Computers and Electrical Engineering 52 (2016) 284–292

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Efficient elimination of erroneous nodes in cooperative sensing for cognitive radio networks☆

Sesham Srinu *, Amit Kumar Mishra

Department of Electrical Engineering, University of Cape Town, Cape Town, South Africa

ARTICLE INFO

Keywords:
Cognitive radio networks
Cooperative spectrum sensing
Random cognitive users
Shapiro–Wilk test
Extended generalized extreme studentized deviate
Erroneous cognitive user

ABSTRACT

Cooperative spectrum sensing is a process of achieving spatial diversity gain to make global decision for cognitive radio networks. However, accuracy of global decision effects owing to the presence of malicious users/nodes during cooperative sensing. In this work, an extended generalized extreme studentized deviate (EGESD) method is proposed to eliminate malicious nodes such as random nodes and selfish nodes in the network. The random nodes are carried off based on sample covariance of each node decisions on different frames. Then, the algorithm checks the normality of updated soft data using Shapiro–Wilk test and estimates the expected number of malicious users in cooperative sensing. These are the two essential input parameters required for classical GESD test to eliminate significant selfish nodes accurately. Simulation results reveal that the proposed algorithm can eliminate both random and frequent spectrum sensing data falsification (SSDF) attacks in cooperative sensing and outperforms the existing algorithms.

1. Introduction

In cognitive radio networks (CRN), cooperative spectrum sensing (CSS) is an effective technique to combat the multipath fading, shadowing and the receiver uncertainty present in the channel [1,2]. Cooperative sensing is a way of getting spatial diversity gain by receiving signal from different cognitive users in the vicinity of a fusion center (central node). A wide range of fusion techniques have been proposed to achieve spatial diversity gain. All these techniques can be classified into either soft decision (EGC and WGC) or hard decision (AND, OR, and MOST) based fusion methods. The classification is based on the type of data that the central node received from the cooperative cognitive users. Each fusion method has its own pros and cons. In practice, the central node does not have any prior information about signal to noise ratio (SNR) to generate the weights. The soft decision method named as equal gain combining (EGC) assigns equal weight to all nodes to generate a global decision. However, it is an unconventional method and degrades the sensing reliability. In weighted gain combining (WGC), different sensing techniques have been reported to estimate the weight for each cognitive radio (CR) user. Most of these methods require the signal characteristics a priori. In order to avoid this, differential evolution (DE) optimization method has been considered to estimate the weights for each CR user in [3–5]. Moreover, evolutionary algorithms are better to consider in the process because of their flexibility to generate proper weights with multiple constraints such as link budget, false alarm probability, belief value of each node, and distance of CR from primary user transmitter.

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Sabu Thampi.

* Corresponding author.
E-mail addresses: seshamsrinu83@gmail.com (S. Srinu), akmishra@ieee.org (A.K. Mishra).

http://dx.doi.org/10.1016/j.compeleceng.2015.05.004
0045-7906/

In practice, most of the current schemes assume that secondary/cognitive users send the correct measurement/decision to the fusion center (FC) to make the global decision [1,6]. This opens a window for malicious users to use the vacant spectrum selfishly. The malicious cognitive user (MCR) can send false information and mislead the spectrum sensing machine leading to collision or inefficient spectrum usage. In particular, the performance/reliability of the CSS degrades as the number of malicious users increases. There are two types of malicious attacks in CSS [7,8]. The first one is the incumbent emulation attack (IEA), where some malicious users know the characteristics of the primary signal and transmit a signal with similar characteristics so that other secondary users would believe that a primary user is present [9–11]. The second one is the spectrum sensing data falsification attack (SSDF) also termed as Byzantine attack, where malicious users send false sensing information intentionally to a central node [12,13]. The data falsification attacks associated with the malicious/erroneous users exist in the network is mainly due to malfunction of sensing hardware or/and presence of selfish nodes that intend to use the radio spectrum selfishly.

