

doi:10.14132/j.cnki.1673-5439.2017.03.011

模拟主用户攻击下协作频谱感知 检测阈值的优化研究

李莎¹,戴建新²,程崇虎¹,汪鹏¹,王军¹

(1. 南京邮电大学 通信与信息工程学院,江苏 南京 210003)
(2. 南京邮电大学 理学院,江苏 南京 210023)

摘要:认知无线电网络中提出的协作频谱感知技术利用多个认知用户的本地感知,克服了多径效应、阴影效应等问题,提高了系统的检测性能。然而动态频谱接入方法也给系统带来了主用户模拟攻击(PUEA)的威胁,即一些恶意用户试图模仿主用户信号来欺骗次级用户,从而阻止次级用户访问空闲频段。文中提出了一个智能攻击者能够感知并判决主用户是否存在,并在主用户不存在时发送伪造信号的系统。在这个系统中推导了基于能量检测的协作频谱感知检测概率,并进一步对检测阈值进行了优化,从而得到了总误差概率最小时的最佳检测阈值。最后通过在PUEA存在情况下,基于能量检测的协作频谱感知的最佳检测阈值的仿真进一步验证了推导结果。

关键词:认知无线电;协作频谱感知;主用户模拟攻击(PUEA);最佳检测阈值

中图分类号:TN929.5 文献标志码:A 文章编号:1673-5439(2017)03-0083-05

Optimal detection threshold of cooperative spectrum sensing in presence of primary user emulation attack

LI Sha¹, DAI Jianxin², CHENG Chonghu¹, WANG Peng¹, WANG Jun¹

(1. College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)
(2. School of Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

Abstract: In cognitive radio network, a cooperative spectrum sensing technology can overcome the problems of multi-path effects, shadow effects and such constraints by using local sensing results of cognitive users, thus improving the detection performance. However, the dynamic spectrum access imposes some threats to the network. One of these common threats is primary user emulation attack (PUEA), where some malicious users try to mimic the primary signal and deceive secondary users to prevent them from accessing the vacant frequency bands. A system is considered in which a smart attacker performs its own spectrum sensing according to its acquired knowledge about the presence or absence of the primary signal. And fake signals are sent when the primary user signal is not presented in the radio environment. In the system, the detection probability of cooperative spectrum sensing based on energy detection in the presence of a PUEA is deduced, and the detection threshold is optimized, thus the optimal detection threshold on the minimum total error probability is obtained. Finally, the optimal detection threshold for the cooperative spectrum sensing based on the energy detection in the presence of PUEA is simulated. The results verify the conclusions of theory deducing.

Keywords: cognitive radio; cooperative spectrum sensing; primary user emulation attack (PUEA); optimal detection threshold

收稿日期:2016-09-28;修回日期:2016-12-23 本刊网址:<http://nyzr.njupt.edu.cn>

基金项目:国家自然科学基金(61401399)、江苏省博士后科研资助计划(1501073B)、南京邮电大学自然科学基金(NY214108)和东南大学移动通信国家重点实验室开放课题(2016D05)资助项目

通讯作者:戴建新 电话:025-85868604 E-mail:daijx@njupt.edu.cn

近年来,无线通信技术快速发展,3G 网络已经全面普及,4G 也已经开始投入使用之中。而用户日益增长的无线通信需求与有限的无线频谱资源之间的矛盾日益凸显,这已经成为摆在全世界无线通信技术研究者面前的问题^[1-2]。认知无线电(CR)可以通过动态访问空闲频段来提高频谱效率^[3]。在 CR 网络中,授权的用户被称为主用户(PU),未授权的用户被称为次级用户(SU)或 CR 用户。当无线电环境中不存在主用户时,次级用户被允许使用该频段,所以 CR 用来频谱感知和估算信道中是否存在主用户^[4-5]。

在 CR 网络的各种传感方法中,协作频谱感知(CSS)方法具有较高的频谱感知性能^[6]。CSS 方法可以在衰落环境下有效地提高传感精度。在 CSS 中,每个次级用户使用某些检测方法独立地进行频谱感知,然后将他们的本地感知结果报告给融合中心,最后由融合中心做出最后的判决^[7]。文献[8]介绍了在虚警概率不变的情况下,通过优化 CR 数目来达到最好的检测性能。文献[9]讨论了系统性能与用于感知的 CR 数目之间的平衡问题。文献[10]探讨了检测阈值、感知时间和判决准则的共同优化问题。

