

模拟主用户攻击下的协作频谱感知

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: 认知无线网络中,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、阴影效应等问题的制约,提高了系统的检测性能。然而认知无线电提出的动态频谱接入方法在有效解决了频谱稀缺问题的同时也给网络带来了一些威胁。这些威胁之一就是主用户模拟攻击(PUEA),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。考虑了一个能根据自己的感知并判决主用户是否存在的智能攻击者,它在主用户不存在时发送伪造信号。在此基础上,推导了基于能量检测的协作频谱感知检测概率,通过仿真分析了基于能量检测的协作频谱感知系统在存在主用户模拟攻击时的性能,并验证了它是一种优化检测性能有效且可实现的方法。

关键词: 认知无线电;协作频谱感知;主用户模拟攻击;性能优化

中图分类号: TN929.5

文献标识码: A

文章编号: 1673-629X(2017)02-0072-04

doi:10.3969/j.issn.1673-629X.2017.02.017

Cooperative Spectrum Sensing in Presence of Primary User Emulation Attack

LI Sha¹, DAI Jian-xin², CHENG Chong-hu¹, 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, cooperative spectrum sensing technology overcomes the problems of multipath and shadow effects and such constraints by using local sensing results of cognitive users, hence improving the detection performance. However, cognitive radio which is a solution for spectrum scarcity by means of a dynamic spectrum access, imposes some threats to the network. One of them 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 smart attacker is considered which performs its own spectrum sensing according to its acquired knowledge about the presence or absent of the primary signal, and it sent fake signals when the primary user signal is not present in the radio environment. The detection probability of cooperative spectrum sensing based on energy detection in the presence of a PUEA is deduced. The simulation results show that the measure can effectively improve the performance of the system.

Key words: cognitive radio; cooperative spectrum sensing; PUEA; performance optimization

0 引言

近年来,无线通信技术发展迅速,3G网络已经全面普及,4G也已经开始投入应用。而用户日益增长的无线通信需求与有线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)通过动态访问空闲频段来提高频谱效率的方法已被广泛研究^[3]。在CR

的术语中,授权的用户称为主用户(PU),未授权的用户称为次级用户(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执行频谱感知和估算是否存在主用户的任务^[4-5]。

在CR网络的各种传感方法中,协作频谱感知(CSS)方法由于其较高的频谱感知性能脱颖而出^[6]。CSS方法可以在衰落环境下有效提高传感精度。在

收稿日期:2016-03-23

修回日期:2016-07-06

网络出版时间:2017-01-04

基金项目: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)

作者简介:李莎(1989-),女,硕士,研究方向为认知无线电频谱感知;戴建新,副教授,研究方向为5G移动通信系统的关键技术;程崇虎,教授,研究方向为电磁场。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20170104.1039.062.html>

CSS 中,每个次级用户使用某些检测方法独立进行频谱感知,然后将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]探讨了能量阈值,感知时间和决策融合规则的共同优化问题。

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。文献[12]提出了考虑 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,没有考虑与感知时间和 CR 数目等因素的关系。

文中对 PUEA 进行频谱感知,当感知到 PU 不存在时发送假信号。对基于能量检测的协作频谱感知系统存在主用户模拟攻击时的性能情况,以及 PUEA 的存在概率、感知时间、CR 数目和检测性能之间的均衡问题进行了分析和仿真。

1 系统模型

如图 1 所示,系统模型由一个 PU,共存于一个认知无线网络(CRN)的 N 个 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。

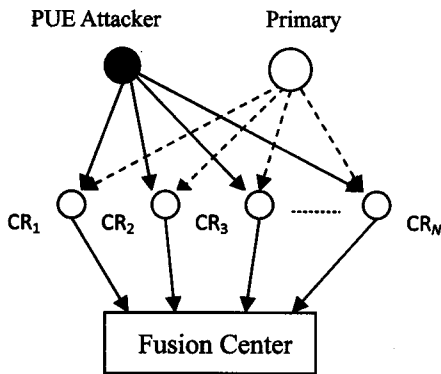


图 1 CR 网络的系统模型

在这个协作认知无线网络中,每个次级用户独立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,来推断在观察的这个频段内是否存在主用户。认知无线网络中的次级用户运用能量检测进行本地频谱感知,使用 OR/AND 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 下的协作频谱感知

