International Journal of Computer Science Engineering & Technology
IJCSET
Approved by
National Science Library (NSL)
National Institute of Science Communication and Information Resources (NISCAIR)
Council of Scientific and Industrial Research (CSIR)- New Delhi India .
ISSN :2455-9091

RF-SPECTRUM OPPORTUNITIES FOR COGNITIVE RADIO NETWORKS MANAGEMENT FRAMEWORK & ATTACKS

[1] R.Kiruba Kumari, [2] S.Anusuya,
[1] Head Of the department, [2] M.Phil Research Scholar,
[1,2] Department of Computer Science & Applications,
[1,2] Padmavani arts and Science college for women, Salem-11.

ABSTRACT- Cognitive radio networks are intelligent networks that can automatically sense the environment and adapt the communication parameters accordingly. These types of networks have applications in dynamic spectrum access, co-existence of different wireless networks, interference management, etc. They are touted to drive the next generation of devices, protocols and applications. The paper represents the benefits of cognitive WSNs over conventional WSNs. It also shows the spectrum management framework for cognitive radio networks, inter cell spectrum sharing and finally types of cognitive radio attacks in wireless sensor network

Keywords - Inter-Cell Spectrum, Physical & Link Layer, Framework, Cognitive Radio Networks.

1. INTRODUCTION

In Cognitive Radio Networks the transmission channel is licensed to the primary users (PUs), while secondary users (SUs) only access the channel in an opportunistic way when the PUs are inactive, i.e., when the PUs do not use the channel. Because the channel is used by the SUs opportunistically, a SU transmission must be halted whenever a PU becomes active. In a scenario where a SU needs to transmit multiple packets (e.g., in a file transmission), or when a packet may be too long, the amount of time required to finish the SU's service (Service Time) depends on the number and duration of the PUs' transmissions. By definition, the service time is the interval of time from the instant when the data arrives at the head of the SU transmitting queue (e.g., a packet or a file, depending on the network stack layer), until the instant when its transmission ends. Service time is an important metric in CRNs because it incorporates the level of activity of the PUs. In this work we characterize the service time of a cognitive radio network operating in a GSM channel. Wireless communication in which the transmission or reception parameters are changed to communicate efficiently without interfering with licensed users. Parameter changes are based on the active monitoring off several factors in the radio environment (e.g. radio frequency spectrum). This approach is enabled by software-defined radio frequency spectrum. Spectrum sensing: Detecting the unused Spectrum and sharing the spectrum without harmful interference with other users. Spectrum Management: Capturing the best available spectrum to meet user communication requirement. Spectrum Mobility: Maintaining seamless communication on requirements during the transition to better spectrum. Spectrum Sharing: Providing the fair spectrum scheduling method among coexisting CR users.

There are main two types of cognitive radio, full cognitive radio and spectrum-sensing cognitive radio. Full cognitive radio takes into account all parameters that a wireless node or network can be aware of. Spectrum –sensing cognitive radio detects the possible channels in the radio frequency spectrum. A WSN comprised of sensor nodes equipped with cognitive radio may benefit from the potential advantages of the salient features of dynamic spectrum access such as: a. Opportunistic channel usage for bursty traffic: Upon the detection of an event in WSN, sensor nodes generate a traffic of packet bursts. At the same time, in densely deployed sensor networks, a large number of nodes within the event area try to acquire the channel. This increases probability of collisions, and hence, decreases the overall communication reliability due to packet losses leading to excessive power consumption and packet delay. Here, sensor nodes with cognitive radio capability may opportunistically access to multiple alternative channels to alleviate these potential challenges. b. Using adaptability to reduce power consumption: Time varying nature of wireless channel causes energy consumption due to packet losses and retransmissions. Cognitive radio capable sensor nodes may be able to change their operating parameters to adapt to channel conditions. This capability can be used to increase transmission efficiency, and hence, help reduce power used for transmission and reception. c. Dynamic spectrum access: In general, the existing WSN deployments assume fixed spectrum allocation. However, WSN must either be worked in unlicensed bands, or a spectrum hire for a licensed band must be obtained. Generally, high costs are associated with a spectrum lease, which would, in turn, amplify the overall cost of deployment. This is also contradictory with the main design principles of WSN. On the other hand, unlicensed bands are also used by other devices such as IEEE802.11 wireless local area network (WLAN) hotspots, PDAs and Bluetooth devices. Therefore, sensor networks experience crowded spectrum problem. Hence, in order to maximize the network performance and be able to co-operate efficiently with other types of users, opportunistic spectrum access schemes must be utilized in WSN as well.

