基于信任节点辅助的安全协同频谱感知策略

曾 昆[1] 彭启航[2] 唐友喜[1]
(1. 电子科技大学通信抗干扰技术国家级重点实验室 四川 成都 611731;
2. 电子科技大学通信与信息工程学院 四川 成都 611731)

摘 要: 在认知无线电网络中, 多个用户相互协作进行频谱感知能有效地提高系统感知性能。然而这种协同方式也带来了新的安全隐患: 当恶意用户出现时, 现有协同感知方法无法确保感知结果的鲁棒性。本文针对这一问题, 提出了一种基于信任节点辅助的安全协同感知策略。该策略通过借助网络中信任节点的感知结果, 在用户域和时间域两个维度上消除恶意用户的影响, 确保了算法在较多恶意用户环境中的稳定性。仿真结果表明, 新算法的性能优于 Kaligineedi 所提算法, 在恶意用户数目为网络用户总数一半时, 仍能有效地进行协同感知, 具有良好的鲁棒性。

关键词: 认知无线电; 频谱感知; 协同; 恶意用户; 信任节点辅助
中图分类号: TN92 **文献标识码**: A **文章编号**: 1003-0530(2011)04-0486-05

Secure Cooperative Spectrum Sensing based on Trusted Nodes Assistance

ZENG Kun[1] PENG Qi-hang[2] TANG You-xi[1]
(1. National key Lab of Communications, UESTC, Chengdu, 611731, China;
2. School of Communications and Information Engineering, UESTC, Chengdu, 611731, China)

Abstract: Cooperation among multiple cognitive users provides an improvement for primary user detection. However, this paradigm also poses new security vulnerabilities in cognitive radio system. Specifically, malicious users falsify sensing data can decrease cooperative sensing performance. In this paper, we propose a secure cooperative sensing scheme to resist malicious user attack. The proposed scheme is performed in both user-wise and time-wise detections with trusted nodes assistance, where the stability of the scheme in the context of several malicious users is guaranteed. Simulations show that the performance of our scheme outcomes the one proposed by Kaligineedi. The proposed scheme can work effectively in the scenario where a half of the users are malicious.

Key words: cognitive radio; spectrum sensing; cooperative; malicious users; trusted nodes assistance

1 引言

作为解决无线频谱资源紧缺的新技术,认知无线电[1](Cognitive Radios, CR)通过感知周围频谱环境,机会接入已分配给授权系统,但在某一特定时刻和环境下并未占用的频带,有效地提高了无线频谱的使用效率,正日益受到人们的重视。

为保证不对授权用户造成干扰,可靠地检测频谱使用情况(即频谱感知)是 CR 运用的首要任务。单用户感知由于受无线信道传播特性和感知时间等因素的制约,其性能并不理想。因此,通过网络中多个认知用户的相互协作进行频谱感知的方法受到越来越多的认可。现有研究[2]-[4]表明,用户间合作取得的空间分集能有效提升系统感知性能。

然而,这种协同方式也同样带来了新的安全隐患。由于在协同感知中,各用户首先独自进行本地感知,然后才将结果送至中心节点参与协作。这一过程中心节点对授权频段的实际使用情况缺乏必要的先验信息,无法判断本地感知结果的真实性。因此,一旦存在恶意用户发送错误的感知信息,将会对最终协同感知造成严重的影响。文献[4]的研究表明,当网络中存在恶意用户时(即使是极少数),也会严重恶化系统的感知性能。所以,协同频谱感知的安全问题已成为近期 CR 研究的热点课题[4]-[7]。

Kaligineedi 等人[7]基于"局外人(Outlier)"理论,通过在用户域(user-wise)上的预滤波以及在时间域

收稿日期: 2010 年 10 月 30 日; 修回日期: 2010 年 12 月 8 日
基金项目: 国家自然科学基金(60832007, 60902027, 60572090)和国家重大科技专项(2009ZX03003-008-01)

