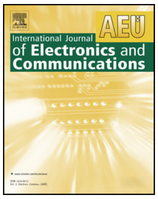
Int. J. Electron. Commun. (AEÜ) 94 (2018) 359–366

Contents lists available at ScienceDirect

Int. J. Electron. Commun. (AEÜ)

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



Regular paper

Distributed cooperative spectrum sensing based on reinforcement learning in cognitive radio networks

Mengbo Zhang[a,b], Lunwen Wang[a,b,*], Yanqing Feng[a,b]

[a] State Key Laboratory of Pulsed Power Laser Technology, Anhui 230037, China
[b] Electronic Countermeasure Institute, National University of Defense Technology, Anhui 230037, China

ARTICLE INFO

Keywords:
Cognitive radio
Spectrum sensing
Reinforcement learning
Consensus fusion

ABSTRACT

Spectrum sensing is an initial task for the successful operation of cognitive radio networks (CRN). During cooperative spectrum sensing, malicious secondary user (SU) may report false sensing data which would degrade the final aggregated sensing outcome. In this paper, we propose a distributed cooperative spectrum sensing (CSS) method based on reinforcement learning (RL) to remove data fusion between users with different reputations in CRN. This method regards each SU as an agent, which is selected from the adjacent nodes of CRN participating in CSS. The reputation value is used as reward to ensure that the agent tends to merge with high reputation nodes. The conformance fusion is adopted to promote consensus of the whole network, while it's also compared with the decision threshold to complete CSS. Simulation results show that the proposed method can identify malicious users effectively. As a result, the whole CRN based on RL is more intelligent and stable.

1. Introduction

Cognitive radio (CR) is a form of wireless communication where a transceiver can intelligently determine which communication channels are being used, thus it could instantly move into vacant channels while avoiding occupied ones [1,2]. In CR communication, priority of the authorized band is often given to the primary user (PU). The secondary users (SUs) can coexist with the PU on the same spectrum bands to improve the spectrum efficiency under the condition that the interference of SUs on PUs is regulated [3]. Reliable spectrum sensing is essential to enable the normal operation of a cognitive sensor network [4,5]. In other words, the spectrum sensing is an important component of CR, which has drawn attention from many researchers and given rise to many contributions dealing with it. Hence, accurate spectrum sensing algorithms are required to continuously monitor the radio spectrum.

During the past few years, researches on spectrum sensing have been widely carried out. The most commonly conventional methods of spectrum sensing include matched filtering detection [6], energy detection [7] and cyclostationarity detection [8]. Compared with single node spectrum sensing, the cooperative spectrum sensing (CSS) is prevailing, due to its capability of mitigating channel fading, shadowing and hiding node problems by taking advantage of spatial diversity [9,10]. In [11], the authors utilize the properties of Wishart matrix to decompose the covariance matrix, and a spectrum sensing method based on the maximum eigenvalue of covariance matrix is proposed to reduce the computational complexity. In [12], the authors use a double threshold energy detection method to select the local SU with the best SNR, and consequently complete the CSS. Without taking into account the interference from malicious SUs, the above CSS methods assume that all SUs are involved in collaboration. However, one critical challenge in above CSS methods is the uncertainty of the quality of sensing data that may be corrupted by unreliable, untrustworthy, or even malicious spectrum sensors [13]. Those SU nodes would refuse to collaboration, and sometimes they may even destroy the collaboration procedure.

The Byzantine attack in CSS, also known as the spectrum sensing data falsification (SSDF) attack in the literature, is one of the key adversaries to the success of cognitive radio networks (CRN) [14]. Generally, for a CRN with malicious users, information exchange between neighbor nodes is usually used to reduce the interference among malicious users to the entire perception network [15]. To design cooperative algorithms for CRN, the cooperative game theory that deals with the interaction between groups of cooperating rational players to improve their overall outcome, is a widely used mathematical tool [16]. In particular, coalition game theory as a branch of the cooperative game theory, where rational player organizes themselves into coalitions to improve their performance, has been utilized by many researchers to

[*] Corresponding author at: Electronic Countermeasure Institute, National University of Defense Technology, Anhui 230037, China
E-mail address: 664803893@qq.com (L. Wang).

https://doi.org/10.1016/j.aeue.2018.07.029
Received 6 March 2018; Accepted 25 July 2018

study CRN and wireless networks in general [17–19]. An excellent survey of coalition formation in CRN using game theory is presented in [20,21], where various research challenges in coalition formation in CRN are described. However, all above-mentioned coalition game theory has the drawback that the prior knowledge on SU locations and historical information are needed. The neighboring nodes of SUs get the corresponding dynamic trust value according to their behavior, which restricts the impact of the malicious behavior on the premise to ensure information interaction of normal nodes. In [22–24], the authors define the reputation value as the similarity between SU decision result and neighbor user decision. When the reputation value of SU is below threshold, it is considered as a malicious user which doesn't participate in spectrum sensing. However, the determination of threshold has high computational complexity. In [25,26], the authors use reinforcement learning (RL) to identify malicious users in CRN based on RL, which shows that the CSS network is intelligent. They only improve CRN performance by selecting reliable SU, and do not involve spectrum sensing. Considered the communication channel in real application is often complex and changeable, the forward-looking cognitive ability is further demanded for CR in addition to the basic cognitive ability. This motivates us to propose a new CSS method to meet all above requirements.

