



研究与开发

一种能效优先的认知无线电模仿主用户 攻击防御策略设计与性能分析

王云川, 许晓荣, 姚英彪, 伍伟伟

(杭州电子科技大学通信工程学院, 浙江 杭州 310018)

摘要: 研究了一种能效优先的认知无线电 PUEA 防御策略并对其进行了性能分析。以 PUEA 存在时 CSS 能效作为目标函数, 以 CSS 安全检测性能作为约束条件, 从而构建一个安全的 CSS 系统模型进而求解该优化问题, 实现保障能量有效性的安全频谱检测。在 CSS 中, 融合中心以 K 秩准则 (K -out-of- N 准则) 作为全局判决准则, 保证能效最大化时得到最佳门限 K 和最佳认知用户数 N 。通过与最大比合并 (MRC) 准则下的安全 CSS 进行比较, 所提 PUEA 防御策略在保证系统能效的同时提高了系统的检测性能, 即所提 PUEA 防御策略可以有效折中能效与检测性能。数值仿真结果表明, 所提策略不受 PUE 干扰功率影响, 对于 PUEA 攻击具有较高的顽健性。

关键词: 认知无线网络; 模仿主用户攻击; 防御策略; 能效; 检测性能

中图分类号: TP393

文献标识码: A

doi: 10.3969/j.issn.1000-0801.2017116

Design and performance analysis of energy efficiency based CR primary user emulation attack defensive scheme

WANG Yunchuan, XU Xiaorong, YAO Yingbiao, WU Weiwei

College of Telecommunication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China

Abstract: Energy efficiency based PUEA defensive scheme was investigated with performance analysis. In this scheme, CSS energy efficiency was constructed as the optimum objective in the presence of PUEA with secure detection probability and false alarm probability threshold as the constraint conditions. Secure CSS model and PUEA defensive scheme were proposed to achieve energy efficiency based secure CSS. K -out-of- N criterion is set as global decision criterion in the scheme. Optimal fusion threshold K and optimal cooperative SUs N can be determined in secure CSS with the guarantee of energy efficiency. Compared with the traditional maximum ratio combining (MRC) fusion rule, the proposed PUEA defensive scheme not only guarantees system energy efficiency, but also improves system detection performance. Namely, the proposed scheme makes a trade-off between energy efficiency and detection performance in the presence of PUEA. The numerical simulation results show that the proposed strategy is not affected by the PUE interference power, and it has a high degree of persistence for PUEA attack.

Key words: cognitive radio network, primary user emulation attack, defensive scheme, energy efficiency, detection performance

收稿日期: 2017-02-28; 修回日期: 2017-04-25

基金项目: 浙江省自然科学基金资助项目 (No.LY15F010008); 杭州电子科技大学研究生科研创新基金资助项目 (No.CXJJ2016035); 浙江省科协青年科技人才培养工程资助项目 (No.2016YCGC009)

Foundation Items: Zhejiang Provincial Natural Science Foundation of China (No. LY15F010008), Graduate Scientific Research Foundation of Hangzhou Dianzi University in 2016 (No.CXJJ2016035), Young Talent Cultivation Project of Zhejiang Association for Science and Technology (No.2016YCGC009)

