DOI: 10.13718/j.cnki.xdzk.2018.04.018

CR 网络中基于最优阈值选取的攻击感知算法①

王　会[1]，　余　阳[2]，　李旭伟[3]

1. 成都东软学院 计算机科学与工程系，成都 611844；
2. 成都东软学院 信息管理系，成都 611844；3. 四川大学 计算机学院，成都 610064

摘要：由于认知无线电(Cognitive Radio，CR)网络允许多个未知无线设备接入频谱，使其存在模仿主用户攻击(Primary User Emulation Attack，PUEA)的安全隐患，为此，提出一种具有攻击感知能力的协作感知方案. 首先，在授权主用户信号频谱资源处于占用和空闲这 2 种情况下，估计 PUEA 伪信号出现的概率；然后，利用得到的估计参数确定最小化总误差概率的最优阈值；最后，融合中心通过感知报告与阈值来判断主用户信号是否存在，以达到感知模仿主用户攻击的能力. 仿真试验结果表明：与最优用户选择(Optimal User Selection，OUS)方法相比，提出的方法在应对主用户仿真攻击时具有更好的安全性能，提高了 CR 网络的安全效能.

关　键　词：认知无线电网络；协同频谱感知；主用户仿真攻击；阈值选取；安全性能

中图分类号：TN929.5　　**文献标志码**：A　　**文章编号**：1673－9868(2018)04－0132－07

无线通信服务的快速增长带来了严重的频谱短缺问题，认知无线电(Cognitive Radio，CR)的引入很好地解决了这一问题[1－3]. 在 CR 网络中，次级或非授权用户仅在对授权主用户(Primary User，PU)的操作不产生干扰的前提下，才被允许使用属于授权主用户的空闲频段. 而频谱感知方法用于检测 CR 网络中的 PU 信号，存在一系列不确定性问题[4]. 为了缓解各种衰减问题[5－6]，一般采用协同频谱感知方法(Cooperative Spectrum Sensing，CSS). 在 CSS 中，每个用户独立进行局部感知，随后向融合中心报告测量值. 基于接收数据的性质，融合中心选择一个软性或硬性的组合规则以确定信道状态. 然而，CR 网络架构具有允许多个不同的未知无线设备伺机接入频谱的特性，使得 CR 网络存在严重的安全隐患[7]. 例如一些恶意用户通过伪造发射参数和仿真信号从而伪装成一个授权主用户，造成其他 CR 用户无法正常接入信道，此类攻击被称为模仿主用户攻击[8－9]. 由于模仿主用户攻击较为常见且破坏大，如何抵御模仿主用户攻击，提高网络的安全性能一直是 CR 网络的研究热点.

如文献[8]提出了一种基于位置的防御机制，利用 PU 信号发射机的物理位置信息和接收信号强度特征进行信息验证. 文献[9]讨论了在不使用任何位置信息的情况下抵御模仿主用户攻击的方法，该方法首先基于 Fenton 近似法推导恶意用户信号接收功率的概率密度函数，然后提出 Neyman-Pearson 复合假设检测法和 Wald 序贯概率比检测法，以检测恶意用户. 文献[10]研究了一种不同于以上方法的协同频谱感知方案. 首先在融合中心对不同 CR 用户的感知信息进行加权组合；然后，对分配的权重进行优化，以最大化虚报警率进行概率检测. 然而，该方案假设模仿主用户攻击在广播环境中始终存在，不符合实际，且造成的能耗更大. 文献[11]研究无线信道的特征参数，从用户中独立提取信道特征参数，基于硬判决联合检查方法对发射机身份进行验证，抵御攻击者发起模仿主用户攻击，即最优用户选择(Optimal User Selection，

① 收稿日期：2017－06－20
基金项目：国家自然科学基金项目(60902038)；四川省教育厅项目(14ZA0366，18SB0028)；教育部高等教育司项目(201701004019).
作者简介：王　会(1978－)，女，四川成都人，硕士，副教授，主要从事网络信息安全、软件工程等方面的研究.

OUS)的协同频谱感知. 文献[12]基于改进的能量检测算法和软融合策略推导系统的检测概率和虚警概率之间的关系，在虚警概率一定的情况下，求出最优加权系数矩阵，利用该矩阵抑制 PUEA 信号.

