ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE
Your ult-MATE Research Paper !!!

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 8, Issue 10, October 2022

DATA TRANSMISSION USING OFDM COGNITIVE RADIO UNDER INTERFERENCE ENVIRONMENT

Vinothkumar J[1], Shanthamathi K S[2]

[1] Assistant Professor, Department of Electronics and Communication, Thanthai Periyar Government Institute of Technology, Vellore, (TN)

[2] Assistant Professor, Department of Electronics and Communication, Ganadipathy Tulsi's Jain Engineering College, Vellore, (TN)

[1]jpvinoth87@gmail.com, [2] shanthamathi@gmail.com

***Abstract*—A cognitive radio-based wireless mesh network is considered. We consider a cognitive radio (CR) network that makes opportunistic use of a set of channels licensed to a primary network. During operation, the CR network is required to carry out spectrum sensing to detect active primary users, thereby avoiding interfering with them. Interference temperature model is used to define the occupancy and availability of a channel. The interference temperature (IT) model offers a novel way to perform spectrum allocation and management. Efficient and reliable subcarrier power allocation in orthogonal frequency-division multiplexing (OFDM)-based cognitive radio networks is a challenging problem.**

***Keywords*— Cognitive radio, Interference temperature, Sensing techniques, OFDM-CR.**

I. INTRODUCTION:

THE traditional approach of fixed spectrum allocation to licensed networks leads to spectrum under-utilization. In recent studies by the FCC, it is reported that there are vast temporal and spatial variations in the usage of allocated spectrum. This motivates the concepts of *opportunistic spectrum access* that allows cognitive radio (CR) networks to opportunistically exploit under-utilized spectrum. On the one hand, opportunistic spectrum access can improve the overall spectrum utilization. On the other hand, transmission from CR networks can cause harmful interference to primary users of the spectrum. To mitigate such a problem, CR networks can frequently carry out spectrum sensing to detect active primary users. Upon detecting an active co-channel primary user, a CR network can either change its operating parameters, e.g., reduce its transmit powers, or move to another channel to avoid interfering with the primary user. In most cases, to achieve reliable spectrum sensing for a particular channel, a CR network has to postpone all of its transmissions on that channel, i.e., *quiet sensing periods* must be scheduled. Note that scheduling quiet sensing periods results in negative impacts to various performance metrics of CR networks, such as throughput and latency. One approach to reduce these negative impacts is to design efficient spectrum sensing algorithms that require short sensing time. One of the criteria, proposed by the Interference Protection Working Group of Spectrum Policy Task Force (set up by FCC) to opportunistically share the licensed spectrum bands and to quantify and manage the interference is interference temperature. Interference temperature is a measure of the RF power available at a receiving antenna to be delivered to receiver – power that is generated by other emitters and noise sources. FCC in its Notice for Proposed Rule Making (NPRM) has suggested that unlicensed devices can be allowed to use licensed spectrum bands in a geographical region provided the interference temperature at each licensed receiver in the region does not exceed an interference temperature threshold. [1] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). [2] discussed that the activity related status data will be communicated consistently and shared among drivers through VANETs keeping in mind the end goal to enhance driving security and solace. Along these lines, Vehicular specially appointed systems (VANETs) require safeguarding and secure information correspondences. Without the security and protection ensures, the aggressors could track their intrigued vehicles by gathering and breaking down their movement messages. A mysterious message confirmation is a basic prerequisite of VANETs.

II. GENERAL CR SYSTEM MODEL:

We consider a CR deployment on licensed band, as depicted in Fig. 1. Each CR network consists of a set of nodes that are supported by a base station (BS). Each CR network operates based on making opportunistic use of the channels that belong to a primary network. This is one of the CR network architectures similar to the future deployment of IEEE802.22 technologies.

