stochastic control process is in some state, and the decision maker, the cluster head, chooses an action available in the state. The system

randomly, following the transition function derived in section 4.3.2, transit into a new state, and the decision maker gets rewarded according to the action and transition. The transition between states depends on the current state and the cluster head action. Transitions are conditionally independent of all previous states and decisions. In other words, the state transitions of our system satisfy the Markov property, and hence the formulated stochastic control process is a Markov decision process (MDP).

The knowledge the cluster head has about the system model is what determines how to derive the optimal solution of the process. In case cluster head knows the adversary model, optimal solution can be determined analytically via Bellman equation. Bellam equation summarizes the principle of optimality. The optimal value of a state s, denoted by $V^*(s)$, is defined as the expected sum of future discounted rewards a decision maker gets if it acts optimally from the time the state s visited and on words. Bellam equation characterizes $V^*(s)$ as

$$V^*(s) = \max_{d^s} \sum_{s'} T(s'|s, d^s) \left[R(s, d, s') + \gamma V^*(s') \right] \tag{4.6}$$

There are number of algorithms solve Equation (4.6) to determine the optimal policy. E.g. value iteration algorithm [98] and policy iteration algorithm [99]. However, these algorithms require state transition function (the jamming transition model as well as the stochastic environment model) to be explicitly specified. Since in a practical settings, having such a knowledge might not be possible, we use reinforcement learning instead to derive our policy. With reinforcement learning methods, optimal policy can be derived without specifying any underline models. In this chapter, we adapt the Q-learning method originally proposed in [100]. This method associates for each state and action $d^s \in D_s$ a Q-value, denoted by $Q(s, d^s)$. The Q-value quantifies the expected sum of reward as result of committing to decision d^s and acting optimally afterword. The Q-value of a state estimates how good a decision is, and hence used as

a criteria for obtaining the optimal policy. For an observed state s, at the k^{th} decision interval, cluster head takes, with a probability ϵ $\left(\text{we assume it to be equal to } 1 - \frac{1}{\log k+2}\right)$, a decision $d^s \in D_s$ that maximizes $Q(s, d^s)$. As a result of committing to d^s, system lands probalistically into state s', and cluster head updates the Q-value according to the following equation

$$Q(s, d^s) \leftarrow (1-\alpha)\, Q(s, d^s) + \alpha \left[R(s, d^s, s') + \gamma \max_{d^{s'}} Q(s', d^{s'}) \right] \quad (4.7)$$

The first term in equation (4.7) corresponds to the old value of the expected discounted sum of rewards. The other term updates $Q(s, d^s)$ based on current experienced reward $R(s, d^s, s')$ and the estimate of optimal future value $\max_{d^{s'}} Q(s', d^{s'})$ discounted. α is the update coefficient. The value of α at the k^{th} time stage is given, by assumption, by $\frac{1}{\sqrt{k+2}}$. α decays with time to make the influence of future observations less.

Details on how we derive the optimal policy is given in Algorithm 2. The description of the main parts of the algorithm is given below.

Initialization The values of the discount factor γ, update rate α, and the probability ϵ are initialized in this part. Based on the speed of the cluster head v and frame duration T_f, the distance traveled during a frame transmission, denoted by dis_f, is determined.

Decision Making There are two different decisions can be taken in the control process, the transmission decisions and mobility decisions. Transmission decisions are made at each time frame. Mobility actions, however, are taken at the waypoints only. Cluster head holds on taking

decisions for $counter$ number of frames through which cluster head moves between waypoints. Recall that the distance traveled during a frame transmission is denoted by dis_f, and denote the distance between waypoints by dis_w, $counter$ can be expressed as $\left\lceil \frac{dis_w}{dis_f} \right\rceil$. At each time frame k ($k \in \{1, 2, .., K\}$), the system state s is observed. If the state has not been previously observed and cluster head is at a waypoint, a set of available decisions D^s is generated and an action d^s is taken uniformly randomly from the set. The cluster head transmits d_t^s packets uniformly randomly allocated over the k^{th} frame N slots and moves to the d_m^s cluster. If, however, the state has been previously observed, with probability $1 - \epsilon$ (this probability decays with time), it commits uniformly randomly to one of the actions in D^s. With probability ϵ it takes the action that maximizes the Q-value. At any decision interval, cluster head keeps committing to new transmission decisions, it, however, holds to the mobility decision chosen at a previous waypoint until it gets to a new waypoint.

Learning At each time stage k, the Q value corresponds to the observed state and committed action $Q(s, d^s)$ is updated. The value of α and ϵ are also updated. The algorithm is repeated till convergence. The policy, for every state s in the state space, is d^s that maximizes $Q(s, d^s) \forall d^s \in \mathcal{D}^s$.

Algorithm 2 Optimal policy derivation

Initialization:

Set the value of discount factor γ. Initialize the update coefficient $\alpha \leftarrow \frac{1}{\sqrt{2}}$, and action choice probability $\epsilon \leftarrow 1 - \frac{1}{\log 2}$.

Set the distance traveled during a frame transmission dis_f to be vT_f. v is the velocity, and T_f is time frame duration.

Initialize a location tracking counter, $counter \leftarrow 0$, and time stage counter, $k \leftarrow 1$.

Decision Making: Executed each time frame k.

Observe system state, s.

if s is not previously observed **then**

    Generate the admissible decisions set for the state, $\mathcal{D}^s$ (the joint of $\mathcal{D}_t^s$ and $\mathcal{D}_m^s$).