To defend the basic SSDF attacks, the generalized extreme studentized deviate (GESD) test is the prominent method for detection and elimination of multiple selfish users in a cognitive radio network [14,2]. It has been also reported that, if the model follow a normal distribution, GESD test is the best method for multiple erroneous cognitive user elimination [14,15]. To detect multiple MCR user, the GESD method requires two essential input parameters a priori, those are, (1) distribution of the soft decision data (since the test is more efficient for normally distributed data), (2) estimation of expected number of malicious user in the data. A modified largest gap method to estimate the exact number of malicious users or upper limit of outliers in the cooperative sensing under attack is presented in [12]. However, GESD test, modified largest gap method, and Tietjen-Moore tests can not eliminate the random cognitive nodes in the cooperation.

In the current work, we propose an algorithm named as *extended generalized extreme studentized deviate* test (EGESD) which can eliminate probable SSDF attacks that comes from failure of sensing hardware and the presence of selfish nodes in the CRNs. To achieve this, we studied and modeled the three possible cases of soft decision data that a hardware failure node can send, those are, the random data that follow uniform distribution, random data that follow Gaussian distribution (also occurs due to strong fading environment), and the data that is random between 'always high or low'. The failure nodes are termed as random cognitive radios (RCR). In the case of selfish nodes, we consider two well-known basic attacks termed as 'always Yes/No' in the analysis. The proposed algorithm can estimate two essential input parameters required for efficient elimination of erroneous nodes in the network. Hard and soft decision fusion methods are considered to analyze the performance of cooperative sensing.

Rest of this paper is organized as follows. Cooperative sensing algorithm using DE and EGESD test is presented in Section 2. Simulation results are given in Section 3. Finally, our conclusions are drawn in Section 4.

2. CSS algorithm with elimination of erroneous nodes

2.1. CSS based on DE

Assuming that there are M nodes in the cooperation that contains both genuine and malicious nodes. In addition, received signal of all nodes are statistically independent. Then, the composite hypothesis test can be written as

$$H_0 : r_m(n) = w_m(n),\ m = 0, 1, 2\ \ldots' \ (M-1)$$
$$H_1 : r_m(n) = h_m s_m(n) + w_m(n),\ n = 0, 1\ \ldots' \ (N-1)$$

where H_0 and H_1 denote the null and alternative hypothesis. The null hypothesis states that there is only noise present in a frequency band to be scanned. The alternative hypothesis states that there is a primary/incumbent user signal present along with the noise in the frequency band to be scanned. The received signal sequence by the mth secondary user is denoted as $r_m(n)$, whereas $s_m(n)$ is the primary user's transmitted signal sequence, $w_m(n)$ is the additive white Gaussian noise (AWGN) observed by mth node, and h_m is the channel gain. It is assumed that the channel is slowly varying such that the channel frequency response or channel gain remains constant during the sensing duration.

In this work, both hard and soft decision logics are considered. In case of WGC fusion, the weight vector is evaluated using DE algorithm [16]. Mathematically, the problem can be expressed as

$$\max \sum_{m=1}^{M} \psi_m \Theta_m, \quad s.t \ \sum_{m=1}^{M} \Theta_m = 1, \quad 0 < \Theta_m < 1. \tag{1}$$

In DE algorithm, the sum of the product (soft decision (ψ_m) and its corresponding weight (Θ_m)) of all cooperative nodes are considered as the objective function. The notation ψ_m represents the energy measurement of the mth node, given as $\psi_m = \sum_{n=0}^{N-1} |r[n]|^2$.

Since the DE optimization algorithm is the development of Genetic algorithm, the proposed method generates an optimal weight vector based on the three important steps: mutation, crossover, and selection. Let it be, ($\mathbf{\Theta_{opt}} = [\Theta_{opt(1)}, \Theta_{opt(2)} \ldots' \Theta_{opt(M)}]$). Then, the cooperative detection probability with the optimal weights can be computed as [16]

$$Q_{d-wgc(opt)} = \sum_{m=1}^{M} \psi_m \Theta_{opt(m)} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_e, \tag{2}$$

where ψ_m is the soft measurement of mth node and λ_e is the threshold value.