A Comprehensive Review and Analysis of Solutions for Different Layers of the TCP/IP Layer Stack and Security Issues for Cognitive Radio Networks

Natarajan Meghanathan

Department of Computer Science, Jackson State University
Jackson, MS 39217, USA

Corresponding Author Email: natarajan.meghanathan@jsums.edu

Abstract

A cognitive radio network (CRN) is composed of both the secondary users with CR-enabled radios and the primary users whose radios need not be CR-enabled. In this paper, we provide an exhaustive analysis of the issues and the state-of-the-art literature solutions available for the following four layers of the TCP/IP protocol stack, in the context of CRNs: physical layer (spectrum sensing), medium access control, routing, and transport layers. We discuss the various techniques/mechanisms/protocols proposed for each of these four layers, in the context of CRNs. In addition, we discuss several security attacks that could be launched on CRNs and the countermeasure solutions proposed to avoid or mitigate them. This paper would serve as a good comprehensive review and analysis of all the critical aspects for CRNs as well as would lay a strong foundation for someone to further delve onto any particular aspect in greater depth.

Keywords: *Cognitive Radio, Secondary User, Spectrum Sensing, MAC Protocols, Routing Protocols, Transport Layer Protocols, Security Attacks and Solutions.*

1. Introduction

A cognitive radio is defined as a radio that can change its transmitter parameters based on the interaction with the environment in which it operates [1]. A cognitive radio (CR) has the ability (cognitive capability) to sense and gather information (such as the transmission frequency, bandwidth, power, modulation, etc) from the surrounding environment [2] as well as has the ability (reconfigurability) to swiftly adapt the operational parameters, for optimal performance, according to the information sensed [3]. With the above features, the cognitive radio technology is being perceived as the key enabling technology for the next generation dynamic spectrum access networks that can efficiently utilize the available underutilized spectrum allocated by the Federal Communications Commission (FCC) to licensed holders, known as *primary users*. Cognitive radios facilitate a more flexible and comprehensive use of the limited and underutilized spectrum [4] for the *secondary users*, who have no spectrum licenses.

Cognitive radios enable the usage of temporally unused spectrum, referred to as *spectrum hole* or *white space* [3], and if a primary user intends to use this band, then the secondary user should seamlessly move to another spectrum hole or stay in the same band, altering its

transmission power level or modulation scheme to avoid interfering with the primary user. Traditional spectrum allocation schemes [5] and spectrum access protocols may no longer be applicable when secondary unlicensed users coexist with primary licensed users. If secondary users are allowed to transmit data along with primary users, the transmissions should not interfere with each other beyond a threshold. On the other hand, if secondary users can transmit only in the absence of primary users, then a secondary user transmitting data in the absence of a primary user should be able to detect the reappearance of the primary user and vacate the band. There is a significant amount of research currently being conducted and more need to be performed to develop new spectrum management approaches related to cognitive radio for both spectrum sensing and dynamic spectrum sharing.

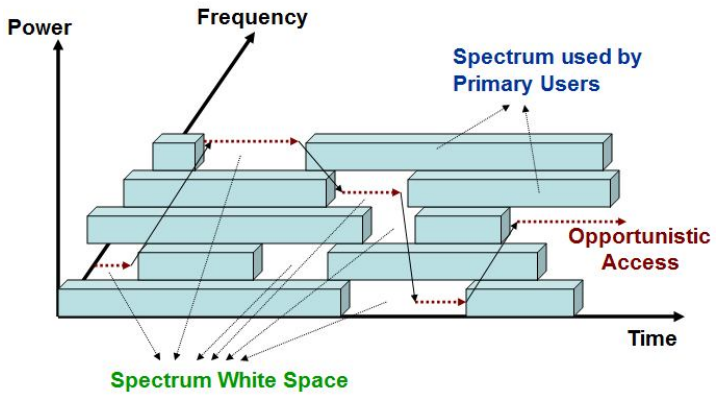

Fig 1: Spectrum Usage – Opportunistic Access of Spectrum White Space and Channel Switching by a Cognitive Radio User

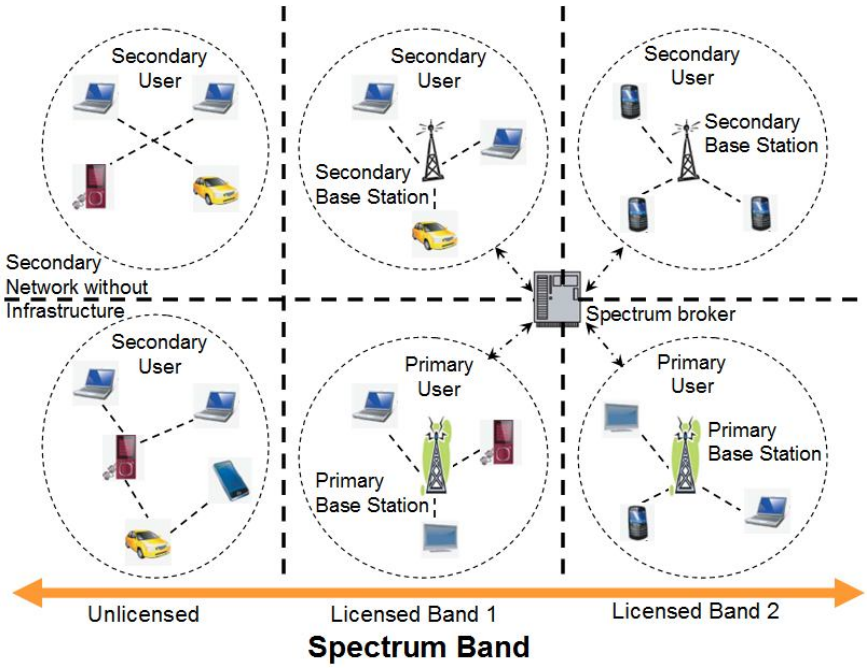

Fig 2: A Cognitive Radio Network Architecture with Primary and Secondary User Networks

A cognitive radio network architecture (Figure 2) includes components corresponding to both the secondary users (secondary network) and the primary users (primary network). The secondary network is composed of a set of secondary users with or without a secondary base station, all of which are equipped with CR functions. A secondary network with a base station is referred to as the infrastructure-based CR network; the base station acts as a hub collecting the observations and results of spectrum analysis performed by each CR secondary user and deciding on how to avoid interference with the primary networks. As per this decision, each CR secondary user reconfigures his communication parameters. A secondary network without a base station is referred to as the infrastructure less – cognitive radio ad hoc network (CRAHN). In a CRAHN, the CR secondary users employ cooperation schemes to exchange locally observed information among the devices to broaden their knowledge on the entire network, and decide on their actions based on this perceived global knowledge. A primary network comprises of primary users and one or more primary base stations, all of which are in general not equipped with CR functions. Hence, if a secondary network shares a licensed spectrum band with a primary network, the secondary network is required to be able detect the presence of a primary user and direct the secondary transmission to another available band that will not interfere with the primary transmission. Figure 1 illustrates the opportunistic access of the spectrum white space and switching of the frequency bands by a CR secondary user at the incidence of use by a primary user. Figure 2 illustrates cognitive radio network architecture with both the primary user network and the secondary user network (with and without infrastructure – base station support).

The current spectrum allocation and sharing schemes according to three criteria: (1) Spectrum bands in use by a CR user; (2) Network architecture and (3) Access behavior of CR users.

- **Classification based on Spectrum Bands used by the CR User:** Based on the spectrum bands in use by a secondary user, the spectrum sharing scheme could be classified as open spectrum sharing and hierarchical spectrum access model. In the open spectrum sharing model, the secondary users access the unlicensed spectrum band and no user owns any spectrum license; hence, all users have the same access rights in using the unlicensed spectrum. In the hierarchical spectrum access model [22], the secondary users share the licensed spectrum bands with the primary users. Since primary users need not be equipped with cognitive radio, they have all the priority is using the spectrum band. Hence, when a primary user reclaims a spectrum band for use, the secondary users currently using the spectrum band and the near by bands will have to adjust their operating parameters (such as power, frequency and bandwidth) to avoid interrupting the primary users. The hierarchical spectrum access model can be further divided into two categories, depending on the access restrictions on the secondary users:
  - ***Spectrum underlay*:** With this model, the secondary CR users coexist along with the primary users, and use the licensed spectrum band without exceeding the interference temperature limit/threshold. If primary users transmit data all the time in a constant mode, there is no need for the secondary CR users to detect for available spectrum band; instead, they can just continue to use the spectrum (of course, only for short-range communication, as explained in Section 2.3).
  - ***Spectrum overlay*:** With this model, the secondary CR users can only use the licensed spectrum when the primary users are not transmitting. So, there is no need for the CR

users to operate under an interference temperature limit; however, the tradeoff is that the CR users need to repeatedly sense the licensed frequency band and detect the spectrum white space, to avoid interfering with the primary users. If a primary user is detected, the CR users have to change to another spectrum.

- **Classification based on the Network Architecture:** Based on the network architecture, the spectrum sharing model can be divided into centralized and distributed architectures. Under the centralized model, a central entity controls and coordinates the spectrum allocation and access of secondary users. With the distributed spectrum sharing model, the users make their own decision regarding spectrum access based on their local observation of the spectrum dynamics. The centralized controller model is expensive and also not suitable for ad hoc emergency or military use. The distributed spectrum sharing model is relatively less expensive and can be used in infrastructure less mode.
- **Classification based on Access Behavior of Secondary CR Users**: Based on the access behavior of secondary users, the spectrum sharing model can be categorized as either cooperative or non cooperative. Under the cooperative model, the secondary users often belong to the same service provider and coordinate between themselves to collectively maximize the benefit to the entire group. On the other hand, under the non cooperative model, secondary users access the open spectrum band, and aim at maximizing their own benefit from using the spectrum resources.

2. Spectrum Sensing

In this section, we will describe some of the well-known spectrum sensing methods in the realm of cognitive radio networks. The three broad classes of spectrum sensing methods discussed here are: (1) Transmitter detection, (2) Cooperative detection and (3) Inference-based detection. The objective is to detect spectrum holes as well as to identify the presence of a primary user (transmitter and/or receiver).

