STUDY OF BYZANTINE ATTACKS AND COUNTERMEASURES IN SPECTRUM SENSING

By

MANOJ KUMAR VEGI

Bachelor of Engineering in Electronics and
Communications Engineering
GITAM University
Visakhapatnam, Andhra Pradesh, INDIA
2012

Submitted to the Faculty of the
Graduate College of
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
July, 2014

STUDY OF BYZANTINE ATTACKS AND COUNTERMEASURES IN SPECTRUM SENSING

Thesis Approved:

Dr. Qi Cheng

Thesis Advisor

Dr. Louis Johnson

Dr. Ramakumar

Name: Manoj Kumar Vegi

Date of Degree: July, 2014

Title of Study: STUDY OF BYZANTINE ATTACKS AND COUNTERMEASURES IN SPECTRUM SENSING

Major Field: Electrical Engineering

Abstract: Cognitive radio is viewed as a novel approach for improving the utilization of the spectrum as it utilizes the under-utilized spectrum bands of the primary users. Cognitive radio is aware of its environment and can modify its transmission configuration accordingly. Spectrum sensing is the most important component of a cognitive radio network. Various types of security threats like incumbent emulation attacks and Byzantine attacks are present in the cognitive radio environment. In this thesis, we mainly concentrate on Byzantine attacks. We consider an energy detection scheme which is used to detect primary users, and the decision fusion rule to obtain a decision regarding the primary user at the fusion center. Byzantine attacker strategies and reputation based schemes to counter the attackers have been proposed. Analysis of the model is performed to assess the game between attackers and the fusion center with the help of simulations.

Byzantine attackers and the fusion center are aware of strategies of each other. The aim of the attackers is to cause maximum damage to the system and the aim of the fusion center is to eliminate the attackers from the system and improve the system performance. Based on the performance metrics chosen, when attackers are being eliminated from the system, they tend to decrease the rate of isolation by attacking with lower probabilities such that they cannot be identified and can cause more damage to the system. At the same time, the fusion center wants to eliminate more attackers, so it tries to change the reputation threshold and time windows accordingly. The proposed algorithm is verified by conducting experiments with the help of simulations in Matlab.

TABLE OF CONTENTS

Chapter Page

LIST OF FIGURES

Figure Page

CHAPTER 1

INTRODUCTION

The demand for radio spectrum (which is a limited resource), is an emerging problem because of enormous increase in the field of wireless devices and applications. Earlier, the usage of the spectrum is given to the licensed users. However, recent studies show that the fixed spectrum assignment policy enforced today results in poor spectrum utilization, as great portion of licensed spectrum is not effectively utilized.

1.1 Dynamic Spectrum Access

The Federal Communications Commission(FCC) [1] in order to counter this spectrum requirement problem, opted for efficient use and better utilization of the spectrum by opening up the licensed bands to unlicensed operations. When the spectrum is not occupied by the licensed users, the unlicensed operations can be done in the available spectrum on a non interference basis. Under this scheme two types of users exist. They are Primary users(PU) and Secondary users(SU) [2]. Incumbent users who have a license to transmit are known as the primary users and those who use the spectrum for unlicensed operations are known as the secondary users.

The spectrum consists of dormant bands or gaps which are known as white spaces or spectrum holes. As defined in [3], *Spectrum hole, is a band of frequencies assigned to a particular user, but, at a particular time and geographic location, the band is not being utilized by the user.* These spectrum holes can be used by the unlicensed users on an opportunistic basis without interfering the licensed users. This method of

sharing is often called Dynamic Spectrum Access (DSA) [4]. However, during DSA, the FCC prescribes that *no modification should be done to the primary network to accommodate the opportunistic use of spectrum by the secondary users* [5]. If the incumbent users require the channel, then the secondary users must immediately vacate to another channel without causing any interference. In order to combat this salient necessity, Cognitive radio technology [6] has been proposed as the means to promote the efficient use of the spectrum by exploiting the spectrum holes.

1.2 Cognitive Radio

As defined in [3], *Cognitive radio(CR) is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit-power, carrier frequency, and modulation strategy) in real-time.*

Unlike conventional radio technology that operates in fixed channels, cognitive radio networks have the capability to sense and understand its environment and change its mode of operation based on the requirement. The primary objectives of CR include:

1. highly reliable communications whenever and wherever needed;
2. efficient utilization of the radio spectrum.

One of the key functions of the CRs is spectrum sensing [7]. In CR, identification of the available spectrum and prevention of interference between secondary users with primary users are achieved through spectrum sensing. So, cognitive radio networks should target on these idle bands to check the availability of the spectrum. Cognitive

radios need to carry on spectrum sensing and its management in the wireless environment without interfering the licensed users. Cognitive radio networks incorporate mechanisms like cooperative spectrum sensing and self coexistence, to sense the current band and utilize the spectrum efficiently.

In spatially distributed CRs, they generally experience the problem of fading and receiver uncertainty. This problem can be overcome by cooperating during detection. Cooperative spectrum sensing can significantly improve the spectrum sensing accuracy than the individual spectrum sensing [8]. The main idea of cooperative sensing is to enhance the sensing performance and detection reliability by exploiting the spatial diversity in the observations of spatially located CR users. By cooperation, CR users can share their sensing information for making a combined decision more accurately than the individual decisions. Cognitive radios compete to use the underutilized spectrum and carry on data transmissions in the available bands. As mentioned in [9], this competition for spectrum results in misuse of the spectrum, as they experience contention in attempt to use the available bands. This can be minimized by incorporating self coexistence mechanism in CRs. In areas with significantly more licensed users, open channels will be a commodity of demand. Therefore, it is important that interference between CRs is avoided. Self coexistence mechanism is needed in overlapping coverage areas of CR networks. So that, CRs can significantly foster better spectrum utilization without any interference.

In this thesis, we consider a centralized cooperative spectrum sensing method as shown in Fig1.1 [8]. It consists of a fusion center (FC) which is the central identity in the network. First, FC selects a band of interest where it instructs all the CRs in the network to perform individual sensing. Second, all the CRs report their sensing decisions via a dedicated communication channel. Based on the local decisions from

all the CRs, a final global decision is taken at FC regarding the presence of the primary user and this decision is sent back to the CRs for the spectrum utilization if available.

Figure 1.1: Centralized cooperative sensing

Primary user detection is the major part in DSA. There are many techniques that can be used for PU detection like energy detection, matched filter and Cyclostationary feature detections [15]. The most common technique that is employed in many cooperative sensing techniques is energy detection due to its simplicity and no requirement of prior knowledge of primary user signal. Energy detection is a non-coherent detection method that detects the PU signal based on the sensed energy. Matched filter is a linear filter designed to maximize the output signal to noise ratio for a given input signal. This technique requires the prior knowledge of primary users. If this information is not accurate, it delivers a poor performance. Cyclostationary feature detection exploits periodicity in the received primary signal to identify the primary users and also requires the prior knowledge of primary users. In this thesis, we adopt the energy detection technique. CRs are equipped with energy detectors to obtain a

decision about the presence of primary user. These decisions are then forwarded to FC. Various decision making techniques can be employed at FC to obtain a global decision about PU in the frequency band.

After PU detection at the CRs, we need to obtain a global decision at FC. Techniques like decision fusion, Neyman-Pearson test, Bayesian detection, SPRT (Sequential Probability Ratio Test) can be used to obtain the global decision at FC. In this thesis, we consider decision fusion rule which is the most simple and common technique. Decision fusion is a process of fusing all the local decisions together for hypothesis testing. There are different methods of decision fusion methods like soft fusion, hard fusion and quantized soft combining.

(i) Soft Combining [16]: CR users can transmit the entire local sensing samples or the complete local test statistics for soft decision fusion.

(ii) Quantized Soft Combining [17]: CR users can quantize the local sensing results and send only the quantized data for soft combining to alleviate control channel communication overhead.

(iii) Hard Combining [18]: CR users make local decisions and transmit the one-bit decisions for hard combining.

In this thesis, we use the one bit hard decision fusion method which requires less communication overhead and bandwidth requirement. These decisions are fused at FC to obtain a global decision. Many techniques were proposed for the global decision making. In this thesis, we consider the k-out-of-N rule. OR and AND rule are easy and simple logics to implement which are mainly considered as special cases that are derived from the k-out-of-N rule [18] where $k = 1$, N respectively.

