Cognitive Radio Networks and Security: A Survey

Feng Wang
GuangDong University of Technology
30 PUBLICATIONS **402** CITATIONS

Cognitive Radio Networks and Security: A Survey

Feng Wang, *Student Member, IEEE*

***Abstract*—In cognitive radio networks (CRNs), cognitive radio (CR) nodes adaptively access the spectrum aiming to maximize the utilization of the scarce resource. Crucial to the successful deployment of CRNs, security issues have begun to receive research interests recently. This article surveys the research advances in CRNs. First, the fundamentals of CRNs including the basic components (*i.e.*, characteristics, opportunistic links, and network architectures), opportunistic spectrum access (OSA), and the inherent issues in CRNs are reviewed. Then, we present the current issues in security for CRNs. The current works on attacks in different layers of CRNs along with the state-of-the-art counter-strategies are investigated in detail.**

***Index Terms*—Cognitive radio networks, security, dynamic spectrum allocation, opportunistic spectrum access.**

I. Introduction

Communication and networking, both of the deepest needs of the human being, is essential to forming social unions, to expressing a myriad of emotions and needs, and it is central to a civilized society. Digital communication [1] and computer networking [2] in engineering have the purpose of providing technological aids to human communication. Recent increases in demand for high quality of service (QoS) ubiquitous digital communication have driven researchers to rethink the implications of the traditional engineering (more bandwidth, more resource, and more of everything, *etc.*) designs and approaches to communications and networking. As a novel communication paradigm, cognitive radio (CR) [3][4] is a key technology that enables dynamic spectrum access networks to utilize the spectrum more efficiently in an opportunistic fashion [5][6][7], and offers a revolutionary perspective in the designs of modern intelligent communication networks [8][9][10]. In a cognitive radio network (CRN), secondary users (SUs), *i.e.*, unlicensed users, are envisioned to be able to sense and analyze their environment, learn from the environment variations, and access the licensed bands to achieve highly reliable communications without interference with the primary users (PUs), *i.e.*, licensed users. Specifically, the main functions of CR technology in CRNs include: (1) *spectrum sensing*, *i.e.*, to determine the available spectrum and detect the presence of PUs; (2) *spectrum management*, *i.e.*, to select the best available channel spectrum sensing to meet users' communication requirements; (3) *spectrum sharing*, *i.e.*, to coordinate access to this channel with other users; and (4) *spectrum mobility*, *i.e.*, to vacate the channel when a PU is detected.

In the past decade, CR and CRNs have been receiving growing attention and extensive research interests. The authors in [11] surveyed the fundamental capacity limits and associated transmission techniques for different wireless network design paradigms based on CR. Spectrum sensing, a first fundamental element in CRNs, was recently surveyed in [12]; Cooperative spectrum sensing in CRNs to enhance the reliability of detecting PUs was reviewed in [13]. The opportunistic spectrum access (OSA) strategies were discussed in [6][7][14]-[15] for CRNs. Recently proposed dynamic spectrum sharing, access, and management schemes have been presented in [16], such as medium access control and scheduling, spectrum handoff, cross-layer design, power control, routing, and cooperation enforcement, *etc*.

Since users in CRNs are intelligent and have the ability to observe, learn, and act to optimize their performance adaptively, *graph theory* and *game theory* are two well-developed tools underpin extensive investigations of networking and users' behaviors [17]. Graph theory is the study of network structure, while game theory provides models of individual behaviors in strategic interaction, such as cooperation and competition. In CRNs, to address the interactions of the dynamics among conditions, resources, environments, and users, A game theoretic modeling is presented that analyzes the behaviors of PUs and SUs. Mechanism design is proposed to suppress the cheating behavior of SUs in open spectrum sharing and accessing by introducing cost functions of users utility.

Because of the interaction and cooperation in CRNs, ensuring security becomes a major and crucial issue. Some users who are attackers are assumed to be malicious, *i.e.*, their goal is to damage the system's functionality, instead of maximizing their own interest. In fact, CRNs are extremely vulnerable to malicious attacks compared to the traditional networks, partly due to SUs' opportunistic access cannot be protected from adversaries. Also, highly dynamic spectrum availability and mobility make it difficult to implement effective security countermeasures. In addition, as CRNs benefit from the technology to adaptively utilize spectrum, the same technology can also be adopted by malicious attackers to launch more complicated and unpredictable attacks. Authors in [10] presented three main themes in the security of CRNs: trust modeling and evaluation, defense mechanism and strategies, and game-theoretically analysis of security. In [18], security threats - *primary emulation* and *spectrum sensing data falsificatin* which destroy the CRNs in distributed spectrum sensing are discussed. An information secrecy game was developed in [19] to foster collaboration between PUs and SUs against eavesdroppers. [20] proposed a channel hopping defense strategy based on the Markov decision process to combat the jamming attacks in CRNs. The authors in [21] gave an overview of the security threats and challenges that CRNs face, along with the current state-of-the-art to detect the

F. Wang is with the Department of Communication Technology Research in SHARP Laboratory of China co., LTD, 201203, Shanghai, China, e-mail: 09210720101@fudan.edu.cn and feng.wang@cn.sharp-world.com.

corresponding attacks.

