Detecting Primary User Emulation Attacks in Cognitive Radio Networks

By

Fan Jin
Supervised by: Prof. Vijay Varadharajan

A thesis submitted to Macquarie University
for the degree of Mres
Department of Computing
February 2015

Except where acknowledged in the customary manner, the material presented in this thesis is, to the best of my knowledge, original and has not been submitted in whole or part for a degree in any university.

Fan Jin
Supervised by: Prof. Vijay Varadharajan

Acknowledgments

First and foremost, I want to thank my supervisor Professor Vijay Varadharajan, who has brought me to the world of cognitive radio, accompanied me to overcome the difficulties along the way, and encouraged me to pursue excellence. I would also like to thank Dr Udaya Tupakula, who helped me a lot during the time when I was learning and writing the thesis. Whenever I am overwhelmed or need help, Professor Varadharajan and Dr Tupakula are always there to show me the correct direction and provide me necessary instructions. Professor Varadharajan and Dr Tupakula instruct me to identify, formulate, and solve problems during the research. I have no doubt that the skills I have learned from them will stay with me throughout my life and help to maximize the chance of success in my career. My gratitude towards them is beyond words.

During my MRes degree, the excellent courses in computing department of Macquarie University have shaped my knowledge base and enriched my skill sets. I definitely appreciate the lectures and trainings provided by Macquarie University.

I would also like to thank my manager at work, Andy Mccarthy, who gave me necessary support for me to do my research degree in part time. Special thanks to my colleague Daniel Baker, who spent time reviewing my thesis.

Last but not least, I am grateful to my family. My parents, Professor Jin Zhonghui and Professor Shi Ge, and my wife Tingting Wang. I am not able to achieve what I have achieved without their whole-hearted support and encouragement. They are the people who care me; who give me strength to take on any challenges that are ahead of me; and who always stand by me and make everything in my life simpler.

Abstract

Cognitive radio (CR) is a promising technology for future wireless networks in order to efficiently utilize the limited spectrum resources and satisfy the rapidly increasing demand for wireless applications and services. However, CR wireless networks are susceptible to various security attacks. In this thesis, we identify security threats to spectrum sensing, which referred to as primary user emulation (PUE) attacks. In this attack, an adversary's CR transmits signals whose characteristics emulate those of incumbent signals. The highly flexible, software-based air interface of CRs makes such an attack possible. This thesis first covers an introduction of cognitive radio, dynamic spectrum access and spectrum sensing, as well as the potential security threats and their impacts to cognitive radio networks. Then we focus on PUE attacks and investigate existing techniques for detecting this threat such as energy detection, localization, cyclostationary feature calculation and artificial neural network. To counter the PUE attack, an improved energy detection method with multiple thresholds is proposed. Then we propose two new schemes that combine the improved energy detection method with TODA localization and cyclostationary feature detection respectively to identify PUE attackers in different scenarios in cognitive radio networks.

Contents

List of Figures

1 Introduction

1.1 Current State of Wireless Applications

Our modern society heavily depends on the wireless spectrum for communication purposes. Telecommunications, financial transactions, health services, military services, environment surveillance, entertainment and social activities are just several of the numerous applications examples in our daily life. The increasing demand of the above applications requires reliable access to spectrum at a reasonable cost. Figure 1.1 displays the overall mobile data traffic is expected to grow to 15.9 exabytes per month by 2018, nearly an 11-fold increase over 2013. The figure clearly shows that wireless communication continues to grow quickly nowadays [1].

However, with the rapid increasing of mobile devices and their requirements for the spectrum, the limited available spectrum becomes a constrained resource. One of the major reasons is because the current wireless networks are characterized by a static spectrum allocation policy, where governmental agencies assign wireless spectrum to license holders on a long-term basis for large geographical regions. For example, most of the wireless spectrum ranging between 0 Hz and 3 GHz has already been allocated via static assignments to a range of governmental, corporate, and academic entities [2], and there exist numerous instances where multiple spectrum assignments have been made for several frequency bands. This assignment situation has resulted in fierce competition for the use of wireless spectrum. This is especially true in frequency bands located below 3 GHz, which is considered to be prime spectral real estate.

In contrast, a large portion of the assigned spectrum has been observed during several spectrum measurement campaigns [3][4] that is sparsely and sporadically utilized. In particular, spectrum occupancy by licensed transmissions is often concentrated across specific frequency ranges while a significant amount of the spectrum remains either underutilized or completely unoccupied. A study made at the Berkeley Wireless Research Center (BWRC)

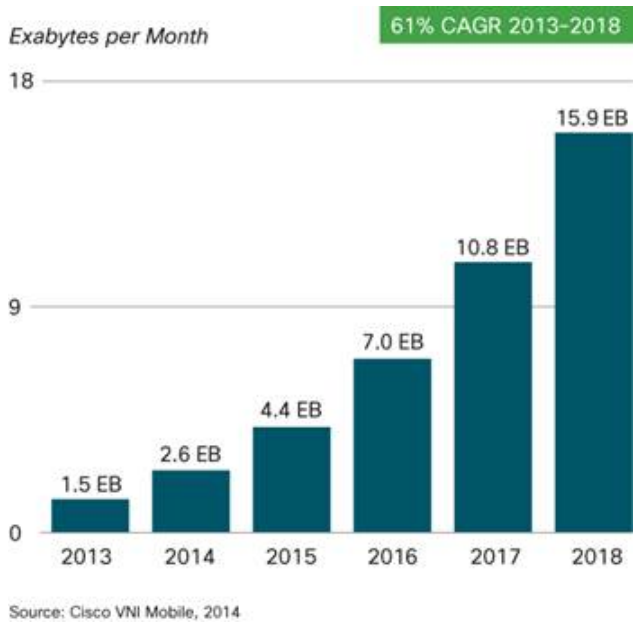

FIGURE 1.1: Cisco Forecasts 15.9 Exabytes per Month of Mobile Data Traffic by 2018.

shows that most spectrum, particularly from 1 GHz to 10 GHz is under-utilized, as shown in Figure 1.2. Hence, it appears that the spectrum scarcity issue described above can be considered to be artificially generated due to the legacy regulatory and licensing processes as well as the inefficient utilization of assigned spectrum by the licensed transmissions.

1.2 Cognitive Radio and Cognitive Radio Network

To remedy this spectrum scarcity issue, cognitive radio (CR) was proposed as an efficient and opportunistic use of the frequency spectrum in order to increase spectral efficiency. CR is one of the key technologies that provide the capability to share the wireless channel with licensed users in an opportunistic manner. The wireless devices with CR capability are called CR nodes, which can sense their environment and spectrum, analyze the discovered information, and adjust to the sensed environment. CR nodes are capable of discovering temporally unused spectrum, i.e., spectrum hole or white space by performing spectrum sensing, and then adapt themselves to use the idle band without causing an interference.

A cognitive radio network (CRN) is an intelligent network that contains both licensed users and unlicensed wireless users who have CR capabilities; these users are referred to as primary users (PUs) and secondary users (SUs) respectively. The CRNs adapt to changes in their environment to make a better use of the radio spectrum and help to address the problem of spectrum shortage by allowing SUs to use primary systems without interference.

In the following two sections, cognitive radio and cognitive radio networks will be introduced and discussed with more details.

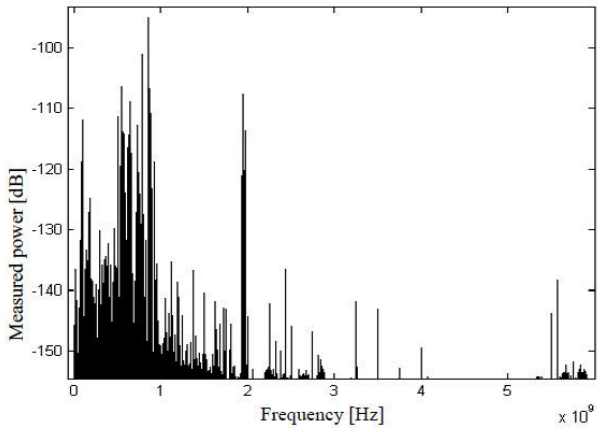

FIGURE 1.2: Spectrum utilization measurement at BWRC.

1.2.1 Cognitive Radio (CR)

The concept of CR was first proposed by Joseph Mitola III [5][6] as an extension of Software Defined Radio (SDR) and formally introduced to the radio community in 1999, which served to improve the overall performance of the radio in relation to its interaction with the spectrum and hence alleviate the spectrum shortage problem by enabling unlicensed users equipped with CR functionalities to co-exist with licensed users. In 2003, the FCC formally defined CR as a radio that has the technical capability to adapt their use of the spectrum in response to information external to the radio [7]. Such a definition implies two characteristics of a CR: cognitive capability and reconfigurability [8], which can be defined as below:

- *cognitive capability*: Through real-time interaction with the radio environment, the portions of the spectrum that are unused at a specific time or location can be identified. As shown in Figure 1.3, CR is capable of detecting spectrum hole or white space. Consequently, the best spectrum can be selected, shared with other users, and exploited without interference with the licensed user.

- *reconfigurability*: A CR can be programmed to transmit and receive on a variety of frequencies, and use different access technologies supported by its hardware design [9]. Through this capability, the best spectrum band and the most appropriate operating parameters can be selected and reconfigured.

In the other words, the definition of CR specifically means that CRs used by SUs need to be able to scan a certain spectrum range and intelligently decide which spectrum band to use for its transmission. Accordingly, the cognitive capability specifically refers to the ability to detect spectrum hole or white space, and the reconfigurability refers to the ability to dynamically vary the modulation scheme, transmission power, time, and frequency.

In order to provide these capabilities, CR requires a novel radio frequency (RF) transceiver architecture. The main components of a CR transceiver are the radio front-end and the base-band processing unit that were originally proposed for software-defined radio (SDR) [5], as

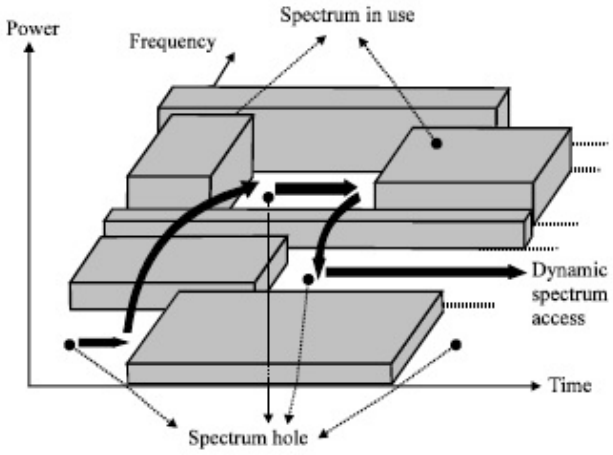

FIGURE 1.3: Overview of cognitive radio: the spectrum hole concept.

shown in Figure 1.4. At the RF front-end the received signal is amplified, mixed, and analog-to-digital (A/D) converted. At the baseband processing unit, the signal is modulated/demodulated. Each component can be reconfigured via a control bus to adapt to the time-varying RF environment. The novel characteristic of the CR transceiver is the wideband RF front-end that is capable of simultaneous sensing over a wide frequency range. This functionality is related mainly to the RF hardware technologies, such as wideband antenna, power amplifier, and adaptive filter. RF hardware for the CR should be capable of being tuned to any part of a large range of spectrum. However, because the CR transceiver receives signals from various transmitters operating at different power levels, bandwidths, and locations, the RF front-end should have the capability to detect a weak signal in a large dynamic range, which is a major challenge in CR transceiver design [10].

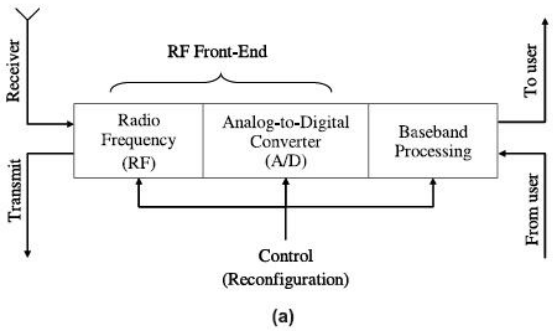

FIGURE 1.4: Cognitive radio transceiver architecture.

On the other hand, CR can be classified as two types [11]: Policy Radios and Learning Radios. Policy radios have some predefined policies that determine the behavior of a radio. When a radio gathers information from the surrounding environment, the information is then turned into statistics that determines state of the radios. Learning radios have an extra

component that is a learning engine; this engine allows them to configure and re-configure their states. Radios with a learning engine are able to try out different parameters and determine which works well in a particular environment. It is important to point out that similar attacks may lead to different effects on the different types of CR. For example, in a policy radio, an attacker with knowledge of how statistics are calculated can force a desired output. This attack can affect learning radios as well; however, as they have a learning engine, the attack can have a longer effect on them, as they learn or accumulate information from this experience which may dictate a certain behavior in the future. The PUE attack that will be discussed in Section 2.3 is an example of such an attack that has a bigger impact on learning radios than policy radios. In this thesis, we will only be considered with the learning radios.

1.2.2 Cognitive Radio Networks(CRNs)

A cognitive radio network (CRN) is a network composed of CR nodes that, through learning and reasoning, can dynamically adapt to varying network conditions in order to optimize end-to-end performance [8]. Mitola first made a brief mention of how the CRs could interact within the system-level scope of a cognitive network [6]. Generally, there are three types of classification for the CRN [8].

The first classification is based on the network architecture, which can be described as the infrastructure-based CRNs or, ad-hoc based CRNs [12] or a mesh based CRN. An infrastructure based CRN (see Figure 1.5) has base stations or access points. A device with CR capabilities may communicate with other devices within the range of the base station through the base station itself and communication between devices in different cells is routed by the base stations. On the other hand, ad-hoc based CRNs (See Figure 1.6) are formed by devices without the need for base stations. The devices can establish links between each other using different communication protocols. For example, they may use existing protocols such as bluetooth or they may use spectrum holes. The final architecture is the mesh based one (See Figure 1.7), which is basically a combination of the aforementioned architectures. It allows devices to connect to the base stations through neighboring devices, and then the base stations work as routers and forward the packets.

Secondly, the access behaviour of CRNs can be based on cooperation or non-cooperation. Cooperation based solutions consider the effect of the node's communication on other nodes [16]. Cooperative based solutions can be centralized or distributed. On the contrary, non-cooperative solutions consider only the node at hand [17].