2.1 Transmitter Detection

The idea behind the transmitter detection technique is to detect the presence of a weak signal from the primary transmitter that is part of the signal received at a CR user. The detection is done independently at a CR user through local observations and there is no cooperation with peer CR users. The basic hypothesis model [6] for transmitter detection is shown below:

$$X(t) = \begin{cases} n(t) & H_0, \\ h*s(t) + n(t) & H_1 \end{cases} \qquad \text{…….. (1)}$$

where $X(t)$ is the signal received by the CR user, $s(t)$ is the transmitted signal of the primary user, $n(t)$ is the additive White Gaussian noise and h is the amplitude gain of the channel. H_0 is the null hypothesis, which states that there is no licensed user signal in a certain spectrum band; and H_1 is the alternate hypothesis, which indicates the presence of a signal corresponding to a licensed user. We now discuss three techniques that have been proposed for transmitter detection: (1) Matched filtering and coherent detection; (2) Energy detection and (3) Feature detection.

Matched Filtering: The matched filtering technique [7] requires a CR user to know, *a priori*, information (such as the operating frequency, bandwidth, modulation type and order, pulse shape, packet format and etc) about a primary user signal and feed it to the matched filter as part of its transceiver. The matched filter correlates the received signal with that of the already known signals of prospective primary users and detects the presence of any primary user. The matched filter typically requires very few signal samples and hence can detect the presence of a primary user in a short time. However, as the signal to noise ratio (SNR) of the received signal decreases, the number of signal samples required for detecting a primary user increases; thus, there exists a SNR wall [11] for a matched filter to operate effectively and efficiently. The greater the accuracy of the information fed into the matched filter, the lower the probability of false alarm and a missed detection [8]. But, if wrong information is used, the performance of the matched filter degrades significantly. Matched filters also suffer from high implementation complexity and power consumption [9]. The performance of matched filters can be improved using coherence detection [10] – a technique that uses certain patterns (such as pilot tones, preambles, midambles, spreading codes, and etc) of the received signal to assist control, equalization and synchronization and effectively detect the transmission of a primary user.

Energy Detection: The energy detection technique is based on computing the average energy (T – see equation 2) of signal samples (of strength $X(t)$ as modeled in equation 1) collected at the receiver and comparing the average with that of a pre-determined threshold λ. The performance of the energy detector is characterized based on two probabilities: P_D – the probability of detection and P_F – the probability for false alarm. While the probability of detection P_D (shown in equation 3) indicates the probability that the test correctly decides the alternate hypothesis H_1 identifying the presence of a primary user; the probability for false alarm P_F (shown in equation 4) indicates the probability that the test decides on the alternate hypothesis H_1, whereas, it is actually H_0.

$T = \frac{1}{N}\sum_{t=1}^{N}|X(t)|^2$ …… (2), where N is the # signal samples used to compute the average

P_D = Prob ($T > \lambda \mid H_1$) ……... (3) P_F = Prob (T > λ | H_0) …… (4)

The energy detection method is more apt if the CR receiver could not gather sufficient information about the primary user's signal. However, the energy detection approach is susceptible to uncertainty in the noise level of the received signal. In [7], the authors propose to use a pilot tone from the primary transmitter to improve the accuracy of the energy detector. Also, an energy detector cannot differentiate different types of signals, and can only determine the presence or absence of a signal. Thus, the energy detector is more liable to false detection in the presence of unintended signals. To alleviate the above problems, several improvements to the energy detection method (e.g., [12][13][14]) have been proposed in the literature. The focus of these improvements is on threshold optimization to reduce the probability for false alarm as well as to find and localize narrowband signals without prior knowledge about their noise level.

Feature Detection: The feature detection method is based on the idea of analyzing the received signals for periodicity in the appearance of certain features (referred to as cyclostationary features [16] such as pulse trains, hopping sequences, cyclic prefixes, etc) considered to be characteristic of signals that can be presumed to come from a primary user, rather than considered as a noise

[18]. In addition, the inherent periodicity associated due to the modulation rate, carrier frequency, etc., as part of the signals could also be used as reference features [15] to classify and determine the presence of a primary user. Noise is generally wide-sense stationary with no correlation; whereas, cyclostationary features exhibit autocorrelation. Unlike an energy detector that uses time-domain signal energy as test statistics, a cyclostationary feature detector is not susceptible to the noise associated with the received signal as it conducts the hypothesis test in a frequency feature domain (obtained as a result of transformation from the time-domain). Thus, cyclostationary feature detectors have better detection robustness in low SNR regime. As mentioned above, in addition to the cyclostationary features of a primary user signal, certain general features [17] (such as energy distribution across different frequencies, channel bandwidth and shape, power spectrum density, center frequency, idle guard interval for OFDM signals, FFT-type feature, etc) that are characteristic of the transmission technologies used can also be extracted from the received signal and matched with the *a priori* information that is characteristic of the primary users' transmission characteristics. From a security point of view, feature detectors are vulnerable to the primary user emulation attack in which a malicious secondary user transmits signals whose characteristics emulate those of the primary signals. In [19], the authors propose a secure trustworthy spectrum sensing method based on the location verification of the primary user.

2.2 Cooperative Detection

The transmitter detection is effective only if the CR user can receive the signal from the primary user without much interference from peer CR and primary users. Also, a CR transmitter can have a good line-of-sight to a primary receiver; but not able to detect a primary transmitter due to shadowing [6]. Cooperative detection refers to the use of information collected at multiple CR users to detect the presence of a primary user, and can be implemented either in a centralized fashion (with the CR secondary base station gathering the sensing information from all CR users to detect the spectrum holes) or in a distributed fashion (through exchange of observations among the CR users). In [20], the authors observe a suboptimal spectrum decision when cooperative detection is performed on the same secondary network on which data transmission is conducted. To alleviate the conflict between data transmission and sensing, the authors in [20] advocate the use of two distinct networks – a sensor network and an operational network. The sensors integrated with the CR device sense the spectrum in the desired target area and forward the information to a central controller that processes the gathered information and generates a spectrum occupancy map for the operational network. The operational network uses the occupancy map to determine the available spectrum space. While cooperative detection can be more effective in environments prone to multi-path shading, interference and shadowing, the method is not appropriate for resource-constrained networks due to the sensing and traffic overhead. Also, like the non-cooperative transmitter detection method, the cooperative sensing and detection method suffers if there is lack of sufficient information about the location of the primary receiver.

2.3 Interference-based Detection

The idea behind the interference-based detection method is to have a CR user model the expected interference at a primary receiver due to the transmissions from the CR user in the form

of an interference temperature. The interference temperature is basically the expected increase in the noise at a primary receiver due to interference of signals from the unlicensed CR users in the neighborhood. As long as the interference temperature is within a threshold, the CR user continues to use the spectrum along with the primary receiver. Figure 3 illustrates the interference temperature model [21], as explained above. The implicit assumptions (which are indeed also the limitations of this method) are that the CR user knows the location of the primary receiver as well as that the reception at the primary receiver is to be interrupted only by the particular CR user. Also to be noted is that the interference-detection method is primary receiver-centric, while the transmitter and cooperative detection methods are primary transmitter-centric. In order to maintain the interference at a primary receiver within the temperature threshold, secondary users are often constrained to only short-range communication, even though they are able to use a wide range of spectrum.

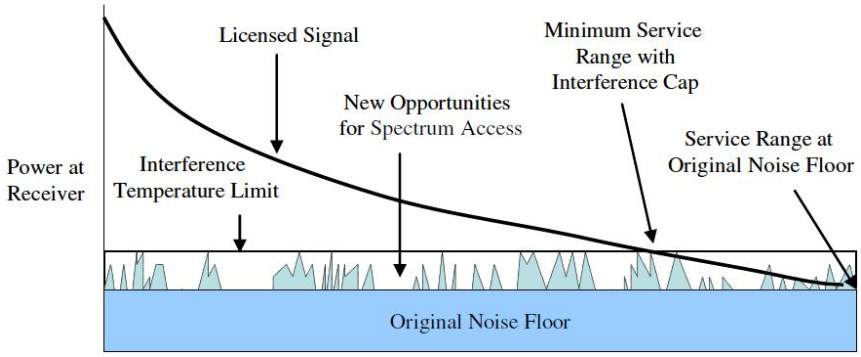

Fig 3: Interference Temperature Model [21]

2.4 Issues in Spectrum Sensing

In this section, we discuss two major issues that are critical to the design of spectrum sensing methods for cognitive radio networks. These are: (i) Optimization of spectrum sensing and transmission duration and (ii) Spectrum band search sequence.

Optimization of Spectrum Sensing and Transmission Duration: The total time for which the spectrum may be used (T_f) is the sum of the sensing time (T_s) and the actual data transmission time (T_t). While the overall objective is to maximize the throughput, spectrum sensing methods differ on how they accomplish that – either by independently optimizing the sensing time or the data transmission time or by jointly optimizing them. In [23], the authors aim to optimize the sensing time for a fixed data transmission time so that the channel efficiency, T_t / T_f, can be maximized. In [24], the authors propose a scheme to optimize the sensing time across multiple spectrum bands, in case a primary user surfaces in the band that is currently in use by a CR user. In [8], it is further shown that for a fixed data transmission time, if the primary traffic is assumed as a random On/Off process, the search time for available spectrum could be minimized, thereby leading to a maximum throughput for the CR network. In [25], the problem of optimizing the transmission duration for a fixed sensing duration was studied. Though larger the data transmission time, the larger the throughput, it has been observed in [25] that the sensing time has to be at least a certain minimum value to maintain the packet collision probability for the primary network under a certain threshold. A theoretical framework for jointly optimizing the sensing and

data transmission durations to maximize the spectrum efficiency was proposed in [26]. In a multi-user and multi-spectrum environment of cooperating users, it is observed that an approach of periodic sensing and transmission (with separate observation and transmission periods) is the best (at least theoretically) to balance the sensing accuracy vs. spectrum utilization efficiency tradeoff; though this approach is inherently more complex to be implemented in a real-time setup.

