中国科学: 信息科学 2016 年 第 46 卷 第 6 期: 789–799
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
论 文

一种基于信号循环平稳特征的抵御恶意模仿主用户攻击协作频谱检测算法

马彬[①②], 方源[①②*], 谢显中[①②]

① 重庆邮电大学宽带接入网研究所, 重庆 400065
② 重庆邮电大学重庆市计算机网络与通信技术重点实验室, 重庆 400065
* 通信作者. E-mail: fy498441454@126.com

收稿日期: 2015–09–07; 接受日期: 2015–10–20; 网络出版日期: 2016–04–13
国家自然科学基金 (批准号: 61271259, 61301123, 61471076)、重庆市基础与前沿研究计划 (批准号: cstc2015jcyjA40047)、重庆市计算机网络与通信技术重点实验室基金 (批准号: CY-CNCL-2010-02) 和重庆邮电大学博士启动资金 (批准号: A2015-16) 资助项目

摘要 现有的抵御恶意模仿主用户攻击 (PUEA) 算法大多基于能量检测, 有着应用环境特殊, 易被模仿等缺点. 针对上述情况, 本文提出了一种基于信号循环平稳特征的抵御 PUEA 协作频谱检测算法, 该算法通过对次用户的本地判决结果进行统计分析, 并与不含恶意用户情况下的理论统计特性作比较, 来识别系统是否受到恶意用户攻击. 仿真结果表明, 该算法在保证良好的频谱检测性能的同时可以有效抵御 PUEA, 是一种简单有效的抵御策略.

关键词 认知无线电 协作频谱检测 恶意模仿主用户攻击 循环平稳特征 频谱决策协议

1 引言

认知无线电 (cognitive radio, CR) 技术作为一种动态频谱再利用技术, 可以提高稀缺频谱资源利用率 [1]. CR 中存在两种类型的用户, 一种是对频谱具有绝对使用权的主用户 (primary user, PU), 另一种是次用户 (secondary user, SU), SU 主动检测 PU 的授权频段, 如果频谱空闲 (即 PU 没有使用该频段), 那么 SU 就伺机接入. 但是如果频谱空闲时存在恶意模仿主用户攻击 (primary user emulation attacks, PUEA) 时, 恶意用户 (malicious user, MU) 通过模仿主用户信号导致次用户的频谱检测结果为频谱繁忙 (即 PU 正在使用该频段), 导致次用户放弃接入该频段, 严重降低了频谱利用率 [2]. 因此, 如何抵御 PUEA 是当今认知无线电频谱检测的研究热点之一.

现有的抵御 PUEA 方法主要分为以下两种类型: 基于定位的检测技术与定位无关的检测技术. 基于定位的检测技术通过对接收信号的发送者进行定位, 并和主用户位置进行对比来判断信号发送者是否是主用户信号, 但是基于定位的方法在攻击者位于主用户附近时将失效 [3,4]. 在定位无关的检测技术中, 基于能量检测的抵御机制被广泛研究 [5~9]. 文献 [5] 利用 SU 的接收功率和感知节点之间的距离来进行对数正态和分布的估计, 减少 PUEA 对系统的影响. 文献 [6] 提出了一种利用小区位置可信度

引用格式: 马彬, 方源, 谢显中. 一种基于信号循环平稳特征的抵御恶意模仿主用户攻击协作频谱检测算法. 中国科学: 信息科学, 2016, 46: 789–799, doi: 10.1360/N112015-00168

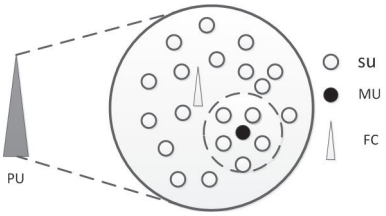

图 1　系统模型

Figure 1　The system model

和恶意用户行为分析的方法来提高对恶意用户的检测. 文献 [7] 提出了根据信道状态信息为每个 SU 的感知节点提供权重来获得最佳融合判决结果, 进一步提高了基于协作频谱检测的抵御 PUEA 性能. 文献 [8] 中, Jin 提出了一种利用单个 SU 判决结果的中心式方法进行合作判决的 PUEA 抵御机制, 与基于能量检测的单个 SU 抵御机制相比提升了性能. 文献 [9] 考虑了次用户移动场景下的基于能量检测和方差检测的协作频谱检测.

能量检测在被广泛考虑的同时也存在着一些局限性. 首先, 应用环境特殊, 能量检测中需假设主用户和 PUEA 的信道传输模型不同、发射功率不同、不考虑噪声等加性干扰 [5~9]; 其次, 判决门限难以确定 [10], 能量检测的判决门限易随信号传输信道的状况变化而变化; 最后, 基于能量检测的次用户判决统计量是信号的接收功率, 很容易被恶意用户模仿, 此时能量检测将失效 [11]. 而调制信号的循环平稳特征与周期性的余弦载波、重复扩展、脉冲、跳频序列或者循环前缀等多种因素有关, 导致信号的循环平稳特征稳定且复杂, 相比于信号功率, 更难被恶意用户模仿 [11]. 主要的信号循环平稳特征检测有两种, 一种是单循环频率检测 (single-cycle detector, SC), 即 SU 检测 PU 信号在单个循环频率处的循环平稳统计特性; 另一种是多循环频率检测 (multi-cycle detector, MC), 即 SU 检测 PU 信号在其全部循环频率处的循环平稳统计特性. 当信号有多个有效循环频率时, MC 检测多个循环频率可以实现高准确率的频谱检测, 是最优的循环平稳特征检测方法 [12], 但是由于要遍历多个循环频率, 存在着计算复杂度高的缺点.

