Chapter 1
Cognitive Radio Network Technologies and Applications

Rajorshi Biswas and Jie Wu

Abstract Mobile devices are advancing every day, creating a need for higher bandwidth. Because both the bandwidth and spectrums are limited, maximizing the utilization of a spectrum is a target for next-generation technologies. Government agencies lease different spectrums to different mobile operators, resulting in the underutilization of spectrums in some areas. For some operators, limited licensed spectrums are insufficient, and using others' unused spectrums becomes necessary. The unlicensed usage of others' spectrums is possible if the licensed users are not using the spectrum, and this gives rise to the idea of cognitive radio networks (CRNs). In CRN architecture, each user must determine the status of a spectrum before using it. In this chapter, we present the complete architecture of CRN, and we additionally discuss other scenarios including the applications of the CRN. After the Federal Communications Commission (FCC) declared the 5GHz band unlicensed, Wi-Fi, LTE, and other wireless technologies became willing to access the band, leading to a competition for the spectrums. Because of this, ensuring that the spectrum is fairly shared among different technologies is quite challenging. While other works on DSRC and Wi-Fi sharing exist, in this chapter, we discuss LTE and Wi-Fi sharing specifically.

1.1 Introduction

Currently, governmental agencies assign wireless spectrums to license holders in large areas for long terms. For this kind of static spectrum allocation, licensed users of any spectrum cannot use others' licensed spectrums. This

Temple University
Philadelphia, PA 19122, USA

Rajorshi Biswas e-mail: rajorshi@temple.edu · Jie Wu e-mail: jiewu@temple.edu

increase in data transmission results in a spectrum crisis for the mobile users. One method that can help in this situation is dynamic spectrum allocation. Users use their spectrum in an opportunistic manner. This way, if others' spectrums are free, then any licensed user can use their licensed spectrum. Users in this kind of network architecture need to sense channels to find a free channel. If they find more than one free channel, they need to choose the best channel for their transmissions. Generally, the number of users is greater than the number of free channels and users need to share a channel. While using a free, unlicensed channel, users must be cautious about licensed transmissions because if any licensed transmission is detected, the user must vacate the channel. Therefore, the operations of users can be divided into four major steps: spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility. From these four major operations in a CRN, we can conclude that there are two kinds of transmissions. One is transmissions in a licensed band; this we call the *primary transmissions* and we call the user transmitting in the licensed band a *primary user* (PU). The other type is transmissions in the unlicensed band, which we call the *secondary transmissions*; the user transmitting in the unlicensed band is an *SU* (SU).

Transmissions in an unlicensed channel depend on the sensing information of CR users. There are various methods for detecting transmissions in a spectrum. Primary transmitter detection, primary receiver detection, and cooperative sensing are the most common techniques. Cognitive radio (CR) users must be able to decide the best channel out of all the available channels. This notion is called *spectrum decision.* Spectrum decision depends on the channel characteristics and operation of PUs. *Spectrum sharing* deals with sharing the same channel with multiple CR users. Many users can detect that the same channels are free and their channel choice decisions can be the same. Because of this, the same channel must sometimes be shared between different CR users. While a CR user is transmitting in a secondary channel, a PU may need to use the channel. In this situation, the SU vacates the channel to the PU, but a secondary transmission cannot be stopped. The SU must find another channel and resume transmissions in that channel.

At the end of this chapter, we discuss some coexistence scenarios in the 5GHz band which is currently an unlicensed band. Currently, some Wi-Fi standards (802.11ac and 802.11ax) are operating in the 5GHz band. Dedicated Short Range Communication (DSRC) also operates in the 5GHz band. LTE shareholders are now trying to operate in that band. We discuss two co-existence scenarios: the co-existence between LTE and Wi-Fi and the co-existence between Wi-Fi and DSRC.

1.2 Network Architecture of Cognitive Radio Networks

This subsection describes the network architecture and components of a CRN. Figure 1.1 depicts the whole network system. User devices, primary base stations, and CR base stations are the components of a basic CRN. In Figure 1.1, there are two channels: channel 1 and channel 2. One primary base station operates in channel 1 and another in channel 2. Transmissions with the primary base station are done through licensed channels by mobile users, and the transmissions are called primary transmissions (denoted by solid lines). Transmissions with the CR base station can be done through either licensed or unlicensed channels and these transmissions are called secondary transmissions (marked by dotted lines). There is also another kind of transmission in which any user device can transmit directly to another user device. Therefore, transmissions in a CRN can be grouped into three classes:

- **Primary transmissions:** Primary transmissions are most prioritized transmissions and cannot be compromised with other transmissions. These transmissions are done in a licensed channel between primary base stations and PUs. Primary transmissions are denoted by solid lines in Figure 1.1.
- **Secondary transmissions:** Secondary transmissions are done in the absence of primary transmissions. Transmissions between the CR base station and the CR user are usually secondary transmissions.
- **Secondary ad hoc transmissions:** User to user communications are called ad hoc transmissions. These transmissions can continue without base stations or other components of the network architecture. Users create their own network topology and adapt any routing protocols of ad hoc networks. Users in the gray area form an ad hoc network in Figure 1.1. There are a lot of routing protocols for mobile ad hoc networks. For example, the proposed routing algorithm in [1], which ensures a fair amount of communications among nodes and improves the load concentration problem, can be used in secondary ad hoc networks. The on-demand cluster-based hybrid routing protocol proposed in [2] can also be applicable here.

1.3 Spectrum Sensing

Secondary transmissions depend on spectrum sensing information, so this step should be done very accurately. Inaccurate sensing detection can lead to interferences with the PU that are highly unexpected. Though false alarms (in which channel is not occupied, but is detected as occupied) do not create interferences with the primary transmissions, it makes the CR user choose a channel from a narrower range of channels. As a result, a channel must be shared with many CR users and there will be increased competition among

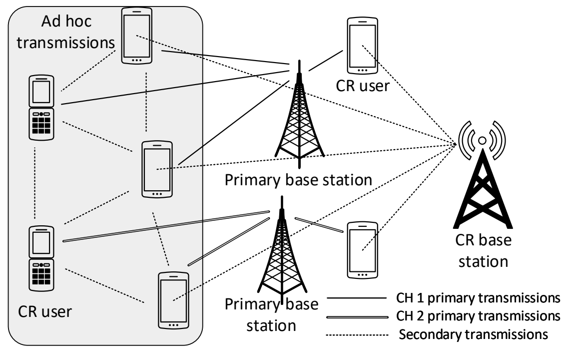

Fig. 1.1 Network architecture of a CRN.

CR users to access the channel. The authors of [3] present a classification of spectrum sensing techniques. First, they classify sensing techniques into three groups: non-cooperative sensing, cooperative sensing, and interference-based sensing. Non-cooperative sensing is again classified into three groups: energy detection, matched filter detection, and cyclostationary feature detection. The classification is depicted in Figure 1.2.

