Physical Communication 4 (2011) 26–39

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

A survey of common control channel design in cognitive radio networks

Brandon F. Lo *

Broadband Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 30332, United States

ARTICLE INFO

Article history:
Received 26 December 2010
Accepted 30 December 2010
Available online 4 January 2011

Keywords:
Channel hopping
Cognitive radio
Common control channel
Dynamic spectrum access
Medium access control
Neighbor discovery

ABSTRACT

Cognitive radio networks have been recognized as a promising paradigm to address the spectrum under-utilization problem. To improve spectrum efficiency, many operations such as sharing data in cooperative spectrum sensing, broadcasting spectrum-aware routing information, and coordinating spectrum access rely on control message exchange on a common control channel. Thus, a reliable and "always on" common control channel is indispensable. Since the common control channel may be subject to primary user activity, the common control channel design in cognitive radio networks encounters unprecedented challenges: cognitive radio users are unable to negotiate a new control channel when the original one is occupied by primary users. In this paper, the problem of common control channel design is presented by its classification, design challenges, design schemes, and its applications in network protocol layers. The issues of control channel saturation, robustness to primary user activity, limited control channel coverage, control channel security are identified as design challenges. Moreover, the major control channel design schemes such as sequence-based, group-based, dedicated, and ultra wideband approaches are presented. Lastly, the relation of the common control channel with radio interface, cooperative sensing, medium access control, and routing are discussed.

1. Introduction

The recent skyrocketing growth of the research on cognitive radio (CR) networks has shown the promises of the CR paradigm as the enabling technology to the spectrum under-utilization problem [1,2]. CR users improve spectrum efficiency by opportunistic spectrum access when the licensed spectrum is not occupied by the primary users (PUs). CR users also need to sense the spectrum and vacate the channel upon the detection of the PU's presence to protect PUs from harmful interference. To achieve these fundamental CR functions, CR users usually coordinate with each other by using a common medium for control message exchange. This common medium is known as a common control channel (CCC) [1–3].

A CCC in CR networks facilitates a variety of operations from transmitter–receiver handshake, neighbor discovery, channel access negotiation, topology change and routing information updates, to the cooperation among CR users [1,2]. Specifically, CR users show their existence by broadcasting control messages on the CCC for neighboring users in the proximity to maintain the contact and the network's connectivity. Moreover, CR users can cooperate and share their spectrum sensing data with each other by using the CCC to improve the detection of PUs [4]. More importantly, CR users need to inform each other on the changes of PU activity, spectrum availability, and network topology so as to improve the CR throughput and spectrum efficiency. Therefore, it is essential to devise CCC schemes that can reliably establish and efficiently maintain CCCs in CR networks.

The CCC design in CR networks is originated from the medium access control (MAC) in multi-channel wireless networks. In multi-channel environments, one channel commonly available to all network nodes is used for exchanging control messages to reserve data channels for data transmission. Such a dedicated CCC facilitates the handshake between the transmitting and receiving nodes.

* Tel.: +1 404 894 6616; fax: +1 404 894 7883.
E-mail address: brandon.lo@ece.gatech.edu.

1874-4907/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.phycom.2010.12.004

However, it may suffer from the *control channel saturation* problem when a large number of nodes access the control channel causing high control packet collisions and throughput degradation [5]. To address this problem, many multi-channel MAC protocols and CCC allocations schemes were proposed for multi-channel wireless networks [6]. As a result, these early CCC studies for legacy wireless networks pave the way for the CCC design in CR networks.

Although the concept of CCC is not new, the CCC design in CR networks faces several new challenges. The challenges arise in the following two aspects: *PU activity* and *spectrum heterogeneity*. First, unless the CCC can be allocated in the frequency band free from PUs, a CCC is susceptible to PU activity and can be occupied by PUs at any given time. Upon PU's return to the CCC, CR users face the difficulty in establishing a new CCC because they are unable to use the original CCC to negotiate a new one. Since this problem significantly complicates the CCC design in CR networks, the *robustness to PU activity* is one of CCC design challenges. Second, unlike multi-channel wireless networks where all channels are at the disposal of all users, CR users usually observe different sets of available channels, each of which is a subset of the set of all licensed channels. Due to this spectrum heterogeneity in CR networks, it is unlikely to find a channel commonly available to all users as the CCC. As a result, the area where CR users share the same CCC, called *CCC coverage*, is limited to a neighborhood in a CR network. Since it affects the efficiency of a control message broadcast and the incurred signaling overhead, CCC coverage is also a CCC design challenge. Even if a dedicated CCC is available to all users in the CR network, the globally available CCC can create a single point of failure and is susceptible to control channel jamming attacks. This raises another design challenge in *control channel security*.

Due to the unique CCC characteristics and challenges in CR networks, a CCC in a CR network is defined as a medium temporarily or permanently allocated in a portion of licensed or unlicensed spectrum commonly available to two or more CR users for control message exchange. Based on this definition, a CCC in CR networks may not be unique and may not always available. Notice that, with the definition, a CCC exists in all MAC or channel allocation schemes in CR networks. For those existing schemes [7–9] claiming that a CCC is not required or needed in the literature, the CCC is more appropriately termed *dedicated CCC*. In this paper, the problem of CCC design in CR networks is addressed first by identifying CCC design challenges. The CCC design schemes and their requirements are then introduced to demonstrate the strong relation between the CCC design challenges and the CR performance. Lastly, the applications of the CCC in different network protocol layers are discussed to show the universal usage of the CCCs in CR networks. The contribution of this paper is summarized as follows.

- *Identify CCC Design Challenges*: The CCC design challenges in CR networks are identified and comprehensively discussed. The primary challenges include control channel saturation, robustness to PU activity, CCC coverage, and control channel security.
- *Analyze CCC Design Schemes*: The design requirements of existing CCC schemes are introduced to provide the insights into the tradeoff between CR performance and CCC establishment overhead and how these schemes address the aforementioned design challenges.

The remainder of this paper is organized as follows: in Section 2, existing CCC design schemes are classified. In Section 3, the challenges and the requirements in CCC design are identified. In Section 4, major CCC design approaches and their performance are presented. In Section 5, the relation of CCCs with different network protocol layers are discussed. Finally, the survey is concluded in Section 6.

2. Classification of common control channel design

The classification of CCC design is the best place to understand the CCC design in CR networks from the bird's-eye view. The CCC design schemes have been classified in several ways in the literature. In [10,11], the authors divide CCC schemes into four categories: *dedicated control channel*, *common hopping*, *split phase*, and *multiple rendezvous control channel* (MRCC) according to the classification of multi-channel MAC protocols [6]. In [2], the CCC design approaches are classified as *in-band* and *out-of-band* based on whether or not data channels are shared by both control and data transmission. In each category, CCC solutions are further classified based on the area covered by the allocated CCCs. Moreover, in [3,12], the CCC designs are classified as *group/cluster-based*, *sequence-based*, and *dedicated* CCC depending on how CCCs are established in CR networks.

The classification based on multi-channel MACs is not suitable for the CCC designs in CR networks for the following reasons: (1) Split-phase approaches result in inefficient spectrum utilization because all nodes are tuned to one channel and most channels are idle during the control phase. These schemes are unlikely to be used in CR networks. (2) Common hopping requires the tight synchronization of all network nodes, which is unlikely to be achieved in a CR network with a large number of nodes. (3) Except for the dedicated CCC cases, CR users are likely to rendezvous on different CCCs owing to spectrum heterogeneity. As a result, multiple rendezvous is not appropriate to categorize a specific type of CCC schemes in CR networks. Therefore, in this paper, we extend the classifications in [2,3,12] and present the comprehensive classification of CCC designs in CR networks to include the overlay schemes and the subcategories in major CCC design approaches based on how CCCs are established.

As shown in Fig. 1, the CCC design classification is first divided into overlay and underlay CCC schemes. This first-level categorization reflects two primary spectrum sharing approaches in the CR paradigm. Contrary to the overlay approaches where the majority of CCC designs are centered, the underlay CCC schemes mainly utilize the ultra-wideband (UWB) transmission technology. Overlay approaches are then divided into in-band and out-band schemes as in [2]. In terms of CCC coverage, in-band approaches are local while the out-of-band schemes are mainly global. The in-band schemes are further classified

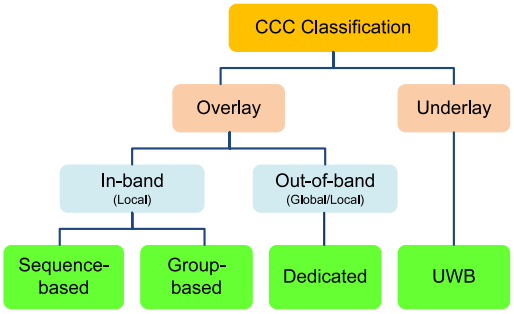


Fig. 1. Classification of common control channel design.

as two categories: link-based and group-based CCC designs. The out-of-band schemes are primarily composed of dedicated CCC designs. Finally, the link-based, group-based, and dedicated CCC designs are classified into subcategories based on the establishment methods. In the following, each level of classification is discussed.