This article surveys the current advances in CRNs and security for CRNs. In Section II, the fundamentals of CRNs are presented in detail, including basic components in CRNs, opportunistic spectrum access, and several inherent reliability issues in CRNs. Section III overviews the challenges and strategies for the security CRNs. The conclusions are drawn in Section IV.

II. Fundamentals in CRNs

In this section, the fundamentals of CRNs, such as basic components, opportunistic spectrum access, and several inherent reliability issues in CRNs, are reviewed in detail.

A. Basic Components in Cognitive Radio

The main motivation behind CR is to increase the limited-spectrum utilization by allowing SUs to opportunistic access the frequency band actually owned by PUs. CR, built on a software radio platform, is a context-aware intelligent radio potentially capable of autonomous reconfiguration by learning from and adopting to the radio environment [3][4]. CR is a link level technology requiring: reliable sensing information for spectrum utilization, dynamic spectrum access, and possible programmable radio to support, *etc*. So SUs could adjust their transmission to fill in the spectral void, as shown in Figure 1. Authors in [5] presented two main characteristics of CR: *cognitive capability* and *configurability*. The ability to capture or sense the information from its radio environment is referred to as *cognitive capability* of CR; *reconfigurability* of CR is the capability of dynamically adjust operating parameters for the transmitter or/and the receiver without any modifications on the hardware component. Therefore, the cognitive capability provides spectrum awareness whereas reconfigurability enables the radio to be dynamically programmed according to the radio environment.

CR represents a much broader paradigm where many aspects of communication systems can be improved via cognition and networking. When multiple CR devices are interconnected, CRNs are formed along with the existing networks. CRNs open up exciting opportunities to enable and support a variety of emerging applications, ranging from smart grid, public safety and broadband cellular, to medical applications [22], *etc*. Figure 2 gives a simplifed CRN model, which is filled with PUs, SUs, relay nodes, and base stations. Figure 3 shows one opportunistic link window in CRNs. There are two types of (CRN) are being deployed [8] in practice: *centralized* and *distributed*. The centralized network is an infrastructure-based network, where the SUs are managed by secondary base stations which are in turn connected by a wired backbone. In a distributed architecture, SUs communicate with each other in an ad hoc manner. Two SUs who are within communication range can exchange information directly, while the SUs who are not within direct communication range can exchange information over multiple hops. Spectrum sensing operation in distributed architecture is usually performed collaboratively. Collaborative sensing techniques [13] highlight the fact that is the SUs share their relative sensing information, then the overall primary user detection for the cognitive network can be improved. However, these protocols do not consider malicious users in the network.

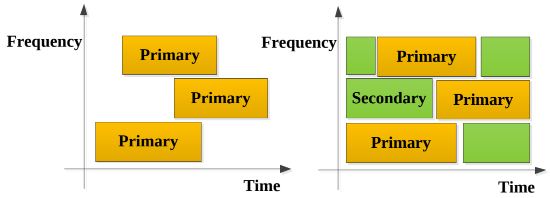

Fig. 1. One of the simplest instance of cognition: a cognitive user senses the time/frequency white spaces and opportunistically transmits over these detected spaces.

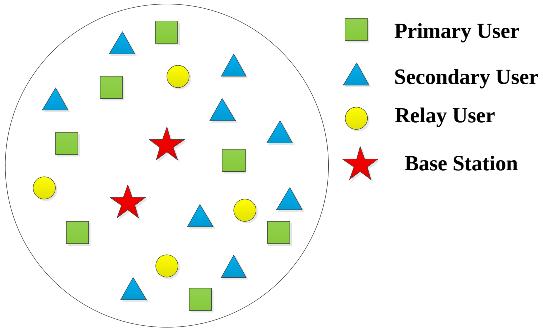

Fig. 2. A simplified cognitive radio network model

Figure 4 shows the CRN terminal architecture. Medium access control (MAC) refers to the policy that controls how a SU should access a licensed spectrum band. Due to the new features of CR networks, such as the collision avoidance with a PU and dynamics in spectrum availability, new medium access protocols need to be designed to address the new challenges in CRNs. A cognitive medium access protocol with stochastic modeling is proposed [23], which enhances the coexistence of CR with WLAN systems based on sensing and prediction. A primary-prioritized Markov approach for dynamic spectrum access is proposed in [15][24], which models the interactions between the PUs and the SUs as continuous-time Markov chains. In order to manage the interference among SUs, or avoid harmful interference to PUs due to secondary spectrum usage, various power control schemes are considered in CRNs to coordinate spectrum sharing [7][12][15].

B. Opportunistic Spectrum Access

Opportunistic spectrum access (OSA) is certainly an important application of CRNs, which include spectrum opportunity

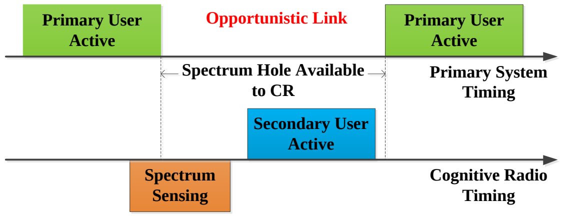

Fig. 3. Opportunistic link in cognitive radio networks

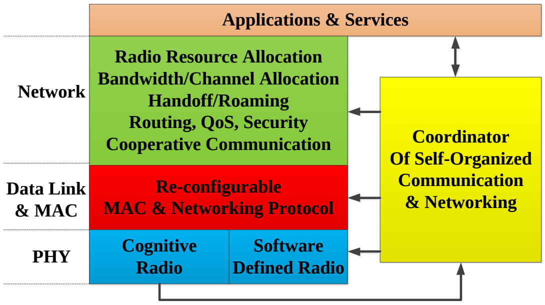
Applications & Services
Network
Radio Resource Allocation
Bandwidth/Channel Allocation
Handoff/Roaming
Routing, QoS, Security
Cooperative Communication
Data Link & MAC
Re-configurable MAC & Networking Protocol
PHY
Cognitive Radio
Software Defined Radio
Coordinator Of Self-Organized Communication & Networking

Fig. 4. Cognitive radio network terminal architecture.