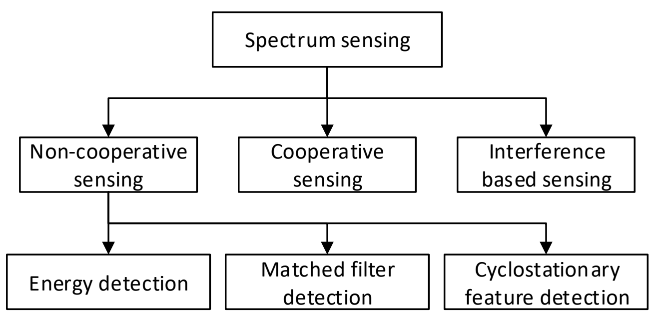

Fig. 1.2 Classification of spectrum sensing technologies.

1.3.1 Non-cooperative sensing

In non-cooperative sensing, CR users do not share sensing information with one another. A CR user makes a decision about the PU's presence using its own sensing information. We discuss primary transmitter detection and primary receiver detection, which are presented in [4] and [5], in the following subsection.

1.3.1.1 Primary Transmitter Detection

Transmitter detection techniques emphasize detecting low power signals from any PU. Low power signals mix with noise from the environment and make it hard for the CR user to detect primary signals. A low signal-to-noise ratio, multipath fading effects, and time depression make primary transmissions detection very difficult for the CR user. We discuss some primary transmitter detection techniques like energy detection, coherent detection, and matched filter detection.

Energy Detection:

This technique does not require CR users to have knowledge of PU signal characteristics, and it is easy to implement. Because of this, it is widely used to detect primary transmissions. Let's assume $S(n)$ is the signal received by the CR user, $W(n)$ is white Gaussian noise, and $P(n)$ is the original signal from the PU.

$$H_0 : S(n) = W(n) \tag{1.1}$$

$$H_1 : S(n) = W(n) + hP(n) \tag{1.2}$$

Hypothesis H_0 indicates the absence of a PU and hypothesis H_1 indicates the presence of the PU transmissions. h denotes the channel gain between the primary and secondary transmissions. Then, the average energy S of N samples is:

$$S = 1/N \sum_{n=1}^{N} S(n)^2 \tag{1.3}$$

The CR user collects N samples, calculates the average energy, and compares it with a threshold λ. If the average energy is greater than the threshold, λ, then the CR user concludes that primary transmissions are present. To measure the performance, we denote the probability of the false positive (CR detects the presence of PU transmissions when there is no PU transmission) as P_f and probability of the detection as P_d.

$$P_f = P(S > \lambda | H_0) \tag{1.4}$$

$$P_d = P(S > \lambda | H_1) \tag{1.5}$$

To improve the performance, we need to keep the PU's transmission secured. Therefore, the false positive probability should be less than 0.1 and the detection probability should be greater than 0.9.

Coherent Detection:

When characteristics like signal patterns, pilot tones, and preambles of primary signals are known, coherent detection techniques can be used. These techniques work better than energy detection in an environment with noise level uncertainties. To describe this technique, we define the binary hypothesis slightly differently than energy detection.

$$H_0 : S(n) = W(n) \tag{1.6}$$

$$H_1 : S(n) = \sqrt{\epsilon} P_{pt}(n) + \sqrt{1-\epsilon} P(n) + W(n) \tag{1.7}$$

Here, pilot signal energy is denoted by P_{pt}, and ϵ is the fraction of energy allocated to the pilot tone. Pilot signals are special kinds of signals used to send control signals. Hypothesis H_0 indicates the absence of primary transmissions, and hypothesis H_1 indicates the presence of primary transmissions.

If the CR user collects N samples and $\hat{X}_p$ is the unit vector in the direction of the pilot tone, then the average energy, S, is:

$$S = 1/N \sum_{n=1}^{N} S(n)^2 \times \hat{X}_p(n) \tag{1.8}$$

Problems of Transmitter Detection:

There are some situations where this detection technique does not work. We discuss two such situations: the hidden terminal problem and shadowing and multipath effects. Figure 1.3 depicts a scenario where a CR user remains outside of a base station's coverage area and it detects that the channel is free. Because it thinks the channel is free, it transmits in the channel and interference occurs at the other PU remaining in the coverage of the base station and the CR user. Figure 1.4 depicts the shadowing effect. The CR user behind the wall cannot detect primary transmissions. So, the same problem occurs.

1.3.1.2 Primary Receiver Detection:

The most effective way to detect PU transmissions is to detect the primary receivers who are receiving from the primary channel. The circuit in Figure

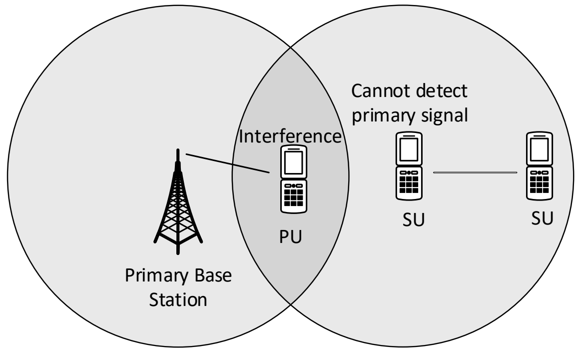

Fig. 1.3 Hidden terminal problem.

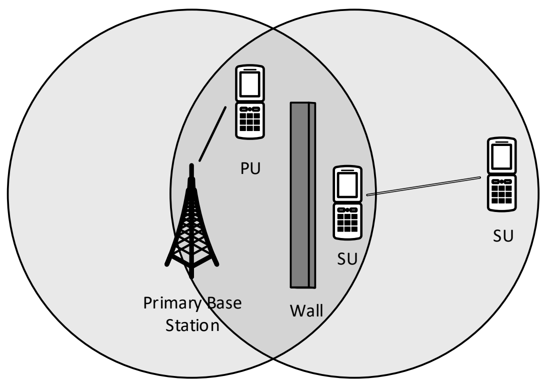

Fig. 1.4 Shadowing effect.

1.5 shows a simple RF receiver. It has a local oscillator that emits a very low power signal for its leakage current in the circuit. A CR user can detect the leakage signals from the RF receiver circuit and identify the presence of primary transmissions. This detection technique solves both the hidden terminal and shadowing effect problems. Since the signal power is very low, it is very challenging and costly to implement the circuit for primary receiver detection.

