IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Common Control Channel Design Schemes in Cognitive Radio Networks

Kalyana Chakravarthy Chilukuri[1], Swetha Devrapalli C[2]

Professor, CSE Department, MVGR College of Engineering (A), Vizianagaram, India[1]

CSE Department, MVGR College of Engineering (A), Vizianagaram, India[2]

Abstract: Wireless applications have been increasing rapidly due to which the available frequency is overcrowded and cannot satisfy the needs of the users. In static spectrum allocation scheme the frequency is allocated to the user on long term basis which leads to spectrum scarcity. To overcome the spectrum scarcity problem dynamic spectrum allocation came into existence. Cognitive radio network was a key enabling technology for dynamic spectrum allocation, which allows the secondary users to make use of licensed spectrum in opportunistic manner. MAC protocol plays a vital role in opportunistic spectrum utilization, primary user's interference management and secondary user's coordination. Cognitive Radio (CR) users coordinate with each other by making use of Common Control Channel (CCC), which was a common medium used to exchange the control information. When the primary user comes back or when the QOS of the current channel was not satisfied, then CCC moves on to the new available channel. The CCC coverage is one of the most challenging issues in cognitive radio networks and can be addressed by proper control channel design. In this paper, we elaborate on various controls channel design schemes and some security issues in the same.

Keywords: Cognitive Radio (CR), Common Control Channel (CCC), QOS.

I. INTRODUCTION

The wireless communications have been developing tremendously; as a result the number of mobile subscribers is also growing. Wireless communications make use of spectrum. Wireless communications rely on static spectrum allocation i.e, each and every user will be allocated a license to operate the spectrum band on long term basis. The unlicensed user will not be able to make use of the spectrum even though the licensed user is not making use of it. Static spectrum allocation reduces the interference between the users with the help of adequate guard bands. Even though the static spectrum allocation works well, it leads to spectrum scarcity problem as the demand for the spectrum increases.

Static spectrum allocation scheme leads to underutilization of spectrum. To overcome spectrum scarcity, the Federal Communications Commission (FCC) had approved that unlicensed users can also make use of spectrum in licensed bands, so dynamic spectrum allocation scheme came into existence [1]. The key enabling technology for dynamic spectrum allocation was cognitive radio networks.

CR users initially sense for the vacant channels which was termed as spectrum sensing [2]. Each and every CR will have different sensing results. For two cognitive users to communicate with each other, they should have at least one channel in common in their vacant channel list.CR users usually coordinate with each other with the help of Common Control Channel [3]. The CCC allocation can be done temporarily or permanently in a licensed or unlicensed band. The efficiency of the control channel depends on the time taken by the CR nodes to detect the control channel and also on the selection criteria of the control channel band. The communication between the CR nodes is not possible, if the CR nodes are not aware of the available control channels. The CCC facilitates various operations such as transmitter-receiver handshake, neighbour discovery, forwarding topology, route change updates especially CCC was used by the CR users to show their presence by broadcasting control messages on the CCC. Moreover, CR users make use of CCC to exchange the sensing information between the neighbours.

The CCC in cognitive radio networks emanates from the Medium Access Control (MAC) protocol in multi-channel wireless network. In multi-channel network, one channel was commonly available to all the nodes and was used for control messages exchange.

CCC provides different applications in different protocol layers. In the physical layer the CCC was used by the CRs to share their spectrum sensing result which helps in coordinating the various spectrum sensing results. In MAC layer the CCC was used for neighbour discovery, transmitter-receiver handshake and channel negotiation. In the network layer CCC was used for relaying routing, topology change updates.

The CCC allocation faces many challenges initially; the band that was allocated to the CCC should be free from PU activity as CCC should vacate the band if the PU comes back and restores its connection to other vacant band. Due to the heterogeneity of available spectrum bands in the network, it is difficult for the CR users to find a common control channel available to all the users as the CCC. As a result the CCC coverage was limited to the neighbourhood in the network.