    Initialize $Q(s, d^s)$ to zero $\forall d^s \in \mathcal{D}^s$.

    if $counter$ equals zero **then**

        Take a uniformly random decision d^s from $\mathcal{D}^s$. $d^s = (d_t^s, d_m^s)$.

        Transmit d_t^s packets uniformly randomly allocated over the k^{th} frame N slots.

        Select destination waypoint uniformly distributed within the cluster d_m^s.

        Move at velocity v along the line connecting current to newly selected waypoints.

        $dis_w \leftarrow$ distance between waypoints. $counter \leftarrow \left\lceil \frac{dis_w}{dis_f} \right\rceil$.

        Store the mobility decision d_m^s correspondence to d^s in $d_{m.hold}^s$.

        $counter \leftarrow counter - 1$.

    else

        Take a uniformly random decision d_t^s from $\mathcal{D}_t^s$.

        $d^s \leftarrow (d_t^s, d_{m.hold}^s)$.

        Transmit d_t^s packet uniformly randomly allocated over the k^{th} frame N slots.

        Continue to move to the waypoint previously selected in $d_{m.hold}^s$.

        $counter \leftarrow counter - 1$.

22: **else**
23: **if** $counter$ equals zero **then**
24: With probability ϵ, take transmission action d^s maximizes $Q(s, d^s)$. Take a uniformly random action otherwise.
25: Execute 10 to 15.
26: **else**
27: With probability ϵ, while holding to the previous mobility decision $d^s_{m.hold}$, take transmission action d^s_t maximizes $Q(s, d^s)$. Take a uniformly random d^s_t action otherwise.
28: Execute 19 to Execute 21.
Learning: Executed each time frame.
29: Update $Q(s, d^s)$ according to 4.7.
30: $\alpha \leftarrow \frac{1}{\sqrt{k+2}}$, and $\epsilon \leftarrow 1 - \frac{1}{\log k+2}$.
31: Go to 4 until convergence.
32: For every state s is the state space, the policy is $d^s \leftarrow \max_{d^s} Q(s, d^s) \forall d^s \in \mathcal{D}^s$.

4.4 Performance Evaluation

In this section, we evaluate the proposed framework of allocating data over time through formulating the system as an MDP. We compare the performance of our system with that of the cryptography-based allocation system [49]. The anti-jamming scheme proposed in [49] allocates data pseudo-randomly such that the chance a cluster head decides to transmit at any given slot is uniformly random. Throughout this section, we assume that our network has eight-hexagonal clusters, all occupying the same area. The cluster head is assumed to move to neighboring clusters only. The model of the network is presented in Fig.(4.1). The Markov chain model for the communication channel over each cluster is also given in Fig.(4.1). State transition probabilities for the two-state chain are provided in this figure. The two states are labeled idle and busy to represent channel idle and busy events respectively. The channel gain variance for each cluster is also included in Fig. (4.1).

As done in [96], the channel gain is assumed to be partitioned into eight levels. The product

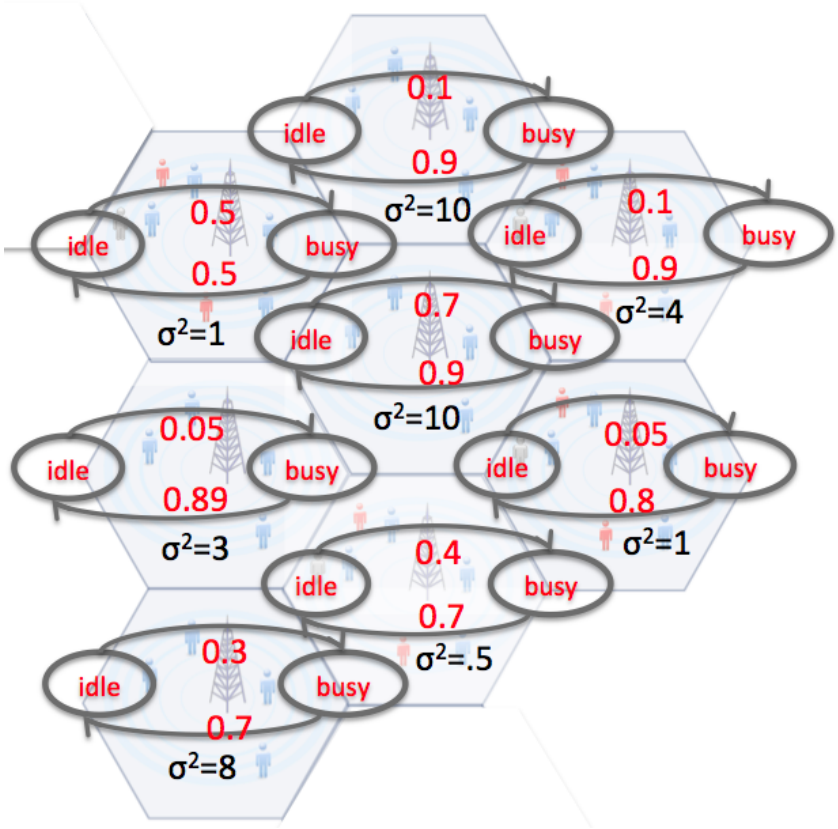

Figure 4.1: Channel model parameters

of Doppler frequency and time frame duration $f_D T_f$ is set to be 0.01. We fix waypoints to cluster centers for simplicity, and assume the distance required to transmit a frame dis_f is the same as the distance traveled from cluster center to cluster edge. In practice, however, there is a number of localization services that can provide a mobile entity with an accurate estimate of its own location and provide directory services and hence waypoints location can be made more general. The discount factor γ in our control process is set to 0.9. The number of slots within each frame N are assumed to be four. Due to jammer energy constraint, we assume it jams fifty percent of the time at most. Jammer evolves as described in 4.3.2.