CR 网络的这种动态访问方式可能会被恶意用户利用,从而造成频谱感知的性能漏洞。主用户模拟攻击(PUEA)是其中的一个威胁,这种攻击是指当某频段不存在主用户时,恶意用户发送与主用户相同的信号,使次级用户腾出该频段^[11]。文献[8-10]均是在不存在主用户模拟攻击的理想环境下进行的讨论,都没有考虑 PUEA 对系统性能的影响。在文献[12]中,作者提出一个考虑 PUEA 的协作频谱感知,但假设 PUEA 始终存在,这与 PUEA 的定义是不相符的。文献[13]只讨论了 PUEA 存在概率与检测性能的关系,没有考虑与检测阈值和判决准则等因素的关系。

在本文中,针对现有文献的不足,考虑了 PUEA 进行频谱感知,当感知到 PU 不存在时发送假信号,推导了基于能量检测的协作频谱感知检测概率,得到了总误差概率最小时的最佳检测阈值,并通过仿真进一步验证结果。

1 系统模型

如图 1 所示,系统模型由一个主用户(PU),共存于一个认知无线电网络(CRN)的 N 个次级用户(CR)以及一个融合中心组成。主用户模拟攻击的

存在是为了蒙骗 CR 网络。

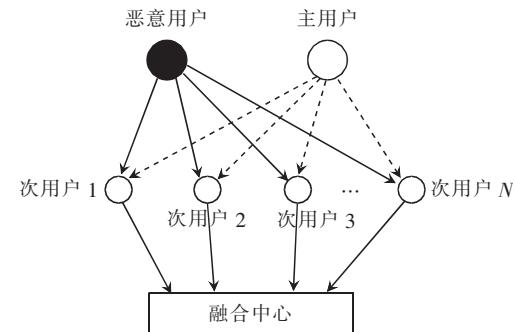


图 1 CR 网络的系统模型

在这个协作认知无线电网络中,每个次级用户独立地执行周期性的本地频谱感知,然后发送一个二进制本地判决结果给融合中心。融合中心结合本地的判决结果做出最后的判决,来推断观察的这个频段内是否存在主用户。认知无线电网络中的次级用户运用能量检测进行本地频谱感知,以及使用 K/N 融合准则进行判决。

根据 PU 和 PUEA 的存在与否(其中 PUEA 只在 PU 不存在时才发送假信号),将模型分成三种情况:

$$S_1 = \{A_0, H_1\}, S_2 = \{A_0, H_0\}, S_3 = \{A_1, H_0\}$$

其中, A_0 表示 PUEA 不存在, A_1 表示 PUEA 存在, H_0 表示 PU 不存在, H_1 表示 PU 存在。

2 PUEA 下的频谱感知

在本节中,我们考虑到在不存在主用户时,PUEA 会发送假信号的情况,制定了合适的频谱感知规则。它有别于不考虑 PUEA 存在的传统的频谱感知。

我们使用检测概率(P_d)和虚警概率(P_f)来评估 CR 频谱感知的性能^[14]。则第 i 个 CR 本地频谱感知的检测概率和虚警概率为

$$P_{d,i} = P(D_1 | H_1) \quad (1)$$

$$P_{f,i} = P(D_1 | H_0) \quad (2)$$

其中, D_1 表示第 i 个 CR 判决 PU 信号存在。

能量检测是整合感知时间 τ 内在带宽 $f_s/2$ 处接收到的信号,然后传感器将收集的能量 E_i 与预设阈值 ε 做比较来判决该频段是否存在 PU^[15]。

在不考虑 PUEA 的情况下,传感器的检测概率和虚警概率的定义是

$$P_{d,i} = P(D_1 | H_1) = P\{E_i > \varepsilon_i | H_1\} = Q\left(\frac{\varepsilon - f_s\tau - \gamma}{\sqrt{2f_s\tau + 4\gamma}}\right) \quad (3)$$

$$P_{f,i} = P(D_1 | H_0) = P\{E_i > \varepsilon_i | H_0\} = Q\left(\frac{\varepsilon - f_s \tau}{\sqrt{2f_s \tau}}\right) \quad (4)$$