Spectrum Search Sequence Optimization: The overall time spent to search for an available spectrum depends on the sequence in which the spectrum bands are searched for. In [27], the spectrum search problem was studied under the correlated spectrum band occupancy models and it was observed that a general *n*-step serial search scheme is the best solution. Also, as primary users are likely to use several licensed bands at a time, a random search scheme may not be effective, especially to detect transmissions of a primary user in the neighboring spectrum of a band that is already known to be occupied. In [28], the authors investigate the possibility of developing an on-demand sensing schedule when both the sensing duration and spectrum search sequence optimization problems are jointly studied.

3. Medium Access Control Protocols for Cognitive Radio Networks

In this section, we will focus on the spectrum access problem wherein multiple CR users share the spectrum and determine who gets access to the channel and when. In this context, we discuss the medium access control (MAC) protocols that have been proposed for both infrastructure-based and ad hoc cognitive radio networks. The MAC protocols for both categories of CR networks can be either time-slotted, random access or both. The time-slotted MAC protocols require network-wide synchronization and operate by dividing time into discrete slots for both the control channel and data transmission. On the other hand, the random access protocols do not require time synchronization, and are based on the CSMA/CA (carrier sense multiple access/collision avoidance) principle wherein a CR user monitors the spectrum band to detect the presence of any transmission from peer CR users and if so, transmits after backing off for a random duration, to reduce collisions due to simultaneous transmissions. Hybrid MAC protocols have also been proposed on two different lines: one category of protocols in which the control signaling occurs in synchronized time slots and the data transmission follows random access channel schemes; the other category of protocols have predefined durations for the control/ data frame – however, the access to the channel within each control or data transmission duration is completely random.

3.1 MAC Protocols for Infrastructure-based Cognitive Radio Networks

Random Access Protocols: In [29], a CSMA based random access protocol was proposed for an infrastructure-based cognitive radio network under the assumption of use of a single transceiver and in-band signaling. The protocol facilitates the coexistence of the primary and CR users by requiring the latter to adapt their transmission power to maintain the interference to the primary users within a pre-decided threshold. The primary users coordinate with a primary base station and the CR users coordinate with a CR base station, and establish a direct single-hop connection with their respective base stations. The primary network follows the classical CSMA protocol according to which a primary user senses the channel for a period (τp) before sending the Request

to Send (RTS) packet to its base station for which the latter may reply with a Clear to Send (CTS) signal if available for the data transfer. The CR users have a relatively much longer carrier sensing time (τs, where $\tau s >> \tau p$) so that the primary users get the priority to access the spectrum. The CR base station decides on the transmission power and data rate for the transfer depending on the distance between itself and the CR users. A CR user is allowed to send just one packet in a round of negotiation to reduce or avoid interference and collisions with the transmissions of other primary users. The random access protocols require significant interaction between the primary and CR networks; otherwise, the CR users are oblivious of any failed transmissions of a primary user. Also, the transmission power of the CR users needs to be partitioned to several discrete levels (not just low and high levels) to reliably protect the primary users from interference as well as to maximize throughput by operating the CR devices at the appropriate level.

Time Slotted Protocols: The time slotted protocols follow the IEEE 802.22 centralized MAC standard [30] for cognitive radio networks. The 802.22 standard uses simple time division multiplexing in the downstream direction, and demand assigned TDMA in the upstream direction. The base station manages all the CR users in its cell. Time is slotted into multiple superframes, each comprising multiple MAC frames preceded by the frame preamble. A Superframe Control Header (SCH) is located at the start of each superframe to inform the CR users about the current available channels, different bandwidths supported, future spectrum access time, and etc. The MAC frame is composed of a DS subframe and a US subframe. The DS subframe consists of a preamble that deals with synchronization and channel estimation, a frame control header containing the sizes of the DS- and US-MAP fields with channel descriptors, and the DS/US-MAPs provide the scheduling information for user bursts. The US subframe consists of an Urgent Coexistence Situation (UCS) notification field that informs about the primary licensees that have just been detected; the other fields are used to derive the distance from the base station and the individual bandwidth requests. The main drawback with the time-slotted protocols is the use of heavy headers as part of the frames, leading to a reduced throughput.

3.2 MAC Protocols for Cognitive Radio Ad hoc Networks

The MAC protocols for infrastructure less cognitive radio ad hoc networks require increased cooperation among neighboring nodes to facilitate a scalable architecture that supports flexible deployment, distributed spectrum sensing, sharing and access. The main design issues include network-wide time synchronization and information exchange among neighboring nodes with minimum overhead.

Random Access Protocols: Two categories of random access protocols exist for CR ad hoc networks – those that support multiple radio transceivers and those using only a single radio transceiver. In this section, we discuss a representative protocol from each category. In [31], the authors proposed a distributed channel assignment (DCA) based MAC protocol that uses multiple transceivers, a dedicated out-of-band control channel for signaling, as well as spectrum pooling to reliably detect the activity of the primary network. Each node maintains a list of currently used channels of its neighbor nodes and a list of free channels derived from the former and the spectrum pool. During a RTS-CTS handshake, the sender and receiver match their list of free channels and agree on a common channel to use. The RTS-CTS messages also facilitate the neighboring CR users to update their used channel and free channel lists. The main drawback of

the DCA protocol is the requirement for a separate control channel to support the RTS-CTS exchange, and also there is no primary user-related adaptation for channel usage. In [32], a single radio transceiver version of the DCA protocol has been proposed with the idea of alternately monitoring the control channel and the data spectrum bands for signals. The Single Radio Adaptive Channel (SRAC) algorithm proposed in [33] uses a frequency division multiplexing like scheme wherein a CR user transmits packets on a larger spectrum but receives return acknowledgments over smaller spectrum bands for efficient spectrum utilization. A CR node maintains the list of receive bands of all its neighbor nodes. When a CR node senses its current transmission channel to be occupied by a primary user, it sends a notification packet in the receive bands of its neighbor nodes, and switches to the band that is confirmed to by all the neighbor nodes. In the meanwhile, the CR node transmits on the receive band of a neighboring node that is yet to acknowledge for the notification packet. The drawback with the above approach is the signaling traffic overhead associated with maintaining the updated receive spectrum bands of all the neighbor nodes. Also, control messages that are not sent on the receive bands of a node are not listened to, leading to longer *deaf* periods.

Time Slotted Protocols: For this category of CR Ad hoc network protocols, we discuss the C-MAC (Cognitive MAC) protocol [34], based on synchronized time slots, and include the use of a rendezvous channel (RC) and a backup channel (BC). The RC is the channel that exists for the longest time for use for the CR users throughout the network and is used for node coordination, primary user detection, as well as multi-channel resource reservation. The BC is locally determined at each CR user, through out-of-band measurements, and is used as an alternate spectrum band in the case of appearance of a primary user. In C-MAC, each spectrum band comprises of recurring superframes, each composed of a beacon period (BP) and a data transmission period (DTP). Each BP is time slotted so that the individual CR users can transmit their beacons without interference. The RC is used to exchange the BP schedules of nodes to prevent simultaneous transmission over all the spectrum bands. A CR user announces the need for any new data spectrum band through the beacons, and also informs about any spectrum change over the RC. Periodic tuning to the RC allows a CR user to re-synchronize and obtain the recent neighborhood topology information. The time slotted nature of C-MAC also facilitates the use of a non-overlapping quiet period (QP) for each spectrum band, through which one could differentiate a primary user from a CR user. The main drawbacks of the C-MAC are that it requires the RC to be a dedicated spectrum band that is not used by any primary user, which is difficult to guarantee in distributed networks. Also, due to the requirement to include the beacons with the load and channel usage information in the BP of a superframe, the protocol is not scalable for a larger number of CR users. It is difficult to enforce the non-overlapping nature of the BPs and the quiet periods, without the presence of a central entity. In [35], a distributed slotted protocol was proposed to circumvent the use of a RC by providing in-band signaling through a dedicated control window in addition to the beacon and data transfer periods.

4. Routing in Cognitive Radio Networks

The problem of routing in multi-hop cognitive radio networks (CRNs) refers to the creation and maintenance of wireless multi-hop paths among the CR users (also called Secondary Users, SUs) by deciding the relay nodes and the spectrum to be used on each of the links in the

path. Even though the above problem definition exhibits similarities with routing in multi-channel, multi-hop ad hoc networks and mesh networks, the challenge in the form of dynamic changes in the available spectrum bands due to simultaneous transmissions involving primary users needs to be handled. Any routing solution for multi-hop CRNs needs to be tightly coupled with spectrum management functionalities [35] so that the routing modules can take more accurate decisions based on the dynamic changes in the surrounding physical environment. As the topology of multi-hop CRNs is highly influenced by the behavior of the PUs, the route metrics should be embedded with measures on path stability, spectrum availability, PU presence, etc. For instance, if the PU activity is low-to-moderate, then the topology of the SUs is almost static, and classical routing metrics adopted for wireless mesh networks could be employed; on the other hand, if PUs become active very frequently, then the routing techniques employed for ad hoc networks could be more applicable [36]. Also, the routing protocols should be able to repair broken paths (in terms of nodes or used channels) due to the sudden reappearance of a PU.

With respect to the issue of spectrum-awareness, the routing solutions for CRNs could be classified as those based on the full spectrum knowledge and local spectrum knowledge. In the former case, the spectrum availability between any two nodes in the network is known to all the nodes (or to a central control entity). This is often facilitated through a centrally-maintained spectrum database to indicate channel availabilities over time and space. The routing solutions built on the top of the availability of full spectrum knowledge are mostly based on a graph abstraction of the CRN and, though not often practically feasible for implementation, are used to derive benchmarks for routing performance. The routing module is not tightly coupled with the spectrum management functionalities for centralized full spectrum knowledge-based solutions. On the other hand, for local spectrum knowledge based solutions, information about spectrum availability is exchanged among the network nodes along with traditional network state information (such as the routing metrics, node mobility, traffic and etc). On these lines, the local spectrum knowledge-based routing protocols could be further classified as those that aim to minimize the end-to-end delay, maximize the throughput and maximize the path stability. In addition to the above, we have also come across probabilistic approaches for routing (e.g., [37][38]) in which CR users opportunistically transmit over any spectrum band available during the short idle periods of the surrounding primary users.