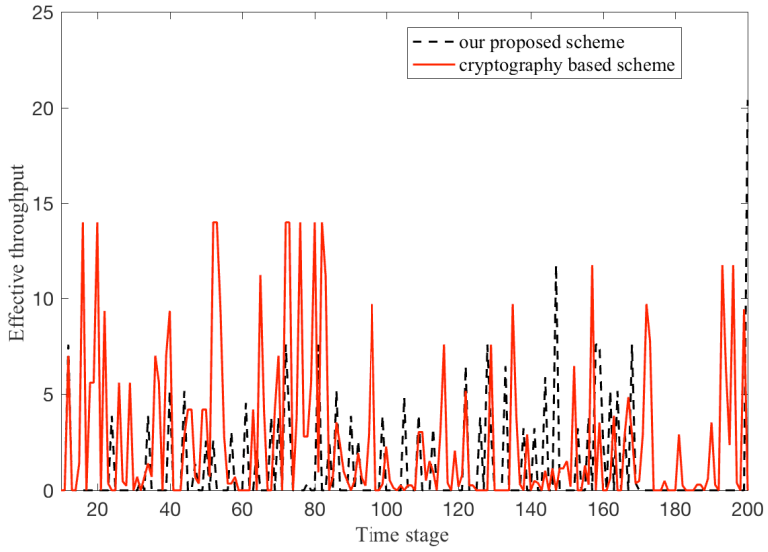

Figure 4.2: Instantaneous effective throughput

We simulate the network with the aforementioned system set up and plot in Fig.(4.2) the instantaneous effective throughput for relatively early time stages. As mentioned before, we consider the cryptography-based allocation time hopping proposed in [49] as our baseline. Transmission decisions in this scheme are made, at any given slot, uniformly random. Mobility decisions are also assumed to be made uniformly random. Fig.(4.2) reveals that our proposed scheme performs similar to our baseline. However, as shown in Fig. (4.3), as we proceed in time, cluster head learns when and how long to transmit and where to move resulting in more successful transmissions.

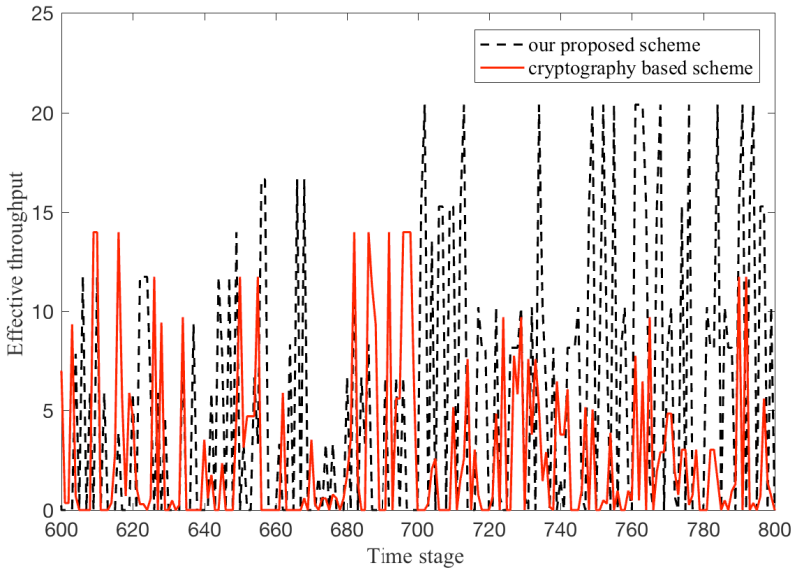

Figure 4.3: Instantaneous effective throughput

The average effective throughput shown in Fig.(4.4) confirms this observation. At any given time stage, the effective throughput is averaged over the current and all preceding stages. This figure shows that our scheme is able to achieve more successful transmissions with better channel conditions.

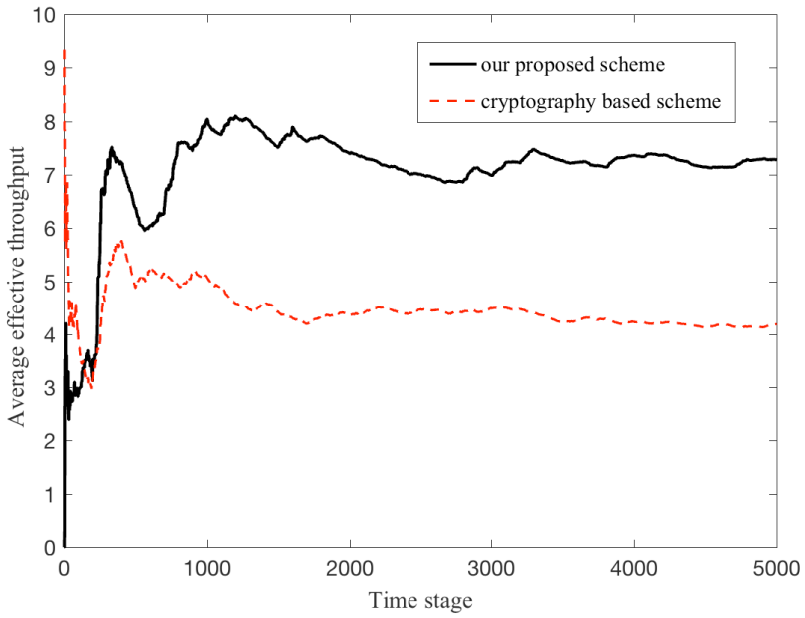

Figure 4.4: Average effective throughput versus time

One might think that we are sacrificing jamming probability for effective throughput. In other words, one might think we, in our scheme, transmit more than the baseline scheme to achieve more throughput and as a result we get jammed more. To show that this is not the case, we plot in Fig.(4.5) the probability of jamming versus time stages. The probability of jamming at any given time stage k is defined as the ratio between the number of jammed packets in stages 1 to k to the number of transmission attempts made in those stages. As the figure shows, our scheme achieves a similar jamming probability in the long term. Due to the randomness introduced by the jammer and the similarity of jamming effects over space, cluster head is not able to gain much over the cryptography based scheme in terms of probability of jamming. However, the goal of our scheme is not to avoid the jamming only but also to get best of resources when there

is no jamming.