现在的大多数研究均是假设 PU 发射机的物理位置或特有性质等先验信息对于 CR 用户或融合中心是已知的，但很多时候这些信息并非完全知晓[13-14]. 为此，本文提出误差概率最小化的阈值选取(Threshold Selection of Minimizing Error Probability，TSMEP)方案，该方案对 PU 信号发射机的物理位置或特定属性的先验信息不做任何要求. 每个 CR 用户检测其自身的频谱感知，并将测量值发送到融合中心；然后，计算感知测量值的第一阶距和第二阶距，完成 2 个攻击参数的估计，2 个攻击参数分别表示 PU 信号存在和不存在时，模仿主用户攻击信号的出现概率，通过使用该攻击参数确定能够最小化总误差概率的最优阈值.

1 系统模型

本文采用集中式 CR 网络系统模型，如图 1 所示，包括一个 PU 发射器、N 个 CR 用户、一个融合中心和一个恶意 PUEA 发射器. 模型假设：N 个 CR 用户随机分布在一个较小的区域内，与 PU 发射器、PUEA 发射器相距较远；同时该 PUEA 能够精确区分分配给主用户的占用频段和空闲频段.

按照 PU 和 PUEA 信号是否存在的情况，有 4 种可能状态，具体表示如下：

H_{s0}：只存在噪声；

H_{s1}：PU+噪声；

H_{s2}：PUEA+噪声；

H_{s3}：PU+PUEA+噪声.

第一种状态 H_{s0} 出现于 CR 用户仅接收到噪声的情况下，信道没有被 PU 或者 PUEA 信号占用；第二种状态 H_{s1} 出现于 PU 在信道上发射信号且不存在 PUEA 信号的情况下；第三种状态 H_{s2} 表示不存在 PU 信号且 PUEA 发射伪装信号，CR 用户只能接收到 PUEA 信号加噪声；最后一种状态 H_{s3} 表示同时存在 PU 信号和 PUEA 信号.

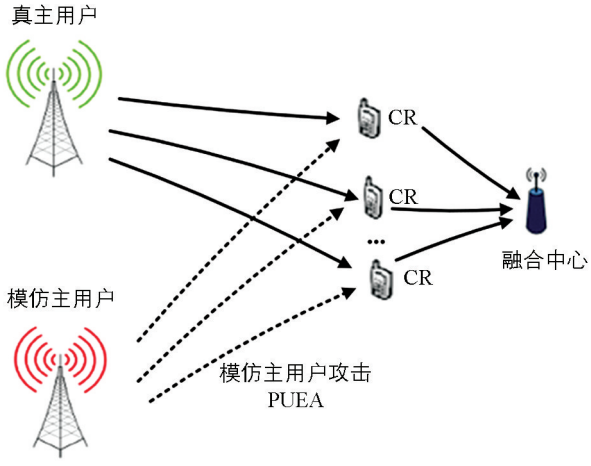

图 1 CR 网络系统模型

本文设定 H_1 和 H_0 分别表示 PU 信号存在与不存在的 2 种情况，E^{on} 和 E^{off} 表示 PUEA 信号存在与不存在的 2 种情况. 基于该种假设，每种可能状态 H_{sk} 的概率表示为 π_k，设参数 α 和 β 分别为 2 个假设情况 H_1 和 H_0 中存在 PUEA 伪信号的条件概率，即

$$\alpha = P(E^{on} \mid H_1) \qquad \beta = P(E^{on} \mid H_0)$$

其与攻击者的策略相关联. 则有：

$$\begin{aligned} \pi_0 &= (1-\beta)P(H_0) \\ \pi_1 &= (1-\alpha)P(H_1) \\ \pi_2 &= \beta P(H_0) \\ \pi_3 &= \alpha P(H_1) \end{aligned} \tag{1}$$