1.3 Security in Spectrum Sensing

CRs are highly reconfigurable due to their software based air interface. So there are many security issues and different kinds of attacks on these CRs. If a few CRs in the network send unreliable data or falsified sensing information, then they can easily influence the decision at the FC. These malfunctioning users or malicious users may intentionally send false information in order to use the limited spectrum band or cause some interference to the incumbent users. These types of attacks are specified in [11], [4] which are known as the Primary User Emulation (PUE) attacks and the Spectrum Sensing Data Falsification (SSDF) attacks. It is challenging for the fusion center to validate the integrity of the sensing reports mainly because of two reasons [10]:

1. lack of coordination between PUs and SUs;
2. unpredictability in wireless channel signal propagation.

So, more efficient and robust techniques are to be employed at FC.

In this thesis, we mainly concentrate on SSDF attacks where the attackers try to induce false sensing information into the process leading to the disruption of the entire network and low network efficiency. These data falsification attackers are generally referred as Byzantines attacker [12]-[14]. CRs (both honest and Byzantine) forward their decisions to FC, to obtain a decision about PU as shown in Fig 1.2 [5]. To address the data falsification problem, existing cooperative sensing schemes aim to detect the anomaly in the reported sensing data and establish a mechanism to distinguish the malicious users from the authentic ones such that malicious users can be excluded from the cooperation to ensure the integrity of the sensing decisions and secure the operations in the system.

In SSDF attacks, the compromised CRs may attack individually or collaborate among

Figure 1.2: Cognitive model showing PU transmission and CRs (both honest and Byzantine) sending their decisions to FC

themselves to degrade the overall performance or reduce spectrum utilization. So to overcome these attacks, additional mechanisms are to be employed at the FC to obtain reliable data.

Assumptions in this thesis are that FC is not compromised and will receive the decisions from all the CRs through dedicated communication channels. We also assume that FC does not know which node is Byzantine but it knows the percentage of attackers in the network. The main aim of the FC is to decrease the probability of error in sensing by eliminating the Byzantine attackers and improve the system performance. At the same time, the Byzantine attackers try to undermine the network capability, i.e., the fusion center's ability of detecting a primary signal.

Byzantine attackers can make the fusion center incapable of making a decision by completely blinding the system. In this case, the fusion center will be unable to decide on a particular decision and the performance at the fusion center can be no better than just a random guess of the state of channel. A critical value of 50% of Byzantine attackers can completely blind the FC [5].

In order to further counter these Byzantine attacks, we propose a reputation metric based detection scheme at the FC, by counting the number of mismatches between the global and local decisions over few sensing periods. Based on the reputation factor we obtain the probability with which Byzantine attackers can be isolated from the decision process and eliminated from the system. Byzantine attackers will change their probability of attack, so that, they can still exist in the system without being eliminated while FC tries to increase the elimination of Byzantine attackers. This results in a game between Byzantine attackers and FC.

1.4 Thesis Outline

The thesis is organized as follows:

Chapter 1: Introduction discusses briefly about the necessity for cognitive radio networks and spectrum sensing. It also includes various types of security threats on cognitive radio networks and decision fusion rules at FC.

Chapter 2: Literature Review: This chapter gives a synopsis of existing techniques to detect the primary user transmission. It covers various cooperative sensing techniques and methods to counter the attackers. It also surveys various defense mechanisms that have been proposed in literature.

Chapter 3: System Model and Problem Formulation: This chapter explains about the type of system, attacks and methods to counter the attackers.

Chapter 4: Analysis: This chapter discusses on the optimal strategies with which the Byzantine attackers and Fusion center make up a game between them.

Chapter 5: Simulation and Results: This chapter consists of few experiments based on simulated data to validate our strategies proposed in literature.

Chapter 6: Conclusions and Future work: This chapter summarizes the results achieved and scope for future work.

CHAPTER 2

LITERATURE REVIEW

2.1 Spectrum Sensing Techniques

Spectrum Sensing is the key function in DSA. Many mechanisms have been proposed for sensing primary users by cognitive radio networks. These techniques can be classified into Matched Filter, Energy Detection and Cyclostationary Feature Detection [15].

2.1.1 Matched Filter

Matched filter is a linear filter designed to maximize the output signal to noise ratio for a given input signal [19]. Block diagram of matched filter is shown in Fig 2.1 [21]. This technique is applied when secondary users has a prior information about the primary user signal, e.g., the packet length, the modulation type, pulse shaping. Matched filter detection requires less detection time. When prior information about primary signal is known, then matched filter detection is the optimal detection. However, the drawback is that cognitive radio will be required to store a lot of information about primary users and also cognitive radio would need a dedicated receiver for every primary user [20].

Figure 2.1: Block diagram of matched filter

2.1.2 Energy Detector

It is a non-coherent detection method that detects the primary signal based on the sensed energy. It is the most popular sensing technique, due to its simplicity and non requirement of prior knowledge of primary signal. Block diagram of energy detector is shown in Fig 2.2 [22]. The working of an energy detector is similar to that of a spectrum analyzer where the received signal is first sampled, then converted to the frequency domain by taking the fast Fourier transform (FFT) followed by squaring the coefficients and then taking the average. This value is then compared to a pre-determined threshold to check for the presence of a PU [23]. The whole process is outlined in Fig 2.2.

Energy detector is a blind signal detector as it ignores the structure of a signal. Presence or absence of a signal is estimated by comparing the energy received with a known threshold. The threshold value can be fixed or variable based on the channel conditions.

Figure 2.2: Block diagram of energy detector

2.1.3 Cyclostationary Feature Detection

Cyclostationary feature detection exploits the periodicity in the received primary signal to identify the presence of primary users. The periodicity is commonly embedded in sine waves, cyclic codes, pilot signals and/or hopping sequences of primary signals. This property can be used for signal detection of a particular type in the presence of random noise and other signals. Block diagram of cyclostationary feature detection is shown in Fig 2.3 [27]. It require the prior knowledge of primary signals and is able to distinguish between CR transmissions from various types of PU signals. Thus cyclostationary feature detection is robust to noise uncertainties and performs better than energy detections in low SNR regions [25].

Implementation of cyclostationary feature detection is as shown in Fig. 2.3. From the figure we can see that the cyclostationary feature detection is similar to the energy detector except that it has an added block which does the correlation. This method requires long sensing time and high computational complexity. So, this detection technique is less commonly used than energy detection [27].

Figure 2.3: Block diagram of cyclostationary feature detector

2.2 Types of Cooperative Sensing

In cognitive radio networks, the high sensitivity requirements can be reduced if multiple cognitive radios participate in spectrum sensing cooperating each other. This cooperative spectrum sensing is classified into three types, centralized[28]-[29],

distributed[30] and relay assisted [31]-[32] as shon in Fig 2.4 [8]

Figure 2.4: Classification of cooperative sensing: (a) centralized, (b) distributed, and (c) relay-assisted

2.2.1 Centralized Cooperative Sensing

In such networks, CR detects the presence or absence of a primary user and then informs to a the fusion center which controls the cooperative sensing. FC notifies all the CRs to sense the frequency band of interest. CRs sense and send their decisions to the FC via a control channel, where it combines the decisions and take the final decision about PU.

2.2.2 Distributed Cooperative Sensing

In such networks, CRs build up a network without FC. They communicate among themselves and obtain a unified decision about the presence or absence of PU. Various algorithms have been proposed for decentralized techniques where CRs form into clusters, auto coordinating themselves.

2.2.3 Relay-assisted Cooperative Sensing

In such networks, each user independently senses the network. As the reporting channels and sensing channels are not perfect, a CR observing weak sensing channel and strong report channel and a CR with strong sensing channel and weak report channel can cooperate with each other to improve the performance. The results are forwarded to the intended CR or FC by multiple hops, where all the intermediate hops are relays.

2.3 Security Issues

Security is an important issue as potential malicious users attempt to disrupt the network and diminish its capability. Data falsification attacks are those attacks which send false information to the FC to disrupt the global inference process [33]. Until recently, security issues in cognitive radio network have not been fully addressed. Existing solutions to combat against the SSDF attacks are specified in the following papers where different techniques have been employed.