A distributed CSS method based on RL is proposed in our study to solve the problem of data fusion between users with different reputation in cognitive wireless networks. The proposed method regards each SU as an agent and uses RL algorithm to select a cooperative user from adjacent nodes for consensus fusion. The reputation value is used as reward to ensure that agent tends to merge with high reputation nodes. This method reduces the interference of malicious users to the perceived network and improves the spectrum sensing performance of the whole network. The main contributions of the proposed algorithm including two aspects: (1) selecting the honest SU for CSS based on the RL algorithm, (2) improving the performance of CRN to make it more intelligent and stable.

The rest of the paper is organized as follows. In Section 2, the system model of a distributed CRN topology is presented. In Section 3 we propose a distributed CSS method based on RL. In Section 4, simulation experiment and result analysis are conducted to evaluate the performance of the proposed method in various scenarios. Finally conclusions are summarized in Section 5.

2. System model

The CRN includes several SUs and a PU as shown in Fig. 1. Generally, malicious users don't have the prior information of licensed channels' real occupation state. Unlike the honest data transmission between honest users, the connection between malicious users modifies data transmission. The malicious users aim to send a false sensing report and destroy the functionality of cooperative spectrum sensing, so that the system cannot trust the aggregated sensing results.

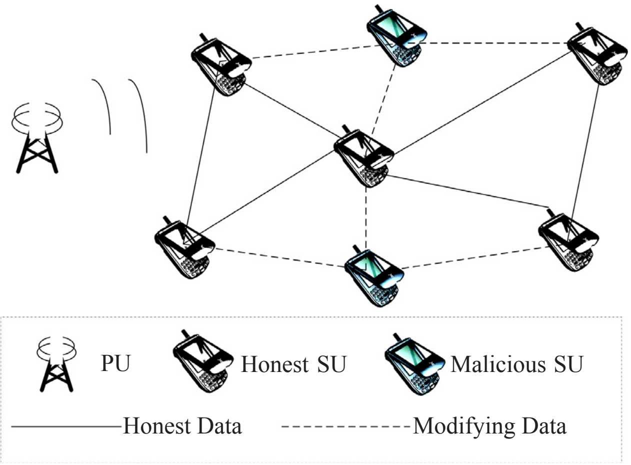


Fig. 1. Distributed CRN topology.

Nevertheless, some extra information, such as the fusion rule, defense strategies, and current sensing results of other malicious users, will improve flexibility of attack strategies and enhance attack intensity [14]. Especially, through communication between malicious users, the malicious user can collude with its peers. In addition, the extra information not only improves the attack efficiency but also increases the complexity of the attack. In our system model, we assume that malicious users adopt the most common SSDF attacks and the current sensing results of other malicious users are given. In [24], the authors define four types of SSDF attacks to test the resiliency of the proposed data aggregation scheme.

1. "always yes" attack: malicious SUs always report the presence of PUs ignoring their real sensing results.
2. "always no" attack: malicious SUs always report the absence of PUs on the channel ignoring the real detection results.
3. "always false" attack: malicious SUs always report the opposite of their sensed channel occupancy.
4. "always random " attack: malicious SUs report true/false channel occupancy randomly.

For convenience of analysis, the topology of CRN and the positions of attackers have the following characteristics:

1. The location of each SU and PU is randomly distributed in the network. During spectrum sensing, the topology of CRN does not change, which means that the relative position of PU and SUs remains stable.
2. Compared to the distance of PU, the distance between each SU is short, so that the transmission loss of its wireless connection could be ignored.
3. Each SU can perform local spectrum sensing independently. The result of spectrum sensing can be exchanged with neighbor SU through wireless connection.

The main issue of spectrum sensing is to determine whether there is a primary user signal in the channel, which can be regarded as the two element hypotheses testing problem. The two assumptions are as follows [27]:

$$\begin{cases} H_0\colon y_i(t) = n_i(t) \\ H_1\colon y_i(t) = h_i s_i(t) + n_i(t) \end{cases} \tag{1}$$

where hypotheses H_0 and H_1 indicate the presence and absence of PU signal, respectively. $y_i(t)$ and $s_i(t)$ represent the received and transmitted signals of the i - th SU. $n_i(t)$ is the additive Gauss white noise (AGWN) with a mean value of 0 and a variance of σ_n^2. The impulse response of channel i is h_i. The normalized energy detection results can be expressed as:

$$x_i = \frac{1}{m\sigma_n^2}\sum_{k=1}^{m} y_i(k)^2 = \begin{cases} \frac{1}{m\sigma_n^2}\sum\limits_{k=1}^{m} n_i(t)^2, & H_0 \\ \frac{1}{m\sigma_n^2}\sum\limits_{k=1}^{m} (h_i s_i(t) + n_i(t))^2, & H_1 \end{cases} \tag{2}$$

where $m = \tau f_s$ represents the number of sampling points. f_s represents the sampling rate and τ represents the perception time. When m is large enough, it is easy to obtain the distribution of x_i, which satisfies the chi square distribution as:

$$x_i \sim \begin{cases} \chi_m^2, & H_0 \\ \chi_m^2(\gamma_i), & H_1 \end{cases} \tag{3}$$