对于 4 种可能状态，第 j 个用户的第 i 个样本的接收信号 x_j^i 可表示为

$$x_j^i \sim \begin{cases} n_j^i & H_{s0} \\ \sqrt{\gamma_j}\, p_j^i + n_j^i & H_{s1} \\ \sqrt{\lambda_j}\, e_j^i + n_j^i & H_{s2} \\ \sqrt{\gamma_j}\, p_j^i + \sqrt{\lambda_j}\, e_j^i + n_j^i & H_{s3} \end{cases} \tag{2}$$

其中，n_j^i 为第 j 个 CR 用户的加性高斯白噪声；参数 $\sqrt{\gamma_j}p_j^i$ 和 $\sqrt{\lambda_j}e_j^i$ 分别为接收到的能量为 γ_j 和 λ_j 的 PU 信号和 PUEA 信号. 本文假设每个 n_j^i 样本、PU 信号 p_j^i 和 PUEA 信号 e_j^i 的噪声均服从独立高斯分布($\mu=0$，$\sigma=1$). 同时假设 CR 用户经过具有相同平均信噪比的独立分组衰减信道. 由于 CR 用户远离 PU 和 PUEA 信号发射器，因此，γ_j 和 λ_j 随着观察周期的不同而改变，其概率密度函数分别服从均值为 $\overline{\gamma}$ 和 $\overline{\lambda}$ 的指数分布. 定义参数 $\rho=\lambda/\overline{\gamma}$ 表示攻击强度，较大的 ρ 值($\rho\geqslant 1$) 表示一次强度较大的 PUEA. 综合式(2) 和上述假设，则接收到的信号 x_j^i 为高斯分布：

$$x_j^i \sim \begin{cases} N(0,\ 1) & H_{s0} \\ N(0,\ \gamma_j+1) & H_{s1} \\ N(0,\ \lambda_j+1) & H_{s2} \\ N(0,\ \gamma_j+\lambda_j+1) & H_{s3} \end{cases} \tag{3}$$

对每个 CR 用户使用 M 个样本进行局部能量检测，根据中心极限定理[15]，如果样本数目较大，可假设第 j 个用户的能量 E_j 为高斯分布，能量 E_j 表示如下：

$$E_j \sim \begin{cases} N(M,\ 2M) & H_{s0} \\ N(M(\gamma_j+1),\ 2M(\gamma_j+1)^2) & H_{s1} \\ N(M(\lambda_j+1),\ 2M(\lambda_j+1)^2) & H_{s2} \\ N((M\gamma_j+\lambda_j+1),\ 2M(\gamma_j+\lambda_j+1)^2) & H_{s3} \end{cases} \tag{4}$$

在 CSS 中，每个 CR 用户的局部能量测量值被发送到融合中心，用来对 PU 信号的存在与否情况进行全局判断. 不存在 PUEA 时，用传统的等增益合并方法[16]计算所有感知报告的总和，并与一个预设阈值相比较. 如果报告的总和超过阈值，则该信道被确定为占用状态；反之，为空闲状态.

通常情况下，PUEA 通过向广播环境中发送伪信号欺骗 CR 用户，以阻止 CR 用户接入空闲频段，因此可通过对攻击者的分析提出适当的频谱感知规则. 设 Q_{fa} 为 CSS 中的全局虚警概率，则

$$\begin{aligned} Q_{\mathrm{fa}} &= P(D^{\mathrm{on}} \mid H_0) = \\ &P(D^{\mathrm{on}} \mid H_0,\ E^{\mathrm{on}})P(E^{\mathrm{on}} \mid H_0) + p(D^{\mathrm{on}} \mid H_0,\ E^{\mathrm{off}})P(E^{\mathrm{off}} \mid H_0) = \\ &P(D^{\mathrm{on}} \mid H_{s2})\beta + P(D^{\mathrm{on}} \mid H_{s0})(1-\beta) \end{aligned} \tag{5}$$

Q_{m} 表示全局漏检概率，则

$$Q_{\mathrm{m}} = P(D^{\mathrm{off}} \mid H_1) = P(D^{\mathrm{off}} \mid H_{s3})\alpha + P(D^{\mathrm{off}} \mid H_{s1})(1-\alpha) \tag{6}$$

式中，D^{on} 和 D^{off} 分别表示融合中心判定 PU 信号存在和不存在的情况.