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。

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 PUEA 是否存在的全面判决结果。在 FC 应用了很多融合准则,例如 OR 准则和 AND 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。而 AND 准则必须是所有的 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^[14]。在 OR 和 AND 融合准则下,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^[15]。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。

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:

$$P_{f,i} = (D_1 | H_0) = P(D_1 | A_0, H_0)P(A_0 | H_0) + P(D_1 | A_1, H_0)P(A_1 | H_0) \quad (3)$$

采用 OR 准则时的检测概率和虚警概率分别为^[16]:

$$P_d = 1 - \prod_{i=1}^N (1 - P_{d,i}) \quad (4)$$

$$P_f = 1 - \prod_{i=1}^N (1 - P_{f,i}) \quad (5)$$

采用 AND 准则时的检测概率和虚警概率分别为:

$$P_d = \prod_{i=1}^N P_{d,i} \quad (6)$$

$$P_f = \prod_{i=1}^N P_{f,i} \quad (7)$$

3 PUEA 下基于能量检测的协作频谱感知

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^[17]。

在不考虑 PUEA 的情况下,传感器的检测概率和虚警概率分别为:

$$P_{d,i} = P(D_1 | H_1) = P\{E_i > \varepsilon_i | H_1\} = Q\left(\frac{\varepsilon - f_s \tau - \gamma}{\sqrt{2f_s \tau + 4\gamma}}\right) \quad (8)$$

$$P_{t,i} = P(D_1 | H_0) = P\{E_i > \varepsilon_i | H_0\} = Q\left(\frac{\varepsilon - f_s \tau}{\sqrt{2f_s \tau}}\right) \quad (9)$$

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

若考虑 PUEA 的存在, 实际上

$$Q\left(\frac{\varepsilon - f_s \tau}{\sqrt{2f_s \tau}}\right) = P(D_1 | A_0, H_0) \quad (10)$$

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(10)可得:

$$\begin{aligned} P_{t,i} &= (D_1 | H_0) = P(D_1 | A_0, H_0)P(A_0 | H_0) + \\ &P(D_1 | A_1, H_0)P(A_1 | H_0) = \\ &\alpha \cdot Q\left(\frac{\varepsilon - f_s \tau}{\sqrt{2f_s \tau}}\right) + \\ &\frac{P(A_1 | H_0 | D_1)P(D_1)}{P(A_1, H_0)}P(A_1 | H_0) = \\ &\alpha \cdot P_t + \frac{P(A_1 | D_1)P(H_0 | D_1)P(D_1)}{P(H_0)} = \\ &\alpha \cdot Q\left(\frac{\varepsilon - f_s \tau}{\sqrt{2f_s \tau}}\right) + P(A_1 | D_1)P(D_1 | H_0) = \\ &\alpha \cdot Q\left(\frac{\varepsilon - f_s \tau}{\sqrt{2f_s \tau}}\right) + P(A_1 | D_1)P_{t,i} \quad (11) \end{aligned}$$

其中

$$\begin{aligned} P(A_1 | D_1) &= \frac{P(D_1 | A_1)P(A_1)}{P(D_1)} = \\ &\frac{P(D_1 | A_1)P(A_1)}{P(D_1 | A_0)P(A_0) + P(D_1 | A_1)P(A_1)} \quad (12) \end{aligned}$$

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

给定一个 $P_{t,i}$, 可得:

$$\varepsilon = \sqrt{2f_s \tau} Q^{-1}\left(\frac{P_{10}P_1P_{t,i} + \alpha P_{10}P_0P_{t,i}}{(P_{10}P_1 + P_{11}P_0 + \alpha P_{10}P_0 - \alpha P_{11}P_0)\alpha}\right) + f_s \tau \quad (13)$$