2.1. Overlay vs. underlay

The CCC schemes are first classified as overlay and underlay approaches. For overlay CCC approaches, the CCC is permanently or temporarily allocated to the spectrum not used by the PUs. When the allocated CCCs are affected by PU activity, CR users must vacate the CCCs and re-establish the new CCCs in other available spectrum. For underlay CCC approaches, the CCC can be allocated to the same band used by PUs. By utilizing the spread spectrum techniques, control messages are transmitted in low power by using short pulses, which are spread over a large bandwidth such that the control transmission appears to PUs as noise. Although CR control messages and PU data are transmitted simultaneously in a licensed spectrum, the underlay CCC approach can be regarded as a dedicated CCC virtually not affected by PU activity. However, there are several issues such as the range of UWB transmission and extra UWB radio that limit its usage as effective CCC design options. The underlay UWB CCC schemes are discussed in detail in Section 4.4. For overlay CCC schemes, they are further classified as in-band and out-of-band schemes.

2.2. In-band vs. out-of-band

For in-band and out-of-band CCC schemes, the CCCs allocated to data channels are called in-band CCCs while the CCCs allocated in dedicated spectrum such as unlicensed bands or the spectrum licensed to CR network operators are called out-of-band CCCs. How the CCCs are allocated in the spectrum is strongly related to the coverage of CCCs. CCC coverage refers to the area where CR users can exchange control messages by one or more hops on the allocated CCC without changing the channel. Since the in-band CCCs are susceptible to PU activity varying from region to region, their coverage is local. On the other hand, the out-of-band CCCs are dedicated ones whose coverage is generally considered global to facilitate network-wide coordination without the switching latency and overhead. However, the coverage can also be local since the dedicated CCCs can be allocated to different bands in different geographical regions.

The in-band CCCs are allocated in licensed data channels, which are affected by PU activity. As a result, the main challenge of this approach is to re-establish the CCCs whenever PUs return to these channels. In addition to CCC establishment overhead, the control message overhead must also be minimized to achieve satisfying the CR data throughput. However, in some applications such as military or emergency networks where the allocation of dedicated CCCs may not be feasible, in-band CCC solutions provide an alternative way for control message exchange. Unlike in-band CCCs, out-of-band CCCs are generally not affected by PU activity, as all CR users know that the CCCs are always available in the dedicated spectrum. However, if out-of-band CCCs are allocated in unlicensed bands, they may not always be reliable because of the interference from other wireless services. If the out-of-band CCCs are allocated in the bands licensed to CR network operators, this seems to defy the principles of dynamic spectrum access where flexible spectrum assignment is necessary for improving spectrum utilization efficiency, not to mention the extra license cost to the operators. Nevertheless, compared to in-band ones, out-of-band CCCs provide a relatively more reliable CCC establishment for control purposes.

2.3. Major CCC design schemes

The overlay/underlay and in-band/out-of-band classifications provide the top two level classification of CCC design approaches. As in [3,12], more precise CCC classification can be obtained by using CCC establishment. Based on this method, the CCC designs are classified as three methods: *sequence-based* [13–17], *group-based* [18–21,3], and *dedicated* [22–26,12]. The first two are the in-band schemes while the dedicated CCC design is the out-of-band approach. The last major design scheme is the underlay UWB CCC design [27,28,17,29]. All major design schemes and its subcategories are introduced in Section 4.

All the CCC design schemes considered in this paper are tabulated in Table 1. In the table, the categorized type, in-band/out-of-band CCC allocation, and CCC coverage are listed for each CCC design scheme. In addition, the number of radio transceivers required (*Radio*) and whether or not the CCC design requires the synchronization of CR users (*Sync*) and includes the mechanism for neighbor discovery (*Disc*) are listed next. The last four columns indicate whether the proposed schemes address the challenges of control channel saturation (*Sat*), robustness to PU activity (*PU*), the evaluation of CCC coverage (*Cov*), and control channel jamming (*Jam*). These CCC design challenges will be discussed in Section 3.

3. Control channel design challenges

The design of CCC in CR networks faces a variety of challenges. Some of these challenges such as control channel saturation are originated from multi-channel wireless networks while some of those such as robustness to PU activity are new in CR networks. Since the importance of these challenges has been emphasized in

Table 1
CCC design schemes in CR networks.

CCC design schemes	Type	Allocation	Coverage	Radio	Sync	Disc	Sat	PU	Cov	Jam
Baldo et al. (NC^4-MAC/DSA) [30,16,31]	Sequence	In-band	Local	Single	Yes	No	No	Yes	No	No
Bian et al. (quorum-based) [14,32]	Sequence	In-band	Local	Single	Yes	No	Yes	Yes	No	No
Cormio and Chowdhury (AMRCC) [15,33]	Sequence	In-band	Local	Single	No	Yes	No	Yes	No	No
DaSilva and Guerreiro (sequence based) [13]	Sequence	In-band	Local	Single	Yes	No	No	Yes	No	No
Kondareddy and Agrawal (SYN-MAC) [7]	Sequence	In-band	Local	Two	Yes	Yes	Yes	Yes	No	No
Lazos et al. [34]	Sequence	In-band	Local	Single	Yes	No	No	No	No	Yes
Liu and Ding (ESCAPE) [35]	Sequence	In-band	Global	Single	No	Yes	No	Yes	No	No
Xin and Cao [9]	Sequence	In-band	Local	Single	No	No	No	Yes	No	No
Zhao et al. (POMDP) [36,37]	Sequence	In-band	Local	Single	Yes	No	No	Yes	No	No
Chen et al. (CogMesh) [18]	Group	In-band	Local	Single	No	Yes	Yes	Yes	Yes	No
Chen et al. (Swarm Intelligence) [19]	Group	In-band	Local	Single	No	Yes	No	Yes	Yes	No
Cordeiro and Challapali (C-MAC) [38]	Group	In-band	Local/global	Single	Yes	Yes	Yes	Yes	Yes	No
Doerr et al. [39,20]	Group	In-band	Local/global	Single	No	No	No	No	No	No
Kim and Yoo (DCP-CCC) [40]	Group	In-band	Local	Single	No	Yes	No	Yes	No	No
Lazos et al. (SOC) [21]	Group	In-band	Local	Single	No	Yes	No	Yes	No	No
Lo et al. (ERCC) [3]	Group	In-band	Local	Two	No	Yes	Yes	Yes	Yes	No
Ma et al. (SRAC) [41]	Group	In-band	Local	Single	No	No	Yes	No	No	Yes
Zhao et al. (HD-MAC) [42]	Group	In-band	Local	Single	No	Yes	Yes	No	No	No
Chowdhury and Akyildiz (O-CCC) [12]	Dedicated	Out-of-band	Global	Single	No	Yes	Yes	Yes	Yes	No
Hamdaoui and Shin (OS-MAC) [23]	Dedicated	Out-of-band	Global	Single	No	Yes	No	No	No	No
Jia et al. (HC-MAC) [24]	Dedicated	Out-of-band	Global	Single	No	No	No	Yes	No	No
Le and Hossain (OSA-MAC) [25]	Dedicated	Out-of-band	Global	Single	Yes	No	Yes	No	No	No
Ma et al. (DOSS MAC) [43]	Dedicated	Out-of-band	Global	Three	No	No	Yes	No	Yes	No
Montamedi and Bahai [22]	Dedicated	Out-of-band	Global	Two	No	No	No	No	No	No
Raychaudhuri and Jing (CSCC) [44,45]	Dedicated	Out-of-band	Global	Two	No	Yes	No	No	No	No
Su and Zhang (Opp. MAC) [46,26]	Dedicated	Out-of-band	Global	Two	Yes	Yes	Yes	No	No	No
Su and Zhang (CREAM-MAC) [47]	Dedicated	Out-of-band	Global	Two	No	No	No	Yes	No	No
Cabric et al. [27]	UWB	Both	Local	Two	No	No	No	No	No	No
Masri et al. [17,29]	UWB	Both	Local	Two	No	Yes	No	No	No	No
Sahin and Arslan [28]	UWB	Both	Local	Two	No	No	No	No	No	No

the literature, existing CCC solutions have been trying to address some if not all these challenges in the CCC design. Thus, we would appreciate more how those CCC solutions are devised in Section 4 by understanding these design issues first in this section.

The CCC design challenges in spotlights include control channel saturation [43,41], robustness to PU activity [2,3], CCC coverage [2], and control channel security [41].

3.1. Control channel saturation

Control channel saturation [5] refers to the throughput degradation phenomenon in wireless networks when the collision rate of control packets is high due to the large network load. In other words, the capacity of the CCC cannot accommodate the control traffic from a large number of users for satisfying performance. Although this problem is more likely to occur on a dedicated CCC, it can occur in other types of CCCs. For example, this problem is termed *rendezvous convergence* in [14,32] to indicate the rendezvous of a large number of neighboring users on the same channel by using sequence-based CCC designs. However, proper CCC design can effectively mitigate this problem. For example, CCC bandwidth can vary with control traffic load to reduce the possibility of saturation. Moreover, sequence-based CCC approaches diversify the allocated CCCs for different node pairs over different frequencies such that each CCC is not shared by a large number of nodes. This problem is related to the CCC bandwidth, the node density in the area sharing the same CCC, the transmission range of CR users, and the amount of control traffic.

In [43], three techniques are adopted to alleviate the saturation problem: (1) limit the control traffic on the CCC, (2) adjust the bandwidth ratio of the CCC over the data bands, and (3) allow slow migration of the CCC based on the traffic load. First, limiting the amount of control traffic is application-dependent. For example, the amount of control traffic on the CCC in cooperative sensing schemes depends on whether or not the local sensing data is quantized and how often the local sensing data is reported. Second, the adjustment of bandwidth ratio is not always feasible because the CCC bandwidth is predetermined and usually the same as data channel bandwidth in many in-band CCC schemes. The last technique involves moving the CCC to a better channel in terms of channel quality and bandwidth efficiency. This is generally desired in the CCC design.