1.3.1.3 Matched Filter Detection

When primary signal features like modulation type, pulse shape, operating frequency, packet format, noise statistics, etc. are known, matched filter de-

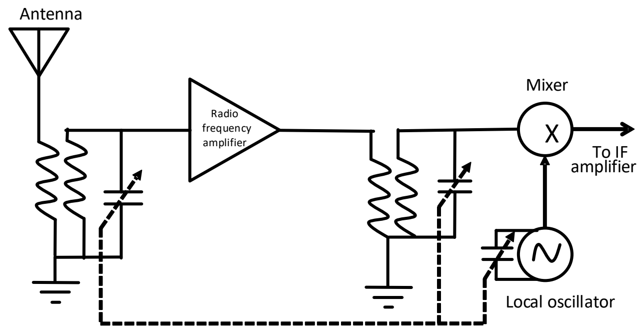

Fig. 1.5 Simple RF receiver circuit.

tection can be an optimal detection technique. If these parameters are known, the CR user only needs to calculate a small number of samples. As the signal-to-noise ratio decreases, the CR user needs to calculate a greater number of samples. The disadvantages of this technique are the complexities in low signal-to-noise ratio, the high cost of implementation, and the very poor performance if the features are incorrect.

1.3.1.4 Cyclostationary Feature Detection

In a broader sense, a signal can be called a cyclostationary process if its statistical properties vary cyclically with time. In [6], the authors presented a signal classification procedure that extracts cyclic frequency domain profiles and classifies them by comparing their log-likelihood with the signal type in the database. This technique can work very well in a low SNR. The drawback of this technique is that it needs a huge amount of computation and thus, a high speed sensing is hard to achieve [7].

1.3.2 Cooperative Sensing

Cooperative sensing deals with sharing CR users' sensing information and making decisions by combining this information. A CR user collects sensing information from other CR users (in a distributed system) or from the base station (in a centralized system). Then, it analyzes the sensing information and makes a decision about whether the primary transmission is ongoing or not. Though this detection technique overcomes the hidden terminal problem and the shadowing and multipath problems, it is more complex than previously mentioned detection techniques. Though its implementation is costly and its time complexity is higher, this technique has the best sensing accuracy and very few false alarms.

1.3.2.1 Data Aggregation Center of Cooperative Sensing

This system can be located either in user devices (distributed system) or in base stations (centralized system). A *Data aggregation center* is responsible for the collection and combination processes of sensing information. The system runs some aggregation functions over the collected data continuously and emits results about the primary transmission status. There are different methodologies to combine and calculate, but we must discuss the hard combining and the soft combining methodologies.

Hard Combining:

CR users send their sensing results to the data aggregation center. This is just one bit information: 1 for the presence of primary transmissions and 0 for the absence of primary transmissions. After receiving the sensing information, the data aggregation center calculates the final result. The final result can be calculated based on AND, OR, or MAJORITY voting.

Soft Combining:

Unlike the hard combining methodology, CR users send their raw sensing information (energy level w.r. to time, signal power, SNR, etc.) to the data aggregation center. Then, the data aggregation center decides the presence of primary transmissions.

1.3.3 Interference Based Sensing

One user's transmissions can interfere with another user's transmissions at the receivers. The FCC introduced a new model to measure interference. According to the model, a receiver can tolerate up to a certain level of interference. This limit is called the *interference-temperature limit*. As long as CR users do not exceed this limit, they can use any spectrum. In this sensing method, the PU will calculate the noise level and send the information to the CR users. The CR users will use the information to control their transmissions to avoid exceeding the interference-temperature limit for PUs. The authors in [8] present interference-based sensing and a technique to calculate the interference at a PU.

1.3.4 Predicting Channel to Sense

Due to limitations in the hardware, the CR users cannot sense a wide range of channels at a time. In addition, sensing a wide range of channels will raise the CR users' power consumption. Instead of sensing a huge number of channels, a CR user can predict which channel to sense. The authors in [9] model the prediction as a *multi-armed-bandit* problem. In the multi-arm-bandit problem of probability theory, a gambler tries to maximize his reward by playing different slot machines. The gambler has to decide which slot machine to play, how many times to play each machine, and in which order to play. The main objective of the gambler is to learn through every play and to predict which machine to play next so that the cumulative reward maximizes.

Let's assume there are N SUs and K channels, and SUs are trying to learn from their past history to predict the next channel to sense. Every CR user keeps a log of the transmitting channel in an array of length K. We will denote the array by B_n where $n \in \{1, ..., N\}$.

$$B_n[k] = \begin{cases} 1, & \textit{if CR user n transmitted in channel k} \\ 0, & \textit{Otherwise} \end{cases} \tag{1.9}$$

CR users share their B_n with the other CR users. CR users preserve B_n with the time of arrival t_{B_n}. Then, CR users apply $\epsilon - GREEDY$ methods to predict the channel for sensing [9].

ϵ-GREEDY method:

This is the simplest solution of the multi-arm-bandit problem. The next channel is selected randomly with a probability of ϵ. The rest of the time, the maximum average valued channel is selected. The average value of channel k is denoted by A_k.

$$A_k = \frac{1}{N} \sum_{n=1}^{N} B_n[k] \tag{1.10}$$

Another approach that considers forgetting factor β while averaging the channel values works better. Let transmission logs B_{n_1}, B_{n_2}, ..., B_{n_z} come to a CR user at t_1, t_2, ..., t_z. The forgetting factors for t_1, t_2, ..., t_z are β_{t_1}, β_{t_2}, ..., β_{t_z}, respectively. The average value of channel k is denoted by A_{k_β}.

$$B_{n_\beta}[k] = \sum_{z=1}^{Z} \beta_{t_z} \times B_{n_z}[k] \tag{1.11}$$

$$A_{k_\beta} = \frac{1}{N}\sum_{n=1}^{N} B_{n_\beta}[k] \tag{1.12}$$

$B_{n_\beta}[k]$ denotes the effective value of channel k for CR user n. The effective values of different CR users for a channel are averaged to find the average effective value of the channel. The channel with the maximum average effective value is selected to sense next.

1.4 Spectrum Decision

CR users get a list of free channels after completion of the sensing process. A CR user can transmit in only one channel at a time. Therefore, the CR user must choose one channel among all the free channels. It is likely that any rational CR will choose the best channel. A channel can be characterized as "good" or "bad" according to some channel properties. Channel choice not only depends on channel characteristics, but also on other CR users' activities. For example, if a channel is crowded by many CR users, despite being a good channel, a CR may not choose that channel. Normally, the spectrum decision process is done in two steps. We discuss some characteristics of channel in the following.

Interference:

Interference in a channel represents the channel's capacity. If interference is high, its capacity is low. A CR user should choose a channel with low interference. The permissible power of a CR can be calculated from the interference at the receiver.

