ABSTRACT

Cognitive Radio (CR) and Long Term Evolution in unlicensed band (U-LTE) are the recently evolved technologies, both contributing to the wireless communication era. Cognitive radio technology has the potential to resolve the efficient utilization of available spectrum by the legitimate unlicensed users. The IEEE 802.22 WRAN standard was developed with the objective to apply cognitive radio techniques to share the unused television broadcast spectrum on a non-interference fashion to facilitate the broadband access to less populated area and during disaster time. The successful deployment of Cognitive Radio Network (CRN) has made it essential to research into its security issues. The Primary User Emulation attack (PUEA) is unique to CRN and it is the fundamental threat to CRNs. In PUE attack, a greedy or a malicious secondary user mimics the characteristics of a primary user signal and achieves the priority over other secondary users.

In this research work a computationally efficient algorithm to detect the PUE attack has been developed and tested. The PUE attack is detected by distinguishing the malicious secondary user signals from legitimate primary user signals. The malicious user signals are detected by investigating their cyclostationary properties by the cognitive radios in the secondary users. The cyclostationary feature detection technique studies the periodicity of the primary user signal to confirm its presence in the spectrum. The periodic features of primary user signal are extracted by the spectral correlation function. Absence of such periodicity in the investigated signals infers the presence of malicious user signals. The detection algorithm is implemented in a simulated cognitive radio network environment of UHF vi Band IV (470 – 590 MHz). The malicious signals are generated to mimic the power levels of the primary signals in both high- and low- signal to noise ratio (SNR) levels. The detection probability ( ) of the malicious user signals are investigated under low and high noise levels. At low noise level, the detection probability is 0.5. But, at high noise level, the detection probability of 1.0 is achieved successfully.

The performance of the developed algorithm is improved under a Cooperative Cognitive Radio Network environment. The cooperative model consists of a centralized Fusion Centre (FC) synchronized with multiple cooperative secondary users. The cooperative secondary users report the diagnosed sensing results to the FC at regular intervals. The diagnosed signals are used to anticipate the greedy secondary users at the earliest stage. The performance of the system model is analysed in terms of detection accuracy and detection latency. In the simulated environment with one FC and five cooperative secondary users, 100% detection accuracy is achieved during high noise level conditions. At the same time, the detection latency increases due to the overhead caused at the Fusion Centre by the cooperative SUs which is considered to be negligible.

Long Term Evolution in unlicensed band (U-LTE) extends the benefits of Long Term Evolution to deploy in 5 GHz unlicensed spectrum, enabling mobile operators to offload data traffic onto unlicensed frequencies. The coexistence of LTE users with incumbent unlicensed users in a non-interference style is the major issue of U-LTE.

A Cognitive Radio based system model to enhance the coexistence of LTE with Wi-Fi/IoT users in the unlicensed 5GHz spectrum is developed and evaluated. In the unlicensed 5GHz spectrum, the Wi-Fi/IoT and LTE users are assumed as primary and secondary users respectively. The vii developed system model achieves the Listen-Before-Talk (LBT) regulatory enforcement of radio communication in U-LTE. The U-LTE network is simulated in compliance with Rel.13 3GPP standards. The range of 5 GHz band is considered as from 5.0 GHz to 5.8 GHz with 23 channels, each assumed with a bandwidth of 20MHz. Based on the dynamic spectrum access property of CR, a channel and traffic model is formulated. With the experimental setup, the Coexistence of U-LTE with Wi-Fi/IoT is investigated in two fashions (i) in non_LBT feature and (ii) including LBT feature, in terms of the performance metric: Wi-Fi back off rate. The back off rate of Wi-Fi is efficiently reduced to 30% with the application of CR in LBT scenario.

The effectiveness of CR based U-LTE coexistence model in different types of IEEE 802.11 (a/n/ac) 5 GHz band with varying data rates and bandwidth capacity is also investigated. The behaviour of the system is studied by proposing two resource allocation algorithms namely (i) dedicated channel capacity allocation algorithm and (ii) Shared channel capacity allocation algorithm. In the dedicated channel allocation algorithm, the channel‘s service capacity is utilized either by LTE data or Wi-Fi/IoT data for a particular time slot. In shared channel capacity allocation algorithm, the resource allocation is based on subcarriers of 802.11 standards. The performance of both allocation algorithms are measured in terms of two performance metrics (i) Wi-Fi back-off rate and (ii) Wi-Fi throughput. The Wi-Fi back-off rate is efficiently reduced to less than 10% and the Wi-Fi throughput is achieved above 90%. The major security challenge of CR to mitigate the Primary User Emulation attack is also addressed. viii The focus of the above research work is to reduce the interference caused by LTE in unlicensed 5GHz band which is achieved and the performance of the Wi-Fi systems are improved. Since the upcoming IoT communications are one of the incumbent users of unlicensed spectrum, the need for their spectrum utilization is considered in this research work.