Reliable Cooperative Sensing in Cognitive Networks
(Invited Paper)

Mai Abdelhakim, Jian Ren, and Tongtong Li

Department of Electrical & Computer Engineering,
Michigan State University, East Lansing, MI 48824, USA
{abdelhak,renjian,tongli}@egr.msu.edu

Abstract. In this paper, we consider reliable cooperative spectrum sensing in cognitive networks under the Spectrum Sensing Data Falsification (SSDF) attacks. One effective method to mitigate the SSDF attacks is the $q$-out-of-$m$ fusion scheme, where the final decision is based on $q$ sensing reports from $m$ polled users. In this paper, first, we derive the asymptotic behavior of the fusion scheme as the network size increases. It is found that the false alarm rate decreases exponentially as the network size increases, even if the percentage of malicious users remains fixed. Second, we propose an iterative approach to obtain the best scheme parameters that minimizes the false alarm rate and enforces the miss detection constraint. Third, we discuss different attack scenarios and propose a malicious user detection method to further improve the performance. It is shown that by exploiting the malicious user detection scheme, the system performance is improved significantly under various attacks.

Keywords: cognitive networks, cooperative sensing, malicious attack, data fusion.

1 Introduction

Spectrum is the most precious resource for communication networks. Due to the wide range of existing and emerging applications, spectrum scarcity has become an urgent problem. Meanwhile, according to the Federal Communication Commission FCC, the utilization of the licensed spectrum bands in space and time has shown to be between 15% and 85% [1]. The spectrum scarcity and underutilization issues have motivated the development of a new paradigm based on dynamic spectrum access and known as cognitive networks [2]. In cognitive networks the spectrum is used opportunistically by secondary users when it is not utilized by the licensed (primary) users. To do this, the spectrum is sensed and the spectrum holes are identified prior to transmissions.

In order to improve the accuracy of the spectrum sensing process, cooperative spectrum sensing was proposed [3], where multiple cognitive radios share their

* Corresponding author.
sensing information with the fusion center, which makes the final decision accordingly. However, the reliability of the cooperative sensing is threatened by the presence of malicious attacks. One serious threat is the Spectrum Sensing Data Falsification attack (SSDF) [4]. In the SSDF attack, some authenticated users are compromised and intentionally report false sensing information. This would lead to a low spectrum utilization and/or high interference to the primary system. In order to mitigate the SSDF attack several approaches has been proposed in [5–9]. In [5–7], the sensing reports (energy levels) are weighted according to a certain weighting functions, and the weights are updated based on the radios instantaneous behavior.

In [8,9], we proposed a simple, yet effective, hard fusion rule based on the q-out-of-m scheme. In the q-out-of-m scheme, the final decision is based on q sensing reports out of m polled users. In [9], we presented a linear approach to obtain the scheme parameters, which significantly reduces the computational complexity of the optimal exhaustive search. In this paper, first, the asymptotic performance of the linear approach is analyzed and the effect of the network size on the detection accuracy is derived. It is found that the false alarm rate decreases exponentially as the network size increases, even if the percentage of malicious users is unchanged. Second, we extend our work by proposing a modified linear approach that provides near-optimal solution. As opposed to the direct-linear approach, the modified approach enforces the miss detection constraint through an iterative method. The convergence of the modified linear approach has shown to be fast. Third, we present different attack strategies and propose a scheme to detect malicious users. With malicious node detection, the system performance is improved significantly under various attacks. Several simulation examples are carried out to demonstrate the effectiveness of the proposed schemes.

2 Problem Formulation

We assume that the network consists of n active users including k malicious users. We refer to n as the network size. We first assume that malicious users can detect the primary signal with no errors and always report false information. More general attack strategies will be discussed in Section 4. The percentage of malicious users k/n is denoted by $\alpha$. Each node in the network performs spectrum sensing and reports its one bit hard decision result to a central node (fusion center) through a control channel. The control channel is assumed to be error free. The sensing result is either ‘1’ which means that the primary user is present, or ‘0’ which means that the band is not used by the primary. All users experience independent and identically distributed (i.i.d) fading with the same average signal to noise ratio (SNR), such that each user has a probability of false alarm $P_f$, and a probability of detection $P_d$.

The fusion center is then responsible for making the final decision based on the received sensing reports from all users. $\alpha$ is assumed to be known, or can be estimated, at the fusion center. The q-out-of-m scheme is an effective hard fusion rule that can mitigate the SSDF attacks, as will be illustrated in the next subsection.