(time-wise)对每一参与协同的用户分配信任因子进行加权处理,提出了一种安全的协同频谱感知算法。该算法能有效地检测网络中存在的恶意用户,阻止其参与协同,从而避免了它们对系统协同性能造成负面影响。不过,由于总是基于全部用户信息确立比较基准(如预滤波的上下限),对于存在较多恶意用户(>20%)的网络场景,该算法并不稳定。针对这一情况,本文提出了一种更为鲁棒地安全协同感知策略。该策略通过网络中存在的信任节点(如中心节点、基站或者簇节点等)的辅助,在用户域和时间域两个维度上确保了比较基准的准确性。仿真结果证明了新算法的性能优于文献[7],当恶意用户数为网络用户数目比例的 50% 时,新算法仍然能有效地进行协同感知。

本文的其余部分安排如下:第 2 节给出了系统模型;第 3 节分别从用户域和时间域两个角度阐述了基于信任节点的安全协同频谱感知算法;第 4 节是仿真验证;最后是本文结论。

2　系统模型

考虑一个单信道网络(即只存在一个授权用户),包含 N 个认知用户(Cognitive User, CU),如图 1 所示。每一感知时隙结束时,各 CU 将本地感知结果发送至中心节点(被指定的一 CU)。本文假设不同时隙不同 CU 的感知结果相互独立。中心节点根据这些结果经融合做出判决后,再以广播的形式告知各 CU 授权频段的使用情况。上述的信息交换均是基于特定的控制信道完成,不失一般性,本文假设该信道为理想信道。

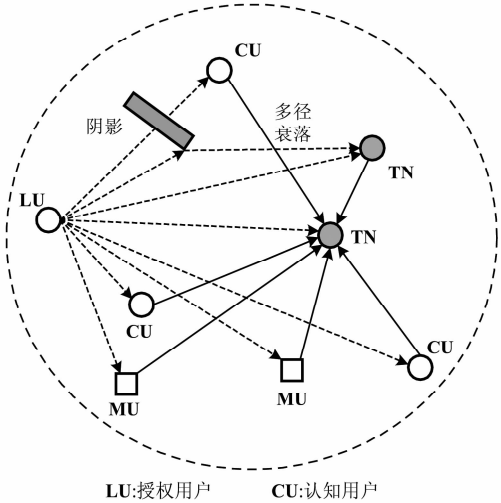


图 1　认知无线电协同频谱感知模型

各 CU 选用能量检测进行本地感知。因此,第 n 个 CU 在第 k 个感知时隙的能量检测输出 $u_n[k]$ 可表示为

$$u_n[k]^{(\mathrm{dB})}=\begin{cases}10\log_{10}\left(\int_{T_k}^{T_k+T-1}|h_n(t)s(t)+z_n(t)|^2dt\right); & \mathbf{H}_1\\ 10\log_{10}\left(\int_{T_k}^{T_k+T-1}|z_n(t)|^2dt\right); & \mathbf{H}_0\end{cases} \tag{1}$$

式中,$\mathbf{H}_1$、$\mathbf{H}_0$ 分别表示授权用户信号的存在、不存在;T 表示感知时隙长度;$s(t)$ 表示授权用户发射信号;$h_n(t)$ 表示授权用户与第 n 个 CU 间的信道增益;$z_n(t)$ 表示第 n 个 CU 处的加性高斯白噪声。

假设各 CU 处的感知信噪比未知,中心节点采用等增益合并(EGC)准则对各 CU 的能量检测值进行处理,如文献[7]。因此,

$$\begin{aligned}&\mathbf{H}_1:\quad \frac{1}{N}\sum_{n=1}^{N}u_n[k]>e_T\\ &\mathbf{H}_0:\quad \frac{1}{N}\sum_{n=1}^{N}u_n[k]\le e_T\end{aligned} \tag{2}$$