Path Loss:

Path loss is the reduction in power density of an electromagnetic wave as it propagates through space. It is related to both distance and frequency. If the carrier frequency is high, the path loss is also high. To reduce path loss, a CR can increase the transmission power. Interference with other users also increases with the increase of transmission power. Usually, a CR user chooses a channel with low path loss. If the distance between the sender and the receiver is short enough that the path loss is ineffective, then the CR user can ignore the path loss's effects.

Wireless Link Error:

Errors are more likely to happen in wireless than in wired connections. The error rate also depends on modulation techniques. These errors are handled by transport layer protocols. Therefore, CR users choose channels with low link error rates.

Transmission Delay:

Different channels have different interference levels, packet loss rates, wireless link errors, and path loss effects. As a result, different types of link layer protocols are appropriate for different channels. For this heterogeneity, different transmission delays are observed in different channels. A CR user might choose a channel with few transmission delays.

PU Activity:

If PU transmissions are very likely in the channel, then the CR cannot continue transmission for a long time in that channel. In this sense, the CR should choose the channel with the lowest user activity.

Contagious Frequency Channel:

If a CR user can find some channels with contagious frequencies, it can extend the channel's bandwidth by combining channels. However, if PU activities are seen in any of the channels, it cannot yield one particular channel. As a result, the CR segregates the channels and takes different channels for transmission. Since the probability of PU activity increases by the number of combined channels, combining channels may not be a good spectrum decision in situations with high user activity channels. In addition, channel aggregation and segregation takes time that increases the latency of a transmission.

1.5 Spectrum Sharing

Usually, the number of available free channels is less than the number of CR users. Therefore, CR users must share channels. CR users can be competitive or cooperative with each other. A scenario where CR users are competitive can be modeled as a static game where each CR user tries to maximize their reward by transmitting in the shared channel. There are three paradigms (underlay, overlay, and interleave) that are used to facilitate the spectrum sharing.

Underlay:

In this paradigm, secondary and primary transmissions are done simultaneously. CR users transmit in very low power that appears as noise to the primary receiver. Secondary transmission power can be determined by the interference-temperature limit. If the secondary transmission power does not exceed the interference-temperature limit, then it does not hamper the primary transmission. The biggest advantage is that CR users do not need to sense PU transmissions, so, secondary transmissions can be operated regardless of PUs' activities. SUs suffer from packet loss due to primary transmissions. The authors in [10] propose an energy-efficient algorithm to minimize the loss rate of SUs. The algorithm also maximizes energy-efficiency in information bits per Joule.

Overlay:

In this paradigm, CR users utilize the unused portion of the primary spectrum. Using a portion of the spectrum reduces interference with a PU who uses the whole spectrum. Unlike the underlay, there is no transmission power limit; an SU can transmit in its maximum power. SUs must have knowledge (codebook, message format, frequency etc.) about the primary spectrum. CR users can get this knowledge from the broadcasting of the PU or from a uniform standard. Since the CR user knows the codebook, it can divide its power between its own message transmissions and relay the primary message [4].

Interweave:

This is the original proposal for CRN. In this paradigm, the SU can only transmit if there is no PU activity. This requires that one sense the primary channel. SUs use their detection techniques to detect primary transmissions, and if a channel is not occupied by a PU, then the SU starts transmitting.

1.5.1 Spectrum Allocation in Centralized Interweave Cognitive Radio Network

In a centralized system, channel allocations to SUs are done by a base station, and secondary transmissions can occur in the absence of PUs in a interweave system. We assume a heterogeneous network with M number of PUs $m \in \{1,..,M\}$. An N number of SUs $n \in \{1,..,N\}$ compete with each other to get access to any $k \in \{1,..,K\}$ channel among K free channels. $P_p(x)$ and $P_s(y)$ are the transmission powers of the PU x and the SU y, respectively. $g_p(x)$ denotes the gain of the signal of PU x in the channel and $g_s(y)$ denotes the gain of the signal of SU y. So, the total noise in any channel, k, at any SU, s, is:

$$Total\,Noise = \sum_{n=1}^{N} g_s(n)P_s(n) + \sum_{m=1}^{M} g_p(m)P_p(m) + N_k \tag{1.13}$$

N_k denotes white Gaussian noise from external sources. The first part of the total noise equation is caused by the signals of other secondary transmissions and the second part is caused by the signals of all primary transmissions. Therefore, the signal-to-noise ratio at the SU y in channel k is:

$$SNR_k(y) = \frac{g_s(y)P_s(y)}{Total\,Noise} \tag{1.14}$$

Figure 1.6 shows the bipartite graph formulation by the SUs and the free

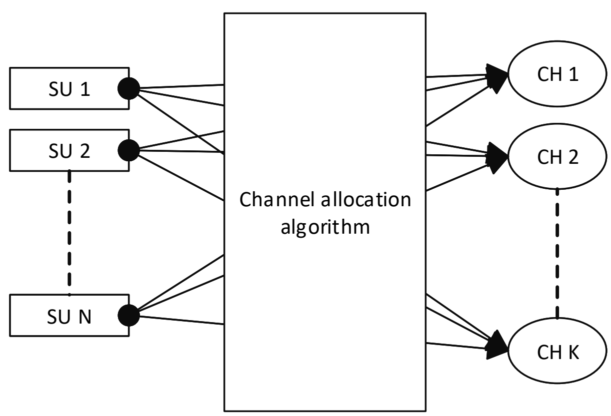

Fig. 1.6 Channel allocation algorithm.

channels. An N number of SUs form a disjoint set, and a K number of channels form another disjoint set of a bipartite graph. Edges in this graph represent an allocation of the channel to an SU. The graph in Figure 1.6 is a weighted graph whose edge weight represents the allocation cost of the channel in terms of the decrease in the total signal-to-noise ratio. Let's assume that after allocating channel k to SU n, the total signal-to-noise ratio decreases from SNR_p to SNR_n. Then, the cost of allocation is:

$$C(n,k) = \frac{SNR_p - SNR_n}{SNR_p} \tag{1.15}$$

We can also call $C(n,k)$ the weight of the edge (n,k) in the bipartite graph constructed by N SUs and K free channels. Now, the problem converts to minimizing the matching cost in a bipartite graph. The hungarian algorithm provides the solution to the maximum weight matching [11], which can be adapted to minimize the cost of the matching by inverting the cost.