The onion peeling approach [34] has been proposed based on Bayesian statistics. All the nodes were assigned suspicion levels. If this suspicion level exceeds certain threshold, it is considered as a malicious user and immediately removed from decision making process. However, they also assume that the fusion center has prior knowledge about the activities of the attackers and if thresholds are approximated without such information, it will result in false detections of attackers.

Another method is proposed by Chen *et al.* [11] which combines weight and the sequential probability radio test to identify the malicious users known as weighted sequential probability radio test (WSPRT). However, this mechanism assigns weights based on the threshold parameters. If honest CRs sense false information, they also

can be eliminated from the system which results in much havoc. Apart from these weight based methods, Chen *et al.* also proposed a new technique to identify the Byzantine attackers. The Outlier factor has been proposed to identify the attackers in the network.

In [35], pre-filtering of the sensing data is done for removing the malicious users where upper and lower bounds are calculated to identify the extreme outliers and eliminate them. The chance of eliminating honest CRs is also present. After that, trust factors are assigned to the remaining CRs through which the decision about PU is considered. This mechanism works on 'always yes' or 'always no' scenarios. This sort of mechanism cannot counter intelligent Byzantine attackers as they cannot be identified when they attack with arbitrary probability.

Praveen *et al.* [36] have established a robust fusion center decision algorithm to overcome the elimination of honest CRs. The compiled set of reports from the secondary users are analyzed using bi-weight location estimate and bi-weight scale estimate instead of mean and standard deviation, as they are not robust and can be easily manipulated by the malicious users. Bi-weight estimate calculates a weighted mean with lower weightage being given to the observations away from the estimate and Bi-weight scale is sensitive to the data points that are at a moderate distance and ignores data from extreme data points. These parameters have the magnitudes that are compared to the thresholds given by the system. However, this method may result in failure to detect the primary signal, increases the misdetection when using incorrect thresholds and inaccuracy of the secondary user elimination.

The K-neighborhood distance algorithm is another approach presented to detect the malicious users [37]. This approach does not need any prior knowledge of the

attacker distribution. This mechanism exposes the attackers in multiple sensing periods. However, the system can be easily evaded when attackers have the knowledge about secondary user's data and collaborate with each other.

In summary, many methods have been proposed on eliminating the attackers from the network by assigning few parameters like suspicion levels, weights to the local decisions of the CRs. These proposed methods may not be robust or reliable.

2.4 Objective of the study

In this work, our main objective is to observe the game between the fusion center and Byzantine attackers. We propose a parallel fusion network to obtain a decision about the presence or absence of primary user. Byzantine attackers and the fusion center in the network are aware of each other and their strategies. So, when decisions about the PU are considered at FC, attackers try to disrupt the system by sending false information. As the attackers want to degrade the network, they do not want to get eliminated easily. So they attack with different probabilities. Fusion center aware of the attackers strategy tries to induce a reputation based algorithm in the network to eliminate the Byzantine attackers. Byzantine attackers in order to exist in the system try to attack with optimal probabilities. When the threshold at the FC is varied, this optimal attacking strategies can also be countered.

CHAPTER 3

SYSTEM MODEL

The entire system is modeled into a parallel network. The distributed network consists of N CRs and a fusion center trying to detect the primary user. The CRs sense the available spectrum in periodic slots and forward the results to the FC. Each secondary user uses an energy detection scheme for making its decision because of its computational and implementation simplicity.

In essence, this primary user detection process is a hypotheses testing problem and all the detections by the CRs are assumed conditionally independent of each other. Consider a binary hypotheses testing problem with two hypotheses H_0 and H_1. Prior probabilities of the two hypotheses are given by P_0 and P_1, $P_0 + P_1 = 1$.
H_0: Represents the absence of primary user
H_1: Represents the presence of primary user

Let $Y[n]$ denote the n^{th} received sample at each CR, $W[n]$ be the noise, $X[n]$ be the primary user signal and assumed to be an independent and identically distributed random process of zero mean and variance of σ_s^2. The hypothesis testing for the network is given by:

$$H_0 : Y[n] = W[n], n = 1, 2, 3.....M; \tag{3.1}$$

$$H_1 : Y[n] = X[n] + W[n], n = 1, 2, 3.....M; \tag{3.2}$$

Noise corrupts the signal strength measurements of a secondary user, where the noise is assumed to be additive white Gaussian(AWGN) with zero mean and variance σ_w^2. The energy detector at the CR calculates the energy of the M accumulated samples by $Z = \sum_{n=1}^{M} \mid Y[n] \mid^2$. Consider the i^{th} CR. CR_i compares the statistic Z_i with local decision threshold δ_i to make a binary local decision about the PU and transmit the decision to the FC.

$$U_i = 1,\ if\ Z_i \geq \delta_i, \tag{3.3}$$

$$U_i = 0,\ otherwise. \tag{3.4}$$

The fusion center then compares the system threshold with the sum of received decisions and makes a final decision whether the primary user is present or absent.

Figure 3.1: Parallel topology with a fusion center

Since CR_i denotes the i^{th} CR under consideration in the network, u_i represents the channel usage information observed (decision of the CR about the primary user based on the energy detection) and this is sent through the control channel which is assumed to be perfect. v_i is the information received at the fusion center. If the node is hon-

est, then it forwards a decision correctly, i.e., $u_i = v_i$. If it is a Byzantine attacker, in order to degrade the performance of the system, it may alter its decisions. So u_i may not be the same as v_i.

We define the following probabilities for honest and Byzantine CRs.
Honest CRs:

$$P_{1,1}^{H} = 1 - P_{0,1}^{H} = P^{H}(v_i = 1|u_i = 1) = 1 \tag{3.5}$$

$$P_{1,0}^{H} = 1 - P_{0,0}^{H} = P^{H}(v_i = 1|u_i = 0) = 0 \tag{3.6}$$

Byzantine CRs:

$$P_{1,1}^{B} = 1 - P_{0,1}^{B} = P^{B}(v_i = 1|u_i = 1) = 1 - P \tag{3.7}$$

$$P_{1,0}^{B} = 1 - P_{0,0}^{H} = P^{B}(v_i = 1|u_i = 0) = P \tag{3.8}$$

Typically Byzantine attackers attack with these probabilities when they are unaware of the fusion center strategies. When attackers have a knowledge of the FC strategies, they vary their probability of attacking based on their requirement.

In spectrum sensing, hypotheses testing is typically performed to obtain a decision about the presence of PU. Several decision fusion techniques can be incorporated in the system which consists of different strategies such as
Bayesian detection : This strategy requires the knowledge of prior probabilities of H_i's when H_i is zero or one. Each decision situation will be associated with a cost, i.e., any of the situations when u_i is decided as 1/0 while H_i is actually 1/0. The total cost can be minimized using Bayesian detection.
Neyman-Pearson test : This strategy does not rely on the knowledge of any cost associated with each decision situation. It requires that the maximum acceptable probability of false alarm (i.e., u_i is decided as one when H_i is actually zero) be defined. The Neyman-Pearson test guarantees that the probability of miss detection

(i.e., u_i is decided as zero when H_i is actually one) is minimized while the false alarm probability remains acceptable.

Sequential test : Sequential Test, or Sequential Probability Ratio Test (SPRT), takes a variable number of observation samples as inputs based on need. Given the knowledge of a *priori* probabilities of H_i's when H_i is zero or one and given the maximum acceptable false alarm probability and miss detection probability, SPRT minimizes the number of observations.

In this thesis, due to its frequent utilization and implementation simplicity, we focus on the k-out-of-N fusion rule where FC decides that the primary user is present when k or more received local decisions are in support of the presence of the primary user, else the FC announces that the primary user is absent and cognitive users can use the relevant band. If $k = 1$, the fusion rule becomes the OR-fusion rule and if $k = N$ it becomes the AND-fusion rule. Local binary sensing decision of the i^{th} cognitive radio is given by, $u_i = 0$ for absence of primary user and $u_i = 1$ for presence. Thus the resulting k-out-of-N hypothesis testing at the fusion center is given by $I = \sum_{i=1}^{N} v_i < k$ for deciding H_0 and $I = \sum_{i=1}^{N} v_i \geq k$ for deciding H_1.