本文提出了一种基于信号循环平稳特征的抵御 PUEA 协作频谱检测方案, 采用循环平稳特征频谱检测可以克服现有能量检测的缺点, 并且将次用户的本地检测统计结果与理论统计结果进行对比来识别出 PUEA, 是一种简单有效的抵御 PUEA 策略. 本文的主要贡献可以概括为以下两点.

(1) 提出了一种混合循环频率协作频谱检测方法. 次用户本地判决时采用 SC, 并将判决结果发送给融合中心 (fusion center, FC), FC 通过对判决结果进行统计分析, 相当于在 FC 处实现了 MC, 该混合循环频率协作频谱检测结合了 SC 计算复杂度低和 MC 检测准确率高的优点, 但是相对于传统的能量检测更容易发生误检情况, 并且计算复杂度较高.

(2) 提出了一种简单且有效的抵御 PUEA 策略, 该策略通过对次用户的判决结果进行统计分析, 在与不含恶意用户下的理论统计结果进行比较, 来确定发射信号是否为恶意用户, 该策略适用于常用的无线环境, 且本地检测门限采用一定的范围值, 检测结果更加准确.

2　系统模型

本文考虑了如图 1 所示的场景, 认知用户和恶意用户位于距离主用户一定距离的区域内, 该区域内含有一个融合中心, 用于收集次用户返回的本地判决结果, 主用户信号是一般的电视信号.

(1) 认知区域内次用户数目为 n, SU 的位置服从参数为 λ 的 Poisson 分布 [13].

(2) 本文采用有限移动网络 [13], 即 SU 和 MU 只在覆盖区域内自由移动, 各个用户所处的位置和检测结果相互之间统计独立.

(3) 主用户为电视塔, 其信号有着稳定的循环平稳特征, 由于主用户位置固定且常为地标性建筑, 其位置信息被次用户和恶意用户所熟知.

(4) 次用户为移动手机用户, 自带定位模块, 即可以获得自己的位置信息 [4].

(5) 恶意用户是一种存在恶意攻击行为特殊次用户, 其通过模仿主用户信号的发射功率等信号信息进行 PUEA 攻击, 由于电源的限制, 单个恶意用户的影响范围有限, 如图 1 中虚线圆所示. 本文考虑复杂的恶意模仿主用户攻击, 即当 PU 存在时, MU 将不发射干扰信号; PU 不存在时, MU 以一定概率发射干扰信号.

CR 网络中 SU 的检测周期内, 存在恶意用户情况下的系统模型可以转化为如下三元假设, 其中 H_0 状态表示不存在用户信号, H_1 状态表示存在主用户信号, H_2 状态表示存在恶意用户信号, 即发生 PUEA, SU 接收到的信号 $y(t)$ 经采样之后得到式 (1):

$$y[m]=\begin{cases} n[m], m=1,2,\ldots,N_s, & H_0,\\ d_{\mathrm{PU}}^{-\alpha}x_{\mathrm{PU}}[m]+n[m], m=1,2,\ldots,N_s, & H_1,\\ d_{\mathrm{PUEA}}^{-\alpha'}x_{\mathrm{PUEA}}[m]+n[m], m=1,2,\ldots,N_s, & H_2, \end{cases} \tag{1}$$

N_s 表示采样点数, $y[m]$ 为 SU 的接收信号, $x_{\mathrm{PU}}[m]$ 为 PU 的发射信号, $x_{\mathrm{PUEA}}[m]$ 为恶意用户信号, d_{PU} 表示次用户到主用户的距离, d_{PUEA} 表示次用户到恶意用户的距离, α 为主用户到次用户之间的路径损耗系数, α' 为次用户到恶意用户之间的路径损耗系数, $n[m]$ 为复 Gauss 白噪声, 服从均值为 0, 方差为 σ^2 的 Gauss 分布.

3 协作频谱检测

3.1 循环平稳特征

循环平稳信号是一种统计特性随时间周期性变化的随机信号 [13]. 设随机过程 $x(t)$, 如果其均值 $m_x(t)$ 和自相关函数 $R_x(t)$ 在一段时间内具有周期性, 则称 $x(t)$ 广义循环平稳. 由于 $R_x(t)$ 具有周期特性, 可将其展开为 Fourier 级数形式, 得到式 (2):

$$R_x\left(t+\frac{\tau}{2},t-\frac{\tau}{2}\right)=\sum_{\alpha_k}R_x^{\alpha_k}(\tau)\mathrm{e}^{\mathrm{j}2\pi\alpha_k t}, \tag{2}$$

其中 $\alpha_k=k/T(k=0,1,2,\ldots)$ 称为信号的循环频率, $k=0$ 时, 循环自相关函数就是传统意义上的自相关函数. $R_x(t)$ 是 Fourier 级数的系数, 称为循环自相关系数 (cyclic autocorrelation function, CAF), 可由式 (3) 计算得到

$$R_x^{\alpha_k}(\tau)=\frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}}R_x\left(t+\frac{\tau}{2},t-\frac{\tau}{2}\right)\mathrm{e}^{-\mathrm{j}2\pi\alpha_k t}\mathrm{d}t. \tag{3}$$

