Abstract

The rapid growth of wireless applications has increased the importance for efficient utilization of the scarce spectrum resources. Cognitive Radio Network (CRN) is an emerging technology which leads to solve these problems through dynamic utilization of the unused licensed spectrum. Spectrum sensing is a key function of cognitive radio to find the spectrum holes and Collaborative or cooperative sensing has been proposed to improve the ability. On the other hand, the flexibility in collaborative spectrum sensing opens way to a number of security vulnerabilities. While the set of security challenges in CRN are diverse, this work focus on one of these major threats called Spectrum Sensing Data Falsification (SSDF) attack or Byzantine
attack. In SSDF attack, the malicious member of the network sends false sensing reports to the cooperative sensing process and that can break down the normal activities of the whole CRN. This paper presents a novel trust calculation based mechanism that consists of two major steps: Trust value evaluation stage and malicious node detection stage to thwart SSDF attack in the cooperative sensing process of CRN.

References


**Index Terms**

Computer Science  
Networks

**Keywords**
Cognitive Radio Network; Spectrum Sensing Data Falsification (ssdf) Attack; Trust; Security Threats; Malicious Node Detection