传统方法不考虑 PUEA 能量，本文定义总误差概率 Q_{e} 评价存在恶意 PUEA 情况时 CSS 的性能. 参数 Q_{e} 表示 PU 信号检测中作出错误判定的概率，即融合中心判断存在 PU 信号而实际上并不存在，或融合中心判定不存在 PU 信号而实际上存在的情况. 总误差概率可以表示为

$$Q_{\mathrm{e}} = P(H_0,\ D^{\mathrm{on}}) + P(H_1,\ D^{\mathrm{off}}) = P(H_0)Q_{\mathrm{fa}} + P(H_1)Q_{\mathrm{m}} \tag{7}$$

结合式(1)、式(5)和式(6)，式(7)可变为：

$$Q_{\mathrm{e}} = P(D^{\mathrm{on}} \mid H_{s0})\pi_0 + P(D^{\mathrm{on}} \mid H_{s2})\pi_2 + P(D^{\mathrm{off}} \mid H_{s1})\pi_1 + P(D^{\mathrm{off}} \mid H_{s3})\pi_3 \tag{8}$$

2　本文攻击感知算法

2.1　攻击参数估计

本小节基于接收到的感知测量数值对 $P(H_0)$ 和 $P(H_1)$ 中攻击参数 α 和 β 进行统一估计. $E(E_j)$ 和 $E(E_j^2)$ 分别为接收到的感知测量值的均值和二阶距，通过式(4)可以得出：

$$\begin{aligned} E(E_j) &= E(E_j \mid H_{s0})\pi_0 + E(E_j \mid H_{s1})\pi_1 + E(E_j \mid H_{s2})\pi_2 + E(E_j \mid H_{s3})\pi_3 = \\ &M\pi_0 + M(\gamma_j+1)\pi_1 + M(\lambda_j+1)\pi_2 + M(\gamma_j+\lambda_j+1)\pi_3 \end{aligned} \tag{9}$$

$$E(m)=M\pi_0+M(\bar{\gamma}+1)\pi_1+M(\bar{\lambda}+1)\pi_2+M(\bar{\gamma}+\bar{\lambda}+1)\pi_3 \tag{10}$$

其中，

$$\bar{\gamma}=\frac{1}{N}\sum_{j=1}^{N}\gamma_j \qquad \bar{\lambda}=\frac{1}{N}\sum_{j=1}^{N}\lambda_j$$

从而有

$$E(E_j^2)=(M^2+2M)\{\pi_0+(\gamma_j+1)^2\pi_1+(\lambda_j+1)^2\pi_2+(\gamma_j+\lambda_j+1)^2\pi_3\} \tag{11}$$

$$E(v)=(M^2+2M)\{\pi_0+(2\bar{\gamma}^2+2\bar{\gamma}+1)\pi_1+(2\bar{\lambda}^2+2\bar{\lambda}+1)\pi_2+(2\bar{\gamma}^2+2\bar{\lambda}^2+2\overline{\gamma\lambda}+2\bar{\gamma}+2\bar{\lambda}+1)\pi_3\} \tag{12}$$

考虑到瞬时信噪比 γ_j 和 λ_j 的指数分布，可得出

$$\frac{1}{N}\sum_{j=1}^{N}\gamma_j^2=2\bar{\gamma}^2$$

和

$$\frac{1}{N}\sum_{j=1}^{N}\lambda_j^2=2\bar{\lambda}^2$$

将式(1)代入式(10)和式(12)，有

$$\begin{cases}\Psi_0\alpha+\Psi_1\beta=\varphi_0\\ \Psi_2\alpha+\Psi_3\beta=\varphi_1\end{cases} \tag{13}$$

