Digital Signal Processing 74 (2018) 56–71

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

# On optimal sample checkpoint for energy efficient cooperative spectrum sensing

Avik Banerjee, Santi P. Maity *

*Department of Information Technology, Indian Institute of Engineering Science and Technology, Shibpur, Howrah, 711 103, India*

ARTICLE INFO

*Article history:*
Available online 18 December 2017

*Keywords:*
Cognitive radio
Cooperative spectrum sensing
Relay
Sample checkpoint
Energy savings
PUEA

ABSTRACT

Energy efficient and fast yet reliable spectrum sensing in cognitive radio networks (CRNs) is an important issue and is often met through the involvement of (optimal) multiple sensing nodes in collaboration known as cooperative spectrum sensing (CSS). However, due to severe fading, sometimes transmission of sensing samples over some reporting channels (R-channels) consume much energy but contribute very little on global sensing decision. To address the problem, this work explores the scope of using an optimal checkpoint to stop further transmission of sensing samples over the deeply faded R-channels. First an energy minimization problem under the constraints of detection and false alarm probabilities is developed in an amplify forward relay assisted CSS system in terms of optimal sample checkpoint, the number of essential sensing/relay nodes and relay power gain. The problem is further extended in presence of primary user emulation attack (PUEA). Simulation results show that a performance gain ∼77.17% and ∼71.25% in energy consumption can be achieved for the proposed approach as compared to the existing two works at $P_d = 0.9$ and $P_f = 0.05$.



## 1. Introduction

Radio frequency spectrum is becoming a limited natural resource day by day due to the meteoric rise in the use of wireless devices with bandwidth intensive applications such as interactive and multimedia services. In the static spectrum allocation mode, the available frequency spectra are divided into different sub-bands and each one (or a set) is assigned exclusively to provide specific service. The user of this specific sub-bands or service is then called as licensed users or primary users (PUs). However, it is observed that static frequency allocation leads to spectrum under-utilization scenario as mentioned in the some recent studies [1,2], reports published by Federal Communications Commission (FCC) [3] in USA and other regulatory bodies e.g. Office of Communications (OFCOM) [4] in UK. Cognitive Radio (CR) emerges as a potential solution to address the problem of spectrum under-utilization and spectrum scarcity by providing the means of an opportunistic transmission for secondary users (SUs) (also called cognitive users) over the licensed band assigned to the PUs [5].

Among the various research issues in CR system design, spectrum sensing (SS) is the most crucial one as it can reliably detect the unused spectrum by monitoring PU's transmission over the frequency band and thereby offers the scope of opportunistic transmissions for SUs. Fast yet reliable SS plays the pivotal role in CR system design. Several SS techniques, namely matched filtering (MF) [6], cyclostationary feature detection (CFD) [7], generalized likelihood ratio test (GLRT) [8,9], energy detection (ED) [10] etc. are reported. Among all these techniques ED is found to be the simplest and the widely used one. The method of ED is also reported to be the optimal and blind for detecting the zero mean constellation signals when the sensing is done without prior knowledge of the PU signal [11]. However, its performance degrades at low signal-to-noise ratio (SNR) and under noise uncertainty [12]. Performance of SS is mainly quantified through (i) probability of detection ($P_{det}$), which refers to the probability of finding PU transmission over a specific frequency band on spatio-temporal basis and (ii) probability of false alarm ($P_{fa}$), which represents the probability of deciding in favor of PU's transmission over a spectrum, although that particular spectrum remains idle [13]. Reliable SS is ensured through high $P_{det}$ and low $P_{fa}$ values, which can be met through longer sensing duration (larger number of samples) and/or the involvement of more number of sensing nodes. The latter one is called cooperative SS (CSS) [14,15] where sensing nodes (often SUs do sensing) exchange their sensing information among themselves or send the same to the Fusion Center (FC) to develop a global decision of spectrum access.

* Corresponding author.
*E-mail addresses:* b_avik.rs2015@it.iiests.ac.in (A. Banerjee), santipmaity@it.iiests.ac.in (S.P. Maity).

https://doi.org/10.1016/j.dsp.2017.12.003
1051-2004/

In CSS, increase in the number of SUs or relays (often used as sensing nodes) enhances the sensing performance [16] but at the expense of higher energy consumption [17]. This is because as more number of sensing nodes are involved, more number of samples are transmitted to the FC. Thus there always exists a trade-off between the energy consumption and detection reliability. Again energy consumption in CSS mostly depends on the number of relays (sensing nodes) involved, the number of samples of the PU signal transmitted to the FC (sensing duration) and relay amplifying gain on the reporting channels (R-channels) formed between the sensing nodes and the FC [18]. It is worth mentioning that when the distances from PU to relays and relays to FC are quite large, the energy consumption for sample transmission is relatively much larger than the same required for the operation of the sensing circuits [18]. Thus designing an energy efficient (minimization) CSS is a major challenge while meeting different sensing reliability constraints [19,20]. Furthermore, SUs being battery driven, transmission power minimization also becomes essential in this scenario.

