Computers and Electrical Engineering 52 (2016) 240–252

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Enhancing the throughput of cognitive radio networks through malevolent presence

J. Christopher Clement*, D.S. Emmanuel**

School of Electronics Engineering, VIT University, Vellore-632007, India

ARTICLE INFO

Article history:
Received 11 July 2014
Revised 15 September 2015
Accepted 15 September 2015
Available online 9 October 2015

Keywords:
Cognitive radio
Throughput
Spectrum sensing
Sensing phase
Secondary user transmission phase
Malicious cognitive radio user

ABSTRACT

Enhancing the throughput of cognitive radio network in the presence of malicious cognitive radio user (MCRU) is addressed in this paper. We have considered the impact of MCRU on the sensing performance and achievable throughput of secondary network during two phases, namely, sensing phase (SP) and secondary user transmission phase (SUTP), respectively. This impact is mitigated by employing cognitive radio (CR) users equipped with multiple receiving antennas. We have performed diversity combining and have formulated the optimization problems with solutions during SP and SUTP. Moreover, the method of estimating the channel between MCRU and CR receiver is integrated into the solution. Simulation results show that this method achieves 89% detection and 3.5 bits/s/Hz of achievable throughput, while maximal ratio combining technique offers only 22% and 0.4 bits/s/Hz, respectively, when MCRU is active with ten times stronger power than the primary user.

1. Introduction

Cognitive Radio (CR) resolves spectrum under-utilization problem in today's wireless communication systems [1]. One of the intelligent modules of CR is spectrum sensing. Among many sensing algorithms reported so far, energy detection is the simplest, and relies not on the prior knowledge of primary users's (PU's) signal [2–4], and is employed in most of the reported works. Apart from energy detection, spectrum sensing is implemented through many other techniques namely, matched filter [5], cyclo-stationary based detection etc. [1,6,7].

However, performance of spectrum sensing is degraded, if MCRU exists in a cognitive radio network (CRN). These MCRUs exist, for two reasons. Firstly, there could be a detection deficiency due to failure in the hardware part and/or malfunctioning of software algorithmic part of CR. Secondly, one or more CR users intentionally do malpractice by transmitting a signal similar to that of PU's. In case of cooperative spectrum sensing, malicious activity is identified as reporting the combining center using bogus sensing data or sensing decision [8]. These MCRUs' intention is to take advantage of available spectrum - whenever the primary user (PU) is absent - by confusing or defeating other CR users' sensing algorithm [8,9].

So far, many contributions have been made towards spectrum sensing, when MCRU exists in a CRN. The first work on PU emulation attack is found in [10], where the MCRU occupies the vacant channels of the licensed user by transmitting the signal similar to that of the PU's so that access to the vacant channels by any other CR is denied.

* Corresponding author. Tel.: +91 4162243091; fax: +91 4162202411.
** Principal corresponding author.
E-mail addresses: christopher.clement@vit.ac.in (J.C. Clement), dsemmanuel@vit.ac.in (D.S. Emmanuel).

http://dx.doi.org/10.1016/j.compeleceng.2015.09.012
0045-7906/© 2015 Elsevier Ltd. All rights reserved.

In the work reported by authors in [11], MCRU is modeled as an unreliable user, which transmits signal of similar nature to that of PU's signal and defeats other CR users' sensing algorithm. To avoid that, authors have proposed a localization-based defense scheme, which estimates location of the transmitter by observing its signal characteristics. Using those estimates, it verifies whether a received signal is that of a PU's signal. An anti-primary-user-emulation attack is addressed in [12], where the secondary users (SUs) randomly choose channels to sense and avoid the attack of MCRU. The statistical nature of the signal of the attacker and his environment is assumed to be unknown to the SU. Further, to eliminate the problem of unknown environment, the technique of adversarial bandit problem is applied in the same work [12].

In as much as spectrum sensing is vital to a CRN, achievable throughput of a secondary network is also equally important [13]. A trade-off between sensing and throughput has been reported in [13], where sensing is performed periodically in each frame followed by SU's transmission. Authors in [14] have considered a number of MCRUs in a CRN, who report bogus sensing data to the combining center. Moreover, they have developed a scheme to detect them and minimize their interference during the data combining stage. But this work requires a priori knowledge of number of MCRUs that exist in a CRN. Hence the algorithm is not so successful in a situation, where MCRUs change their intention dynamically.

Authors in [15] have reported a sensing methodology for PU detection in the presence of MCRU by exploiting cooperation between CR users. But that work suffers from two severe drawbacks. First, it demands a dedicated reporting channel to exist between every CR user and combining center, notwithstanding the fact that demanding such a channel is irrational when addressing the problem of spectrum under-utilization. Secondly, fusion center's decision is based on the data sent from every CR user, which will include a few MCRUs, in a network. So, the received data itself is suspect. Finally, authors in [15], have dealt with sensing method, but they have not dealt with throughput of a secondary network which is paramount [13] and without it, the effort is inadequate. Notwithstanding these efforts, to improve the throughput of a CRN in a situation where MCRU is active, not much has been reported.

In this paper, we take cognizance of the existence of MCRU during both sensing phase (SP) and secondary user's transmission phase (SUTP), and present a method to alleviate its effect during both the phases. We employ CR user equipped with multiple receiving antennas [16] for diversity combining, so that we do not depend on cooperation between CR users, which demands a dedicated reporting channel. We have formulated the optimization problems with solution during SP and SUTP. Using this method, we have improved the sensing performance and achievable throughput of a secondary network, when MCRU coexists in a CRN. Moreover, by assuming the known channel-coefficients between PU and cognitive radio receiver (CRR), we have presented a scheme to estimate the channel between MCRU and CRR.

Rest of the paper is organized as follows. Section 2 presents the system model of the proposed work, followed by optimization problem during SP and channel estimation. Section 4 deals with achievable throughput and finding the optimal weights to increase the throughput. Simulation results are presented in Section 5 with discussions. Section 6 concludes the work.

2. System model

System model during SP and SUTP is shown in Figs. 1 and 2, respectively. We consider the existence of one PU, and one MCRU in a CRN. We assume that PU transmits its signal of power Z_p, and MCRU transmits a similar signal of power M_p. We consider that

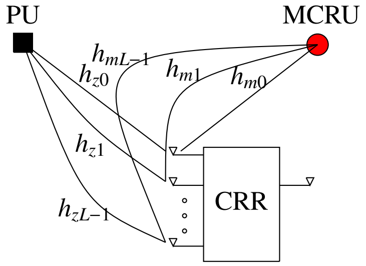

Fig. 1. System model during SP, *i.e.* $\beta = 0$, $\alpha = 1$ and $\delta = 1$.

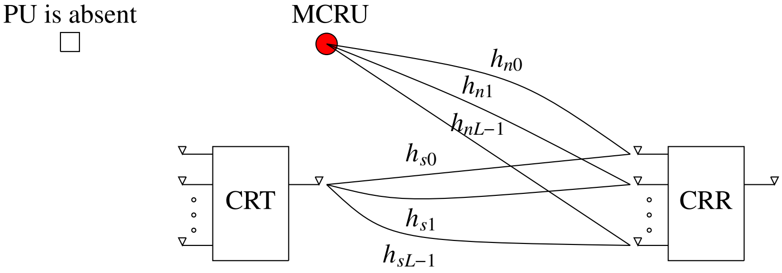

Fig. 2. System model during SUTP, *i.e.* $\alpha = 0$, $\delta = 0$, $\beta = 1$.