Finally, considering the access technology, CRNs can also be classified as spectrum overlay or spectrum underlay [1]. A CR node using spectrum overlay approach accesses the spectrum which has not been used by licensed users. So, interference to PUs is minimized. Spectrum underlay exploits the spread spectrum techniques developed for cellular networks [18]. A CR using spectrum underlay approach operates below the noise floor of PUs. In other words, its transmit power at a certain portion of the spectrum is regarded as noise by the PU.

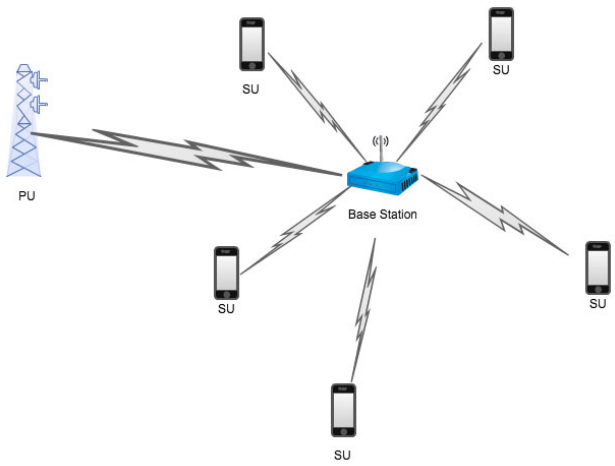

FIGURE 1.5: An infrastructure based CRN.

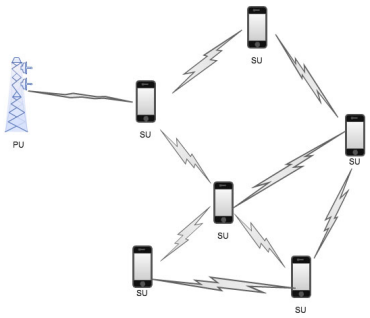

FIGURE 1.6: An Ad Hoc based CRN.

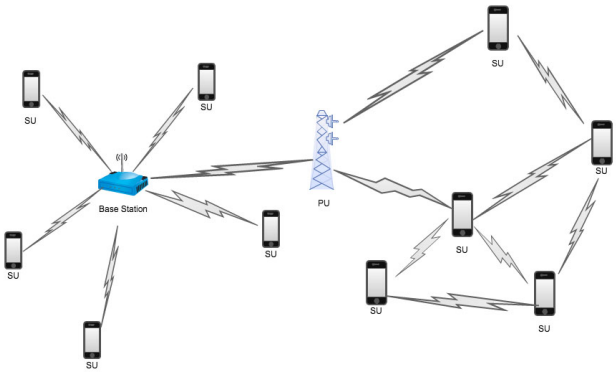

FIGURE 1.7: A mesh based CRN.

1.3 Security Issues in CRN

However, as many other new techniques, in the initial period of adoption, the security issues in CR have not been properly addressed. Compared with the traditional radio, CR is more flexible and exposed to the wireless network medium. As a result, there are more security threats and attacks in CRNs than in a traditional radio environment.

Previous research has been done by Wassim El-Hajj et al. [13] and Ian F. Akyildiz et al. [12] that categorize the security attacks in CRNs into four major classes: Physical Layer attacks, Link Layer attacks (also known as MAC attacks), Network layer attacks, and Transport Layer attacks. From their research we can see despite the benefits of employing this innovative technology, CRNs are vulnerable to new and specific security weakness due to the intelligent behavior of CRNs.

Primary user emulation (PUE) attack is one of the well known malicious attacks that is specific to CRNs. In a PUE attack, since SUs own cognitive and reconfigurability characteristics, these nodes can emulate PUs' behavior by manipulating their radio parameter values. Malicious users may exploit this drawback, impairing the spectrum sharing opportunity of legitimate nodes [14]. Hence, attackers can increase their own opportunities to access licensed bands. PUE attack leads to a low spectrum utilization and inefficient cognitive network operation.

1.4 Organization of the thesis

The remainder of the thesis is organized as follows: In Chapter 2, the background of dynamic spectrum access, cognitive radio, cognitive radio network and spectrum sensing are discussed. Also, security threats in cognitive radio networks, especially the PUE attack is elaborated in a detailed manner.

In Chapter 3, we introduce the basic outline of the techniques that can be utilized to mitigate PUE attacks. In this chapter, we illustrate energy detection, localization, cyclostationary feature detection and artificial neural network, which will be used in our proposed solutions in the following chapter.

Chapter 4 dives into two specific categories for PUE detection. We first propose an improved energy detection by using multiple thresholds and the result generated by all participating SUs in Section 4.2. Then, Section 4.3 proposes the first category based on a combination of signal energy detection and localization. In Section 4.4, we study the second category based on a combination of energy detection and cyclostationary feature detection in artificial neural networks. Finally, simulations are done in Section 4.5.

In Chapter 5, we discuss potential future work that we anticipate in relation to the progress of the PUE detection described in the thesis. Finally Chapter 5 presents the conclusions of the thesis.

2 Background

2.1 Dynamic Spectrum Access, Cognitive Radio, Spectrum Sensing and Cognitive Radio Networks

In Chapter 1, we have briefly introduced the cognitive radio and cognitive radio networks. In this section, they are elaborated again with other concepts which are relevant to our work in the thesis.

2.1.1 Dynamic Spectrum Access (DSA)

As we mentioned in Chapter 1, today's wireless networks are regulated by a fixed spectrum assignment policy, i.e. the spectrum is regulated by governmental agencies and is assigned to license holders or services on a long term basis for large geographical regions [8]. Although the fixed spectrum assignment policy has generally worked well in the past, there is a dramatic increase in the access to the limited spectrum for mobile services in recent years. However, according to FCC, temporal and geographical variations in the utilization of the assigned spectrum range from 15% to 85% [6]. This unbalanced situation is due to the constraints of the traditional spectrum policies.

Such discrepancy between FCC allocations and actual usage indicates that a new approach to spectrum licensing is needed. This approach should provide the incentives and efficiency of unlicensed usage to other spectral bands, while accommodating the present users who have higher priority or legacy rights (PUs) and enabling future systems a more flexible spectrum access [4]. This new approach is called dynamic spectrum access (DSA).

DSA is the process of increasing spectrum efficiency via the real-time adjustment of radio resources, i.e. via a process of local spectrum sensing, probing, and the autonomous establishment of local wireless connections among cognitive nodes and networks. As originally proposed in [5], CR envisions real time spectrum auctions among diverse constituencies, such

as spectrum allocated for cellular radio and public safety. Conversely, the number of radio access points for public safety can also be used more efficiently and commercially during peak periods.

in order to multiply both the number of radio access points for public safety and to more efficiency use public safety spectrum commercially during peak periods.

2.1.2 Spectrum Sensing

The cognitive capability of a CR is realized in the form of spectrum sensing. This important function helps a CR to learn the spectrum holes in its radio environment. However, there are several factors that make spectrum sensing practically challenging. First, signal-to-noise ratio (SNR) can be very low. For example, wireless microphones operating in TV bands only transmit signals with a power of about 50 MW and a bandwidth of 200 kHz. If the SUs are several hundred meters away from the microphone devices, the received SNR may be well below -20 dB. Secondly, multipath fading and time dispersion of wireless channels complicate the sensing problem. Multipath fading may cause signal power to fluctuate as much as 30 dB. On the other hand, unknown time dispersed channel turns coherent detections unreliable. Thirdly, noise/interference level may change with time and location, which yields noise uncertainty [15][16][17].

Several spectrum sensing methods have been proposed so far, including energy detection [15][16][18][19], matched filtering [16][20] and cyclostationary feature detection [21][22]. We briefly discuss the advantages/disadvantages of each of these methods below.

- *Energy detection:* Energy detection is the simplest technique for local spectrum sensing. An energy detector infers the existence of an PU based on the measured signal energy level. To measure the signal energy level in a band, the received signal is first processed using a bandpass filter and then the output signal is squared and integrated over an observation interval. The output of the integrator is then compared with a predefined threshold to decide whether the band is being used or not. When a receiver has no sufficient information about the primary signal, such as the characteristics of the primary signal or the power of the random Gaussian noise, an energy detector is optimal [23].

- *Matched filter detection:* In signal processing, a matched filter (originally known as a North filter [24]) is obtained by correlating a known signal, or template, with an unknown signal to detect the presence of the template in the unknown signal. This is equivalent to convolving the unknown signal with a conjugated time-reversed version of the template. The matched filter is the optimal linear filter for maximizing the SNR in the presence of additive stochastic noise. Matched filters are commonly used in radar, in which a known signal is sent out, and the reflected signal is examined for common elements of the out-going signal. Pulse compression is an example of matched filtering. It is so called because impulse response is matched to input pulse signals. Two-dimensional matched filters are commonly used in image processing, e.g., to improve SNR for X-ray. Matched filters is a demodulation technique with LTI filters to maximize SNR [25].

For spectrum sensing in CRN, when there is a priori knowledge about the primary signal, such as its modulation type, pulse shape, pilot, preambles and synchronization codes, the matched filter is the optimal detector in stationary Gaussian noise because it maximizes the received SNR [23]. The advantage of a matched filter is that it requires less number of samples compared to an energy detector. Moreover, the matched filter can also potentially distinguish different signal types in a band. On the other hand, a disadvantage of the matched filter is that its performance heavily depends on the accuracy of the a priori knowledge about the primary signal.

- *Cyclostationary feature detection:* Modulated signals are generally coupled with sine wave carriers, thereby exhibiting periodicity in their signal structure. Cyclostationary feature detection utilizes the cyclic feature of a signal to detect it. For example, the cyclic autocorrelation function (CAF) and the spectral coherence function (SOF) can both be used to detect signal features [26]. The advantage of the cyclostationary feature detection includes its ability to distinguish different signal types in a band and its robustness against stationary noise with unknown variance. The disadvantage of this technique lies in its computational complexity and long observation time.

Advantages of each spectrum sensing method can be displayed in:

Spectrum Sensing methods	Advantages
Energy detection	Do not require sufficient information about primary signal.
Matched filter detection	Requires less number of samples compared to energy detection; Can also potentially distinguish different signal types in a band.
Cyclostationary feature detection	Able to distinguish different signal types in a band and robust against stationary noise with unknown variance.

While matched filtering based methods require perfect knowledge of the channel responses from the PU to the receiver and accurate synchronization (otherwise, its performance will be reduced dramatically) [27][20]. This may not be possible if there is no cooperation between the primary and secondary users. Cyclostationary feature detection needs to know the cyclic frequencies of the primary signals, which may not be realistic for many applications. Furthermore, it demands excessive analog to digital converter requirement and signal processing capabilities [16]. Energy detection, unlike the other two methods, does not require any information of the source signal and is robust to unknown dispersed channel and fading. Therefore, it is optimal for detecting independent and identically distributed signals [18], but it is not optimal for detecting correlated signals.

In the thesis, we will employ and combine both energy detection and cyclostationary feature detection to identify whether the incoming signal is from the PUs or not. Both techniques will be elaborated with more details in Chapter 3 and an improved energy detection scheme will be proposed as well in order to improve the overall performance. Matched filter detection, as another spectrum sensing method, will not be considered in the thesis since its accuracy heavily depends on the priori knowledge of the primary signal, and we assume the receivers are not required to have such sufficient information about primary signals in our designed systems.

After spectrum hole or white space has been found by spectrum sensing, CR users can allocate a channel based on spectrum availability. This allocation not only depends on spectrum availability, but is also determined based on internal (and possibly external) policies. The allocation procedure has to guarantee that PUs will not be interfered and the whole process works as follows: the SUs scan the spectrum channels by spectrum sensing, once an available channel has been detected, the SUs can share the channel based on their access priority and one of them can start communication in the channel in a given time. If the specific portion of the spectrum used by a SU is required by a PU, the SU has to leave the channel immediately since the PU has the highest priority to use the spectrum channel. And the communication of the SU must be continued in another vacant portion of the spectrum. Such allocation process is also called spectrum management, which includes spectrum sensing, spectrum decision, spectrum sharing and spectrum mobility.

2.2 Security Threats in CRN

As we mentioned in Chapter 1, very little research has examined new threats on CR due to its intelligent behavior. In previous research works, security threats in CRN can be categorized according to the layers they target: Physical, Link, Network, and Transport. Security threats in CRNs are also classified based on the DSA process by some other researchers. Such security threats are specific to CRNs and they will be elaborated below:

- *Spectrum sensing threats:* In DSA environment, PUs have the licence to use the certain frequency band whenever they want. When the PUs do not use their spectrum, the spectrum is idle, and SUs could use the available spectrum opportunistically. Such SUs need sensing algorithms to detect spectrum holes for communication since they have the capability to do so. In addition, a SU has to vacate the channel when the PU uses it.

  One of the threats comes from attackers who want to spoof or mask the PU. The attackers provide a feint of the channel will be used by a PU. Hence the SUs within the transmitting range will believe a PU is active, and vacate the channel. This kind of attack is called Primary User Emulation (PUE), which is introduced in [28] [29], and is the focus in the following parts of the thesis. As a result, the PUE attack provides the attacker access to the spectrum. However, this attack is transient, because when attacker vacates the channel, or stops to spoof a PU, the SUs could detect the idle channel and use it.

There is also another kind of threat called Control Channel Jamming (CCJ), which prevents CR from receiving sensor information or provides the CR with false information. If the CR cannot receive information about spectrum holes or active PUs, or it receives false information, then it cannot make right communication decisions. In some CR, sensor information is transmitted through a common control channel. In this case, it is easy for the attackers to jam or control the unique channel. Thus, designers of CRN who want a common control channel should consider this problem. Paper [11] addresses the leveraged jamming examples. In some CRNs, the sensor and the radio share the same front end. Even when they are separate, the sensor sensitivity can be impaired by a nearby transmitter. So sensing and transmission cannot occur at the same time. The radio can only operate for some fraction of the time, f, with the remaining time being used for sensing. In this case, any jamming becomes leveraged by a factor $1/f$. For instance, because of sensing, the radio can only operate for $f = 70\%$ of the time. Then jamming 35% of the time will reduce the time for communication by $35\%/f = 50\%$. Jamming the sensing time can impact the communication time seriously. The key to avoid leveraged jamming is to make the fraction of time devoted to transmission, f, as close to one as possible. Therefore, good sensing strategies are required in CRNs for mitigating CCJ attacks.

- *Spectrum management threats:*

  Through spectrum sensing, CR detects the idle spectrum bands for communication. These spectrum bands show different characteristics according to time-varying radio environment, operating frequency, bandwidth, and so on. Spectrum management should have the capacity of selecting the most appropriate bands from these bands for users. It should decide on the best spectrum band to meet the Quality of Service (QoS) requirement over all available spectrum bands [8]. In [8], the functions of spectrum management are classified as spectrum analysis and spectrum decision. Spectrum analysis enables the characterization of different spectrum bands; while spectrum decision select the appropriate spectrum band for the current transmission considering the QoS requirements and the spectrum characteristics.