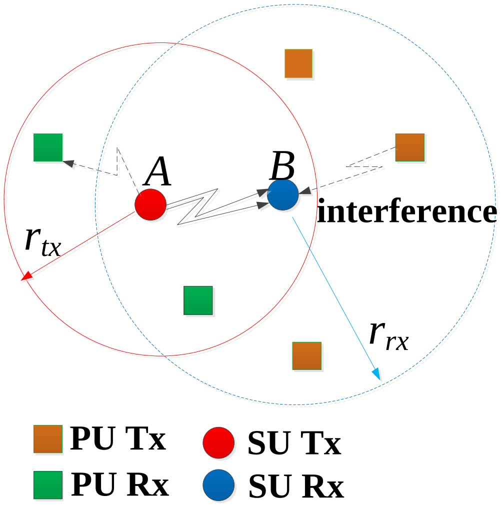

Fig. 5. Illustration of spectrum opportunity (SU A wishes to transmit to SU B, where A should watch for nearby primary receivers and B nearby primary transmitters.)

identification, spectrum opportunity exploitation, and regulatory policy [6]. The overall design objective of OSA is to provide sufficient benefit to SUs while protecting spectrum licensees from interference [7].

Consider a pair of SUs where A is the transmitter and B its intended receiver in Figure. 5. One *channel*[1] is opportunity to A and B if they can communication successfully over this channel while limiting the interference to primary users below a prescribed level determined by the regulatory policy. This means that receiver B will not be affected by primary transmitters, and transmitter A will not interfere with primary receivers. Consider monotonic and uniform signal attenuation and omnidirectional antennas, a channel is an opportunity to A and B if no primary users within a distance of r_{tx} from A are receiving and no primary users within a distance of r_{rx} from B are transmitting over this channel. Clearly, r_{tx} is determined by the secondary users' transmission power and the maximum allowable interference to primary users, while r_{rx} is determined by the primary users' transmission power and the secondary users' interference tolerance. Four classical signal detection techniques [7][12][16] can be employed for spectrum sensing as follows.

1) Energy Detector: Energy detection is the most common type of spectrum sensing because it is easy to implement and requires no priories knowledge about the primary signal. A good detector should ensure a high detection probability P_D and a low false alarm P_F, or it should optimize the spectrum usage efficiency while guaranteeing a certain level of primary user protection. There also exist some challenges in designing a good energy detector. First, the detection threshold depends on the noise power, which may change over time and hence is difficult to measure precisely in real time. Moreover, an energy detector can only decide the primary user's presence by comparing the received signal energy with a threshold; thus, it cannot differentiate the primary user from other unknown signal source.

2) Feature Detector: There are specific features associated with the information transmission of a primary user. In a more general sense, features can refer to any intrinsic characteristics associated with a primary user's transmission, as well as the cyclostationary features. For example, center frequencies and bandwidths extracted from energy detection can also be used as reference features for classification and determining a primary user's presentence. Different from an energy detector which uses time-domain signal energy as test statistics, a cyclostationary feature detector performs a transformation from the time-domain into the frequency-domaiin and then conducts a hypothesis test in the new domain. Specifically, define the cyclic autocorrelation function (CAF of the received signal $y(t)$ by

$$R_y^{\alpha}(\tau) = E[y(t+\tau)y^*(t-\tau)e^{j2\pi\alpha t}], \tag{1}$$

where $E[.]$ is the exprction operation, $*$ denotes complex conjugation, and α is the cyclic frequency. Since periodicity is a common property of wireless modulated signals, while noise is WSS, the CAF of the received signal also demonstrates periodicity when the primary signal is present. Thus, we can represent the CAF using its Fourier series expansion, called the cyclic spectrum density (CSD) function, expressed as

$$S(f,a) = \sum_{r=-\infty}^{\infty} R_y^{\alpha} e^{-j2\pi f\tau}. \tag{2}$$

The CSD function have peaks when the cyclic frequency α equals to the fundamental frequencies of the transmitted signal $x(t)$, *i.e.*, $\alpha = (k/T_x)$ with T_x being the period of $x(t)$.

3) Matched Filtering and Coherent Detection: If secondary users know information about a primary user' signal a priori, then the optimal detection method is the matched filtering, such a matched filter can correlate the already known primary signal with received signal to detect the presence of the primary user and thus maximize the SNR in the presence of additice stochastic noise. Matched filtering requires perfect knowledge of the primary user's signal, such as the operating frequency, bandwidth, modulation type and order, pulse shape, packer format, *etc*.