2. SPECTRUM MANAGEMENT FRAMEWORK FOR COGNITIVE RADIO NETWORKS

CR networks impose unique challenges due to the coexistence with primary networks as well as diverse QoS requirements. Thus, new spectrum management functions are required for CR networks with the following critical design challenges:

1. Interference Avoidance: CR network should avoid interference with primary networks. 2. QoS Awareness: In order to decide an appropriate spectrum band, CR networks should support QoS-aware communication, considering dynamic and heterogeneous spectrum environment. 3. Seamless Communication: CR networks should provide seamless communication regardless of the appearance of the primary users.

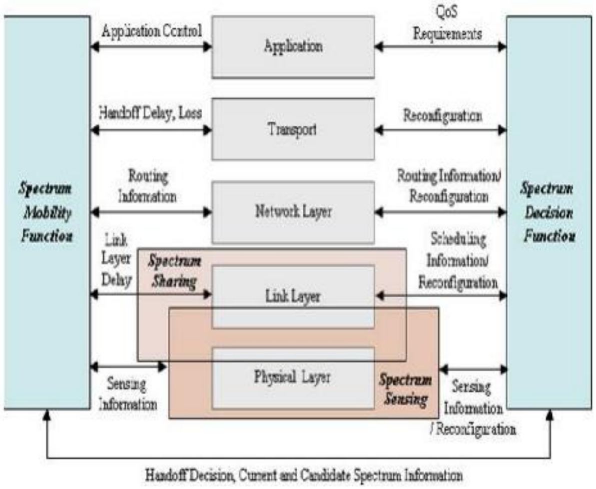
Spectrum Mobility Function
Application Control
Application
QoS Requirements
Handoff Delay, Loss
Transport
Reconfiguration
Routing Information
Network Layer
Routing Information/ Reconfiguration
Link Layer Delay
Spectrum Sharing
Link Layer
Scheduling Information/ Reconfiguration
Physical Layer
Spectrum Sensing
Sensing Information
Sensing Information / Reconfiguration
Spectrum Decision Function
Handoff Decision, Current and Candidate Spectrum Information

Figure 1: Spectrum Management Framework

In order to address these challenges, we provide a directory for different functionalities required for spectrum management in CR networks. The spectrum management process consists of four major steps: 1. Spectrum Sensing: A CR user can only allocate an unused portion of the spectrum. Therefore, the CR user should monitor the available spectrum bands, capture their information, and then detect the spectrum holes. 2. Spectrum Decision: Based on the spectrum availability, CR users can allocate a channel. This allocation not only depends on spectrum availability, but it is also determined based on internal (and possibly external) policies. 3. Spectrum Sharing: Since there may be multiple CR users trying to access the spectrum, CR network access should be coordinated in order to prevent multiple users colliding in overlapping portions of the spectrum. 4. Spectrum Mobility: If the specific portion of the spectrum in use is required by a primary user, the communication needs to be continued in another vacant portion of the spectrum. The spectrum management framework for CR network communication is illustrated in Figure 1. It is evident from the significant number of interactions that the spectrum management functions necessitate a cross-layer design approach. Thus, each spectrum management function cooperates with application, transport, routing, medium access and physical layer functionalities with taking into consideration the dynamic nature of the underlying spectrum.

2.1 Inter-Cell Spectrum Sharing in Cognitive Radio Networks

Cognitive radio (CR) networking achieves high utilization of the scarce spectrum resources without causing any performance degradation to the licensed users. Since the spectrum availability varies over time and space, the infrastructure-based CR networks are required to have a dynamic inter-cell spectrum sharing capability. This allows fair resource allocation as well as capacity maximization and avoids the starvation problems seen in the classical spectrum sharing approaches. A joint spectrum and power allocation framework is proposed that addresses these concerns by (i) opportunistically negotiating additional spectrum based on the licensed user activity (exclusive allocation), and (ii) having a share of reserved spectrum for each cell (common use sharing). Our algorithm accounts for the maximum cell capacity, minimizes the interference caused to neighboring cells, and protects the licensed users through a sophisticated power allocation method.