4.1 Common Control Channel

A common thread among the distributed local spectrum knowledge-based routing protocols discussed in Section 5.2 is that they assume the availability of a Common Control Channel (CCC) [50] across all the CR nodes in the network. The CCC is used for neighbor discovery as well as for path discovery and establishment. Nodes share their neighbor information on different interfaces through the broadcast messages sent out on the CCC to all the potential neighbors, using a high transmission power, corresponding to the maximum transmission range of the CR nodes. Route discovery is launched through a Route-Request-Reply (RREQ-RREP) cycle (similar to that of the classical ad hoc networks) run on the CCC at all the nodes. An alternate strategy for route discovery without using the CCC is to broadcast the RREQ packets on all the available channels and let a flood of RREQ packets reach the destination, on multiple paths and on multiple channels. The destination processes these RREQ packets and selects the best path(s)

that satisfies the route selection criteria. Broadcasting across all the spectrum bands for route discovery would be too much of an overhead compared to broadcasting the RREQ packets on a single CCC and including information about all the available channels at each node in these RREQ packets.

The CCC could be either in-band or out-of-band with respect to the data channels. If in-band, the CCC may be one of the data channels to which all nodes can tune in; if a data channel common to all CR nodes is not possible to be found, then the network could employ more than one CCC, each of which having certain region of coverage. In the case of out-of-band CCC, a dedicated control channel, separate from the data channels, is used for control signaling, either network-wide or coverage-based. The CCC and the data channels could all be accessed through a single radio, in which case the routing solutions are prone to the channel deafening problem wherein the control message received on one channel is not received when the radio is tuned to a different data channel. If a dedicated radio is allotted for the CCC, one could avoid the channel deafening problem [50]; however it would be expensive to employ more than one radio per CR node, and also CR nodes employing more than one radio suffer from the cosite interference problem [50] according to which when two or more radios are located on the same device – signals transmitted and/or received on one radio interfere with signals transmitted and/or received on the other radio.

4.2 Routing Solutions based on Full Spectrum Knowledge

The general strategy under this approach is to first abstract the physical network as a graph with nodes and edges with weights, all capturing the network dynamicity and spectrum availability, and then run a route calculation algorithm on the graph to find a path/tree or any appropriate communication topology connecting the nodes (source-destination pairs for unicast routes; source-receiver nodes for multicast communication and etc). In [39], the authors propose a generic framework for modeling CRNs comprising of nodes with a single half-duplex cognitive radio transceiver, which can be tuned to the various available spectrum bands or channels. The framework is based on creating a layered graph that features a number of layers equal to the number of available channels. Each CR device is represented in the layered graph with a node, *A*, and *M* additional sub nodes A_1, A_2, …, A_M, one for each available channel, and *M* is the total number of available channels. Three kinds of edges exist in this layered graph: The *access* edges connect a node with all its corresponding sub nodes; the *horizontal* edges connect the sub nodes of two different nodes on the same logical layer if the two nodes can be tune to the corresponding channel; the *vertical* edges connect sub nodes of different layers of a single CR device to switch from one channel to another. Figure 4 illustrates a layered graph with four nodes and two channels. The weights of the horizontal edges typically capture the involved in propagating data from one CR device to another node on the particular channel and the weights of the vertical edges typically capture the cost involved in switching from one channel to another at a particular CR device. Graph theoretic algorithms optimizing the overall cost of a path between every source-destination pair, or trees connecting a group of nodes (including all the nodes in the graph, in the case of spanning trees) could then be run on such a weighted layered graph. As an example of the application of the layered graph model, in [40], the authors represent the horizontal edge weights to be proportional to the traffic load and interference, and propose a centralized heuristic algorithm to calculate shortest paths. The main weaknesses of the layered graph model presented

above are that it requires a network-wide signaling to generate such a global graph at each node and it may not scale well as the network dimensions increase.

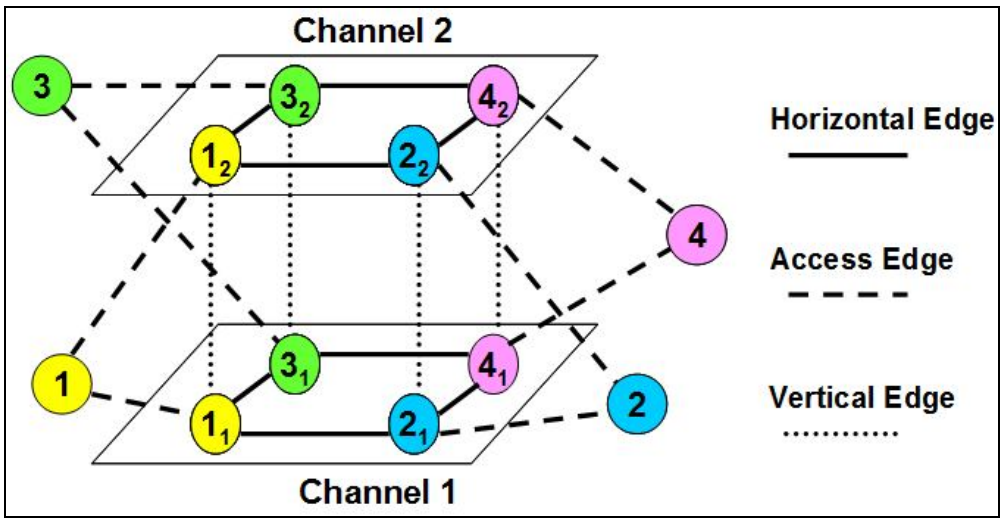

Fig 4: Example for Layered Graph Model

To circumvent the scalability problem, an edge coloring model was proposed in [41] that gets away with representing sub nodes of a node in multiple layers, and instead connects the nodes with edges of different colors, with each edge color indicating whether the nodes can communicate on a particular channel (i.e., one color per channel). Another solution is to capture the network as a conflict graph [42] where each node in the conflict graph is actually an edge between two nodes in the network graph and there exists an edge in the conflict graph only if the edges corresponding to the two end nodes of the conflict graph cannot be active at the same time. One can then run a maximum independent set (or maximum clique) heuristic on the conflict graph to derive a conflict-free channel assignment for the original network graph. Nevertheless, all of the three graph theory models (layered, colored or conflict graphs) suffer from the weakness of being centralized in nature and requiring the full knowledge of the network topology and the available spectrum bands.

4.3 Routing Solutions based on Local Spectrum Knowledge

The routing solutions based on local spectrum knowledge (that varies both in time and space) are distributed in nature and differ depending on the specific metric used to assess the route quality.

In the **minimum power routing protocol** proposed in [43], the weight of a link (for each interface) is modeled as the transmission power to be spent to reach the other end of the link within an appreciable received signal threshold. An energy loss is associated to switch from one frequency channel to another. An intermediate forwarding node includes in the RREQ the transmission power loss to be incurred for each of its outgoing channels. The destination receives the Route Request packets along all the paths and finds the path that minimizes the sum of the energy lost across all the links and their corresponding channels as well as the switching energy loss, if any, is incurred. The Route-Reply packet containing information on the chosen route is

sent through the CCC. The main weakness of the minimum power routing protocol is that it is oblivious to the presence of primary users and their impact on neighbor discovery among the CR users.

In [44], a **bandwidth footprint (BFP) minimization-based routing protocol** has been proposed to find an appropriate channel and capacity for a session with minimal impact (with respect to interference and throughput) on the ongoing sessions of the PU and SU users. The BFP for a node refers to the interference area of the node for a given transmission power. With a node switching from one band to another and each band incurring a certain footprint corresponding to its transmission power, the objective of the protocol is to minimize the network-wide BFP, which the sum of the BFPs of all the nodes. The routing protocol goes through an iterative procedure to fit in an incoming session request with the existing sessions. First, the session is assigned to an available capacity on a channel; if this is not sufficient, the transmission power of the band is increased to increase the session rate (referred to as Conservative Iterative Procedure, CIP). However, if the increase in transmission power violates the interference constraints and significantly increases the BFP, the alternative channels are considered to migrate the session to achieve the targeted session rate. To do this, the capacity allocated for the existing sessions in the alternate channel need to be reduced (referred to as Aggressive Iterative Procedure, AIP). If the reduction impacts the quality-of-service guaranteed for these sessions beyond a limit, then the new session is accommodated; otherwise, it is allocated a capacity in the alternate channel.

In [45], the authors proposed a routing protocol whose objective is to choose the next hop that would **minimize the interference** to the PUs operating in the vicinity of the transmission and satisfying the QoS parameters for the SUs to the maximum. In this context, they evaluated the use of Nearest Neighbor Routing (NNR) and Farthest Neighbor Routing (FNR) to decide the next hop neighbor for a CR node employing geometric forwarding. The tradeoff observed is that the FNR scheme achieves a better end to end channel utilization and reliability; whereas, the NNR scheme has a better energy efficiency.

In [46-49], the authors propose routing protocols aimed at optimizing the various components of the delay incurred at a node, with the overall objective of **minimizing the delay incurred on a path**. The delay at a relay node is conceived as the sum of the delays incurred due to switching from channel to another; accessing the channel corresponding to the chosen spectrum band; and the queuing delay suffered by the packet before it is transmitted on the particular channel. The switching delay includes two components: the delay to switch the packet from one frequency band to another frequency band – a measure of the separation of the two frequency bands, and also the delay incurred due to the scheduling (the round-robin scheduling is often chosen for fairness) of the packet transmissions at the node across the spectrum bands in use. Note that the queuing delay suffered by a packet is also influenced by the channel scheduling component of the switching delay. While [46, 47] focused on minimizing the sum of the switching and access delays incurred at the relay nodes; [48] focused on minimizing the sum of the queuing delays at the relay nodes. In [49], the authors proposed a routing protocol that lets an intersecting node (a node that lies on more than one path from the source to the destination) to locally coordinate among the neighboring nodes to decide whether to accommodate an incoming new flow or to redirect it to one of its neighbors to obtain a relief to the workload on the node. If such

a route redirection materializes, this would actually lead to a scenario wherein the route discovery RREQ-RREP packets and the data packets traverse different paths – the RREQ-RREP packets traverse through the intersecting node, and the data packets traverse through the neighbor node that took up the load from the intersecting node to provide relief to the latter's workload.