4) Collaborative Spectrum Sensing: It is known that wireless channels are subject to fading and shadowing. When secondary uses experience multipath fading or happen to be

[1] Here the term *channel* is defined in a broad way, *i.e.*, a channel can be a frequency band with certain bandwidth, a collection of spreading codes in a code division multiple access (CDMA) network, or a set of tones in an orthogonal frequency division multiplexing (OFDM) system..

shadowed, they may fail to detect the existence of primary signal. As a result, it will cause interference to primary users if they try to access this occupied spectrum. To cope with this problem, *collaborative spectrum sensing* [13] is proposed, which combines sensing results of multiple secondary users to improve the probability of primary user detection. Cooperative spectrum sensing can be performed: every CR performs its own local spectrum sensing measurements independently and then makes a binary decision on whether the PU is present or not; all of the CRs forward their decisions to a common receiver; the common receiver fuses the CR decisions and makes a final decision to infer the absence or presence of the PU. The performance of *hard-decision* combining scheme and *soft-decision* combining scheme is investigated. In these schemes, all SUs send sensing reports to a common decision center. Cooperative sensing can also be done in a distributed way, where SUs collect reports from their neighbours and make the decision individually. One collaborative scheme is based on graph coloring, where a topology-optimization allocation algorithm is used for a *fixed* topology. For *mobile* CRNs, a distributed spectrum allocation based on local bargaining is proposed, where mobile users negotiate spectrum assignment within local self-organized groups. For resource-constrained cognitive devices, a rule-based spectrum management is proposed, where SUs access spectrum according to some predetermined rules and local spectrum observations.

The OSA strategies [14][23][15] can be broadly categorized under three models: dynamic exclusive model, open sharing Model, and hierarchical access model. The dynamic exclusive model maintains the basic structure of the current spectrum regulation policy: Spectrum bands are licensed to services for exclusive use. The main idea is to introduce flexibility to improve spectrum efficiency. Two approaches have been proposed under this model: spectrum property rights and dynamic spectrum spectrum allocation. Based on an exclusive-use model, these approaches cannot eliminate white space in spectrum resulting from the burst nature of wireless traffic. Open sharing model employs open sharing among peer users as the basis for managing a spectral region. Advocates of this model draw support from the phenomenal success of wireless services operating in the unlicensed industrial, scientific, and medical (ISM) radio band (*e.g.*, WiFi). The underlay approach imposes severe constraints on the transmission power of secondary users so that they operate below the noise floor of primary users. By spreading transmitted signals over a wide frequency band (UWB), secondary users can potentially achieve short-range high data rate with extremely low transmission power. Based on a worst-case assumption that primary users transmit all the time, this approach does not rely on detection and exploitation of spectrum white space. Spectrum overlay was first envision by Mitola under the term spectrum pooling and then investigated by the DARPA Next Generation (XG) program under the term *opportunistic spectrum access*. Differing from spectrum underlay, this approach does not necessarily impose severe restrictions on the transmission power of secondary users, but rather on when and where they may transmit. it directly targets at spatial and temporal spectrum white space by allowing secondary users to identify and exploit local and instantaneous spectrum availability in a nonintrusive manner [20][21].

Compared to the dynamic exclusive use and open sharing models, this hierarchical model is perhaps the most compatible with the current spectrum spectrum management policies and legacy wireless systems. Furthermore, the underlay and overlay approaches can be employed simultaneously to further improve spectrum efficiency.

Due to noise uncertainty, shadowing, and multipath effect, detection performance of single user sensing is pretty limited. Cooperative sensing [13][23][24] has been consider effective in improving detection accuracy by takeing advantage of the spatial and multi-user diversity. In cooperative spectrum sensing, how to select proper users for information, and how to perform distributed spectrum sensing are issues worth studying.

C. Inherent Reliability Issues in CRNs

1) High Sensitivity to Primary User Signals: To prevent interference to licensed PUs, SUs should detect the primary transmissions in the first place. There are two prominent ways to detect the PUs transmissions: (a) energy-based and (b) waveform-based sensing. Energy-based sensing does not require any knowledge of the PU transmission signal, it is based on the simple fact that any information-baring signal has finite signal strength. However, energy-based sensing techniques are prone to false detections and usually take a longer time when the signal is low power. Waveform-based sensing is applied when information about the waveform and signal patterns of the PUs transmission signal is known, which makes the waveform-based sensing techniques perform better than energy-based sensing in terms of speed and reliability.

2) Unknown Primary Receiver Location: One issue that has received very little attention so far is the lack of knowledge of the primary receivers' location. In order to minimize the interference to the PU network. the secondary transmitters need to know the locations of the primary receivers. Most of the interference models proposed to minimize interference temperature, but the primary receivers' location is unknown. This may lead to hidden terminal problems in CRNs.

3) Synchronization Requirement: The SUs in centralized CRNs perform fast sensing operations between periods of transmissions. Therefore, synchronization of secondary users in time is an important requirement to detect the presence of PUs.

III. Security in CRNs

One of the fundamental requirements for any type of a network is *security*. This section presents the issue of security in CRNs, describes the security requirements, and reviews the attacks against CRNs along with the current state-of-the-art techniques to detect or/and combat the corresponding attacks. Compared to traditional networks, security in CRNs becomes a crucial and challenging issue, since more chances are exposed to attackers due to the introduction of CR. Most of the attacks (*e.g.*, denial of service (DoS), jamming, and butter overflow attacks, *etc.*) on network queues are all targeted towards rendering the network unavailable either temporarily or permanently. The research future of security in CRNs is also presented.