其中, $\gamma = \sigma_x^2 / \sigma_n^2$ 表示接收信噪比。

如前所述, 当不存在 PU 时, CR 用户将接收到 PUEA 发送的信号。所以, 在这种攻击存在的情况下, P_f 将受到影响。考虑到 PUEA 的存在, 可以得到

$$P_{f,i} = P(D_1 | H_0) = P(D_1 | A_0, H_0)P(A_0 | H_0) + P(D_1 | A_1, H_0)P(A_1 | H_0) \quad (5)$$

若考虑 PUEA 的存在, 实际上

$$Q\left(\frac{\varepsilon - f_s \tau}{\sqrt{2f_s \tau}}\right) = P(D_1 | A_0, H_0) \quad (6)$$

定义 $P(A_0 | H_0) = \alpha$, $P(H_0) = P_0$, $P(H_1) = P_1$ 。

由贝叶斯定理和式(6)可得

$$\begin{aligned} P_{f,i} &= P(D_1 | H_0) = P(D_1 | A_0, H_0)P(A_0 | H_0) + \\ &\quad P(D_1 | A_1, H_0)P(A_1 | H_0) = \\ &\quad \alpha \cdot Q\left(\frac{\varepsilon - f_s \tau}{\sqrt{2f_s \tau}}\right) + \frac{P(A_1, H_0 | D_1)P(D_1)}{P(A_1, H_0)}P(A_1 | H_0) = \\ &\quad \alpha \cdot P_f + \frac{P(A_1 | D_1)P(H_0 | D_1)P(D_1)}{P(H_0)} = \\ &\quad \alpha \cdot Q\left(\frac{\varepsilon - f_s \tau}{\sqrt{2f_s \tau}}\right) + P(A_1 | D_1)P(D_1 | H_0) = \\ &\quad \alpha \cdot Q\left(\frac{\varepsilon - f_s \tau}{\sqrt{2f_s \tau}}\right) + P(A_1 | D_1)P_{f,i} \end{aligned} \quad (7)$$

其中,

$$\begin{aligned} P(A_1 | D_1) &= \frac{P(D_1 | A_1)P(A_1)}{P(D_1)} = \\ &\quad \frac{P(D_1 | A_1)P(A_1)}{P(D_1 | A_0)P(A_0) + P(D_1 | A_1)P(A_1)} \end{aligned} \quad (8)$$

根据等式 $P(H_0 | A_1)P(A_1) = P(A_1 | H_0)$

$P(H_0)$ 可得

$$P(A_1) = \frac{P(A_1 | H_0)P(H_0)}{P(H_0 | A_1)} = \frac{(1 - \alpha)P(H_0)}{P(H_0 | A_1)}$$

又 $P(H_0 | A_1) = 1$, 故

$$P(A_1) = (1 - \alpha)P(H_0)$$

$$P(A_0) = 1 - P(A_1) = 1 - (1 - \alpha)P(H_0)$$

此外, $P(D_1 | A_0), P(D_1 | A_1)$ 的值可以通过 CRN 网络发送训练序列获得, 令

$$P(D_1 | A_0) = P_{10}, P(D_1 | A_1) = P_{11}$$

$$P(H_0) = P_0, P(H_1) = 1 - P(H_0) = P_1$$

则 $P(A_0) = P_1 + \alpha P_0, P(A_1) = (1 - \alpha)P_0$ 。

由此可得到 PUEA 下频谱感知的虚警概率和检测概率

$$P_{f,i} = \frac{P_{10}P_1 + P_{11}P_0 + \alpha P_{10}P_0 - \alpha P_{11}P_0}{P_{10}P_1 + \alpha P_{10}P_0}.$$

$$\alpha \cdot Q\left(\frac{\varepsilon - f_s \tau}{\sqrt{2f_s \tau}}\right) \quad (9)$$

$$P_{d,i} = Q\left(\frac{\varepsilon - f_s \tau - \gamma}{\sqrt{2f_s \tau + 4\gamma}}\right) \quad (10)$$

以及漏检概率

$$P_{m,i} = 1 - P_{d,i} \quad (11)$$

3 PUEA 下的协作频谱感知

在进行 CCS 时, 每个 CR 将本地判决结果发送到 FC, 然后给出一个 PU 是否存在的全面判决结果。FC 应用了很多融合准则, 例如 OR 准则、AND 准则和 K/N 准则。OR 准则是指只要有一个 CR 检测到主用户信号, FC 就判决存在 PU, 否则频段就被认为是空闲的。AND 准则是必须所有的 CR 都检测到主用户信号, 才判决存在 PU, 否则就认为频段是空闲的。而 K/N 准则是指有 N 个 CR, 其中 K 个检测到主用户信号就判决存在 PU^[16]。其实 OR 准则和 AND 准则是 K/N 准则的特例, 当 K 等于 1 时是 OR 准则; 而 K 等于 N 时是 AND 准则。