  The threats are normally called Spectrum Sensing Data Falsification (SSDF). Such attacks come from the possibility of false or fake spectrum characteristic parameters. The false or fake parameters impact the results of spectrum analysis and then impact the results of spectrum decision. So a CR may select the wrong band or the sub-optimal band, and the performance of communication may be impaired.

- *Spectrum mobility threats:*

  The function of spectrum mobility is to make sure seamless connection when a CR vacates a channel and moves to a better channel. In a CRN, the available spectrum bands depend on the factors such as time and place. One should vacate the current band if the band is not available for reasons such as: a PU is active, or one moves from one place to another. In order to maintain a smooth communication, the CR needs to select a new appropriate spectrum band and move to the new band immediately. The

process from a CR vacating the current spectrum band to the CR moving to a new available spectrum band is called spectrum handoff [8].

During spectrum handoff, the security threats could be serious as a failed handoff may need a long time to resume the communication. An attacker can induce a failed spectrum handoff through methods such as: compelling the CR vacating the current band by masking PUs; jamming to slower the process of selecting for a new available band or causing a communication failure.

For example, some CRNs use common control channel. Attackers can gain control of the common control channel to change the characteristic parameters of available band, or to interfere with the PUs. Then they can prevent the smooth transmission functionality of spectrum mobility. Thus, robust and simple algorithms for seamless connection of spectrum mobility are needed.

In this thesis, our focus is on PUE attack, which is a typical form of spectrum sensing security threat. A detailed introduction of PUE attack will be illustrated in the following section; we will also propose two different mitigating approaches in the next chapter in order to solve various security problems.

2.3 Primary User Emulation (PUE) Attack

2.3.1 Introduction to PUE Attacks in CRNs

PUE attack is a well-known malicious attack in CRN that is first introduced in [28]. PUE attack is unique to CRN, in which the attackers may modify their radio transmission frequency to mimic a primary signal, thereby misleading the legitimate SUs to erroneously identify the attacker as a PU. As a result, the attacker can obtain the full bands of a given spectrum without having to share them with other SUs. A successful PUE attack may force legitimate SUs to quit current channel and look for another available channel, or occupy the idle channels and waste the spectrum opportunities of the SUs.

2.3.2 Classification of PUE Attacks

In PUE attacks, attackers only transmit in fallow bands. Hence, the aim of the attackers is not to cause interference to PU, but to preempt spectrum resources that could have been used by legitimate SUs. Depending on the motivation behind the attack, PUE attacks can be classified as either selfish PUE attacks or malicious PUE attacks [28].

- *Selfish PUE attacks*: A selfish PUE attacker aims at stealing bandwidth from legitimate SUs for its own transmissions. The attacker will first monitor the spectrum. Once an unoccupied spectrum band is discovered, the attacker will compete with the legitimate SUs by emulating the primary signal. Normally selfish PUE attackers will only prevent legitimate SUs to enter a fallow band for attacker's own purpose. This attack can be carried out by multiple SUs, whose intention is to establish dedicated communication links, or can also be carried by a single SU that aims to solely use the fallow band.

- *Malicious PUE attacks*: The objective of malicious PUE attack is to obstruct the DSA process of legitimate SUs but not to exploit the spectrum for its own use. Unlike selfish PUE attacks, a malicious PUE attacker doesn't necessarily use fallow spectrum band for its own communication purpose. It is quite possible for an attacker to attack either an unoccupied spectrum band or a band currently used by legitimated SUs.

PUE attackers can also be categorized as power-fixed & power-adaptive attackers and static & mobile attackers depending on the ability to emulate the power levels of a primary signal and the location of attackers.

The ability to emulate the power levels of a primary signal is crucial for PUE attackers since most of the SUs employ an energy detection technique in spectrum sensing. A power-fixed attacker uses an invariable predefined power level regardless of the actual transmitting power of the PUs and the surrounding radio environment. Compared to the power fixed attacker, the power-adaptive attacker is smarter in the sense that, it could adjust its transmitting power according to the estimated transmitting power of the primary signal and the channel parameters [30]. Specifically, the attacker employs an estimation technique and a learning method against the detection by the legitimate SUs. It is demonstrated that such an advanced attack can defeat a naive defense approach that focuses only on the received signal power.

On the other hand, the location of a signal source is also a key characteristic to verify the identity of an attacker. A static attacker has a fixed location that would not change in all round of attacks. By using positioning techniques such as Time Difference of Arrival (TDOA) or dedicated positioning sensors [28], the location of a static attacker could be revealed. A static attacker will be easily recognized due to the difference between its location and that of the PUs. A mobile attacker will constantly change its location so that it is difficult to trace and discover. A viable detection approach that exploits the correlations between RF signals and acoustic information is proposed in [31] to verify the existence of a mobile PUE attacker.

In the thesis, we assume the PUE attackers are power-adaptive attackers that have the ability to reconfigure their transmitting power level. Moreover, the attackers are considered as mobile attackers that are capable of changing their locations.

2.3.3 Impact of PUE Attacks

Since the PUE attack aims to prevent SUs using the available spectrum band instead of interfering PUs, it could have disruptive effects to SUs in CRNs in most cases. However, it is still possible for a PUE attack to interfere with a PU, which may bring disastrous impact to the whole CRN. Below are some potential consequences of a PUE attack:

- *Bandwidth waste*: The objective of deploying CRNs is to address the under-utilization problem caused by current fixed spectrum usage policy. CRNs allow SUs to be able to find out and access "white spaces" of a spectrum dynamically without wasting spectrum resources. However, the PUE attacker may mislead SUs to believe a given spectrum is already taken and lead to spectrum bandwidth waste again.

- *Quality of Service (QoS) degradation*: With the presence of PUE attacks, a SU may be forced to leave current available spectrum band since it mistakenly believes the PU comes and switches to another available spectrum band. Such frequent spectrum handoff will induce unsatisfying delay and jitter for the secondary services [14].

- *Connection unreliability*: A secondary service will be forced to drop off if it is under PUE attack and couldn't find an available channel when performing a spectrum handoff. Therefore, the existence of PUE attacks in CRNs increases the unreliability of the connection and the quality of the service cannot be guaranteed.

- *Denial of Service*: In the worst case of PUE attacks, all idle spectrum bands are under attack and all SUs cannot find a spectrum opportunity to set up a channel for communication. As a consequence, the whole CRN will be suspended and unable to serve any SU. This is called Denial of Service (DoS) in CRNs.

- *Interference with the PU*: Although PUE attacks target stealing bandwidth from SUs only and will leave the spectrum band as soon as the PU arrives, it will still cause interference with PU if the attacker fails to detect the signal from PU correctly and decides to stay in the channel. On the other hand, as a SU, if it incorrectly identifies a PU as the attacker and refuses to leave the band, then the SU will interfere with the PU. In any case, interference with the PU is strictly forbidden in a CRN.

2.4 Chapter Summary

In this chapter we have elaborated on dynamic spectrum access, cognitive radio, spectrum sensing, cognitive radio networks, and potential security threats in CRNs. In the rest of the thesis we will focus on the PUE attack and propose a modified energy detection method, as well as two novel techniques to detect PUE attacks. In the next chapter, related research methods of detecting PUE attacks that will be utilized in our two proposed techniques are discussed. These include energy detection, localization, cyclostationary feature detection and artificial neural network.

3

Literature Review: PUE Attack Detection Techniques

As we have discussed in the previous chapter, in a PUE attack, a malicious SU tries to gain priority over other SUs by transmitting signals that emulate the characteristics of a primary signal. Due to the reconfigurability of CRs, it is possible for an adversary to modify the radio software of a CR to change its emission characteristics (such as modulation, frequency and power) so that the emission characteristics resemble those of a PU. The potential impact of the PUE attacks depends on the ability of legitimate SUs to distinguish the attacker's signal from actual primary signals while conducting spectrum sensing.

In this chapter, we discuss some traditional techniques for SUs to identify the signal from PUs that include energy detection, localization, cyclostationary feature detection and artificial neural network. We will use these techniques in the design of new methods of PUE attack detection in Chapter 4.

These techniques will also be utilized in Chapter 4 as PUE detections.

3.1 Energy Detection

We have discussed in section 2.1.2 that the energy detection technique infers the existence of a PU based on the measured signal energy level. It is clear that energy detection is unable to distinguish primary signals and secondary signals when the PUs' signal strength level is similar with that of SUs. An improved scheme proposed in [32] suggests the use of periodic "quiet periods". During a quiet period, all SUs refrain from transmitting to facilitate spectrum sensing. When quiet periods are observed by all SUs, detecting PUs becomes straightforward, any terminal which receives signal energy level that is beyond a given threshold can be considered as a primary transmitter. However, such a detection strategy breaks down completely when malicious SUs deliberately transmit during quiet

periods.

Other energy detection techniques have also been proposed using a predefined threshold [33][34]. These techniques are based on the fact that the signal energy level received on each SU is inversely proportional to the distance between the SU and the signal source. In other words, the detected energy level decreases while the detecting SU moves further from the signal source. Furthermore, above approaches assume the PUs' signal strength is much higher than that of the PUE attackers, which means the received signal energy levels are different even if the PU and the PUE attacker are at the same distance from a particular SU. Therefore, a SU can identify the transmitting signal as an attacker's signal as long as the received energy level is much lower or higher than a specific threshold. However, in most environment, it is observed that the radio signal strength falls as some power of the distance, called the power-distance gradient or path-loss gradient [35]. As a result, an attacker may deceive SUs by changing its transmitting location.

To solve such a major problem in energy detection, an improved energy detector with multiple thresholds is proposed in Chapter 4. Instead of detecting energy level using a single SU, detection from multiple SUs are utilized for generating a global result, which can significantly improve the accuracy of energy detection. The improved energy detection method is used in our proposed PUE attack detection schemes, which will also be described in Chapter 4.

3.2 Localization

3.2.1 Existing Localization Algorithms

Nowadays, locating the signal source in wireless networks has become a very important issue in a variety of applications such as habitat monitoring, environmental monitoring, health application and target tracking. In such applications, users or base stations must know the locations of the nodes once the data are received from them and hence the locations can be identified as soon as there is a status change.

The localization capability can be very helpful to the countermeasures of PUE attacks [34], especially in cases where the PUs' locations are fixed and already known to SUs. Our existing TV networks is a good example. All TV towers can be viewed as PUs and their locations are public information. Once a signal is detected by SUs, the position of the signal source will be estimated and compared with the list of known locations of PUs. The signal source can be identified as a PUE attacker if the estimated position doesn't match any of the existing PUs. Besides that, localization can also be used to pinpoint the attacker once the attack is detected. However, PUE detection may fail if the attacker is in the vicinity of one of the PUs. To resolve such problem, localization is normally combined with energy detection for PUE detection.

Up to now, most existing localization algorithms can be classified into two categories: range-based and range-free [22]. Range-based protocols [22][36][37] employ absolute point-to-point distance or angular information to identify the locations among neighboring nodes. The measurements used in range-based localization including Time of Arrival (TOA) [22][38][39] , Time Difference of Arrival (TDOA) [40][41], Angle of Arrival (AOA) and Received Signal

Strength (RSS) based schemes. On the other hand, range-free techniques only use connectivity information between unknown signal sources and landmarks with known locations. As the requirement doesn't allow any modification to be done on PUs in CRNs for the purpose of attacks detecting, rang-free localization is not applicable since we cannot include any location information in the connectivity information between PUs and SUs. Therefore, we will only focus on range-based localization algorithms and the algorithms will be elaborated below:

- *Time of Arrival (TOA)*: TOA uses the travel time from the transmitter to the receiver, or time-of-flight (TOF), to measure the distance between the two. In order to properly localize with TOA, there must be at least three reference nodes. When the distances from three different nodes are known, the location can be found at the intersection of the three circles created around each node with the radius being the distance calculated [42]. See Figure 3.1.

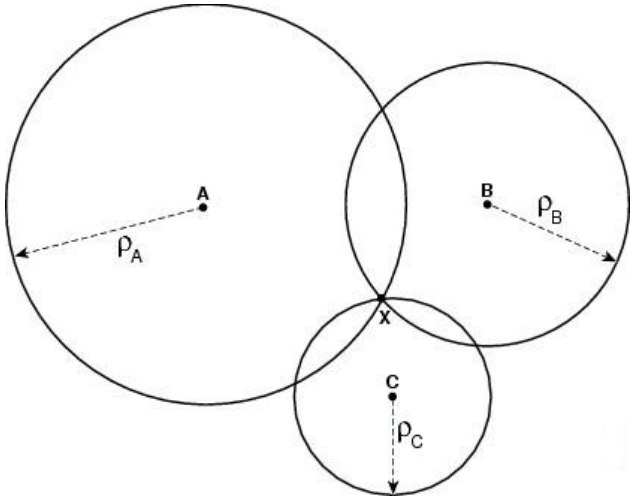

FIGURE 3.1: A TOA based localization.

  However, the accuracy of range estimation may be affected by noise and the multi-path components, thus the spheres will not always intersect at one single point. The goal of the location estimation is to find out the closest coordinates to the actual position.

- *Time Difference of Arrival (TDOA)*:

  Localization by time difference of arrival (TDOA) utilizes the differences between the arrival times of pulses transmitted by an emitter without any knowledge of pulse transmit times. Instead of using the travel time from each receiver to find the distance between the transmitter and receiver that used in TOA, the difference in travel times from each receiving node are used to find the distance between each receiver. The intersection of the result hyperbolas indicates the location of the transmitter [43]. See Figure 3.2. Therefore, TDOA does not require the use of a synchronized time source at the point of transmission (i.e. the unknown signal source) in order to resolve timestamps and determine location. With TDOA, a transmission with an unknown starting

time is received at various receiving nodes, with only the receivers requiring time synchronization. Several techniques for TDOA localization have been proposed in the literature [44][45][40].

