

文章编号:1004-9037(2014)05-0688-06

基于节点识别的协作频谱检测算法

张士兵 宋莲莲 刘 燕 王 镇

(南通大学电子信息学院,南通,226019)

摘要:在认知无线网络协作频谱感知过程中,感知节点所处的恶劣信道环境会导致本地频谱检测结果发生偏差,有时一些故障节点或恶意节点发送的误导信息来干扰认证网络融合中心的全局判决。根据认知网络感知节点的历史感知信息,将感知节点分为可信节点、不可信节点和故障或恶意节点,提出了一种基于节点识别的协作频谱检测算法。在该算法中,融合中心舍弃故障或恶意节点,使其不得参与数据融合,同时也不考虑不可信节点当前发送的本地检测结果。这样,一方面消除了故障或恶意节点对全局频谱判决的影响,另一方面降低了融合中心计算复杂度。仿真结果表明,该算法能有效克服故障或恶意节点的干扰,提高认证网络协作频谱检测性能。

关键词:认知无线网络;协作频谱检测;节点识别;故障或恶意节点

中图分类号:TN911.23

文献标志码:A

Cooperative Spectrum Detection Algorithm Based on Node Recognition

Zhang Shibing, Song Lianlian, Liu Yan, Wang Zhen

(School of Electronics and Information, Nantong University, Nantong, 226019, China)

Abstract: The poor channel environment of cognitive radio networks often results in the decline of local spectrum detection performance during cooperative spectrum sensing. Sometimes, fault nodes or malicious nodes deliberately send some wrong information to disturb the fusion center to make global decision. According to the historical sensing information of sensing nodes, the sensing nodes are classified into reliable nodes, fault or malicious nodes and unreliable nodes, and a cooperative spectrum detection algorithm is proposed based on node recognition. Therefore, the fault or malicious nodes are discarded and prevented from data fusion in fusion center. At the same time, the current local detection results of unreliable nodes are not considered in current global decision. Thus, not only the effect of fault or malicious nodes on the global decision is eliminated, but also the calculation complexity of fusion center is reduced. The simulation results show that the proposed algorithm can avoid the interference of fault or malicious nodes and improve spectrum sensing performance effectively.

Key words: cognitive radio network; cooperative spectrum sensing; node recognition; fault or malicious node

引 言

随着无线数据业务的增长^[1],频谱资源日益紧张,认知无线电(Cognitive radio, CR)应运而生^[2]。它的主导思想是实现伺机的动态频谱接入^[3-5],认知用户通过频谱检测机会性地接入已分配给主用

户但暂时未被使用的空闲频段,从而提高频谱利用率。显然,准确快速的频谱感知,找到空闲频谱是提高频谱利用率的关键所在。由于信道多径、阴影衰落等复杂多变的传播环境,单个认知节点难以保证频谱检测的准确,协作频谱检测可以有效地改善频谱检测性能^[6-9]。

但在协作频谱感知过程中,是否每个节点都是

可以信赖,若存在故障或恶意节点^[10],如何及时发现并抵抗它的行为,是必须考虑和值得研究的。文献[11]提出了一种基于分组的合作感知算法,根据节点的检测概率进行可靠性判断,但在检测性能上没有显著提高。文献[12,13]提出了基于信噪比加权的协作频谱感知算法,在一定程度上改善了协作频谱检测性能。文献[14,15]提出了基于可信度的协作频谱感知算法,降低了不可信节点的影响,提高了频谱检测性能。但它们均没有考虑可能存在的故障节点或恶意节点对频谱检测性能的影响。

本文研究可能存在的故障节点或恶意节点对频谱检测性能的影响,提出一种基于节点识别的协作频谱检测算法(Cooperative spectrum detection algorithm based on node recognition, NRCS)。该算法通过节点的历史感知信息对感知节点进行识别分类,拒绝故障或恶意节点进行数据融合,对于不可信节点暂缓其参与协作处理,从而消除故障或恶意节点对全局判决结果的影响,降低了融合中心的计算复杂度,提高协作频谱检测性能。

1 系统模型

不妨假设一个认知无线网络中包括一个主用户, N 个次用户,如图1所示。存在两种假设 H_1 和 H_0 ,其中 H_1 表示网络中检测段的频谱忙碌,主用户在使用该段频谱, H_0 表示网络中检测段的频谱空闲,主用户不在使用该段频谱。第 i 个用户(感知节点)的频谱检测, $i=1, \dots, N$,可建模为一个二元假设检验问题

$$\begin{aligned} H_1: x_i(t) &= h_i(t) \cdot s(t) + n_i(t) \\ H_0: x_i(t) &= n_i(t) \end{aligned} \quad (1)$$

