Detection scheme for primary user emulation attacks in cognitive radio network using game theoretic approach

**Jobanmeet Kaur (1452677)**

# ABSTRACT

In the present world, the ubiquity of wireless technologies is more a reality than a goal, even in many developing economies. Radio communication and engineering is in the phase of an exciting transformation. With the advent of Software Defined Radios, the analog devices are greatly scrutinized to meet the ever-increasing demands so as to gain access to the spectrum in greater parts. Radio propagation is notoriously ragged in its spatial extent, even between 300 MHz and 3 GHz. Radio communication systems requires high security from interfering systems and this is guaranteed by spectrum licensing. However, licensing sometimes wastes the precious radio resource. Thus, paradoxically, 90-95% of the licensed radio spectrum is not in use at any location at any given time and the spectrum is wasted.

Cognitive Radio provides an evolutionary series of frameworks towards an ultimate realisation of 'better use of radio spectrum for the user. This requires advanced products, better networks, innovative technologies and related systems to keep up with the growing demands. However, the Cognitive Radio Networks face unconventional security challenges which are potential system degraders. One such attack, called Primary User Emulation Attack (PUEA), can affect all operations in a cognitive cycle and pollute the RF environment by sending fake primary user signals.This directly makes the Cognitive Radio Network enter a cascading state which affects spectrum sensing, spectrum analysis as well as the decision making process.A sturdy security scheme is important for preventing the broadcast of distorted information which weakens security during environment sensing. Therefore, to ensure secure access, an efficient selfish attack detection mechanism applying game theory is proposed.

This thesis work proposes an algorithm to detect such attacks in a Cognitive Radio Ad-Hoc Network using a non-cooperative game in which each node acts as a player of the game to find the malicious secondary user. The devised mechanism attains greater detection accuracy and improved system performance than the heuristic detection techniques used previously.Using simulations, the manner in which the selfish strategies of the players affect the system performance and how the detection of such attacks improves system performance parameters are discussed. The proposed algorithm shows a reasonably improved detection rate when compared to the detection technique built around the conventional COOPON technique. The system throughput exhibited an increase of around 20% and the Packet Delivery Ratio increased by 3% to 4% by the use of the proposed technique as compared to` the existing technique, which proves the efficiency of the proposed approach.