Less sample-Cooperative Spectrum Sensing Against Large-scale Byzantine Attack in Cognitive Wireless Sensor Networks

Jun Wu¹, Mingyuan Dai¹, Xuyang Teng¹, Chao Wu¹, Meilin He¹, Haoyu Liang¹, Hao Chen², and Ye Jin¹

¹Hangzhou Dianzi University School of Communication Engineering
²Hubei Business College

March 25, 2024

Abstract

Cooperative spectrum sensing (CSS) has emerged as a promising strategy for identifying available spectrum resources by leveraging spatially distributed sensors in cognitive wireless sensor networks (CWSNs). Nevertheless, this open collaborative approach is susceptible to security threats posed by malicious sensors (MSs), specifically Byzantine attack, which can significantly undermine CSS accuracy. Moreover, in extensive CWSNs, the CSS process imposes substantial communication overhead on the reporting channel, thereby considerably diminishing cooperative efficiency. To tackle these challenges, this article introduces a refined CSS approach, termed weighted sequential detection (WSD). This method incorporates channel state information (CSI) to validate the global decision made by the fusion center (FC) and assess the trust value of sensors. The trust value based weight is assigned to sensing samples, which are then integrated into a sequential detection framework within a defined time window. This sequential approach prioritizes samples based on descending trust values. Numerical simulation results reveal that the proposed WSD outperforms conventional fusion rules in terms of error probability and sample size, even under varying degrees of Byzantine attack. This innovation signifies a substantial advancement in enhancing the reliability and efficiency of CSS.

Hosted file