式中,e_T 为中心节点处的检测门限。

3　基于信任节点辅助的安全协同感知策略

在实际的网络环境中,由于感知设备故障或者出于某种恶意的动机,部分 CU 隐瞒了本地真实的判决结果,将错误的感知信息送至中心节点。这两种情况都会对中心节点判决的准确性造成影响,不失一般性,本文将这类发送错误感知信息的用户统称为恶意用户[4][5](Malicious Users, MU)。假设第 2 节系统模型中存在 N_0 个这样的 MU。

同样需要注意地是,在实际网络中也会存在一部分 CU,由于网络设计的因素,它们的感知结果在任何时刻都值得信赖,如中心节点自身、基站或簇节点等等,这类用户称为信任节点(Trusted Nodes, TN),同样假设第 2 节模型中 TN 的个数为 N_T,并且相关信息中心节点已知。

接下来,本文将从用户域和时间域分别介绍基于 TN 辅助的安全协同感知策略。

3.1　用户域检测

在协同感知中,每一感知时隙结束时中心节点均会收到来自各 CU 的能量检测值。用户域检测的目的就是从这些检测值中辨识出结果明显异常的用户,禁止它们参与到当次协同中。

令 $S_T\subset\{1,2,\cdots,N\}$ 表示 TN 的集合。根据“局外人”检测[8]理论,在第 k 个感知时隙,用户域检测的上下限 $u_U[k]$、$u_L[k]$ 分别为

$$u_U[k]=u_3[k]+3u_{iqr}[k]$$

$$u_L[k]=u_1[k]-3u_{iqr}[k] \tag{3}$$

式中，$u_1[k]$ 和 $u_3[k]$ 分别表示集合 $\{u_j[k], j\in S_T\}$ 的第一四分位数和第三四分位数；$u_{iqr}[k]=u_3[k]-u_1[k]$ 为 $\{u_j[k], j\in S_T\}$ 的四分位距。

对第 n 个 CU，若下列关系成立

$$u_n[k]\notin[u_L[k], u_U[k]] \tag{4}$$

表明该 CU 的能量检测值超过了用户域检测区间，属于“局外人”，不参与当次协同感知合并。

因此，在第 k 个时隙能参与协同感知的 CU 集合可表示为

$$S(k)\triangleq\left\{i\,|u_i[k]\in\left[u_L[k], u_U[k]\right], i\in\{1,2,\cdots,N\}\right\} \tag{5}$$

定义 $S(k)$ 的势为 $N_{S(k)}$。

3.2 时间域检测

当然仅通过一次检测就判定一个用户是否为 MU，显然不够（因有些 MU 可能在某一时刻未发动攻击，或者有些正常用户感知信道条件恶劣被误判为 MU）。因此，为弥补用户域检测在观测样本上的不足，需要通过多个时隙的检测来消除误差，这就是时间域检测。

首先对网络中每个 CU 均分配一个权值，该权值用于衡量参与协同的感知数据的可靠性，权值越大表明该 CU 的感知数据越可靠。

定义第 n 个 CU 在第 k 个时隙的权值为 $\omega_n[k]$。因此，式(2)所示的合并准则可变换为

$$\begin{aligned}\mathbf{H}_1:&\quad\sum_{n=1}^{N}\omega_n[k]u_n[k]>e_T\\ \mathbf{H}_0:&\quad\sum_{n=1}^{N}\omega_n[k]u_n[k]\le e_T\end{aligned} \tag{6}$$

式中，

$$\sum_{n=1}^{N}\omega_n[k]=1 \tag{7}$$

$$\omega_n[k]=0,\ n\notin S(k) \tag{8}$$

本节剩余部分将介绍如何计算 $\omega_n[k]$，$n\in S(k)$。

初始化 $\omega_n[k]=1/N_{S(k)}$，$n\in S(k)$。在第 k 个时隙，基于各用户的能量检测值，可计算出各自的偏转函数[9]（Deflection function）为

$$d_n[k]=\frac{\left|u_n[k]^{(\mathrm{dB})}-\mu_{S(k)}\right|}{\sigma_{S(k)}},\ n=1,2,\cdots N \tag{9}$$