In [41], dynamic channelization is proposed to address the CCC saturation problem. In this approach, an atomic channel is defined as a basic unit of b Hz for CCC allocation. When the CCC migration is required, a composite channel centered at new carrier frequency can be formed by combining the atomic channels. For example, the CCC is originally allocated at frequency f_0 with bandwidth b. The new CCC centered at $f = f_0 + mb$, $m = 0, \pm 1, \pm 2, \ldots$ with bandwidth kb, $k = 1, 3, 5, \ldots$, can be obtained by the channelization. In Fig. 2, the adaptive CCC channelization is illustrated for the case of $(m, k) = (4, 3)$. This scheme provides the mechanism to utilize the original set of

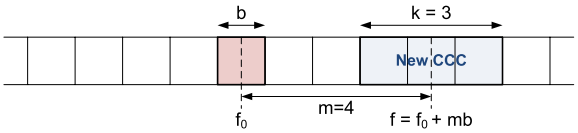


Fig. 2. Dynamic channelization for new CCC $(m, k) = (4, 3)$ [41].

channels to form a logical CCC of larger bandwidth and better quality to alleviate the saturation problem.

3.2. Robustness to PU activity

The primary CCC design challenge in CR networks is how to maintain control communications when PUs appear in the allocated CCC. While many out-of-band dedicated CCCs allocated to licensed or unlicensed bands are assumed to be free of PU activity, the primary concerns of in-band CCC schemes are the impact of PU activity. The robustness to PU activity can be evaluated by how soon the CCC can be re-established if the original one is occupied by PUs.

In [35], a channel evacuation protocol is proposed to notify CR users in the event of a PU's return to the CCC. When a PU is detected, the CR user broadcasts a predefined warning message to other users such that other users can immediately stop data transmission to avoid interfering with the PU. Since the warning messages are sent as a CDMA signal by using a predefined spreading code, they can tolerate the interference from the PU and produce minimum interference to the PU. Moreover, multiple users can send the notifications that can be reliably received by other users with little coordination. This scheme provides a reactive way of protecting PUs from CR user transmission in response to PU's return. However, it does not address the problem of how to reestablish the new CCC.

In the study of [10], a sequence-based hopping CCC (MRCC) scheme is considered robust to PU activity owing to the diversity of CCC allocation over all channels at the cost of stringent synchronization and the difficulty for control message broadcast. On the other hand, a group-based CCC scheme can provide the robustness to PU activity if re-grouping after PU's return on the CCC incurs low CCC establishment overhead. The robustness issue of these two design schemes are further discussed in Sections 4.1 and 4.2. By the nature of their schemes, dedicated and UWB CCCs are generally the most robust to PU activity without much design effort.

3.3. CCC coverage

One of the operations on a CCC is control message broadcast. Due to spectrum heterogeneity, it is unlikely for all CR users to listen to the same channel. As a result, the coverage of a CCC is limited to an area where a set of CR users are tuned to the same channel for control message exchange. Since large CCC coverage facilitates control packet forwarding and incurs less control signaling overhead, it is usually desirable to increase the CCC coverage. However, increasing the CCC coverage is not always possible and can be quite a challenge.

For sequence-based CCC design, the CCC coverage is usually limited to a node pair because the design is mainly concerned with the rendezvous of a transmitting node and a receiving node. For group-based CCC design, on the other hand, the CCC coverage varies with the group size depending on the grouping algorithms. For example, the coverage is limited to one-hop neighbors of the clusterhead in the clustering scheme [18]. The cluster size and the CCC coverage can be increased b cluster merging algorithms. For other grouping-based schemes, the CCC coverage may be increased by the majority votes of neighbors [19,3].

3.4. Control channel security

While the CCCs facilitate cooperation among CR users and other network operations, they are exposed to the risks of security attacks. Among those attacks, control channel jamming is the most effective way to destroy the entire network systems. This is because CCCs is the easy target for the single point of failure. By injecting a strong interference signal to the control channel, the attackers can disable any reception of valid control messages at the CR receivers, which can result in the denial of service (DoS). Compared to jamming the entire band, it is more energy efficient and effective by several orders of magnitude for the attackers to jam the CCC [48,49]. Thus, designing a CCC scheme resilient to control channel jamming attack is crucial to the reliability of the CCC and the entire network.

Traditionally, spread spectrum techniques are utilized to mitigate the jamming attacks by introducing the pseudo random channel access unknown to attackers. However, they become ineffective if any compromised CR user reveals the pseudo-random number (PN) sequences. Moreover, the compromised users cannot be easily identified under jamming. To deal with these problems, there are two main CCC anti-jamming approaches: (1) dynamic CCC allocation [41,34] and (2) CCC key distribution [48–50]. Although these anti-jamming schemes may not be specifically proposed for CR networks, they can be utilized to mitigate the control channel jamming problem in CR networks.

3.4.1. Anti-jamming by dynamic CCC allocation

The dynamic CCC allocation methods combat control channel jamming by dynamically allocating the CCC to maintain the control communications in response to jamming attacks. The dynamic allocation can be achieved by (1) cross-channel communication [41] and (2) frequency hopping [34].

The cross-channel communication scheme proposed in [41] utilizes the fact that successful communications under jamming attack only require CR users receiving messages on a channel not affected by the jamming signals. In other words, CR users can continue to transmit on the jammed channel under interference and notify others the new CCC for receiving control messages if the receiving nodes are free of jamming. As a result, the channels for transmitting and receiving control messages can be different to maintain the control message exchange with neighbors under jamming. Although this scheme provides

a mechanism to maintain control communications under jamming, it incurs high channel switching overhead with a single transceiver. In addition, any CR user compromised by the jammer will receive the notification of CCC change and be able to jam the new CCC.

In addition to cross-channel communication, another dynamic control channel allocation scheme based on hopping sequences is proposed in [34] to mitigate the control channel jamming attacks in cluster-based ad hoc networks. In this method, the clusterhead (CH) of each cluster determines the hopping sequences and the operating control channels within the cluster. During the jamming attack, the affected area is reduced due to the clustering of the network. Since the CCCs are inserted in the sequences, CR users hopping on different sequences in the cluster can rendezvous on the predetermined CCC in the designated time slots without knowing the hopping sequences of others. In addition, the compromised cluster members can be identified if they follow their unique hopping sequences. On the other hand, all hopping sequences will be known to the jammer and all CCCs will be jammed if the CH is compromised. In this case, it can only be resolved by the rotation of CHs so that new sequences including the designated CCCs are assigned by the new CH. Thus, this method temporarily and intermittently restores the CCC over time and frequency until the jammer is removed.

3.4.2. Anti-jamming by CCC key distribution

The second anti-jamming approach hides the CCC locations from the attackers by using the key distribution techniques. In this approach, each authorized user with a valid key will be able to locate the allocated CCCs by using keyed hash functions. Since the control messages are repeatedly transmitted on multiple CCCs, any compromised nodes having only partial keys in the key space will not be able to jam all the CCCs. Thus, control information exchange can be maintained by sufficiently large key distribution and duplicate messages under jamming attacks.

The jamming-resilient key assignment can be polynomial-based [48] or randomly distributed [49,50]. In [48], the polynomial-based scheme utilizes the key space consisting of $p \times q$ keys and repeated control transmission by simultaneously sending the control message over q CCCs in each of p time slots in a period. Each user including the malicious ones can be identified by a unique polynomial over the Galois field $GF(q)$ with degree $\leq c$. This scheme guarantees at least one CCC access in a period less than $T \log_T N$ time slots with at most $(T \log_T N)^2$ duplicate control messages when T out of N users are compromised and become traitors to jam the CCCs. Since this scheme utilizes the key space size in terms of a sufficiently large number of time slots (p) and number of CCCs (q) to combat the jamming by T compromised users, it may incur large control retransmission overhead and delay when T is large. More importantly, the number of traitors T is unknown in advance. As a result, once the number of traitors is greater than a threshold guaranteed by the key space size, the system performance degrades considerably.

To counter the shortcomings of the polynomial-based scheme, a random key distribution scheme is proposed in [49,50] for CCC access under node capture jamming attacks. Similar to [48], this scheme utilizes the CCC keys to mask the CCC allocation in time slots with duplicate control transmission on multiple CCCs. The random CCC key assignment reduces the risks of the key assignment structure being learned from the attackers. That is, by increasing the diversity of keys assigned to users, authorized users also increase the probability of holding keys unknown to compromised users. However, this method also increases the communication and storage overhead due to the increase of the number of keys. To limit the key space size and the corresponding storage overhead, the keys are periodically reused in time slots. To prevent the attackers from knowing CCC locations by finding the correlation in transmission patterns, the cryptographic hash functions are used to map the CCC keys to the allocated CCC frequency and time slot for CCC relocation in each key reuse period. Furthermore, the compromised users can be identified by using statistical estimation based on the likelihood of users being compromised.

3.4.3. Integrity of control messages

In addition to control channel jamming where the availability of CCC is concerned, another level of control channel security concerns with the authentication of users and the integrity of control data being transmitted on CCCs.