A. Security Requirements in CRNs

As the continuous evolution of networks and mobile applications, Security requirements play an increasingly important role in any type of networks. For CRNs [9], some security requirements are supposed to be considered besides the requirements [21] in general wireless networks due to SUs access the spectrum belonged to PUs in an opportunistic fashion. Such security requirements in CRNs are presented below.

- *Availability*: This is the availability of data (user information, routing tables,transmission medium *etc.*) users in networks. In the context of CRNs, availability refers to the ability of PUs and SUs to access the spectrum. Specially, PUs are able to transmit in licensed band without harmful interference from SUs, and the chunks of spectrum are available for SUs' opportunistic use without causing harmful interference to the PUs. In centralized cognitive networks, availability also refers to the availability of secondary base stations. Security mechanisms should ensure that DoS attacks against secondary base stations are appropriately countered.
- *Integrity*: Integrity is an assurance that the data received is exactly as sent by an authorized entity, which is extremely important in wireless networks due to the wireless medium is easily accessible to intruders. Adding an additional layer of security at the link layer could be employed in CRN to make the wireless links as secure as the wired links.
- *Identification*: Identification is one of the basic security requirements for any communication device, which is a method to associate a user/device with their name or identity, *e.g.*, in cellular networks, the mobile devices are provided with an equipment identification called international mobile equipment identifier (IMEI). This identifier is used to uniquely identify the mobile devices in the cellular networks. Similarly, a tamper-proof identification mechanism should be built into the SUs' devices in CRNs.
- *Authentication*: Authentication is an assurance that the communicating entity is the one that it claims to be, which is mainly to prevent unauthorized users from gaining access to protected systems. Most of the mechanisms that ensure authentication rely on a centralized certificate authority(CA), where CA is trusted by all the users in the network. A typical authentication protocol would require the peer entities to get their identities signed (using public key encryption) by the CA and the digitally signed certificates are exchanged and verified by the peers to ensure authenticity. Once the authenticity of peers is established, regular communication is initiated. CRNs have an inherent requirement to distinguish between PUs and SUs. Therefore, authentication can be considered as one of the basic requirements for CRNs. However, for distributed CRNs with multiple SUs dispersed over a large geographical area, providing the functionalities of a CA can be quite a challenge. In CRNs, conditional authorization is proposed due to that the SUs are authorized to transmit in licensed bands only as long as they do not interfere with PUs' communications. As it is difficult to pinpoint exactly which of the SUs is responsible for harmful interference to the PUs' transmission, this type of authorization is difficult to enforce and even more so in a distributed setting.
- *Confidentiality*: Confidentiality assures that the data is transformed unintelligible to an unauthorized entity, which is achieved by employing ciphers and encrypting the data to be transmitted with a secret key which is share only with the recipients. The encrypted data is then transmitted and only the recipients with a valid key can decrypt and read the data.

In short, multiple consideration factors are need to be considered when security is investigated in CRNs due to the characteristics of CR implementation, such as the flexible access of frequency spectrum and unscheduled appearances of different PUs. Therefore, special security requirements and issues need be taken into account especially.

B. Attacks on CRNs

Crucial to the successful deployment of CRNs, security issues [21][25] have begun to receive research interests recently. Defining an attack on CRNs as any activity that results in (a) unacceptable interference to the licensed PUs or (b) missed opportunities for SUs. Security threats [18] related to the cognitive capability include attacks launched by adversaries that mimic primary transmitters (*i.e.*, primary emulation), and transmission of false observations related to spectrum sensing (*e.g.*, data falsification), and reconfiguration can be exploited by attackers through the use of malicious code installed in CRs. An attack is considered strong if it involves a minimal number of adversaries performing minimal operations but causing maximum damage/loss to the PUs and/or SUs. Primary emulation, spectrum sensing data falsification attacks, and attacks of five layers in the protocol stack [8], *i.e.*, the physical layer, link layer, network layer, transport layer and application layer are presented as bellows.

1) Primary Emulation: When a PU is detected in a given band, all SUs avoid accessing that band. In primary emulation (PE) attack, a malicious SU tries to gain priority over other SUs by transmitting signals that emulate the characteristics of a PU. An adversary may have two different motives for launching PE attacks: *selfish* and *malicious*. Selfish motivation is to gain an unfair advantage in accessing spectrum in the spectrum sharing paradigm of DSA. Because SUs will avoid accessing a band if an incumbent signal is detected in the band. an attacker can preempt and monopolize a band if it manages to fool others into believing that it is an PU. The malicious motivation is to suppress legitimate SUs from accessing spectrum, thereby causing Dos. Both types of PE attacks can drastically decrease the available bandwidth opportunities that each legitimate SU can detect.

2) Spectrum Sensing Data Falsification (SSDF): An attack may send false location spectrum sensing results to a data collector, causing the data collector to make a wrong spectrum-sensing decision [24]. Shadow fading can cause the ”hidden node” problem where a SU fails to detect primary transmissions, although it is located within the transmission range of a primary network. The data fusion sums all of the collected local spectrum-sensing results using the techniques of *Bayesian detection* or *Neyman-Pearson test*, which share two properties in common that contribute to their vulnerability to SSDF attacks. First, these techniques treat all sensing terminals indiscriminatingly, regardless of whether a sensing terminal is reporting true or false sensing data. Secondary, both techniques cannot guarantee both a bounded false alarm probability and a bounded miss detection probability.