In [51-52], **throughput-based solutions for routing** in CRNs have been proposed. The Spectrum Aware Mesh Routing (SAMER) protocol [51] first establishes paths based on the periodically collected global states, and at the time of packet transmissions, the packets are delivered opportunistically along the path with the highest value for a throughput metric, referred to as the Path Spectrum Availability (PSA). The PSA captures the number of available spectrum blocks at each node as well as their aggregated bandwidth and loss rate. Though throughput is the primary routing objective, SAMER imposes an upper bound on the number of intermediate nodes to be used on the path and for which the PSA values are calculated. In [52], the authors propose a spectrum utility based routing protocol to maximize the throughput. The spectrum utility of a link (i, j) is the product of the achievable capacity of the link and the maximum differential backlog of packets between nodes i and j.

5. Transport Layer Issues and Solutions for Cognitive Radio Networks

Research on transport layer protocols for cognitive radio networks is very much in its nascent stages. We have come across only two proposals ([75, 77]) for transport layer protocols for CRNs and a performance evaluation study [76] of the traditional TCP protocols for CRAHNs. In this section, we first identify the reasons for possible packet drops in a mobile wireless CRN; analyze the potential performance degradation when the traditional TCP is run on a CRN; and then discuss the currently available solutions for transport layer protocols for CRNs in the literature.

5.1 Transport Layer Issues and Motivating Examples

Packet losses in a CRN involving mobile wireless nodes may occur due to one of the following factors: (i) Traditional network congestion that could be further aggravated due to reduced link capacity and loss of connection, (ii) Link error, (iii) Collision due to simultaneous transmissions, (iv) mobility of a node from one base station to another, (v) mobility of the intermediate forwarding nodes, (vi) the intermittent spectrum sensing undertaken by the CR users, (vii) the switching of a CR-node between transmitting and spectrum sensing states, (viii) the activity of the primary licensed users of the spectrum, and (ix) large-scale bandwidth variation due to spectrum availability. Factors (vi) through (ix) are characteristic of CRNs and these factors have not been considered in the design of the transport layer protocols for other categories of wireless networks (e.g. wireless mobile ad hoc networks or sensor networks), motivating the need to design transport layer protocols exclusively for CRNs.

Fig 5: A Hybrid Cognitive Radio Network Layout for Example 1 (adapted from [75])

Example 1: Assume a CR-node is sending data to a destination node in the Internet through an intermediate router (refer Figure 5). Let the link between the router and the destination node be wired and the link between the source node and the router be a CR-link. As is characteristic of a CRN, the source-router CR-link alternates between spectrum sensing and transmission modes. When the nodes for the CR-link enter into the spectrum sensing mode, the source does not receive any acknowledgment packets and hence cannot estimate a RTT (round trip time) for the link. Once spectrum sensing is completed, the source node starts receiving the acknowledgment packets that were waiting at the router. The RTTs for these acknowledgment packets that waited in the network would be quite high as they correspond to the spectrum sensing duration and do not capture the congestion level in the network. Once the backlog of the acknowledgment packets is cleared, the source node starts receiving the acknowledgments for the packets sent at the end of the sensing mode and notices a sudden decrease in the RTT. However, the retransmission timeout (RTO) value for the congestion control algorithm gets unnecessarily increased to extraneous values because of the RTTs of the acknowledgment packets that waited at the router. These acknowledgment packets would have been received if the source node were not in the sensing mode. It takes awhile for the congestion control algorithm to lower its estimate for the RTO value even if the RTT value starts decreasing abruptly once the backlog of acknowledgment packets is cleared. Additive Increase and Multiplicative Decrease (AIMD) is a core principle of standard TCP congestion control algorithms. This contributes to a lower throughput and an under utilization of the available bandwidth.

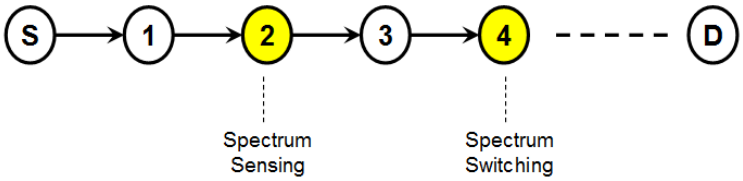

Fig 6: A Multi-hop Cognitive Radio Ad hoc Network Layout for Example 2 (adapted from [77])

Example 2: Consider a multi-hop CRAHN (cognitive radio ad hoc network) shown in figure 6, with nodes S and D as the source and destination nodes respectively (adapted from [77]). As we can see from the figure, due to node 2 entering into the spectrum sensing mode, the S-D path is virtually broken into two connected segments: S – 1 and 3 – D. Source S may eventually timeout waiting for the acknowledgment packets for the transmitted data packets, and this could trigger a retransmission of the data packets, even in the absence of true congestion. If the source S does not limit its transmission rate during the spectrum sensing duration and continues to transmit/retransmit the data packets, the queue at the intermediate node 1 may soon be overwhelmed and will succumb to a buffer overflow. In addition, a proper balance has to be maintained between the sensing interval and the data packet transmission time so that the throughput of the connection can be maintained as well as the interference with the PU activities is minimized [79]. A longer sensing interval would correspond to the CR user spending most of the time monitoring the channel rather than transmitting the data packets; on the other hand, a shorter sensing interval could increase the risk of interfering with the activity of a PU [78].

Another factor that needs to be considered in the design of transport layer protocols for CRNs is the uncertain delay caused due to the need for a CR user to successfully search for an

available channel once a PU activity is detected in the currently used channel. Unlike spectrum sensing, the time spent to hunt for an available channel is not deterministic and cannot be known in advance to the source on a multi-hop path. This necessitates the need for transport layer protocols to differentiate the spectrum switching state from other causes of route disconnections by requiring an explicit feedback from the nodes affected by the PU activity (node 4 in Figure 6).

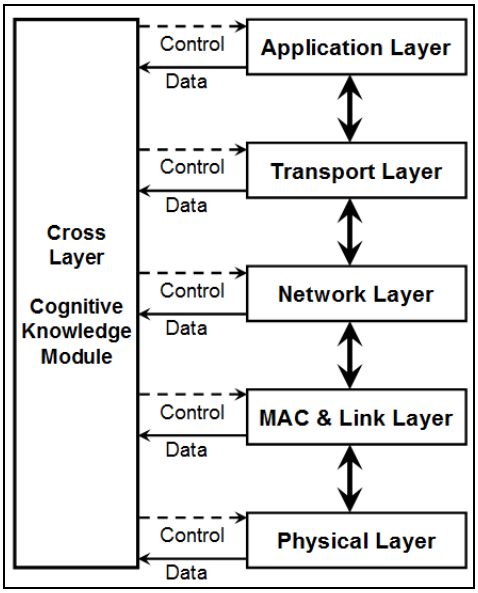

Fig 7.1: Cross-Layer Approach

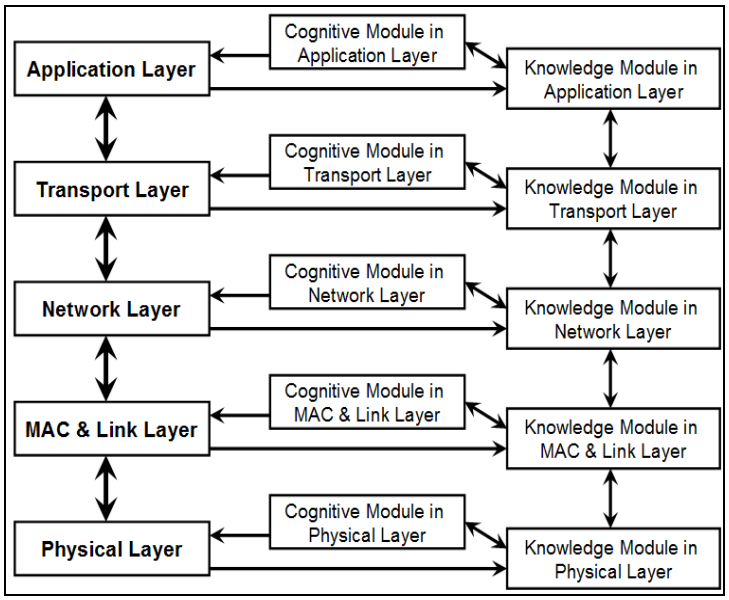

Fig 7.2: Layer-Preserving Approach

Fig 7: Approaches to Extend the Standard TCP/IP Layer Suite for Cognitive Radio Networks (adapted from [75])

5.2 Cross-Layer Approach for Transport Layer Solutions

The solutions to handle the RTO-increase problem and other related issues at the transport layer due to a CR-node entering the spectrum sensing/switching states can be effective only if at least the current status of the node (could be: normal, spectrum sensing, spectrum switching and route failure) is known at the higher end-to-end layers, starting from the network layer. A cross-layer approach to solve the above problems could involve the use of a cognitive knowledge module that is shared by all the layers (Figure 7.1). The physical layer could update a Boolean flag to indicate the current status of the node, and all the other layers could refer to this information to infer whether the node is in the normal transmission mode or spectrum sensing/switching/route failure modes. However, a cross-layer approach involving a node-wide globally shared module would incur considerable management overhead to maintain the consistency of the information that can be updated by/accessible by all the layers, and it would not be a scalable solution for CRNs of moderate or larger size.

5.3 Layer Preserving Approach for Transport Layer Solutions

In [75], the authors propose a layer-preserving approach to extend the standard TCP/IP layer suite for cognitive radio networks. The idea is to implement two modules – Knowledge module and Cognitive module – as part of each of the layers. The *Knowledge module* at a layer

stores information about the application's need and status of local and global networks, all pertaining to the appropriate layer; the Cognitive module at a layer is responsible for the algorithms/heuristics to gather knowledge and to generate control signals for managing the operation of the layer based on the information in the Knowledge module. The separation of the knowledge and cognitive decision making modules from the standard modules for each layer preserves the modularity and abstraction concept of the TCP/IP protocol stack as well as reduces the development and maintenance time of new software that would need to be implemented for any of these layers in the context of cognitive radio networks. The layer-preserving architecture (shown in Figure 7.2) can serve as a generic architecture to deploy families of protocols to fulfill the requirements of individual applications, without affecting the core functionality of the layers in the standard TCP/IP layer stack.

