International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-2 Number-1 Issue-3 March-2012

Authentication of Primary User in Cognitive Radio

Sudesh Gupta [1], Rajesh Nema [2], Puran Gour [3]
PG scholar in Department of Electronics & comm. Engineering NIIST Bhopal[1]
Assistant professor in Electronics & comm. Engineering NIIST Bhopal[2]
Assistant professor in Electronics & comm. Engineering NIIST Bhopal[3]

Abstract

Cognitive Radio (CR) or software defined radio is a new concept for maximizing the utilization of the radio spectrum. The CR can sense the unused frequency spectrum at any time from the wide range of wireless radio spectrum. This gives the efficient use of radio resources. In cognitive radio environment, a primary licensed user (PU) can share spectrum availability information with a secondary user, the secondary user will then be able to access available frequency spectrum. However, a secondary user should always need to verify the authenticity of the spectrum occupancy information whether it comes from the authentic primary users. Without the verification, a malicious user can give false information about the spectrum occupancy. This can result interference to the primary users and minimize available spectrum for the secondary usage. In this paper, we have develop an efficient technique to verify the source of the spectrum occupancy information is to be from the authentic primary user , by doing this we are maximizing the spectrum utilization efficiency and minimizing any interference to the primary licensed users.

Keywords

CR, CRN, FCC, CCC, Primary User (PU)

1. Introduction

Cognitive radio network (CRN) is a novel concept of wireless communication, in which the secondary users (cognitive radio users) are allowed to use frequency spectrum without the permission of the primary licensed user (PU), provided that the secondary users do not introduce harmful interference to the PU. From this definition, we extract two components and one requirement. The components are the PU who has the license to use the spectrum band and the CR user who wants to use the spectrum without having a license. The requirement is a non-harmful interference to the PU. To achieve the above requirement, generally, sensing algorithms adopt the periodic sensing structure, where CR users have periodic detection cycle. This detection cycle is divided into sensing and transmission times.

This periodic sensing is called in-band sensing. Sensing efficiency is measured by the ratio of the transmission time to the transmission plus sensing times. Long sensing time is necessary to achieve high throughput by reducing false alarms that result from short sensing times, and to prevent hidden terminal problem which requires the CRs to be far more sensitive than Pus (by 30-40 dB [1]). However, longer sensing time decreases transmission time which means less sensing efficiency and less throughput. Therefore, there is a tradeoff between sensing time and throughput. For example, when the PU's required detection probability is 0.999, the best channel efficiency that can be achieved is only about 27% [2]. Therefore, in-band sensing time forms a non-negligible overhead.

Many papers have been proposed thus far to reduce in-band sensing time. But, they still require the node to do periodic sensing like [3], [4], and [5]. They still have low sensing efficiency on low SNR and high required detection probability. Some of the used methods to enhance sensing efficiency is to use cooperative sensing techniques that reduces the required sensing time, or to use energy detection sensing that is fast. These two methods come on the cost of security.

2. Fundamental of Cognitive Radio

In 2004, the FCC issued a notice of proposed rulemaking (NPRM) that raised the possibility of permitting unlicensed users to temporarily “borrow” spectrum from licensed holders as long as no undue interference is seen by the primary user [6]. Devices that borrow spectrum on a temporary basis without generating harmful interference are commonly referred to as “cognitive radios” [7].Basic cognitive radio techniques, such as dynamic frequency selection (DFS) and transmit power control (TPC), already exist in many unlicensed devices. However, to reach the full promise of cognitive radios, many significant design challenges lie ahead. Before beginning operations, cognitive radios must obtain an estimate of the power spectral density (PSD) of the radio spectrum to determine which frequencies are used and which frequencies are unused. In order to accurately measure the spectrum, a highly sensitive radio will be required to measure signals at their cell edge. Consider the example of digital TV which lies at the cell edges; the received signal will be just barely above the sensitivity of the receiver. For a cognitive radio to be able to detect this signal, it needs to have a radio that is considerably more sensitive. If the cognitive radio is not capable of detecting the digital TV signal, then it will incorrectly determine that the spectrum is unused; thereby leading to potential interference if this radio spectrum is used, i.e., the signal transmitted by the cognitive radio will interfere with the signal the digital TV is trying to decode. This situation is often referred to as the "hidden node problem".