Limited CCC coverage increases the channel switching delay and control signalling overheads. Even though we allocate a dedicated common control channel which was globally available, this can lead to single point of failure and dedicated control channel is also more vulnerable to the control channel jamming attacks.

II. CLASSIFICATION OF CONTROL CHANNEL DESIGN SCHEMES

The CCC design classification may be initially divided into the overlay and underlay CCC schemes. The underlay approach can again be classified into in-band and out-of-band schemes [3]. The in-band scheme consists of two sub categories, sequence-based and group-based schemes. The out-of-band schemes comprise of dedicated CCCs. The underlay approach is composed of ultra-wide band and multi-carrier spread spectrum control channel designs.

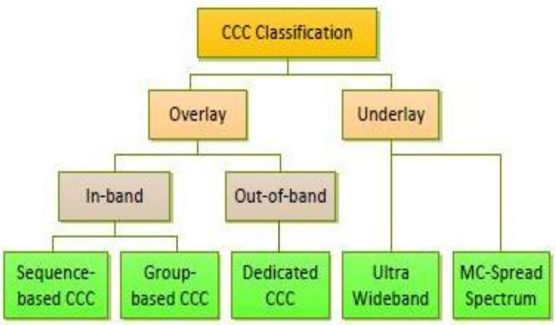

Figure 1: Classification of control channel design

II- A. Overlay-based Common Control Scheme

In overlay based CCC schema, the CCCs are allocated to either permanent or short term allocated spectrum which was not used by the primary user. When the primary user comes back for the allocated spectrum then the cognitive users have to evacuate that control channel and have to restore their connection to the other available CCCs.

- **In-band:** In in-band the CCCs were allocated to the licensed bands which were used by the primary users. Different intervals of time are used to transmit data and control messages. These in band CCCs enhances the spectrum efficiency and the security. The coverage of the in-band CCCSs was limited due to the spectrum heterogeneity.
- **Out-of-band:** In out-of-band the CCC was allocated to the unlicensed bands or licensed bands. The out-of-band CCCs are globally available. If we make use of unlicensed dedicated common control channel, it will lead to interference with other networks as most of the cognitive radio network protocols make use of unlicensed bands. If we make use of single dedicated common control channel then it will lead to security attacks such as denial of service (DOS) which will place the entire network at single point of failure. So designing out-of-band will leads to many security issues.

II- B. Underlay-based Common Control Scheme

In underlay based scheme, the CCCs can make use of the band which was used by the primary user [4]. Control messages and the primary user data can be relayed simultaneously in the licensed spectrum. With the help of spread spectrum techniques, the Control messages are relayed in low power by utilizing short pulses, which are transmitted over a high bandwidth so that the transmission appears as noise to the primary users.
Primary user's transmission is effected by the underlay schema if the number of cognitive users making use of the control channel increases.

III. CONTROL CHANNEL DESIGN SCHEMES

III- A. Sequence-based control channel design

In sequence based CCC assignment scheme, the control channels are allocated according to the random sequence or predefined channel hopping sequence [5]. These are built by taking the permutations among the available control channels, adaptive-MRCC or quorum based. In sequence based CCC, the channel hopping sequence was the key element. As each and every CR may use different hopping sequences so that neighbouring

CR's may make use of different control channels. This scheme will reduce the impact of PU activity on the control channel. In this scheme the sequences were predefined, which reduces the time required for the cognitive users to establish a connection with another common control channel. But when the number of common control channels is high then it will take more time to coordinate.

The time taken for the two CR's to communicate on the single control channel was known as time to rendezvous which can be reduced by this approach. This sequence based control channel does not provide large coverage area. So the sequence based approach incurs high signalling overhead during the broadcast of control messages. This approach has another drawback - as the sequences were predefined, it was not adjustable to new control channel opportunities.