式中: $x_i(t)$ 是第 i 个感知节点的接收信号, $s(t)$ 是主

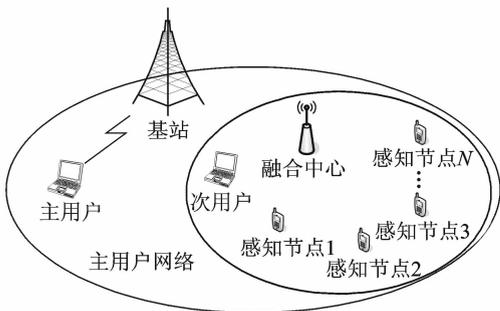


图1 系统模型

Fig.1 System model

用户信号, $h_i(t)$ 表示第 i 个感知节点所在的信道增益, $n_i(t)$ 表示第 i 个感知节点所在信道的加性高斯白噪声。

协作频谱检测过程分为两个阶段:本地检测和融合。在本地检测阶段,第 i 个感知节点对收到的信号 $x_i(t)$ 进行假设检验,得到本地检测结果“1”或“0”,“1”表示假设 H_1 成立,“0”表示假设 H_0 成立。在数据融合阶段,融合中心根据各感知节点发送的本地检测结果进行数据融合,并根据相应的判决规则和判决门限得到最终判决结果。

2 基于节点识别的协作频谱检测算法

基于节点识别的协作频谱检测算法其实现过程分为本地频谱检测和数据融合判决。感知节点将本地频谱检测结果发送至融合中心。融合中心根据节点的频谱检测准确率及其信噪比对感知节点进行分类识别。可信节点参与融合中心的数据融合,得到全局判决结果;不可信节点不参加融合中心的本次数据融合,等待下一次分类识别;故障或恶意节点进入融合中心“黑名单”,融合中心拒绝与之合作。

定义1 定义 m 次频谱检测中融合中心判断主用户信号存在 ($d_{FC} = H_1$),感知节点 i 也判断主用户信号存在 ($d_i = H_1$) 的概率,即为感知节点 i 在第 m 次频谱检测的检测概率函数,记 $P_{d_i}(m)$ 。

定义2 定义 m 次频谱检测中融合中心判断主用户信号不存在 ($d_{FC} = H_0$),感知节点 i 判断主用户信号存在 ($d_i = H_1$) 的概率,即为感知节点 i 在第 m 次频谱检测的虚警概率函数,记 $P_{f_i}(m)$ 。

定义3 对于给定的频谱检测性能门限 T_d 和 T_f ,若感知节点 i 的检测概率函数 $P_{d_i}(m)$ 及虚警概率函数 $P_{f_i}(m)$ 满足条件 $\{ P_{d_i}(m) \geq T_d, P_{f_i}(m) \leq T_f \}$,则该节点定义为可信节点;若感知节点 i 的检测概率函数 $P_{d_i}(m)$ 及虚警概率函数 $P_{f_i}(m)$ 不满足条件 $\{ P_{d_i}(m) \geq T_d, P_{f_i}(m) \leq T_f \}$,但节点 i 的信噪比 SNR 大于节点平均信噪比 SNR_T ,则该节点定义为故障或恶意节点;若感知节点 i 的检测概率函数 $P_{d_i}(m)$ 及虚警概率函数 $P_{f_i}(m)$ 不满足条件 $\{ P_{d_i}(m) \geq T_d, P_{f_i}(m) \leq T_f \}$,同时节点 i 的信噪比 SNR 不大于节点平均信噪比 SNR_T ,则节点定义为不可信节点。

在第 m 次协作频谱感知时,参与协作的各个节点将其频谱检测结果传送至融合中心。融合中

心根据节点信息计算节点的检测概率函数 $P_{d_i}(m)$ 、虚警概率函数 $P_{f_i}(m)$ 和节点平均信噪比 SNR_T ，其中节点平均信噪比为

$$\text{SNR}_T = \frac{1}{\text{card}(\Theta + \Omega)} \sum_i \text{SNR}_i \quad (2)$$