3. Threats and Attack in cognitive Radio

There are two types of architectures in CRN, centralized and distributed. And there are two types of access behaviors, cooperative and non-cooperative. The centralized and cooperative types are more vulnerable. In the cooperative approach, attacking one node and taking control of that node will impact the network because it will send spoof packets to other nodes. In centralized approach, if the attacker can manipulate the common control channel, then this makes the whole network under control of the attacker. On the other hand, in distributed and non-cooperative approaches, attacking a node effect will not propagate to other nodes.

Security must be taken into account at the early design stages before deploying the standards. Solving security problems after deploying a CRN designs and standards may be impractical. IEEE 802.22 [8] is the first standard in CRNs. It uses the security standard IEEE 802.16e for solving the CRN security problems. But, IEEE 802.16e does not consider the unique aspects of the CRN. Therefore, there must be some modifications to the IEEE 802.16e standard to CRNs. The authors in [9] categorized security attacks in CRNs as conventional and non-conventional attacks. The conventional attacks are the attacks that are related to confidentiality, authenticity and other security problems that can be countered by conventional cryptography techniques. Non-conventional attacks are the attacks that cannot be countered by the cryptography systems alone like: Primary User Emulation (PUE), Byzantine failure in cooperative sensing, and network self-coexistence when two different CRNs coexist with each other. CRN is subject to conventional attacks that are similar to other wireless networks; they can be classified as passive or active attacks [11].

Active attacks include:

- Masquerade: when one entity tries to pretend to be another one.
- Replay: when an attacker eavesdrops packets and re-sends them.
- Fabrication: it refers to generating and spreading wrong messages in the network.
- Modification: when part of a message is altered, or the order of a stream of messages is changed, or the arriving time of the message is delayed.
- Denial of Service: when a malicious node prevents or delays some legitimate users from taking a service.
- Wormhole: it is creating a tunnel between two colluding nodes.

Passive attacks include:

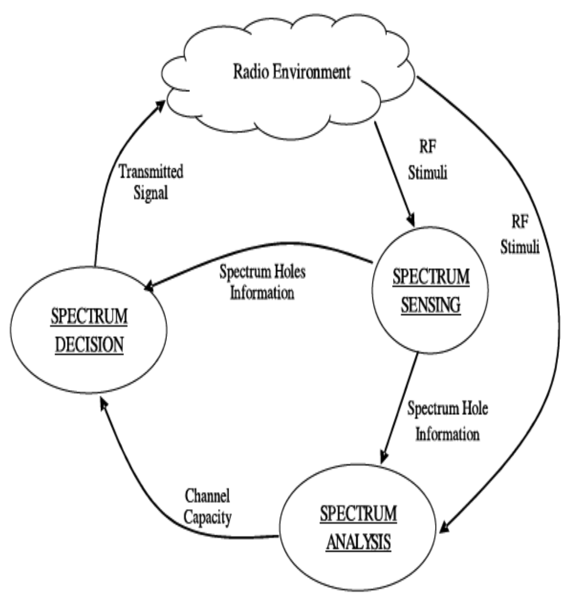

Figure 1: Cognitive Cycle

1. Eavesdrop: because of the broadcasting nature of wireless medium.
2. Black hole: which is filtering out some portions of the received packets.

CRNs use dynamic spectrum access (DSA) techniques. In order to adapt to dynamic spectrum environment, the CRN necessitates the spectrum-aware operations, which form a cognitive cycle as shown in Fig. 1 [10], the cognitive cycle consists of four spectrum management functions: spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility.