3) Physical Layer Attacks: The physical (PHY) layer is the most basic layer in the protocol stack, which provides the means of transmitting raw signals over the transmission medium, and determines the bit rate, channel capacity, bandwidth and maximum throughput of the connection. In CRNs, the PHY layer has the capability to transmit at various frequencies across most of the spectrum band. Jamming attacks from the malicious attacks, the major threats in PHY layer for CRNs include *intentional jamming* and *primary receiver jamming*.

In order to prevent interference to the primary network, some PUs detection techniques have higher sensitivity toward s primary transmissions, which leads to frequent false detections and missed opportunities for the SUs. A malicious entity can amplify the sensitivity and hence the number of missed opportunities by replaying the primary transmissions. what makes this attack more lethal is that even an adversary with low transmit power can transmit in spectrum band boundaries and still cause multiple SUs operating in multiple spectrum bands to incur missed opportunities and render spectrum usage inefficient. In both centralized and distributed CRNs, multiple secondary networks may coexist over the same geographical region. In such cases, transmissions from malicious entities in one network can cause harm to the primary and secondary users of the other network. This type of attack is hard to prevent because the malicious entities may not be under the direct control of the secondary based station/users of the victim network.

4) Link Layer Attacks: This is the second layer in the network protocol stack. The main purpose of the link layer is to transfer data from one node to the next node in one hop, which provides the functional means to allow fragmentation of data, error correction and modulation. The medium access control (MAC) layer is one of the important sublayers of the link layer, which controls channel assignment. Fairness is one of the primary requirements for channel assignment protocols. In CRNs, besides signal-to-noise ratio (SNR), other parameters such as holding time, interference, path loss, wireless link error rate and delay are just as important as the SNR. For this reason, channel assignment is a more complex operation in cognitive networks. For protocols that rely on SUs exchanging information, false feedback from one or a group of malicious users could make other secondary users take inappropriate actions and violate the goals of the protocol.

5) Network Layer Attacks: The network layer provides functional means for performing routing, flow control and ensuring quality of service (QoS). Routing refers to selecting path along the network through which data is transmitted from source to destination. While the data link layer is responsible for node-to-node packet delivery, the network layer is responsible for end-to-end packet delivery. When a connection needs to be established, every node determines which of its neighbours should be the next link in the path towards the destination. Every node in the network is responsible for maintaining routing information about its neighbouring nodes. A malicious node in the path can disrupt routing by either broadcasting incorrect routing information to its neighbours or by redirecting the packets in the wrong direction. *Routing attacks* can be classified into two categories: routing disruption attacks and resource consumption attacks. *Network endo-parasite attack* attempts to increase the interference at heavily loaded high priority channels. Most of the time, the affected links are along the routing path through the malicious nodes towards the wired gateway. Under normal channel assignment operation, a node assigns the least loaded channels to its interfaces and transmits the latest information to its domain neighbours. However, it does not inform its neighbors about this change, which results in hidden usage internal/hidden parasites. The links using these channels experience interference, decrease in available bandwidth and continuous degraded performance.

6) Transport Layer Attacks: The transport layer provides functional requirements to transfer data between two end hosts. It is primarily responsible for flow control, end-to-end error recovery, and congestion control. There are two main protocols that operate in the transport layer, the User Datagram Protocol (UDP) and the Transport Control Protocol (TCP). UDP is connectionless while TCP is connection oriented and guarantees ordered packet delivery. TCP performance is usually measured by a parameter called round trip time (RTT). In CRNs, highly frequent spectrum band changes by SUs due to spectrum handoff at the link layer increases RTT, which could be exploited by malicious users.

7) Application Layer Attacks: The application layer is the final layer of the communication protocol stack, which provides application for users of the communication devices. Some of the basic application layer services include file transfer protocol (FTP), Telnet, email and lately multimedia streaming. Protocols that run at the application layer rest on the services provided by the layers below it. Therefore, any attack on physical, link, network or transport layers impact adversely on the application layer. One of the most important parameters in the application layer is the quality of service (QoS). This is especially important for multimedia streaming applications. Physical and link layer delays due to spectrum handoffs, unnecessary rerouting and stale routing due to network layer attacks and delays due to frequent key exchanges cause degradation of the QoS in the application layer protocols.

8) Cross-layer Attacks: Cross-layer attacks are referred to that malicious operations performed at one layer to cause security violations at another layer. In CRNs, there is an inherent need for greater interaction between the different layers of the protocol stack, which is why cross-layer attacks need to be given special attentions in CRNs. For example, *Jellyfish attack* is performed at the network layer but it affects the performance of the transport layer, specially reduces the throughput of the TCP protocol. There are three variants of this attack: misordering, dropping and delay variance. *Routing information jamming attack* makes use of the lack of a common control channel in CRNs and the spectrum handoff delay to jam the exchange of routing information among neighbouring nodes. The attack is initiated when a malicious node causes spectrum handoff in the victim node just before routing information is exchanged. When this happens, the victim node stops all ongoing communication, vacates the spectrum band, opportunistically selects a new spectrum for transmission, scans the entire spectrum band to identify the neighboring nodes and informs the neighboring nodes of the new frequency. This attack can be extended by performing spectrum handoff attacks on the victim node successively just before routing information exchange.