Adaptive multiple rendezvous common control channel scheme was proposed to overcome the performance issues of classic rendezvous common control channel scheme. In adaptive multiple rendezvous common control channel scheme the sequences are not predefined but chosen dynamically. The AM-RCC scheme does not follow any strict synchronization and achieves better performance by changing the sequence when the primary user activity was detected.

This scheme was robust and scalable to the dynamic PU activity as the sequence formation was adaptive and based on the sensing results. This scheme also hasa drawback that there was no guarantee on the coverage of CCC beyond the rendezvous node pair.

A quorum based scheme was proposed for designing sequences for common control channel establishment in dynamic channel allocation. This QCH scheme uses the intersection of quorum systems to generate a sequence. QCH schemes also enable to establish the control channels on different frequencies so the secondary network is less vulnerable to unpredictable signals.

III- B. Group-based control channel design

Group based control channel assignment scheme allows different clusters to make use of different control channels. In this approach control channels were commonly available to the users in the proximity [6].The group of cognitive users are divided in to clusters based on the neighbour coordination or clustering schemes. In neighbour coordination approach, users vote for the commonly available channels and exchange the voting information based on the majority number of votes of cognitive users. In clustering mechanism the cognitive users are divided in to clusters. Clustering mechanism aims to have maximum coverage area and elects the CR user as the cluster head which has more number of neighbours.

Each and every cluster makes use of common channel as CCC in a cluster which facilitates control messages relayed within the group. Inter-cluster communication was a challenge, as communication has to take place between two different clusters making use of different control channels and efficiency of regrouping was another challenge. If a cluster has more number of free common channels then cognitive user can move easily to the other common channel if the current control channel was occupied by the primary user and also makes the cooperative sensing easier. The main disadvantage of this scheme was that it was very difficult to synchronize nodes in the cluster.

III-C. Dedicated control channel design

Dedicated control channels are unaffected by the primary user activity and have the global coverage [3]. If dedicated control channels were allocated to the licensed bands, it incurs high cost. On the other hand, they lead to high interference when allocated to the unlicensed bands.

A dedicated common control channel has many disadvantages. Initially, one major drawback was wastage of the spectrum allocated and a dedicated control channel will became overloaded when the number of secondary users making use of control channel increases. When compared with other approaches, dedicated control channels are more susceptible to security attacks due to their fixed location. Synchronized MAC protocol was proposed to overcome the drawbacks of dedicated control channel [7]. In this scheme, the total time was divided in to fixed time intervals, so that a time slot can be used as a channel to relay data or control messages. This protocol also reduces the saturation and jamming of common control channel.

III- D. Underlay control channel design

In UWB control channel approach, the data is relayed in low power short pulses to exhibit ultra-wide band signal bandwidth [8]. As UWB transmission was perceived as noise, this transmission scheme was used to relay control traffic in overlay UWB channel without interfering with primary user's traffic. The transmission range of UWB traffic was limited due to strict limitations on limited transmission power.

Multi-carrier spread spectrum make use of filtered multi-tone spread spectrum control channel design which is capable of dynamic masking of sub-carriers and helps in detecting the PU activities, reducing the interference with the primary users.

IV. CONTROL CHANNEL SECURITY

MECHANISMS

IV- A. Common control channel jamming attack:

CCC jamming was one of the most effective ways for the attacker to destroy the entire network. In this attack the intruder intentionally relays strong interference signals on the CCC so that the cognitive users will not be able to receive valid control messages. This results in DoS.

Control channel jamming attack can be mitigated by dynamic CCC allocation. The dynamic channel allocation can be taken place in two ways cross control communication scheme [10] and frequency hopping scheme [11].

In cross control communication scheme [10] the cognitive users can make use of other control channel which was not affected by the jamming attack. Cognitive users can make use of the jammed control channel to inform the other cognitive users who had not experienced jamming, about the new control channel for receiving control messages. This scheme provides successful communication during the jamming attack by making use of different channels for transmit ion and reception of control messages. This scheme has high switching overhead for the radios which are equipped with single transceiver. If any compromised cognitive user was present in the network, that node will also receive the information about the new CCC and leads to jamming of the new available CCC.