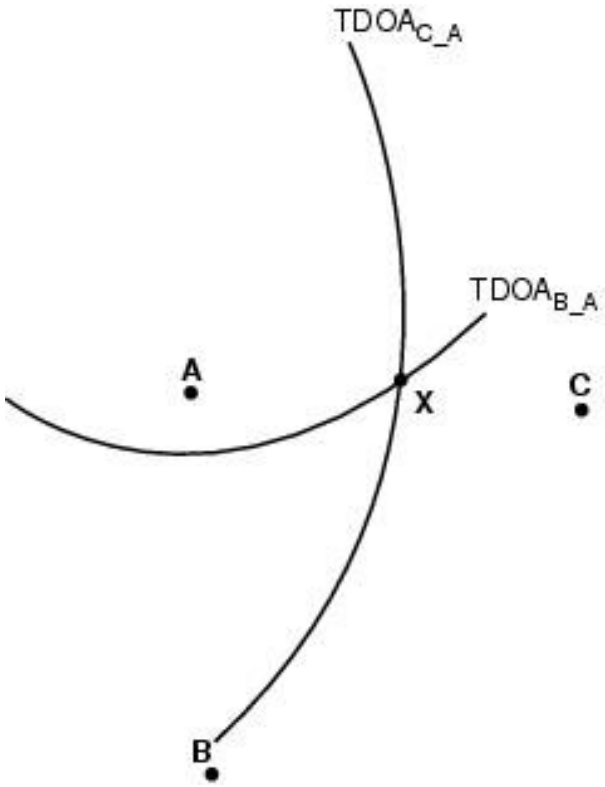

FIGURE 3.2: A TDOA based localization.

- *Angle of Arrival (AOA)* The Angle of Arrival (AOA) technique, sometimes referred to as Direction of Arrival (DOA), locates the signal source by determining the angle of incidence at which signals arrive at the receiving node.

  When an incident wave is propagated to a receiving node, it forms an angle with some reference direction, which is known as orientation. Orientation, defined as a fixed direction against which the AOAs are measured, is represented in degrees in a clockwise direction from the North. When the orientation is 0° or pointing to the North, the AOA is absolute, otherwise, relative [46]. Besides equipping an ominidirectional antenna array on receiving nodes or using several ultrasound receivers, other techniques to detect the angles between nodes have also been discussed in [47] and [48]. By using above methods, geometric relationships can then be used to estimate location from the intersection of two lines of bearing (LOBs) formed by a radial line to each receiving node. See Figure 3.3.

- *Received Signal Strength (RSS) based localization*

  Besides the localization algorithms mentioned above, unknown signal source can also be localized by received signal strength (RSS) in place of time. The basic idea of this

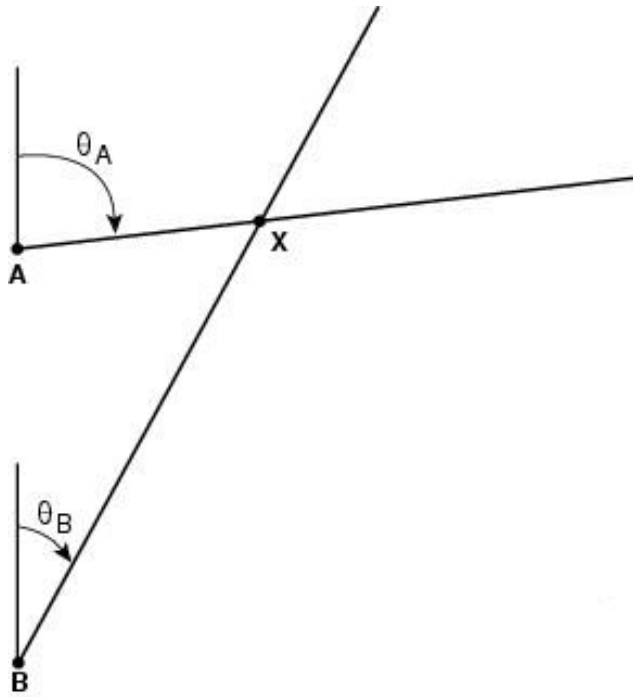

FIGURE 3.3: An AOA based localization.

approach uses the fact that the magnitude of an RSS value typically decreases as the distance between the signal transmitter and the receiver increases [49]. Therefore, if one is able to collect a sufficient number of RSS measurements from a group of receivers spread throughout a large network, the location with the peak RSS value is likely to be the location of a transmitter.

The requirement to collect RSS distribution in a network naturally leads us to resort to an underlying wireless sensor network (WSN) that can help collecting RSS measurements across the network. If sensor nodes in a WSN have the capability to measure RSS and are aware of their positions [49], they can be used to solve the localization problem.

In the next section, we will elaborate a detailed TDOA implementation as our localization scheme and a combination of TDOA with energy detection to identify PUE signals will be illustrated in Chapter 4.

3.2.2 Implementation of TDOA Localization Scheme

As discussed before, several localization schemes have been proposed in previous research such as TOA, TDOA, AOA and RSS based localization. TOA uses the travel time from the transmitter to the receiver and requires the transmitting signal includes the transmitting time. This approach violates the non-modification requirement and hence cannot be used in CRN. AOA requires localization devices to equip with ominidirectional antenna array

because it locates the signal source by determining the angle of incidence at which signals arrive at the receiving node. Such hardware cost may not be feasible in the system design. Moreover, AOA suffers from decreased accuracy and precision when confronted with signal reflections from surrounding objects since it only works well in situations with direct line of sight. RSS based localization does not require additional hardware expense, but it needs numerous location aware nodes to be widely distributed in the signal transmitting range, which may incur a big cost or management issues. SUs can be used as the sensing nodes when RSS localization is utilized but it can not be guaranteed that there are enough SUs in the network in a given moment for an accurate estimation. TDOA is suitable in CRN since it utilizes the difference between the arrival times of pulse transmitted by an emitter without any knowledge of pulse transmit times; it is a non-interactive localization scheme. Furthermore, it does not require base stations to equip with extra ominidirectional antenna array like AOA. Finally, the base stations update SUs who require such information as soon as the signal source is localized. Therefore, the system delay can be effectively reduced because the limited number of base stations and communication hops between base stations and SUs. The drawback of TDOA is that all the base stations have to be time synchronized for accurately detecting the time difference when a same signal pulse is received. This issue is not unsurmountable since GPS time synchronization techniques can be utilized to base stations, and the cost can be kept low and acceptable.

Therefore, a generic TDOA localization scheme can be used to detect PUE attacks when PUs are fixed and their locations are known such as a TV network we discussed previously. Besides above assumptions, we also assume there is a certain number base stations distribute throughout the network. These base stations are time synchronized and are capable of detecting the time difference while a signal is received. They can also exchange information with each other and SUs using a reliable communication channel. Moreover, each base station is equipped with a GPS unit and knows its own location. Finally, the base stations can be either fixed or mobile devices, or even some of these base stations can themselves be SUs in the CRN. The TDOA based location scheme can be illustrated as follow:

First we use Euclidean Distance to describe the distance between the signal source and base stations as below,

$$(x - x_i)^2 + (y - y_i)^2 + (z - z_i)^2 = m_i^2, (i = 1, 2, \ldots, n) \tag{3.1}$$

where (x_i, y_i, z_i) are the known coordinates of the base stations, $m_i (i = 1, 2, ..., n)$ are the range estimations between signal source and base stations respectively. n is the number of base stations. The coordinates of the signal source to be estimated are referred to as (x, y, z).

Then we assume all the TDOA is measured with respect to the first base station. Therefore,

$$m_{i,1} = r_i - r_1, (i = 2, 3, \ldots n) \tag{3.2}$$

where $m_{i,1} (i = 2, 3, \ldots n)$ are the TDOA range estimations. $r_i (i = 2, 3, \ldots n)$ are the unknown parameters of true distances between the reference nodes and the target node. n is the number of the reference nodes.

Combining (3.1) and (3.2) we can get following equations:

$$\begin{cases} (x-x_1)^2+(y-y_1)^2+(z-z_1)^2=r^2 \\ (x-x_2)^2+(y-y_2)^2+(z-z_2)^2=(r_1+m_{2,1})^2 \\ \dots \\ (x-x_n)^2+(y-y_n)^2+(z-z_n)^2=(r_1+m_{n,1})^2 \end{cases} \tag{3.3}$$

The minimum number of base stations is four because there are four unknowns x, y, z and r_1 in (3.3).

Let

$$x'=x-x_1, y'=y-y_1, z'=z-z_1 \tag{3.4}$$

and

$$x_i'=x_i-x_1 \qquad (i=2,3) \tag{3.5}$$

Substituting (3.4) and (3.5) into (3.3) and subtracting the first one ($i=1$) from it for $i=2,3,4$ results in an equation set in the matrix form as

$$\begin{bmatrix} x_2' & y_2' & z_2' \\ x_3' & y_3' & z_3' \\ x_4' & y_4' & z_4' \end{bmatrix} \begin{bmatrix} x' \\ y' \\ z' \\ r_1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} x_2'^2+y_2'^2+z_2'^2-m_{2,1}^2 \\ x_2'^2+y_2'^2+z_2'^2-m_{3,1}^2 \\ x_2'^2+y_2'^2+z_2'^2-m_{4,1}^2 \end{bmatrix} \tag{3.6}$$

where

$$r_1=x'^2+y'^2+z'^2 \tag{3.7}$$

We make one of the unknowns a parameter (such as r_1) and the other three as functions of this parameter. Putting them into (3.4), we get a quadratic equation in terms of r_1. The solution of the quadratic equation will lead to the solution of the coordinates of the signal source.

In the above discussion, we have neglected to discuss a very important aspect of TDOA's feasibility in our system model. If the temporal separation between two consecutive synchronization pulse (or symbols) is too small, the TDOA scheme may be infeasible. Suppose that the separation between pulses, represented by δ, is small enough for the relation ($t_\Delta \geq \delta/2$) to hold. In this case, it is almost impossible for two base stations to make sure that they are receiving the same pulse since the time instants during which the two base stations see the same pulse may be separated by more than the length of the time duration in which each of them observes a different pulse. The value t_Δ is determined by the distance difference between the signal source to two different base stations. Let s_1 and s_2 denote the two distances, they can form a triangle with the distance between two base stations, denoted by s_3. See Figure 3.4. Using the triangle inequality theorem, the distance difference s_3 is always less than $|s_1-s_2|$. In order for TDOA to be feasible, s_3 must be small enough so that the relation $|s_1-s_2| \leq \delta \cdot c/2$ is satisfied, where c is the speed of light. Hence, as long as the distance between the two base stations is small enough to satisfy $s_3 \leq \delta \cdot c/2$, TDOA

is feasible. For example, in an analog TV system, two consecutive synchronization pulse are separated by $64\mu s$ [50], which is equivalent to around 19,200m spatial separation. As long as the two base stations are less than 9,600m away from each other, TDOA is feasible. For a digital TV system, on the other hand, each symbol spans $224\mu s$, in which $7\mu s$ is a silent period for inter-symbol separation [50]. The minimum distance between a pair of base stations for utilizing TDOA successfully is around 1,050m.

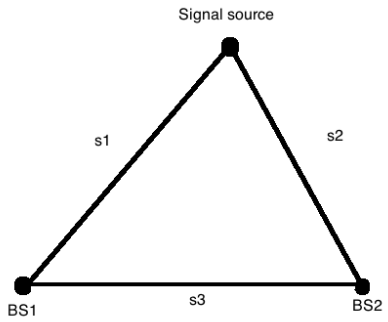

FIGURE 3.4: TDOA is only feasible if $s_3 < s_1 + s_2$.

Due to environment noise, the accuracy of TDOA localization can be affected, and hence the signal source cannot be precisely positioned. There are two different cases that will happen in the system model. First, the position of the signal source is not correctly estimated by some base stations. To overcome this problem, we can deploy different sets (each set should have at least four base stations in order to solve the system of equations successfully) of base stations to employ TDOA localization schemes. As long as the majority (more than half of the total utilized base stations sets) sets of base stations estimate the same result include a given error range, the result generated by them is taken to be the real position of the signal source. The other case is the position of a signal source cannot be estimated due to not sufficient number of base stations within the transmitting range, or the result cannot be estimated by majority of base station sets. In this case, the signal is assumed to be generated by an attacker since the base stations are supposed to be distributed within the PU's transmitting range and any single PU's location should be able to be estimated.

3.3 Cyclostationary Feature Detection

Modulated signals are generally coupled with sine wave carriers, thereby exhibiting periodicity in their signal structure. By definition, a signal $x(t)$ is wide-sense cyclostationary if its mean and autocorrelation are periodic:

$$M_x(t) = M_x(t + T_0), \tag{3.8}$$

$$R_x(t,\tau) = R_x(t+T_0,\tau), \tag{3.9}$$

where $M_x(t)$ is the mean value of the signal $x(t)$, and $R_x(t,\tau)$ is the autocorrelation function of the signal $x(t)$.

Cyclostationary feature detection utilizes the cyclic feature of a signal to detect it. For example, the spectral correlation function (SCF) and the spectral coherence function (SOF) can both be used to detect signal features [51][52][53].

The SCF represents the periodic nature of the signal and can be defined as:

$$S_X^{\alpha}(f) = \lim_{T\to\infty}\lim_{\Delta t\to\infty}\frac{1}{\Delta t}\int_{\Delta t/2}^{-\Delta t/2}\frac{1}{T}X_T(t,f+\frac{\alpha}{2})X_T(t,f-\frac{\alpha}{2})dt, \tag{3.10}$$

where $\{a\}$ is the set of Fourier components and $X_T(t,f)$ is the time varying Fourier transform defined as:

$$X_T(t,f) = \int_{t-T/2}^{t+T/2} x(u)e^{j2\pi fu}du. \tag{3.11}$$

A significant advantage of the SCF is its lack of sensitivity due to additive noise. Since the spectral components of white noise are uncorrelated, it does not contribute to the resulting SCF for any value of $\alpha \neq 0$; This is the case especially when the noise power exceeds the signal power, which would make the signal undetectable when using a simple energy detector. At $\alpha = 0$, where noise is observed, the SCF reduces into a Power Spectral Density (PSD) [54].

To derive a normalized version of the SCF, the SOF is given as:

$$C_X^{\alpha}(f) = \frac{S_X^{\alpha}(f)}{[S_X^0(f+\alpha/2)\times S_X^0(f-\alpha/2)]^{1/2}} \tag{3.12}$$

The SOF is seen to be a proper coherence value with a magnitude in the range of [0, 1] and it represents strength of second order periodicity within the signal. Moreover, the SOF contains the spectral features of interest and these features are non-zero frequency components of the signal at various cyclic frequencies. All modulation schemes contain a range of spectral components at different cyclic frequencies, thus distinguishing them from other modulation schemes. That is, the spectral components form a spectral fingerprint for the specific modulation scheme. An additional benefit of the SOF is its insensitivity to channel effects since the channel effects are removed when SOF is formed. As a result, the SOF is preserved as a reliable feature for identification even when considering propagation through multipath channels.