C. Counter-Strategies Against Attacks in CRNs

In the scenario where both the SUs and attackers are equipped with a single radio and access only one one channel at any time, the SU hops proactively between channels as the defense strategy. In [25], Markov decision process-based hopping is a good approximation to the game equilibrium. Moreover, in order to gain knowledge about the adversaries, learning schemes are proposed for the secondary user based on maximum likelihood estimation and Q-learning. SUs can exploit the flexible access to multiple channels as the means of anti-jamming defense [14][25], where a jamming game was formulated with the transmission cost considered, and generalized water-filling was proved to be the unique Nash equilibrium. The blocking probability was analyzed for different kinds of attack strategies and defense strategies. Besides, an uncoordinated frequency hopping scheme was developed where a transmitter and several receivers followed their own hopping patterns to mitigate the jamming impact, and communication link was established when the transmitter and a receiver happened to choose the same unjammed channel. However, the problem becomes more complicated in a cognitive radio network where PUs' access has to be taken into consideration.

The key to defending against PE attacks is to devise a robust technique for verifying the authenticity of an incumbent signal. An energy detector infers the existence of an incumbent based on the measured signal energy level. Obviously, the energy detection cannot distinguish primary signals and secondary signals. An improved scheme proposed suggests the use of periodic *quiet period*. To facilitate spectrum sensing during a quiet period, all SUs refrain from transmitting. When quiet periods are observed by all SUs, detecting PUs becomes straightforward– that is, any terminal whose received signal energy level is beyond a given threshold can be considered an primary transmitter. However, such a detection strategy breaks down completely when malicious SUs deliberately transmit during quiet periods. Signal feature detection is an alternative technique that uses either cyclostationary feature detection or matched filter detection to capture special characteristics of a primary signal. However, relying sole on signal feature detection may not be sufficient to reliably distinguish an incumbent's signal from those of an attacker. One naive approach for verifying PUs is simply to embed a signature in a primary signal. Another method is to employed an authentication protocol between a primary transmitter and a verifier.

Location-based schemes utilize both the location information of the primary transmitter and the received signal strength characteristics (RSS). This approach consists of three phases: verification of signal characteristics, received signal energy estimation, and localization of the transmitter. Based on the distribution of the RSS values, a decision is made about if the transmitter is an primary transmitter or an attacker. Here, the location of the primary transmitter has to be known a priori. Performing energy detection by SUs has three advantages: (i) it is easily implemented; (ii) a sophisticated attacker can emulate several characteristics of the primary signal such as cyclostationary characteristics and modulation, thus it would be more difficult for a SU to detect the attack when using the matched filter or the cyclostationary spectrum sensing approach, and (iii) the method proposed here can be extended for the other spectrum sensing methods.

It is proposed to develop defense solutions against one or multiple malicious SUs in soft-decision reporting collaborative spectrum sensing. The *suspicious level* of each node is estimated by their reporting histories. When the suspicious level of a node goes beyond certain threshold, it will be considered as malicious and its report will be excluded in decision-making. The idea is to detect malicious users in a batch-by-batch way. The nodes are classified into two sets, honest set and malicious set. Initially all users are assumed to be honest. When one node is detected to be malicious according to its accumulated suspicious level, it will be moved into malicious set. The way to calculate suspicious level will be updated when the malicious node set is undated. This procedure continues until no new malicious node can be found.

D. Future Directions

In this subsection, some future directions are provided that need to be taken to make secure cognitive radio network against both accidental and intentional attacks [8][10].

1) Using Existing Security Protocols: Security services provided in cellular, WLAN and wireless ad hoc networks can be applied to CRNs as well. It is the last hop between the wireless base stations and the wireless terminals that needs to be protected over the air. As cellular networks are centralized, security solutions in existing cellular networks could be used as a model to provide security in CRNs. In distributed networks, SUs communicate with each other over one or more hops. These types of networks usually employ a two-level security mechanism: one level of security is provided at the link layer to protect every hop of communication, and the other level of security is employed at the network/transport or application layer to protect the end-to-end communication path. Two most complicated operations in ad hoc wireless networks are *key management* and *secure routing*.

2) Using Cryptographic Primitives: Most of the attacks performed at the link layer involve a malicious entity masquerading as a primary user. Therefore primary user identification is very important for both centralized and decentralized cognitive networks. A digital signature based primary user identification mechanism that can be used by secondary users to distinguish malicious transmissions from primaries has been proposed recently. Further research in the use of cryptographic primitives to solve inherent security issues in cognitive network needs to be performed.

3) Reactive Security Mechanisms: Reactive security mechanisms that detect malicious activity in cognitive networks need to be developed. For example, mechanisms that can detect unusually high spectrum handoff is useful to prevent jamming and spectrum handoff attacks. Detection mechanisms combined with non-repudiation mechanisms enable secondary users to identify and block malicious users from the network.

4) Spectrum Aware Approach: There are two ways to handle spectrum mobility and associated delays. One is to make spectrum sensing, analyzing and handoff process fast and transparent to the higher protocols. Another approach is a cross-layer methodology to incorporate spectrum mobility as state information in protocols operating in upper layers. Although this approach increases cross-layer dependencies, it will make the entire communication protocol spectrum aware and hence better defend some of the attacks on the upper layer protocols in CRNs.