式中的参数 $\Psi_0,\Psi_1,\Psi_2,\Psi_3,\varphi_0,\varphi_1$ 定义如下：

$$\Psi_0=P(H_1)M\bar{\lambda}$$

$$\Psi_1=P(H_0)M\bar{\lambda}$$

$$\Psi_2=(2M+M^2)P(H_1)(\bar{\gamma}+\bar{\lambda}+1)2\bar{\lambda}$$

$$\Psi_3=(2M+M^2)P(H_0)(\bar{\lambda}+1)2\bar{\lambda}$$

$$\varphi_0=E(m)-M[P(H_0)+P(H_1)(\bar{\gamma}+1)]$$

$$\varphi_1=E(v)-(2M+M^2)[P(H_0)+P(H_1)(2\bar{\gamma}^2+2\bar{\gamma}+1)]$$

从式(13)中可知，未知攻击参数 α 和 β 的数值为

$$\hat{\alpha}=\frac{\Psi_1\varphi_1-\Psi_3\varphi_0}{\Psi_1\varphi_2-\Psi_0\varphi_3} \qquad \hat{\beta}=\frac{\Psi_2\varphi_0-\Psi_0\varphi_1}{\Psi_1\varphi_2-\Psi_0\varphi_3} \tag{14}$$

满足

$$\Psi_1\Psi_2\neq\Psi_0\Psi_3(\gamma\neq 0)$$

下面将对 α 和 β 函数的最优阈值进行计算.

2.2 最优阈值计算

首先，确定不存在 PUEA 信号($\alpha=\beta=0$)情况下的最优检测阈值. 若不存在 PUEA 信号，将不会出现 H_{s2} 和 H_{s3} 这 2 种状态($\pi_2=\pi_3=0$). 因此，全局误差概率 Q_e 为状态 H_{s0} 和 H_{s1} 检测时的误差概率. 则式(8)为

$$Q_e=P(\Lambda>\eta\mid H_{s0})\pi_0+P(\Lambda<\eta\mid H_{s1})\pi_1 \tag{15}$$

利用如下公式求取最小化误差概率 Q_e 的最优阈值 η^*：

$$\frac{\partial Q_e}{\partial\eta}=0\ \Rightarrow\ \eta^*=\frac{\mu_0\sigma_1^2-\mu_1\sigma_0^2+\sqrt{\xi}}{\sigma_1^2-\sigma_0^2} \qquad \sigma_1^2\neq\sigma_0^2 \tag{16}$$

当 PUEA 存在时，分别在 $\rho\leqslant 1$ 和 $\rho>1$ 两个不同条件下计算最优阈值.

对于 $\rho\leqslant 1$，式(8)中的全局误差概率 Q_e 可表示为

$$Q_e=P(\Lambda>\eta\mid H_{s0})\pi_0+P(\Lambda<\eta\mid H_{s2})\pi_2+P(\Lambda<\eta\mid H_{s1})\pi_1+P(\Lambda>\eta\mid H_{s3})\pi_3 \tag{17}$$

则最优阈值 η^* 为

$$\frac{\partial Q_e}{\partial \eta}=0$$

$$\Rightarrow -\pi_0 F(\eta^*,\mu_0,\sigma_0)+\pi_1 F(\eta^*,\mu_1,\sigma_1)-\pi_2 F(\eta^*,\mu_2,\sigma_2)+\pi_3 F(\eta^*,\mu_3,\sigma_3)=0 \quad (18)$$

式中的函数 $F(\cdot)$为正态分布的概率密度函数，

$$F(x,\mu,\sigma)=\frac{1}{\sigma\sqrt{2\pi}}\exp\frac{-(x-\mu)^2}{2\sigma^2}$$

对于式(18)，可利用数值计算方法求取最优阈值 η^*.

3　仿真实验结果和分析

本文提出的系统模型中，假定一个检测间隔中共有 8 个 CR 用户($N=8$)，样本数 $M=20$；信道为分组衰减；已知 PU 和 CR 用户间的平均信噪比 $\bar{\gamma}$，以及 PUEA 和 CR 用户间的平均信噪比 $\bar{\lambda}$；先验概率 $P(H_0)$和 $P(H_1)$分别为 0.8 和 0.2. 通过超过 10 000 轮的蒙特卡洛仿真得出结果.

为了体现所提方案的优异性，将文献[11]视为对照组. 文献[11]从用户中独立提取信道特征参数，基于硬判决联合检查方法对发射机身份进行验证，即最优用户选择 OUS 的协同频谱感知. 本文提出的误差概率最小化的阈值选取 TSMEP 方案，其特点是对 PU 信号发射机的物理位置或特定属性的先验信息不做任何要求. 2 种方案均考虑了不同的攻击参数和不同的阈值选择情况，如最优阈值和非最优阈值等情况.