Figure 3.2: Spectrum sensing using the k-out-of-N rule.

Let P be the probability that a byzantine attacker sends false information and α be the percentage of attackers present in the network. Let P_f and P_d denote the probabilities of false alarm and detection respectively of local spectrum sensing, where P_f represents the probability that PU is actually absent when a CR declaring that PU is present and P_d represents that CR declares that PU is present when indeed the spectrum is actually occupied by PU. Another important probability parameter is called missed-detection probability P_m when the energy detector indicates the primary user is absent while actually is present, and P_m = 1 - P_d.

The overall probabilities of the secondary users at the i^{th} cognitive radio and fusion center are given as follows:
Probability of Byzantine attackers is given by:

$$P(v_i = 1|H_1) = P_d^B = P(1 - P_d) + (1 - P)P_d \tag{3.9}$$

$$P(v_i = 1|H_0) = P_f^B = P(1 - P_f) + (1 - P)P_f \tag{3.10}$$

Probability of honest users is given by:

$$P(v_i = 1|H_1) = P_d^H = P_d \tag{3.11}$$

$$P(v_i = 1|H_0) = P_f^H = P_f \tag{3.12}$$

where P_d^H and P_f^H are the probabilities of detection and false alarm if the i^{th} CR is honest.

Based on the decision fusion model discussed above, global decisions are made by comparing the summation of all local decisions sent by the fusion members in the network with threshold k at the FC, the false alarm rate is given in eq(3.14).
Probabilities at the fusion center without considering the attackers are given by:

$$Q_d = \sum_{i=k}^{N} \binom{N}{i} {P_d}^i (1 - P_d)^{N-i} \tag{3.13}$$

$$Q_f = \sum_{i=k}^{N} \binom{N}{i} {P_f}^i (1 - P_f)^{N-i} \tag{3.14}$$

where k represents the threshold.

According to the De Moivre-Laplace theorem, when N is large enough, Q_f can be calculated approximately as[38]

$$Q_f \simeq Q\left(\frac{k - \sum_{i=1}^{N} P_f}{\sqrt{\sum_{i=1}^{N} P_f(1 - P_f)}}\right) \tag{3.15}$$

where $Q(.)$ is the complementary cumulative distributed function(CCDF) of a standard normal distribution; that is,

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_{\delta}^{\infty} \mathrm{e}^{-} t^2/2 \, \mathrm{dt} \tag{3.16}$$

Similarly, Q_d can also be calculated as

$$Q_d \simeq Q\left(\frac{k - \sum_{i=1}^{N} P_d}{\sqrt{\sum_{i=1}^{N} P_d(1 - P_d)}}\right) \tag{3.17}$$

Q_m is calculated by $Q_m = 1$ - Q_d as follows,

$$Q_m \simeq \Phi\left(\frac{k - \sum_{i=1}^{N} P_d}{\sqrt{\sum_{i=1}^{N} P_d(1 - P_d)}}\right) \tag{3.18}$$

where $\Phi(x)$ is the cumulative distribution function (CDF) of a standard normal distribution.

According to the Bayesian detection condition of minimum system detection cost as given in [39], we have the costs for deciding on H_i, when H_j is true as $M_{ij}|i, j \in \{0, 1\}$.

By considering $P_0 = P_1 = 0.5$, $M_{00} = M_{11} = 0$ and $M_{01} = M_{10} = 1$, we can get the condition of minimum system detection cost as: $Q_f = Q_m$

$$Q\left(\frac{k - \sum_{i=1}^{N} P_f}{\sqrt{\sum_{i=1}^{N} P_f(1 - P_f)}}\right) = \Phi\left(\frac{k - \sum_{i=1}^{N} P_d}{\sqrt{\sum_{i=1}^{N} P_d(1 - P_d)}}\right) \tag{3.19}$$

Since $Q(.)$ is the complementary cumulative distributed function of standard normal distribution, we have $Q(-x) = 1 - Q(x)$ and $Q(x) = 1 - \Phi(x)$. By integrating the above equations we can find threshold k^*

$$k^* = \frac{Np_0 . \sqrt{p_1(1 - p_1)} + Np_1 . \sqrt{p_0(1 - p_0)}}{\sqrt{p_0(1 - p_0)} + \sqrt{p_1(1 - p_1)}} \tag{3.20}$$

where p_1 and p_0 is average of detection and false alarm probabilities respectively of all fusion members. Here, $p_1 = P_d$ and $p_0 = P_f$ since all CRs have the same local probabilities.

From the entire set of decisions that are observed at the fusion center, i.e.,
$u_i, i \in [1, 2, 3, ...N]$

$$V_0 = \sum_{i=1}^{N} v_i \geqslant k^*, \ \textit{decide on } H_1 \tag{3.21}$$

$$V_0 = \sum_{i=1}^{N} v_i < k^*, \ \textit{decide on } H_0 \tag{3.22}$$

CHAPTER 4

ANALYSIS

Optimal Byzantine and fusion center strategies: Game between attackers and fusion center

Byzantine attackers try to degrade the network in such a way that it results in maximum damage of the entire system by making the fusion center blind. At the same time, the fusion center tries to defend its network by minimizing the damage caused by the Byzantine attackers by introducing defense mechanism and eliminating the Byzantine attackers from the system. So, this leads to a game between the attackers and the fusion center in the network. Consider Byzantine attackers and FC aware of each other strategies.

Byzantine attackers try to send the false decisions to the FC by flipping their decisions and interrupting the efficient utilization of the spectrum. In the extreme attack, Byzantines try to flip their decisions with $P = 1$, i.e., $v_i = 0$ when $u_i = 1$ and $v_i = 1$ when $u_i = 0$. If Byzantines continuously send false information with a probability $P = 1$, then FC can eliminate these attackers with simple performance metrics by counting number of mismatches between the local and global decision.

Byzantines implement few strategies in attacking so that they are not eliminated easily and continue disrupting the system.

4.1 Possible Attack Strategies of Byzantines

Malicious users that are present in the network try to degrade the system by modifying their decisions about the primary user and sending false information. This can be done in three different strategies:

Case1: In this strategy, the Byzantine attackers continuously report false information i.e., with probability $P = 1$. Continuously attacking with this probability leads to exposure and attackers can be identified easily after a few sensing periods using different detection schemes.

Case2: In this strategy, the Byzantine attackers report false data with an arbitrary probability $P \in (0, 1)$ which represents that they are not continuously sending false data. Here the attackers may not be identified easily.

Case3: In this strategy, the Byzantine attackers introduce attack with a probability that changes after each sensing period based on the previous probability of attacking information.

$$P_n = P_{n-1} + \triangle_1 y - \triangle_2 (1 - y) \tag{4.1}$$

where P_n represents the attacking probability in the n^{th} sensing periods and P_{n-1} represents the probability in the $(n-1)^{th}$ sensing period. y is a Bernoulli random variable that is equal to '1' with probability P_x, and $\triangle_1$ and $\triangle_2$ are increment and decrement steps respectively, where $\triangle_1, \triangle_2 \in [0, 1]$.

4.2 Fusion Center Strategies

FC is aware of Byzantine attackers in the network and their attempt to send false information. We propose a strategy that can be employed at the fusion center to counter the Byzantine attackers from the decision fusion process. We divide the SS process into T sensing periods. Over T sensing windows, the local decisions forwarded

by the i^{th} CR can be represented by $v_i = [v_i[1], v_i[2], ..., v_i[T]]$. For the same time windows, the final decisions of FC are $V_0 = [V_0[1], V_0[2], ..., V_0[T]]$. So, the fusion center allocates a reputation measure n_i to each CR representing how many times its final decision is different from the local decision during T time windows. So, larger the value of n_i, the less reliable is the CR.