式中，$\mu_{S(k)}$ 和 $\sigma_{S(k)}$ 分别表示集合 $\{u_{j\in S_T}[k]\}$ 的样本均值和方差。

经 L 个时隙后，第 n 个 CU 的偏转函数的和值

$$D_n[k]=\sum_{k'=k-L+1}^{k}d_n[k'],\ n=1,2,\cdots N \tag{10}$$

该和值在统计意义上表示了时间窗 L 内各 CU 与比较基准的偏离度，值越大表示在时间统计上为 MU 的几率越大。显然，由 $D_n[k]$ 设计满足式(7)、(8)要求的权值 $\omega_n[k]$ 有多种选择，为方便仿真比较，本文采用文献[7]所述的两种设计方案。

方案 1：“局外人”检测

类似第 3.1 节，先根据“局外人”检测理论，求解出第 k 个感知时隙集合 $\{D_n[k]\}$ 的上下限

$$\begin{aligned}D_U[k]&=D_3[k]+1.5D_{iqr}[k]\\ D_L[k]&=D_1[k]-1.5D_{iqr}[k]\end{aligned} \tag{11}$$

式中，$D_1[k]$ 和 $D_3[k]$ 分别表示集合 $\{D_j[k], j\in S_T\}$ 的第一四分位数和第三四分位数；$D_{iqr}[k]=D_3[k]-D_1[k]$ 为四分位距。

若第 n 个 CU 的偏转函数的和值 $D_n[k]$ 落在上下限的区间内，则对其分配相等的权值，反之则视为 MU，禁止参与协同，即

$$\omega'_n[k]=\begin{cases}1: D_n[k]\in[D_L[k], D_U[k]], n\in S(k)\\ 0: \text{其他}\end{cases} \tag{12}$$

式中，$\omega'_n[k]$ 表示尚未归一化的权值。

方案 2：基于指数衰减函数的加权

数值 $D_n[k]$ 表示时间域上各 CU 与比较基准的偏离度，不妨假设相应的权值与该偏移距离成指数衰减。因此，第 n 个 CU 在第 k 个时隙的未归一化权值可表示为

$$\omega'_n[k]=\begin{cases}\exp\left(-\left|m_D[k]-D_n[k]\right|\right): n\in S(k)\\ 0: \text{其他}\end{cases} \tag{13}$$

式中，$m_D[k]$ 表示集合 $\{D_j[k], j\in S_T\}$ 的中位数[8]。

最后，对 $\omega'_n[k]$ 进行归一化处理，即

$$\omega_n[k]=\frac{\omega'_n[k]}{\sum_{n'=1}^{N}\omega'_n[k]} \tag{14}$$

4 仿真验证

本节基于 MATLAB 平台进行了仿真。

考虑图 1 所示的单信道网络，包含 $N=50$ 个 CU，其中 MU 和 TN 的个数分别为 N_0、N_T。授权用户信号为 QPSK 调制，$\Pr(\mathbf{H}_1)=0.2$。不考虑感知信道的阴影效应，各 CU 的感知信噪比假设相等，为 −10dB。能量检测的采样点数 $T=50$。时间域检测的感知时隙个数 $L=50$。

本文讨论两种典型的 MU：始终占用（Always Busy，AB）和始终空闲（Always Free，AF）[4][7]。在仿真中，始终占用类的 MU 的能量检测值为检测门限（e_T）的 2 倍，即高于门限 3dB；而始终空闲类的 MU 的能量检测值为

检测门限的一半,即低于门限 3dB。此外,算法的时间域检测部分均是选择方案 1:“局外人”检测来获取未归一化权值。

4.1　有效性

图 2 和图 3 分别给出了两种典型 MU 场景中系统的感知性能曲线,P_{FA} 表示系统虚警概率,P_D 表示系统检测概率,并且与(1)理想环境中($N-N_0$)个正常 CU;(2)同样 MU 场景中无任何安全措施;两种情况下的感知性能曲线进行了对比。仿真中,MU 和 TN 在网络用户数中的比例均假设为 10%,即 $N_0=N_T=5$。