将式(13)代入式(8)得到考虑 PUEA 情况下的检测概率:

$$P_{d,i} = Q\left(\frac{\sqrt{2f_s \tau} Q^{-1}\left(\frac{P_{10}P_1P_{t,i} + \alpha P_{10}P_0P_{t,i}}{(P_{10}P_1 + P_{11}P_0 + \alpha P_{10}P_0 - \alpha P_{11}P_0)\alpha}\right) - \gamma}{\sqrt{2f_s \tau + 4\gamma}}\right) \quad (14)$$

4 仿真结果及分析

在本节中, 假设基站可以确定每个 CR 的位置, 且每个 CR 接收到的信号有相同的信噪比。设定 $\gamma = -20$ dB, $P_0 = 0.1$, $P_1 = 0.9$, $P_{10} = 0.3$, $P_{11} = 0.8$ 。

图 2 显示的是分别在 OR 和 AND 准则下, 是否考虑 PUEA 的存在对基于能量检测的协作频谱感知接收机工作特性的影响。

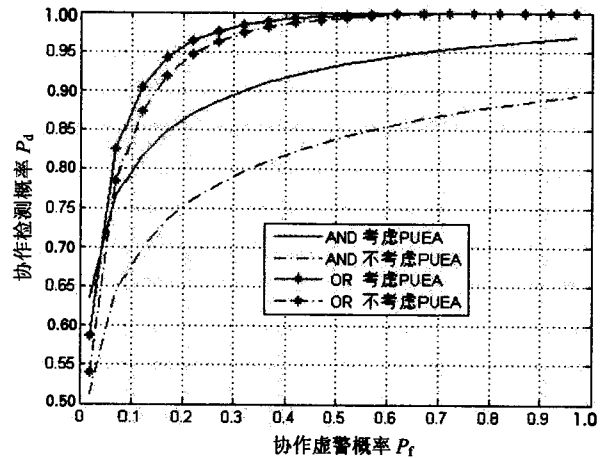


图 2 ROC 特性曲线 ($\alpha = 0.8, N = 5, \tau = 0.02$)

由图可以看出, 在 PUEA 真实存在时, 考虑 PUEA 存在的检测概率较高, 而不考虑 PUEA 存在的检测概率较低。且考虑 PUEA 的存在对 AND 准则的工作特性影响更大。AND 准则下, 考虑 PUEA 的存在比不考虑 PUEA 的存在, 感知的检测概率有明显提高; 而在 OR 准则下, 检测概率的提高不太明显, 随虚警概率的增加, 是否考虑 PUEA 对检测概率的影响越来越小, 当虚警概率大于 0.7 时已经没有影响了。

图 3 显示的是在考虑 PUEA 存在的情况下检测概率与 CR 数量的关系。

由图可以看出, 在考虑 PUEA 存在的情况下, 使用 OR 准则时, 检测概率随 CR 个数的增加而增大; 而使用 AND 准则时, 存在一个最优点使检测概率达到最高。

图 4 显示的是在考虑 PUEA 存在的情况下检测概率与感知时长的关系。

由图可以看出, 在考虑 PUEA 存在的情况下, 检测概率随感知时长的增加而增大。AND 准则下, 检测

性能的提高更加明显。

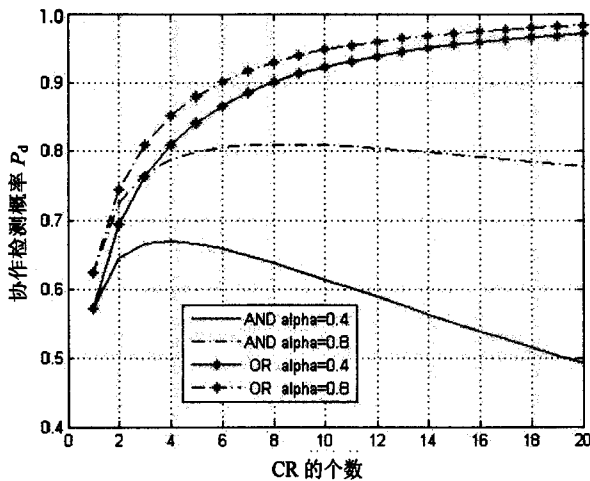


图3 检测概率随CR个数变化的曲线
($P_t = 0.1, \tau = 0.02$)