1.6 Spectrum Mobility

After the spectrum choice, any CR user can access a secondary spectrum, but a PU is sensed to be present when a CR user is transmitting. The CR user must vacate the channel for the PU. The transmissions of the CR user cannot be stopped and may be continued in another channel. This process is referred to as spectrum mobility. The main function of spectrum mobility is to do a spectrum handoff. The spectrum handoff process consists of two phases: the evaluation phase and the link maintenance phase [12]. The evalution phase deals with observing the environment to find handoff-triggering events, like primary transmission detection or channel condition degradation. After the handoff triggering event, SUs decide to handoff and go to the link maintanace phase. In the link maintainance phase, SUs stop the ongoing transmission and resume transmissions in another free channel. After completing this phase, SUs return to the evaluation phase. In [13], authors present different handoff strategies:

- **Non-handoff Strategy:** In this strategy, the CR user remains idle while the primary transmissions continue. The CR user expects to transmit in the same channel. This strategy is inefficient if the primary transmissions continue for a long time. Long waiting times will cause the QoS to degrade. This strategy is preferable when CR users know the channel statistics and short time primary transmissions are likely in the channel.
- **Pure Reactive Handoff Strategy:** In this strategy, the CR user hands off the channel after detection of a primary transmission in the current channel. The CR must choose another free channel to continue the transmission. Finding the next free channel can take time, which is not acceptable for the smooth data connection. Since the CR user finds the next channel after the handoff-triggering events, the majority of the time is spent finding the free channel.
- **Pure Proactive Handoff Strategy:** In the proactive handoff strategy [14], the CR user finds the next free channel before the detection of the primary channel; the free channel can work as a backup channel. The CR user can predict the time of the PU's presence and handoff channel before handoff-triggering events occur. This strategy needs hardware support to

sense and transmit simultaneously. Still, there is the possibility of the presence of a PU in the backup channel that could lead to transmission delays. Predicting the time of the presence of primary transmissions requires a lot of machine learning and can lead to a high power consumption by CR users due to computation complexities.

- **Hybrid Handoff Strategy:** This strategy is a combination of the pure reactive and pure proactive handoff strategies. In the hybrid handoff strategy, finding the free channel is done before the handoff-triggering event (like in the proactive handoff strategy) but the channel handoff is done after the triggering event (like reactive handoff strategy). This strategy can achieve a faster channel handoff, but the possibility that the backup channel will be obsolete is still a concern.

Multiple strategies for selecting the next channel exist. The hidden markov model is used to predict channel behavior in [15], [16], and [17]. However, prediction-based channel selection can be harmful when predictions are wrong. Delays in selecting the next channel can deteriorate the QoS. Therefore, we consider a search-based approach to select the next channel. Let's consider a 2-D search space of time and frequency. We consider all slots as nodes in a graph. An edge between one node to another represents the channel switching cost, which is either zero or one. Figure 1.7 shows the formation of the graph. Let's denote a slot by (T, CH), where T represents the time and CH represents the channel. For example, the switching cost from ($T1$, $CH3$) to ($T2$, $CH3$) is 0 because the CR user actually continued transmission in the same channel. The switching cost from ($T1$, $CH1$) to ($T2$, $CH1$), ($T2$, $CH2$), and ($T2$, $CH4$) is 1. The weight of an edge can be found by adding the switching cost and the channel density. In the figure, darker slots have more channel density. Now, we get a directed weighted graph. Graph traversal algorithms like Dijkstra can be applied to this graph to find the best slot. However, spectrum mobility is challenging. When a CR user switches its channel, the routing breaks and the routing table needs to be updated. Routing recalculation is a costly and time-consuming process. Therefore, routing calculation becomes a part of the channel handoff process. Instead of recalculating the routing before the handoff, a CR user can prepare a backup channel. The CR user needs to maintain the backup channel periodically so that it can transfer communication links immediately to the backup channel after a handoff-triggering event.

1.7 Security Issues in Cognitive Radio Networks

In the last few years, CRNs have become a promising technology in solveing the spectrum scarcity. However, this network technology has a lot of security challenges. Authors in [18], [19], and [20] describe a lot of security issues and solutions in CRNs. In a primary user emulation attack (PUEA), an attacker

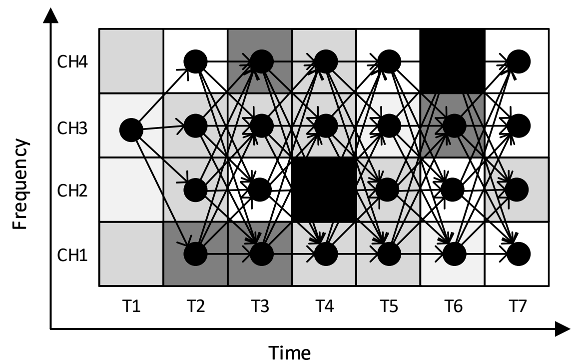

Fig. 1.7 Spectrum search space.

mimics a PU's signal to fool SUs so that they refrain from using the channel. As a result, network congestion and a denial of service happens. To solve the PUEA, classification methods are used to classify whether a signal is from a PU or an attacker. Location verification-based solutions are proposed in [21, 22]. Though a PUEA mimics PU signals, it is very hard to mimic the signal's energy distribution of a PU. Based on this principle, [23, 24] propose solutions which classify signals based on power mean, power variance, and the Walds Sequential Probability Ratio. Usually, all SUs know all PUs' locations. Based on the received signals' power, an SU can determine whether the power level is feasible if the signal comes from the PU's location [25].

The spectrum sensing data falsifying (SSDF) attack is applicable in a cooperative spectrum sensing system with a data aggregation center or fusion center. Malicious SUs (MSU) send false information to data aggregation centers so that other SUs take wrong decisions. In the worst case, MSUs and the benign SUs with the wrong sensing information can win the election. So, it is important to detect the MSUs and exclude them from the voting. Solutions for SSDF attacks are based on clustering the benign SUs to a group and reputation-trust based. Authors in [26, 27], propose two different clustering algorithms based on the hamming distance between the sensing results of different time slots of different SUs. Associative rule mining-based classification is proposed in [28]. Authors propose an apriory algorithm to get a frequent subset of the sensing results from all the SUs. They assume that the MSU will remain in the frequent subset of the sensing result. Based on the probability of PUs' presence, they classified the SUs into benign SUs and MSUs. A trust-based spectrum sensing scheme against SSDF attacks is proposed in [29]. In the proposed method, data aggregation center selects some of the SUs to take local decisions and combines the detection results based on their reliability. Authors in [30] propose a distributed spectrum sensing method. The reputation computed based on the deviation form the majority's decision.

A PU emulation-based testing scheme, FastProbe, is proposed in [31]. FastProbe creates PU signals to test whether the SUs are reporting honestly or not. This detection technique is now ineffective because there are a lot of mechanisms that detect PU emulation signals [32, 33, 34, 35, 25]. These mechanisms are based on distribution, mean, variance of energy, and transmitter localization. So, any MSU can detect the PU-emulated signal from the data aggregation center and report correct results in that time slot to get a high reputation and keep reporting false results in other time slots.