In [51], the proposed CCC security framework includes an authentication phase followed by encrypted transactions for channel negotiation between the transmitter–receiver pair to ensure secure communications on CCCs in CR ad hoc networks (CRAHNs). Although this security procedure can prevent eavesdropping and unauthorized access to the CCC, it cannot exclude the access of the compromised users and the manipulation of the control data. For example, CR users share their spectrum sensing data on CCCs to improve the probability of detection in cooperative sensing. The compromised users in this case can manipulate spectrum sensing data in encrypted control messages after passing the authentication. As a result, additional security measures are required to detect these malicious users and the manipulation of control information. Since the integrity of control message contents is application-dependent, it is beyond the scope of this paper. Interested readers can find the discussion of security issues in cooperative sensing in [4].

3.4.4. Research challenges

Regardless of its important in CR networks, control channel security is seldom addressed in the literature. Although existing anti-jamming techniques may be applied to CCC designs in CR networks, new challenges in CR networks cannot be well-addressed by those existing solutions.

- *Impact of jamming on PU activity*: When CR networks are under jamming attacks, primary networks are most likely under the same attacks, and vice versa. This is because CR networks share the licensed spectrum with primary networks. As a result, PUs will change their behavior or activity patterns to combat jamming, which in turn affects the CCC allocation in CR networks. In other words, the CCC allocation under the circumstances is

exacerbated by both the PU activity change and the jamming. To the best of our knowledge, this issue has not been investigated in the literature.

- *CCC jamming in CRHANs under node capture attacks*: The key distribution schemes require the secure authority in CR networks to handle the key assignments. Such an authority is not available in CRHANs. On the other hand, the cluster-based dynamic CCC allocation scheme in [34] cannot counter jamming and guarantee the CCC access when the CH is compromised. Therefore, it is a challenge to design a jamming-resilient CCC scheme for CRAHNs under node capture attacks.

4. Control channel design schemes

In this section, major CCC design schemes are introduced including sequence-based, group-based, dedicated, and UWB CCCs.

4.1. Sequence-based CCC design

In sequence-based control channel design, control channels are allocated according to a random or predetermined channel hopping sequence. The primary goal of this design is to diversify the control channel allocation over spectrum and time spaces in order to minimize the impact of PU activity. Since CR users may use different hopping sequences, different neighboring pairs in a neighborhood may communicate on different control channels. As a result, this approach, also known as multiple rendezvous control channel (MRCC) in the literature, may reduce the number of control channels affected by a PU's return. In the sequence-based CCC design, the channel hopping sequence is the key element for dynamic channel access. The construction of hopping sequences can be pseudo random [16], permutation-based [13], adaptive MRCC-based [15], or quorum-based [14].

4.1.1. Channel hopping sequence

The simplest predefined pattern for channel hopping is the sequential channel hopping in round robin fashion. In SYN-MAC protocol [7], all CR users in a multi-hop CR network are synchronized to successively switch to one channel for control access in predefined time slots. Each user can contend for channel access in the time slot and reserve the channel for data transmission with its neighbor. With a dedicated control radio, each node can exchange control messages in the predefined control slot while data transmission is ongoing in another channel. When a PU returns to a channel, the CR user observing this activity can notify its neighbor in the control slots commonly available to them. Although this scheme does not require a dedicated CCC and control slots are predefined in time and frequency, it has several disadvantages. First, control message exchange is not always feasible because CR users have to wait for next available control slot if the current one is occupied by a PU. As a result, CR users may not respond to PU activity in a timely fashion, not to mention throughput degradation may occur. Second, SYN-MAC requires tight synchronization, which may be difficult to achieve in a multi-hop environment. Lastly, sequential frequency hopping in predefined time slots is an easy target for control channel jamming.

One of techniques to introduce randomness and certain desired properties to channel hopping sequence is permutation. In the permutation-based sequence scheme [13], CR users construct non-orthogonal channel hopping sequences by using the permutation of available channels to increase the probability of two CR users hopping to the same channel. It is shown that the expected time to rendezvous (TTR), the time for two CR users to meet each other on a channel, is bounded by the quadratic function of the number of available channels. As a result, it may take a long time to find a neighboring node on a channel for control message exchange, especially when the number of available channels is large. Although the channel newly occupied by PUs can be removed from the hopping sequence in the event of the PU's return, the hopping sequence is predefined and is not adaptable to new channel opportunities. In addition, the proposed scheme does not address the issue of two CR users observing different available channels. In this case, the expected TTR is not bounded and it may take an even longer time for two CR users to rendezvous.

To address the issues in [13], an adaptive multiple rendezvous control channel (AMRCC) scheme is proposed in [15]. In this scheme, a channel ranking table is first established with channels in the order of increasing PU activity based on the results of periodic sensing. A biased pseudo-random sequence is then generated with smaller values occurring more frequently in the sequence. Finally, the adaptive hopping sequence is constructed by mapping the biased pseudo-random sequence to the channel ranking table such that the channel with smaller interference with PUs appears more times in the hopping sequence. By allocating a longer slot to the highest ranking channel, the proposed scheme with variable slots can compensate for the performance degradation caused by a long sequence as the number of available channels increases. Moreover, unlike [13], this scheme does not require tight synchronization between CR users for channel hopping. The handshaking routine provided by this scheme ensures a pair of CR users are synchronized by exchanging packets for synchronization and seed exchange when they rendezvous. Though PU activity is considered in the hopping sequence, the main drawbacks of AMRCC are twofold: (1) The average TTR may not be bounded, which may result in long CCC link establishment time. This is especially true for the sequence with a large number of available channels. (2) There is no guarantee on the CCC coverage beyond the rendezvoused node pair.

In [14], a quorum-based scheme is proposed for CCC establishment in CR networks. The channel hopping sequence constructed from quorum systems can increase the overlapping of multiple sequences to facilitate the rendezvous of two or more CR users with reduced and bounded average TTR. A quorum is an element of the system S (quorum system) that satisfies the intersection property: $p \cap q \neq \emptyset$, $\forall p, q \in S$. Based on this property, a cyclic quorum system can be constructed by a relaxed cyclic (n, κ)-difference set $D \subset \mathbf{Z}_n$, where n is the number of channels and κ is the number of elements in D.

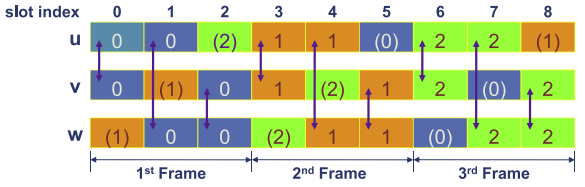


Fig. 3. Quorum channel hopping system with $(n, \kappa) = (3, 3)$ [14].

Depending on the value of κ $\left(\kappa \approx \sqrt{n} \text{ or } \kappa = \left\lceil \frac{n+1}{2} \right\rceil\right)$, two synchronous channel hopping systems can be constructed from the majority and minimal cyclic quorum systems to minimize the TTR and maximize the frequency diversity of rendezvous channels, respectively. By assuming at least one commonly available channel and utilizing the rotation closure property of quorum systems, the proposed asynchronous maximum overlapping hopping system in [32] enables at least one rendezvous in N^2 slots under the impact of PU activity, where N is the total number of channels. If a PU returns to the CCC for rendezvous, all quorum-based channel hopping systems simply replace the CCC with a randomly selected available channel to avoid interfering with PUs. While this may increase the TTR by a factor of N for synchronous quorum systems, it preserves the desired properties of quorum systems in the hopping sequences. In Fig. 3, a quorum channel hopping system $S = \{\{0, 1\}, \{0, 2\}, \{1, 2\}\}$ over $\mathbf{Z}_3 = \{0, 1, 2\}$ is illustrated with $(n, \kappa) = (3, 3)$.

4.1.2. Research challenges

Due to the diversity of CCC allocation in time and frequency, sequence-based CCC designs are in general affected less by PU activity and jamming. However, they establish connections on a link-by-link basis and thus have difficulty in supporting control broadcast without incurring a high overhead. Moreover, the hopping sequences are not adaptable to PU activity. In summary, the challenges of sequence-based designs are the following:

- *Sequence design for PU activity*: Most sequence-based schemes react to PU activity *after* the sequences are constructed. To minimize the impact on the rest of the sequences, the common approaches are to simply remove PU-occupied channels from the sequences or replace them with other channels. However, to improve the performance and the interruption of CCC allocation, it is desired to consider or even predict PU activity in constructing the hopping sequences.
- *Sequence design for CCC coverage*: Sequence-based designs seldom consider the control broadcast in the sequence. To support broadcast, a novel hopping scheme can be devised to facilitate regular control broadcast for the rendezvous of the nodes in a neighborhood while regular link-by-link based hopping is used for other control purposes or data transmission.

4.2. Group-based CCC design

Regardless of spectrum heterogeneity in CR networks, a control channel can be allocated to a channel commonly available to a group of CR users in proximity. This can be achieved because CR users usually observe similar spectrum availability in a neighborhood. By grouping CR users that uses a common channel as the CCC in a local area, group-based CCC designs facilitate control message broadcast within the group. As a result, compared to sequence-based schemes, the group-based schemes can generally achieve a better CCC coverage. However, control channel saturation can still occur if the node density of the group is high. Moreover, how efficient the group responds to PU activity and control channel jamming attacks depends on the grouping schemes and algorithms. Some group-based schemes select CCCs after forming groups while others form groups according to the availability of common channels. Due to the capability of regrouping, the latter approach is more robust to PU activity and is jamming-resilient. The challenges in group-based designs come from the inter-group communication that requires the delivery of control messages between two neighboring groups with different allocated CCCs. Thus, different grouping techniques have been developed for CCC allocation and message broadcast, which can be divided into two broad categories: (1) neighbor coordination [42,38,19,39,3] and (2) clustering [18,21] schemes.