Based on above discussions, the advantage of the cyclostationary feature detection includes its ability to distinguish different signal types in a band and its robustness against stationary noise with unknown variance. The disadvantage of this technique lies in its computational complexity and long observation time.

3.4 Artificial Neural Network (ANN)

The human brain provides proof of the existence of massive neural networks that can succeed at cognitive, perceptual, and control tasks in which humans are successful. The brain is capable of computationally demanding perceptual acts (e.g. recognition of faces, speech) and control activities (e.g. body movements and body functions). The advantage of the brain is its effective use of massive parallelism, the highly parallel computing structure, and the imprecise information-processing capability.

Artificial neural networks (ANN) have been developed as generalizations of mathematical models of biological nervous systems. A first wave of interest in neural networks (also known as connectionist models or parallel distributed processing) emerged after the introduction of simplified neurons by McCulloch and Pitts (1943). Their paper outlined some concepts concerning how biological neurons could be expected to operate. The neuron models proposed were modeled by simple arrangements of hardware which attempted to mimic the performance of the single neural cell [55].

An ANN consists of some basic processing elements called *artificial neurons* or *nodes*, which are connected to each other. Each connection has a weight or strength value associated with it, and these values determine the state of the artificial neural network [56]. Moreover, an activation function of a node is needed, which defines the output of that node.

To set up an ANN, first of all a set of input and output nodes should be defined. Secondly an accurate set of data samples are employed for training the ANN. After that, to verify the accuracy of the ANN, the ANN needs to be tested against a new set of data samples.

From an architectural view, an ANN is normally made by three types of neuron layers: input, hidden, and output layers. The nodes in each layer are called input nodes, hidden nodes and output nodes respectively (See Figure 3.5). Such architecture is also referred as a multi-layer neural network and the activation of the hidden nodes (H_j) is calculated as follows:

$$H_j = f(\sum_{i=1}^{ni} w_{1ij} I_i) \tag{3.13}$$

where I_i is the activation of the ith input node, ni is the total number of input nodes, w_{1ij} is the weight number associated with the connection between hidden node i and the input node j, and f is a function that smooths the resultant activation and bounds it between -1 and 1. The function f can be assumed that $f(x) = \tanh(x)$

Once the activation of the hidden nodes have been calculated, the activation of the output nodes are calculated by:

$$O_j = f(\sum_{i=1}^{nh} w_{2ij} H_i) \tag{3.14}$$

where nh is the number of hidden nodes, and w_{2ij} is the weight factor associated with the connection between the ith hidden node and the jth output node.

The process of choosing the appropriate weight factors can be done by various methods. One way is to set the weights explicitly by a priori knowledge. Another way is to train the

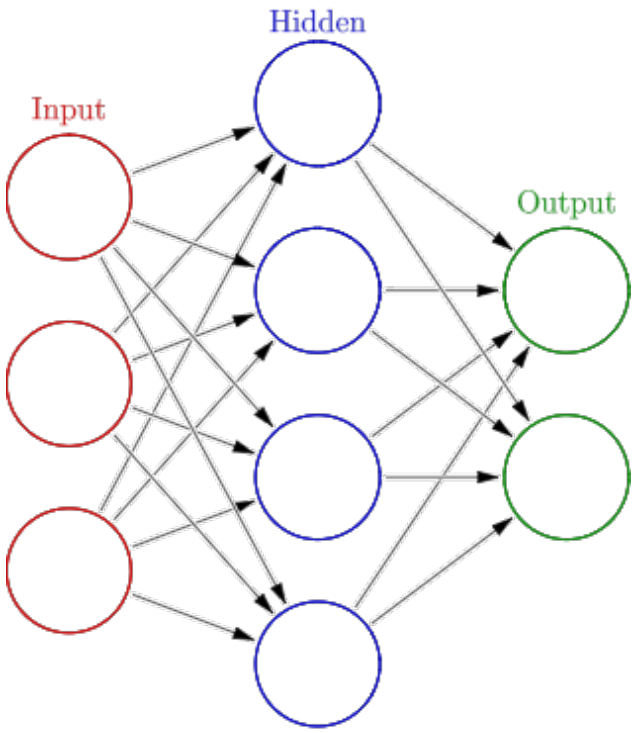

FIGURE 3.5: An architectural view of artificial neural network.

neural network by feeding it teaching patterns and letting it change its weights according to some learning rule. One of the best known training algorithms is the back propagation algorithm [57].

The main reason of utilizing ANN to classify real PU signals from PUE signals is because creating a linear algorithm for signals classification in real time is a difficult problem due to the unique features of each signal that need to be programmed in, and the ambient noise level that needs to be considered. However, this problem can be solved by using an artificial neural network approach due to the following facts: First, an ANN can simply be trained to recognize the unique features of the signal by giving it sample signal data, and specifying what signal type to associate with each set of data [56]. Second, ANNs have been shown to have a high noise tolerance if the data to be classified is not very similar [58]. Third, ANNs are adequate for real time applications, as long as the output activation is well defined.

3.5 Chapter Summary

In this chapter, we described four different research methods that are normally used in PUE detection: energy detection, localization, cyclostationary feature detection and artificial neural network. We also illustrated a detailed implementation of TODA localization scheme, as well as the calculation of SCF and SOF, and the architecture of artificial neural network. An improved energy detection method and PUE attack detection schemes that combine the

techniques mentioned in the chapter will be proposed in the next chapter.

4

Improved PUE Detection Schemes

In this chapter, first we propose an improved energy detection method. Then we propose two novel PUE detection schemes using a combination of our improved energy detection with localization and cyclostationary feature detection in artificial neural networks. These two schemes address different attacking scenarios and have different assumptions. We begin this chapter with a brief discussion on existing research in PUE attack detection.

4.1 Existing research in PUE detection

Currently, there are several techniques for the detection of PUE attacks in CRNs. LocDef (localization-based defense [28]) is a transmitter verification scheme, it is designed to verify whether an intercepted signal belongs to an incumbent licensed transmitter by estimating its location and observing its signal characteristics. More recently, [59] proposed an approach that integrates cryptographic signatures and wireless link signatures to enable PUE detection. Another paper [60] analyzes the PUE attack problem within a Bayesian game framework, in which users are unsure of the legitimacy of the claimed types of other users. The authors show that depending on the beliefs about the fraction of PUs in the system, a policy maker can control the occurrence of emulation attacks by adjusting the gains and costs associated with performing or checking for emulation attacks. In [61], the authors proposed a method that allows PUs to add a cryptographic link signature to its signal so the spectrum usage by PUs can be authenticated. Moreover, [33] proposed a belief propagation based model to detect PUE attack. However, the system model is preliminary and the compatibility function is considered only as a constant.

Given the published solutions currently available in the open literature, there still exist several technical challenges associated with enabling detection of PUE attacks in CRNs. These include:

- Simple energy detection-based schemes possess significant probabilities of missed detection and false alarm.
- Localization-based detection can only verify if the signal source's location matches with the PUs and cannot estimate the actual position.
- Cryptographic signature and wireless link signature detection requires an additional helper node. Specifically, this approach can only be employed when the helper node is physically close to a PU.

In this thesis, we propose two PUE detection schemes that combine energy detection with localization and cyclostationary feature calculation in artificial neural networks, which resolve above problems by increasing the accuracy of energy detection and estimating the actual location of signal source. Unlike the previous studies in this area, our proposed schemes address two different type of scenarios: stationary PUs and mobile PUs. The benefits of our approach include the following: (i) robustness in the presence of noise and fast processing; (ii) a significant improvement in accuracy of energy detection by using multi-thresholds and distributed results collecting. (iii) can identify PUE attacks while the PUs are either stationary (with known coordinates) or the PUs are mobile (have unknown coordinates).

The rest of the chapter is organized as follows. In Section 4.2, we propose and elaborate a revised energy detection. In Section 4.3, we present a combination of our improved energy detection and TDOA localization to detect PUE attacks with the assumption that PUs are fixed and their coordinates are known to SUs. In Section 4.4, we propose a PUE detection scheme that combines energy detection with cyclostationary feature detection. This scheme is designed for mobile PUs with unknown coordinates.

4.2 Improved Energy Detection Scheme

In our system model, we assume all users, including PUs, SUs, PUE attackers and base stations are distributed in a certain transmitting range. In order to avoid interference, we also assume there is only one PU or a PUE attacker is transmitting in the network at a given point in time. Furthermore, while the PU or the PUE attacker is transmitting, the transmitted signal power is much higher than that of any SU or the environmental noise level in the system.

Let $x(t)$, $h(t)$ and $n(t)$ denote the transmitted signal, channel impulse response and the thermal noise of the channel between the transmitted signal and the receiver respectively. Moreover, let $s(t)$ and $s'(t)$ denote a real PU signal and a PUE attacker's signal. Then the transmitted signal $x(t) = s(t)$ for the real PU signal, $x(t) = s'(t)$ for the signal from the PUE attacker and $x(t) = 0$ when only SUs are transmitting or there is no signal in the channel. The three possible received signals can be described as follow:

$$y(t) = \begin{cases} n(t) & \text{SU or none} \\ h(t) * s(t) + n(t) & \text{PU} \\ h(t) * s'(t) + n(t) & \text{PUE} \end{cases}$$

where $y(t)$ is the received signal at the SU that is acting as the PUE detector. Our improved energy detecting algorithm will differentiate these three cases by using the energy value received on each SU with multiple thresholds, which is different from conventional energy detection that uses only one threshold.

First, for each time interval, all SUs involved in energy detection scan the frequency channel. Let n_s denote the number of samples received by a SU i in one sensing period. After sampling, squaring and aggregation, the signal pre-processing unit generates the sampled energy vector $e = e[n](n = 1, 2, \cdots, n_s)$ and the aggregated energy value E, which $E = \sum_1^{n_s} e[n]$. After that, the aggregated energy E is sent to our energy detector for a comparison to a predefined threshold θ_0. If E is less than θ_0, it indicates there is no signal or there are only SU signals present in the channel, which is the situation that $x(t) = 0$. Otherwise, we set up two new thresholds, denoted by θ_1 and θ_2. Here, $\theta_0 < \theta_1 < \theta_2$. The two new thresholds θ_1 and θ_2 are used to distinguish the signal from a PU or a PUE attacker. If the input $\theta_0 < E < \theta_1$ or $E > \theta_2$, it is decided that a PUE attack is detected. If the input $\theta_1 < E < \theta_2$, the transmitted signal is diagnosed to be a PU signal. After comparing with predefined thresholds locally, local decision on each SU will be sent to a base station and compared with the aggregated result from other SUs. Assuming there are M SUs and the local decision for each SU is 1 if it decides a PU's signal is present and 0 otherwise. Denoting D_i as the every local decision and D_M as the aggregated results observed by M SUs, $D_M = \sum_1^M D_i$. For an unknown signal, the global decision can be described as:

$$r_{global} = \begin{cases} 1 & D_M >= \frac{M}{2} \\ 0 & D_M < \frac{M}{2} \end{cases}$$

where r_{global} is the global result concluded by all SUs.

In a conventional energy detection, there is only one threshold to distinguish the presence or absence of a primary signal. However, a PUE signal tries to emulate the transmitting power of a real PU and hence this single threshold detector is not efficient for detecting a PUE attack signal. Our proposed multi-threshold detector provides a capability and a higher probability to distinguish whether the signal is from PU or PUE. Furthermore, introducing local decision and global decision is based on the following principle. It is difficult for the attacker to fabricate a signal so that all of the SUs receive the signal with the power level similar to that of the real PU. In other words, if the majority of the SUs decide the signal is from a potential PUE attacker, then the global decision that the PUE attacker is present will be made. Therefore, by randomly assigning (M) SUs to measure the received signal power, letting these SUs know the signal power of the real PUs and exchanging the local decisions made by them for generating a global decision, a PUE attack can be identified with a high probability

Generally, for each SU, the received energy E has the form of a Chi-Square distribution. Since the number of samples is large in most cases, we can use the Central Limit Theorem (CLT) to approximate the Chi-Square distribution by a Gaussian distribution. Let H_0,H_1 and H_1' denote the hypothesis of receiving no signal, a real PU signal and a PUE attack signal, respectively. Let $P_d(\theta_1, \theta_2)$ and $P_f(\theta_1, \theta_2)$ denote the PUE attack detection and false alarm probabilities, respectively. We have $P_d(\theta_1, \theta_2) = P\{\theta_0 < E < \theta_1)|H_1'\} + P\{E > \theta_2|H_1'\}$, and $P_f(\theta_1, \theta_2) = P\{\theta_0 < E < \theta_1)|H_1\} + P\{E > \theta_2|H_1\}$.

A typical improved energy detector can be shown in Figure 4.1. Each SU has an energy detection unit that contains a signal pre-processing unit and followed by an energy comparator. After the signal has been sampled, squared and aggregated, the energy level is compared with three thresholds. Then a local decision is generated and is ready to be sent to its nearest base station for receiving a global decision.

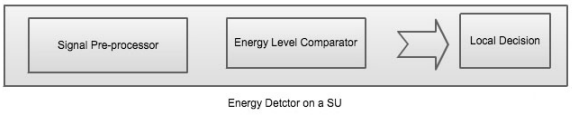

FIGURE 4.1: An energy detector on a SU.

In practice, the three thresholds can be set based on the signal propagation model, geographical environment and environmental noise level. The threshold values may be various for energy detectors in different locations.

Though our modified energy detection scheme significantly improves the possibility of successful PUE detection, attackers can still deceive SUs due to the reconfiguration ability of CR, either by changing their transmitting signal strength or transmitting location. Therefore, in order to provide a further enhancement to the success rate. We combine the improved energy detection scheme with localization or cyclostationary feature detection. This results in two novel PUE detection techniques that will be discussed in the following sections.

In reality, it is possible that base stations do not exist in some CRNs. Such cases will be discussed in future research and in this thesis, we assume base stations are required in the system.