若信号具有循环遍历性, 统计平均可以由时间平均来代替, 有

$$R_x^{\alpha_k}(\tau)=\lim_{T\to\infty}\frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}}x\left(t+\frac{\tau}{2}\right)x^*\left(t-\frac{\tau}{2}\right)\mathrm{e}^{-\mathrm{j}2\pi\alpha_k t}\mathrm{d}t, \tag{4}$$

其中, $t=m\Delta t$ (Δt 是采样周期, $m=1,2,\ldots,N_s$), $T=N_s\Delta t$ (N_s 是采样数), $T_c=M\Delta t$ (T_c 是码片或位长) 对 $R_x(t)$ 求离散形式, 得到

$$R_x^{\alpha_k}\simeq\frac{1}{N_s}\sum_{m=1}^{N_s}|x\,[m]|^2\mathrm{e}^{-\mathrm{j}2\pi\alpha_k' m}, \tag{5}$$

其中 $\alpha_k'=\frac{k}{M}(k=0,1,2,\ldots)$.

在循环平稳特征检测中, 判决统计量的选取往往与循环自相关系数有关. 合适的判决统计量不仅可以显著地减少运算量, 而且可以实现更好的检测性能. 本文采用 CAF 的离散形式 $Y_{\alpha_k'}^i$ 作为判决统计量, 考虑实际情况中的路径损耗和传输距离得到下式:

$$Y_{\alpha_k'}^i=R_x^{\alpha_k'}(\tau=0)\simeq\frac{d^{-\alpha}}{N_s}\sum_{m=1}^{N_s}|x\,[m]|^2\mathrm{e}^{-\mathrm{j}2\pi\alpha_k' m}, \tag{6}$$

其中 $Y_{\alpha_k'}^i$ 表示次用户 i 在循环频率 α_k' 处的 CAF, d 为接收机和发射机的距离, α 为接收机和发射机之间的路径损耗. 当信号在某个的循环频率处的 CAF 大于一定阈值 η 时, 称该循环频率为有效循环频率.

3.2 循环自相关系数的统计特性分析

本文中假设噪声 $n(t)$ 是服从均值为 0, 方差为 σ^2 的复 Gauss 白噪声, 即 $n[m]=n_r[m]+\mathrm{j}n_i[m]$, 有 $\mathrm{E}\{|n[m]|^2\}=\sigma^2$, $\mathrm{var}\{|n[m]|^2\}=\mathrm{var}\{n_r[m]^2+n_i[m]^2\}=\sigma^4$. 假设信号 $x(t)$ 与噪声 $n(t)$ 相互独立, 则 $\mathrm{E}\{|x[m]+m[m]|^2\}=|x[m]|^2+\sigma^2$.

当不存在 PU 时, 根据中心极限定理, 当 $N_s\gg1$ 时, $Y_{\alpha_k'}^i$ 近似服从 Gauss 分布 [14], 有 $\alpha_k'=\frac{k}{M}$, $\sum_{m=1}^{M}\mathrm{e}^{-\mathrm{j}2\pi\frac{k}{M}m}=0$, $N_s=N_cM$, 所以其分布的均值和方差为

$$E\left\{Y_{\alpha_k'}^i|H_0\right\}=\frac{\sigma^2}{N_s}\sum_{m=1}^{N_s}\mathrm{e}^{-\mathrm{j}2\pi\alpha_k' m}=0, \tag{7}$$

$$\mathrm{var}\left\{Y_{\alpha_k'}^i|H_0\right\}=\frac{1}{N_s^2}\sum_{m=1}^{N_s}\left|\mathrm{e}^{-\mathrm{j}2\pi\alpha_k' m}\right|^2\mathrm{var}\left\{|n[m]|^2\right\}=\frac{\sigma^4}{N_s}. \tag{8}$$

当 PU 存在时, 根据中心极限定理, 当 $N_s\gg1$ 时, $Y_{\alpha_k'}^i$ 近似服从 Gauss 分布 [14], 所以其分布的均值和方差为

$$E\left\{Y_{\alpha_k'}^i|H_1\right\}=E\left\{\frac{1}{Ns}\sum_{m=1}^{N_s}\left(|x\,[m]|^2+\sigma^2\right)\mathrm{e}^{-\mathrm{j}2\pi\alpha_k' m}\right\}=E\left\{\frac{1}{N_s}\sum_{m=1}^{N_s}|x\,[m]|^2\mathrm{e}^{-\mathrm{j}2\pi\alpha_k' m}\right\}=P_{\alpha_k'}, \tag{9}$$

$$\mathrm{var}\left\{Y_{\alpha_k'}^i|H_1\right\}=\frac{1}{N_s^2}\sum_{m=1}^{N_s}\left|\mathrm{e}^{-\mathrm{j}2\pi\alpha_k' m}\right|^2\mathrm{var}\left\{|x[m]+n[m]|^2\right\}=\frac{2P\sigma^2+\sigma^4}{N_s}, \tag{10}$$

其中 $P_{\alpha_k'}$ 代表信号在循环频率 α_k' 处的功率值, $P=\frac{1}{N_S}\sum_{m=1}^{N_s}|x[m]|^2$.