1 引言

认知无线网络 (cognitive radio network, CRN) 作为一个开放并且可以随意接入的网络环境, 特别容易受到恶意用户 (malicious user, MU) 的攻击^[1-3]。CRN 不但面临传统无线网络所面临的所有安全威胁, 比如窃听攻击、数据篡改攻击等^[4,5], 而且面临许多新的安全威胁, 比如模仿主用户攻击 (primary user emulation attack, PUEA)^[5]和频谱感知数据伪造攻击 (spectrum sensing data falsification, SSDF)^[6]。之前无线网络的安全问题主要通过发射信号进行加密实现^[4], 但是加密算法和密钥管理机制的复杂性将导致安全传输的能耗显著增大, 因而物理层安全技术作为对密钥加密技术的替代, 近年来受到了网络安全领域研究者的关注。其基本思想是利用噪声通信信道的随机性确保恶意窃听用户无法获取信息。物理层安全问题的研究包括两个方面: 一方面是从信息论的角度, 对 CRN 的安全容量进行理论分析; 另一方面是从信号处理和优化的角度, 对如何使系统安全通信速率达到其安全容量进行研究^[7,8]。协作频谱感知 (cooperative spectrum sensing, CSS) 是 CRN 中的一项关键技术, 它通过多个认知用户 (又称次用户, secondary user, SU) 共同协商确定授权频段的使用情况, 融合中心再通过对多个 SU 感知数据的协同处理来提高频谱感知的精确性。在 CSS 中, 通常可以采用两种方式进行感知数据的传递和融合: 一种是直接传递本地节点感知到的原始信息, 称为软合并方式^[9]; 另一种是本地节点先根据感知到的信息给出单个比特的判决信息, 然后将这个单比特的判决信息发送给融合中心来进行最终的判决, 称为硬合并方式^[10]。当 PUEA 攻击时, 协作频谱感知可以发挥其特有的优势, 降低单个 SU 感知的不确定性, 提高 PUEA 抵御性能。Jin^[11]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, 与单个 SU 的检测

方法相比, 提升了系统的检测性能。进而 Jin^[12]又提出了一种利用单个 SU 判决结果的分布式合作判决的 PUEA 抵御机制, SU 节点通过与其具有单跳距离的邻居节点进行感知结果交互, 获取更准确的频谱信息以应对 PUEA。Chen^[5]为了进一步提高基于合作检测的 PUEA 抵御机制的性能, 提出了为每个 SU 提供权重来获得最佳融合结果的判决结果融合方式。Liu^[13]提出通过最大最小特征值法 (maximum-minimum eigenvalue) 来选择最佳合作用户, 将相关性比较大的用户去除, 尽量降低由于阴影、遭受攻击等原因而获得错误感知结果的 SU 对判决结果产生不良影响。参考文献[14]针对 CRN 移动场景下的 PUEA 攻击及防御策略进行了研究, 提出了一种以 PUEA 攻击检测为主的混合策略抵御机制, 根据攻击者与合法感知用户之间距离动态切换 PUEA 检测机制, 以充分利用能量检测与方差检测的优势, 在更低的资源消耗、更快的判决决策情况下满足系统对 PUEA 检测过程中虚警概率与检测概率的要求。

协作频谱检测中感知灵敏度的提升是以额外的通信开销为代价的, 然而, 在追求 CRN 高频谱利用率、高传输效率的同时, CRN 对能量有效性和系统安全性等方面提出了更高的要求。研究表明, 节点进行频谱感知与传输的功耗是 CRN 能耗主要的开销^[15]。随着 CRN 中 SU 的增加和网络覆盖面积的扩大, CRN 的能耗问题已日益受到关注, “绿色 CRN”已经成为未来 CRN 的发展方向之一^[15,16]。保障 CRN 的物理层安全是能量有效性 CRN 的研究重点。参考文献[16]同时指出, CRN 能量有效性与传输安全性之间存在着最佳折中关系。针对不同的恶意用户攻击方式, 系统采用不同的物理层安全策略所需要的能耗大不相同。因此, 在保障数据安全、可靠传输的前提下, 需要针对特定攻击方式的能耗研究开销最小的安全策略。

针对 CRN 中安全性与能效的折中问题^[15,16], 本文重点研究了一种保障能量有效性的 PUEA 防



御策略。假设存在 PUEA, 在 CSS 中, 每个 SU 对感知到的授权频段进行二元判决, 然后将本地感知结果采用硬合并的方式汇报给融合中心, 融合中心再通过 K 秩准则 (K -out-of- N 准则) 做出全局判决, 同时, 重点考虑了 CSS 中的能效问题, 详细推导了所提策略的能效表达式, 并以能效作为目标函数, 以协作频谱感知安全检测概率和安全虚警概率作为约束条件, 通过构造和求解该优化问题, 得到能效最优时安全协作频谱感知最佳认知用户数和最佳门限, 实现存在 PUEA 攻击时保障能量有效性的安全频谱检测。