4.3 Proposed PUE Detection Scheme 1: Combined Energy Detection and Localization

As we have discussed previously, besides energy detection, locating the signal source is another way to identify the PUE attacks in CRN, especially when PUs are fixed and their geographic information is already known to SUs. A classical example is the TV networks. The PU is assumed to be a network composed of TV signal transmitters (i.e. TV broadcast towers). A TV tower's transmitter output power typically has hundreds of thousands of Watts [62], which corresponds to a transmission range from several kilometers to tens of kilometers. SUs are hand-held devices that have CR capabilities and are located in the PUs' transmission range. Each SU is assumed to have a maximum transmission output power that is within the range from a few hundred milliwatts to a few watts, which typically corresponds to a transmission range of a few hundred meters. A PUE attacker can be either a mobile or a fixed device equipped with a CR and is capable of changing its modulation mode, frequency and transmission output power. However, the attackers' signal strength is several orders of magnitude smaller than that of a typical TV tower and the difference cannot be emulated by changing the output power of attackers. Furthermore, we assume the transmitted signal

power is much higher than that of the SU or the environmental noise level in the system while PU or PUE attacker is transmitting and there is only one PU or PUE attacker is transmitting in the network at any given time. Such a CRN can be displayed in Figure 4.2.

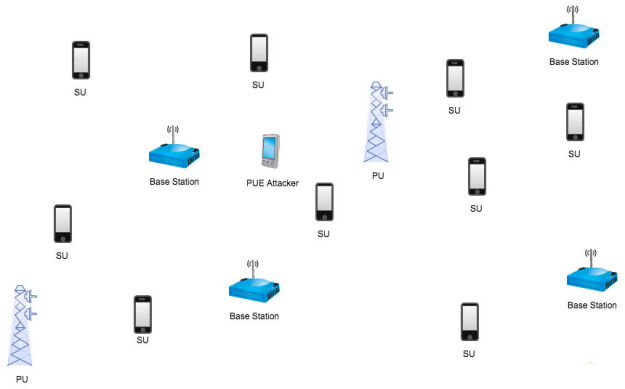

FIGURE 4.2: A CRN with fixed PUs and a mobile PUE attacker.

Based on the above assumptions, while the attacker is transmitting in the network at a given time, its location can be estimated by a set of SUs (or base stations in our case) distributed within the transmitting range. If the signal's estimated location deviates from the known location of the PUs and the signal characteristics resemble those of PU signal, then it is likely that the signal source is launching a PUE attack. It is quite possible that the signal's location cannot be estimated since the number of base stations is limited in the signal's transmitting range. In this case, the signal source should be identified as an attacker because base stations are supposed to be distributed so that at least one PU can be successfully positioned.

However, an attacker can attempt to circumvent this location based detection by transmitting the signal in the vicinity of one of the PUs. To address this problem, a combination of energy detection and localization can be utilized for detecting PUE attackers. It would be infeasible for an attacker to mimic both the PU signal's transmission location and energy level since the attacker's transmission power is several orders of magnitude smaller than that of a PU. Another advantage of using localization is that once a PUE attack is identified, the estimated location can be further used to pinpoint the attacker.

Different from conventional localization schemes in a wireless network, localization in CRN is more challenging as *no modification should be made to PUs to accommodate the DSA of licensed spectrum*. Because of this requirement, the PU signal cannot be expected to include location information. Moreover, using a localization protocol that involves the interaction between a PU and localization devices is also not a viable solution. Therefore, localization in CRN is a non-interactive localization [34]. No PUs are allowed to be modified and only base stations can be used to localize the signal source.

Based on our discussions about the improved energy detection in Section 4.2 and TDOA localization schemes in Section 3.2.2. We have developed a new PUE attack detection scheme. Our complete scheme for detecting PUE attacks in CRN with fixed PUs can be described as follows See Figure 4.4:

While an incoming signal is detected, all SUs in its transmitting range first perform measurements to calculate the energy level in a certain period. The calculated result E of each SU is then sent to its energy detector for comparison with three threshold values θ_1, θ_2 and θ_3, which are predefined based on PUs' signal strength, transmitting range, propagation model and noise in the environment. If $E < \theta_1$ or $E > \theta_2$, we believe the signal is from an PUE attacker and makes a local decision $D_{local} = 0$. Otherwise, the SU identifies the signal as a PU if $\theta_1 \leq E \leq \theta 2$ and makes a local decision $D_{local} = 1$. After local decisions have been made by all SUs in the transmission range, SUs will submit their local decisions (0 or 1) to their nearest base station for a data fusion. Assume there are M SUs in the transmitting range. As long as the majority of SUs (more than $M/2$) identifies the signal is from a PUE attacker, the global decision will be made as $D_{global} = 0$. Then all the SUs are updated and the signal source is identified as a PUE attacker, and the system will terminate. Otherwise, a global decision is made as $D_{global} = 1$ and all the SUs are updated by the base stations. Then SUs will send requests to their nearest base station for a further localization result.

In the localization step, base stations in the signal transmission range are assumed to be time synchronized. The base stations attempt to locate the signal source while a signal is detected in the channel. Base stations only locate the signal if its strength is above a certain level in the channel so that environmental noise and SUs' signal will be ignored. Based on our assumption that there is only one PU or one PUE attacker transmitting in the channel at a given time, it is guaranteed that the signal is either from a PU or a PUE attacker.

TDOA will be utilized by base stations to perform a localization and a position may or may not be estimated. If the signal source cannot be localized, the signal will be identified as an attacker and then the system terminates. Otherwise, the system queries its database with the estimated location in an error range. If it matches any of the existing known PU's location, the signal is identified as coming from a real PU. Otherwise, the system makes the decision that the signal is from an attacker.

After a localization based decision has been made by the base stations, the decision will be sent back to SUs and the system generates a final result as to whether the signal is from a real PU or a PUE attacker. Figure 4.4 provides a flow diagram of the proposed PUE detection scheme with a combined energy detection and TDOA localization technique.

4.4 Proposed PUE Detection Scheme 2: Combined Energy Detection and Cyclostationary Feature Detection in Artificial Neural Networks

In the previous scheme, we proposed a combination of energy detection and localization approach to detect PUE attacks in CRNs. This approach has certain intrinsic limitations and can only successfully identify the PUE signals while the PUs are fixed, and their locations are known to SUs or base stations. Furthermore, the signal strength of PUs is several orders of magnitude bigger than the PUE signal. To overcome such limitations, we propose another scheme that combines energy detection with cyclostationary feature classification by employing artificial neural networks (ANNs).

Unlike the first proposed PUE detection, PUs do not have to be fixed and their locations

are not necessarily to be known to SUs (See Figure 4.3). Furthermore, even the signal strength of PUs' can be at the same level as attackers. However, we assume the signal of PUE attackers have different cyclic features or modulation types.

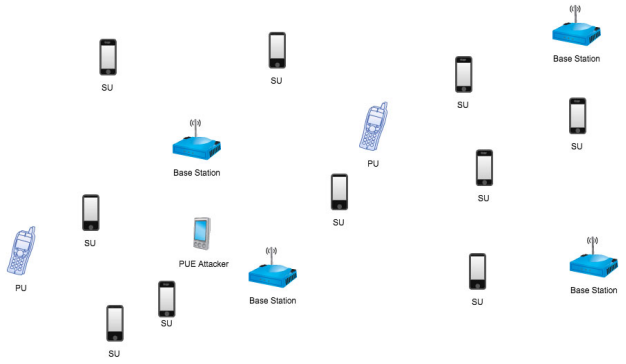

FIGURE 4.3: A CRN with mobile PUs and a mobile PUE attacker.

As in the previous scheme, this scheme also employs an energy detector with multiple thresholds. After a global decision has been made by all SUs that participate in energy detection, the system uses a cyclostationary feature classification step if the global decision of energy detection is 1.

In cyclostationary feature classification step, the cyclostationary feature of the incoming signal is calculated first, and then fed into ANNs for a further classification. See Figure 4.5

To actually use an ANN to classify a signal, the following steps need to be taken: First, the signal must be clearly intercepted. Then, signal statistics need to be computed. In our case, to classify a real PU signal from a PUE signal, the cyclostationary feature of the incoming signal, the SOF defined in Equation 3.12 is used. Next, this data is fed into a system of ANNs, each of which is trained to identify a given signal. In the end, the network with the largest output activation is found, and the identity of the signal is known.

Additionally, a reliability parameter [63] can be used to detect whether the ANN has failed. This parameter is defined as half of the difference between the largest and second largest output activations:

$$\chi = \frac{O_{Largest} - O_{2ndLargest}}{2} \tag{4.1}$$

where $O_{Largest}$ is the value of the largest output activation, and $O_{2ndLargest}$ is the value of the second largest output activation. Therefore, if one ANN has an activation of 1, which implies a perfect match, and all the others have an activation of -1, which implies that there is no match, then the reliability is 1. On the other hand, if two of the ANNs have an activation of 1, then the reliability would be 0. If the reliability is close to 0, then there is a good chance that the ANN has incorrectly classified the signal, and the classification should be disregarded. By discarding suspect classifications, the percentage of correct classifications can be improved.

The classification can be either done by the SU itself or through a base station in the SU's transmission range. If it is done by a single SU, the result can be exchanged with

other SUs in it's transmission range for generating a global decision. Similar to the energy detection step, a global decision can be made while the majority of the SUs make the same local decision. If the ANNs are deployed in base stations, the result will be simply returned to SUs which have requested for this information. Figure 4.5 provides a flow diagram of the proposed PUE detection algorithm with combined energy detection and cyclostationary feature classification.

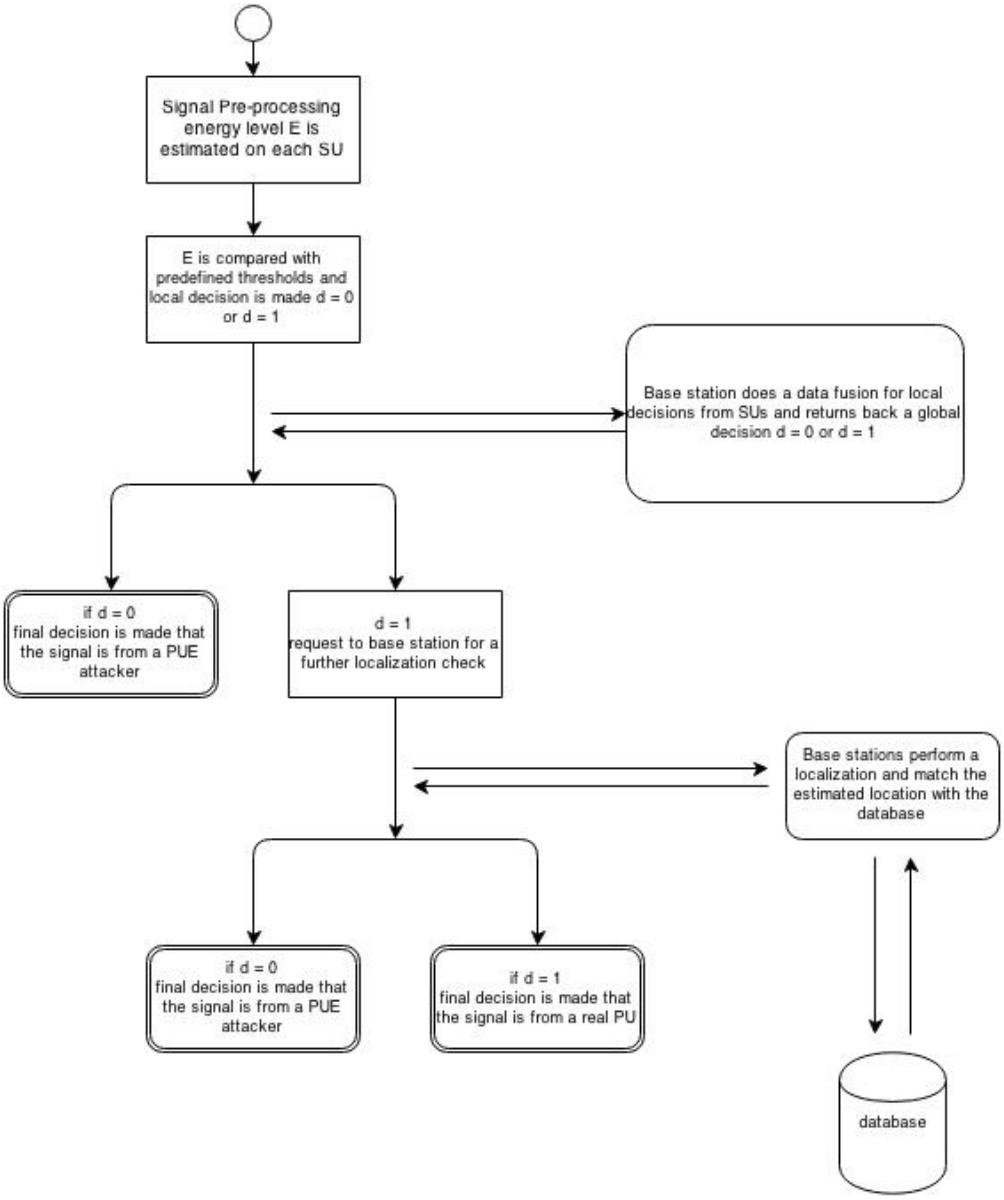

FIGURE 4.4: A combination of energy detection and TDOA localization.