1.8 Applications of Cognitive Radio Networks in LTE and Wi-Fi

Wi-Fi and LTE are the most prominent wireless access technologies nowadays. The migration from PCs to mobile devices leads to an exponential increase of data usage in wireless technologies. The 84.5 MHz of unlicensed spectrum in the 2.4 GHz band which is allocated for Wi-Fi has been saturated, and is unusable for new wireless applications [36]. Therefore, Wi-Fi stockholders have been showing interest in using the 5GHz bands. There is up to 750MHz of unlicensed spectrums in the 5GHz band that falls under the Unlicensed National Information Infrastructure (U-NII) rules of the FCC.

Some LTE stakeholders, including Qualcomm (an American multinational semiconductor and telecommunications equipment manufacturer), are also keenly interested in the 5GHz bands. They proposed extending the deployment of LTE-Advanced (LTE-A) to the 5GHz band using channel aggregation (CA) and supplemental downlink technologies (SDL). Carrier aggregation in LTE-A enables using multiple carriers to provide high data rates. A supplemental downlink is a multi-carrier scheme for enhancing the downlink capacity in Evolved High Speed Packet Access(HSPA+). Some Wi-Fi systems, such as 802.11a and 802.11n, are already operating in 5GHz bands. However, Wi-Fi stakeholders have been lobbying the government for access to more spectrums within the 5 GHz bands. In response, the FCC issued a Notice of Proposed Rule Making (NPRM) 13-22 in 2013 [37] that recommends adding 195 MHz of additional spectrums for use by unlicensed devices. The Wi-Fi Innovation Act was introduced in the U.S. Senate and House [38] recently. This act directs the FCC to conduct tests to assess the feasibility of opening the upper 5 GHz band, including the Intelligent Transportation System (ITS) band, for unlicensed use. ITS stakeholders are very concerned about sharing spectrums with Wi-Fi. They fear that coexistence with Wi-Fi may severely degrade the performance of ITS applications, especially safety applications that are sensitive to communication latency. When the ITS band was first allocated in 1999, the FCC's original intention was for this band to support

Dedicated Short Range Communications (DSRC) for ITS exclusively. As a result, ITS protocol stacks and the relevant applications are not designed to coexist with unlicensed devices. Access to the 5 GHz spectrum has be-

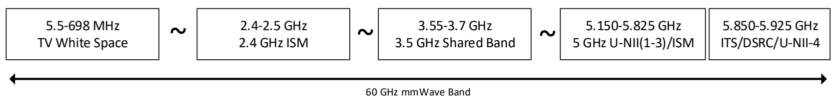

Fig. 1.8 Different bands for wireless applications.

came a cause of contention between the LTE, Wi-Fi, and DSRC stakeholders, but more importantly, the 5 GHz bands have become a proving ground for spectrum sharing between three heterogeneous wireless access technologies: LTE-U, Wi-Fi (802.11ac/802.11ax), and DSRC. Recognizing the importance of this problem, a research opportunity focusing on two coexistence scenarios has opened: the coexistence between LTE-U and Wi-Fi and the coexistence between DSRC and Wi-Fi.

1.8.1 LTE and Wi-Fi Coexistence

Enabling harmonious coexistence between LTE and Wi-Fi in 5 GHz bands is particularly challenging for two main reasons. First, Wi-Fi networks are contention-based, whereas LTE communications are schedule-based. Figure 1.9 shows the basic resource block of LTE. Each user is assigned to a slot in the time and frequency domain of the spectrum. LTE HeNB (LTE base station) does not sense before tranmission. On the other hand, Wi-Fi is a CSMA/CA-based protocol, which means a Wi-Fi device senses before transmission and if the channel is occupied, it does not transmit. As a result, LTE always shows eminent behavior while coxisting with Wi-Fi. In fact, experiments done by Nokia Research [39] show that in coexistence scenarios, the Wi-Fi network is heavily influenced by LTE-U interference. Specifically, the Wi-Fi APs stay on LISTEN mode more than 96% of the time, which causes severe degradation to their throughput. So, the challenge facing LTE and Wi-Fi coexistence is ensuring a fair share between them. There are several studies on ensuring a fair share and coexistence between LTE and Wi-Fi. We discuss some of the approaches next.

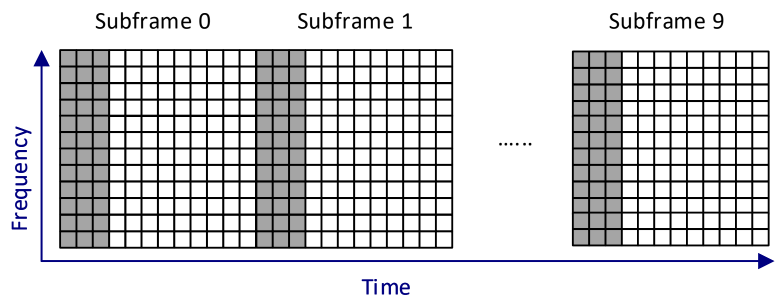

Fig. 1.9 LTE subframe and resource allocation to users.

1.8.1.1 Self Interference Suppression Technology with LTE and Wi-Fi

Wi-Fi and LTE conexistence can be achieved using Self interference suppression (SIS) and Full Duplex (FD) capabilities. The SIS is a technique to remove interference induced by its own transmission. The self-interference cancellation circuits [40] can be used to achieve full duplex capabilities. We consider a coexistence scenario that consists of one or more Wi-Fi networks along with several LTE operators. Each Wi-Fi network is comprised of an 802.11 AP and several Wireless Users (WUs). Figure 1.10 shows the LTE and Wi-Fi coexistence scenario. At the beginning, LTE-U starts the transmission only in the licensed spectrum (without CA). After a while, LTE aggregates an unlicensed channel, f_2, with the licensed spectrum and continues transmission for some time. After that, LTE releases f_2 because of channel quality degradation, and it aggregates another unlicensed channel, f_1. Wi-Fi starts with CSMA/CA activity (sensing the channel) and starts transmission in channel f_1. At the same time, it also starts sensing f_1. When LTE switches channels from f_2 to f_1, the Wi-Fi sensing detects the transmission and releases the channel f_1. Then, Wi-Fi again does CSMA/CA on another channel (f_2) and continues transmitting if the channel is free.

1.8.1.2 Backward Compatibility Approaches

The previous approach focuses on interactions between Wi-Fi and LTE-U and advocates the design of new FD/SIS-based interference mitigation techniques without consideration of the issue of fairness. In this section, we study fair spectrum sharing in heterogeneous systems.