1. Spectrum sensing threats: Fig. 1 shows that spectrum decision and spectrum mobility take their inputs from spectrum sensing. Therefore, a security attack or threat on sensing will affect the functions of spectrum mobility and spectrum decision as well which affects spectrum sharing.
2. Spectrum decision threats: it is divided into spectrum analysis and spectrum decision. Threats come from the possibility of false or fake spectrum characteristics parameters generated by sensing. Therefore, wrong decisions will be taken. Results of spectrum decision threats are either deciding to use a channel that is not free which means interfering the PU, or decide not to use a free channel, which results in underutilizing the spectrum.
3. Spectrum sharing threats: When multiple CR nodes or even multiple CRNs want to use the channel, they must share the channel. Therefore, there is a need for resource allocation techniques. These techniques can be susceptible to selfish behaviors, where a malicious node may try to fool other nodes in the network to monopolize the channel.
4. Spectrum mobility threats: An attacker can induce a fail handoff attack by: compelling the CR to vacate the used spectrum by PUE, slowing down the process of selecting a free spectrum by jamming the communication, or making communication failure. What exaggerates security problems in CRNs are: first, Federal Communications Commission (FCC) requires that the followed techniques in CRNs must not interfere with the incumbent primary users. Second, CR nodes should not interact with the PU or change their work method. Third, the inherent programmability of cognitive radios where the nodes have the ability to work on multiple frequencies, bandwidths, data rates, modulations, spectrum access technology, and different transmission powers. These parameters can be changed dynamically while running. This makes nodes easily spoof others. Fourth, the absence of authentication information where any node can join the network and starts sharing the channel because all the CR nodes are not licensed.

4. Authentication of Primary User

In this work, we analyzed the importance of ensuring authentication of the Spectrum Occupancy Information and propose an efficient technique to verify the source of the information is from the authenticate primary user.
For our research, we make the following assumptions:

1. Our first assumption is based on path loss, by using the path loss we can estimate the Distance between transmitter and receiver.
2. In our second assumption we are using thumb rule to find the distance between transmitter and receiver. Using thumb rule we can find coordinates for primary and secondary users. so the location of the primary users should be known by the secondary user as well. A cognitive radio user, can calculates the distance between the secondary user and the primary user based on various parameters. If distance calculated with the different techniques match, then a cognitive radio user knows that it is talking with a legitimate trustworthy user; otherwise it is a malicious user.

In the cognitive radio network, users can share spectrum occupancy information for correct evaluation of the unused spectrum. A malicious user can claim to be a primary user and can give false information about the spectrum occupancy, thereby minimizing the available spectrum utilization efficiency. As the cognitive radios are limited resources, a robust and well established security techniques developed in Computer Networks may not be a suitable solution in cognitive radio environment. Based on the above assumptions, we propose an efficient technique for validating the source of the spectrum occupancy information

4. 1 Proposed Algorithm:

In our proposed methodology, by using thumb rule, we calculate distance between a cognitive radio user and other users based on location coordinates as well as by using path loss method. If the distance calculated with both of these techniques is approximately equal, then the user is a Authentic user. Otherwise, it would be considered as malicious user.

4.1.1 Calculation of distance based on Thumb rule:

A common rule of thumb that is used in RF engineering is: 6 dB increase in link budget results in doubling the transmission distance. This rule is correct for the Free-space path loss model but is overly optimistic and does not hold true for more realistic models. Using the above thumb rule we can find location coordinates and based on the location coordinates, distance between the users can be calculated. Consider (x,y) is x and y coordinates of a cognitive radio and (x_1,y_1) is x and y coordinates of an existing (primary) users. The distance between a cognitive radio and an existing user, d, is given by the following equation:

$$d = \sqrt{(x - x_1)^2 + (y - y_1)^2}$$

With this information, distance between any users can be computed.

4. 2 Calculation of distance by Path Loss:

For radio transmission systems we are using the Free Space Path Loss model in determining transmitter and receiver separation, A typical RF transmission system is shown in Figure 1. The received signal strength (link budget) in Figure 4.2 is equal to:

$$P_r = \frac{P_t G_T G_r \lambda^2}{(4\pi)^2 d^2}$$

Path loss and distance calculations:

Path Loss is the largest and most variable quantity in the link budget. It depends on used frequency, antenna height, receive terminal location relative to obstacles and reflectors, and link distance, among many other factors. Usually a statistical path loss model or prediction program is used to estimate the median propagation loss in dB. Based on the noise level, the distance calculated with received power level may not be very accurate. However, statistically, the distance calculated with both of the methods should come close. We expect the trust values to be close to 1 for authentic users. Similarly, we expect the trust value to be low for unauthentic users.