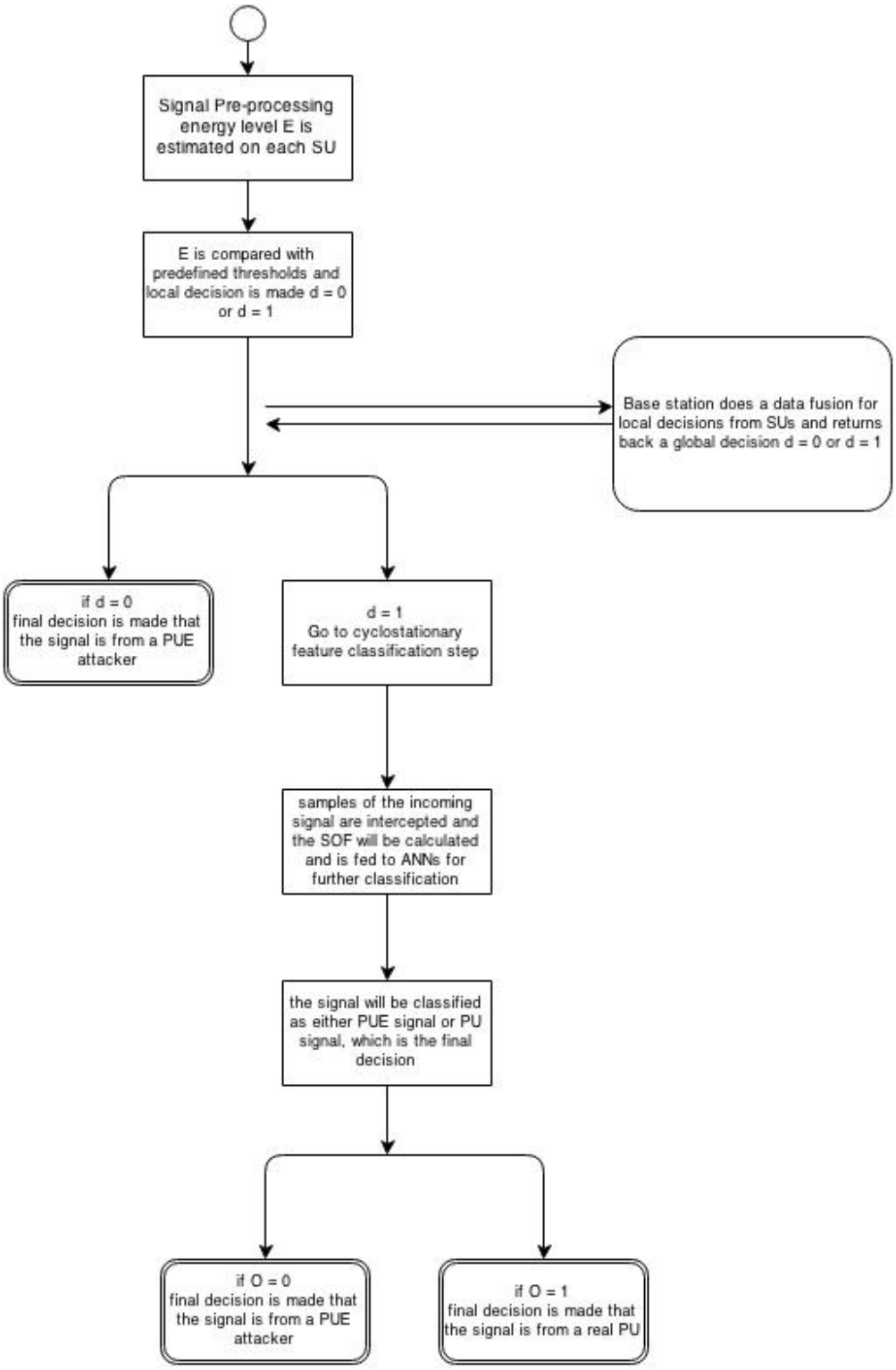

FIGURE 4.5: A combination of energy detection and cyclostationary feature classification in artificial neural networks.

4.5 Simulation

As discussed in Section 4.2, a global decision of the improved energy detection is made by all the local decisions from SUs participated in the detection process. In other words, the global decision in the energy detection is based on the local decisions from the majority of participated SUs. Ideally, the accuracy of the energy detection will be improved if more SUs are involved.

In the simulation, we first set a probability randomly for the energy detector with each SU, which means that each SU has a random possibility to fail its own energy detection and create an inaccurate local decision. Then we arrange 5 SUs in the simulation at the beginning and increase 3 SUs for each step. For the purpose of creating a reliable simulating result, for each step, we iterate the decision making process 100 times and use the average value as the probability of making an accurate decision. After 100 steps, the total numbers of SUs reaches to 305, and the success detecting rate ranges from around 51% to 98%.

Figure 4.6 displays a nice curve of the improved energy detection scheme. This clearly indicates that the accuracy of global decision increases with the increment of number of SUs involved in decision making. Furthermore, the lower curve in the figure represents the traditional energy detection. Since the traditional energy detection uses a single threshold and runs on a single SU, its detection probability is irrelevant to the number of SUs in the CRN. From Figure 4.6, we can see that the detection results are randomly distributed along the lower curve due to the random probability set in each SU and the overall detecting accuracy of our improved scheme is significantly improved compared to the tradition energy detection scheme while more and more SUs are involved.

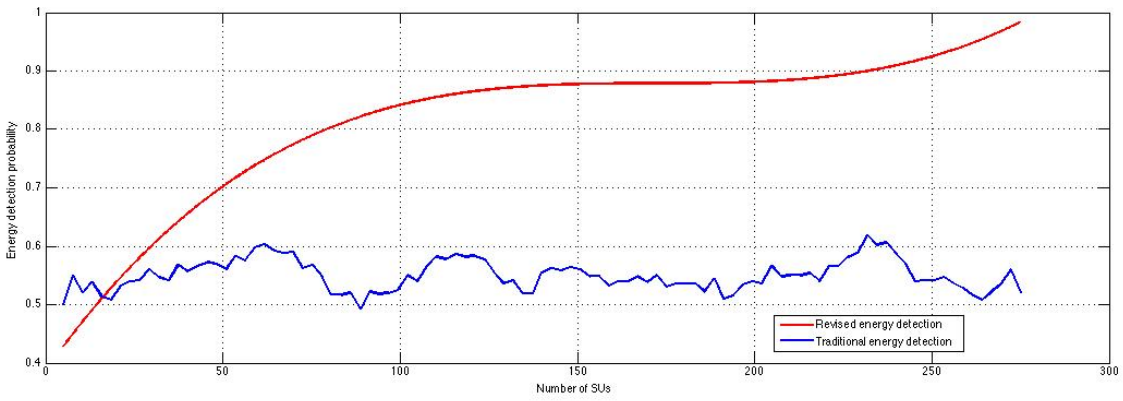

FIGURE 4.6: Simulation results of improved energy detection: more involved SUs lead to better accuracy.

Besides the simulation of our improved energy detection scheme, we have carried out another simulation for the TDOA localization scheme. As we have discussed in Section 3.2.2, TDOA localization requires at least four base stations for estimating the position of a signal source. The basic assumption for the trilateral positioning method in Equation 3.3 is that the measurement distances from anchors to the unknown sensor do not have errors.

However, this assumption is almost impossible in practice. When the Equations 3.4 are ill-conditioned, even small measurement errors result in a large amplified error of the estimated position of the unknown sensors. In the simulation, we considered the measurement errors caused by environmental noise and propagating errors, and estimated the effects they bring to the overall accuracy of TDOA localization algorithm.

We used geometric distance measurement error (GDME) in our simulation to measure the localization accuracy [64]. The GDME is defined as follows:

$$GDME = max \left\{ \frac{|d_i - \hat{d}_i|}{d_i}, i = 1 : N \right\} \tag{4.2}$$

where d_i is the measurement distance between the signal source and the ith base station around this transmitter, $\hat{d}_i$ is their distance computed according to the estimated coordinate of the signal source and the coordinate of the ith base station by Euclidean distance formula.

The simulation model is generated as follows. There are 10 points randomly generated in a 10km by 10km square area. Then, we randomly pick one point as the signal source (p_0) and use the other points as the base stations (p_i) and compute their Euclidean distances d_i. Moreover, we add a multiplicative random noise to every given distance as the measurement distance [64]:

$$\hat{d}_i = d_i(1 + nf * randn(1)) \tag{4.3}$$

where nf is a given noise factor and $randn(1)$ is a standard Gaussian random variable function.

In practice, there is always a measurement error due to noise, which has been randomly set in our simulation. We have used error tolerance thresholds to avoid this problem. A bigger error tolerance always leads to a bigger localization probability. In the two extreme cases of error tolerance 0 or infinity, the localization probability should be zero or 1 respectively.

In the simulation, we used the error tolerance and the successful localization probability to evaluate the performance of an algorithm. At the beginning, we set the error tolerance to be 0 and then increase it by 10 meter for each iteration. The error tolerance is more than 10 km after $1,000$ steps, which is even bigger than the total area size, and hence the localization probability converges towards 100%.

From Figure 4.7, we find that the successful localization probability of the algorithm goes to 100% as the error tolerance is increased, which proves our assumption.

We repeat the process 100 times for generating an average result, which is only for the research purpose and not practical in reality. In real life environment simulation, we can randomly choose a set of base stations multiple times and get the average detecting results from them for the simulation result.

4.6 Chapter Summary

In this chapter, we have discussed existing research in PUE detection, and have proposed two new schemes for identifying PUE attackers by using our improved energy detection scheme. For the situation where the PUs are fixed and their coordinates are already known

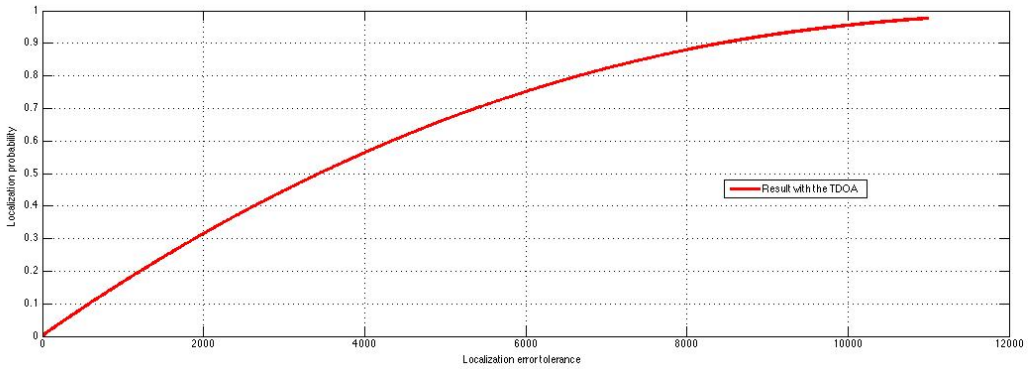

FIGURE 4.7: Localization probability with an increasing error range.

to SUs, we have combined the energy detection with TDOA localization. On the other hand, for mobile PUs with unknown positions, energy detection is combined with cyclostationary feature detection in artificial neural networks for a signal classification. In the next chapter, we discuss the potential problems with these two proposed schemes and followed by potential future work.

5 Conclusion and Future Work

The CR technology promises to alleviate the spectrum shortage problem and bring about remarkable improvements in the efficiency of spectrum utilization. Although the operational aspects of CRs and CRNs have attracted a significant research interest, research on their security aspects has been very limited. In this thesis, we have addressed security issues that pose serious threats to CRNs. We have focused on PUE attacks and explored possible countermeasures against these security threats. This research has provided us with a deep understanding of the PUE attacks in CRNs. We have proposed two new schemes which we believe could be useful in practice to achieve an improved PUE attack detection in CRNs. In this chapter, we summarize the research work and highlight our major contributions. We also discuss future directions to extend the current work.

5.1 Research Summary

This thesis has discussed PUE attacks, which can be classified as a spectrum sensing attack. In a PUE attack, a malicious secondary tries to gain priority over other SUs by transmitting signals that emulates the characteristics of a PU's. PUE attacks could wreak havoc to the normal operation in CRNs.

To countermeasure PUE attacks, the thesis has presented two new schemes and we have discussed these schemes in Chapter 4. One scheme is a combination of energy detection and localization; and the other scheme is a combination of energy detection and cyclostationary feature detection in artificial neural networks. One of the distinguish features of the proposed schemes is that instead of detecting received energy level with a single threshold on a single SU, multiple thresholds have been used on each SU and the global decision is concluded by the majority of participating SUs, such an approach increases the level of accuracy in detecting attacks. The simulation results have shown that with increased number of SUs involved in our improved energy detection, the accuracy rate in detection has also increased.

Furthermore, in cases where PUs are stationary and their coordinates are already known to SUs, we have combined our improved energy detection with a TDOA localization scheme for detecting PUE attacks. In cases where PUs are mobile and their coordinates are unknown to SUs, we have combined the improved energy detection with cyclostationary feature calculation and used the calculating results in artificial neural networks in order to classify the transmitting signal. Simulation results showed that the proposed scheme has been effective and robust against a number of attacks.

This research on PUE attacks and their countermeasures shows a promising approach to address security issues in CRs and CRNs. While a large scale deployment of CRs and CRNs still face many difficulties, it is worthwhile to examine carefully the PUE attacks as early as possible. By doing so, we can minimize the possible risks induced by insecure network implementation and minimize the costs involved in the applications of security measures. For these reasons, we believe that this research has a practical significance in the design and deployment of real-world CR systems in the future.

5.2 Future Work

Since this thesis has represented the preliminary correspond to the first year of PhD, the research is far from complete. In fact, the schemes proposed in this research could open up new areas in security in CR and CRNs.

As far as the attacks and countermeasures discussed in the thesis are concerned, further issues still remain. For example, our two proposed PUE detections are designed to address the cases that PUs are either stationary or mobile. In the first case where PUs are fixed, we have assumed that the transmitting signal power of PUs is much higher than SUs or PUE attackers. TV networks is one such an example. However, in practice, some PUs may not have very powerful signal strength and hence the PUE attackers are able to mimic a PU's signal strength at the vicinity of the PU. Such a situation will make the proposed scheme inefficient. For the second case that uses cyclostationary feature detection, we have assumed the cyclic features of PUs' signal are different from the attackers'. However, if the attackers use the exact same signal feature, for example, a recorded signal fragment from the PU, our PUE detection will make a false decision. To resolve such problems, we believe it is worth investigating a method based on action recognition [65]. Action recognition is widely used in computer vision and gaming industries for identifying action changes of the same identity. As discussed previously in Section 2.3.2, in a PUE attack, selfish attackers aim to steal bandwidth from legitimate SUs for its own transmissions. This means the attackers may not transmit the recorded signal from PUs ever. As soon as the selfish attacker gains the fallow band, it will change the recorded signal from PUs to its own communication. Therefore, action recognition can be potentially utilized to identify such an action change by the attacker. However, this method is infeasible against malicious PUE attackers who just want to obstruct the DSA process of legitimate SUs but not to exploit the spectrum for their own use. Therefore, it is quite possible that malicious PUE attackers will keep transmitting recorded signals from PUs, which can lead to false detection results.

Furthermore, sufficient signal samples of PUs' signal are essential for a successful cyclostationary feature calculation employing artificial neural networks for a signal classification.

This implies that an insufficient pre-knowledge of PUs in PUE detector may lead to an inaccurate result.

Therefore, it is necessary to investigate alternative approaches that can utilize the intrinsic characteristics of radio frequency signals to distinguish and identify emitters, e.g. radio fingerprinting, to detect PUE attacks. Radio fingerprinting is a process that identifies a cellular phone or any other radio transmitter by the unique "fingerprint" that characterizes its signal transmission [66][67]. An electronic fingerprint makes it possible to identify a wireless device by its unique radio transmission characteristics even if they are manufactured by the same assembly line. It is clear that radio fingerprinting would have the advantage of being able to verify a mobile, low-power PU, as well as identifying malicious attackers that keep transmitting recorded signals from PUs.

Finally there are the issues related to implementations. As of now, we have only carried out basic simulations (note it is the first year in PhD). In practice, the environmental noise and the propagation model of the signal can have a big influence on both energy detection and localization. We need to address these practical issues during implementation. For instance, an attacker may hack the base stations and modify the global energy detection decision and send it back to all SUs, which poses a certain operational challenges to our proposed implementation. To successfully deploy a CRN in practice, such operational issues need to be considered.

