Available online at www.sciencedirect.com

ScienceDirect

Cognitive Systems Research 52 (2018) 21–26

Cognitive Systems RESEARCH

www.elsevier.com/locate/cogsys

Localization algorithm of energy efficient radio spectrum sensing in cognitive internet of things radio networks

Wu Yubao

Nanjing Forest Police College, Department of Information Technology, Nanjing, Jiangsu 210023, China

Received 8 May 2018; received in revised form 2 June 2018; accepted 5 June 2018

Abstract

Spectrum sensing is a key problem of implementing cognitive radio (CR). Some malicious users falsify data, which reduces the performance of spectrum sensing. To this end, trustful cluster-based cooperative compressed spectrum sensing (TCBCSS) algorithm is proposed orienting to malicious user environment. Maximum likelihood (ML) is firstly used for estimating the distance from the cluster to the primary user, and the distance is compared with the preset threshold value so as to seek for the trustful cluster. Then, the channel condition is detected using the compressed spectrum sensing algorithm according to the information provided by the trustful cluster. The simulation result indicates that the proposed TCBCSS algorithm could cope with the malicious user environment effectively, detect the malicious user accurately, and maintain high spectrum detection rate.

Keywords: Cognitive radio; Spectrum sensing; Wireless network; Perceptual location; Trustful cluster

1. Introduction

As wireless spectrum resource is scare increasingly, cognitive radio (CR) technology receives wide concern. Spectrum sensing is one of the most key technologies in CR network. If the spectrum is not sensed correctly, the performance of primary system is damaged. Each secondary user (SU) senses the spectrum periodically, If the channel is not used by the primary user (PU), SU uses such channel. In addition, when PU starts to use the channel for transmitting information, SU must release the channel. At present, many researchers pay close attention to spectrum sensing technology. Author proposes estimating time-space detection performance in the spectrum sensing process (Chan, Zhang, & Uhrich, 2015). In Literature (Malarkodi, Arunkumar, & Venkataraman, 2013), the author considers the sleep mode of CR, and thus proposes the minimal energy consumption scheme in the spectrum sensing process. In addition, to enhance the detection performance, Literature (Stephygraph & Arunkumar, 2016) proposes related detection algorithm. However, shadow fading and multipath impact reduce the sensing performance of users. One of effective methods of solving the problem is that multiple SU carry out cooperative sensing. At present, cooperative sensing has been widely studied (Pan, Chen, & Feng, 2013; Yijiu Zhao, Hen, & Liu, 2017). However, the attack from the malicious users is not considered in these schemes. Once encountering the malicious users, the detection performance of the spectrum declines sharply.

A trustful cluster-based compressed spectrum sensing algorithm that defends the attack of SSDF and PUEA effectively is proposed in this paper. Through TCBCSS algorithm, the raw data sent to the fusion center is reduced and the accuracy of detecting the malicious users is improved. The SU is made cluster classification, and then

E-mail address: yangqiqiyqqyqq@163.com

https://doi.org/10.1016/j.cogsys.2018.06.003
1389-0417/© 2018 Elsevier B.V. All rights reserved.

the distance from each cluster to the PU is used for estimating the transmission power of the PU. In TCBCC algorithm, suppose there are N_T cooperative SUs and they form N_C clusters. At each segment of spectrum sensing stage, the information perceived by the user in the cluster is sent to the fusion center by the cluster (Chen, Tang, Bao, Tang, & Chen, 2016; Du et al., 2017; Lv, Halawani, Feng, Li, & Réhman, 2014; Stephygraph, Arunkumar, & Venkatraman, 2015; Zhang, Li, Welsh, Moghe, & Uhrich, 2016). Based on cluster $i(i = 1, 2 \cdots, N_c)$ information, the fusion center estimates the distance from the cluster i to the PU using maximum likelihood (ML). The difference between the true distance and the estimated distance is called the distance error of cluster i. When the distance error of the cluster is smaller than the preset threshold value, the cluster is deemed as that excludes the malicious users and it is called the trustful cluster. Once the trustful cluster is discovered, other clusters stop sending information to the fusion center, and the fusion center judge the channel condition using the information provided by the cluster. The simulation result shows that the proposed scheme could enhance the detection performance effectively in the existence of malicious users (Arunkumar & Mohamed Sirajudeen, 2011; Faeq Hussein et al., 2018; Wei, Meng, & Arunkumar, 2018; Zhang, Mintzer, & Uhrich, 2016).