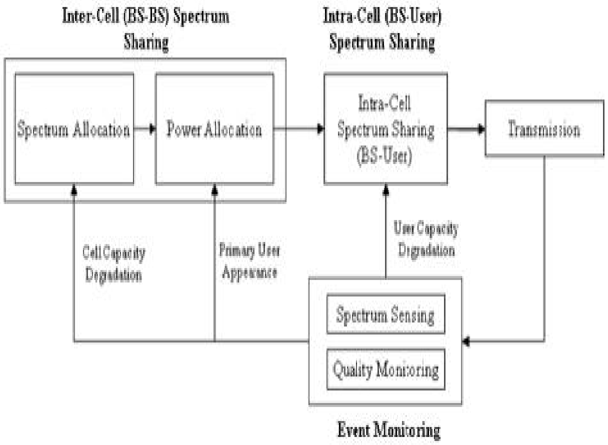
Inter-Cell (BS-BS) Spectrum Sharing
Intra-Cell (BS-User) Spectrum Sharing
Spectrum Allocation
Power Allocation
Intra-Cell Spectrum Sharing (BS-User)
Transmission
Cell Capacity Degradation
Primary User Appearance
User Capacity Degradation
Spectrum Sensing
Quality Monitoring
Event Monitoring

Figure 2: Inter Cell Spectrum Sharing Framework

Infrastructure-based CR networks are required to provide two different types of spectrum sharing schemes: intra-spectrum sharing and inter-spectrum sharing. In order to share spectrum resource efficiently, CR networks necessitate a unified framework to support cooperation among inter- and intra-cell spectrum sharing schemes and other spectrum management functions. Figure 2 shows the framework for spectrum sharing in infrastructure based CR networks, which consists of inter-cell spectrum sharing, intra-cell spectrum sharing, and event monitoring.

1. Event Monitoring: The event monitoring has two different functionalities. One is to detect the Primary User (PU) activities, called spectrum sensing. CR users sense the radio environment continuously and send monitoring results to their base-station. The periodic sensing has separate time slots for sensing and transmission. In addition, CR users monitor the quality-of-service (QoS) of their transmission. According to the detected event type, the base-station determines the spectrum sharing strategies and allocates the spectrums to each user adaptively to the radio environments.

2. Cell Spectrum Sharing: The intra-cell spectrum sharing enables the base-station to avoid the interference to the primary networks as well as to maintain the QoS of its CR users by allocating spectrum resource adaptively to the event detected inside its coverage. If a new CR user appears in this cell, the base-station determines its acceptance and selects the best available spectrum band if it is admitted. Furthermore, when some of its CR users cannot maintain the guaranteed QoS or lose their connections due to the PU activities, the base-station should re-allocate the spectrum resource to them immediately. Also a CR MAC protocol is required to allow multiple CR users to access to the same spectrum band. The intra-cell spectrum sharing has been widely investigated in many literatures and is out of the scope in this project.

3. Inter-Cell Spectrum Sharing: In CR networks, the available spectrum bands vary over time and space which makes it difficult to provide reliable spectrum allocation. Especially in the infrastructure-based networks, the inter-cell interference also needs to be considered in spectrum sharing so as to maximize the network capacity. In the framework, the inter-cell spectrum sharing is comprised of two subfunctionalities: spectrum allocation and power allocation. In the spectrum allocation, the base-station determines its spectrum bands by considering the geographical information of primary networks and current radio activities. The power allocation enables the base-station to determine the transmission power of its assigned spectrum bands so as to maximize the cell capacity without interference to the primary network. When the service quality of the cell becomes worse or is below the guaranteed level, the base-station initiates the inter-cell spectrum sharing and adjusts its spectrum allocation. Based on the spectrum allocation, the base-station determines its transmission power over the allocated spectrum bands

3. ATTACKS IN COGNITIVE RADIO NETWORK

There are many attacks in cognitive radio networks, only few attacks we categorized through three major layers: physical layer, link layer (also known as MAC layer), network layer.

A. Physical Layer: The physical layer is the lowest layer of the protocol .It provides interface to the transmission medium. It consists of anything that is used to make two network devices communicate, such as the network cards, fiber, or, as in the cognitive radio network framework, the atmosphere. The operation of the cognitive radio network is more complicated than other wireless communication networks because the cognitive radio uses the frequency spectrum dynamically.

i)Primary User Emulation Attack(PUE): The cognitive radio network requires ability to distinguish between the primary and secondary user signals. In the primary emulation attack, an attacker may modify their air interface such that it emulates the primary user's signal characteristics causing other secondary users to falsely determine that the frequency is in use by the primary user, and so vacate the frequency. The imposter may perpetrate the attack selfishly, so he can use the spectrum, or maliciously, so the other legitimate users will have their communication disrupted, resulting in a denial of service attack. Therefore, the primary user attack (PUE) can lead to an objective function attack.

ii)Objective function attack: Cognitive radios are adaptive to the environment. Many radio parameters are available for manipulation in the effort to adapt the radio to the environment by maximizing objective functions, and therefore the radio's ability to communicate over the medium. Objective function attacks apply to an attack on any learning algorithms that utilize objective functions. Another name for objective function attacks is belief manipulation attacks [9]. Parameters manipulated include, but are not limited to, bandwidth, power, modulation, coding rate, frequency, frame size, encryption type, and channel access protocol.