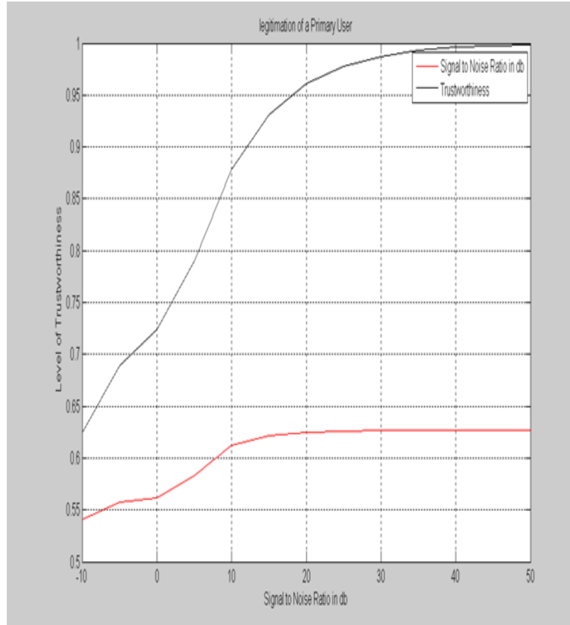

Figure 2: Signal to Noise Ratio in DB

5. Conclusion

Cognitive radio introduces a new level of worldliness to wireless communications technology. Basic cognitive radios operate autonomously and depend on highly sensitive receivers and device learning to know when and how spectrum can be accessed.

The Cognitive Radio gives an efficient solution to the spectrum scarcity problem by sensing the unused spectrum of the licensed users and providing that unused spectrum to the secondary users without causing any interference between primary user and the secondary user. Cognitive radio increases the efficiency of the spectrum significantly. But the secondary user must make sure that the information regarding the occupancy of the spectrum is provided by a authentic primary user. Thus we can conclude that our algorithm is an efficient technique to authenticate the primary user.

Reference

[1] D. Cabric, S.M. Mishra, and R.W. Brodersen. Implementation issues in spectrum sensing for cognitive radios. In Asilomar Conference on Signals, Systems, and Computers, volume 1, pages 772-776. Citeseer, 2004.

[2] P. Wang, L. Xiao, S. Zhou, and J. Wang. Optimization of detection time for channel e±ciency in cognitive radio systems. In IEEE

Wireless Communications and Networking Conference, 2007. WCNC 2007, pages 111{115, 2007.
[3] W.Y. Lee and I.F. Akyildiz. Optimal spectrum sensing framework for cognitive radio networks. IEEE Transactions on Wireless Communications, 7(10):3845{3857, 2008.
[4] A. Ghasemi and E.S. Sousa. Optimization of spectrum sensing for opportunistic spectrum access in cognitive radio networks. In Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC), pages 1022{1026, 2007.
[5] Y.C. Liang, Y. Zeng, E.C.Y. Peh, and A.T. Hoang. Sensing-throughput tradeo® for cognitive radio networks. IEEE Transactions on Wireless Communications, 7(4):1326{1337, 2008.
[6] Federal Communications Commission, "Unlicensed Operation in the TV Broadcast Bands," ET Docket No. 04-186, 2004.
[7] J. Mitola, III, "Cognitive Radio for Flexible Mobile Multimedia Communications," Mobile Multimedia Communications, 1999. IEEE International Workshop, page 3.
[8] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar. IEEE 802.22: an introduction to the ¯rst wireless standard based on cognitive radios. Journal of communications, 1(1):38{47, 2006.
[9] Jung-Min Park. Securing the Airwaves So You Dont Have To Seeking a Secure Cognitive Network.
[10] I.F. Akyildiz, W.Y. Lee, M.C. Vuran, and S. Mohanty. NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey. Computer Networks, 50(13):2127{2159, 2006.
[11] T. Chen, H. Zhang, G.M. Maggio, and I. Chlamtac. Topology management in CogMesh: a cluster-based cognitive radio mesh network. In IEEE CogNet Workshop in conjunction with IEEE ICC 2007. Citeseer, 2007.

Sudesh Gupta, PG Scholar, Department of Electronics and Communication Engineering, NIIST, Bhopal(India). I'm doing my M.Tech. with specialization in Digital communication. I have done my B. E. From Government Engineering College Jabalpur. I have also done C-DAC From ACTS Badnera.