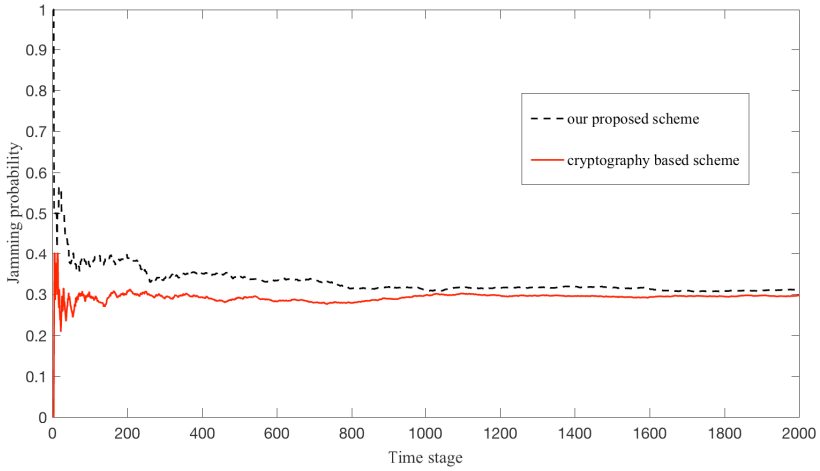

Figure 4.5: Probability of jamming versus time

Since we control mobility in our scheme, it is important to analyze the effect of speed on the performance. Since Doppler frequency is directly proportional to the speed, we only vary the normalized Doppler frequency ($f_D T_f$) and evaluate the performance. We consider $f_D T_f = 0.01$ as our reference value, we use it to normalize other values of $f_D T_f$. In Fig. (4.6), we plot the average throughput for different values of $f_D T_f$ normalized to the reference $f_D T_f$. To come up with the results shown in Fig. (4.6) (and the figures come later), we simulate our network, run our decision algorithm and evaluate the average effective throughput. We repeated the same thing hundreds of times (or iterations). The results in Fig. (4.6) correspond to the average over all iterations of obtained average effective throughput. We assume that for $f_D T_f$ equals 0.01, cluster head holds from taking mobility decisions for two frames after it gets to a new waypoint. For the other values of $f_D T_f$, cluster head holds for twice the ratio between the $f_D T_f$ and the $f_D T_f$ reference.

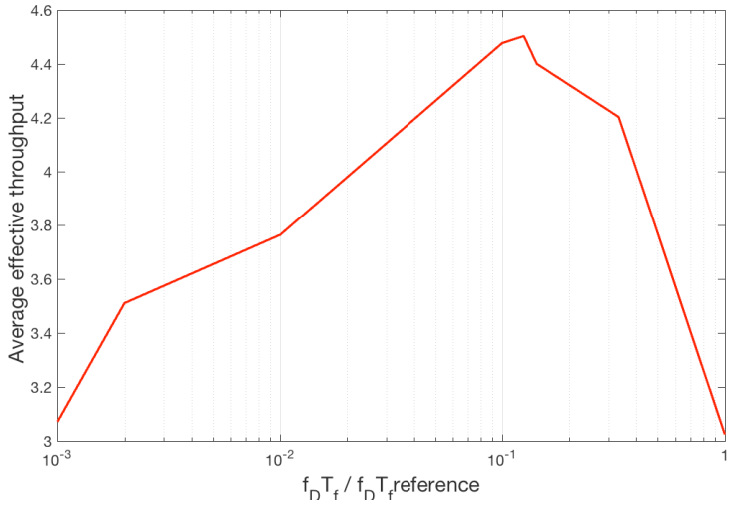

Figure 4.6: Average effective throughput versus normalized $f_D T_f$

As we can see form Fig. (4.6), for a relatively low mobility speed, the average effective throughput is relatively low. However, as speed becomes higher, the performance starts to improve. This is intuitive as the cluster head takes more advantage of the environment variations as it moves faster. The performance starts to degrade again, however, as the speed increases more and more. That is also intuitive. As the cluster head speeds up more, the fading effects becomes more significant, hence degrading the performance.

To analyze the effect of speed even more, in Fig. (4.7) we plot, for different $f_D T_f$ to $f_D T_f reference$ ratio, the average effective throughput for various iteration numbers. In each iteration we limit the simulation to several million time frames and evaluate the performance. It is important to evaluate the performance over a limited amount of time as it is important to evaluate if the network can achieve a desired quality of service not only in the long term but also in the short term as well.