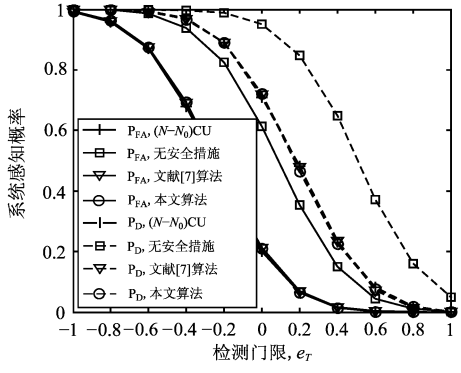


图 2　存在 10% 的 CU 为始终占用类 MU 时协同频谱感知的系统性能,$N_0=N_T=5$

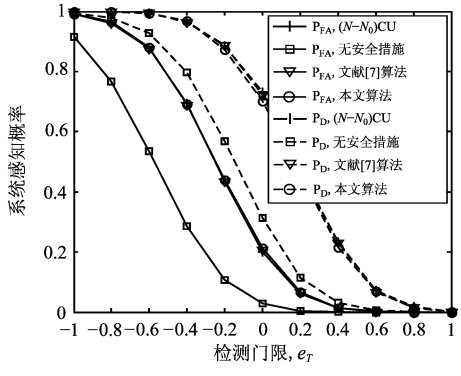


图 3　存在 10% 的 CU 为始终空闲类 MU 时协同频谱感知的系统性能,$N_0=N_T=5$

由图可知,文献[7] Kaligineedi 所提算法和本文算法的性能曲线基本与理想环境中($N-N_0$)个正常 CU 合并的性能曲线重合。这表明,两种算法均成功检测出网络中存在的 MU,通过摒弃它们的感知结果,确保了协同感知的稳定性。

4.2　鲁棒性

图 4 研究了算法的系统感知性能与网络中 MU 比例的变化关系,仿真中 MU 为始终占用类,检测门限 e_T 设置为使得理想环境中 N 个正常 CU 合并的系统虚警概率为 0.01,TN 的数目为 $N_T=5$。同样地,图 4 给出了(1)理想环境中($N-N_0$)个正常 CU;(2)同样 MU 场景中无任何安全措施;两种参照场景。

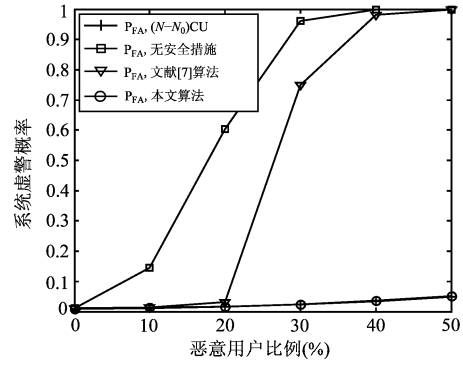


图 4　当 MU 为始终占用类时,系统虚警概率与 MU 比例的变化关系,$N_T=5$

从图中可以看到,当网络中 MU 比例未超过 20% 时,Kaligineedi 和本文所述的两种算法均工作正常。然而,当网络中 MU 数目不断增多,由于缺乏 TN 辅助,Kaligineedi 算法因比较基准失真,性能急剧恶化。本文所述算法在网络中存在半数的 MU 时,性能仍与理想环境中($N-N_0$)个正常 CU 合并的性能曲线吻合,表现了良好地鲁棒性。MU 为始终空闲类时的曲线(即系统检测概率与 MU 比例的变化关系)得到的结论类似,本文就没有一并给出。

4.3　算法性能与信任节点比例的关系

图 5 给出了算法性能与网络中信任节点比例的关系曲线。仿真条件与图 4 仿真类似。考虑三种不同比例 MU 的网络场景,分别为 10%、30% 及 50%,具体对应的 MU 数量 $N_0=5$、15、25。