假设所有的 CR 用户使用相同的阈值 ε 。这就使 $P_{f,i}$ 和 $P_{d,i}$ 都与 i 无关, 从而可以表示为 P_f 和 P_d , 则 $P_m = 1 - P_d$ 。

K/N 准则下, 协作频谱感知的虚警概率和漏检概率分别为^[17]

$$\begin{aligned} Q_f &= \Pr\{H_1 | H_0\} = \\ &\quad \sum_{l=K}^N \binom{N}{l} [\Pr\{H_1 | H_0\}]^l [\Pr\{H_0 | H_0\}]^{N-l} = \\ &\quad \sum_{l=K}^N \binom{N}{l} P_f^l (1 - P_f)^{N-l} \end{aligned} \quad (12)$$

$$\begin{aligned} Q_m &= \Pr\{H_0 | H_1\} = 1 - \Pr\{H_1 | H_1\} = \\ &\quad 1 - \sum_{l=K}^N \binom{N}{l} [\Pr\{H_1 | H_1\}]^l [\Pr\{H_0 | H_1\}]^{N-l} = \\ &\quad 1 - \sum_{l=K}^N \binom{N}{l} P_d^l (1 - P_d)^{N-l} \end{aligned} \quad (13)$$

4 PUEA 下协作频谱感知检测阈值的优化

在本文中, 我们以总误差概率 $Q_f + Q_m$ 最小化为目标, 探讨存在主用户攻击情况下的协作频谱感知的最佳检测阈值。

定理 以总误差概率 $Q_f + Q_m$ 最小化为目标的最小检测阈值是存在的。

证明:

将式(12)改写为

$$\begin{aligned} Q_f^{(K,n)} &= \sum_{l=K}^n \binom{n}{l} P_f^l (1 - P_f)^{n-l} = \\ &\sum_{l=K-1}^{n-1} \binom{n-1}{l} P_f^l \times P_f (1 - P_f)^{n-l-1} + \\ &\sum_{l=K}^{n-1} \binom{n-1}{l} P_f^l (1 - P_f)^{n-l-1} \times (1 - P_f) = \\ &Q_f^{(K-1,n-1)} P_f + Q_f^{(K,n-1)} (1 - P_f) \end{aligned} \quad (14)$$

同理,式(13)可以改写为

$$\begin{aligned} Q_m^{(K,n)} &= 1 - \sum_{l=K}^{n-1} \binom{n}{l} P_d^l (1 - P_d)^{n-l} = \\ &1 - \sum_{l=K-1}^{n-1} \binom{n-1}{l} P_d^l \times P_d (1 - P_d)^{n-l-1} - \\ &\sum_{l=K}^{n-1} \binom{n-1}{l} P_d^l (1 - P_d)^{n-l-1} \times (1 - P_d) = \\ &1 - Q_d^{(K-1,n-1)} P_d - Q_d^{(K,n-1)} (1 - P_d) \end{aligned} \quad (15)$$

其中, $Q_f^{(0,n)} = Q_d^{(0,n)} = 1$, 且当 $K > n$ 时, $Q_f^{(K,n)} = Q_d^{(K,n)} = 0$ 。

由式(14)和式(15)可得

$$\frac{\partial Q_f^{(K,n)}}{\partial \varepsilon} = Q_f^{(K-1,n-1)} \frac{\partial P_f}{\partial \varepsilon} - Q_f^{(K,n-1)} \frac{\partial P_f}{\partial \varepsilon} \quad (16)$$

$$\frac{\partial Q_m^{(K,n)}}{\partial \varepsilon} = -Q_d^{(K-1,n-1)} \frac{\partial P_d}{\partial \varepsilon} + Q_d^{(K,n-1)} \frac{\partial P_d}{\partial \varepsilon} \quad (17)$$

定义 $\varepsilon^* = \arg \min_{\lambda} (Q_f + Q_m)$, 当 $\frac{\partial Q_f}{\partial \varepsilon} + \frac{\partial Q_m}{\partial \varepsilon} = 0$