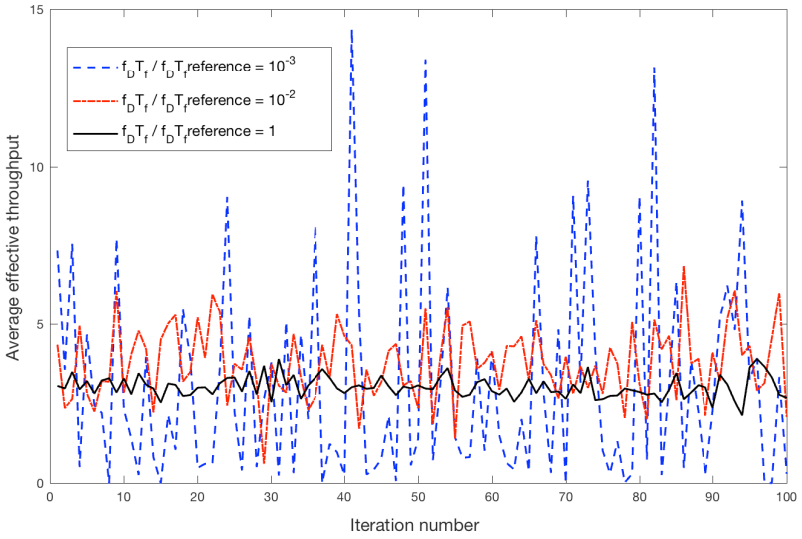

Figure 4.7: Average effective throughput versus iteration number

As we can notice from this figure, as the speed gets slower, the performance varies more drastically from iteration to another. The variation becomes less and less as the speed reaches the reference speeds. The reason behind this is that as the cluster head moves faster it becomes able to achieve a performance close to the average no matter what the initial condition is. However, as the speed gets slower, the cluster head takes longer time to leave a cluster, and as a result, it might "stuck" to poor transmission conditions for a while and hence, depending on the initial system state, it performs poorly.

To conclude, at a relatively low speed, the system can achieve a performance that is higher than any other speed. However, achieving such a performance is very sensitive to the initial state of the system. As speed increases, sensitivity to system initial state starts to diminish, but with more mobility fading effects. It is important to choose a cluster head speed that leads to achieving a desired quality of service.

4.5 Conclusion

In this chapter, we have proposed a time based environment aware anti-jamming scheme. Specifically, we proposed a mathematical framework for modeling decision process that allocates resources and controls network mobility over time. The model takes into account jamming attacks, channel gain variations, and spectrum availability dynamics. We showed that our resource allocation scheme outperforms other cryptography-based schemes.

Chapter 5: Dissertation Conclusions

In this thesis, we have modeled the spectrum dynamics in cognitive networks, and studied its impact on a number of performance metrics. Specifically, we characterized the spectrum handoff process cognitive radio users need to perform as a way to adapt to their wireless environment. We also derived some important statistics of the network outage that results from the lack of access opportunities. Furthermore, we modelled, characterised, and analyzed analytically the average of both the queueing and service delays. We also showed the impact of spectrum dynamics on network stability measured in terms of the total packet delay of the cognitive user. Moreover, in this thesis, we proposed and studied methods for mitigating jamming when considering mobile cognitive users in cognitive radio networks. We proposed a time-hopping based countermeasure solutions, where hopping patterns are derived based on cryptographic, estimation, as well as on learning techniques. Our findings showed that these techniques outperform some other existing ones.

Bibliography

[1] F. S. P. T. Force, "Report of the spectrum efficiency working group," 2002.

[2] D. Datla, A. M. Wyglinski, and G. J. Minden, "A spectrum surveying framework for dynamic spectrum access networks," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 8, pp. 4158–4168, 2009.

[3] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, pp. 13–18, Aug 1999.

[4] B. Hamdaoui and K. G. Shin, "OS-MAC: An efficient MAC protocol for spectrum-agile wireless networks," *Mobile Computing, IEEE Transactions on*, vol. 7, no. 8, pp. 915–930, 2008.

[5] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 201–220, Feb 2005.

[6] I. F. Akyildiz, W.-Y. Lee, M. C. 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.

[7] M. NoroozOliaee, B. Hamdaoui, and K. Tumer, "Efficient objective functions for coordinated learning in large-scale distributed osa systems," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 931–944, 2013.

[8] M. Guizani, B. Khalfi, M. B. Ghorbel, and B. Hamdaoui, "Large-scale cognitive cellular systems: resource management overview," *IEEE Communications Magazine*, vol. 53, no. 5, pp. 44–51, 2015.

[9] M. NoroozOliaee, B. Hamdaoui, and M. Guizani, "Maximizing secondary-user satisfaction in large-scale dsa systems through distributed team cooperation," *IEEE Transactions on Wireless Communications*, vol. 11, no. 10, pp. 3588–3597, 2012.

[10] M. B. Ghorbel, B. Hamdaoui, M. Guizani, and B. Khalfi, "Distributed learning-based cross-layer technique for energy-efficient multicarrier dynamic spectrum access with adaptive power allocation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 1665–1674, 2016.

[11] M. J. N. Oliaee, B. Hamdaoui, and M. Guizani, "Adaptive service function for system reward maximization under elastic traffic model," in *2013 IEEE Global Communications Conference (GLOBECOM)*, pp. 4781–4785, IEEE, 2013.

[12] B. Khalfi, M. B. Ghorbel, B. Hamdaoui, and M. Guizani, "Dynamic power pricing using distributed resource allocation for large-scale dsa systems," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1090–1094, IEEE, 2015.

[13] M. B. Ghorbel, B. Khalfi, B. Hamdaoui, and M. Guizani, "Power allocation analysis for dynamic power utility in cognitive radio systems," in *2015 IEEE International Conference on Communications (ICC)*, pp. 3732–3737, IEEE, 2015.

[14] T. Touzri, M. B. Ghorbel, B. Hamdaoui, M. Guizani, and B. Khalfi, "Efficient usage of renewable energy in communication systems using dynamic spectrum allocation and collaborative hybrid powering," *IEEE Transactions on Wireless Communications*, vol. 15, no. 5, pp. 3327–3338, 2016.