Inconsistency of an observation received from a CR with final decisions can be expressed as $h_{i[t]} = I(v_i[t] \neq V_0[t])$, where I is the indicator function representing $(v_i[t] \neq V_0[t])$.
Now $P(h_{i[t]}) = P(I(v_i[t] \neq V_0[t]))$ is given by

$$P(h_{i[t]} = 1|H_j) = P(v_i[t] = 0|H_j)P(V_0[t] = 1|v_i[t] = 0, H_j) + P(v_i[t] = 1|H_j)P(V_0[t] = 0|v_i[t] = 1, H_j) \quad (4.2)$$

where $j \in \{0, 1\}$.

The reputation of the i^{th} CR is given by

$$n_i = \sum_{t=1}^{T} I(v_i[t] \neq V_0[t]) \quad (4.3)$$

Generally, if a random variable O follows the binomial distribution with parameters λ and p (i.e., $O \sim$ B(λ,p)), the probability of getting exactly o success in λ trails is given by

$$P(O = o) = f(o; \lambda, p) = \binom{\lambda}{o} p^o (1 - p)^{\lambda - o} \quad (4.4)$$

The total number of CRs in our system is N, where we consider L honest CRs and M Byzantine attackers in them, i.e., $N = L + M$. By using the k-out-of-N rule at the FC in a given time window, the relevant probabilities for honest and Byzantine CRs are given as follows.

For honest CRs

$$P(V_0[t]=0|v_i[t]=1,H_1)=1-\sum_{l=k-1}^{N-1}\sum_{j=a}^{b}f(j;M,P_d^B)f(l-j;L-1,P_d^H) \tag{4.5}$$

where $a=\max(0,k-L+1)$ and $b=\min(k,M)$

$$P(V_0[t]=1|v_i[t]=0,H_1)=\sum_{l=k}^{N-1}\sum_{j=a}^{b}f(j;M,P_d^B)f(l-j;L-1,P_d^H) \tag{4.6}$$

$$P(V_0[t]=0|v_i[t]=1,H_0)=1-\sum_{l=k-1}^{N-1}\sum_{j=a}^{b}f(j;M,P_f^B)f(l-j;L-1,P_f^H) \tag{4.7}$$

$$P(V_0[t]=1|v_i[t]=0,H_0)=\sum_{l=k}^{N-1}\sum_{j=a}^{b}f(j;M,P_f^B)f(l-j;L-1,P_f^H) \tag{4.8}$$

For Byzantine CRs

$$P(V_0[t]=0|v_i[t]=1,H_1)=1-\sum_{l=k-1}^{N-1}\sum_{j=a}^{b}f(j;M-1,P_d^B)f(l-j;L,P_d^H) \tag{4.9}$$

where $a=\max(0,l-L)$ and $b=\min(k,M$ -1)

$$P(V_0[t]=1|v_i[t]=0,H_1)=\sum_{l=k}^{N-1}\sum_{j=a}^{b}f(j;M-1,P_d^B)f(l-j;L,P_d^H) \tag{4.10}$$

$$P(V_0[t]=0|v_i[t]=1,H_0)=1-\sum_{l=k-1}^{N-1}\sum_{j=a}^{b}f(j;M-1,P_f^B)f(l-j;L,P_f^H) \tag{4.11}$$

$$P(V_0[t]=1|v_i[t]=0,H_0)=\sum_{l=k}^{N-1}\sum_{j=a}^{b}f(j;M-1,P_f^B)f(l-j;L,P_f^H) \tag{4.12}$$

Let P_B and P_H be the $P(I(v_i[t]\neq V_0[t]))$ for Byzantine and honest CRs respectively. P_B and P_H can be calculated using the above equations (4.2), (4.5)-(4.12).

For $P(h_{i[t]}=1|H_1)$

$$P_B^1=P_f^B\cdot(\sum_{l=k-1}^{N-1}\sum_{j=a}^{b}f(j;M-1,P_f^B)f(l-j;L,P_f^H)) + P_d^B\cdot(1-\sum_{l=k}^{N-1}\sum_{j=a}^{b}f(j;M-1,P_f^B)f(l-j;L,P_f^H)) \tag{4.13}$$

$$P_H^1 = P_f^H \cdot (\sum_{l=k}^{N-1} \sum_{j=a}^{b} f(j; M, P_d^B) f(l-j; L-1, P_d^H)) + P_d^H \cdot (1 - \sum_{l=k-1}^{N-1} \sum_{j=a}^{b} f(j; M, P_d^B) f(l-j; L-1, P_d^H)) \quad (4.14)$$

For $P(h_{i[t]} = 1|H_0)$

$$P_B^0 = P_d^B \cdot (\sum_{l=k-1}^{N-1} \sum_{j=a}^{b} f(j; M-1, P_f^B) f(l-j; L, P_f^H)) + P_f^B \cdot (1 - \sum_{l=k}^{N-1} \sum_{j=a}^{b} f(j; M-1, P_f^B) f(l-j; L, P_f^H)) \quad (4.15)$$

$$P_H^0 = P_d^H \cdot (\sum_{l=k}^{N-1} \sum_{j=a}^{b} f(j; M, P_d^B) f(l-j; L-1, P_d^H)) + P_f^H \cdot (1 - \sum_{l=k-1}^{N-1} \sum_{j=a}^{b} f(j; M, P_d^B) f(l-j; L-1, P_d^H)) \quad (4.16)$$

$$P_B = P_0 P_B^0 + P_1 P_B^1 \quad (4.17)$$

$$P_H = P_0 P_H^0 + P_1 P_H^1 \quad (4.18)$$

In this thesis, this reputation metric is used to counter the Byzantine attackers by isolating them from the network when its reputation metric η_i exceeds a particular threshold η where $\eta < T$. For further analysis of P_{iso}^B and P_{iso}^H, the Gaussian approximation is employed on the Binomial distribution. The reputation metric for both Byzantine and honest CRs are distributed as:

$$P_{iso}^B = P(n_i > \eta) = Q\left(\frac{\eta - T \cdot P_B}{\sqrt{T \cdot P_B(1-P_B)}}\right) \quad (4.19)$$

$$P_{iso}^H = P(n_i > \eta) = Q\left(\frac{\eta - T \cdot P_H}{\sqrt{T \cdot P_H(1-P_H)}}\right) \quad (4.20)$$

where $Q(.)$ is the complementary cumulative distribution function of standard Gaussian random variable. The cutoff probability of honest CRs and Byzantine attackers

can be constrained by selecting the threshold η with targeted false alarm constraint w.

$$\eta = (\sqrt{T \cdot P_H(1 - P_H)})Q^{-1}(w) + T \cdot P_H \tag{4.21}$$

The Byzantines detection performance can be influenced by w and T, where w is a constant ranging between $[0, 1]$. For small value of w, the probability of honest CRs being cut off from the system will be very low. But, decreasing w will result in increase of η which results in decreased value of P_{iso}^B. So, there is a trade off while selecting w. Also a larger sensing period T with a suitable w can provide a better detection performance. However, larger T leads to delay resulting in more damage to the network. If the Byzantine attackers are aware of these strategies at the fusion center, then they try to deceive the network by changing their probabilities of attacking.

The global false alarm probability Q_f and detection probability Q_d by considering the attackers are given by

$$Q_D = \sum_{i=k}^{N} \binom{N}{i} {P_D}^i (1 - P_D)^{N-i} \tag{4.22}$$

$$Q_F = \sum_{i=k}^{N} \binom{N}{i} {P_F}^i (1 - P_F)^{N-i} \tag{4.23}$$

where P_D and P_F are the overall detection probability and false alarm probability respectively. Specifically, P_D and P_F can be calculated as

$$P_D = \alpha(P_d^B) + (1 - \alpha)P_d^H \tag{4.24}$$

$$P_F = \alpha(P_f^B) + (1 - \alpha)P_f^H \tag{4.25}$$

Hence, based on these equations the probability of error Q_E is given by

$$Q_E = P_0 Q_F + P_1(1 - Q_D) \tag{4.26}$$

4.3 Optimal Byzantine attack strategies

Byzantine attackers try to degrade the network performance by attacking independently relying on its own observation and decision based on the parameters α and P. P_{iso}^{B} is the probability that a byzantine attacker is detected by the defense mechanism and eliminated from the system. So, based on the tradeoff values between w and T, FC derives threshold η such that only the Byzantine attackers will be removed and the honest CRs remain in the network.