iii)Overlapping secondary user: Such a situation places dynamic spectrum access sharing at risk through both objective function and primary user vulnerabilities by one malicious node. A malicious user in one network may transmit signals that cause harm to the primary and secondary users of both networks. Signals transmitted maliciously may provide false sensing information, thereby negatively affecting the objective function in one or both networks. The malicious user may intermittently falsely emulate the primary users of each network causing each network to vacate the channel.

iv)Jamming: Jamming, one of the most basic types of attacks in the cognitive radio network, attempts to adversely affect the signal to noise ratio. In this attack, the malicious user intentionally and continuously transmits on a licensed band, making it unusable by the primary or other secondary users. The attack is amplified by transmitting with high power in several spectral bands. Jamming can be detected with triangulation and energy based techniques. However, the time lost with these techniques allows the attacker to severely impact the network. A mobile attacker can be even more difficult to locate.

B. Link Layer Attacks:

i)Spectrum Sensing Data Falsification (Byzantine attack): In the Byzantine attack, also known as spectrum sensing data falsification, the attacker injecting the false sensing information into the decision stream is a legitimate member of the network and is referred to as the Byzantine. Byzantines may perpetrate the attack to selfishly acquire increased spectrum availability for themselves, or the attackers may have a goal of disrupting the throughput of the network for other nefarious reasons.

ii) Control channel saturation: The control channel saturation attack is based on the fact that if a cognitive radio is unable to complete negotiations during the limited time of the control phase, the radio defers from transmission during the next data phase. This situation may naturally occur when the channel is saturated by a large number of contending cognitive radios. An attacker can broadcast a large number of packets with the intent to saturate the control channel. By sending different types of packets, a malicious node reduces the risk of detection. Combining the control channel saturation attack with the small window backoff attack the attacker may be able to ensure the malicious node captures the control channel before other users.

iii)Control channel jamming: Control channels facilitate the cooperation among cognitive radio users. As a single point of failure, common control channel jamming (CCC) is the most effective and energy efficient way for an attacker to destroy the entire network system. With common control channel jamming, receivers are prevented from receiving valid control messages when a strong signal is injected into the control channel. This results in denial of service for users of the network.

C.Network layer Attacks:

The network layer provides the ability to route data packets from a source node on one network to a destination node on another network, while maintaining quality of service. It also performs fragmentation and reassembly of packets, if required. The cognitive radio network shares security issues with the classic wireless communication networks due to the three shared architectures of mesh, ad hoc, and infrastructure. Cognitive radio networks also share similarities with wireless sensor networks. These include multi-hop routing protocols and power constraints. In addition, there are special challenges faced by cognitive radio networks due to the required transparency of the network activities to the primary user. Routing in the cognitive radio network is further complicated by the requirement of the radio to vacate the frequency when the primary user is sensed as present. Cognitive radio security vulnerabilities are therefore also inherited from these architectural requirements.

i)Sinkhole : Cognitive radio networks often use multi-hop routing. A sinkhole attacker takes advantage of multi-hop routing by advertising itself as the best route to a specific destination. This activity spurs neighboring nodes to use it for packet forwarding. In addition, the neighbors of the attacker will advertise the offender as the best route, creating a „„„sphere of influence‟‟‟‟ for the attacker. The attacker can begin the attack by building a trust base. The attacker can use a higher level of power so it can send any received packets directly to the base station. It can advertise that it is one hop from the base station, and forward all received packets appropriately for a time. After trust has been established, and advertising of the node as the best route has been propagated through the local area, the perpetrator can begin other types of attacks, such as eavesdropping.

ii)Wormhole: The wormhole attack is closely related to the sinkhole attack. Basically, an attacker tunnels messages received in one part of the network over a low latency link. The messages are replayed in another part of the network. In the simplest example, a node situated between two other nodes forwards messages between the two of them. Wormhole attacks are usually administered by two malicious nodes that understate the distance between them by relaying packets along an out-of-bound channel that is unavailable to the other nodes.

iii)HELLO attack The attacker broadcasts a message to all nodes in a network. The packet may be advertising a high quality link to a specific destination. Enough power is used to convince each node that the attacking node is their neighbor. The nodes receiving the packets assume the attacker is very close due to the strength of the received signal, when in fact the attacker is a great distance away. Packets sent from the network nodes at the regular signal strength would be lost. In addition, network nodes may find themselves with no neighbors available to forward packets to a particular destination, since all nodes are forwarding packets towards the attacker. Protocols that depend upon localized information exchange between neighbors for topology maintenance are also subject to the attack. Note that an adversary need not to be able to read or construct legitimate traffic; the attacker needs only to capture and rebroadcast overheard packets with enough power to reach every node in the network.