[15] N. Adem and B. Hamdaoui, "The impact of stochastic resource availability on cognitive network performance: modeling and analysis," *Wireless Communications and Mobile Computing*, vol. 16, no. 12, pp. 1642–1653, 2016. wcm.2640.

[16] N. Adem and B. Hamdaoui, "Mitigating jamming attacks in mobile cognitive networks through time hopping," *Wireless Communications and Mobile Computing*.

[17] N. Adem and B. Hamdaoui, "Delay performance modeling and analysis in clustered cognitive radio networks," in *Global Communications Conference (GLOBECOM), 2014 IEEE*, pp. 193–198, Dec 2014.

[18] O. Filio-Rodriguez, S. Primak, V. Kontorovich, and A. Shami, "On a cognitive radio networks random access game with a poisson number of secondary users," *IEEE Communications Letters*, 2015.

[19] L.-C. Wang, C.-W. Wang, and C.-J. Chang, "Modeling and analysis for spectrum handoffs in cognitive radio networks," *Mobile Computing, IEEE Transactions on*, vol. 11, no. 9, pp. 1499–1513, 2012.

[20] R. Hamdi, M. B. Ghorbel, B. Hamdaoui, M. Guizani, and B. Khalfi, "Implementation and analysis of reward functions under different traffic models for distributed dsa systems," *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 5147–5155, 2015.

[21] S. Ehsan, B. Hamdaoui, and M. Guizani, "Feasibility conditions for rate-constrained routing in power-limited multichannel wsns," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pp. 1–6, IEEE, 2011.

[22] S. Wang, J. Zhang, and L. Tong, "Delay analysis for cognitive radio networks with random access: A fluid queue view," in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–9, IEEE, 2010.

[23] A. Laourine, S. Chen, and L. Tong, "Queuing analysis in multichannel cognitive spectrum access: A large deviation approach," in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–9, IEEE, 2010.

[24] S. Feng and D. Zhao, "Supporting real-time cbr traffic in a cognitive radio sensor network," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, pp. 1–6, IEEE, 2010.

[25] K. Zheng, J. Luo, J. Zhang, W. Wu, X. Tian, and X. Wang, "Cooperation improves delay in cognitive networks with hybrid random walk,"

[26] Z. Liang, S. Feng, D. Zhao, and X. S. Shen, "Delay performance analysis for supporting real-time traffic in a cognitive radio sensor network," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 1, pp. 325–335, 2011.

[27] V. K. Tumuluru, P. Wang, D. Niyato, and W. Song, "Performance analysis of cognitive radio spectrum access with prioritized traffic," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 4, pp. 1895–1906, 2012.

[28] M. M. Rashid, M. J. Hossain, E. Hossain, and V. K. Bhargava, "Opportunistic spectrum access in cognitive radio networks: A queueing analytic model and admission controller design," in *Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE*, pp. 4647–4652, IEEE, 2007.

[29] M. NoroozOliaee and B. Hamdaoui, "Analysis of guard-band-aware spectrum bonding and aggregation in multi-channel access cognitive radio networks," in *2016 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2016.

[30] N. Adem and B. Hamdaoui, "Delay performance modeling and analysis in clustered cognitive radio networks," in *Global Communications Conference (GLOBECOM), 2014 IEEE*, pp. 193–198, Dec 2014.

[31] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 17, pp. 1023–1043, Secondquarter 2015.

[32] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, pp. 25–37, Jan 2008.

[33] D. Shan, K. Zeng, P. Richardson, and W. Xiang, "Detecting multi-channel wireless microphone user emulation attacks in white space with noise," in *Cognitive Radio Oriented Wireless Networks (CROWNCOM), 2013 8th International Conference on*, pp. 154–159, July 2013.

[34] K. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*, pp. 2935–2939, May 2013.

[35] W.-L. Chin, C.-L. Tseng, C.-S. Tsai, W.-C. Kao, and C.-W. Kao, "Channel-based detection of primary user emulation attacks in cognitive radios," in *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th*, pp. 1–5, May 2012.

[36] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *INFOCOM, 2013 Proceedings IEEE*, pp. 2751–2759, April 2013.

[37] S. Liu, H. Zhu, R. Du, C. Chen, and X. Guan, "Location privacy preserving dynamic spectrum auction in cognitive radio network," in *Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference on*, pp. 256–265, July 2013.

[38] M. Grissa, A. Yavuz, and B. Hamdaoui, "An efficient technique for protecting location privacy of cooperative spectrum sensing users," in *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, 2016.

[39] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *Wireless Communications, IEEE Transactions on*, vol. 9, pp. 3554–3565, November 2010.

[40] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *Wireless Communications, IEEE*, vol. 19, pp. 106–112, December 2012.

[41] M. Grissa, A. Yavuz, and B. Hamdaoui, "LPOS: locaion privacy for optimal sensing in cognitive radio networks," in *Global Communications Conference (GLOBECOM), 2015 IEEE*, 2015.

[42] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pp. 64–78, May 2008.

[43] Y. Wu, B. Wang, and T. Liu, K.J.R. ; Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *Selected Areas in Communications, IEEE Journal on*, vol. 30, pp. 4–15, January 2012.

[44] L. Xiao, J. Liu, Y. Li, N. Mandayam, and H. Poor, "Prospect theoretic analysis of anti-jamming communications in cognitive radio networks," in *Global Communications Conference (GLOBECOM), 2014 IEEE*, pp. 746–751, Dec 2014.