式中： Θ 为上次（第 $m-1$ 次）协作频谱感知时产生的可信节点集合， Ω 为上次（第 $m-1$ 次）协作频谱感知时产生的不可信节点集合， $\text{card}(\Theta + \Omega)$ 表示集合 Θ 和集合 Ω 中元素的个数， SNR_i 为集合 Θ 和集合 Ω 中感知节点 i 当前的信噪比。融合中心根据这些信息将集合 Θ 和集合 Ω 中的所有节点分为可信节点、故障或恶意节点以及不可信节点，并更新可信节点集合 Θ 和不可信节点集合 Ω 。

应当注意到，感知节点的信任度是一个累积的结果。也就是说，感知节点当前的信任度与节点的感知历史有关。因此，融合中心计算集合 Θ 中各个节点信任度为

$$r_i = \begin{cases} r_{i,m-1} \cdot \rho + \dots + r_{i,1} \cdot \rho^{m-1} + 1 \\ d_{i,m-1} = d_{\text{FC}} \\ r_{i,m-1} \cdot \rho + \dots + r_{i,1} \cdot \rho^{m-1} - 1 \\ d_{i,m-1} \neq d_{\text{FC}} \end{cases} \quad i \in \Theta \quad (3)$$

其加权系数为

$$w_i = \frac{r_i}{\sum_i r_i} \quad i \in \Theta \quad (4)$$

式中： r_i 是感知节点 i 的信任度， ρ 是一个表征感知节点历史关联强度的因子，其取值为 $0 < \rho < 1$ 。集合 Θ 的感知节点 i 根据上次（第 $m-1$ 次）频谱检测时的本地检测结果与全局判决结果计算节点信任度，通过累积更新信任度使可靠性高的节点在分配加权系数时拥有较大的权重，通过衰减因子 ρ 间接地增加最新信任度的权重，这样可以尽可能地减小感知节点本地检测时的偶发性错误对频谱检测的影响，使协作频谱检测的检测概率更高。

融合中心加权融合集合 Θ 中所有节点的频谱检测信息，得到全局检测统计量

$$T_{\text{FC}} = \sum_i w_i d_i \quad i \in \Theta \quad (5)$$

最后，融合中心根据判决门限 λ [16] 作出全局判决，得到第 m 次协作频谱检测结果 d_{FC} 完成频谱检测

$$d_{\text{FC}} = \begin{cases} 1 & T_{\text{FC}} \geq \lambda \\ 0 & T_{\text{FC}} < \lambda \end{cases} \quad (6)$$

上述基于节点识别的协作频谱检测算法的主要步骤可归纳为

步骤 1 计算感知节点 i 的检测概率函数 $P_{d_i}(m)$ 和虚警概率函数 $P_{f_i}(m)$ ， $i \in \Theta + \Omega$ 。

步骤 2 根据式(2)，计算集合 Θ 和集合 Ω 中感知节点的平均信噪比 SNR_T 。

步骤 3 将集合 Θ 和集合 Ω 中的感知节点分为可信节点、故障或恶意节点以及不可信节点。

步骤 4 更新可信节点集合 Θ 和不可信节点集合 Ω 。

步骤 5 计算集合 Θ 中的感知节点信任度及其加权系数。

步骤 6 根据式(5,6)得到协作频谱检测结果 d_{FC} 。

算法流程如图 2 所示。

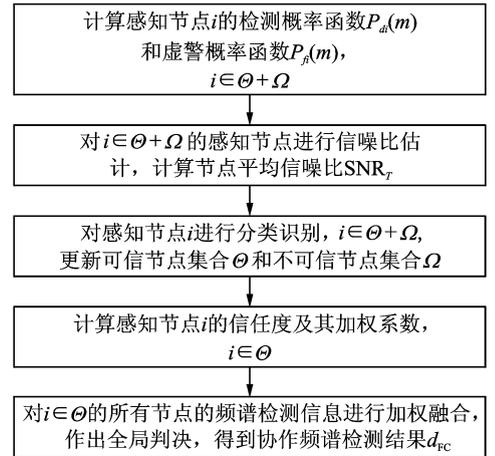


图 2 NRCS 算法流程图

Fig. 2 Flowchart of NRCS algorithm

3 仿真与分析

本文在 AWGN 信道环境下对基于节点识别的 NRCS 算法进行了仿真，并与基于可信度的加权协作频谱检测算法 (Reliability based weighted cooperative spectrum sensing algorithm, WC-SA) [15] 进行了比较。网络仿真参数如下：主用户信号为 PSK 信号，其波特率为 5 000 Bd，载波频率为 10 MHz，抽样频率为 100 MHz，采样点数为 512，感知节点总数 $N=8$ ，节点的信任度衰减因子 ρ 取 0.5，节点频谱检测性能门限分别是 $T_d=0.8$ ， $T_f=0.2$ 。实验分别对摇摆式恶意节点和伪装式恶意节点 [17] 进行仿真。