考虑实际环境中的路径损耗, 式 (9) 和 (10) 改写为

$$\begin{cases}\mu_{\mathrm{PU}}=E\left\{\dfrac{d_{\mathrm{PU}}^{-\alpha}}{N_s}\displaystyle\sum_{m=1}^{N_s}|x_{\mathrm{PU}}\,[m]|^2\mathrm{e}^{-\mathrm{j}2\pi\alpha_k' m}\right\}=P_{t(\mathrm{PU})_{\alpha_k'}}d_{\mathrm{PU}}^{-\alpha},\\ \sigma_{\mathrm{PU}}^2=\dfrac{d_{\mathrm{PU}}^{-\alpha}}{N_s^2}\displaystyle\sum_{m=1}^{N_s}\left|\mathrm{e}^{-\mathrm{j}2\pi\alpha_k' m}\right|^2\mathrm{var}\left\{|x_{\mathrm{PU}}[m]+n[m]|^2\right\}=\dfrac{2P_{t(PU)}d_{\mathrm{PU}}^{-\alpha}\sigma^2+\sigma^4}{N_s},\end{cases} \tag{11}$$

其中 PU 发射功率 $P_{t(\mathrm{PU})}=\frac{1}{N_s}\sum_{m=1}^{N_s}|x_{\mathrm{PU}}[m]|^2$, d_{PU} 为该次用户到主用户的距离, α 为接收机和发射机之间的路径损耗.

3.3 次用户本地判决

当信号有多个有效循环频率时, 多循环频率检测是最优的检测方法 [12], 但是为了降低本地检测复杂度, 本地采用次优的单循环频率检测. 即次用户随机计算某个循环频率处的 CAF 并进行本地判决, 然后将此循环频率值和判决结果一起发送给融合中心.

由于主用户信号的循环平稳特征稳定, 所以循环频率处的 CAF 将收敛于一定范围之内. 本文认为当次用户检测的 CAF 值符合下式时, 判决为主用户信号:

$$\mu_{\mathrm{PU}}-A\sigma_{\mathrm{PU}}\leqslant Y^i_{\alpha'_k}\leqslant\mu_{\mathrm{PU}}+A\sigma_{\mathrm{PU}}. \tag{12}$$

所以对应在循环频率 α'_k 处的检测概率为

$$\begin{aligned}P_{d\alpha'_k}&=\Pr\left\{\mu_{\mathrm{PU}}-A\sigma_{\mathrm{PU}}\leqslant Y^i_{\alpha'_k}\leqslant\mu_{\mathrm{PU}}+A\sigma_{\mathrm{PU}}\right\}\\&=Q\left(-A\right)-Q\left(A\right),\end{aligned} \tag{13}$$

其中 $Q\left(x\right)=\frac{1}{\sqrt{2\pi}}\int_x^\infty\exp(-\frac{t^2}{2})$.

当预设目标检测概率 $P^{\mathrm{DES}}_{d\alpha'_k}$ 确定时可以求得 A 的值, 例如通常 $P^{\mathrm{DES}}_{d\alpha'_k}=0.9$ [15], 本文设置 $P^{\mathrm{DES}}_{d\alpha'_k}=0.9$, 此时 $A=2.3$.

由于 $\{Y^i_{\alpha'_k}|H_0\}$ 为一 Gauss 过程, 同理得到虚警概率:

$$\begin{aligned}P_{f\alpha'_k}&=\Pr\left\{\mu_{\mathrm{PU}}-A\sigma_{\mathrm{PU}}\leqslant Y^i_{\alpha'_k}\leqslant\mu_{\mathrm{PU}}+A\sigma_{\mathrm{PU}}\right\}\\&=Q\left(\frac{\mu_{\mathrm{PU}}-A\sigma_{\mathrm{PU}}}{\sigma_0}\right)-Q\left(\frac{\mu_{\mathrm{PU}}+A\sigma_{\mathrm{PU}}}{\sigma_0}\right),\end{aligned} \tag{14}$$

其中 $\sigma_0^2=\mathrm{var}\{Y^i_{\alpha'_k}|H_0\}=\frac{\sigma^4}{N_s}$.

当次用户检测循环频率 α'_k 处的 CAF 符合式 (12) 时, 向 FC 发送 $\{\alpha'_k,1\}$, 若不符合, 则发送 $\{\alpha'_k,0\}$.

3.4 融合中心处融合判决算法

由于次用户数目远大于信号的有效循环频率数, 可以认为每个有效循环频率都至少被一个次用户检测到, 即 FC 可以获得全部的有效循环频率和其对应的判决结果, 相当于在 FC 处实现了多循环频率检测, 实现了最优的循环平稳特征检测.