We employ the Kullback-Leibler divergence as a network performance metric that characterizes the detection performance. The KLD between the distributions $q = P(u_i = j|H_0)$ and $r = P(u_i = j|H_1)$ is given by

$$D(r \parallel q) = \sum_{j} P(u_i = j|H_1) \log \frac{P(u_i = j|H_1)}{P(u_i = j|H_0)} \tag{4.27}$$

where $j \in \{0, 1\}$.

Byzantine attackers want to make maximum damage to the spectrum sensing process as possible by sending falsified data as many times as possible. This can be achieved by reducing KLD between probability density function(pdfs) resulting in more decision errors. So minimizing the KLD between two hypotheses at the fusion center is $D(P(u_i|H_1) \parallel P(u_i|H_0)) = 0$ or equivalently $P(u_i|H_1) \equiv P(u_i|H_0)$. The KLD under the data falsification attack can be given as [5]:

$$\begin{aligned} D(r \parallel q) = (1 - \alpha P - P_d(1 - 2\alpha P)) \log \frac{1 - \alpha P - P_d(1 - 2\alpha P)}{1 - \alpha P - P_f(1 - 2\alpha P)} \\ + (\alpha P - P_d(1 - 2\alpha P)) \log \frac{\alpha P + P_d(1 - 2\alpha P)}{\alpha P + P_f(1 - 2\alpha P)} \end{aligned} \tag{4.28}$$

We discuss KLD as a function of flipping probability P. Fig 5.4, illustrates that KLD is a monotonically increasing function of $t = (1 - 2\alpha P)^2$ when $P_d = 0.6$, $P_f = 0.2$.

Lemma 1:Let $t = (1-2\alpha P)^2$ or $\alpha P = \frac{1\pm\sqrt{t}}{2}$. KLD is a monotonically increasing function of t for any $P_d > 0.5$ and $P_f < 0.5$,

Proof. : When $\alpha P = \frac{1-\sqrt{t}}{2}$,

$$D(r \parallel q) = \Big(\frac{1+\sqrt{t}}{2} - P_d\sqrt{t}\Big)\log\frac{1+\sqrt{t}-2P_d\sqrt{t}}{1+\sqrt{t}-2P_f\sqrt{t}} + \Big(\frac{1-\sqrt{t}}{2} + P_d\sqrt{t}\Big)\log\frac{1-\sqrt{t}+2P_d\sqrt{t}}{1-\sqrt{t}+2P_f\sqrt{t}} \quad (4.29)$$

$$\begin{aligned}\frac{dD}{dt} &= \frac{2P_d-1}{4\sqrt{t}}\Big[\Big(1-\frac{1+\sqrt{t}(2P_d-1)}{1+\sqrt{t}(2P_f-1)}\frac{2P_f-1}{2P_d-1}+\log\Big(\frac{1+\sqrt{t}(2P_d-1)}{1+\sqrt{t}(2P_f-1)}\Big)\Big)\\ &\quad-\Big(1-\frac{1-\sqrt{t}(2P_d-1)}{1-\sqrt{t}(2P_f-1)}\frac{2P_f-1}{2P_d-1}+\log\Big(\frac{1-\sqrt{t}(2P_d-1)}{1-\sqrt{t}(2P_f-1)}\Big)\Big)\Big]\\ &= \frac{2P_d-1}{4\sqrt{t}}\Big[\log\Big(\frac{1+\sqrt{t}(2P_d-1)}{1+\sqrt{t}(2P_f-1)}\Big)-\log\Big(\frac{1-\sqrt{t}(2P_d-1)}{1-\sqrt{t}(2P_f-1)}\Big)\Big]\\ &\quad+\frac{2P_f-1}{4\sqrt{t}}\Big[\frac{1-\sqrt{t}(2P_d-1)}{1-\sqrt{t}(2P_f-1)}-\frac{1+\sqrt{t}(2P_d-1)}{1+\sqrt{t}(2P_f-1)}\Big] \quad (4.30)\end{aligned}$$

Therefore, when $\alpha P = \frac{1-\sqrt{t}}{2}$, we have

$$D(r \parallel q) = \left(\frac{1-\sqrt{t}}{2} + P_d\sqrt{t}\right)\log\frac{1-\sqrt{t}+2P_d\sqrt{t}}{1-\sqrt{t}+2P_f\sqrt{t}} + \left(\frac{1+\sqrt{t}}{2} - P_d\sqrt{t}\right)\log\frac{1+\sqrt{t}-2P_d\sqrt{t}}{1+\sqrt{t}-2P_f\sqrt{t}} \quad (4.31)$$

Now, to prove that $D(r \parallel q)$ is monotonically increasing, we need to prove that $\frac{dD}{dt} > 0$. To prove that we need to show that $\frac{2P_f-1}{4\sqrt{t}}\left[\frac{1-\sqrt{t}(2P_d-1)}{1-\sqrt{t}(2P_f-1)} - \frac{1+\sqrt{t}(2P_d-1)}{1+\sqrt{t}(2P_f-1)}\right] > 0$ which is equivalent to show that ,

$$\frac{2P_f-1}{4\sqrt{t}} < 0 \quad (4.32)$$

and

$$\left[\frac{1-\sqrt{t}(2P_d-1)}{1-\sqrt{t}(2P_f-1)} - \frac{1+\sqrt{t}(2P_d-1)}{1+\sqrt{t}(2P_f-1)}\right] < 0 \quad (4.33)$$

To show that this is true, we use the fact that $\frac{(1+a)}{(1+b)} > \frac{(1-a)}{(1-b)}$ iff $a > b$ where $a, b < 1$. As $0.5 < P_d < 1$ and $0 < P_f < 0.5$ implies that $P_d > P_f$ and above inequality is

true. Now, we show that $\frac{2P_d-1}{4\sqrt{t}}\left[\log\left(\frac{1+\sqrt{t}(2P_d-1)}{1+\sqrt{t}(2P_f-1)}\right)-\log\left(\frac{1-\sqrt{t}(2P_d-1)}{1-\sqrt{t}(2P_f-1)}\right)\right] > 0$ which is equivalent to,

$$\frac{2P_d-1}{4\sqrt{t}} > 0 \tag{4.34}$$

and

$$\left(\log\frac{1+\sqrt{t}(2P_d-1)}{1+\sqrt{t}(2P_f-1)}\right) > \left(\log\frac{1-\sqrt{t}(2P_d-1)}{1-\sqrt{t}(2P_f-1)}\right) < 0 \tag{4.35}$$

Based on the above inequalities from (4.23), (4.24) is is clear that $\frac{dD}{dt} > 0$, which completes the proof. ■

Optimization of attack by Byzantines is given by minimizing $(1-2\alpha P)^2$.

Case1: When $\alpha \leq 0.5$: Attackers try to decrease P_{iso}^B, such that, they cannot be identified immediately. So, based on the Byzantine attackers can vary their probability of attack P.

Case2:When $\alpha > 0.5$: The optimal flipping probability for the attackers is $P = \frac{1}{2\alpha}$ as KLD $= 0$.

When the Byzantine attackers are trying to degrade the network by choosing the optimal probabilities, the fusion center also try to minimize their attacks by changing the threshold η.

CHAPTER 5

Simulations and Results

In this chapter, we present simulation results that illustrate the performance of the proposed method. We assume the cognitive radios are detecting the presence or absence of primary user. Fig 5.1, Fig 5.2 shows the effect of Byzantines on the probability of detection and probability of false alarm.

Figure 5.1: Effect of Byzantines on probability of detection

Figure 5.2: Effect of Byzantines on probability of false alarm

As we can see from both figures fraction of Byzantines affects the performance of the network. Also, as the number of Byzantines increases we can observe the degradation in the probability of detection, i.e., as number of Byzantines increase P_d decreases.

In Figure 5.3, we plot the CDF for P_n, i.e., third strategy. It can be seen that P_n is spread over wide range of values.

Figure 5.4 illustrates the result that KLD is a monotonically increasing function of $t = (1 - 2\alpha P)^2$ when $P_d = 0.6$ and $P_f = 0.2$.