图 3 是伪装式恶意节点数 $Num=3$ 的情况下 WCSA 和 NRCS 感知算法的检测概率。随着信噪比的增大，两种算法的检测概率均得到提升，但 NRCS 感知算法的检测性能具有明显的优势，特别

是在低信噪比的环境下。当信噪比为 -15.5 dB 时, NRCS 算法的检测概率已高于 0.9 , 而 WCSA 感知算法的检测概率不到 0.75 。

图 4 是伪装式恶意节点数 $Num=3$ 的情况下 WCSA 和 NRCS 感知算法的虚警概率。随着信噪比的增大, 两种算法的虚警概率均得到减小, 但 NRCS 感知算法的虚警概率相对稳定并较小。当信噪比为 -16 dB 时, NRCS 算法的虚警率已低于 3.5×10^{-2} , 而 WCSA 感知算法的虚警率要高于 10^{-1} 。

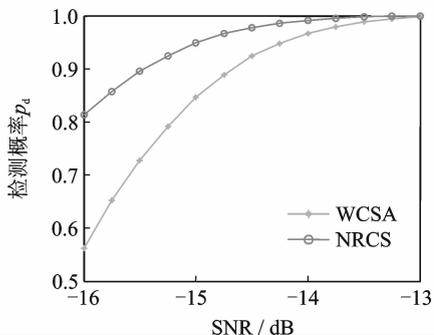


图 3 伪装式恶意节点情况下 WCSA 和 NRCS 算法的检测概率

Fig. 3 Detection probabilities of WCSA and NRCS algorithms under condition of disguised pattern malicious nodes

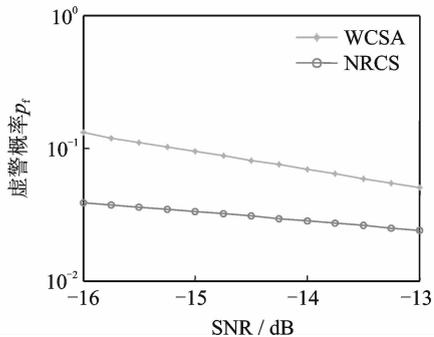


图 4 伪装式恶意节点情况下 WCSA 和 NRCS 算法的虚警概率

Fig. 4 False alarm probabilities of WCSA and NRCS algorithms under condition of disguised pattern malicious nodes

图 5,6 是摇摆式恶意节点数 $Num=3$ 的情况下 WCSA 和 NRCS 算法的检测概率和虚警概率。同样, 随着信噪比的增大, 两种算法的检测概率均增大, 虚警概率均减小, 但 NRCS 感知算法的性能更优。

比较图 3,5 可以得出: 摇摆式恶意节点下的频谱检测概率比伪装式恶意节点下的频谱检测概率

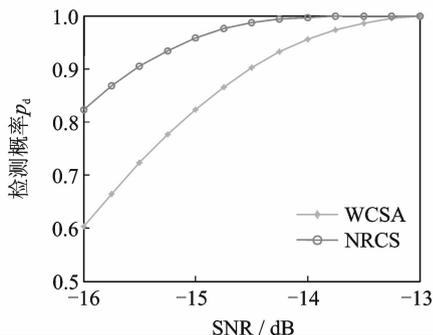


图 5 摇摆式恶意节点情况下 WCSA 和 NRCS 算法的检测概率

Fig. 5 Detection probabilities of WCSA and NRCS algorithms under condition of swing pattern malicious nodes

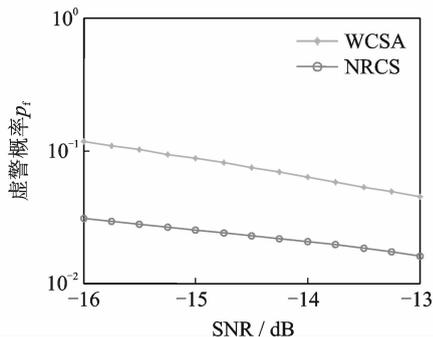


图 6 摇摆式恶意节点情况下 WCSA 和 NRCS 算法的虚警概率

Fig. 6 False alarm probabilities of WCSA and NRCS algorithms under condition of swing pattern malicious nodes