A dynamic control channel allocation on the basis of hoping sequence was proposed in [11] to mitigate the jamming attack in cluster based networks. The cluster heads finds the hopping sequence and the control channels within the cluster. The affected network area was reduced due to clustering. These hopping sequences are encrypted by the public key of each cognitive user. These sequences can be obtained by the intruder with the help of node capture attack.

Jamming attack can also mitigated with the help of control channel key distribution. In this scheme hides the location of CCC from the intruders with the help of key distribution techniques. The users with valid key are only able to locate the CCC. The control messages are transmitted on different control channels, so any compromised node will only have few keys with it, So that the compromised node cannot be able to jam all the control channels. The key distribution can be polynomial based [12] or randomly distributed [13].

In polynomial based key distribution scheme [12] the key space contains p*q keys. P was the number of time slots in the period and q as the number of control channels. The control packets were transmitted over all the control channels in each time slot. Each and every node was identified by the unique polynomial. This scheme provides only limited time access to the control channel in certain period. This scheme incurs high retransmission over head and delay.

Random based key distribution scheme [13] also makes use of CCC keys to hide the allocation of control channel in time slots with duplicate transmission on multiple control channels. It was difficult for attackers to identify the random based key assignment structure due to the increased diversity of keys assigned to the users. This scheme incurs high communication and storage overheads due to the increase in the number of keys. To reduce the key space size and its storage overhead the keys are reused periodically in time slots. Hash functions are used to map the CCC keys to allocated CCC frequency, timeslot for CCC relocation in reuse period.

IV- B. Common control channel saturation:
An intruder intentionally relays huge number of packets to saturate the CCC. If the number of users using the control channel increases this may also leads to control channel saturation as all the users make use of CCC to exchange the data packets. This leads to control channel congestion and there were also the chances for collision of packets as the number of user's increases.

In paper [17] the author proposed a method to mitigate the common control saturation problem with the help of alternate decision making strategy on the basis of rendezvous negotiation

IV- C. Integrity of control messages:
The control channel security also involves the authentication of users to access the data and the integrity of data should also be maintained. Cognitive users share the spectrum sensing data with the help of CCC. If the integrity of data and authentication were not taken in to consideration it gives an opportunity for an intruder to inject the falsified data in to the sensing results which will mislead the cognitive users.

A CCC security frame work is proposed in [15] which includes authentication followed with encrypted transactions to provide secure communication between the transmitter and receiver

IV- D. Primary user emulation attack:
In Primary User Emulation attack the intruders transmits signal similar to the primary users, due to this the secondary users will vacate the channel and senses for vacant channels. Primary User Emulation attack decreases the number of channels that were available for control channel allocation and also reduces the spectrum utilization.

The primary user emulation attack can be mitigated by transmitter verification scheme on the basis of localization based defence [16]. Localization based Defence (Locdef) was a transmitter verification scheme which was used to verify the transmitters signal based on the location, by observing the signal characteristics. So that secondary user can easily differentiate between intruder and the primary user.

V. CONCLUSION

Cognitive radio networks provide solution to the spectrum under-utilization problem. To enhance the spectrum efficiency, many operations such as transmitter-receiver handshake, neighbour discovery, forwarding topology, route change updates especially CCC was used by the CR users to show their presence by broadcasting control messages on the CCC. To address the common control channel assignment various schemes has been proposed by the researchers. Each and every scheme has its pros and cons. We have to choose an optimal scheme according to the network, so that the secondary users can easily sense for the vacant channels and can easily exchange the information about the sensing result. We hypothesize that, for dense Cognitive Radio networks, group-based schemes work better and for sparse CRNs, sequence or dedicated control channel-based designs offer better results. This might be verified in future work