时可以实现,即

$$\begin{aligned} (Q_f^{(K-1,n-1)} - Q_f^{(K,n-1)}) \frac{\partial P_f}{\partial \varepsilon} \Big|_{\varepsilon_n^*} &= \\ (Q_d^{(K-1,n-1)} - Q_d^{(K,n-1)}) \frac{\partial P_d}{\partial \varepsilon} \Big|_{\varepsilon_n^*} \end{aligned} \quad (18)$$

对式(18)求解得

$$\varepsilon_n^* = \frac{f_s \tau}{2} + \sqrt{\frac{f_s^2 \tau^2}{4} + \frac{f_s \tau \gamma}{2} + \frac{2f_s^2 \tau + 4f_s \tau \gamma \ln(\eta \beta \sqrt{1 + 2\gamma})}{\gamma}} \quad N = 1, 2, \dots, n \quad (19)$$

其中

$$\beta = \frac{P_{10}P_1 + P_{11}P_0 + \alpha P_{10}P_0 - \alpha P_{11}P_0}{P_{10}P_1 + \alpha P_{10}P_0} \cdot \alpha$$

$$\eta = \frac{Q_f^{(K-n,n-1)} - Q_f^{(K,n-1)}}{Q_d^{(K-1,n-1)} - Q_d^{(K,n-1)}}$$

5 仿真结果及分析

在本节中,我们提供了一些数值结果来证明模拟主用户攻击情况下协作频谱感知的最优检测阈值。以下仿真均是在 AWGN 信道条件下进行的。

图 2 比较了传统非协作方法和协作频谱感知方法下的 ROC 曲线。从图 2 中可以直观地看出在虚警概率一定时,协作频谱感知方法有效地提高了系统的检测概率;在相同的检测概率下,采用协作频谱感知方法的系统的虚警概率更小。从而可以得到,协作频谱感知方法可以有效提高系统性能。

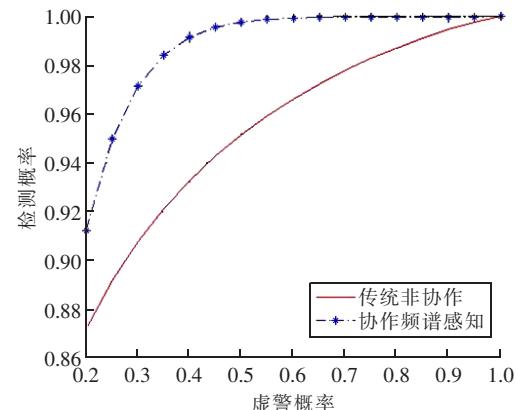


图 2 ROC 曲线

图 3 直观地显示了在不同的融合准则下,总错误率 $Q_f + Q_m$ 与检测阈值的关系。我们设定该认知无线电网络共有 10 个 CR 用户。

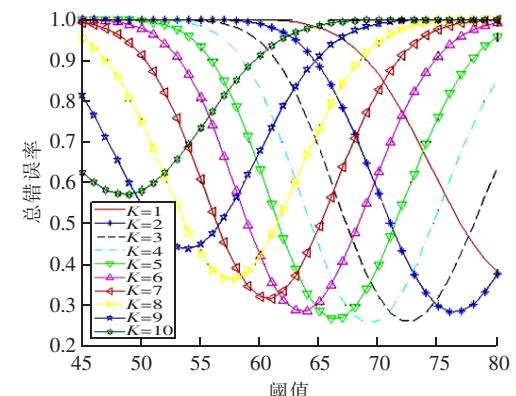


图 3 总错误率随检测阈值变化的曲线($N=10$)

由图 3 可以看出,在 K 从 1 取到 10 的 10 种情况下,总错误率总是随着检测阈值先下降后上升。换句话说就是在不同的融合准则下,都存在一个最佳的检测阈值使总错误率最小。

图 4 显示的是在相同的融合准则下,是否考虑 PUEA 对总错误率的影响。由图 4 可以看出,当系统中存在 PUEA 时,考虑 PUEA 的存在比不考虑时的总错误率小,从而提高了系统的检测概率。而当检测阈值超过最佳检测阈值时,两条曲线逐步接近直至重合。也就是说,当检测阈值小于最佳检测阈值的时候,考虑 PUEA 可以有效降低错误率。所以,相对于上述文献中的方法,本文提出的在系统中加