Two solutions, which adhere to the layer-preserving approach, have been proposed in [75] to avoid the abnormal increase in the RTO values because of spectrum sensing/switching. One solution is not to consider the RTTs of the acknowledgment packets that are forced to wait in the network due to the source node or the network (i.e., the intermediate nodes on a multi-hop path) entering the spectrum sensing/switching states. The Knowledge module at the transport layer learns about the node or the network entering into the spectrum sensing/switching states through its interaction with the Knowledge module at the lower layers and updates the Cognitive module. Once the Cognitive module learns about the node or the network entering into the spectrum sensing/switching states, it marks every data packet (that were already sent) whose acknowledgment is yet to be received and updates the TCP process accordingly. When the source node or the network gets back to the transmission mode, the TCP process at the source node, in consultation with the Knowledge and Cognitive modules, decides not to consider (to estimate the RTO value) the RTTs of the acknowledgment packets received for the data packets marked during the node/network's sojourn in the spectrum sensing/switching states in the past.

Another related solution proposed in [75] is to mark an acknowledgment ACK packet (or a sliding window worth of ACK packets) as delayed due to the node/network entering the spectrum sensing/switching states if the RTT of the acknowledgment packet (or the window of packets) at the time of reception is greater than the RTT of the latest acknowledgment packet (or the latest window of packets) received plus 0.9*the spectrum sensing/switching duration. The value for the spectrum sensing/switching duration is estimated by the Cognitive module through the interactions of the Knowledge module with its counterparts in the lower layers. While the duration for spectrum sensing may be fixed per node, the duration for spectrum switching is a stochastic parameter that can be only best estimated, mostly based on the past history (including the statistics of the PU activities). Once an ACK packet (or a window of ACK packets) is perceived to be delayed because of the node/network entering into the spectrum sensing/switching states, the TCP process does not update the RTO and the estimated current estimated RTT. If the RTO timer expires while the node/network is in the spectrum sensing/switching states, the RTO timer is simply reset and no further action is taken.

6. Security Attacks on Cognitive Radio Networks and Countermeasures

In this section, we discuss several security attacks that could be launched on cognitive radio networks and the countermeasure solutions to thwart or mitigate them.

6.1 Attacks on the Common Control Channel (CCC) and Solutions

The centralized and cooperative CRNs are more vulnerable to masquerade and denial of service attacks. The CCC is a single point of failure and is vulnerable for a jamming attack that can effectively destroy the entire CRN. An attacker can inject a strong interference signal to the CCC and disable the reception of valid control messages at the CR receivers, essentially leading to a denial of service (DoS). It is a more energy-efficient and effective strategy for an attacker to just jam the CCC and bring the network down, rather than jamming the entire spectrum band [53, 54]. For centralized CRNs, one can avoid CCC saturation attacks by requiring the MAC control frames to be authenticated and stamped by the base station. The CCC anti-jamming solutions that are currently available for distributed/cooperative CRNs include: (1) Dynamic CCC allocation and (2) CCC key distribution. Dynamic CCC allocation can be accomplished using cross-channel communication [55] and frequency hopping [56]. The idea behind the cross-channel communication approach is to use a CCC currently under jamming attack to notify CR users about the new CCC for receiving control messages if the receiving nodes are free of jamming. Information about the new CCC can be conveyed through a unique frequency hopping sequence that is known only to the CR users. However, any CR user who is compromised by the jammer could receive the notification about the change of the CCC and be able to jam the new CCC. For increased robustness against CCC jamming attacks, the CCC key distribution method is preferable, though it involves significant overhead. The idea behind the CCC key distribution method is to use multiple CCC channels for transmitting control signals. A CR user is assigned the keys for only certain CCCs and not to all of them. This way, even if a CR user is compromised, he cannot extract information from the CCCs for which he does not know the key. The random key distribution approach [54, 57] has been observed to be the most effective approach for CCC key distribution.

6.2 Primary User Emulation (PUE) Attacks

The primary user emulation (PUE) attack [58] is launched by a malicious or selfish secondary user emulating or masquerading as a primary user to obtain complete access to the spectrum bands of a given channel and not sharing it with other secondary users. While a selfish PUE attack could be intended to increase the attacker's share of the spectrum resources, the malicious PUE attack is typically targeted at preventing the legitimate secondary users from using the spectrum holes. More sophisticated PUE attacks could be performed if the attacker has knowledge about the CRN. For example [59], an attacker can transmit during the "quiet period" of a CRN and masquerade as a primary user to the rest of the nodes (secondary users). A quiet period is the time period during which all secondary users desist from transmitting to facilitate spectrum sensing.

PUE attacks can also be launched when the CRN makes a frequency handoff (i.e. switches from one channel to another), leading to degradation in the data throughput. For a while, the TCP (transmission control protocol) process at the transport layer of the sender side will be unaware of the frequency handoff at the physical layer and will keep creating logical connections/sending data packets without receiving acknowledgments. Perceiving this as an impending congestion, the TCP process backs off and doubles its retransmission timeout value, resulting in transient delays and

packet losses. If an attacker is able to intercept the messages and predict the frequency bands used in a handoff, he can launch the PUE attack on both the old and new frequency bands, leading to total network starvation. Such a manifestation of the PUE attack disrupting TCP connections at the transport layer is called the Lion attack [74].

Several solutions have been proposed to defend against PUE attacks. An important criterion for these solutions is that they should not require any change in the operating mode or characteristics of the primary users. In [58], the authors suggest the use of a Distance Ratio Test (DRT) or a Distance Difference Test (DDT) to determine the location of a transmitting source and crosscheck the transmitter location with trusted location verifiers (LVs) that have a database of the coordinates of the primary users (e.g., TV broadcast towers) obtained through secure GPS systems. The LVs need to be tightly synchronized with each other and exchange information in encrypted form. Still, attackers could subvert the LV-DRT/DDT detection mechanism by transmitting signals from the vicinity of a primary user. A solution [60] to detect such PUE attacks is to measure the energy level of the received signals and compare them with that expected from an authentic primary user. The assumption behind this strategy is that primary users (such as TV towers) have a fixed location and the energy level of their received signal would be much stronger than that of the signals received from secondary users who are also often mobile. Various mechanisms (such as the Time Difference of Arrival, TDOA [61]) are available in the wireless network literature to estimate the location of a transmitter based on its received signal strength. Apart from localization, another category of solutions (e.g., [62][63]) based on fingerprinting have been proposed for CRNs. These solutions are based on the idea of extracting unique distinctive patterns in the initial waveforms emitted by a transceiver and use these as an authentic means of identifying the transmitting source. Though relatively more credible, the fingerprinting-based solutions have been observed to require large samples of training data as well as more storage and significant computation plus signal processing overhead.

To mitigate the chances a TCP session from being intercepted and subjected to a PUE attack/Lion attack during frequency handoff, the authors in [74] suggest cross-layer data sharing between the physical and transport layers. This would facilitate the TCP session to freeze the connection parameters until the frequency handoff is completed and adapt them to the new network. In addition, a group key management mechanism could facilitate the CRN members to encrypt, decrypt and authenticate each other and prevent an attacker from intercepting the TCP session/frequency handoff to infer the control parameters.

6.3 Objective Function Attack

The cognitive engine of a cognitive radio is responsible for adjusting the radio parameters (such as center frequency, bandwidth, power, modulation type, coding rate, channel access protocol, etc) to meet specific requirements (such as low energy consumption, high data rate, high security and etc). An attacker could launch an attack to manipulate the values of the parameters that he has on control to tailor the results of the objective function to suit his interests. For example, consider a scenario (presented in [64]) of a cognitive engine attempting to maximize an objective function f composed of transmission rate (R) and security (S) given by: $f = w_1R + w_2S$, where w_1 and w_2 represent the weights for parameters R and S. If the attacker gets to know that the cognitive engine is attempting to maximize f by increasing S, he may launch a jamming attack

on the radio and reduce *R*, so that the overall value of f could get lower. To prevent the value of f from getting lowered, the cognitive engine may choose to operate at a lower value for the security level. Though no concrete solutions have been proposed for the Objective function attacks, an idea proposed in [59] is to impose a threshold on the values for every updatabale radio parameter and stop the communication if the values of the parameters fall outside the thresholds.

6.4 Jamming Attack

The jamming attack is the most common mode of attack for triggering denial of service (DoS) to legitimate primary and secondary users in a CRN. Jamming attacks could be of four types [65]: Constant jammer, Deceptive jammer, Random jammer, and Reactive jammer. A constant jammer sends out data packets continuously without any regards to other users on that channel. A deceptive jammer tricks a legitimate user to switch to "receive" state as they detect a constant stream of incoming data packets. A random jammer takes random breaks while sending jamming signals; during its jamming phase, it may behave either as a constant or random jammer. A reactive jammer senses the channel all the time and transmits the jamming signals upon sensing a communication in the channel. Jamming driven DoS attacks at the physical layer requires an attacker to use a device that is capable of emitting energy at the same frequency used by other devices to communicate and interfere with their communication. In [67], the authors describe an attack scenario involving a single cognitive radio that can repeatedly switch back and forth between several channels after sending the jamming packets in each of them for a fixed period. Jamming driven DoS attacks at the link layer [66] involve the attacker sending out packets on a specific radio channel forcing all the devices within the radio range to assume that the channel is not idle and postpone their data transmission.

Several detection techniques have been proposed for user at the devices to conclude whether they have been subjected to a jamming driven DoS attack. If a device never passes the carrier-sensing phase of the CSMA (Carrier Sense Multiple Access) medium access control protocol, then it could conclude that it is a victim of a DoS attack. At the physical layer, a strategy proposed [66] is to have a legitimate device collect enough data packets and build a statistical model to distinguish between normal and abnormal levels of noise on the channel. In [65], the authors propose a jamming detection technique that leverages the relationship between signal strength (SS) and packet delivery ratio (PDR): A node concludes itself to having been a victim of jamming attack if its SS is high and PDR is low, and none of its neighbors have a high SS as well as a high PDR. Another related technique, called the Location Consistency Checks technique, suggested in [65] is based on the idea that if all the nearby neighbors of a node have low PDR values, then either the node is being jammed or the quality of the links with its neighbors is poor. Given the above jamming detection techniques, two strategies for defense against jamming attacks have been suggested in the literature [66]: frequency hopping (switch to a different channel) or spatial retreat (legitimate users change their location to escape from the interference range imposed by an attacker).