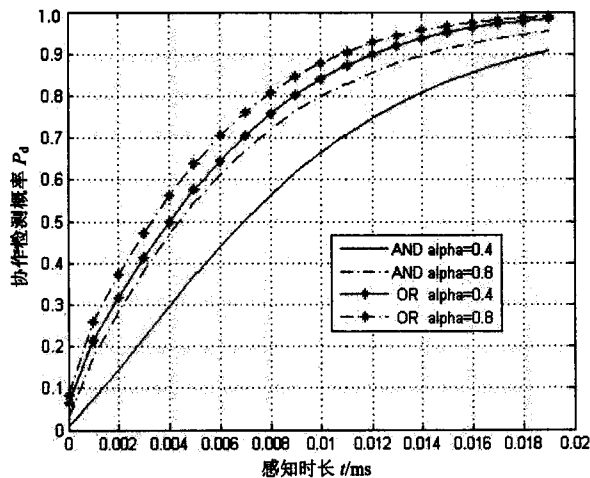


图4 检测概率随感知时长变化的曲线
($P_t = 0.1, N = 5$)

由图3和图4还可以看出,检测性能随 α 的增大而提高,这是因为 α 越大,PUEA在 H_0 情况下出现的概率就越小,对检测性能的影响就越小。

5 结束语

文中研究了考虑PUEA存在情况下的协作频谱感知性能。PUEA能够进行频谱感知和有计划的发送信号。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。文中在OR和AND准则下,对基于能量检测的协作频谱感知系统存在PUEA时的性能进行了分析和仿真。仿真结果表明,考虑PUEA的存在可以有效提高检测性能,尤其在AND准则下效果更明显;且PUEA在 H_0 情况下出现的概率越小,对检测性能的影响越小。

参考文献:

- [1] Andrews J G, Buzzi S, Wan C, et al. What will 5G be? [J]. IEEE Journal on Selected Areas in Communications, 2014, 32 (6): 1065-1082.
- [2] 罗曼. 认知无线电协作频谱感知技术的研究[D]. 哈尔滨: 哈尔滨工业大学, 2015.
- [3] 李佳俊. 认知无线电中协作频谱感知技术研究[D]. 北京: 北京交通大学, 2012.
- [4] Haykin S. Cognitive radio: brain-empowered wireless communications[J]. IEEE Journal on Selected Areas in Communications, 2006, 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] 彭涛, 郭晨, 王文博. 认知无线网络高效协作频谱感知技术[J]. 北京邮电大学学报, 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. [s. l.]: IEEE, 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[J]. IEEE Transactions on Vehicular Technology, 2009, 58(9): 5294-5299.
- [11] Chen Z, Cooklev T, Chen C, et al. Modeling primary user emulation attacks and defenses in cognitive radio networks[J]. Polish Journal of Pharmacology, 2009, 55(2): 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. [s. l.]: [s. n.], 2012: 148-151.
- [14] 董彩萍. 认知无线电中协作频谱感知技术[D]. 成都: 电子科技大学, 2012.
- [15] 梁红玉, 陈宏滨, 赵峰. 认知无线电协作频谱感知技术综述[J]. 广西通信技术, 2011(2): 38-44.
- [16] 杜红. 认知无线电中频谱感知优化与无线资源管理的研究[D]. 北京: 北京邮电大学, 2012.
- [17] 刘仕奇. 基于认知无线电的协作频谱感知技术研究[D]. 广州: 华南理工大学, 2014.