REFERENCES

[1] I Ian F. Akyildiz, Mehmet C. Vuran, W Won-Yeol Lee, and Shantidev Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," Elsevier computer networks, vol. 50, no. 13, pp. 2127-2159, september 2006.
[2] Won-yeol Lee and Ian. F. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," IEEE, vol. 7, no. 10, pp. 3845-3857, October 2008.
[3] Brandon F. Lo, Ian F. Akyildiz, and Abdullah M. Al-Dhelaan, "Efficient Recovery Control Channel Design in Cognitive Radio Ad Hoc Networks," IEEE, vol. 59, no. 9, pp. 4513-4526, november 2010.
[4] Daryl Leon Wasden, Hussein Moradi, and Behrouz Farhang-Boroujeny, "Design and implementation of an underlay control channel for cognitive radios," IEEE, vol. 30, no. 10, pp. 1875 - 1889, november 2012.
[5] Kaigui Bian, Jung-Min Park, and Ruiliang Chen, "Control Channel Establishment in Cognitive Radio Networks using Channel Hopping,"

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

IEEE, vol. 29, no. 4, pp. 689 - 703, April 2011.

[6] Sisi Liu, Loukas Lazos, and Marwan Krunz, "Cluster-Based Control Channel Allocation in Opportunistic Cognitive Radio Networks," IEEE, vol. 11, no. 10, pp. 1436 - 1449, Oct 2012.

[7] Y. R. Kondareddy and P. Agrawal, "Synchronized MAC Protocol For Multi-Hop Cognitive Radio Networks," in IEEE International Conference on Communications, vol. 2, Beijing,china, August 2008.

[8] Ahmed M. Masri, Carla-Fabiana Chiasserini, Claudio Casetti, and Alberto Perotti, "Common control channel allocation in cognitive radio networks through UWB communication," IEEE, vol. 14, no. 6, pp. 710 - 718, December 2012. Kaushik R. Chowdhury and Ian F. Akyldiz, "OFDM-Based Common Control Channel Design for Cognitive Radio Ad Hoc Networks," IEEE, vol. 10, no. 2, pp. 228 - 238, february 2011.

[9] Liangping Ma, Bo Ryu, and Chien-Chung Shen, "Single-Radio Adaptive Channel Algorithm for Spectrum Agile Wireless Ad Hoc Networks," in 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2007, pp. 547-558.

[10] Loukas Lazos, Sisi Liu, and Marwan Krunz, "Mitigating control-channel jamming attacks in multi-channel ad hoc networks," in Proceedings of the second ACM conference on Wireless network security, 2009, pp. 169-180.

[11] Agnes Chan, Xin Liu, Guevara Noubir, and Bishal Thapa, "Broadcast Control Channel Jamming: Resilience and Identification of Traitors," in IEEE International Symposium on Information Theory, 2007, pp. 2496–2500.

[12] Patrick Tague, Mingyan Li, and Radha Poovendran, "Probabilistic Mitigation of Control Channel Jamming via Random Key Distribution," in 18th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2007, pp. 1-5.

[13] Patrick Tague, Mingyan Li, and Radha Poovendran, "Attacks, Mitigation of Control Channel Jamming under Node Capture," IEEE, vol. 8, no. 9, pp. 1221 - 1234, september 2009.

[14] G. A. Safdar and M. O'Neill, "Common Control Channel Security Framework for Cognitive Radio Networks," in IEEE Vehicular Technology Conference, , 2009, pp. 1-5.

[15] Ruiliang Chen, Jeffrey H. Reed, and Jung-Min, Park, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," IEEE, vol. 26, no. 1, pp. 25-37, january 2008.

[16] Seyed Morteza Mirhoseni Nezhadal, Reza Berangi, and Mahmood Fathy, "Common Control Channel Saturation Detection and Enhancement in Cognitive Radio Networks," International Journal of Distributed and Parallel Systems, vol. 3, no. 1, January 2012.