不同信号有不同的有效循环频率, 现在对有多个有效循环频率的主用户信号频谱检测的情景进行分析. 假设认知无线电网络中有 10 个次用户, 主用户信号有 3 个有效循环频率 $\alpha_1,\alpha_2,\alpha_3$. 当 PU 存在时, 10 个 SU 返回给 FC 的数据为 $\{(\alpha^1,1),(\alpha^2,1),(\alpha^3,1)\cdots(\alpha^{10},1)\}$. 由于次用户随机选择一个有效循环频率, 可以认为 10 个次用户返回的结果中含有全部的 3 个有效循环频率, 假如结果如下:

(1) 检测有效循环频率的次用户编号是 1, 3, 6: $\{(\alpha^1_1,1),(\alpha^3_1,1),(\alpha^6_1,1)\}$;

(2) 检测有效循环频率的次用户编号是 2, 7, 8, 9: $\{(\alpha^2_2,1),(\alpha^7_2,1),(\alpha^8_2,1),(\alpha^9_2,1)\}$;

(3) 检测有效循环频率的次用户编号是 4, 5, 10: $\{(\alpha^4_3,1),(\alpha^5_3,1),(\alpha^{10}_3,1)\}$.

FC 对次用户返回的结果进行检验分析, 由于 FC 已知 PU 信号的循环平稳特征, 当次用户返回的结果中, 包含主用户信号的全部有效循环频率且对应的判决结果为 1 时, 则认为检测到主用户信号.

4 抵御 PUEA 策略

恶意用户通过模仿主用户信号, 可以使次用户在进行本地检测时误认为其为主用户信号, 影响本地检测结果进而影响 FC 的最终判决结果, 达到占用频谱资源的目的. 针对此情况, 本文提出了一种基于对本地检测结果进行分析对比的抵御 PUEA 策略.

当用户可以在认知区域内自由移动时, 可以认为任意一个次用户出现在任意位置的概率服从 Poisson 分布 [13]. 用 V 表示当主用户存在时发生漏检的次用户数目, 各个次用户发生漏检的概率相互独立, 并且次用户的数目是一个 Poisson 变量. 根据 Bernoulli 过程, 所以 V 也是一个以 nP_{miss} 为参数的 Poisson 分布, 则次用户中发生漏检的次用户均值 μ_V 和方差 σ_V^2 满足

$$\mu_V = \sigma_V^2 = nP_{\text{miss}}, \tag{15}$$

其中 $P_{\text{miss}} = 1 - P_{d\alpha_k'}$, 由于主用户信号的循环平稳特征稳定, 所以其均值 μ_V 和方差 σ_V^2 收敛于一定范围.

用 L 表示主用户不存在时发生虚警的次用户数目, 同理有, 次用户中发生虚警的次用户均值 μ_V, 方差 σ_V^2 满足

$$\mu_L = \sigma_L^2 = nP_{f\alpha_k'}. \tag{16}$$

由于虚警概率与噪声有关, 所以其均值 μ_L 和方差 σ_L^2 收敛于一定范围.

当不存在恶意用户时, 根据式 (15) 的 μ_V 和 σ_V^2, 可以估计 PU 存在时, 成功检测到 PU 的次用户数目: 同理, 根据式 (16) 的 μ_L 和 σ_L^2, 可以估计 PU 不存在时, 由于虚警而检测到 PU 的次用户数目. 因此, 可以根据每次判决结果为 PU 的次用户数目 N_g 来识别此时的发射信号是否是 PUEA.

当存在 PU 时, N_g 是次用户中成功检测到主用户的数目, 满足

$$N_g \geqslant N_d = n - \lceil \mu_V \rceil - \lceil B\sigma_V \rceil, \tag{17}$$

其中 $\lceil \cdot \rceil$ 表示向上取整数, 系数 B 可由实验得到.

当不存在 PU 时, N_g 是次用户中发生虚警的数目, 满足

$$N_g \leqslant N_f = \lceil \mu_L \rceil + \lceil C\sigma_L \rceil, \tag{18}$$

其中, 系数 C 可由实验得到.

当存在 MU 时, N_g 是受 PUEA 影响导致 SU 检测到 PU 的数目, 若满足

$$N_f < N_g < N_d. \tag{19}$$

即同时不满足式 (17) 和 (18), 则认为此检测周期内的发射信号为 MU, 这是由于主用户信号和噪声信号稳定, 每次检测中有很大的概率满足式 (18) 和 (19).

然而, 如果受 PUEA 影响的次用户数目很少时, 可能满足式 (18); 或者受 PUEA 影响的次用户数目很多时, 可能满足式 (17), 此时该方法则检测不出恶意攻击者. 但是值得注意的是, 当系统环境良好时, N_f 值较小而 N_d 值较大, 本文的抵御策略可以抵挡很大一部分的 PUEA.

当存在恶意用户时, 可以用 PUEA 对系统造成的恶意影响概率 P_m 来反映系统受 MU 影响的程度:

$$P_m = \frac{N_g}{n}. \tag{20}$$

表 1 主要参数

Table 1 The main parameters

Parameter	Value	Parameter	Value
n	200	f_s	50 MHZ
a	2.3	f_c	4 MHZ
α	3.5	f_d	1 Mbps
α'	3.5	N_s	51200

算法描述如下:

(1) 次用户遍历循环频率, 任选其中一个有效循环频率, 并根据式 (12) 进行本地判决, 将判决结果 $(\alpha,1)$ 或 $(\alpha,0)$ 发送给融合中心;

(2) 融合中心统计分析次用户发送的本地判决结果, 根据 3.4 小节的融合规则来判决是否含有主用户;

(3) 如果 FC 判决结果为含有主用户, 则统计分析次用户发送的本地判决结果中 $(\alpha,1)$ 的数目 N_g, 并且根据式 (17) 和 (18) 计算出 N_d 和 N_f;

(4) 融合中心将 N_g 与 N_f、N_d 比较, 若满足式 (17) 或 (18), 则认为是主用户信号, 否则判决为恶意用户.