4.2.1. Neighbor coordination

CR users can form groups by the coordination of neighbors. By exchanging information among neighboring users, the best channel can be selected as the CCC based on the information collected from all the users in the neighborhood.

A distributed coordination scheme is proposed in [42] to form groups according to spectrum heterogeneity in the CR network. After initial neighbor discovery, each CR user knows its neighbor and their available channels. To select CCCs, CR users vote for the channel commonly available to the largest number of neighbors and exchange the voting information by broadcast until all neighbors are connected. This distributed voting scheme enables the largest connectivity in the neighborhood via CCC selections. In addition, by using the dedicated control window at the beginning of each MAC frame, the CR user connected to different groups can send group beacons and the control messages to a specific group on the CCC. However, this scheme has two shortcomings. First, CCC selection requires messages to be broadcast when the CCC is not yet available. As a result, the CCC establishment overhead can be high. For this reason, regrouping and new CCC selection may not promptly respond to PU activity change. Second, when a PU occupies the CCC, the notification of new CCC is broadcast on the original one, which results in interference with PUs.

Inspired by the social behavior of insects called swarm intelligence, a distributed CCC assignment scheme is proposed in [19]. In this scheme, CR users exchange quantized channel quality information by regularly broadcasting Hello messages and adaptively update their choice of control channels according to the decision of the majority of neighbors. As more CR users gradually agree upon the selected CCCs, this method reduces the number of CCCs in the network and thus increasing the CCC coverage. However, it is unclear how Hello messages can reach the

neighbors if a PU returns to the CCC and how CR users communicate with neighbors in different groups. If CR users must listen to different CCCs of their neighbors in different groups to maintain connectivity, the CCC assignment in this scheme may fluctuate with the choices of neighbors when two neighboring groups observe heterogeneous channel conditions. Thus, the performance of this method may not be consistent or stable in some cases. Moreover, since the adaptability of this scheme relies on frequent Hello message exchange, high broadcast rate could result in control signalling overhead.

One of the major challenges in group-based design is the efficiency of reacting to PU activity and reestablishing a new CCC. In [3], a distributed CCC design scheme is proposed for efficient recovery of CCCs in response to PU's return. In this method, CR users maintain the ordered common channel list based on local sensing results and neighbors' channel list information. Since this list combines local preference with neighbors' choices of CCCs, it removes possible oscillation of CCC selections. When a PU occupies the CCC, all CR users in the neighborhood autonomously rendezvous on the new CCC individually selected from the top choice of their list to reestablish the link without any message exchange. This ensures that the network's connectivity can be maintained to the largest degree in a timely fashion under the circumstances. Though this scheme requires the exchange of a common channel list among neighbors, the control overhead can be justified by the robustness to PU activity required by network functions in CRHANs. Other issues such as CCC coverage, the interference from PU are also addressed in this scheme.

4.2.2. Clustering

Clustering is a popular grouping technique in distributed wireless networks. CR users are divided into clusters based on cluster formation algorithms. One member of the cluster is elected as the clusterhead (CH), which acts as the central entity for coordination. As a result, the CH selects one channel commonly available to all cluster members as the CCC of the cluster. Since neighboring clusters use different channels as the CCC, the CHs or the cluster members on the cluster border are responsible for inter-cluster communication. For CCC designs, how clusters are formed is related to how the CCC is allocated, or vice versa. PU activity and jamming attacks, which may force the CCC to change, directly affect the clusters' maintenance and reconfiguration. Thus, the efficiency of cluster formation and reconfiguration algorithms has the large impact on the CCC establishment overhead.

The authors in [18] proposed a one-hop clustering structure with a CCC selected by the CH of each cluster. The clusters are formed by the neighbor discovery process via channel scanning and beacon broadcast. Since the CH is the user initiating the beacon broadcast, the initial clustering is not optimal. To minimize the number of clusters and corresponding CCCs, the cluster optimization algorithm is proposed in [52] based on the problem of finding the minimal dominating set. However, this cluster reconfiguration process incurs large control overhead among clusters. It may not provide a stable and responsive change to PU activity. In addition, the coverage of a CCC is limited to the area of a cluster, which is the one-hop neighbors of the CH. Thus, this heuristic clustering scheme is not efficient in response to highly dynamic PU activity.

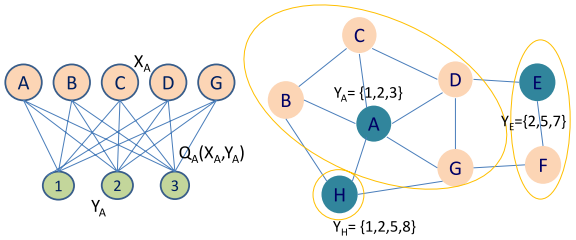


Fig. 4. (a) Maximum edge biclique constructed by CR user A and (b) clustering using SOC [21].

To improve the efficiency of cluster formation and provide stable network partition, the spectrum-opportunity clustering (SOC) design in [21] is formulated as a maximum edge biclique problem. The proposed scheme aims to balance the tradeoff between the number of common channels and the number of nodes (cluster size) in a cluster. First, a set of CR users and a set of channels are two disjoint sets of a bipartite graph in which the channels available to CR users are connected by edges. A biclique is a bipartite graph when a edge connects each node to each channel. That is, a biclique represents a cluster where all cluster members have a set of channels in common. As a result, the proposed greedy algorithm enables each user to find the biclique with the largest number of edges. CR users then exchange their biclique graphs and compare them in terms of channel size and cluster size. The CR users in proximity will converge to the largest biclique representing the best clustering in the neighborhood. In Fig. 4, the maximum edge biclique constructed by CR User A is illustrated. $Q_A(X_A, Y_A)$ represents the cluster A with cluster member set $X_A = \{A, B, C, D, G\}$ and the common channel set $Y_A = \{1, 2, 3\}$. The clustering after convergence shows three clusters with clusterheads A, E, and H. For inter-cluster communications and the CCC change to avoid the encounter with PUs, the cluster-wide channel hopping over all CCCs of the cluster is used. However, the hopping of the entire cluster requires strict synchronization among cluster members. More importantly, neighboring clusters may not be able to communicate with each other by such hopping. For example, if the sets of common channels for two neighboring clusters are 1, 2, 3 and 4, 5, respectively, these two clusters are still isolated with the control channel hopping.

4.2.3. Research challenges

Group-based design schemes facilitate control broadcast within a group and achieve better CCC coverage than the sequence-based designs. Since the CCC in a group changes only if it is interfered by PU activity or jamming, efficient group maintenance or regrouping is a challenge. Another challenge comes from inter-group communications, which requires the delivery of control messages from one group to another via different CCCs.

- *Inter-group communications*: The communication between groups is always a challenge in group-based

designs. Without reliable inter-group communications, the network may be partitioned into isolated groups. Certain hopping between groups may be necessary for the node to relay the messages across the group boundary. Advanced techniques may be needed for this purpose.

- *Efficiency of regrouping*: Group maintenance and regrouping are crucial to the performance because they are directly related to the maintenance of network connectivity, the robustness of CCC allocation to PU activity, and the CCC establishment overhead.

4.3. Dedicated control channel design

Dedicated CCCs are control channels predetermined in licensed or unlicensed bands. They are attractive solutions for several reasons: (1) dedicated CCCs are usually unaffected by PU activity and considered always available ("always on"), (2) dedicated CCC are available network-wide with global coverage, and (3) many existing CR MAC protocols and cooperative sensing schemes assume the availability of dedicated CCCs. However, in addition to possible licensing cost, dedicated CCCs are more susceptible to control channel saturation and security attacks compared to other CCC designs. These two major drawbacks are discussed in Sections 3.1 and 3.4, respectively.

Due to the dynamic behavior of PUs, dedicated CCCs in a band licensed to PUs are usually not practical. However, a recent development [12] makes it possible by allocating CCCs in the guard bands. Generally, the dedicated CCCs are more often allocated in a band licensed to secondary networks or in an unlicensed band. However, in the latter case, dedicated CCCs are subject to interference from any radio operating in that band. Thus, how to coordinate the access in unlicensed bands to avoid the interference becomes an important issue [44,45].

4.3.1. Dedicated CCCs in licensed bands

The majority of dedicated CCC solutions in licensed bands are proposed by existing CR MAC protocols. For example, OSA-MAC [25], Opportunistic MAC [46,26], and OS-MAC [23] uses a dedicated CCC in a band licensed to the CR network for control message exchange. Others such as DOSS MAC [43] and CREAM-MAC [47] do not specify the preference, which can allocate CCCs in licensed bands owned by CR network operators. In these CR MAC solutions, CCCs are assumed to be free from PU activity. As a result, compared to in-band CCC schemes, they are relatively simple from the perspective of CCC design.