CONCLUSION

Cognitive radio is an immature but rapidly developing technology area. In terms of spectrum regulation, the key benefit of CR is more efficient use of spectrum, because CR will enable new systems to share spectrum with existing legacy devices, with managed degrees of interference. There are significant regulatory, technological and application challenges that need to be addressed and CR will not suddenly emerge. Cognitive radio networks are being studied intensively. The major motivation for this is the currently heavily underutilized frequency spectrum. A fundamental property of the cognitive radio networks is the highly dynamic relationship between the primary users having an exclusive priority to their respective licensed spectrum and the secondary users representing the cognitive network devices. From the traffic point of view careful attention must be paid in order to guarantee an effcient usage of the wireless medium while simultaneously providing fairness between competing users and respecting the priority of the primary users.

REFERENCES

[1] Jai Sukh Paul Singh, Jasvir Singh, A.S. Kang, “Cognitive Radio: State of Research Domain in Next Generation Wireless Networks - A Critical Analysis”, International

Journal of Computer Applications (0975 – 8887) Volume 74– No.10, July 2013.

[2]Blaine Chamberlain And Geogette Jordan“ Applications of Wireless Sensors in Monitoring Indoor Air Quality in the Classroom Environment”, Research Experiences for Teachers in Sensor Networks, Summer Internship 2012,University of North Texas,NSF-1132585.

[3]Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris, “A high-throughput path metric for multi-hop wireless routing”, Wireless Networks, vol. 11, no. 4, pp. 419–434, 2005.

[4] Prof. B.N. Jagdale and Prof. Pragati Patil, “Analysis and Comparison of Distance Vector, DSDV and AODV Protocol of MANET”, International Journal of Distributed and Parallel Systems (IJDPS),Vol.3, No.2, March 2012.

[5] H. Yang, Y. Qin, G. Feng, and H. Ci, “Online monitoring of geological CO2 storage and leakage based on wireless sensor networks,” IEEE Sensors Journal, vol. 13, no. 2, pp. 556–562, Feb. 2013.

[6] X. Mao, X. Miao, Y. He, X.-Y. Li, and Y. Liu, “Urban CO2 monitoring with sensors,”in Proc. IEEE INFOCOM, Mar. 2012, pp. 1611–1619.

[7] Zhou Hongqing and Yang Chunying, ``A Mobile Ad Hoc Networks Algorithm Improved AODV Protocol’’, 2011 International Conference on Power Electronics and Engineering Application (PEEA 2011).

[8] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, “Wireless sensor networks for habitat monitoring”, Proceedings of the 1st ACM International workshop on Wireless sensor networks and applications, Atlanta, Georgia, USA, 88-97, 2002.

[9] Nor Surayati Mohamad Usop, Azizol Abdullah and Ahmad Faisal Amri Abidin,“Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment”, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7, July 2009.

[10] GodblessSwagarya, ShubiKaijage and Ramadhani S. Sinde“A Survey on Wireless Sensor Networks Application for Air Pollution Monitoring”, International Journal of Engineering and Computer Science, vol.3,no.5, ISSN:2319-7242,MAY 2014.

[11]Ozgur B. Akan Osman B. Karli Ozgur Ergul “Cognitive radio sensor networks” ,Next generation Wireless Communications Laboratory (NWCL), Department of Electrical and Electronics Engineering.

[12] Deepak Kumar Patel, Rakesh Kumar, A.K.Daniel, “Performance Analysis and Behavioural Study of Proactive and Reactive routing protocols in MANET ”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, April 2013.

[143]V.Rajeshkumar, P.Sivakumar, “Comparative Study of AODV, DSDV and DSR Routing Protocols in MANET Using Network Simulator-2”, International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 2, Issue 12, December 2013.

[14]P. Spachos and D. Hantzinakos, “Scalable dynamic routing protocol for cognitive radio sensor networks,” IEEE Sensors J., vol. 14, no. 7, pp. 2257–2266, Jul. 2014.

[15] D. Hatzinakos, P. Chatzimisios and P. Spachos, “Cognitive networking with opportunistic routing in wireless sensor networks”, in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2013, pp. 2433–2437.

[16] PetrosSpachos and DimitriosHatzinakos,” Real-time Indoor Carbon dioxide Monitoring through Cognitive Wireless Sensor Networks”, IEEE SENSOR JOURNAL, vol.16, no. 2, January 15, 2016.