入对 PUEA 的考虑可以有效降低系统的错误率。

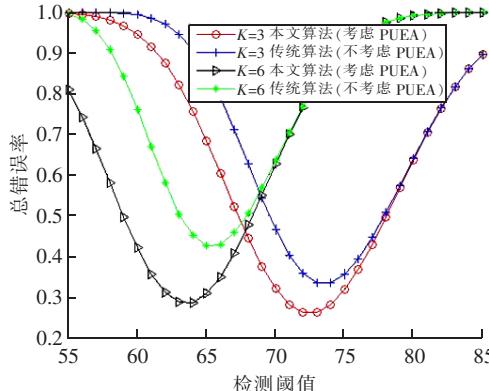


图 4 考虑 PUEA 对总错误率的影响($N=10$)

6 结束语

本文研究了考虑 PUEA 存在情况下协作频谱感知的最佳检测阈值。PUEA 能够进行频谱感知和有计划地发送信号。在主用户不存在的情况下,攻击者模拟主用户信号随机发送。考虑 PUEA 的存在能有效提高系统性能。本文对存在 PUEA 时基于能量检测的协作频谱感知系统的检测阈值进行了优化分析和仿真。仿真结果表明,在不同的融合准则下,始终存在一个最佳检测阈值使总误差率最小,且当设定的阈值小于最佳检测阈值时,考虑 PUEA 可以有效降低错误率。

参考文献:

- [1] ANDREWS J G, BUZZI S, CHOI W. What will 5G be? [J]. IEEE Journal on Selected Areas in Communications, 2014, 32(6):1065–1082.
- [2] LUO Man. Research on cooperative spectrum sensing in cognitive radio[D]. Harbin: Harbin Institute of Technology, 2015.
- [3] LI Jiajun. Research on cooperative spectrum sensing in cognitive radio[D]. Beijing: Beijing Jiaotong University, 2012.
- [4] HAYKIN S. Cognitive radio: brain-empowered wireless communications[J]. IEEE Journal on Selected Areas in Communications, 2005, 23(2):201–220.
- [5] LETAIEF K B, ZHANG W. Cooperative communications for cognitive radio networks[J]. Proceedings of the IEEE, 2009, 97(5):878–893.
- [6] PENG Tao, GUO Chen, WANG Wenbo. Energy-efficient cooperative spectrum sensing in cognitive radio networks[J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(4):93–96.
- [7] MITOLA J, MAGUIRE G. Cognitive radio: making software radios more personal[J]. IEEE Personal Communications, 1999, 6(4):13–18.
- [8] ZHANG W, MALLIK R K, LETAIEF K. Cooperative spectrum sensing optimization in cognitive radio networks[C]//IEEE International Conference on Communications. 2008:3411–3415.
- [9] CHEN Y. Optimum number of secondary users in collaborative spectrum sensing considering resources usage efficiency[J]. IEEE Communications Letters, 2008, 12(12):877–879.
- [10] PEH E C Y, LIANG Y C, GUAN Y, et al. Optimization of cooperative sensing in cognitive radio networks: a sensing throughput tradeoff view[C]//IEEE International Conference on Communications. 2009:1–5.
- [11] CHEN Z, COOKLEV T, CHEN C, et al. Modeling primary user emulation attacks and defenses in cognitive radio networks[C]//IEEE International Performance Computing and Communications Conference. 2009:208–215.
- [12] CHEN C, CHENG H, YAO Y D. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack[J]. IEEE Transactions on Wireless Communications, 2011, 10(7):2135–2141.
- [13] HAGHIGHAT M, SADOUGH S M S. Cooperative spectrum sensing in cognitive radio networks under primary user emulation attacks[C]//6th International Symposium on Telecommunications(IST). 2012:148–151.
- [14] LIANG Hongyu, CHEN Hongbin, ZHAO Feng. Cooperative spectrum sensing in cognitive radio networks[J]. Guangxi Communication Technology, 2011(2):38–44.
- [15] LIU Shiqi. Research on cooperative spectrum sensing based on cognitive radio[D]. Guangzhou: South China University of Technology, 2014.
- [16] DONG Caiping. Cooperative spectrum sensing in cognitive radio networks[D]. Chengdu: University of Electronic Science and Technology of China, 2012.
- [17] DU Hong. Research on spectrum sensing optimization and radio resource management in cognitive radio[D]. Beijing: Beijing University of Posts and Telecommunications, 2012.

作者简介:



李 莎(1989-),女,山东济宁人。南京邮电大学通信与信息工程学院硕士研究生。主要研究方向是认知无线电。