5 实验仿真

本文考虑一个含有 $n=200$ 个次用户, $m=1$ 个恶意用户的 CR 网络区域, 该区域以 $(0,0)$ 为圆心, 半径 $r=200$ 的圆形区域. FC 位于圆心 $(0,0)$ 处, 主用户位于 $(0,2000)$ 处, 主用户信号采用 BPSK 调制, 工作在电视频谱频段. 根据式 (13), 当预设目标检测概率 $P_{d\alpha_k'}^{\mathrm{DES}}=0.9$ [15], 可以求得 $A=3$, 利用 MATLAB 进行仿真, 详细参数如表 1 所示.

图 2 表示不存在 PUEA 时, 在 SNR $=-20$ dB 情况下, 信号进行不同数目的有效循环频率检测时的 ROC 曲线. 图中可以看出, 随着信号的有效循环频率数目的增多, 相同虚警概率下的检测概率有所下降. 这是由于在本文的融合算法中, 如果 PU 信号含有多个有效循环频率, 只有在各个有效循环频率处的 CAF 都满足式 (12) 时, 才可以判定为主用户, 因此系统检测概率 $P_d=P_{d\alpha_1}\times P_{d\alpha_2}\times\cdots\times P_{d\alpha_k}$, 其中 $P_{d\alpha_k}$ 表示在有效循环频率 α_k 处的检测概率, $k=1,2,\ldots$, $P_{d\alpha_k}\in[0,1]$, 所以当 PU 含有多个有效循环频率时, 检测概率会有一定程度的下降.

图 3 表示本文的频谱检测方案与传统能量检测方案的误检概率对比. 误检概率 $P_e=P_1\cdot P_{\mathrm{miss}}+P_2\cdot P_f$, 其中 P_{miss} 为漏检概率, P_f 为虚警概率, P_1 和 P_2 为主用户存在和不存在的概率, $P_1+P_2=1$ 且主用户随机到达的概率服从 Poisson 分布, 那么主用户到达网络的时间间隔服从指数分布 $f(\tau)=\lambda\mathrm{e}^{-\lambda\tau},\tau>0$, 其中 λ 为用户业务量强度或者称之为到达率. 图中可以看出, 当 $\lambda=100$ 时, $P_1=0.9$, 随着 SNR 的增大, 两者的误检概率随之下降, 但是在 $-30\sim-15$ dB 区间内, 传统能量检测相对于本文的频谱检测方案有着更低的误检概率, 说明本文的频谱检测方案相对于能量检测更易产生错误检测.

图 4 表示不进行 PUEA 抵御时, 不同信噪比情况下不同程度的 PUEA 对系统虚警概率的影响. 图 4 分别给出了 10 个、50 个、100 个次用户受 PUEA 影响的情况, 将 3 者的曲线与未受恶意用户攻击的虚警概率作比较, 可以看出, 随着 PUEA 影响的 SU 数目增多, 虚警概率呈快速恶化趋势. 这是由于当频谱空闲时, MU 通过模仿 PU 信号使其攻击范围内的 SU 误认为频谱繁忙, 造成频谱资源没有

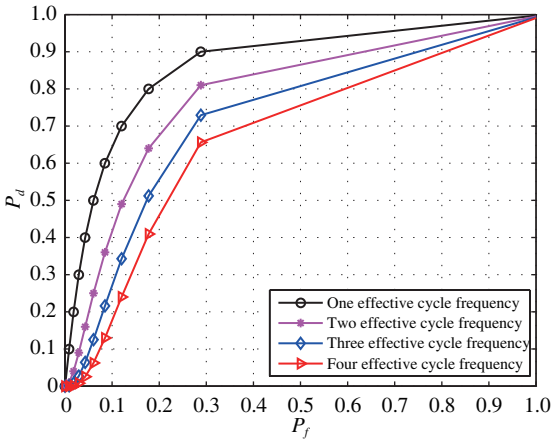

图 2 (网络版彩图) 不同有效循环频率数目下的 ROC 曲线

Figure 2 (Color online) Different ROC under different number of effective cycle frequency