Unlike dedicated CCCs in CR MAC protocols, a recent study in [12] suggests the use of OFDM subcarriers in the guard bands of the licensed spectrum as the out-of-band dedicated CCCs for control broadcast and unicast communications. Due to the power leakage from adjacent licensed channels, these CCCs in guard bands are subject to adjacent channel interference. To minimize the impact of PU activity on the CCCs, the OFDM subcarrier allocation in guard bands is formulated as an optimization framework. The framework finds the allocated CCC bandwidth (optimal number of OFDM subcarriers in a guard band), the optimal OFDM symbol time, and the optimal OFDM subcarrier transmission power under the constraints such as guard band bandwidth, CR transmission range, control data rate, PU interference power, and OFDM peak to average power ratio (PAPR). For broadcast operations, only the central subcarriers are utilized to provide the largest separation between the CCC and the PU in adjacent channel. For unicast messaging, a multi-arm bandit algorithm is used for the transmitter–receiver pair to learn the optimal combinations of active subcarriers in guard bands based on the channel conditions observed at the receiver. This process improves the selection of subcarriers over time according to the past experience of the CCC allocation. Since this scheme relies on the availability of guard bands in the licensed spectrum, it may be less attractive if the licensed channels are tightly packed in the licensed spectrum leaving guard bands of small bandwidth for CCC allocation and interference avoidance. Furthermore, the control transmission may be unreliable or interrupted if a strong PU interference exists in proximity, which is known as the near-far problem.

4.3.2. Dedicated CCCs in unlicensed bands

Similar to dedicated CCCs in licensed bands, dedicated CCCs can be allocated in unlicensed bands. Many CR MAC protocols such as HC-MAC [24] adopt this approach. Although dedicated CCCs in unlicensed bands are not affected by PU activity, they are subject to the interference from any unlicensed users of different networks. Thus, the coordination and spectrum sharing among unlicensed users from different networks is an important function of CCCs in unlicensed bands.

In [44,45], a common spectrum coordination channel (CSCC) is proposed for users from different networks (e.g. WiFi and WiMAX) to coexist and negotiate the access in unlicensed band. This protocol enables neighboring radios of different types to locate each other and share the spectrum by periodically broadcasting their radio parameters and spectrum usage information in a specific packet format. Regardless of the advantage in improving spectrum coexistence of heterogeneous networks, this protocol incurs overhead on top of standard radio interface such as the usage of additional dedicated control radio and the modified protocol stack with the additions of CSCC specific PHY and MAC layers to handle the CSCC access.

4.4. Ultra wideband CCC design

In UWB communications, information is modulated on spreading sequences and transmitted in low power as short pulses to exhibit an ultra wide signal bandwidth compared to channel bandwidth. Since the UWB transmission is perceived as noise in narrowband channels, this transmission scheme can be utilized to send control traffic in the overlay UWB channel without harmful interference with the PU traffic in licensed data channels. Cabric et al. suggest in [53] that a CCC can be implemented as an underlay UWB channel for cooperative sensing in CR networks. In addition, different groups of CR users can use different spreading sequences for control transmission to facilitate the cooperation among CR users. However, owing to the

strict limitation on UWB transmission power, the transmission range is limited.

There are two issues related to transmission range in UWB CCC design: (1) how to increase the limited transmission range and (2) how to resolve the range difference between the UWB control radio and other type of data radio. First, experimental studies show that UWB radios can achieve a range of 100 m or more [17]. Moreover, in most CCC applications that require low control data rate, the range can be increased to an adequate level by the spreading gain [27]. For example, an on–off keying (OOK) modulated UWB scheme is proposed in [28] for transmitting the spectrum sensing data in cooperative sensing. In this approach, it is shown that low bit error rate (BER) and large range can be achieved by increasing the number of UWB pulses per symbol or equivalently repeating the control transmission at the cost of reduced control throughput.

When a different type of data radio (e.g. 802.11 radio) is used, a neighbor that can be reached by the data radio in one hop may not be reachable by the UWB radio in one hop. To resolve this range difference issue, a UWB CCC scheme with multi-hop control routing is proposed in [17,29]. In Fig. 5, R_{UWB} and R_{WLAN} represent the transmission range of UWB radio and WIFI radio. CR users *B* and *C* are both one-hop UWB neighbor and one-hop WIFI neighbor of CR user *A* while CR users *D* and *E* are one-hop WIFI neighbor but not reachable by the UWB radio of CR user *A*. In this approach, a simple CCC routing table is established during neighbor discovery for routing control packets to all neighbors (reachable by one hop for data and *k* hops for control). In other words, all the intermediate nodes between the source and destination (CR user *C* in the figure) forward the control packets back and forth to complement the difference between the control and data radio ranges. However, the control overhead increases as the node density or the distance between the source and destination increases (i.e. the range difference increases). Although this problem can be resolved by using UWB radio interface for both control and data transmission, the applications of UWB data transmission in CR networks may be limited due to the limitation on the range and the achievable data rate.

4.4.1. Research challenges

The following research challenges arise in UWB CCC designs:

- *Range vs. rate tradeoff*: The primary challenge in UWB CCC design involves in the tradeoff between extending the transmission range and increasing the control throughput. Although control traffic is generally transmitted at a low bit rate, the required control data rate may be compromised by the spreading sequences for enlarging the transmission range. The tradeoff must be carefully considered in UWB CCC design.
- *Spreading code design*: As discussed previously, the spreading code used in UWB transmission can be utilized to group CR users for cooperation and balance the tradeoff between range and data rate. As a result, the design of spreading sequences has a significant impact on the CCC performance. It is a challenge to design the sequences pertinent and adaptable to different control traffic needs such as broadcast and unicast messaging.

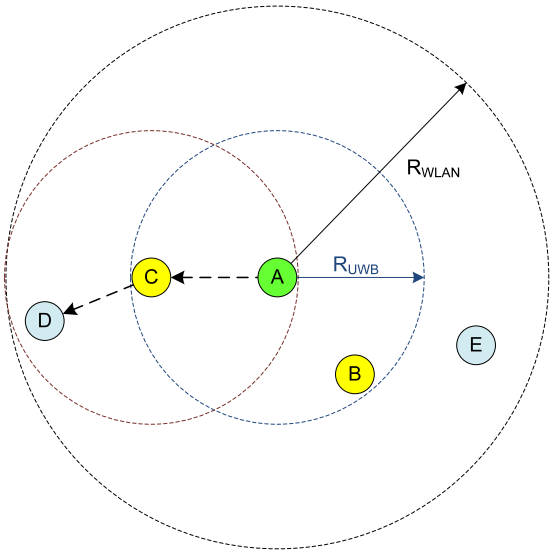


Fig. 5. UWB CCC with multi-hop routing to WIFI neighbors [17].

5. Control channel in network protocol layers

Common control channels provide the medium for control message exchange required by network operations in different network protocol layers. First of all, the radio interface used for control transmission is directly related to the CCC performance. In physical (PHY) layer, CCCs are used as reporting channels for CR users to share their local spectrum sensing results in cooperative sensing. In the MAC layer, CCCs are used for neighbor discovery, channel negotiation, and transmitter–receiver handshake. In the network layer, CCCs are used for sending route updates and topology change. These CCC applications in different network protocol layers are discussed as follows.

5.1. CCC and radio interface

The radio interface used for control transmission generally is the same as the one for data transmission unless different types of radios are used for control and data as in the UWB CCC case. The first question concerns the CCC design regarding radio interface is then whether or not a dedicated radio for control purposes is necessary. If a dedicated control radio is used, the CCC design needs to address the issue of cosite interference in which two radios collocated in proximity may interfere with each other resulting in performance degradation.

5.1.1. Dedicated control radio

Since using more than one radio incurs extra hardware cost, the necessity of using a radio dedicated to a control channel called a dedicated control radio is in question. As can be seen in Table 1, most in-band CCC solutions use single radio for both control and data transmission while dedicated CCC solutions may prefer to use a dedicated control radio tuned to the dedicated CCC. For in-band solutions, single radio is usually sufficient because control message exchange occurs in data channels unless a virtually "always on" CCC can be dynamically allocated in

data channels to improve the CCC establishment efficiency in multi-hop environments [3].

Although a dedicated control radio is unnecessary if the CCC is not always available, the problem of using single radio for both control and data is obvious: a CR user is unable to transmit or receive any control message during data transmission. As a result, the single-radio CCC solutions are required to synchronize CR users in order to exchange control messages in a predefined control window or time period. Nevertheless, the synchronization of CR users is not always feasible. In these scenarios, a dedicated control radio is preferred.

5.1.2. Cosite interference

Dedicated control radio raises the concern with the issue of cosite interference. Due to the collocation of two radios in one user, the out-of-band (OOB) emission [54] from a transmitting radio can block the transmission or corrupt the reception at the other radio operating in different channel within the same band [55]. This phenomenon, called *cosite interference*, can degrade the performance of both control and data transmission.

In [3], the MAC techniques including prioritized time sharing, power control, and dynamic channel allocation proposed in [54] are utilized to mitigate the issue of cosite interference. First, *prioritized time sharing* is required because it is shown in [55] that only one radio can be active at a given time when both control and data radios are transmitting. Since control transmission is short due to its low bit rate, it can be assumed to have a higher priority than data without significantly compromising the performance of data transmission. As a result, whenever the control radio transmits or receives, the data radio is temporarily refrained from transmission. For *power control and rate adaptation*, the transmitting node can be notified to perform transmission power control and adjust the transmission rate in the data channel to reduce the power leakage from the receiving data channel to the CCC. For *dynamic channel allocation*, the data channel can be dynamically reallocated to the channel away from the CCC while the control channel can be dynamically changed if the CCC quality degrades.