6.5 Spectrum Sensing Data Falsification (SSDF) Attack

The SSDF attack (a.k.a. Byzantine attack) [69][70] happens when an attacker sends false local spectrum sensing results to its neighbors (for a distributed CRN) or a fusion center (for a

centralized CRN) to make them take a wrong spectrum sensing decision. A Byzantine attack on distributed CRNs is hard to control because the false information can propagate quickly; whereas, in a centralized CRN, the fusion center (that collects all the sensed data and makes a decision on which frequency bands are occupied and which are free) can lessen the impact of false information by comparing the data received from all the CR nodes.

One category of data fusion techniques proposed to detect the Byzantine attack are based on the idea [71] of summing up the number of sensing terminals reporting "busy" and if the sum is greater than a fixed threshold, then the channel is considered to have been occupied. While a threshold value of 1 (one attacker is sufficient to mislead the neighborhood) may trigger several false alarms; a larger value for the threshold could lead to detection misses (i.e., the presence of a primary user may not be detected) and could be still prone to Byzantine attack if multiple attackers collude.

Another category of data fusion techniques proposed to detect Byzantine attacks is based on the notion of trust factor/indicator, typically built up based on the past behaviors. The trust value for a node increases slowly with time due to good behavior but decreases quickly due to bad behavior [73]. In [68], the authors proposed a data fusion technique called the Weighted Sequential Ratio Test (WSRT) that takes into consideration both the actual status reported by a CR node as well as its reputation value (initialized to 0 and incremented by 1 for each correct local spectrum report). A similar trust-based scheme was proposed in [72] that (in addition to the regular nodes) also assigns a trust factor for permanently malicious nodes – "Always Yes" and "Always No" nodes – such that the reports from these malicious nodes help to identify the malicious nodes that are only sometimes faulty.

7. Conclusions

In this paper, we have presented an exhaustive review and analysis of a host of issues and mechanisms that have been proposed in the literature for cognitive radio networks – both for infrastructure-based and infrastructure less networks. We have analyzed the following four layers and the corresponding mechanisms/techniques/protocols in greater detail: Physical layer/spectrum sensing (transmitter detection, cooperative detection and interference-based detection); Medium access control (time-slotted and random access protocols for both infrastructure-based and ad hoc CRNs); Routing (protocol solutions based on full spectrum knowledge and local spectrum knowledge); and Transport layer (issues for effective design of new protocol solutions, and existing solutions based on cross-layered and layer-preserving approaches). Finally, the last section of the chapter analyzed in detail the various security attacks (control channel saturation attack, primary user emulation attack, jamming attack, objective function attack and spectrum sensing data falsification attack) and solutions that could be deployed to counter these attacks. The security attacks analyzed in this paper are characteristic of CRNs. In addition to these attacks, a CRN could be subjected to security attacks (for example, routing re-direction based sink-hole and Hello flood attacks on multi-hop topologies) that are characteristic of wireless networks in general.

From a design point of view, a common thread that should be prevalent in any proposed mechanism for CRNs is that the solution should not require the primary user to be capable of

adapting its transmission parameters due to the presence of the secondary CR user. In fact, a licensed user need not be even aware of the presence of the unlicensed CR users, and there should be no appreciable degradation in the quality of service for the primary users. While the solutions proposed for centralized and/or infrastructure-based CRNs are typically construed to provide performance benchmarks for the appropriate paradigm, the solutions proposed for distributed/cooperative and/or infrastructure less ad hoc CRNs capture the practical difficulties and performance bottlenecks in real-time implementations. Most of the active research conducted in the area of CRNs has been so far focused on spectrum sensing, allocation and sharing, and medium control access. Recently, the research community has also started looking at development of end-to-end solutions, starting from the routing protocols (see Section 4) and transport layer protocols (see Section 5), which are needed to fully realize the potential of cognitive radios from an application standpoint. Of course, security of the underlying CRN and the end users would also need to be a key ingredient/design criterion for any proposed solution.

References

[1] FCC, ET Docket No 03-222, "Notice of Proposed Rule Making and Order", December 2003.
[2] FCC, ET Docket No 02-135, "Spectrum Policy Task Force Report", November 2002.
[3] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," IEEE Journal of Selected Areas in Communications, vol. 23, no. 2, pp. 201–220, February 2005.
[4] 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, pp. 2127–2159, May 2006.
[5] Z. Han and K. J. R. Liu, "Resource Allocation for Wireless Networks: Basics, Techniques and Applications", Cambridge University Press, Cambridge, UK, 2008.
[6] A. Ghasemi and E. S. Sousa, "Collaborative Spectrum Sensing for Opportunistic Access in Fading Environment," Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 131-136, November 2005.
[7] A. Sahai, N. Hoven and R. Tandra, "Some Fundamental Limits on Cognitive Radio," Proceedings of the 42nd Allerton Conference, Monticello, October 2004.
[8] A. Sahai and D. Cabric, "A Tutorial on Spectrum Sensing: Fundamental Limits and Practical Challenges," Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, November 2005.
[9] D. Cabric, S. Mishra and R. Brodersen, "Implementation Issues in Spectrum Sensing for Cognitive Radios," Proceedings of the 38th Asilomar Conference on Signals, Systems and Computers, vol. 1, pp. 772-776, November 2004.
[10] A. Sahai, R. Tandra, S. M. Mishra and N. Hoven, "Fundamental Design Tradeoffs in Cognitive Radio Systems," Proceedings of the 1st International Workshop on Technology and Policy for Accessing Spectrum, 2006.
[11] R. Tandra and A. Sahai, "SNR Walls for Signal Detection," IEEE Journal of Selected Topics in Signal Processing, vol. 2, no. 1, pp. 4-17, February 2008.
[12] F. Weidling, D. Datla, V. Petty, P. Krishnan and G. Minden, "A Framework for RF Spectrum Measurements and Analysis," Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 573-576, November 2005.
[13] D-C. Oh, and Y-H. Lee, "Energy Detection based Spectrum Sensing for Sensing Error Minimization in Cognitive Radio Networks," International Journal of Communication Networks and Information Security, vol. 1, no. 1, pp. 1-5, April 2009.
[14] J. Vartiainen, H. Sarvanko, J. Lehtomki, M. Juntti, and M. Latva-aho, "Spectrum Sensing with LAD-based Methods," Proceedings of the 18th Annual IEEE International Symposium on Personal, Indoor, Mobile Radio Communications (PIMRC), pp. 1-5, 2007.

[15] T. Yucek and H. Arslan, "Spectrum Characterization for Opportunistic Cognitive Radio Systems," Proceedings of the IEEE Military Communications Conference, pp. 1805-1810, October 2006.
[16] W. Gardner, "Signal Interception: A Unifying Theoretical Framework for Feature Detection," IEEE Transactions on Communications, vol. 36, no. 8, pp. 897-906, August 1998.
[17] D. Cabric and R. W. Brodersen, "Physical Layer Design Issues Unique to Cognitive Radio Systems," Proceedings of the 18th Annual IEEE International Symposium on Personal, Indoor, Mobile Radio Communications (PIMRC), vol. 2, pp. 759-763, 2005.
[18] H. Tang, "Some Physical Layer Issues of Wide-band Cognitive Radio System," Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 151-159, November 2005.
[19] R. Chen and J. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," Proceedings of the 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, pp. 110-119, September 2006.
[20] S. Shankar, "Spectrum Agile Radios: Utilization and Sensing Architecture," Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 160-169m November 2005.
[21] FCC, ET Docket No 03-237, "Notice of Inquiry and Notice of Proposed Rulemaking", November 2003.
[22] Q. Zhao and B. Sadler, "A Survey of Dynamic Spectrum Access," IEEE Signal Processing Magazine, vol. 24, no. 3, pp. 79-89, May 2007.
[23] P. Wang, L. Xiao, S. Zhou and J. Wang, "Optimization of Detection Time for Channel Efficiency in Cognitive Radio Systems," Proceedings of Wireless Communications and Networking Conference, pp. 111-115, March 2008.
[24] A. Ghasemi and E. S. Sousa, "Optimization of Spectrum Sensing for Opportunistic Spectrum Access in Cognitive Radio Networks," Proceedings of IEEE Consumer Communications and Networking Conference, pp. 1022-1026, January 2007.
[25] Y. Pei, A. T. Hoang, and Y-C. Liang, "Sensing Throughput Tradeoff in Cognitive Radio Networks: How Frequently should Spectrum Sensing be carried out?," Proceedings of the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 5330-5335, September 2007.
[26] W. Y. Lee, and I. F. Akyildiz, "Optimal Spectrum Sensing Framework for Cognitive Radio Networks," IEEE Transactions on Wireless Communications, vol. 7, no. 10, pp. 845-3857, 2008.
[27] L. Luo, and S. Roy, "Analysis of Search Schemes in Cognitive Radio," Proceedings of IEEE Workshop on Networking Technologies for Software Defined Radio Networks, pp. 647-654, June 2007.
[28] H. Kim and K. G. Shin, "Efficiency Discovery of Spectrum Opportunities with MAC-Layer Sensing in Cognitive Radio Networks," IEEE Transactions on Mobile Computing, vol. 7, pp. 533-545, May 2008.
[29] S-Y. Lien, C-C. Tseng, and K-C. Chen, "Carrier Sensing based Multiple Access Protocols for Cognitive Radio Networks," Proceedings of IEEE International Conference on Communications, pp. 3208-3214, May 2008.
[30] C. Cordeiro, K. Challapali, and M. Ghosh, "Cognitive PHY and MAC Layers for Dynamic Spectrum Access and Sharing of TV Bands," Proceedings of IEEE International Workshop on Technology and Policy for Accessing Spectrum, p. 222, August 2006.
[31] P. Pawelczak, R. Venkatesha Prasad, L. Xia, and I. G. M. M. Niemegeers, "Cognitive Radio Emergency Networks – Requirements and Design," Proceedings of the IEEE Dynamic Spectrum Access Networks, pp. 601-606, November 2005.
[32] H. Su and X. Zhang, "CREAM-MAC: An Efficient Cognitive Radio-Enabled Multi-Channel MAC Protocol for Wireless Networks," Proceedings of the IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks, pp. 1-8, June 2008.
[33] L. Ma, C-C. Shen and B. Ryu, "Single-Radio Adaptive Channel Algorithm for Spectrum Agile Wireless Ad hoc Networks," Proceedings of the IEEE Dynamic Spectrum Access Networks, pp. 547-558, April 2007.
[34] C. Cordeiro and K. Challapali, "C-MAC: A Cognitive MAC Protocol for Multichannel Wireless Networks," Proceedings of the IEEE Dynamic Spectrum and Access Networks, pp. 147-157, April 2007.
[35] J. Zhao, H. Zheng, and G-H. Yang, "Spectrum Sharing through Distributed Coordination in Dynamic Spectrum Access Networks," Wireless Communications and Mobile Computing, vol. 7, no. 9, pp. 1061-1075, 2007.