攻击参数 $\alpha=0.3$，$\beta=0.7$ 时的收敛情况如图 2 所示. 在进行大约 1 000 和 2 000 轮感知测量后，α 和 β 的估计值分别收敛至常数. $P(H_1)=0.2$，$\alpha=0.3$ 意味着 PUEA 在假设情况 H_1 中仅有 30%的概率发射伪信号，α 的收敛性小于 β 的收敛性. 在仿真中，前 2000 个感知间隔可设为初始阶段，对攻击参数进行估算，之后寻找最优阈值，以提高恶意 PUEA 存在的情况下 CSS 的性能.

在没有 PUEA 伪信号时，虚警概率 Q_{fa}、漏检概率 Q_m 和误差概率 Q_e 与决策阈值的函数曲线如图 3 所示. 平均信噪比 $\bar{\gamma}$ 为−5 dB，阈值变化范围为 0～270. 可以看出，Q_{fa}随着阈值的增加而降低. Q_m 与 Q_{fa}相反，Q_m 随着阈值的增加而增加. 根据图 3 中显示的 Q_e 的形状和 Q_e 最小值存在的特性，可以验证在最优阈值 η^* 处存在最小误差概率 Q_e.

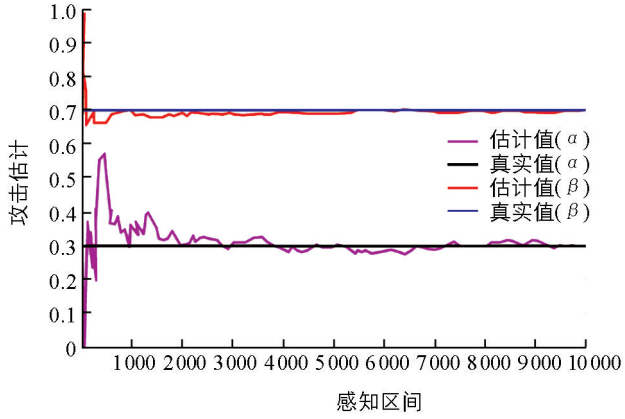

图 2　攻击参数的收敛曲线

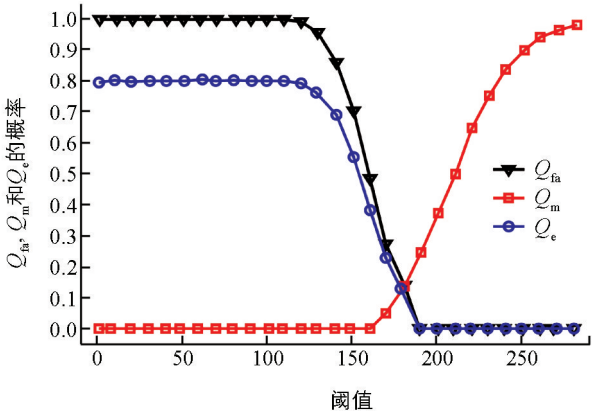

图 3　虚警概率，漏检概率，误差概率与阈值的关系

在不存在攻击和存在攻击的 2 种情况下，融合中心利用最优阈值和非最优阈值时，其总误差概率 Q_e 随着平均信噪比 $\bar{\gamma}$ 的变化情况如图 4 所示. 其中，攻击强度 ρ 设定为 0.5；非最优阈值通过将式(8)中的总虚警概率设为常值 0.1 获得. 对比最优阈值和非最优阈值选取方法的误差概率，文献[11]提出的 OUS 主要是研究无线信道的特征参数，从用户中独立提取信道特征参数，是一种最优用户选择的 CSS. 从图 4 可以看出，最优阈值方法的误差概率更低. 本文的所有后续仿真实验均选取最优阈值.

当攻击强度 ρ 为 0.1，1 和 10 时，误差概率 Q_e 与平均信噪比 $\bar{\gamma}$ 的关系曲线如图 5～图 7. 当 $\rho=0.1$ 时，

本文提出的TSMEP方法有效地抵御了PUEA的破坏性影响. 在$\rho=1$的情况下，本文方法的误差概率也没有超过0.2. 通过与文献[11]的OUS技术相比，本文提出的TSMEP方法显著提高了CSS抵御恶意PUEA信号攻击的性能.