5.2. CCC for cooperative sensing

In cooperative sensing, CCC is commonly used by CR users to report local sensing data to a central entity for data fusion or share the sensing results with neighboring nodes [4]. For reporting sensing data, three major control channel requirements must be satisfied in cooperative sensing: bandwidth, reliability, and security. The security issues such as control channel jamming have been discussed in Section 3.4. In this subsection, we focus on the bandwidth and reliability requirements.

5.2.1. Bandwidth requirement

The bandwidth of the control channel is identified in [56] as one the factors of determining the level of cooperation. This is because the amount of local sensing data that can be transmitted to the FC or shared with the neighbors is limited by the control channel's bandwidth.

To satisfy the bandwidth requirement, the most common approach in cooperative sensing is to reduce the amount of data reported on the CCC by censoring and quantizing the local sensing results. In [57], the problem of cooperative sensing under control channel bandwidth constraints is addressed by censoring and quantizing local sensing data. Each cooperating CR user performs the censoring by reporting the result only if the local decision is determined by the sequential probability ratio test. Thus, censoring reduces the unnecessary reporting data and the usage of control channel bandwidth.

5.2.2. Reliability requirement

In addition to bandwidth requirement, the reliability of the control channel has the great impact on cooperative sensing performance. Like data channels, the control channel is susceptible to multipath fading and shadowing. Hence, the channel impairments such as the effect of Gaussian noise, multipath fading, and correlated shadowing must be considered in the reliability issue of control channel.

In [58], the issue of correlated log-normal shadowing on the reporting channel (a.k.a. the CCC) is investigated. The results show that the performance degradation caused by the shadowing correlation on the reporting channel can be as severe as that on the sensing channel.

5.3. CCC for medium access control

As an original part of CR MAC protocols, CCC and MAC protocols are inseparable. For MAC operations, CCCs are primarily used to facilitate neighbor discovery and channel negotiation. All these operations require the handshake between transmitter and receiver on the CCC.

5.3.1. Neighbor discovery

A CCC can facilitate neighbor discovery while neighbor discovery is an inseparable part of the CCC design. This is because a CR user joining the network can find neighbors quickly by listening to neighbors' broadcast messages on the CCC when a CCC is already established. However, during network initialization, it is a challenge for all CR users to find their neighbors and establish initial network connectivity when no CCC is available.

In sequence-based CCC design, two neighboring nodes discover each other when they rendezvous on the common channel. In this case, neighbor discovery is achieved by channel hopping naturally followed by CCC allocation. As a result, no separate neighbor discovery scheme is necessary. In group-based design, certain hopping schemes similar to channel hopping sequences are required to establish initial CCC links among CR users. Since CR users can tolerate some delay during initial neighbor discovery, many schemes use simple channel scanning to find neighbors while other schemes use more sophisticated hopping sequences to accelerate the neighbor discovery process. In [3], a probability-based hopping sequence is used for neighbor discovery and initial CCC establishment. Since the channel with a higher quality appears in the sequence more frequently, CR users with similar channel availability in a neighborhood are likely to rendezvous on the channel with the best quality in a timely manner.

5.3.2. Channel negotiation

Channel negotiation on the CCC is the standard operation in every MAC protocol. By exchanging RTS/CTS packets, a transmitter–receiver pair reserves a channel for data transmission while other nodes overhearing the control message exchange will keep silent to avoid collisions for the predetermined time period as in the IEEE 802.11 CSMA/CA protocol.

5.4. CCC for routing

As the CCCs in cooperative sensing and MAC protocols, many existing routing solutions assume the availability of a reliable CCC for route formation and maintenance. For route formation, the source node may need to broadcast link state advertisements [59] or the route request packets [60] over the CCC. In the event of link failures, which may result from CR user mobility or PU activity, a CCC may need to be established before the routing maintenance can be performed. Without a reliable CCC, all routing operations have difficulty in proceeding. For example, in the distributed routing algorithm [61], each backlogged node needs to sense an idle control channel before the joint routing and scheduling algorithm can be performed.

6. Conclusions

The CCC in CR networks facilitates a variety of network operations in different network protocol layers such as enabling CR users to share the sensing data in cooperative sensing, broadcast routing information, and coordinate the spectrum's access. However, the major challenge in CCC design is how to establish a reliable CCC when it is affected by PU activity. In this paper, four major control channel issues: control channel saturation, robustness to primary user activity, CCC coverage, and control channel security are identified as primary design challenges in CCC design. Moreover, the CCC design schemes are classified into four major design approaches: sequence-based, group-based, dedicated, and UWB CCCs. These CCC design schemes are discussed and evaluated according to the identified design challenges. The applications of the CCC in cooperative sensing, MAC, and routing show the versatile of CCCs and their importance for proper CR network operations in different network protocol layers.

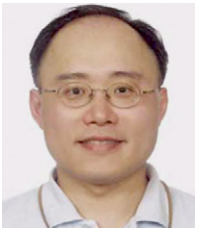
Acknowledgement

This work was supported by the US National Science Foundation under Award ECCS-0900930.

References

[1] I.F. Akyildiz, W.-Y. Lee, M.C. Vuran, S. Mohanty, Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey, Computer Networks 50 (13) (2006) 2127–2159.
[2] I.F. Akyildiz, W.-Y. Lee, K.R. Chowdhury, CRAHNs: cognitive radio ad hoc networks, Ad Hoc Networks 7 (5) (2009) 810–836.
[3] B.F. Lo, I.F. Akyildiz, A.M. Al-Dhelaan, Efficient recovery control channel design in cognitive radio ad hoc networks, IEEE Transactions on Vehicular Technology 59 (9) (2010) 4513–4526.
[4] I.F. Akyildiz, B.F. Lo, R. Balakrishnan, Cooperative spectrum sensing in cognitive radio networks: a survey, Physical Communication (Elsevier) Journal 4 (1) (2011) 40–62.
[5] J. So, N.H. Vaidya, Multi-channel MAC for ad hoc networks: handling multi-channel hidden terminals using a single transceiver, in: Proc. of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc'04, 2004, pp. 222–233.
[6] J. Mo, H.-S. So, J. Walrand, Comparison of multichannel MAC protocols, IEEE Transactions on Mobile Computing 7 (1) (2008) 50–65.
[7] Y.R. Kondareddy, P. Agrawal, Synchronized MAC protocol for multi-hop cognitive radio networks, in: Proc. of IEEE ICC 2008, 2008, pp. 3198–3202.
[8] Y. Kondareddy, P. Agrawal, K. Sivalingam, Cognitive radio network setup without a common control channel, in: IEEE Military Communications Conference, MILCOM 2008, 2008, pp. 1–6.
[9] C. Xin, X. Cao, A cognitive radio network architecture without control channel, in: IEEE Global Telecommunications Conference, GLOBECOM 2009, 2009, pp. 1–6.
[10] P. Pawelczak, S. Pollin, H.-S.W. So, A. Motamedi, A. Bahai, R.V. Prasad, R. Hekmat, State of the art in opportunistic spectrum access medium access control design, in: Proc. of IEEE CrownCom 2008, 2008, pp. 1–6.
[11] P. Pawelczak, S. Pollin, H.-S. So, A. Bahai, R. Prasad, R. Hekmat, Comparison of opportunistic spectrum multichannel medium access control protocols, in: IEEE Global Telecommunications Conference, GLOBECOM 2008, 2008, pp. 1–6.
[12] K. Chowdhury, I. Akyildiz, OFDM based common control channel design for cognitive radio ad hoc networks, IEEE Transactions on Mobile Computing 10 (2) (2011) 228–238.
[13] L.A. DaSilva, I. Guerreiro, Sequence-based rendezvous for dynamic spectrum access, in: Proc. of IEEE DySPAN, 2008, pp. 1–7.
[14] K. Bian, J.-M.J. Park, R. Chen, A quorum-based framework for establishing control channels in dynamic spectrum access networks, in: Proc. of MobiCom 2009, 2009, pp. 25–36.
[15] C. Cormio, K.R. Chowdhury, Common control channel design for cognitive radio wireless ad hoc networks using adaptive frequency hopping, Ad Hoc Networks 8 (2010) 430–438.
[16] N. Baldo, A. Asterjadhi, M. Zorzi, Dynamic spectrum access using a network coded cognitive control channel, IEEE Transactions on Wireless Communications 9 (8) (2010) 2575–2587.
[17] A. Masri, C.-F. Chiasserini, A. Perotti, Control information exchange through UWB in cognitive radio networks, in: IEEE International Symposium on Wireless Pervasive Computing, ISWPC 2010, 2010, pp. 110–115.
[18] T. Chen, H. Zhang, G.M. Maggio, I. Chlamtac, CogMesh: a cluster-based cognitive radio network, in: Proc. of IEEE DySPAN, 2007, pp. 168–178.
[19] T. Chen, H. Zhang, M.D. Katz, Z. Zhou, Swarm intelligence based dynamic control channel in CogMesh, in: Proc. of IEEE ICC 2008, 2008, pp. 123–128.
[20] C. Doerr, D. Grunwald, D. Sicker, Dynamic control channel management in presence of spectrum heterogeneity, in: IEEE Military Communications Conference, MILCOM 2008, 2008, pp. 1–8.
[21] L. Lazos, S. Liu, M. Krunz, Spectrum opportunity-based control channel assignment in cognitive radio networks, in: Proc. of IEEE SECON 2009, 2009, pp. 1–9.
[22] A. Motamedi, A. Bahai, MAC protocol design for spectrum-agile wireless networks: stochastic control approach, in: 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2007, 2007, pp. 448–451.
[23] B. Hamdaoui, K.G. Shin, OS-MAC: an efficient MAC protocol for spectrum-agile wireless networks, IEEE Transactions on Mobile Computing 7 (8) (2008) 915–930.
[24] J. Jia, Q. Zhang, X. Shen, HC-MAC: a hardware constrained cognitive MAC for efficient spectrum management, IEEE Journal on Selected Areas in Communications 26 (1) (2008) 106–117.
[25] L. Le, E. Hossain, OSA-MAC: a MAC protocol for opportunistic spectrum access in cognitive radio networks, in: IEEE Wireless Communications and Networking Conference, WCNC 2008, 2008, pp. 1426–1430.
[26] H. Su, X. Zhang, Cross-layer based opportunistic MAC protocols for QoS provisionings over cognitive radio wireless networks, IEEE Journal on Selected Areas in Communications 26 (1) (2008) 118–129.
[27] D. Cabric, S.M. Mishra, D. Willkomm, R. Brodersen, A. Wolisz, A cognitive radio approach for usage of virtual unlicensded spectrum, in: Proc. of 14th IST Mobile Wireless Communications Summit 2005, 2005.