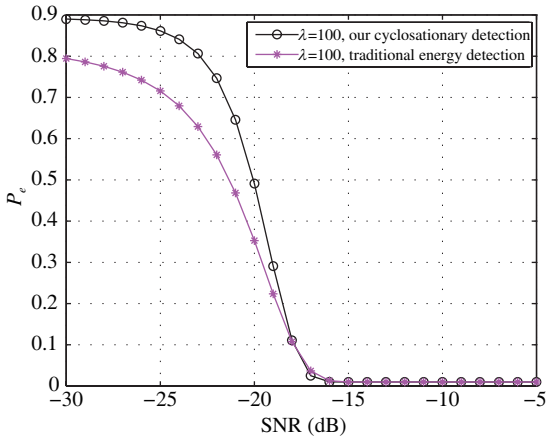

图 3 (网络版彩图) 误检概率对比

Figure 3 (Color online) The comparison of error detection probability

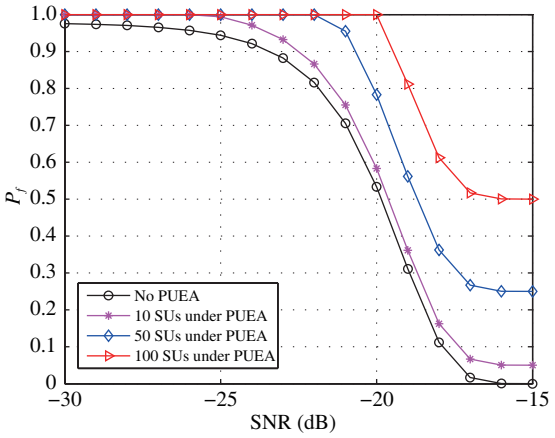

图 4 (网络版彩图) 不同程度的 PUEA 对系统的影响

Figure 4 (Color online) Different impacts of PUEA on the system

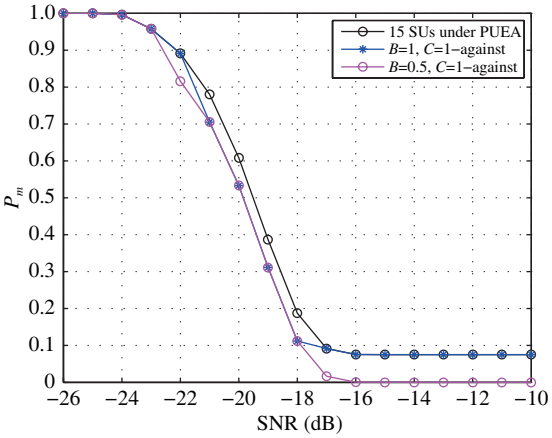

图 5 (网络版彩图) B 和 C 不同取值分析

Figure 5 (Color online) The analysis of different B, C values

被 SU 利用或者被恶意用户占用, 恶化了系统虚警概率, 而随着受 PUEA 影响的 SU 的数目的增多, 越来越多的 SU 检测到 PU 信号, FC 更容易检测到 PU 信号全部的 CAF, 使最终判决结果为存在 PU, 导致系统的虚警概率快速恶化.

图 5 表示当有 15 个 SU 受 PUEA 影响时, B,C 取不同值时的抵御性能, 其中纵坐标为式 (20) 的 PUEA 恶意影响概率 P_m. 当 $B = C = 1$ 时, $N_f = 22$, $N_d = 167$; 当 $B = C = 0.5$ 时, $N_f = 12$, $N_d = 182$. 由式 (19) 可知, 当 $N_g \in (N_f, N_d)$ 时, 本文的抵御策略将有效. 而当受 PUEA 影响的次用户数目小于 N_f 时, 本文的检测方法将失效. 图中可以看出, 当有 15 个 SU 受 PUEA 影响时, $B = C = 0.5$ 时, $N_f = 12$, 本文提出的方法仍有效, 而当 $B = C = 1$ 时, $N_f = 22$, 本文的方法失效. 因此, 在实际的环境中, 可以根据系统要求和实际情况来确定 B 和 C 的值. 图 6 表示在不同程度 PUEA 下, 本文的

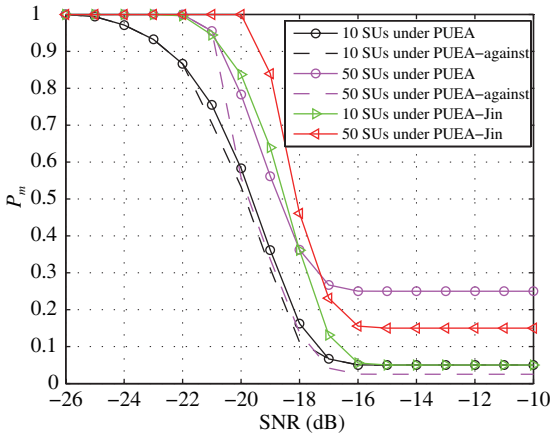

图 6 (网络版彩图) 不同程度 PUEA 下, 本文和 Jin 抵御 PUEA 策略效果

Figure 6 (Color online) This paper's and Jin's resisting effect under different PUEA

和文献 [8] 中 Jin 的抵御 PUEA 策略效果, 其中参数 $B = C = 1$. 图 6 中, 在 SNR $= -16$ dB 情况下, 当有 50 个次用户受 PUEA 影响时, 本文的抵御策略可以减少 60% 的 PUEA 恶意影响. 而当有 10 个次用户受 PUEA 影响时, 抵御前后的 P_m 基本没有变化. 这是由于当 $B = C = 1$ 时, $N_f = 22$, 只有当受 PUEA 攻击的 SU 数目 N_g 大于 22 时本文提出的检测方法有效, 而当 N_g 小于 22 时, 此方法将失效. 并与文献 [8] 中 Jin 的抵御策略进行了对比, 其中参数设置为 $A = B = 3$, 可以看出本文的抵御策略相对于 Jin 有着一定的性能提升, 这是由于 Jin 没有考虑噪声影响, 当信噪比较低且不存在主用户信号时, 系统虚警概率比较高, 影响了其抵御 PUEA 的性能.