由图 5 可以看出,当网络中大致有 10% 的 TN 时,算法在三种场景下性能均能够保持稳定,而当 TN 的比例较少(<10%)时,受到“局外人”检测理论对少样本数存在局限性的影响[8],本算法也会出现相应的性能损失。

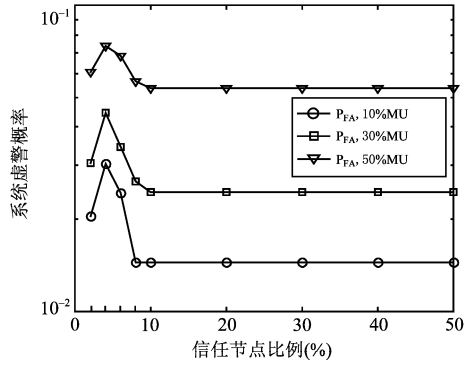


图 5　当 MU 种类为始终占用类时,系统虚警概率与 TN 比例的变化关系

5 结束语

针对认知无线电网络协同频谱感知恶意用户攻击的问题,本文提出了一种安全的协同感知策略。该策略基于网络中存在的信任节点的辅助,在用户域和时间域两个维度上设计了鲁棒地频谱感知策略,有效地解决了多恶意用户(>20%)场景下 Kaligineedi 算法不稳定的问题。计算机仿真显示,本文所述算法在恶意用户数为用户总数一半时,仍能有效地进行协同感知。

参考文献

[1] Mitola J. Cognitive radio architecture evolution [J]. Proc. of the IEEE, 2009, 97(4): 626-641.

[2] 郑学强,王金龙,吴启晖等. 基于 Dempster-Shafer 证据理论的协同频谱感知算法 [J]. 信号处理, 2009, 25(10): 1532-1536.
Zheng X, Wang J, Wu Q, et al. Cooperative spectrum sensing algorithm based on Dempster-Shafer theory in cognitive radio systems [J]. Signal Processing, 2009, 25(10): 1532-1536.

[3] Letailef K, Zhang W. Cooperative communications for cognitive radio networks [J]. Proc. of the IEEE, 2009, 97(5): 878-893.

[4] Mishra S, Sahai A, Brodersen R. Cooperative sensing among cognitive radios [C]. IEEE ICC, Istanbul, Turkey, 2006.

[5] Chen R, Park J, Hou Y, et al. Toward secure distributed spectrum sensing in cognitive radio networks [J]. IEEE Commun. Magazine, 2008, 46(4): 50-55.

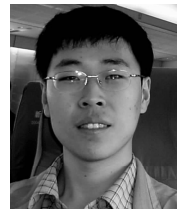
[6] Wei J, Zhang X. Two-tier optimal cooperation based secure distributed spectrum sensing for wireless cognitive radio networks [C]. IEEE INFOCOM, San Diego, USA, 2010.

[7] Kailigineedi P, Khabbazian M, Bhargava V. Secure cooperative sensing techniques for cognitive radio systems [C]. IEEE ICC, Beijing, China, 2008.

[8] Rousseeuw P, Leroy A. Robust regression and outlier detection [M]. Wiley Publication, 2003.

[9] Bronshtein I, Semendyayev K, and Musiol G, et al. Handbook of mathematics (Fifth Edition) [M]. Springer Publication, 2007.

作者简介



曾 昆(1981-),男,湖北钟祥人,博士生,主要研究方向为认知无线电频谱感知关键技术研究。
E-mail: zengkun@uestc.edu.cn

彭启航(1982-),女,四川蓬溪人,讲师,主要研究方向为认知无线电物理层关键技术研究,无线传感器网络等。

唐友喜(1964-),男,河南潢川人,教授,博士生导师,主要研究方向为通信系统中的信号检测与处理、认知无线电等。