Moreover, in the proposed systems, both two schemes are performed sequentially. It is possible to combine them in some ways to make the system works more efficiently, which will be studied in future research.

Finally, the simulation in the thesis only includes the refined energy detection and TDOA localization separately. In the future Phd research, simulation about cyclostationary feature detection and a combined simulation for two different schemes will be carried out and compared to each other.

5.3 Conclusion

This thesis has investigated security issues in CR, CRNs and spectrum sensing. We have focused on the PUE attack security problem in CRNs. We have presented a comprehensive introduction to PUE attacks and discussed several technical challenges including classification of PUE attackers, and impacts of PUE attacks in CRNs. We have proposed an improved energy detection method by using multiple thresholds and making a global decision where the majority of SUs agree on the detection process. In addition, we have introduced the implementations of TDOA localization scheme, cyclostationary feature calculation and artificial neural networks. Then we have proposed new schemes involving combination of energy detection with TDOA localization and cyclostationary feature calculation in artificial neural networks, in order to solve different PUE attack scenarios in CRNs. We have carried out some simulations. The simulation results demonstrated that our improved energy detection scheme is more effective than the traditional one. Finally, we have analyzed the potential problems in our proposed schemes and have identified possible directions for future work.

List of Symbols

CR	Cognitive radio
PUE	Primary user emulation
CRN	Cognitive radio network
PUE	Primary user emulation
TDOA	Time difference
PU	Primary user
SU	Second user
FCC	Federal Communications Commission
SDR	Software defined radio
RF	Radio frequency
DSA	Dynamic spectrum access
SNR	Signal-to-noise ratio
CAF	Cyclic autocorrelation function
SOF	Spectral coherence function
CCJ	Control jamming channel
QoS	Quality of service
SSDF	Spectrum sensing data falsification
DoS	Denial of service
AOA	Angle of arrival
TOA	Time of arrival
RSS	Received signal strength

WSN	Wireless sensor network
GPS	Global positioning system
c	Speed of light
BS	Base station
SCF	Spectral correlation function
ANN	Artificial neural network
GDME	Geometric distance measurement error

References

[1] T. Cisco. *Cisco visual networking index: Global mobile data traffic forecast update, 2013–2018*. Cisco Public Information (2014).

[2] F. C. C. (FCC). *Spectrum inventory table 137 mhz to 100 ghz*. http://transition.fcc.gov/oet/info/database/spectrum/. Accessed: 2010-04-08.

[3] M. A. McHenry, P. A. Tenhula, D. McCloskey, D. A. Roberson, and C. S. Hood. *Chicago spectrum occupancy measurements & analysis and a long-term studies proposal*. In *the first international workshop on Technology and policy for accessing spectrum*, p. 1 (ACM, 2006).

[4] S. Pagadarai and A. M. Wyglinski. *A quantitative assessment of wireless spectrum measurements for dynamic spectrum access*. In *proceedings of 4th International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2009. CROWNCOM'09.*, pp. 1–5 (IEEE, 2009).

[5] J. Mitola. *Cognitive radio for flexible mobile multimedia communications*. In *proceedings of 1999 IEEE International Workshop on Mobile Multimedia Communications, 1999.(MoMuC'99)*, pp. 3–10 (IEEE, 1999).

[6] J. Mitola. *Cognitive radio—an integrated agent architecture for software defined radio* (2000).

[7] F. C. C. (FCC). *Facilitating opportunities for flexible, efficient, and reliable spectrum use employing spectrum agile radio technologies*. http://hraunfoss.fcc.gov/edocspublic/attachmatch/FCC-03-322A1.pdf. Accessed: 2003-12.

[8] 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 **50**(13), 2127 (2006).

[9] F. K. Jondral. *Software-defined radio: basics and evolution to cognitive radio*. EURASIP journal on wireless communications and networking **2005**(3), 275 (2005).

[10] D. Cabric, S. M. Mishra, and R. W. Brodersen. *Implementation issues in spectrum sensing for cognitive radios*. In *proceedings of the thirty-eighth Asilomar conference on Signals, systems and computers, 2004.*, vol. 1, pp. 772–776 (IEEE, 2004).

[11] T. C. Clancy and N. Goergen. *Security in cognitive radio networks: Threats and mitigation.* In *proceedings of 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008.*, pp. 1–8 (IEEE, 2008).

[12] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty. *A survey on spectrum management in cognitive radio networks.* IEEE Communications Magazine **46**(4), 40 (2008).

[13] W. El-Hajj, H. Safa, and M. Guizani. *Survey of security issues in cognitive radio networks.* Journal of Internet Technology **12**(2), 181 (2011).

[14] Z. Jin, S. Anand, and K. P. Subbalakshmi. *Impact of primary user emulation attacks on dynamic spectrum access networks.* IEEE Transactions on Communications **60**(9), 2635 (2012).

[15] A. Sonnenschein and P. M. Fishman. *Radiometric detection of spread-spectrum signals in noise of uncertain power.* IEEE Transactions on Aerospace and Electronic Systems **28**(3), 654 (1992).

[16] A. Sahai and D. Cabric. *Spectrum sensing: fundamental limits and practical challenges.* In *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)* (2005).

[17] R. Tandra and A. Sahai. *Fundamental limits on detection in low snr under noise uncertainty.* In *proceedings of International Conference on Wireless Networks, Communications and Mobile Computing, 2005*, vol. 1, pp. 464–469 (IEEE, 2005).

[18] S. M. Kay. *Fundamentals of statistical signal processing, volume 2: Detection theory* (1998).

[19] H. Urkowitz. *Energy detection of unknown deterministic signals.* Transacions of the IEEE **55**(4), 523 (1967).

[20] H.-S. Chen, W. Gao, and D. G. Daut. *Signature based spectrum sensing algorithms for ieee 802.22 wran.* In *proceedings of IEEE International Conference on Communications, 2007. ICC'07.*, pp. 6487–6492 (IEEE, 2007).

[21] W. A. Gardner. *Exploitation of spectral redundancy in cyclostationary signals.* IEEE Transactions on Signal Processing Magazine **8**(2), 14 (1991).

[22] N. Han, S. Shon, J. H. Chung, and J. M. Kim. *Spectral correlation based signal detection method for spectrum sensing in ieee 802.22 wran systems.* In *proceedings of The 8th International Conference on Advanced Communication Technology, 2006. ICACT 2006.*, vol. 3, pp. 6–pp (IEEE, 2006).

[23] N. Hoven, R. Tandra, and A. Sahai. *Some fundamental limits on cognitive radio.* Wireless Foundations EECS, Univ. of California, Berkeley (2005).

[24] D. O. North. *An analysis of the factors which determine signal/noise discrimination in pulsed-carrier systems.* proceedings of the IEEE **51**(7), 1016 (1963).

[25] Wikipedia. *Matched filter*. http://en.wikipedia.org/wiki/Matched_filter. Accessed: 2014-06-15.

[26] A. Pandharipande, J. Kim, D. Mazzarese, and B. Ji. *Ieee p802. 22 wireless rans: Technology proposal package for ieee 802.22*. IEEE 802.22 WG on WRANs (2005).

[27] D. Cabric, A. Tkachenko, and R. W. Brodersen. *Spectrum sensing measurements of pilot, energy, and collaborative detection*. In *proceedings of Military Communications Conference, 2006. MILCOM 2006.*, pp. 1–7 (IEEE, 2006).

[28] 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 **26**(1), 25 (2008).

[29] Y. Xing, R. Chandramouli, S. Mangold, and N. Sai Shankar. *Dynamic spectrum access in open spectrum wireless networks*. IEEE Journal on Selected Areas in Communications **24**(3), 626 (2006).

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

[31] S. Chen, K. Zeng, and P. Mohapatra. *Hearing is believing: Detecting mobile primary user emulation attack in white space*. In *Transactions of 2011 IEEE on INFOCOM*, pp. 36–40 (IEEE, 2011).

[32] L. Lu, S.-Y. Chang, J. Zhang, L. Qian, J. Wen, V. Lau, R. Cheng, R. Murch, W. Mow, and K. Letaief. *Technology proposal clarifications for ieee 802.22 wran systems*. Transactions of IEEE 802.22 WG on WRANs (2006).

[33] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han. *Defeating primary user emulation attacks using belief propagation in cognitive radio networks*. IEEE Journal on Selected Areas in Communications **30**(10), 1850 (2012).

[34] R. Chen. *Enhancing Attack Resilience in Cognitive Radio Networks*. Ph.D. thesis, Virginia Polytechnic Institute and State University (2008).

[35] K. Pahlavan. *Principles of wireless networks: A unified approach* (John Wiley & Sons, Inc., 2011).

[36] X. Cheng, A. Thaeler, G. Xue, and D. Chen. *Tps: A time-based positioning scheme for outdoor wireless sensor networks*. In *proceedings of Twenty-third AnnualJoint Conference on the IEEE Computer and Communications Societies, INFOCOM 2004.*, vol. 4, pp. 2685–2696 (IEEE, 2004).

[37] T. S. Rappaport *et al. Wireless communications: principles and practice*, vol. 2 (prentice hall PTR New Jersey, 1996).

[38] G. Shen, R. Zetik, and R. S. Thoma. *Performance comparison of toa and tdoa based location estimation algorithms in los environment.* In *5th Workshop on Positioning, Navigation and Communication, 2008. WPNC 2008.*, pp. 71–78 (IEEE, 2008).

[39] R. Kaune. *Accuracy studies for tdoa and toa localization.* In *proceedings of the 15th International Conference on Information Fusion (FUSION) 2012.*, pp. 408–415 (IEEE, 2012).

[40] J. D. Bard, F. M. Ham, and W. L. Jones. *An algebraic solution to the time difference of arrival equations.* In *Transactions of IEEE on Southeastcon'96. Bringing Together Education, Science and Technology.*, pp. 313–319 (IEEE, 1996).

[41] S. Camlica and Y. Tanik. *Emitter localization with kalman filter using tdoa.* In *proceedings of IEEE 19th Conference on Signal Processing and Communications Applications (SIU), 2011*, pp. 154–157 (IEEE, 2011).

[42] R. Dobbins. *Software Defined Radio Localization Using 802.11-style Communications.* Ph.D. thesis, Worcester Polytechnic Institute.

[43] R. Exel and P. Loschmidt. *High accurate timestamping by phase and frequency estimation.* In *proceedings of International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, 2009. ISPCS 2009.*, pp. 1–6 (IEEE, 2009).

[44] J. Abel and J. Smitht. *The spherical interpolation method for closed-form passing source localization using range difference measurements.* In *proceedings of IEEE Int. Conference. Acoustics, Speech, Signal Processing* (Citeseer, 1987).

[45] Y. Chan and K. Ho. *A simple and efficient estimator for hyperbolic location.* IEEE Transactions on Signal Processing **42**(8), 1905 (1994).

[46] R. Peng and M. L. Sichitiu. *Angle of arrival localization for wireless sensor networks.* In *proceedings of 2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 2006. SECON'06.*, vol. 1, pp. 374–382 (IEEE, 2006).

[47] D. Niculescu and B. Nath. *Ad hoc positioning system (aps) using aoa.* In *Processdings of the 22nd Annual Joint Conference of the IEEE Computer and Communications, INFOCOM 2003.*, vol. 3, pp. 1734–1743 (IEEE, 2003).

[48] A. Nasipuri and K. Li. *A directionality based location discovery scheme for wireless sensor networks.* In *proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pp. 105–111 (ACM, 2002).

[49] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher. *Range-free localization schemes for large scale sensor networks.* In *proceedings of the 9th annual international conference on Mobile computing and networking*, pp. 81–95 (ACM, 2003).

[50] E. P. J. Tozer. *Broadcast engineer's reference book* (Taylor & Francis, 2004).

[51] Y. V. Fyodorov and E. Strahov. *An exact formula for general spectral correlation function of random hermitian matrices.* Journal of Physics A: Mathematical and General **36**(12), 3203 (2003).

[52] A. Tkachenko, D. Cabric, and R. W. Brodersen. *Cyclostationary feature detector experiments using reconfigurable bee2.* In *the 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007.*, pp. 216–219 (IEEE, 2007).

[53] S. Enserink and D. Cochran. *A cyclostationary feature detector.* In *proceedings of the Twenty-Eighth Asilomar Conference on Signals, Systems and Computers, 1994.*, vol. 2, pp. 806–810 (IEEE, 1994).

[54] E. Like, V. D. Chakravarthy, P. Ratazzi, and Z. Wu. *Signal classification in fading channels using cyclic spectral analysis.* EURASIP Journal on Wireless Communications and Networking **2009**, 29 (2009).

[55] M. Sivanandam *et al. Introduction to artificial neural networks* (vikas publishing House PVT LTD, 2009).

[56] K. Gurney. *An introduction to neural networks* (CRC press, 1997).

[57] M. Gupta, L. Jin, and N. Homma. *Static and dynamic neural networks: from fundamentals to advanced theory* (John Wiley & Sons, 2004).

[58] K. Matsuoka. *Noise injection into inputs in back-propagation learning.* IEEE Transactions on Systems, Man and Cybernetics. **22**(3), 436 (1992).

[59] Y. Liu, P. Ning, and H. Dai. *Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures.* In *2010 IEEE Symposium on Security and Privacy (SP)*, pp. 286–301 (IEEE, 2010).

[60] R. W. Thomas, R. S. Komali, B. J. Borghetti, and P. Mahonen. *A bayesian game analysis of emulation attacks in dynamic spectrum access networks.* In *2010 IEEE Symposium on New Frontiers in Dynamic Spectrum,*, pp. 1–11 (IEEE, 2010).

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

[62] B. Wild and K. Ramchandran. *Detecting primary receivers for cognitive radio applications.* In *2005 First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pp. 124–130 (IEEE, 2005).

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

[64] X.-l. Luo, W. Li, and J.-r. Lin. *Geometric location based on tdoa for wireless sensor networks.* ISRN Applied Mathematics **2012** (2012).

[65] R. Poppe. *A survey on vision-based human action recognition.* Image and vision computing **28**(6), 976 (2010).

[66] K. Bonne Rasmussen and S. Capkun. *Implications of radio fingerprinting on the security of sensor networks.* In *proceedings of Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007.*, pp. 331–340 (IEEE, 2007).

[67] O. Ureten and N. Serinken. *Wireless security through rf fingerprinting.* Canadian Journal of Electrical and Computer Engineering **32**(1), 27 (2007).