2 协作频谱感知中 PUEA 系统模型

假设 CRN 包含 N 个试图以交叉频谱共享方式访问授权频段的认知用户 (SU)。为了避免与主用户 (PU) 发生冲突, 每个 SU 在一个特定的时间内感知目标频段, 并判断 PU 是否正在使用该频段, SU 将本地感知结果报告给融合中心, 融合中心通过特定的数据融合准则对授权频段使用情况进行全局检测。与此同时, PUEA 也通过发射 PUE 信号伪造 PU 信息特征以欺骗 SU, 使得各 SU 认为 PU 正在使用该授权频段, 则 SU 进行频谱切换, PUEA 以此获得了授权频段的使用权。因此, SU 对 PU 信号与 PUE 信号进行正确判决是防御 PUEA 攻击的关键问题^[5,7,13]。

CRN 协作频谱感知中发生 PUEA 攻击的场景如图 1 所示。

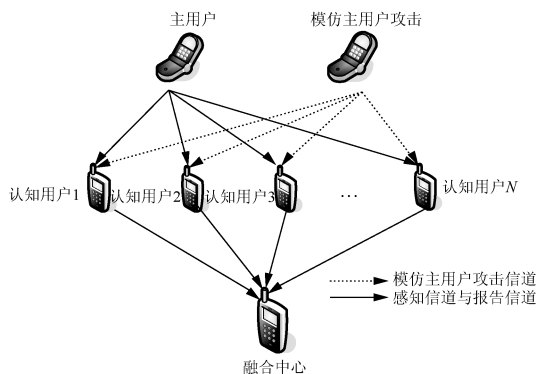


图 1 CRN 协作频谱感知中发生 PUEA 攻击的场景

CRN 常用的频谱感知技术有能量检测、匹配滤波器检测和循环平稳特征检测^[1,2]。本文中 SU 采用能量检测来判断 PU 是否存在。由于存在 PUEA, 在第 i ($1 \leq i \leq M$) 个时隙, 第 j ($1 \leq j \leq N$) 个 SU 接收到的信号可以表示为^[5]:

$$y_j(i) = \begin{cases} P_m h_{m,j} x_{m,j}(i) + w_j(i), & H_0 \\ P_p h_{p,j} x_{p,j}(i) + P_m h_{m,j} x_{m,j}(i) + w_j(i), & H_1 \end{cases} \quad (1)$$

其中, H_0 表示不存在 PU, H_1 表示存在 PU。 $x_{p,j}(i)$ 是 PU 的发送信号, 服从均值为 0、方差为 1 的独立同分布高斯随机变量, 功率为 P_p 。 $x_{m,j}(i)$ 是 PUEA 的发送信号, 由于 PUEA 模仿 PU 信号特征进行攻击, 因此 $x_{m,j}(i)$ 也服从均值为 0、方差为 1 的高斯随机变量, 功率为 P_m 。 $h_{p,j}$ 表示从 PU 到第 j 个 SU 的信道增益, $h_{m,j}$ 表示从 PUEA 到第 j 个 SU 的信道增益。假设所有的链路均为平坦块衰落, 即 $h_{p,j}$ 和 $h_{m,j}$ 在一个时隙内为常数。 $w_j(i)$ 是第 i 个 SU 链路的加性高斯白噪声, 其均值为 0、方差为 σ_w^2 。第 j 个 SU 的接收信噪比可以表示为 $\gamma = h_{p,j}^2 / \sigma_w^2$ 。

第 j 个 SU 检测到 PU 信号的能量可以表示为 $Y_j = \sum_{i=1}^M |y_j(i)|^2$ 。由于 $x_{p,j}(i)$ 和 $x_{m,j}(i)$ 均服从均值为 0、方差为 1 的高斯分布, 故 Y_j 服从自由度为 $2M$ 的中心卡方分布^[5,7], 可表示为:

$$Y_j = \sum_{i=1}^M |y_j(i)|^2 = \begin{cases} Y_0 \sim \chi_{2M}^2(\sigma_0^2) \\ Y_1 \sim \chi_{2M}^2(\sigma_1^2) \end{cases} \quad (2)$$