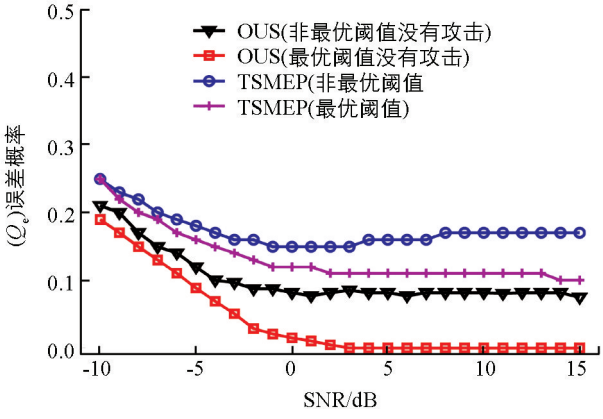

图4 误差概率与平均信噪比$\bar{\gamma}$的关系曲线

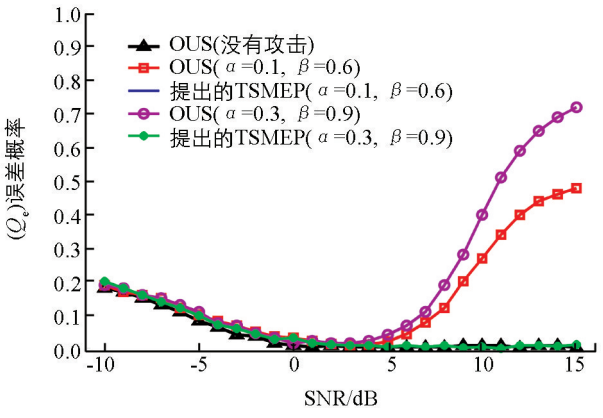

图5 $\rho=0.1$时误差概率与平均信噪比$\bar{\gamma}$的关系曲线

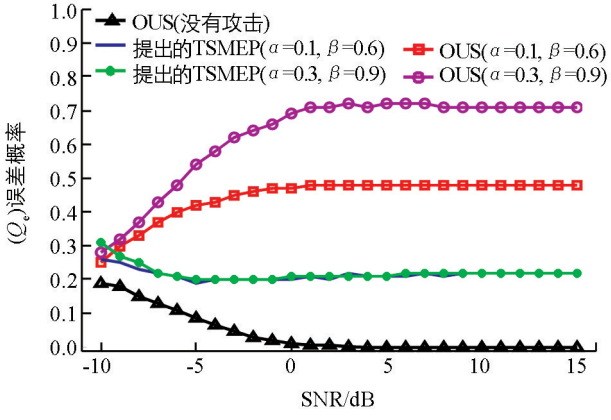

图6 $\rho=1$时误差概率与平均信噪比$\bar{\gamma}$的关系曲线

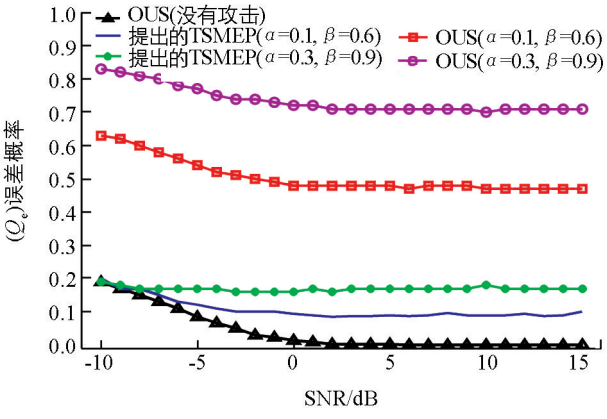

图7 $\rho=10$时误差概率与平均信噪比$\bar{\gamma}$的关系曲线

4 结 论

本文通过对协同频谱感知进行研究，在阈值选取方法的基础上，提出了一种可防御PUEA的协同频谱感知方案. 该方案估计2个攻击参数，即存在和不存在PU信号时，PUEA伪信号出现的概率，并利用该参数确定最小总误差概率的最优阈值，使其可以在PU信号检测中得出较小的概率误差. 仿真实验结果表明，提出的方案较传统方案更加安全有效.