2. System model

Suppose there are N_T SUs and one fusion center in the area with the radius R. N_T SUs form N_T clusters. The formation of cluster is based on the distance from the user to the PU. Users near the PU form a cluster. The cluster formation algorithm is not the emphasis of the paper, so it is omitted here. There are N users in each cluster, and the system model is shown in Fig. 1. Suppose the position information of cluster and PU is known, other information can be acquired form geo-location database (Elhoseny et al., 2018). In addition, two types of users are considered in this paper: trusted user and malicious user (intruder). The intruder belongs to SSDA or PUEA attack.

Suppose the system has M malicious users, and $M < N_C$. It ensures at least one cluster doesn't contain malicious user, namely there is at least one trustful cluster.

At the spectrum sensing stage, the user measures the received signal power sent by PU. The energy detection is implemented simply (Vardhana, Arunkumar, & Abdulhay, 2018), so energy detection is cited for spectrum sensing. Suppose each cluster sends information to the fusion center according to the fixed sequence. It means cluster i sends information to the fusion center at this round of sensing stage. Then, at the next round of sensing stage, cluster i still sends information to the fusion center. Fusion center estimates the state of cluster using the information. Then, the distance error is compared with the threshold value to judge whether malicious users exist in the cluster.

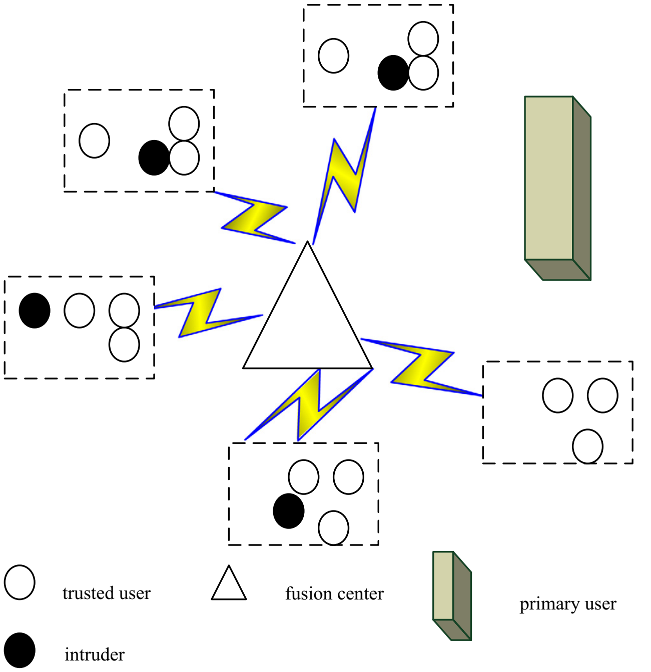

Fig. 1. System model.

Suppose the judgment takes t seconds, so if the fusion center thinks there is malicious user, then it will wait for t seconds. Then, the second cluster sends the sensed data to the fusion center again. If the second cluster also contains malicious users, the fusion center waits for t seconds again. Then, the third cluster sends the sensed data to the fusion center. Such process always goes until the fusion center finds a cluster without containing malicious users, namely finding a trustful cluster. Once the fusion center finds out a trustful cluster, the fusion center will send a piece of message No_Mes to other clusters, and notice them not to send information to it any longer. Then, the fusion center judges whether the channel frequency band is used or not using the cooperative spectrum sensing simultaneous sparsity adaptive matching pursuit (SSAMP) algorithm (Vardhana et al., 2018) based on compressed sensing information channel energy observation.

3. Attack detection analysis

Suppose the signal power $P_{i,n}$ received by the ith user in the nth cluster is:

$$P_{i,n} = P_0 + 10\alpha log\left(\frac{d_0}{d_n}\right) + c_{i,n} + \omega_{i,n} \qquad (1)$$

Hereinto, $i = 1, 2, \cdots, N$ and $n = 1, 2, \cdots, N_c$. d_n means the distance from the n th cluster to the PU transmitter, and d_0 means reference distance. Correspondingly, P_0 means the received power at the reference distance. $\omega_{i,n}$ means zero mean Gaussian random variable, and the variance is σ^2_ω. $C_{i,n}$ means the degree of malicious attack. If the i th user in the n th cluster is trusted, then $C_{i,n} = 0$. Or else,