其中, σ_0^2 和 σ_1^2 分别为 Y_j 在 H_0 和 H_1 两种情况下的方差 (功率), 分别为:

$$\begin{aligned} \sigma_0^2 &= P_m^2 h_{m,j}^2 + \sigma_w^2 \\ \sigma_1^2 &= P_p^2 h_{p,j}^2 + P_m^2 h_{m,j}^2 + \sigma_w^2 \end{aligned} \quad (3)$$

考虑存在 PUEA 攻击时的协作频谱感知, 第 j 个 SU 进行本地频谱检测的虚警概率 P_f 和检测概率 P_d 分别定义为:

$$\begin{aligned} P_f &= \Pr\{Y_j \geq \lambda | H_0\} \\ P_d &= \Pr\{Y_j \geq \lambda | H_1\} \end{aligned} \quad (4)$$

其中, λ 是检测阈值。

在 Rayleigh (瑞利) 衰落信道下, 第 j 个 SU 进行本地频谱检测的虚警概率 P_f 和检测概率 P_d 分别为^[2,7]:

$$\begin{aligned} P_f &= \Gamma(M, \frac{\lambda}{\sigma_0^2}) \\ P_d &= \Gamma(M, \frac{\lambda}{\sigma_1^2}) \end{aligned} \quad (5)$$

各 SU 对频谱状态做出一个二元判决。如果 $Y_j > \lambda$, 则 $d_j = 1$ 表示该频谱正在被 PU 使用; 如果 $Y_j < \lambda$, 则 $d_j = 0$ 表示该频谱未被 PU 使用^[1,2,7]。二元判决可表示为:

$$d_j = \begin{cases} 1, Y_j > \lambda \\ 0, Y_j < \lambda \end{cases} \quad (6)$$

各 SU 本地判决报告给协作频谱检测数据融合中心。融合中心通过特定的融合准则进行最后判决。本文使用 K 秩准则 (K -out-of- N 准则) 进行数据融合, 其中 K 是一个预先设定的门限阈值, 表示检测到正在使用授权频段的 SU 个数 ($1 \leq K \leq N$)。 K 秩数据融合准则可以表示为: 如果融合中心接收到本地检测报告为 1 的 SU 个数小于 K , 则判决该频谱未被 PU 使用; 反之, 则判决该频谱被 PU 占用。

本文同时考虑各认知用户向融合中心进行报告的过程中也存在差错, 报告阶段的差错率记为 P_e , 则 SU 本地检测概率和虚警概率可以修正为^[7]:

$$\begin{aligned} P_x &= P_d(1 - P_e) + (1 - P_d)P_e \\ P_y &= P_f(1 - P_e) + (1 - P_f)P_e \end{aligned} \quad (7)$$

融合中心进行判决的全局虚警概率 Q_f 和全局检测概率 Q_d ^[5,7,14] 分别表示为:

$$\begin{aligned} Q_d &= \sum_{j=K}^N \binom{N}{j} P_x^j (1 - P_x)^{N-j} \\ Q_f &= \sum_{j=K}^N \binom{N}{j} P_y^j (1 - P_y)^{N-j} \end{aligned} \quad (8)$$

3 PUEA 防御策略的能量有效性分析

CRN 频谱感知阶段的能量有效性 (μ) 定义为平均吞吐量 (单位为 bit) 和平均能耗 (单位为 J) 的比值。平均吞吐量定义为成功传输的比特数, 平均能耗是指在协作频谱本地感知和报告阶段数据传输中消耗的平均能量。平均吞吐量^[14]可以表示为:

$$Th = P_0(1 - Q_f)RT \quad (9)$$

其中, P_0 为该频段未被授权用户使用的概率。 R 是数据传输速率, 单位为 bit/s。 T 是数据传输的时间, 单位为 s。 $1 - Q_f$ 表示成功传输数据的概率。

N 个 SU 的平均感知能耗可以表示为:

$$E = Ne_s + P_{\text{unused}}e_t \quad (10)$$

其中, e_s 表示 SU 在协作频谱感知阶段的能耗, e_t 为数据传输能耗。只有当 SU 检测到频谱空闲时才进行数据传输, 因此频谱空闲的概率 P_{unused} 可表示为:

$$\begin{aligned} P_{\text{unused}} &= P_0(1 - Q_f) + P_1(1 - Q_d) \\ &= 1 - P_0Q_f - P_1Q_d \end{aligned} \quad (11)$$