[45] K. Dabcevic, A. Betancourt, L. Marcenaro, and C. Regazzoni, "A fictitious play-based game-theoretical approach to alleviating jamming attacks for cognitive radios," in *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, pp. 8158–8162, May 2014.

[46] L. Xiao, T. Chen, J. Liu, and H. Dai, "Anti-jamming transmission stackelberg game with observation errors," *Communications Letters, IEEE*, vol. 19, pp. 949–952, June 2015.

[47] H. Su, Q. Wang, K. Ren, and K. Xing, "Jamming-resilient dynamic spectrum access for cognitive radio networks," in *Communications (ICC), 2011 IEEE International Conference on*, pp. 1–5, June 2011.

[48] X. Li and W. Cadeau, "Anti-jamming performance of cognitive radio networks," in *Information Sciences and Systems (CISS), 2011 45th Annual Conference on*, pp. 1–6, March 2011.

[49] N. Adem, B. Hamdaoui, and A. Yavuz, "Pseudorandom time-hopping anti-jamming technique for mobile cognitive users," in *2015 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, Dec 2015.

[50] D. P. Bertsekas, R. G. bertsekas1992data, and P. Humblet, *Data networks*, vol. 2. Prentice-Hall International New Jersey, 1992.

[51] T. Wan and A. U. Sheikh, "Performance and stability analysis of buffered slotted aloha protocols using tagged user approach," *Vehicular Technology, IEEE Transactions on*, vol. 49, no. 2, pp. 582–593, 2000.

[52] S. Ehsan, B. Hamdaoui, and M. Guizani, "Radio and medium access contention aware routing for lifetime maximization in multichannel sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 9, pp. 3058–3067, 2012.

[53] R. Hamdi, M. Ben Ghorbel, B. Hamdaoui, and M. Guizani, "Design and implementation of distributed dynamic spectrum allocation protocol," in *Communications Workshops (ICC), 2014 IEEE International Conference on*, pp. 274–278, IEEE, 2014.

[54] C. Cormio and K. R. Chowdhury, "A survey on MAC protocols for cognitive radio networks," *Ad Hoc Networks*, vol. 7, no. 7, pp. 1315–1329, 2009.

[55] M. Maiya and B. Hamdaoui, "iMAC: improved medium access control for multi-channel multi-hop wireless networks," *Wireless Communications and Mobile Computing*, vol. 13, no. 11, pp. 1060–1071, 2013.

[56] A. Sivanantha, B. Hamdaoui, M. Guizani, X. Cheng, and T. Znati, "EM-MAC: An energy-aware multi-channel MAC protocol for multi-hop wireless networks," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International*, pp. 1159–1164, IEEE, 2012.

[57] K. Arshad and K. Moessner, "Robust collaborative spectrum sensing based on beta reputation system," in *Future Network & Mobile Summit (FutureNetw), 2011*, pp. 1–8, IEEE, 2011.

[58] J. Shen, T. Jiang, S. Liu, and Z. Zhang, "Maximum channel throughput via cooperative spectrum sensing in cognitive radio networks," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 10, pp. 5166–5175, 2009.

[59] O. Altrad, S. Muhaidat, A. Al-Dweik, A. Shami, and P. Yoo, "Opportunistic spectrum access in cognitive radio networks under imperfect spectrum sensing," *Vehicular Technology, IEEE Transactions on*, vol. 63, no. 2, pp. 920–925, 2014.

[60] P. Venkatraman, B. Hamdaoui, and M. Guizani, "Opportunistic bandwidth sharing through reinforcement learning," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 6, pp. 3148–3153, 2010.

[61] N. Chakchouk and B. Hamdaoui, "Traffic and interference aware scheduling for multiradio multichannel wireless mesh networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 2, pp. 555–565, 2011.

[62] M. NoroozOliaee, B. Hamdaoui, and K. Tumer, "Achieving optimal elastic traffic rewards in dynamic multichannel access," in *High Performance Computing and Simulation (HPCS), 2011 International Conference on*, pp. 155–161, IEEE, 2011.

[63] M. NoroozOliaee and B. Hamdaoui, "Distributed resource and service management for large-scale dynamic spectrum access systems through coordinated learning," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, pp. 522–527, IEEE, 2011.

[64] O. Alsaleh, P. Venkatraman, B. Hamdaoui, and A. Fern, "Enabling opportunistic and dynamic spectrum access through learning techniques," *Wireless Communications and Mobile Computing*, vol. 11, no. 12, pp. 1497–1506, 2011.

[65] M. Ben Ghorbel, B. Hamdaoui, R. Hamdi, M. Guizani, and M. NoroozOliaee, "Distributed dynamic spectrum access with adaptive power allocation: Energy efficiency and cross-layer awareness," in *Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on*, pp. 694–699, IEEE, 2014.

[66] B. Hamdaoui, "Adaptive spectrum assessment for opportunistic access in cognitive radio networks," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 2, pp. 922–930, 2009.

[67] T. Alshammari, B. Hamdaoui, M. Guizani, and A. Rayes, "Malicious-proof and fair credit-based resource allocation techniques for dsa systems," *Wireless Communications, IEEE Transactions on*, vol. 14, no. 2, pp. 606–615, 2015.

[68] B. Hamdaoui, K. G. Shin, and M. Maiya, "Constraint design and throughput evaluation in multi-band wireless networks using multiple-input multiple-output links," *IETE Technical Review*, vol. 26, no. 2, pp. 101–107, 2009.