参考文献：

[1] 郑元兵，朱韵攸，王 灿，等. 基于线性价格机制的多认知无线网络资源配置框架 [J]. 西南大学学报(自然科学版)，2016，38(6)：172－179.

[2] 贺欢欢，王兴伟，黄 敏. 认知无线电网络的一种演化博弈频谱共享机制 [J]. 系统仿真学报，2016，28(3)：756－763.

[3] 王 凯，卢为党，郭淑琴，等. 基于功率分配的双向协作频谱接入方法 [J]. 西南师范大学学报(自然科学版)，2015，40(8)：92－98.

[4] 申 滨，王 舒，黄 琼，等. 基于Gerschgorin圆盘理论的认知无线电宽带频谱感知 [J]. 通信学报，2014，35(4)：1－10.

[5] 刘永姣. 认知无线电中基于能量检测的频谱感知技术研究 [D]. 天津：南开大学，2012.

[6] SHEN L，WANG H，ZHANG W，et al. Multiple Antennas Assisted Blind Spectrum Sensing in Cognitive Radio Channels [J]. IEEE Communications Letters，2012，16(1)：92－94.

[7] 曾　昆，彭启航，唐友喜. 基于信任节点辅助的安全协同频谱感知策略 [J]. 信号处理，2011，27(4)：486－490.
[8] 曹开田，王东林. 模拟主用户攻击情况下的压缩宽带频谱感知 [J]. 仪器仪表学报，2015，36(1)：167－173.
[9] 李方伟，冯德俊，朱　江. 一种基于 PUE 恶意干扰的认知无线电态势感知方案 [J]. 电信科学，2013，29(12)：21－27.
[10] CHEN R，PARK J M，REED J. Defense Against Primary User Emulation Attacks in Cognitive Radio Networks [J]. IEEE Journal on Selected Areas in Communications，2008，26(1)：25－37.
[11] 申　滨，王　舒，黄　琼，等. 认知无线电最优用户选择协作频谱感知 [J]. 北京邮电大学学报，2014，37(2)：32－37.
[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] 杨天鸿. 认知无线电网络中的基于信道特征的主用户仿真攻击防御技术 [D]. 杭州：浙江大学，2012.
[14] 杨建新. 认知无线电网络抵御恶意模拟主用户攻击方法的研究 [D]. 昆明：云南民族大学，2015.
[15] DIGHAM F F，ALOUINI M S，SIMON M K. On the Energy Detection of Unknown Signals Over Fading Channels [J]. IEEE Transactions on Communications，2007，55(1)：21－24.
[16] MA J，ZHAO G，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.

An Attack Perception Scheme Based on Optimal Threshold Selection in Cognitive Radio Networks

WANG　Hui[1]，　YU　Yang[2]，　LI Xu-wei[3]

1. *Department of Computer Science and Engineering，Chengdu Neusoft University，Chengdu 611844，China*；
2. *Department of Information Management，Chengdu Neusoft University，Chengdu 611844，China*；
3. *College of Computer，Sichuan University，Chengdu 610064，China*

Abstract：Cognitive radio (CR) networks allow multiple unknown wireless devices to access the spectrum，which often makes the networks vulnerable to primary user emulation attacks (PUEA). Aiming at the problem，a novel cooperative sensing scheme with attack-aware capability in the presence of a malicious PUEA is proposed. First，the probability of the occurrence of PUEA pseudo-signals is estimated in two cases，where the licensed user spectrum resources are occupied or idle. Then，the parameters obtained are used to determine the optimal threshold that minimizes the total error probability. Finally，the fusion center can use the sensing report and the threshold to determine whether a primary user signal is present，so as to have the ability to sense a PUEA attack. Simulation results indicate that compared with the method of optimal user selection，the proposed method has better safety against PUEA and improves the performance of CR networks.

Key words：cognitive radio networks；cooperative spectrum sensing；primary user emulation attack；threshold selection；safety

责任编辑　崔玉洁