Figure 5.3: Possible attack strategies of Byzantines

5.1 Effect of Byzantines

Now we consider, probability of detection $P_d = 0.8$ and probability of false alarm $P_f = 0.2$. Further we assume that probability of detection and false alarm for honest and Byzantine CR's, i.e., $P_d^H = 0.8$, $P_f^H = 0.2$. Prior probabilities of the hypotheses are assumed to be equal, $P_0 = P_1 = 0.5$. The Fusion center observes local decisions of the nodes over a time window $T = 20$. Reputation threshold η has been chosen such that probability of honest being removed from the process at the end of time window is low i.e., $w = 0.3$. Toatal number of nodes $N = 100$.

In Figure 5.5 , we plot the achievable (P_{iso}^B) as a function of flipping probability P. It can be observed that probability of Byzantines being isolated from the process increases with increasing of P.

Figure 5.4: KLD as a function of parameter t

In Figure 5.6, we plot (P_{iso}^{B}) as a function of flipping probability $P = \frac{1}{2\alpha}$. It can be observed that (P_{iso}^{B}) increases slowly with decrease in number of attackers.

Figure 5.7, we plot (P_{iso}^{B}) as a function of reputation threshold η and time window T. We choose the value of w such that the probability of an honest CR being isolated from the system is very low, i.e., $w = 0.3$. In this plot the time window varies. As a result the reputation threshold also varies. Decreasing w will result in increase of η, which leads to a decrease in the value of (P_{iso}^{B}). So, there is a trade off while selecting the value of w. Increasing the value of η will result in decrease of (P_{iso}^{B}). So, FC need to choose a suitable w and relatively small for T such that, Byzantine elimination can be done quickly.

Figure 5.5: (P_{iso}^{B}) as a function of flipping probability P

5.2 Game between Attackers and Fusion center

In this section, based on the simulated data, we validate our analysis between attackers and Fusion center. The main aim of an attacker is to degrade the system performance and the aim of Fusion Center(FC) is to improve the performance of the system by eliminating the attackers. So, a game is formulated between attackers and FC based on the probabilities of attack strategies and the performance metric 'reputation threshold η'.

(P_{iso}^{B}) and (P_{iso}^{H}) are the two important factors, which denote the the probabilities of detecting a CR byzantine and isolating them from the system. As per the results in Fig 5.7, we need to choose $w = 0.3$ to reduce the isolation of honest CR's by considering them as Byzantines.

Figure 5.6: (P_{iso}^{B}) as a function of flipping probability $P = \frac{1}{2\alpha}$

In Figure 5.8, we plot (P_{iso}^{B}), (P_{iso}^{H}) and Q_E (before eliminating CRs from the system) as a function of α. Consider if more number of attackers attack the system. We show that as α, i.e., fraction of Byzantine attackers varies, (P_{iso}^{B}) and (P_{iso}^{H}) also varies accordingly. As α approaches 0.5, i.e., '*blinding region*' we can observe that value of (P_{iso}^{B}) decreases and on the other hand value of (P_{iso}^{H}) increases. So, this leads to increase of probability of error Q_E. At $\alpha = 0.5$ we have $Q_E = 0.5$, indicating that if number of attackers in the system exceeds by more than 50% then FC will be incapable of making a decision. So, the decision will purely be a random guess.

In our simulations, we consider M i.e., number of attackers = 40 ($\alpha = 0.4$) as attackers will be incapable of making FC blind. $k = N/2$, i.e., the number of CR's required to obtain a decision about the presence or absence of a PU. In Figure 5.9,

Figure 5.7: (P^B_{iso}) as a function of η and T

Figure 5.10 we plot the differences in (P^B_{iso}), (P^H_{iso}) and Q_E as a function of probability of attack P at $\alpha = 0.4$ and $\alpha = 0.5$. We show that, when $\alpha < 0.5$, Q_E, (P^H_{iso}) will be low and (P^B_{iso}) will be high. We have shown that at $\alpha = 0.5$ we have $(P^B_{iso}) = (P^H_{iso})$, which represents that KLD = 0 i.e., (P^B_{iso}) - $(P^H_{iso}) = 0$.

Now the attackers, wants to remain in the system without being eliminated, so they want to reduce the value of (P^B_{iso}). Whereas, FC wants to eliminate these attackers so that it can improve the performance of the system. By changing the values of probability of attack P, attackers can reduce (P^B_{iso}) and by changing the values η and T, FC can increase the value of (P^B_{iso}). So, according to FC there will be a trade off while selecting the values such that, (P^B_{iso}) will be high. T should not be very high because there will be a delay in decision making and attackers causing more damage

Figure 5.8: (P_{iso}^{B}),(P_{iso}^{H}) and Q_E as a function of α

to the system before they are eliminated.

In Figure 5.11, we show that the value of (P_{iso}^{B}) decreases as P decreases, and (P_{iso}^{B}) $= 0$ as η increases to $T = 15$.

Now we plot Q_D,Q_F and Q_E based on various parameters.
In Figure 5.12, we plot Q_D,Q_F and Q_E (before eliminating CRs from the system) as a function of number of attackers. As the number of attackers increase in the system, we know that the value of Q_D decreases and value of Q_F increases, leading to an increase in the value of Q_E.

In Figure 5.13, we plot Q_D,Q_F and Q_E (before eliminating CRs from the system) as a function of attacking probability P. As P increases, attackers attack with

Figure 5.9: (P_{iso}^{B}),(P_{iso}^{H}) and Q_E as a function of P when $\alpha = 0.4$

higher probabilities, so value of Q_F increases. As a result, (P_{iso}^{B}) also increases which leads to more elimination of the attackers from the system thus reducing the value of Q_E.

In Figure 5.14, we plot Q_D,Q_F and Q_E (after eliminating CRs from the system) as a function of detection probability P_D. As more number of Byzantines are eliminated from the system, it results in a decrease in the value of Q_F and as P_D reaches 1 we can observe that the false alarm and probability of error Q_E reaches 0.

Figure 5.10: (P_{iso}^{B}),(P_{iso}^{H}) and Q_E as a function of P when $\alpha = 0.5$

Figure 5.11: (P_{iso}^{B}) as a function of P and η

Figure 5.12: Q_E,Q_D and Q_F w.r.t the number of Attackers

Figure 5.13: Q_E,Q_D and Q_F w.r.t P

Figure 5.14: Q_E,Q_D and Q_F w.r.t P_d

CHAPTER 6

Conclusions and Future work

In summary, we have analyzed several issues related to CRs in the presence of Byzantine attackers. We have considered, the optimal fusion rule at FC to identify the attackers. First we considered energy detection at each CR and based on k out of N rule we obtained the threshold at FC to fuse the decisions of all CRs. Next we considered the possible attack strategies for the Byzantine attackers in order to escape the identification as an attacker.

In CR networks with binary hypotheses, we found the optimal values at which attackers blind FC and KLD becomes zero. From the FC perspective, we presented an easy, efficient reputation metric scheme to eliminate the attackers by counting the mismatches between local and global decisions. We have shown that the proposed scheme was successful in eliminating the Byzantine attackers from the system. These countermeasures need to be incorporated by the attackers to overcome FC strategies.

We modeled the game between attackers and FC, under the assumption that the attacker and FC are aware of each other strategies. When the Byzantines are identified and eliminated from the system, the attackers want to remain so that they can degrade the network performance. So, they try to decrease P_{iso}^{B} by changing their probability of attack and similarly when FC identifies that attackers decreasing their probability of attack it needs to change the reputation threshold η such that the value of P_{iso}^{B} increases. We also considered the problem of optimizing the strategies

of attackers and FC to achieve their goals.

There are still many interesting questions that remain to be explored in future work which can be conducted on collaboration of the Byzantine attackers to bring down the network, Byzantine attackers forming into small groups, where Byzantine attackers can control the thresholds for making local decisions and deceiving the FC and the counter measures that needs to be incorporated at the FC to overcome these sort of attack strategies. Also it will be interesting if attackers can overhear the honest users and take decisions accordingly.

BIBLIOGRAPHY

[1] Federal Communications Commission, "Facilitating opportunities for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies," ET Docket No. 03-108, Dec. 2003.