PUEA 防御策略能效 μ 的计算式为:

$$\mu = \frac{P_0(1 - Q_f)RT}{Ne_s + e_t(1 - P_0Q_f - P_1Q_d)} \quad (12)$$

以最大化 PUEA 防御策略的能效式 (12) 作为目标函数, 在全局检测概率与全局虚警概率式 (8) 的约束条件下, 构造优化问题:

$$\begin{aligned} \max \quad & \mu \\ \text{s.t.} \quad & Q_d \geq \alpha, Q_f \leq \beta \end{aligned} \quad (13)$$

通过对式 (13) 求导, 使其等于 0, 可以求得 K 值, 即:

$$\begin{aligned} & \frac{-P_0RT \frac{\partial Q_f}{\partial K}}{Ne_s + e_t(1 - P_0Q_f - P_1Q_d)} + \\ & \frac{P_0(1 - Q_f)RTe_t \left(P_0 \frac{\partial Q_f}{\partial K} + P_1 \frac{\partial Q_d}{\partial K} \right)}{[Ne_s + e_t(1 - P_0Q_f - P_1Q_d)]^2} = 0 \end{aligned} \quad (14)$$



Q_f 和 Q_d 的偏导数形式可表示为:

$$\begin{aligned}\frac{\partial Q_f}{\partial K} &= Q_f(K+1) - Q_f(K) = \binom{N}{K} P_y^K (1-P_y)^{N-K} \\ \frac{\partial Q_d}{\partial K} &= Q_d(K+1) - Q_d(K) = \binom{N}{K} P_x^K (1-P_x)^{N-K}\end{aligned}\quad (15)$$

将式 (15) 代入式 (14), 并进行数值计算, 可以得到能效最大时的 K 值, 表示为:

$$K_1 = \frac{\ln\left(\frac{Ne_s + P_{ef}(1-Q_d)}{P_{ef}(1-Q_f)}\right) + N \ln\left(\frac{1-P_y}{1-P_x}\right)}{\ln\left(\frac{P_x(1-P_y)}{P_y(1-P_x)}\right)} \quad (16)$$

因此, 对于给定的 N 值和虚警概率, 检测概率会随着 K 的增加而减小, 满足约束条件使能效最大的最优 K 值可以表示为:

$$K_{\text{opt}} = \min\{K_1, K_2\} \quad (17)$$

其中, K_2 约为:

$$K_2 \approx Q^{-1}(\alpha) \sqrt{NP_x(1-P_x)} + NP_x + 0.5 \quad (18)$$

4 仿真与性能分析

本节给出所提 PUEA 防御策略及其能效优化问题的仿真与性能分析。考虑存在单个 PUEA 时的防御策略。假设感知信道与报告信道均为独立同分布。在一个检测时隙内的采样数 $M=3^{[5]}$ 。仿真参数设置见表 1^[5,7]。

表 1 仿真参数设置

参数	数值	参数	数值
M	3	Q_d	≥ 0.8
Q_f	≤ 0.2	P_0	0.5
e_s/J	10^{-2}	e_r/J	1
T/s	0.3	$R/(\text{kbit}\cdot\text{s}^{-1})$	100

图 2 给出了存在 PUEA 时融合中心采用硬融合准则进行协作频谱感知全局检测的接收机特性曲线 (ROC) ^[14,15]。设定信噪比为 0 dB, PU 和 PUEA 的发送功率均为 $P_p = P_m = 1$ 。由图 2 可知, 若存在

PUEA, 当虚警概率一定时, 单 SU 的检测概率大幅下降。采用 K 秩准则的安全协作频谱感知检测性能较单 SU 检测性能得到大幅提升, 甚至优于不存在 PUEA 时的单 SU 检测性能。采用 K 秩融合准则, 当 SU 用户数一定时, 门限阈值 K 对检测性能具有较大的影响。当虚警概率一定时, 门限阈值 K 越小, 全局检测性能越好。究其原因, K 越小, K 秩融合二元判决准则趋近于或融合准则, 全局检测性能得到提高。