IV. Conclusion

As a new paradigm, CR has offered a revolutionary perspective in engineering designs and approaches to communications and networking. The CRNs and security have received extensive research in recent years. The article presents a brief literature review on CRNs and security in CRNs. The fundamentals of CRNs including the basic components (*i.e.*, characteristics, opportunistic link, and network architecture), OSA, and the inherent issues in CRNs have been presented. Due to new characteristics of CR, CRNs face several unique security challenges compared to traditional networks. The research topics of security in CRNs have also been reviewed, including security requirements, attacks on different layers, the corresponding counter-strategies, and the future directions. However, since there is no consensus notion of a security mechanism and strategies in CRNs, many research issues in this area are still open, such as trust modeling and evaluation, defense mechanism and strategies, and theoretic analysis of security, *etc*.

Acknowledgment

The author gratefully acknowledges the advice from Prof. Yu Zhu in Fudan University (China) and Shunqiao Sun in Rutgers University (U.S.). The author would also like to thanks his colleagues for their helpful comments in the development of this article.

References

[1] R. G. Gallager, *Principles of Digital Communications*. UK: Cambridge University Press, 2008.

[2] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed. USA: Prentice Hall, 2011.

[3] J. Mitola and G. Q. Maguire, “Cognitive radio: making software radios more personal,” *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13 –18, Aug. 1999.

[4] S. Haysin, “Cognitive radio: brain-empowered wireless communications,” *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201 –220, Feb. 2005.

[5] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, “Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey,” *Computer Networks*, vol. 50, no. 13, pp. 2127 – 2159, 2006.

[6] Q. Zhao and B. Sadler, “A survey of dynamic spectrum access,” *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 79 –89, May 2007.

[7] E. Hossain, D. Niyato, and Z. Han, *Dynamic Spectrum Access and Management in Cognitive Radio Networks*. UK: Cambridge University Press, 2009.

[8] Q. H. Mahmoud, C. N. Mathur, and K. P. Subbalakshmi, *Cognitive Networks: Towards Self-Aware Networks*. USA: John Wiley & Sons, May 2007.

[9] N. Devroye, M. Vu, and V. Tarokh, “Cognitive radio networks,” *IEEE Signal Process. Mag.*, vol. 25, no. 6, pp. 12 –23, Nov. 2008.

[10] K. J. R. Liu and B. Wang, *Cognitive Radio Networking and Security: A Game Theoretical View*. UK: Cambridge University Press, 2011.

[11] A. Goldsmith, S. Jafar, I. Maric, and S. Srinivasa, “Breaking spectrum gridlock with cognitive radios: An information theoretic perspective,” *Proc. IEEE*, vol. 97, no. 5, pp. 894 –914, May 2009.

[12] T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” *IEEE Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 116 –130, 2009.

[13] K. Ben Letaief and W. Zhang, “Cooperative communications for cognitive radio networks,” *Proc. IEEE*, vol. 97, no. 5, pp. 878 –893, May 2009.

[14] A. El-Sherif, A. Sadek, and K. J. R. Liu, “Opportunistic multiple access for cognitive radio networks,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 704 –715, Apr. 2011.

[15] A. Anandkumar, N. Michael, and A. Tang, “Opportunistic spectrum access with multiple users: Learning under competition,” in *Proc. IEEE International Conference on Computer Communication (INFOCOM)*, San Diego, USA, Mar. 2010.

[16] B. Wang and K. J. R. Liu, “Advances in cognitive radio networks: A survey,” *IEEE J. Sel. Topics Signal Process.*, vol. 5, no. 1, pp. 5 –23, Feb. 2011.

[17] D. Easley and J. Kleinberg, *Networks, Crowds, and Markets: Reasoning about a Highly Connected World*. UK: Cambridge University Press, 2010.

[18] R. Chen, J.-M. Park, Y. Hou, and J. Reed, “Toward secure distributed spectrum sensing in cognitive radio networks,” *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50 –55, Apr. 2008.

[19] Y. Wu and K. J. R. Liu, “An information secrecy game in cognitive radio networks,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 831 –842, Sept. 2011.

[20] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, “Anti-jamming games in multi-channel cognitive radio networks,” vol. 30, no. 1, pp. 4 –15, Jan. 2012.

[21] A. Fragkiadakis, E. Tragos, and I. Askoxylakis, “A survey on security threats and detection techniques in cognitive radio networks,” *IEEE Commun. Surveys Tuts.*, vol. PP, no. 99, pp. 1 –18, 2012.

[22] J. Wang, M. Ghosh, and K. Challapali, “Emerging cognitive radio applications: A survey,” *IEEE Commun. Mag.*, vol. 49, no. 3, pp. 74 –81, Mar. 2011.

[23] S. Huang, X. Liu, and Z. Ding, “Opportunistic spectrum access in cognitive radio networks,” in *Proc. IEEE International Conference on Computer Communication (INFOCOM)*, Phoenix, USA, Apr. 2008, pp. 1427 –1435.

[24] D. Niyato and E. Hossain, “Competitive spectrum sharing in cognitive radio networks: a dynamic game approach,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2651 –2660, Jul. 2008.

[25] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, “Anti-jamming games in multi-channel cognitive radio networks,” *IEEE J. Sel. Areas Commun.*, vol. 30, no. 1, pp. 4 –15, Jan. 2012.