Physical Communication 17 (2015) 118–127

Contents lists available at ScienceDirect

Physical Communication

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

Full length article

# Outlier-aware cooperative spectrum sensing in cognitive radio networks[☆]

Gaurav Kapoor[a], Ketan Rajawat[b,*]

[a] *Defence Electronics Applications Laboratory, Defence Research and Development Organization, Dehradun 248001, UP, India*

[b] *Department of Electrical Engineering, Indian Institute of Technology, Kanpur 208016, UP, India*

ARTICLE INFO

*Article history:*
Received 22 October 2014
Received in revised form 18 August 2015
Accepted 21 August 2015
Available online 9 September 2015

*Keywords:*
Adaptive filters
Recursive least squares
Cooperative spectrum sensing

ABSTRACT

This paper considers the problem of cooperative spectrum sensing in cognitive radio networks (CRN). Communication in CRNs may be disrupted due to the presence of malicious secondary users (SU) or channel impairments such as shadowing. This paper proposes a spatio-frequency framework that can detect and track malicious users and anomalous measurements in CRNs. The joint problem of spectrum sensing and malicious user identification is posed as an optimization problem that aims to exploit the sparsity inherent to both, spectrum occupancy and malicious user occurrence. Proposed scheme obtains improved performance by utilizing node location information, and can handle missing or inaccurate location information, and noisy SU reports. A distributed block-coordinate descent-based algorithm is proposed that is shown to outperform the state-of-the-art PCA-based approach, and is flexible enough to defeat a variety of attacks encountered in SU networks. An online algorithm, that can handle incorporate multiple SU readings sequentially and adapt to time-varying channels, primary user, and malicious user activity, is also proposed and shown to be consistent. Simulation results demonstrate the efficacy of the proposed algorithms.

## 1. Introduction

With the advent of a large number of social networking and video streaming services, the current "smartphone" generation of applications demands high data rates and ubiquitous connectivity. The traditional approach of frequency licensing however, has resulted in an artificial spectrum scarcity, since the currently allocated spectrum is underutilized [1,2]. The emerging paradigm of secondary spectrum access holds the potential to ease this congestion by utilizing cognitive transmitters and dynamic spectrum access.

Cognitive radios (CR) are smart devices capable of (a) spectrum sensing, (b) opportunistic transmission on available bands, and (c) interference avoidance at the licensed or primary users (PU). CR-equipped secondary users (SU) are expected to not only enable higher data rates via opportunistic spectrum access, but also provide resilience and robustness to channel impairments, node failures, and malicious cyberattacks via cooperative spectrum sensing (CSS) [3]. Going beyond simply detecting band occupancy via energy detection or related methods, the CSS framework utilizes multi-node information-fusion and data-cleansing techniques for robust mapping of the spectrum state [4].

This paper considers the problem of robust CSS in CR networks in the presence of malicious SUs. Within a centralized CSS framework, where multiple sensors report to a

[☆] Part of this paper has been submitted to the *8th International Conference on Signal Processing and Communication Systems*, Gold Coast, Australia, December 2014.

[*] Corresponding author.
*E-mail addresses:* gkapoor.ddn@gmail.com (G. Kapoor), ketan@iitk.ac.in (K. Rajawat).

http://dx.doi.org/10.1016/j.phycom.2015.08.007
1874-4907/© 2015 Elsevier B.V. All rights reserved.

fusion center, even a single SU may disrupt the CR network operation by attacking the spectrum manager at the fusion center. In particular, the focus here is on physical layer attacks that manifest themselves as incorrect or anomalous CSS reports from the SUs to the fusion center. When the attack is initiated by an malicious SU itself, it is termed as a spectrum sensing data falsification (SSDF) attack [5]. On the other hand, an external agent may attack either via a PU emulation attack (PUEA), or by simply jamming or obstructing the received signal at an SU [6]. Finally, shadowing may result in an unintentional "attack", where the reports sent by the SU are correct but misleading.

