**INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI**
**SHORT ABSTRACT OF THESIS**

| | | |
|---|---|---|
| Name of the Student | : | Shivanshu Shrivastava |
| Roll Number | : | 10610214 |
| Programme of Study | : | Ph.D. |
| Thesis Title: | | Security Issues in Cognitive Radios |
| Name of Thesis Supervisor(s) | : | Dr A. Rajesh, Prof. P. K. Bora |
| Thesis Submitted to the Department/ Center | : | Department of Electronics and Electrical Engineering (EEE) |
| Date of completion of Thesis Viva-Voce Exam | : | 14/08/2017 |
| Key words for description of Thesis Work | : | Cognitive Radio, Cooperative Spectrum Sensing, Cooperative Communications, Security Issues |

**SHORT ABSTRACT**

Cognitive Radio (CR) based spectrum sensing has been identified as an effective measure to combat spectrum scarcity. Individual CR sensing may suffer performance deterioration due to deep fading. Cooperative spectrum sensing (CSS) has been realized as an effective means to counter this problem. CSS is severely affected if some secondary users (SUs) become malicious for their selfish intentions. These SUs are called malicious users (MUs). The objective of this research is suppressing the MUs. We aim at suppressing two types of malicious attacks, namely the spectrum sensing data falsification (SSDF) attacks and the primary user emulation attacks (PUEAs). The first part of the thesis investigates the SSDF attacks. The SSDF attacks are caused when the MUs report malicious data to mislead the CSS system. We propose two schemes to enhance the applicability of the Dixon's statistical outlier detection test in discarding single and multiple malicious data. Simulations reveal that the proposed schemes enhance the performance of the Dixon's test significantly. The proposed schemes are also successful in enhancing its applicability to multiple MU detection. These improvements are obtained without significant compromise on the complexity of the system. The second part of the thesis investigates SSDF attacks launched in collusion. We design a comprehensive categorization of the collusion attack scenarios. The PU is considered to impose a collision penalty on the SUs on suffering any interference. We derive bounds on the collision penalty to prevent attacks in each scenario. It is verified that the bounds on the collision penalty successfully suppress each of the attacks. The derived bounds are also successful in suppressing the reluctance of the PU in sharing its spectrum for the fear of interference. The Nash equilibrium showing the best strategy for the SUs to obtain the maximum gain from the PU spectrum is also derived. The third part of the thesis investigates the PUEAs in CSS. We aim at suppressing its effects on the SU throughput. We maximize the SU throughput in the presence of PUEAs. Maximizing the SU throughput results to increased interference to the PU. We formulate an optimization problem to maximize the SU throughput with a constraint on the interference to the PU. We propose an algorithm based on the Nelder Mead simplex method to solve this problem. Simulations reveal that the throughput of the SU in a CSS system facing PUEAs is maximized. The proposed algorithm is successful in bringing the performance of the PUEA affected CSS system close to an unaffected system in terms of the SU throughput.