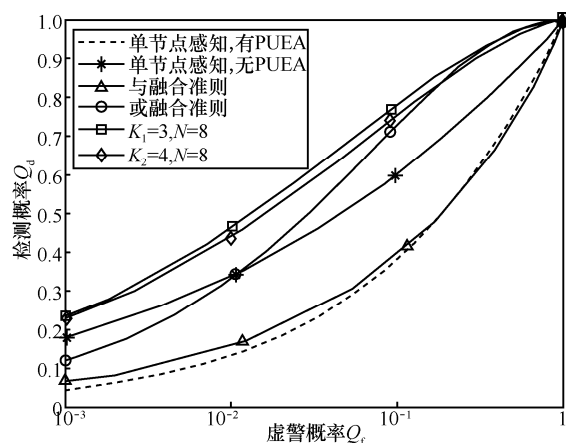


图 2 存在 PUEA 时融合中心采用硬融合准则进行协作频谱感知全局检测的接收机特性曲线

图 3 给出了不同门限阈值与 SU 节点数情况下所提 PUEA 防御策略能效。设定信噪比为 0 dB, 约束条件为 $Q_d \geq 0.8$ 且 $Q_f \leq 0.2$ 。由图 3 可知, 当 SU 节点数 $N=4$, 融合门限阈值 $K=2$ 时, 所提策略可以获得最大能效, 约为 $7.9 \times 10^4 \text{ bit/J}$ 。同时, 达到最大能效的门限阈值 K 随着协作感知节点数 N 的增加而增加。参与协作感知的节点数越多, 其可达最高能效值越小。究其原因, 参与协作的认知节点数越多, 协作检测感知阶段和报告阶段中的能耗越大, 造成能效下降。因此需要探寻达到最大能效时的最佳协作节点数与融合门限阈值。

图 4 给出了存在和不存在 PUEA 攻击情况下, 单 SU、采用 K 秩融合准则的协作感知、软融合判决中最大比合并 (maximum ratio combining, MRC) 准则协作感知的 ROC 性能, 并分别对其进行了性能分析。由图 4 可知, 在相同融合

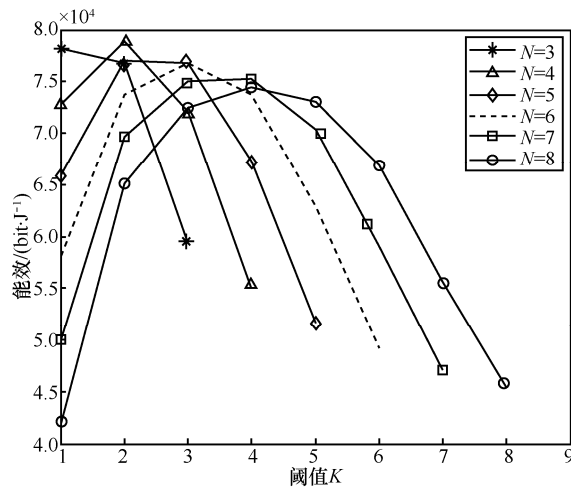


图3 不同门限阈值与SU节点数情况下所提PUEA防御策略能效

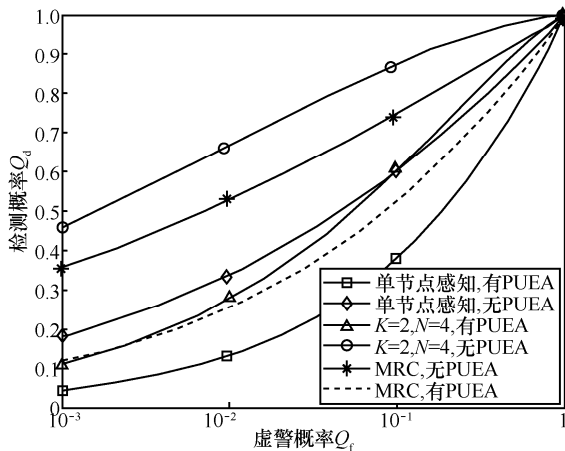


图4 存在和不存在PUEA攻击情况下,不同融合准则的协作感知ROC性能

准则下,不存在PUEA攻击的ROC性能优于存在PUEA攻击的情况。根据图3性能分析,当存在PUEA攻击时,达到最高能效时的最佳融合门限阈值 $K=2$,SU节点数 $N=4$ 。在相同虚警概率情况下,所提 K 秩准则融合方案的PUEA防御策略检测性能优于MRC准则融合方案。当虚警概率大于0.02时,其检测性能甚至优于单SU不存在PUEA的情况。但是,在检测概率增加的同时,虚警概率也随之增加。因此,需要折中安全协作频谱检测ROC性能中两者的关系,在提高检测性能的同时,降低虚警概率。