Existing works have proposed the use of node location information for spectrum sensing and attack avoidance [7,8]. The present paper proposes a generalized robust CSS framework that not only identifies malicious users and spectrum opportunities, but also handles inaccurate or missing distance measurements and noisy SU reports. The proposed approach is flexible enough to be utilized for all types of attacks listed earlier, and exploits the sparsity inherent to both, outlier occurrences and spectrum occupancy. While the formulated optimization problem is non-convex, appropriate change of variables and relaxations are proposed so as to allow a distributed block-coordinate-descent (BCD)-based algorithm. Finally, an online algorithm is proposed that can sequentially incorporate the SU reports and track time-varying PU, SU, and malicious SU activity.

In summary, the following contributions are unique to this paper, and significantly different from the state-of-the-art CSS techniques.

1. A spatio-frequency approach to robust CSS is proposed that incorporates inaccurate location information and noisy spectrum sensing reports.
2. The proposed formulation exploits the sparsity inherent to both, outlier occurrence and spectrum occupancy, and can be approximately solved via a low complexity, distributed BCD routine.
3. The proposed online algorithm tracks slow time-variations in PU activity, SU locations, and malicious SU activity, and is shown to be consistent.

Before proceeding with the description of the system model, a brief review of the related work is provided. There exists a large amount of literature on robust CSS; see e.g., [9] and references therein. To begin with, attacks can be identified while making minimal assumptions about the PU activity or signal environment [10–12]. Another line of work considers the worst-case attack scenario [13–15], where the CR performance is often evaluated in terms of the number of colluding SUs that it can handle. In contrast, the focus here is on *joint* spectrum opportunity detection and malicious user identification by exploiting various aspects of PU activity and SU location. Note that in the absence of any such information, identifying malicious SUs is difficult, if not impossible.

Such extra information available at the SU has been considered for anomaly detection earlier. For instance, [16] utilizes location information for defeating PUEA, [17] detects malicious users by utilizing shadowing correlation in the received signals, and [14] utilizes spatial and temporal correlation between various kinds of information received at the fusion center. A unified approach presented in [9] combines similar ideas and performs joint spectrum sensing and outlier identification by exploiting network topology, node locations, and signal propagation characteristics. Further extensions of this idea are provided in [7], where a robust version of principal component analysis (PCA) is utilized to jointly estimate the PU powers and outlier locations.

In summary, the work in this paper generalizes those in [9,7], by incorporating inaccurate location measurements, noisy sensor reports, and time-varying PU and malicious user activity. As with earlier approaches, the work in this paper can always be combined with a trust-based reputation management system that can track and blacklist malicious SUs [18].

### 1.1. Outline of the paper

This paper is organized as follows: Section 2 describes the signal propagation and outlier contamination model; Section 3 formulates the optimization problem for robust CSS, and solves it via an approximate BCD-based algorithm; Section 4 generalizes the proposed algorithm to handle sequential data and time-varying PU activity; Section 5 provides simulation results and comparisons with existing robust CSS techniques, and finally Section 6 concludes the paper.

## 2. System model

Consider an SU network consisting of $N$ secondary CR nodes and a single PU as shown in Fig. 1. Time is divided into frames and the SUs attempt to opportunistically access vacant bands in every frame. It is assumed that the PU activity remains constant over the duration of a frame, and all SUs perform spectrum sensing at the start of each frame. Specifically, the SUs take RSS measurements over $F$ frequency subbands, and transmit soft readings to a fusion center. The SUs send the RSS reports on the network layer over a separate channel that does not interfere with sensing at other SUs. As with existing works on CSS, the SUs are also required to agree on a common protocol and parameters such as sensing periods and reporting times [3]. The fusion center then makes a collective decision regarding PU activity on each of the $F$ frequencies. Consistent with the measurement campaigns such as [1,2], the PU activity is assumed to be sparse over time and frequency.

### 2.0.1. Signal model

We assume a basic pathloss propagation model similar to that in [9,7]. The secondary users perform wideband sensing over frequency subbands $f \in \{1, 2, \ldots, F\}$. The power received by the $n$th SU in the $f$th frequency subband is given by

$$r_{n,f} = p_f + \alpha 10 \log_{10}(d_0/d_n) + v_{n,f} \quad \text{(dB)} \tag{1}$$

for all $n \in \{1, \ldots, N\}$ and $f \in \{1, \ldots, F\}$. Here, $p_f$ is the power transmitted by the PU in the $f$th frequency band measured at a reference distance of $d_0$ meters, $d_n$ is the distance between the $n$th SU and the PU, and $\alpha$ is the