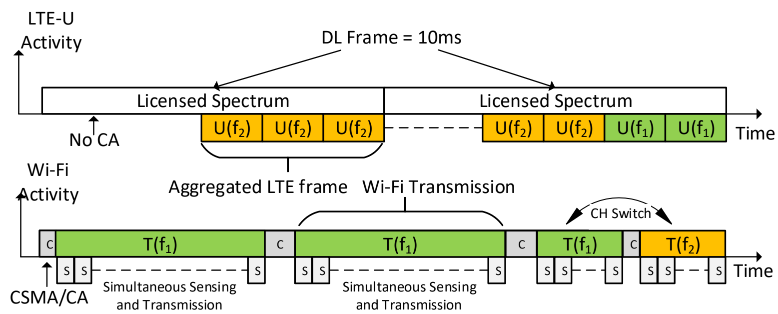

Fig. 1.10 LTE and Wi-Fi activity and channel switching.

Mechanism 1: Indirect Coordination using Carrier Sensing:

In this scenario, there will be no information flow between LTE and Wi-Fi. Wi-Fi and LTE-U may not even know what their fair portions of the spectrum should be. LTE senses the environment and detects the preambles of Wi-Fi and an LTE HeNB determines how many Wi-Fi APs are within its transmission range. Then, the LTE HeNB determines its fair portion of the spectrum based on the number of co-existent Wi-Fi networks. If the LTE-U's spectrum usage so far is larger than its fair portion, then the LTE network will slow down. That is, LTE turns off its transmission for a longer time (i.e., reducing its duty cycle) and lets Wi-Fi transmit more. On the other hand, if the LTE-U's spectrum usage so far is less than its fair portion, it may increase its transmission.

Mechanism 2: Embedding Wi-Fi Information in Preamble:

Fair coexistence between LTE-U and Wi-Fi can be achieved by modifying the Wi-Fi preamble. Only the reserved bits in the preamble can be used for this purpose. Useful information can be embedded in them, and LTE can adjust its operations according to the information; this enables fair usage. There are some options for embedding WiFi usage information in the preamble. There are at least 5 reserved bits that may be used to embed Wi-Fi information. Figure 1.11 shows the Wi-Fi (IEEE 802.11ac) packet format. Based on the information embedded in the Wi-Fi preamble, LTE can adjust its operations accordingly to achieve fairness between the two systems, i.e., the LTE may reduce (or increase) its duty cycle if the Wi-Fi has been using less bandwidth (time) than the fair portion.

			3 reserved bits			2 reserved bits	
L-STF	L-LTF	L-SIG	VHT-SIGA	VHT-STF	VHT-LTF	VHT-SIGB	Data
2-symbols	2-symbols	1-symbols	2-symbols	1-symbols	≥ 1-symbols	1-symbols	N symbols

Fig. 1.11 IEEE 802.11ac packet format.

Mechanism 3: Indirect Communication between LTE and Wi-Fi:

This mechanism can be applied to the scenario where there are some service providers that provide both LTE and Wi-Fi networks. Those service providers' HeNB supports both LTE and Wi-Fi. Suppose provider 1 has both LTE and Wi-Fi networks and provider 2 has only Wi-Fi networks. There can be two kinds of communication. Firstly, indirect communication between provider 1's LTE and provider 1's Wi-Fi. Secondly, communication between provider 1's Wi-Fi AP and provider 2's Wi-Fi AP. The indirect communication may be used for various purposes, such as time synchronization between LTE and Wi-Fi, exchanging spectrum usage information (e.g., aggregated bandwidth, aggregated throughput, or the total air time so far), or for other signaling information to achieve fair spectrum sharing between the two systems.

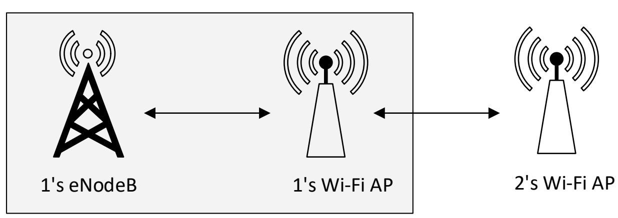

Fig. 1.12 Indirect communication.

1.8.2 Wi-Fi and DSRC Coexistance

The FCC allocates 75 MHz spectrums in the 5.9GHz band for DSRC which is used for vehicle-to-vehicle communications. The DSRC is based on the IEEE 802.11p standard. After the FCC declared the 5.9 GHz unlicensed band (U-NII-4), Wi-Fi could operate in that band. The DSRC remains as a PU and others act as SUs. DSRC's inter-frame space (IFS) parameters are two times longer than 802.11ac/802.11ax. Similarly, the slot time used in the MAC backoff is longer for DSRC (13 μsec) than for 802.11ac/802.11ax (9 μsec). These differences give Wi-Fi effective priority over DSRC when accessing the channel. One solution is changing the IFS values of 802.11ac or 802.11ax so that DSRC gets a higher access priority. For instance, we can increase the values of the Wi-Fi's IFS parameters by adding a DSRC priority time offset value, giving priority to DSRC. Only the IFS adjustment cannot guaratee DSRC's protection. Channelization of U-NII-4 by 802.11ac standards affects DSRC transmissioins significantly. Experiments by the authors of [41] show that if the 802.11ac primary channel remains in the same band as DSRC, then adjusting the DIFS ensures the DSRC's protection. On the other hand, if the primary channel remains in another band and some of the secondary channels remain in the same band as DSRC, adjusting DIFS does not protect the DSRC transmissions.

1.9 Conclusion

Spectrums are a valuable resource in wireless communication systems. The CRN is an excellent method of wireless communication in which underutilized channels are fairly used. The implementation of a CRN includes PU detection, channel choice, channel sharing, channel handoff, and routing reestablishment. Though current mobile devices have hardware that support to operate in 2.4GHz, 5Ghz, GSM, WCDMA, and LTE bands, simultaneous sensing and transmitting is still lacking in them. The promising thing is that most of the physical layers of communication are software managed. Therefore, changing the software may adapt some functionality of CRN and its easier than changing hardware. A lot of changes in the base stations are also required to implement a CRN. Commercial issues inducing usage policies and charges to SUs or cognitive radio operators are also not defined. Therefore, the implementation of a CRN is very complex and expensive. In this chapter, we present the full architecture of CRN at a high level. We discuss applications of a CRN in the 5GHz band for the coexisting Wi-Fi, LTE, and DSRC. We present different mechanisms for ensuring the fair sharing of spectrums between different technologies in the 5GHz band. Therefore, a CRN is an excellent means of wireless communication in which underutilized channels are fairly used.

Acknowledgements

This research was supported in part by NSF grants CNS 1629746, CNS 1564128, CNS 1449860, CNS 1461932, CNS 1460971, and CNS 1439672. We would also like to express our gratitude to the people who provided support, comments, information, proofreading, and formatting.