高, 尤其是摇摆式恶意节点下 WCSA 算法的检测概率提高较大。这就说明了恶意节点的类型对 WCSA 算法的检测概率影响较大, 而对 NRCS 算法几乎没有影响, 从而可以得出 NRCS 感知算法的频谱检测性能更优更稳定。

在 NRCS 算法中, 感知节点当前的信任度与之前的信任度相关, 关联强度则由衰减因子 ρ 决定。图 7,8 给出了衰减因子 ρ 对 NRCS 算法检测性能的影响。衰减因子 ρ 越大, 节点最新信任度对全局判决的影响越小, 那么感知节点当前的本地检测结果对频谱检测的影响就会减小, 从而频谱检测性能就会降低; 衰减因子 ρ 越小, 节点之前的信任度对全局判决的影响就越小, 那么感知节点本地检测时的偶发性错误对频谱检测的影响就会变大, 从而降低了频谱检测性能。从图 7,8 中可以看出, 衰减因子最佳值为 0.5 。

图 9,10 给出了判别门限 T_d 对全局频谱检测

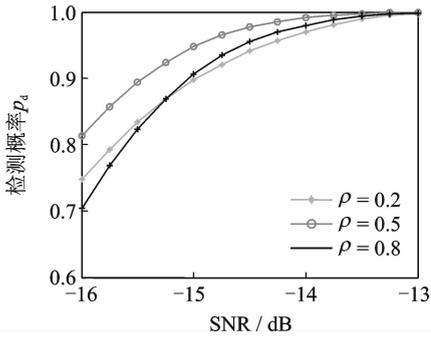


图7 衰减因子 ρ 对 NRCS 算法检测概率的影响

Fig. 7 Effect of attenuation factor ρ on detection probability of NRCS algorithm

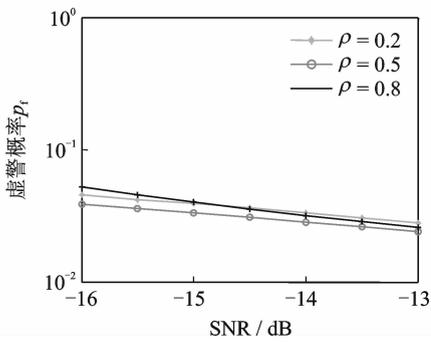


图8 衰减因子 ρ 对 NRCS 算法虚警概率的影响

Fig. 8 Effect of attenuation factor ρ on false alarm probability of NRCS algorithm

性能的影响。判别门限 T_d 越高, 满足可信条件的节点越少, 参与数据融合的节点就越多, 虽然这时参与数据融合的节点发送的本地检测结果正确率很高, 但由于节点数减少, 降低了协作频谱检测的效用, 本地检测时的偶发性错误对全局判决结果的影响就会增大, 从而导致频谱检测性能的降低; 判别门限 T_d 越低, 恶意节点被识别的可能性就越小, 其参与数据融合的可能性就越大, 对全局判决结果的影响也就越大。从图 9, 10 中可以看出, $T_d=0.8$ 是比较合适的。

图 11, 12 给出了判别门限 T_f 对检测性能的影响。判别门限 T_f 越低, 满足可信条件的节点越少, 参与数据融合的节点就越多, 虽然这时参与数据融合的节点发送的本地检测结果正确率很高, 但由于节点数减少, 协作频谱检测的效用也同样降低, 本地检测时的偶发性错误对全局判决结果的影响就会增大, 从而导致频谱检测性能的降低; 判别门限 T_f 越高, 恶意节点被识别的可能性就越小, 其参与数据融合的可能性就越大, 对全局判决结果 T_f 的影响也就越大。从图 11, 12 中可以看出, $T_f=0.2$ 比较合适。