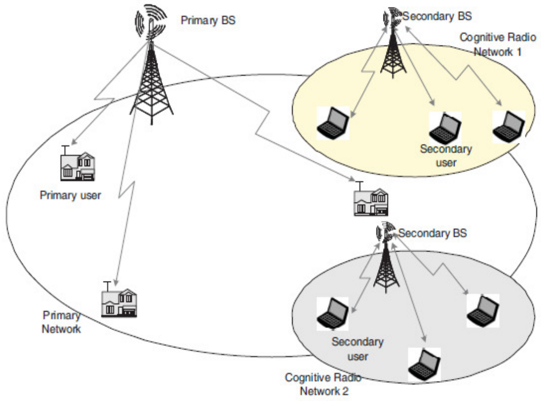

Fig.1.General system model

III. INTERFERENCE TEMPERATURE MODEL:

The concept of interference temperature is identical to that of noise temperature. It is a measure of the power and bandwidth occupied by interference. Interference temperature TI is specified in Kevin and is denoted as

$$T_I(f_c,B)=\frac{P_I(f_{c,}B)}{KB}$$

where PI (fc;B) is the average interference power in Watts centered at fc, covering bandwidth B measured in Hertz. Boltzmann's constant k is 1.38 x 10^23 Joules per Kelvin degree. .

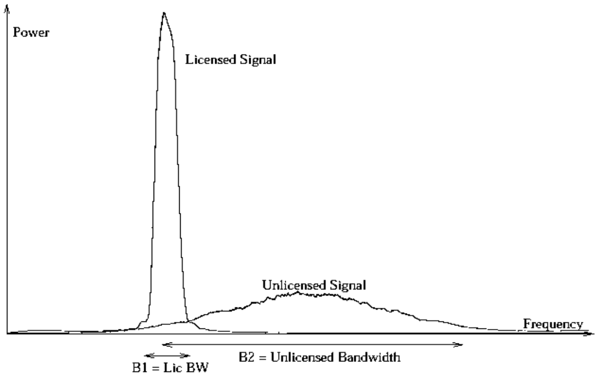

Figure 2: Example PSD for an unlicensed signal partially overlapping a licensed signal.

The idea is that by taking a single measurement, a cognitive radio can completely characterize both interference and noise with a single number. Of course, it has been argued that interference and noise behave differently. Interference is typically more deterministic and independent of bandwidth, whereas noise is not. For a given geographic area, the FCC would establish an interference temperature limit, TL. This value would be a maximum amount of tolerable interference for a given frequency band in a particular location. Any unlicensed transmitter utilizing this band must guarantee that their transmissions added to the existing interference must not exceed the interference temperature limit at a licensed receiver. While this may seem clear cut, there is ambiguity over which signals are considered interference, and which fc and B to use. Should they reflect the unlicensed transceiver or the licensed receiver? For example, consider figure 2 should we use B1 or B2 as our bandwidth for our computations? These ambiguities precipitate the need for our two interpretations.

III .INTERFERENCE TEMPERATURE MEASUREMENT.

The FCC NPRM suggests three possible methods of measuring interference temperature at different locations in a region. In this subsection, we briefly summarize the three methods.

1) Measurement by Primary Receiver

Since, ideally the interference temperature needs to be measured and controlled at primary receivers, the most appropriate approach is that the primary receivers themselves measure the interference temperature at their antenna, and send the values back to the unlicensed secondary devices in the region. Though this approach is most accurate (as primary receivers know the exact modulation type and waveform details of transmitted primary signals), it requires major hardware and software modifications in the primary receivers. This is clearly infeasible, especially for devices (such as TVs, Laptops, Mobile phones, PDAs, etc.) which are already developed and deployed. Moreover, it requires a channel for explicitly transmitting the measured values to the secondary transmitters.

2) Grid of Monitoring Stations

Another approach to measure interference temperature is to deploy a grid of monitoring stations in the target region. These devices are dedicated for measuring the Interference temperature at the location of their deployment, and send these measurements back usually to a well-known sink node in the grid (from which the secondary devices can obtain the interference temperature in their nearby region). A major advantage of this approach is that it does not require any modification in primary system. Moreover, these devices, being dedicated for interference temperature measurement, can be fine tuned for high precision, and are usually not power-starved. This is in contrast to small devices (either secondary or primary), such as mobile phones and PDAs, where incorporating measurement capabilities are costly in terms of silicon real-estate and battery power consumption.