[2] C.S.Hyder, B.Grebur and Li Xiao, "Defense against Spectrum Sensing Data Falsification Attacks in Cognitive Radio Networks," *Security and Privacy in computer networks* , 2012.

[3] S. Haykin,"Cognitive radio: Brain Empowered Wireless Communications," *IEEE Journal Selet. Area on Communications*, vol. 23, no. 2, pp: 201-220, Feb. 2005.

[4] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Jl. on Sel. Areas in Commun.*, vol. 26, no. 1, pp: 25-37, Jan. 2008.

[5] A.S. Rawat , P. Anand, H. Chen and P.K. Varshney, "Collaborative Spectrum Sensing in the Presence of Byzantine Attacks in Cognitive Radio Networks,"*IEEE Transactions in Signal Processing*, vol. 59, no. 2, pp: 774-786, Feb. 2011.

[6] J. Mitola, III and G. Q. Maguire, Jr., "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13-18, Aug. 1999.

[7] D. B. Rawat, G. Yan, C. Bajracharya, "Signal Processing Techniques for Spectrum Sensing in Cognitive Radio Networks," *International Journal of Ultra Wideband Communications and Systems*, vol. 10, pp:1-10, 2010.

[8] I.F. Akyildiz, F.Lo Brandon, R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Broadband Wireless Networking Laboratory*, vol. 4, pp: 40-62, 2011.

[9] K. Ezirim and S. Sengupta, "Self-Coexistence Among Cognitive Radio Networks Using Risk-Motivated Channel Selection Based Deference Structure," *Tsinghua Science and Technology*, ISSN 1007-0214ll04/11 , pp: 242-249, vol. 18, no. 3, June 2013.

[10] L. Duan, Alexander W. Min, J. Huang, K.G. Shin, " Attack Prevention for Collaborative Spectrum Sensing in Cognitive Radio Networks," *IEEE Journoul on selscted areas in Communication*, vol. 30, no. 9, October 2012.

[11] R. Chen, J. M. Park and K. Bian, "Robust Distributed Spectrum Sensing in Cognitive Radio Networks", *INFOCOM: The 27th Conference on Computer Communications*, pp: 1876 -1884, IEEE (2008).

[12] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *Commu-nications Surveys Tutorials, IEEE*, vol. 15, no. 1, pp: 428-445, First Quarter 2013.

[13] H. Rifa-Pous, M. J. Blasco, and C. Garrigues, "Review of robust cooperative spectrum sensing techniques for cognitive radio networks," *Wireless Personal Communications*, vol. 67, no. 2, pp: 175-198, Nov. 2012.

[14] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of byzantine attacks," *Signal Processing, IEEE Transactions*, vol. 57, no. 1, pp: 16-29, Jan. 2009

[15] T. Ikuma and M. Naraghi-Pour,"A Comparison of Three Classes of Spectrum Sensing Techniques," *IEEE GLOBECOM proceedings*, 2008.

[16] Z. Chair and P. K. Varshney, "Optimal data fusion in multiple sensor detection systems," *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-22, no. 1, pp: 98-101, Jan. 1986.

[17] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 2, no. 1, pp: 28-40, Feb. 2008.

[18] P. K. Varshney, "Distributed Detection and Data Fusion," *New York: Springer-Verlag*, 1997.

[19] J. G. Proakis," *Digital Communications*, 4th ed. McGraw-Hill, 2001.

[20] R. Tandra and A. Sahai,"Fundamental limits on detection in low SNR under noise uncertainty," in *Proc. IEEE Int. Conf. Wireless Networks, Commun. and Mobile Computing*, vol. 1, Pacific Grove, California, USA, pp: 772-776, Nov. 2004

[21] A. Shahzad et. al., "Comparative Analysis of Primary Transmitter Detection Based Spectrum Sensing Techniques in Cognitive Radio Systems," *Australian Journal of Basic and Applied Sciences*, vol. 4, pp: 4522-4531, INSInet Publication, Sep. 2010.

[22] A. V. Oppenheim, R. W. Schafer and J. R. Buck," *Discrete-Tme Signal Processing*, Prentice Hall, 1999.

[23] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. IEEE*, vol. 55, pp: 523-531, Apr. 1967.

[24] A. Sahai, N. Hoven, R. Tandra, "Some Fundamental Limits on Cognitive Radio," *Proc. of Allerton Conference*, Monticello, Oct 2004.

[25] U. Gardner, WA, "Exploitation of spectral redundancy in cyclostationary signals," *IEEE Signal Processing Mag.*, vol. 8, no. 2, pp: 14-36, 1991.

[26] K. Kim, I. A. Akbar, K. K. Bae, J. Urn, C. M. Spooner and J. H. Reed, "Cyclostationary Approaches to Signal Detection and Classification in Cognitive Radio," *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 2007.

[27] J. Lunden, V. Koivunen, A. Huttunen and H. V. Poor, "Spectrum sensing in cognitive radios based on multiple cyclic frequencies," *2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, Orlando, FL, Jul. 2007.

[28] E. Visotsky, S. Kuffner, R. Peterson, "On collaborative detection of tv transmissions in support of dynamic spectrum sharing," *Proc. of IEEE DySPAN 2005*, pp: 338-345.

[29] J. Unnikrishnan, V.V. Veeravalli, "Cooperative sensing for primary detection in cognitive radio," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, pp: 18-27, Jan 2008.

[30] Z. Li, F. Yu, M. Huang, "A cooperative spectrum sensing consensus scheme in cognitive radios," *Proc. of IEEE Infocom*, pp: 2546-2550, 2009.

[31] G. Ganesan, Y.G. Li, "Cooperative spectrum sensing in cognitive radio Part I: two user networks," *IEEE Transactions on Wireless Communications*, vol. 6, pp: 2204-2213, June 2007.

[32] G. Ganesan, Y.G. Li, "Cooperative spectrum sensing in cognitive radio Part II: multiuser networks," *IEEE Transactions on Wireless Communications*, vol.6, pp: 2214-2222, June 2007.

[33] A. Vempaty, L. Tong, and P. K. Varshney,"Distributed inference with Byzantine data: state-of-the-art review on data falsification attacks," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp: 65-75, Sep. 2013.

[34] W. Wang, H. Li, Y. Sun and Z. Han, "CatchIt: Detect Malicious Nodes in Collaborative Spectrum Sensing," *IEEE Global Telecommunications Conference*, (GLOBECOM 2009), pp: 1-6 (2009).

[35] K. Praveen , M. Khabbazian, V. K. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," *IEEE Comm. society in ICC proceedings*, 2008.

[36] K. Praveen , M. Khabbazian, V. K. Bhargava, "Malicious User Detection in a Cognitive Radio Cooperative Sensing System", *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, Aug 2010.

[37] H. Li and Z. Han, "Catching Attackers for Collaborative Spectrum Sensing in Cognitive Radio Systems: An Abnormality Detection Approach", *IEEE Symposium on New Frontiers in Dynamic Spectrum*, pp: 1-12 (2010).

[38] O. Sheynin, "Theory of Probability." *A Historical Essay, Berlin, Germany*, 2009.

[39] Z. Yuan, H. Xue, Y. Cao and X. Chang, "Exploiting Optimal Threshold for Decision Fusion in Wireless Sensor Networks", *International journal of Distributed Sensor Networks*, vol .14, Feb. 2014.

VITA

Candidate for the Degree of

Master of Science

Thesis: STUDY OF BYZANTINE ATTACKS AND COUNTERMEASURES IN SPECTRUM SENSING

Major Field: Electrical Engineering

Biographical:

Personal Data:

Born in Visakhapatnam, Andhra Pradesh, India on July 25, 1991.

Education:

Received the B.E. degree from Gandhi Institute of Technology and Management, Visakhapatnam, Andhra Pradesh, India, 2012, in Electronics and Communication Engineering.

Completed the requirements for the degree of Master of Science with a major in Electrical Engineering Oklahoma State University in July, 2014.

Experience:

RF intern at GTL from July 2013 to Aug 2013.

Volunteer at the Statistical Signal Processing Lab under Dr. Qi Cheng from January 2014 to July 2014.

Before joining Oklahoma State University he worked as intern at Electronics corporation of India limited(ECIL), Hyderabad, India over the summer of 2011.