[69] M. NoroozOliaee, B. Hamdaoui, X. Cheng, T. Znati, and M. Guizani, "Analyzing cognitive network access efficiency under limited spectrum handoff agility," *Vehicular Technology, IEEE Transactions on*, vol. 63, no. 3, pp. 1402–1407, 2014.

[70] M. Elmachkour, A. Kobbane, E. Sabir, J. Ben-othman, *et al.*, "Data traffic-based analysis of delay and energy consumption in cognitive radio networks with and without resource reservation," *International Journal of Communication Systems*, vol. 28, no. 7, pp. 1316–1328, 2015.

[71] M. NoroozOliaee, B. Hamdaoui, T. Znati, and M. Guizani, "Forced spectrum access termination probability analysis under restricted channel handoff," in *Wireless Algorithms, Systems, and Applications*, pp. 358–365, Springer Berlin Heidelberg, 2012.

[72] M. Elmachkour, I. Daha, E. Sabir, A. Kobbane, and J. Ben-Othman, "Green opportunistic access for cognitive radio networks: A minority game approach," in *Communications (ICC), 2014 IEEE International Conference on*, pp. 5372–5377, IEEE, 2014.

[73] M. A. Taleghan and B. Hamdaoui, "Efficiency-revenue optimality tradeoffs in dynamic spectrum allocation," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pp. 1–5, IEEE, 2010.

[74] O. F. Rodriguez, S. Primak, V. Kontorovich, and A. Shami, "A game theory interpretation for multiple access in cognitive radio networks with random number of secondary users," *arXiv preprint arXiv:1305.5222*, 2013.

[75] A. Al Daoud, M. Alanyali, and D. Starobinski, "Secondary pricing of spectrum in cellular cdma networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, pp. 535–542, IEEE, 2007.

[76] Z. Fan, "Performance analysis of dynamic spectrum access networks," in *Pervasive Computing and Communications, 2008. PerCom 2008. Sixth Annual IEEE International Conference on*, pp. 336–341, IEEE, 2008.

[77] G. F. Lawler, *Introduction to stochastic processes*. CRC Press, 2006.

[78] H. Takagi, "Queueing analysis. discrete-time systems, vol. 3," 1993.

[79] Huawei, "5G: A technology vision," [Online]. Available: www.huawei.com/5gwhitepaper [Accessed: Nov. 25, 2015].

[80] A. Akki and F. Haber, "A statistical model of mobile-to-mobile land communication channel," *Vehicular Technology, IEEE Transactions on*, vol. 35, pp. 2–7, Feb 1986.

[81] A. Al Daoud, M. Alanyali, and D. Starobinski, "Secondary pricing of spectrum in cellular cdma networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, pp. 535–542, April 2007.

[82] C. Chen, M. Song, C. Xin, and J. Backens, "A game-theoretical anti-jamming scheme for cognitive radio networks," *Network, IEEE*, vol. 27, no. 3, pp. 22–27, 2013.

[83] A. Yavuz, *Lecture notes: Advanced Network Security*. Oregon State University, 2014.

[84] J.-P. Aumasson, L. Henzen, W. Meier, and R. C.-W. Phan, "Sha-3 proposal blake," *Submission to NIST*, 2008.

[85] N. Sha, "Competition, 2007-2012," [Online]. Available: http://csrc.nist.gov/groups/ST/hash/sha-3/index.html [Accessed: Jul. 10, 2016].

[86] O. Goldreich, "Texts in computational complexity: Pseudorandom generators," 2006.

[87] H. Zhang and Y. Li, "Anti-jamming property of clustered ofdm for dispersive channels," in *Military Communications Conference, 2003. MILCOM '03. 2003 IEEE*, vol. 1, pp. 336–340 Vol.1, 2003.

[88] J. Proakis and M. Salehi, *Digital Communications*. McGraw-Hill International Edition, McGraw-Hill, 2008.

[89] A. Petrolino, J. Gomes, and G. Tavares, "A mobile-to-mobile fading channel simulator based on an orthogonal expansion," in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pp. 366–370, May 2008.

[90] P. Bello and B. Nelin, "The effect of frequency selective fading on the binary error probabilities of incoherent and differentially coherent matched filter receivers," *Communications Systems, IEEE Transactions on*, vol. 11, pp. 170–186, June 1963.

[91] P. Bello, "Correction to the influence of fading spectrum on the binary error probabilities of incoherent and differentially coherent matched filter receivers," *Communications Systems, IEEE Transactions on*, vol. 11, pp. 169–169, June 1963.

[92] A. Akki, "Statistical properties of mobile-to-mobile land communication channels," *Vehicular Technology, IEEE Transactions on*, vol. 43, pp. 826–831, Nov 1994.

[93] A. Bletsas, A. Khisti, D. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *Selected Areas in Communications, IEEE Journal on*, vol. 24, pp. 659–672, March 2006.

[94] Q. Zhang and H. Lu, "A general analytical approach to multi-branch selection combining over various spatially correlated fading channels," *Communications, IEEE Transactions on*, vol. 50, pp. 1066–1073, Jul 2002.

[95] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, pp. 41–47, May 2006.

[96] H. S. Wang and N. Moayeri, "Finite-state markov channel-a useful model for radio communication channels," *Vehicular Technology, IEEE Transactions on*, vol. 44, no. 1, pp. 163–171, 1995.

[97] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile computing*, pp. 153–181, Springer, 1996.

[98] R. Bellman, "A markovian decision process," tech. rep., DTIC Document, 1957.

[99] R. A. Howard, "Dynamic programming and markov processes..," 1960.

[100] C. J. Watkins and P. Dayan, "Q-learning," *Machine learning*, vol. 8, no. 3-4, pp. 279–292, 1992.