[36] 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.

[37] H. Khalife, N. Malouch, and S. Fdida, "Multihop Cognitive Radio Networks: To Route or not to Route," IEEE Network Magazine, vol. 23, no. 4, pp. 20-25, 2009.

[38] A. C. Talay and D. T. Altilar, "ROPCORN: Routing Protocol for Cognitive Radio Ad hoc Networks," Proceedings of the International Conference on Ultra Modern Telecommunications & Workshops, pp. 1-6, October 2009.

[39] C. Xin, B. Xie, and C-C. Shen, "A Novel Layered Graph Model for Topology Formation and Routing in Dynamic Spectrum Access Networks," Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 308-317, 2005.

[40] C. Xin, L. Ma, and C-C. Shen, "A Path-centric Channel Assignment Framework for Cognitive Radio Wireless Networks," Mobile Networks and Applications, vol. 13, no. 5m pp. 463-476, 2008.

[41] X. Zhou, L. Lin, J. Wang and X. Zhang, "Cross-layer Routing Design in Cognitive Radio Networks by Colored Multi graph Model," Wireless Personal Communications, vol. 49, no. 1, pp. 123-131, 2009.

[42] Q. Wang and H. Zheng, "Route and Spectrum Selection in Dynamic Spectrum Networks," Proceedings of the 3rd IEEE Consumer Communications and Networking Conference, vol. 1, pp. 625-629, 2006.

[43] C. W. Pyo and M. Hasegawa, "Minimum Weight Routing based on a Common Link Control Radio for Cognitive Wireless Ad hoc Networks," Proceedings of the International Conference on Wireless Communications and Mobile Computing, pp. 399-404, 2007.

[44] Y. Shi and Y. Hou, "A Distributed Optimization Algorithm for Multi-hop Cognitive Radio Networks," Proceedings of the 27th IEEE Conference on Computer Communications, pp. 1292-1300, 2008.

[45] M. Xie, W. Zhang and K-K. Wong, "A Geometric Approach to Improve Spectrum Efficiency for Cognitive Relay Networks," IEEE Transactions on Wireless Communications, vol. 9, no. 1, pp. 268-281, 2010.

[46] H. Ma, L. Zheng, X. Ma and Y. Iuo, "Spectrum Aware Routing for Multi-hop Cognitive Radio Networks with a Single Transceiver," Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, pp. 1-6, 2008.

[47] G. Cheng, W. Liu, Y. Li and W. Cheng, "Spectrum Aware On-demand Routing in Cognitive Radio Networks," Proceedings of the 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 571-574, 2007.

[48] G. Cheng, W. Liu, Y. Li and W. Cheng, "Joint On-demand Routing and Spectrum Assignment in Cognitive Radio Networks," Proceedings of the IEEE International Conference on Communications, pp. 6499-6503, 2007.

[49] Z. Yang, G. Cheng, W. Liu, W. Yuan and W. Cheng, "Local Coordination based Routing and Spectrum Assignment in Multi-hop Cognitive Radio Networks," Mobile Networks and Applications, vol. 13, no. 1-2, pp. 67-81, 2008.

[50] B. F. Lo, "A Survey of Common Control Channel Design in Cognitive Radio Networks," Physical Communication, vol. 4, pp. 26-39, 2011.

[51] I. Pefkianakis, S. Wong and S. Lu, "SAMER: Spectrum Aware Mesh Routing in Cognitive Radio Networks," Proceedings of the 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 1-5, 2008.

[52] L. Ding, T. Melodia, S. Batalama and M. J. Medley, "ROSA: Distributed Joint Routing and Dynamic Spectrum Allocation in Cognitive Radio Ad hoc Networks," Proceedings of the 12th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, pp. 13-20, 2009.

[53] A. Chan, X. Liu, G. Noubir and B. Thapa, "Broadcast Control Channel Jamming: Resilience and Identification of Traitors," Proceedings of the IEEE International Symposium on Information Theory, pp. 2496-2500, 2007.

[54] P. Tague, M. Li and R. Poovendran, "Probabilistic Mitigation of Control Channel Jamming via Random Key Distribution," Proceedings of the 18th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1-5, 2007.

[55] L. Ma, C-C. Shen and B. Ryu, "Single-Radio Adaptive Channel Algorithm for Spectrum Agile Wireless Ad hoc Networks," Proceedings of the 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 547-558, 2007.

[56] L. Lazos, S. Liu and M. Krunz, "Mitigating Control-Channel Jamming Attacks in Multi-Channel Ad hoc Networks," Proceedings of the 2nd ACM Conference on Wireless Network Security, pp. 169-180, 2009.

[57] P. Tague, M. Li and R. Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks," IEEE Transactions on Mobile Computing, vol. 8, no. 9, pp. 1221-1234, 2009.

[58] R. Chen and J-M. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," Proceedings of the 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, pp. 110-119, Reston, VA, September 2006.

[59] O. Leon, J. Hernandez-Serrano and M. Soriano, "Securing Cognitive Radio Networks," International Journal of Communication Systems, vol. 23, no. 5, pp. 633-652, 2010.

[60] 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, pp. 25-37, 2008.

[61] L. Huang, L. Xie, H. Yu, W. Wang and Y. Yao, "Anti-PUE Attack based on Joint Position Verification in Cognitive Radio Networks," Proceedings of the International Conference on Communications and Mobile Computing, vol. 2, pp. 169-173, Shenzhen, China, April 2010.

[62] O. R. Afolabi, K. Kim and A. Ahmad, "On Secure Spectrum Sensing in Cognitive Radio Networks using Emitters Electromagnetic Signature," Proceedings of the 18th International Conference on Computer Communications and Networks (ICCCN), pp. 1-5, San Francisco, CA, August 2009.

[63] O. Ureten and N. Serinken, "Wireless Security through RF Fingerprinting," Canadian Journal of Electrical and Computer Engineering, vol. 32, no. 1, pp. 27-33, 2007.

[64] T. C. Clancy and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," Proceedings of the International Conference on Cognitive Radio Oriented Wireless Networks and Communications, pp. 1-8, Singapore, May 2008.

[65] W. Xu, W. Trappe, Y. Zhang and T. Wood, „The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," Proceedings of the ACM International Symposium on Mobile Ad hoc Networking and Computing, pp. 46-57, Urbana, IL, USA, May 2005.

[66] W. Xu, T. Wood, W. Trappe and Y. Zhang, "Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service," Proceedings of the 3rd ACM Workshop on Wireless Security, pp. 80-89, Philadelphia, PA, USA, January 2004.

[67] A. Sampath, H. Dai, H. Zheng and B. Y. Zhao, "Multi-channel Jamming Attacks using Cognitive Radios," Proceedings of the 16th International Conference on Computer Communications and Networks (ICCCN), pp. 352-357, Honolulu, HI, USA, August 2007.

[68] R. Chen, J-M. Park, Y. T. Hou and J. H. Reed, "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," IEEE Communications Magazine, vol. 46, no. 4, pp. 50-55, 2008.

[69] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127, Berkeley, CA, USA, May 2003.

[70] C. Mathur and K. Subbalakshmi, "Security Issues in Cognitive Radio Networks," Cognitive Networks: Towards Self-Aware Networks, pp. 284-293, Wiley, New York, 2007.

[71] A. Pandharipande et al., "IEEE P802.22 Wireless RANs: Technology Proposal Package for IEEE 802.22," IEEE 802.22 Working Group on WRANs, November 2005.

[72] P. Kaligineedi, M. Khabbazian and V. K. Bhargava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," IEEE International Conference on Communications, pp. 3406-3410, Beijing, China, May 2008.

[73] W. Wang, H. Li, Y. Sun and Z. Han, "Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks," Proceedings of the 43rd Annual Conference on Information Sciences and Systems, pp. 130-134, Baltimore, MD, USA, March 2009.

[74] J. Hernandez-Serrano, O. Leon and M. Soriano, "Modeling the Lion Attack in Cognitive Radio Networks," EURASIP Journal on Wireless Communications and Networking, vol. 2011, article id: 242304, 10 pages, 2011.

[75] D. Sarkar and H. Narayan, "Transport Layer Protocols for Cognitive Networks," Proceedings of the IEEE INFOCOM Workshops, March 2010.

[76] M. Di Felice, K. Roy Chowdhury and L. Bononi, "Modeling and Performance Evaluation of Transmission Control Protocol over Cognitive Radio Ad hoc Networks," Proceedings of the 12th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, pp. 4-12, 2009.

[77] K. R. Chowdhury, M. Di Felice and I. F. Akyildiz, "TP-CRAHN: A Transport Protocol for Cognitive Radio Ad-hoc Networks," Proceedings of the IEEE INFOCOM Conference, pp. 2482-2490, 2009.

[78] W. Y. Lee and I. F. Akyildiz, "Optimal Spectrum Sensing Framework for Cognitive Radio Networks," IEEE Transactions on Wireless Communications, vol. 7, no. 10, pp. 3845-3857, Ocotber 2008.

[79] A. M. R. Slingerland, P. Pawelczak, R. V. Prasad, A. Lo and R. Hekmat, "Performance of Transport Control Protocol over Dynamic Spectrum Access Links," Proceedings of the IEEE International Conference on Dynamic Spectrum Access Networks, pp. 486-495, April 2007.