On the other hand, this approach has several disadvantages too. First, the interference temperature is measured at locations (i.e. at grid nodes), which are different from where it need to be controlled (i.e. at primary receivers). The interference temperature at these different locations may be different due to differing terrain and path loss conditions. This approach also suffers from hidden terminal problem. Grid nodes usually cannot exactly know the path loss between Secondary transmitters and primary receivers, as well as the shadowing and fading effects experienced at primary receivers.

3) Measurement by Secondary Transmitters

The simplest but somewhat inaccurate method to measure the interference temperature is to let a secondary device itself measure the interference temperature locally. This approach neither requires any modification in primary system, nor any additional deployment of measuring services. But the interference temperature that the secondary device measures locally and the one that is present at a primary receiver may differ significantly (unless both the devices are very near to each other), due to location and terrain-dependent multipath interference and shadowing affects. Moreover, secondary devices need to be equipped with interference temperature measurement capabilities.

IV SPECTRUM SENSING IN CR NETWORKS:

Spectrum sensing is crucial for CR networks to detect active primary users and avoid causing interference. Let us briefly go through important parameters that characterize spectrum sensing in CR networks.

1) Signal to Noise Ratio (SNR): When a primary user is active, the higher the SNR of the primary user's signal at the receiver of a CR device, the easier it is to detect. We denote this SNR by γ.

2) Probability of Detection Pd: This is the probability that a CR network accurately detects the presence of an active primary user. The higher the value of Pd, the better the protection for primary operation.

3) Probability of False Alarm Pf: This is the probability that a CR network falsely detects the presence of primary users when in fact none of them are active at the sensing time. From the CR network point of view, the lower the value of Pf, the higher the spectrum utilization.

4) Detection Time T_d: This is the time taken to detect a primary user since it first turns on.

V OFDM- COGNITIVE RADIO:

Orthogonal-Frequency-Division Multiplexing (OFDM) is the best physical layer candidate for a CR system since it allows easy generation of spectral signal waveforms that can fit into discontinuous and arbitrary-sized spectrum segments. Besides, OFDM is optimal from the viewpoint of capacity as it allows achieving the Shannon channel capacity in a fragmented spectrum. Owing to these reasons, in this paper, we consider the problem of Data Transmission in an OFDM based CR system. When we transmit data in OFDM, BER decreases, when signal-to-noise ratio increases. Simulation result is shown in the fig.3.

VI SIMULATION RESULT:

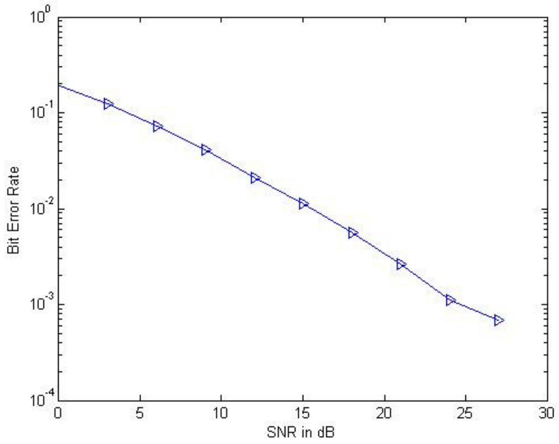

FIGURE.3.BER Vs SNR

VII CONCLUSION:

In this paper we have considered how to use both interference temperature and the regulatory interference temperature limit to select an optimal radio bandwidth for a particular interference environment.Also we discussed both spectrum sensing parameters and the effect of data transmission in OFDM.

REFERENCES

[1] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254).

[2] Christo Ananth, Dr.S. Selvakani, K. Vasumathi, "An Efficient Privacy Preservation in Vehicular Communications Using EC-Based Chameleon Hashing", Journal of Advanced Research in Dynamical and Control Systems, 15-Special Issue, December 2017,pp: 787-792.

[3] Ziaul Hasan, Gaurav Bansal. Ekram Hossain, Vijay K. Bhargava, " Energy Efficient Power allocation in OFDM-Based Cognitive Radio Systems: A Risk Return Model"IEEE Transactions on Wireless Communications, Vol 8, No 12, DEC 2009.

[4] Manuj Sharma, Anirudha Sahoo, K.D. Nayak, "channel Selection Under IT Model in Multi-hop Cognitive Radio Mesh Networks", IEEE transactions on communication, Vol 6,2009.