References

1. M. Yoshimachi and Y. Manabe, "A new aodv route discovery protocol to achieve fair routing for mobile ad hoc networks," in *2016 6th International Conference on Information Communication and Management (ICICM)*, Oct 2016, pp. 222–226.
2. M. Zareei, E. M. Mohamed, M. H. Anisi, C. V. Rosales, K. Tsukamoto, and M. K. Khan, "On-demand hybrid routing for cognitive radio ad-hoc network," *IEEE Access*, vol. 4, pp. 8294–8302, 2016.
3. R. Abdelrassoul, E. Fathy, and M. S. Zaghloul, "Comparative study of spectrum sensing for cognitive radio system using energy detection over different channels," in *2016 World Symposium on Computer Applications Research (WSCAR)*, Mar 2016.
4. I. F. Akyildiz, W. y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 40–48, Apr 2008.
5. A. Wisniewska, "Spectrum sharing in cognitive radio networks: A survey," 2014.
6. K. Kim, I. A. Akbar, K. K. Bae, J. S. Um, C. M. Spooner, and J. H. Reed, "Cyclostationary approaches to signal detection and classification in cognitive radio," in *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Apr 2007.
7. N. Muchandi and R. Khanai, "Cognitive radio spectrum sensing: A survey," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Mar 2016.
8. S. Sinha, S. Mehfiiz, and S. Urooj, "Energy detection of unknown signals over rayleigh fading channel," in *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, Feb 2014.
9. S. K. Rashed, R. Shahbazian, and S. A. Ghorashi, "Spectrum decision in cognitive radio networks using multi-armed bandit," in *2015 5th International Conference on Computer and Knowledge Engineering (ICCKE)*, Oct 2015.
10. J. Martyna, "Green power control in underlaying cognitive radio networks," in *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Nov 2016.
11. H. W. Kuhn, "The hungarian method for the assignment problem," *Naval Research Logistics Quarterly*, vol. 2, 1955.
12. Y. Zhang, "Spectrum handoff in cognitive radio networks: Opportunistic and negotiated situations," in *2009 IEEE International Conference on Communications*, Jun 2009.
13. D. M. Alias and R. G. K, "Cognitive radio networks: A survey," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Mar 2016.
14. I. Christian, S. Moh, I. Chung, and J. Lee, "Spectrum mobility in cognitive radio networks," *IEEE Communications Magazine*, vol. 50, no. 6, Jun 2012.
15. I. A. Akbar and W. H. Tranter, "Dynamic spectrum allocation in cognitive radio using hidden markov models: Poisson distributed case," in *Proceedings 2007 IEEE SoutheastCon*, March 2007.
16. C. H. Park, S. W. Kim, S. M. Lim, and M. S. Song, "Hmm based channel status predictor for cognitive radio," in *2007 Asia-Pacific Microwave Conference*, Dec 2007.
17. Z. Chen and R. C. Qiu, "Prediction of channel state for cognitive radio using higher-order hidden markov model," in *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)*, Mar 2010.
18. J. Li, Z. Feng, Z. Feng, and P. Zhang, "A survey of security issues in cognitive radio networks," *China Communications*, vol. 12, no. 3, Mar 2015.
19. G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Communications Surveys Tutorials*, vol. 14, no. 2, Second 2012.

20. R. K. Sharma and D. B. Rawat, “Advances on security threats and countermeasures for cognitive radio networks: A survey,” *IEEE Communications Surveys Tutorials*, vol. 17, no. 2, Secondquarter 2015.
21. D. Salam, A. Taggu, and N. Marchang, “An effective emitter-source localisation-based puea detection mechanism in cognitive radio networks,” in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Sept 2016.
22. Z. Ma, W. Chen, K. B. Letaief, and Z. Cao, “A semi range-based iterative localization algorithm for cognitive radio networks,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, Feb 2010.
23. Z. Jin, S. Anand, and K. P. Subbalakshmi, “Detecting primary user emulation attacks in dynamic spectrum access networks,” in *2009 IEEE International Conference on Communications*, June 2009.
24. Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Rez, “Modeling primary user emulation attacks and defenses in cognitive radio networks,” in *2009 IEEE 28th International Performance Computing and Communications Conference*, Dec 2009.
25. R. Chen, J. M. Park, and J. H. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, Jan 2008.
26. S. Nath, N. Marchang, and A. Taggu, “Mitigating ssdf attack using k-medoids clustering in cognitive radio networks,” in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2015.
27. K. Rina, S. Nath, N. Marchang, and A. Taggu, “Can clustering be used to detect intrusion during spectrum sensing in cognitive radio networks?” *IEEE Systems Journal*, vol. PP, no. 99, 2017.
28. S. Bhattacharjee, R. Keitangnao, and N. Marchang, “Association rule mining for detection of colluding ssdf attack in cognitive radio networks,” in *2016 International Conference on Computer Communication and Informatics (ICCCI)*, Jan 2016.
29. F. Zeng, J. Li, J. Xu, and J. Zhong, “A trust-based cooperative spectrum sensing scheme against ssdf attack in crns,” in *2016 IEEE Trustcom/BigDataSE/ISPA*, Aug 2016.
30. R. Chen, J. M. Park, and K. Bian, “Robust distributed spectrum sensing in cognitive radio networks,” in *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, Apr 2008.
31. T. Bansal, B. Chen, and P. Sinha, “Fastprobe: Malicious user detection in cognitive radio networks through active transmissions,” in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, Apr 2014.
32. S. Anand, Z. Jin, and K. P. Subbalakshmi, “An analytical model for primary user emulation attacks in cognitive radio networks,” in *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Oct 2008.
33. D. Salam, A. Taggu, and N. Marchang, “An effective emitter-source localisation-based puea detection mechanism in cognitive radio networks,” in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Sept 2016.
34. 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*, May 2010.
35. C. Chen, H. Cheng, and Y. D. Yao, “Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, July 2011.
36. S. R. Group, “The prospect of lte and wi-fi sharing unlicensed spectrum: Good fences make good neighbors,” February 2015.
37. FCC, “Revision of part 15 of the commissions rules to permit unlicensed national information infrastructure (u-nii) devices in the 5 ghz band,” February 2013.

38. H.R.821, "Wi-fi innovation act," https://www.congress.gov/bill/114th-congress/house-bill/821.
39. A. M. Cavalcante, E. Almeida, R. D. Vieira, S. Choudhury, E. Tuomaala, K. Doppler, F. Chaves, R. C. D. Paiva, and F. Abinader, "Performance evaluation of lte and wi-fi coexistence in unlicensed bands," in *2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, Jun 2013.
40. D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*. New York, NY, USA: ACM, 2013.
41. J.-M. J. P. Gaurang Naik, Jinshan Liu, "Coexistence of dedicated short range communications (dsrc) and wi-fi: Implications to wi-fi performance," in *IEEE International Conference on Computer Communications*, June 2017.