6 结论

本文提出了一种基于信号循环平稳特征的抵御恶意模仿主用户攻击协作频谱检测算法, 该算法在保证良好频谱检测性能的同时有着不错的抵御 PUEA 性能, 并且详细给出了信号循环平稳特征的理论分析. 相对于常见的基于能量检测的抵御 PUEA 算法, 本文的抵御算法克服了其适用环境特殊、易被模仿等缺点, 并且该方法简单有效, 不需要额外的硬件设施等条件. 但是, 当受 PUEA 影响的次用户数目过少或过多时, 该算法将失效, 下一步我们将探讨如何改善这种情况.

参考文献

1 Ma B, Xie X Z, Liao X F. An efficient proactive spectrum handover mechanism in cognitive radio networks. Wirel Pers Commun, 2014, 3: 1679–1701

2 Sharma R K, Rawat D B. Advances on security threats and countermeasures for cognitive radio networks: a survey. IEEE Commun Surv Tut, 2015, 17: 1023–1043

3 O1ga L. Cooperative detection of primary user emulation attacks in CRNs. Comput Netw, 2012, 56: 3374–3384

4 Zhou Y, Niyato D, Li H S, et al. Defeating primary user emulation attacks using belief propagation in cognitive radio networks. IEEE J Sel Areas Commun, 2012, 30: 1850–1860

5 Jin Z, Anand S, Subbalakshmi K P. Impact of primary user emulation attacks on dynamic spectrum access networks. IEEE Trans Commun, 2012, 60: 2635–2643

6 Jana S, Zeng K, Cheng W, et al. Trusted collaborative spectrum sensing for mobile cognitive radio networks. IEEE Trans Inf Foren Secur, 2013, 8: 1497–1507

7 Chen C, Cheng H B, Yao Y D. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack. IEEE Trans Wirel Commun, 2011, 10: 2135–2141
8 Jin Z, Anand S, Subbalakshmi K P. Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks. In: Proceedings of IEEE on Global Telecommunications Conference (GLOBECOM), Miami, 2010. 1–5
9 Bao F, Chen H, Xie L. Analysis of primary user emulation attack with motional secondary users in cognitive radio networks. In: Proceedings of IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Sydney, 2012. 956–961
10 Cabric D, Mishra S M, Brodersen R W. Implementation issues in spectrum sensing for cognitive radios. In: Proceedings of the 38th Asilomar Conference on Signals, Systems and Computers, Pacific Grove, 2004. 772–776
11 Nguyen N T, Zheng R, Han Z. On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification. IEEE Trans Signal Process, 2012, 60: 1432–1445
12 Derakhshani M, LE-NGOC T, Nasiri-kenari M. Efficient cooperative cyclostationary spectrum sensing in cognitive radios at low SNR regimes. IEEE Trans Wirel Commun, 2011, 10: 3754–3764
13 Gong Z H, Haenggi M. Interference and outage in mobile random networks: expectation, distribution, and correlation. IEEE Trans Mobile Comput, 2014, 13: 337–349
14 Zhu Y, Liu J, Feng Z Y, et al. Sensing performance of efficient cyclostationary detector with multiple antennas in multipath fading and lognormal shadowing environments. J Commun Netw, 2014, 16: 162–171
15 Liang Y C, Zeng Y H, Peh E C, et al. Sensing-throughput tradeoff for cognitive radio networks. IEEE Trans Wirel Commun, 2008, 7: 1326–1337

Robust cooperative spectrum sensing against primary user emulation attacks based on cyclostationarity

Bin MA[1,2], Yuan FANG[1,2*] & Xianzhong XIE[1,2]

1 *Institute of Broadband Access Networks, Chongqing University of Posts & Telecommunications, Chongqing* 400065*, China*;
2 *Chongqing Key Laboratory of Computer Network and Communication Technology, Chongqing University of Posts & Telecommunications, Chongqing* 400065*, China*
*E-mail: fy498441454@126.com

Abstract The current methods employed to resist primary user emulation attacks (PUEA) are almost all based on energy spectrum detection, which has several shortcomings, such as need for special application environments and relatively easy emulation. We propose a cooperative spectrum sensing algorithm based on cyclostationarity to resist PUEA. The proposed method analyzes the local spectrum sensing results and compares them with the statistical results without a malicious user (MU) to detect the presence of malicious users. Simulation results show that the method performs effectively in terms of sensing spectrum and resistance to PUEA.

Keywords cognitive radio (CR), cooperative spectrum sensing, primary user emulation attack (PUEA), cyclostationarity, spectrum decision protocol

Bin MA received a Ph.D. degree in computer science and technology in 2015. He is currently an associate professor at Chongqing University of Posts and Telecommunications, Chongqing, China. His recent work is focused on spectrum handover in cognitive radio networks and vertical handoffs in heterogeneous wireless networks.

Xianzhong XIE was born in 1966. He received a Ph.D. degree in communication and information systems from Xidian University, Xi'an, in 2000. He is currently with the School of Computer Science and Technology at Chongqing University of Posts and Telecommunications, China, as a professor and director of the Institute of Broadband Access Technologies. His research interests include MIMO precoding and CR networks.

Yuan FANG received a B.S. degree from Nanjing University of Information Science and Technology, China, in 2013. He is a postgraduate student at Chongqing University of Posts and Telecommunications, China, and will receive an M.S. degree in computer science and technology in 2016. His research interests include cognitive radios, spectrum sensing, and cyclostationarity.