Cooperation in SS, from the large number of SUs involved, is vulnerable to various security related issues. One such pernicious operation in SS is spectrum sensing data falsification (SSDF) attack [25,26] where a malicious collaborator flips its local sensing data with varying flip rates, thereby misleading the FC by sending false sensing information. SSDF is also known Byzantine attack, and a state-of-the art works are reported in [29] with a tutorial discussion on distributed inference from Byzantine data. A comprehensive survey on the recent advances in SSDF and the defensive schemes for CSS in CR networks are reported in [30]. The study also analyzed the spear-and-shield relation between SSDF and its defensive mechanism from an interactive game-theory approach. The authors in [31] studied the issue of robust CSS with a crowd of low-end personal spectrum sensors. Closed-form expressions of global false alarm and global detection probabilities are reported in the work. A new malicious user detection method using two proposed conditional frequency check (CFC) statistics was developed in [32] under the Markovian model against SSDF attack. In [33], an overview of applying various Kernel based learning (KBL) methods to statistical signal processing-related open issues in CR networks are presented. The studies demonstrate that KBL method provides a powerful set of tools for CR networks by enabling rigorous formulation and effective solutions to both long-standing and emerging design problems.

CSS also face another security threat when some malicious users, for their own selfish interest, send fake signals to the FC. This results in performance degradation of SS at FC. Malicious users may generate high energy values in absence of PU and thus enhance the probability of false alarm ($P_f$) that leads to decrease in bandwidth available for the CR networks. They may also send low energy values when PU is present. This causes interference of fake signals on sensing process and thereby decreases the detection probability of PU. However, all these security threats affect either the local sensing procedure at individual SU or SS decision at FC. Among various attacks available in the existing literature, primary user emulation attack (PUEA) [27,28] is more vulnerable and has a unique security challenge nowadays. PUEA impersonates PU by sending its own jamming signal to the FC, thus compromises the sensing procedure and thereby misleads other SUs to access vacant frequency bands. To mislead the global sensing decision through SSDF operation, a good number of SUs need participation in the local falsification process, otherwise their impact on the global decision process in FC may not be effective enough. On the other hand, sensing process of all the nodes is expected to be affected in PUEA operation, thus found to be more severe than SSDF. This relative severity of PUEA over SSDF and the challenge of meeting the desired reliability in CSS with energy minimization makes it an important research issue and is explored in this work.

The rest of the paper is organized as follows: Section 2 makes a literature review on ED based SS and threat of PUEA. Section 3 presents the proposed system model while the energy consumption and its savings are discussed in Section 4. In Section 5, the similar analysis of Section 4, in presence of PUEA, is shown while its relevant energy consumption and savings are calculated in Section 6. Extensive simulation results along with the detailed discussions are presented in Section 7. Finally, the paper is concluded in Section 8.

## 2. Literature review: ED based SS and PUEA operation

This section first makes a brief literature review on ED based SS and PUEA operation in CRN. The merits and the limitations of the existing works are discussed here followed by the scope and contributions of the present work in the next sub-section.

Bhowmick et al. [21] found both the optimal sensing time and improved energy detector (IED) parameter that maximize the energy efficiency while maintaining a desired detection probability of PU. In [22], an optimization problem is formulated for obtaining sensing duration to maximize the secondary achievable throughput under the constraint of meeting a target interference limit to the PU. The study showed that using ED scheme there exists an optimal sensing time that achieves the best trade off. The authors in [23] found an optimal number of SUs participating in CSS for minimizing the total error probability. The study also developed an optimal sensing duration that maximizes the throughput of the secondary network. However, closed form solution of the optimal sensing parameter is not reported in the works [22,23]. A censored truncated sequential approach was proposed in [24] based on the combination of censoring and sequential sensing policies. The aim of the study is to minimize the maximum average energy consumption for each SU under the constraints of meeting a global probability of false alarm and detection for both AND and OR fusion rules.

Some notable works on PUEA include the signal activity pattern [34], weighted combining scheme [27], identifying the kind of emulation operation followed by its cancellation [35], etc. In [28], the authors developed an analytical approach based on Fenton's approximation and Markov inequality for obtaining a lower bound on the probability of a successful PUEA by a set of malicious users. In [36], the effect of PUEA in CR system with the correlated signals and spatially-correlated shadow fading is mitigated using the maximum–minimum eigenvalue (MME) detection based method. Collaborative sensing by few SUs with less spatial correlation was considered in their work and further MME value detection based approach was adopted to verify PU's presence. In [37], the authors considered multiple smart malicious users and explored how the performance of CSS is compromised in presence of multiple PUEAs in CR networks. Chen et al. [27] considered a binary hypothesis in CSS that includes the presence of PUEA in both the cases, i.e. during PU's presence as well as in absence. The authors also developed an optimization framework for the weighted combining in CSS at FC with an objective to maximize the PU detection probability under the constraint of meeting a target false alarm rate.

In [38], the throughput of SU is studied in presence of PUEA, where SUs access the spectrum in hybrid mode, i.e., either in overlay mode or in underlay mode. The study developed an optimal sensing time for which the secondary throughput becomes the maximum and the latter is shown to degrade as the attacker's presence probability as well as attack strength increases. Pourgharehkhan et al. [39] proposed a secured CSS scheme in presence of a PUEA network where the presence or absence of the PU and/or PUEA is modeled as a multiple hypotheses problem. FC