[28] M.E. Sahin, H. Arslan, System design for cognitive radio conmunications, in: 1st International Conference on Cognitive Radio Oriented Wireless Networks and Communications, CrownCom 2006, 2006, pp. 1–5.
[29] A. Masri, C.-F. Chiasserini, C. Casetti, A. Perotti, Common control channel allocation in cognitive radio networks through UWB multihop communications, in: The first Nordic Workshop on Cross-Layer Optimization in Wireless Networks at Levi, Finland, 2010.
[30] N. Baldo, A. Asterjadhi, M. Zorzi, Cooperative detection and spectrum reuse using a network coded cognitive control channel, in: 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops, SECON Workshops'09 2009, 2009, pp. 1–7.
[31] A. Asterjadhi, N. Baldo, M. Zorzi, A distributed network coded control channel for multihop cognitive radio networks, IEEE Network 23 (4) (2009) 26–32.
[32] K. Bian, J.-M.J. Park, R. Chen, Control channel establishment in cognitive radio networks using channel hopping, IEEE Journal of Selected Areas in Communications, JSAC (2011) (in press).
[33] C. Cormio, K. Chowdhury, An adaptive multiple rendezvous control channel for cognitive radio wireless ad hoc networks, in: IEEE Int'l Conf. on Pervasive Computing and Communications Workshops, PERCOM Workshops 2010, 2010, pp. 346–351.
[34] L. Lazos, S. Liu, M. Krunz, Mitigating control-channel jamming attacks in multi-channel ad hoc networks, in: WiSec'09: Proceedings of the Second ACM Conference on Wireless Network Security, 2009, pp. 169–180.
[35] X. Liu, Z. Ding, Escape: a channel evacuation protocol for spectrum-agile networks, in: 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2007, DySPAN 2007, 2007, pp. 292–302.
[36] Q. Zhao, L. Tong, A. Swami, Decentralized cognitive MAC for dynamic spectrum access, in: First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005, 2005, pp. 224–232.
[37] Q. Zhao, L. Tong, A. Swami, Y. Chen, Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: a POMDP framework, IEEE Journal on Selected Areas in Communications 25 (3) (2007) 589–600.
[38] C. Cordeiro, K. Challapali, C-MAC: a cognitive MAC protocol for multi-channel wireless networks, in: Proc. of IEEE DySPAN, 2007, pp. 147–157.
[39] C. Doerr, D. Sicker, D. Grunwald, Dynamic control channel assignment in cognitive radio networks using swarm intelligence, in: IEEE Global Telecommunications Conference, GLOBECOM 2008, 2008, pp. 1–6.
[40] M.-R. Kim, S.-J. Yoo, Distributed coordination protocol for common control channel selection in multichannel ad-hoc cognitive radio networks, in: IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WIMOB 2009, 2009, pp. 227–232.
[41] L. Ma, C.-C. Shen, B. Ryu, Single-radio adaptive channel algorithm for spectrum agile wireless ad hoc networks, in: Proc. IEEE DySPAN 2007, 2007, pp. 547–558.
[42] J. Zhao, H. Zheng, G.-H. Yang, Distributed coordination in dynamic spectrum allocation networks, in: Proc. of IEEE DySPAN 2005, 2005, pp. 259–268.
[43] L. Ma, X. Han, C.-C. Shen, Dynamic open spectrum sharing for wireless ad hoc networks, in: Proc. IEEE DySPAN 2005, 2005, pp. 203–213.
[44] D. Raychaudhuri, X. Jing, A spectrum etiquette protocol for efficient coordination of radio devices in unlicensed bands, in: 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, PIMRC, 2003, 2003, pp. 172–176.
[45] X. Jing, D. Raychaudhuri, Spectrum co-existence of IEEE 802.11b and 802.16a networks using the cscc etiquette protocol, in: 2005 First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2005, 2005, pp. 243–250.
[46] H. Su, X. Zhang, Opportunistic MAC protocols for cognitive radio based wireless networks, in: 41st Annual Conference on Information Sciences and Systems, CISS 2007, 2007, pp. 363–368.
[47] H. Su, X. Zhang, CREAM-MAC: an efficient cognitive radio-enabled multi-channel MAC protocol for wireless networks, in: Int'l Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2008, 2008, pp. 1–8.
[48] A. Chan, X. Liu, G. Noubir, B. Thapa, Broadcast control channel jamming: resilience and identification of traitors, in: IEEE International Symposium on Information Theory, ISIT 2007, 2007, pp. 2496–2500.
[49] P. Tague, M. Li, R. Poovendran, Probabilistic mitigation of control channel jamming via random key distribution, in: IEEE 18th Int'l Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC 2007, 2007, pp. 1–5.
[50] P. Tague, M. Li, R. Poovendran, Mitigation of control channel jamming under node capture attacks, IEEE Transactions on Mobile Computing 8 (9) (2009) 1221–1234.
[51] G. Safdar, M. O'Neill, Common control channel security framework for cognitive radio networks, in: IEEE 69th Vehicular Technology Conference, VTC2009-Spring 2009, 2009, pp. 1–5.
[52] T. Chen, H. Zhang, G.M. Maggio, I. Chlamtac, Topology management in CogMesh a cluster-based cognitive radio mesh network, in: Proc. of IEEE ICC 2007, 2007, pp. 6516–6521.
[53] D. Cabric, S.M. Mishra, R.W. Brodersen, Implementation issues in spectrum sensing for cognitive radios, in: Proc. of 38th Asilomar Conference on Signals, Systems, and Computers 2004, 2004, pp. 772–776.
[54] J. Zhu, A. Waltho, X. Yang, X. Guo, Multi-radio coexistence: challenges and opportunities, in: Proc. of Int'l Conf. on Computer Communications and Networks, ICCCN 2007, 2007, pp. 358–364.
[55] S. Kakumanu, R. Sivakumar, Glia: a practical solution for effective high datarate wifi-arrays, in: Proc. of MobiCom 2009, 2009, pp. 229–240.
[56] S. Mishra, A. Sahai, R. Brodersen, Cooperative sensing among cognitive radios, in: Proc. of IEEE ICC 2006, vol. 4, 2006, pp. 1658–1663.
[57] C. Sun, W. Zhang, K. Letaief, Cooperative spectrum sensing for cognitive radios under bandwidth constraints, in: Proc. of IEEE WCNC 2007, 2007, pp. 1–5.
[58] M. DiRenzo, L. Imbriglio, F. Graziosi, F. Santucci, Cooperative spectrum sensing over correlated log-normal sensing and reporting channels, in: Proc. of IEEE GLOBECOM 2009, 2009, pp. 1–8.
[59] H. Khalife, S. Ahuja, N. Malouch, M. Krunz, Probabilistic path selection in opportunistic cognitive radio networks, in: IEEE Global Telecommunications Conference, GLOBECOM 2008, 2008, pp. 1–5.
[60] K.R. Chowdhury, I.F. Akyildiz, CRP: a routing protocol for cognitive radio ad hoc networks, IEEE Journal of Selected Areas in Communications (JSAC) (2011) (in press).
[61] L. Ding, T. Melodia, S. Batalama, J. Matyjas, M. Medley, Cross-layer routing and dynamic spectrum allocation in cognitive radio ad hoc networks, IEEE Transactions on Vehicular Technology 59 (4) (2010) 1969–1979.



Brandon F. Lo received the B.S. (honors) degree in computer science from Tunghai University, Taichung, Taiwan, in 1992 and the M.S. degree in electrical engineering from the University of Michigan, Ann Arbor, in 1995. He is working toward the Ph.D. degree in electrical and computer engineering with the Broadband Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta.

Mr. Lo held an internship position with Idaho National Laboratory working on the cognitive radio testbed system in 2010. Before his doctoral study, he designed processors and application-specific integrated circuit chips for broadband communications and networking in the semiconductor industry. His research interests include cognitive radio networks, mobile ad hoc networks, and wireless communications.