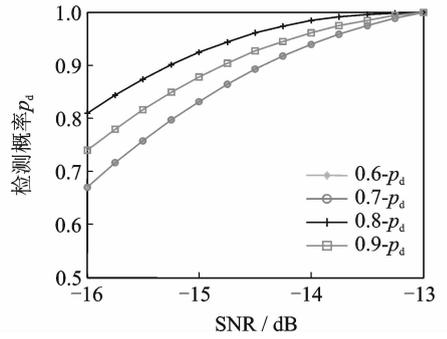


图9 判别上限 T_d 对检测概率的影响

Fig. 9 Effect of node decision threshold T_d on detection probability of NRCS algorithm

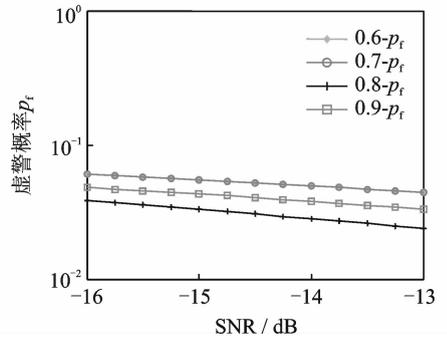


图10 判别上限 T_d 对虚警概率的影响

Fig. 10 Effect of node decision threshold T_d on false alarm probability of NRCS algorithm

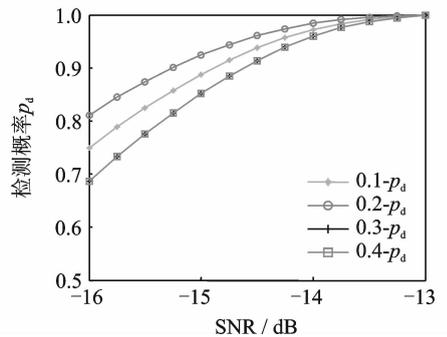


图11 判别下限 T_f 对检测概率的影响

Fig. 11 Effect of node decision threshold T_f on detection probability of NRCS algorithm

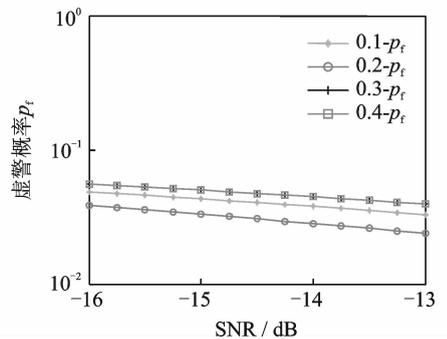


图12 判别下限 T_f 对虚警概率的影响

Fig. 12 Effect of node decision threshold T_f on false alarm probability of NRCS algorithm

4 结束语

为了降低恶意节点对认知无线网络协作频谱检测性能的影响,本文提出了基于节点识别的协作频谱检测算法。该算法利用认知网络感知节点的历史信息将感知节点进行分类识别,判别出故障或恶意节点,并在融合中心数据融合时舍弃这些恶意节点发送的信息,使其不参与数据融合,从而消除恶意节点对全局判决结果的影响,提高了协作频谱检测性能。仿真结果表明,该算法能有效遏制恶意节点的干扰,提高系统的频谱检测性能。

参考文献:

- [1] Federal Communications Commission. Spectrum policy task force [EB/OL]. <http://www.fcc.gov/sptf/>, 2010-06-30/2013-05-30.
- [2] Wang Beibei, Liu K J R. Advances in cognitive radio networks: A survey [J]. *IEEE Journal on Selected Topics in Signal Processing*, 2011, 5(1): 5-23.
- [3] 屈代明, 王志强. OFDM 机会频谱接入的信号频谱成型方法[J]. *电子与信息学报*, 2009, 31(8): 1965-1968.
Qu Daiming, Wang Zhiqiang. Spectral sculpting of OFDM signal for opportunistic spectrum access[J]. *Journal of Electronics and Information Technology*, 2009, 31(8): 1965-1968.
- [4] 杨晓燕, 杨震, 刘善彬. 基于预测机制的认知无线电机会频谱接入[J]. *重庆邮电大学学报*, 2009, 21(1): 14-19.
Yang Xiaoyan, Yang Zhen, Liu Shanbin. Forecast-based opportunistic spectrum access for cognitive radio networks [J]. *Journal of Chongqing University of Posts and Telecommunications*, 2009, 21(1): 14-19.
- [5] 李钊, 赵林靖, 刘勤. 认知无线网络基于空分复用的机会频谱接入[J]. *电子与信息学报*, 2011, 33(5): 1172-1177.
Li Zhao, Zhao Linjing, Liu Qin. Space division multiplexing based opportunistic spectrum access in cognitive radio networks [J]. *Journal of Electronics and Information Technology*, 2011, 33(5): 1172-1177.
- [6] Yu Guicai, Long Chengzhi. Research on energy detection algorithm in cognitive radio systems [C] // 2011 International Conference on Computer Science and Service System, CSSS 2011-Proceedings. Nanjing, China: IEEE, 2011: 3460-3463.
- [7] Atapattu S, Tellambura C, Jiang H. Energy detection based cooperative spectrum sensing in cognitive radio networks [J]. *IEEE Transactions on Wireless Communications*, 2011, 10(4): 1232-1241.
- [8] Zhang Yi, Zhang Lingling, Tang Chengkai. Joint detection of cyclostationary and energy in cognitive radio [C] // Proceedings of 2010 IEEE International Conference on Intelligent Systems and Knowledge Engineering, ISKE 2010. Hangzhou, China: IEEE, 2010: 182-186.
- [9] 胡晓宁, 胡捍英, 仵国锋. 认知无线电协作频谱感知机制的优化[J]. *数据采集与处理*, 2011, 26(6): 691-696.
Hu Xiaoning, Hu Hanying, Wu Guofeng. Optimization for cooperative spectrum sensing in cognitive radio networks [J]. *Journal of Data Acquisition and Processing*, 2011, 26(6): 691-696.
- [10] 韩磊磊, 陈越, 于丽莉. P2P网络的恶意节点检测模型[J]. *计算机工程与设计*, 2011, 32(2): 484-488.
Han Leilei, Chen Yue, Yu Lili. Malicious node detecting model for P2P networks [J]. *Computer Engineering and Design*, 2011, 32(2): 484-488.
- [11] 徐世宇, 尚俊娜, 赵知劲, 等. 一种基于分组的合作感知方法[J]. *现代电子技术*, 2009, 32(1): 51-57.
Xu Shiyu, Shang Junna, Zhao Zhijin, et al. Cooperative spectrum sensing method based on grouping [J]. *Modern Electronics Technology*, 2009, 32(1): 51-57.
- [12] 李玲远, 杨爽. 基于信噪比加权的协作频谱感知技术[J]. *华中师范大学学报:自然科学版*, 2010, 44(4): 577-579.
Li Lingyuan, Yang Shuang. SNR-based weighted cooperative spectrum sensing in cognitive radio [J]. *Journal of Huazhong Normal University: Natural Sciences*, 2010, 44(4): 577-579.
- [13] Wu Suwen, Zhu Jinkang, Qiu Ling, et al. SNR-based weighted cooperative spectrum sensing in cognitive radio networks[J]. *Journal of China Universities of Posts and Telecommunications*, 2010, 17(2): 1-7.
- [14] Feng Jingyu, Lu Guangyue, Bao Zhiqiang. Weighted-cooperative spectrum sensing scheme using trust in cognitive radio networks [C] // International Conference on Signal Processing Proceedings, ICSP. Beijing, China: IEEE, 2012, 3: 1693-1696.
- [15] 王海莲, 张士兵, 郭莉莉. 基于可信度的加权协作频谱检测算法[J]. *数据采集与处理*, 2014, 29(3): 472-477.
Wang Hailian, Zhang Shibing, Guo Lili. Reliability-based weighted cooperative spectrum sensing algorithm [J]. *Journal of Data Acquisition and Processing*, 2014, 29(3): 472-477.
- [16] Zeng Yonghong, Liang Yingchang. Eigenvalue based spectrum sensing algorithms for cognitive radio[J]. *IEEE Transaction on Communications*, 2009, 57(6): 1784-1793.
- [17] 吕兴凤, 高扬. P2P网络中抑制恶意节点的研究综述[J]. *信息技术*, 2012, 36(8): 36-39.
Lü Xingfeng, Gao Yang. Research on the inhibition of malicious nodes in P2P network [J]. *Information Technology*, 2012, 36(8): 36-39.

作者简介:张士兵(1962-),男,博士,教授,博士生导师,研究方向:通信信号处理、协作通信、认知无线网络, E-mail: zhangshb@ntu.edu.cn; 宋莲莲(1990-),女,硕士研究生,研究方向:通信信号处理、认知无线网络; 刘燕(1993-),女,本科生,研究方向:通信信号处理、认知无线网络; 王镇(1993-),男,本科生,研究方向:通信信号处理、认知无线网络。