图5给出了在攻击用户与PU不同发射功率比情况下,采用所提PUEA防御策略的协作频谱

检测性能。其中,定义PUE发射功率与PU发射功率之比^[15]为:

$$p = \frac{P_m}{P_p} \quad (14)$$

p 值越大,表明PUE发射干扰功率越大。在仿真中,设定虚警概率门限 $P_f=0.1$,各SU的信噪比门限相同。图5给出了当 p 值分别为0.1、1、10时,所提防御策略与软融合判决MRC准则的检测性能比较。

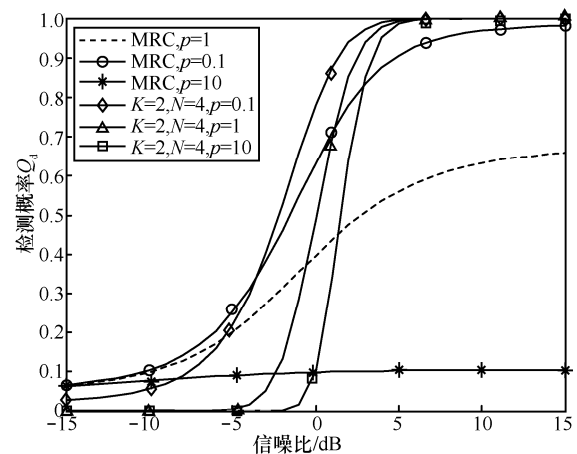


图5 所提PUEA防御策略与软融合判决MRC准则的检测性能比较

由图5可知,两种方案的检测性能随着信噪比的增加显著增加。当 p 值分别取0.1、1、10时,随着PUE发射功率的增加,检测性能显著下降。此时,PUE干扰功率在授权频段中占主导地位,全局检测性能显著下降。通过对比发现,在高SNR情况下,所提 K 秩准则PUEA防御策略的检测性能较MRC准则显著提高,且检测性能与 p 值几乎无关,即PUE干扰功率对所提防御策略几乎无影响,有效保障了PUEA攻击时协作检测的安全性,即所提PUEA防御策略具有较高的稳健性。

5 结束语

本文研究了CRN协作频谱感知中存在PUEA情况下保障能效和物理层安全的防御策略。通过构造保障协作频谱感知检测性能的能效优化问题,得



到以 K 秩融合判决准则下的最佳判决门限阈值 K 和最佳认知用户数 N 以及能效最优情况（融合门限阈值 $K=2$ ，SU 节点数 $N=4$ ）时的 ROC 性能。通过与 MRC 软融合准则相比较，在相同虚警概率情况下，所提 K 秩准则融合方案的 PUEA 防御策略安全检测概率优于 MRC 准则融合方案。在高信噪比情况下，所提 PUEA 防御策略的检测性能较 MRC 准则显著提高，且不受 PUEA 干扰功率的影响，有效保障了协作检测的安全性。同时，所提 PUEA 防御策略折中了 CRN 能效与安全检测性能。

参考文献:

