Cognitive Radio Network (CRN) is an emerging paradigm that makes use of Dynamic Spectrum Access (DSA) to communicate opportunistically, in the unlicensed frequency bands otherwise licensed to incumbent users such as TV broadcast. Interest in the development of CRNs is because of severe underutilization of spectrum bands by the incumbent primary users (PUs) that have the license to use them coupled with an ever-increasing demand for unlicensed spectrum for a variety of new mobile and wireless applications. The essence of Cognitive Radio (CR) operation is the cooperative and opportunistic utilization of licensed spectrum bands by the secondary users (SUs) that collectively form the CRN without causing any interference to PUs’ communications.

CRN operation is characterized by factors such as network-wide quiet periods for cooperative spectrum sensing, opportunistic/dynamic spectrum access and non-deterministic operation of PUs. These factors can have a devastating impact on the overall throughput and can significantly increase the control overheads. Therefore, to support the same level of QoS as traditional wireless access technologies, very closer interaction is required between layers of the protocol stack.

DSA is undertaken in a collaborative manner where SUs periodically carry out spectrum sensing in their respective geographical locations. Collaborative spectrum sensing has numerous security loopholes and can be favorable to malicious nodes in the network that may exploit vulnerabilities associated with DSA such as launching a spectrum sensing data falsification (SSDF) attack. Some CRN standards such as the IEEE 802.22 wireless regional area network employ a two-stage quiet period mechanism based on a mandatory fast sensing and an optional fine sensing stage for DSA. Malicious nodes in the CRN however, can take advantage of the two-stage spectrum sensing mechanism to launch smart denial of service (DoS) jamming attacks on CRNs during the fast sensing stage.

Coexistence protocols enable collocated CRNs to contend for and share the available spectrum. However, most coexistence protocols do not take into consideration the fact that channels of the available spectrum can be heterogeneous in the sense that they can vary in their characteristics and quality such as SNR or bandwidth. Without any mechanism to enforce fairness in accessing varying quality channels, ensuring coexistence with minimal contention and efficient spectrum utilization for CRNs is likely to become a very difficult task.

The cooperative and opportunistic nature of communication has many challenges associated with CRNs’ operation. In view of the challenges described above, this dissertation presents solutions including cross-layer approaches, reputation system, optimization and game theoretic approaches to handle (1) degradation in TCP’s throughput resulting from packet losses and disruptions in spectrum availability due non-deterministic use of spectrum by the PUs (2) presence of malicious SUs in the CRN that may launch various attacks on CRNs including SSDF and jamming and (3) sharing of heterogeneous spectrum resources among collocated CRNs without a centralized mechanism to enforce cooperation among otherwise non-cooperative CRNs.

Major: Computer Science

Educational Career:
Bachelor’s of Software Engineering, BS, 2000, National University of Sciences and Technology, Pakistan.
Master's of Software Engineering, MS, 2004, National University of Sciences and Technology, Pakistan.

Committee in Charge:
Dr. Cliff C. Zou, Chair, EECS
Mostafa Bassiouni, EECS Department, UCF