- [1] 张平, 李建武, 冯志勇, 等. 认知无线网络基础理论与关键技术研究[J]. 电信科学, 2014, 30(2): 1-13.
ZHANG P, LI J W, FENG Z Y, et al. Research on basic theory and key technology of cognitive radio network [J]. Telecommunications Science, 2014, 30(2): 1-13.
- [2] CHATTERJEE S, MAITY S P, ACHARYA T. Energy efficient cognitive radio system for joint spectrum sensing and data transmission[J]. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 2014, 4(3): 292-300.
- [3] HONG X, WANG J, WANG C X. Cognitive radio in 5G: a perspective on energy-spectral efficiency tradeoff[J]. IEEE Communication Magazine, 2014, 52(7): 46-53.
- [4] 陈涛. 无线网络的物理层安全问题研究[D]. 广州: 华南理工大学, 2013.
CHEN T. Study on physical security of wireless networks[D]. Guangzhou: South China University of Technology, 2013.
- [5] 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.
- [6] ZHANG L, DING G, WU Q, et al. Byzantine attack and defense in cognitive radio networks: a survey[J]. IEEE Communication Surveys and Tutorials, 2015, 17(3): 1342-1363.
- [7] LI J, FENG Z, FENG Z, et al. A survey of security issues in cognitive radio networks[J]. China Communications, 2015, 12(3): 132-150.
- [8] ZOU Y, ZHU J, YANG L, et al. Securing physical-layer communications for cognitive radio networks[J]. IEEE Communications Magazine, 2015, 53(9): 48-54.
- [9] MA J, ZHAO G D, LI Y. Soft combination and detection for cooperative spectrum sensing in cognitive radio networks[J]. IEEE Transactions on Wireless Communications, 2008, 7(11): 4502-4507.
- [10] ZHANG R Y, ZHAN Y F, PEI Y K, et al. Weighted hard combination for cooperative spectrum sensing under noise uncertainty[J]. IEICE Transactions on Communications, 2014, 97(2): 275-282.
- [11] JIN Z, ANAND S, SUBBALAKSHMI K P. Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2009, 13(2): 74-85.
- [12] JIN Z, SUBBALAKSHMI K P. Detecting primary user emulation attacks in dynamic spectrum access networks[C]//IEEE International Conference on Communications (ICC 2009), June 14-18, 2009, Dresden, Germany. New Jersey: IEEE Press, 2009: 1-5.
- [13] LIU F, CHEN H, XIE L. Maximum-minimum eigenvalue detection-based method to mitigate the effect of the PUEA in cognitive radio networks[C]//IEEE International Conference on Wireless Communications and Signal Processing (IEEE WCSP 2011), November 9-11, 2011, Nanjing, China. New Jersey: IEEE Press, 2011: 1-5.
- [14] 鲍飞静. 认知无线网络中移动场景下主用户仿真攻击及其防御策略研究[D]. 杭州: 浙江大学, 2013.
BAO F J. Research on primary user emulation attack and countermeasures with mobile secondary user in cognitive radio networks[D]. Hangzhou: Zhejiang University, 2013.
- [15] 王娇, 赵军辉, 杜家娇. 基于跨层的认知无线电绿色网络关键技术综述[J]. 电信科学, 2014, 30(3): 114-119.
WANG J, ZHAO J H, DU J J. Survey on cognitive radio green network with cross-layer technology[J]. Telecommunications Science, 2014, 30(3): 114-119.
- [16] ERYIGIT S, GUR G, BAYHAN S, et al. Energy efficiency is a subtle concept: fundamental tradeoffs for cognitive radio networks[J]. IEEE Communication Magazine, 2014, 52(7): 30-36.
- [17] ALTHUNIBAT S, SUCASAS V, MARQUES H, et al. On the tradeoff between security and energy efficiency in cooperative spectrum sensing for cognitive radio[J]. IEEE Communications Letters, 2013, 17(8): 1564-1567.
- [18] ZOU Y, ZHU J, WANG X, et al. A survey on wireless security: technical challenges, recent advances, and future trends[J]. Proceedings of the IEEE, 2016, 104(9): 1727-1765.

[作者简介]



王云川（1993-），男，杭州电子科技大学通信工程学院硕士生，主要研究方向为认知无线网络中的物理层安全策略等。

许晓荣（1982-），男，博士，杭州电子科技大学通信工程学院副教授，主要研究方向为认知无线网络中的资源分配与资源共享等。

姚英彪（1976-），男，博士，杭州电子科技大学通信工程学院教授，主要研究方向为无线网络的能量有效性与无线资源管理等。

伍伟伟（1992-），男，杭州电子科技大学通信工程学院硕士生，主要研究方向为认知无线网络中的资源分配等。