文章编号：2095-4980(2016)06-0866-06

CRN 合作频谱感知 SSDF 攻击的博弈分析

吴　伟[1,2]，张小飞[1*]

(1.南京航空航天大学 电子信息工程学院，江苏 南京 210016；2.中国空间技术研究院 载人航天总体部，北京 100094)

摘　要：由于认知无线电网络(CRN)的特点，合作频谱感知容易遭受各种不同的安全威胁。针对CRN合作频谱感知中的感知数据错误化(SSDF)攻击，利用博弈论分析了SSDF攻击者和数据融合中心在不同条件下的行为与收益，并研究了双方基于博弈论的最佳策略。数据融合中心采用本文所述的策略可以有效对抗SSDF攻击，且SSDF攻击者无法通过自身策略的调整获得更大的收益。

关键词：认知无线电；合作频谱感知；感知数据错误化攻击；博弈论

中图分类号：TN014　　**文献标志码：**A　　**doi：**10.11805/TKYDA201606.0866

Game theoretic analysis for cooperative spectrum sensing under SSDF attack in cognitive radio networks

WU Wei[1,2], ZHANG Xiaofei[1*]

(1.College of Electronic Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing Jiangsu 210016, China; 2.Institute of Manned Space System Engineering, China Academy of Space Technology, Beijing 100094, China)

Abstract: Because of the characteristics of Cognitive Radio Networks(CRN), cooperative spectrum sensing is vulnerable to a variety of attacks. Considering the cooperative spectrum sensing under the Spectrum Sensing Data Falsification(SSDF) attack in CRN, the SSDF attacker and the fusion center's behavior and payoff under different conditions are analyzed based on the game theory, and the best strategy for both sides from the view of game theory is studied. When the cooperative sensing fusion center adopts the proposed method, the SSDF attack can be resisted effectively, while the SSDF attacker cannot get more profits through adjusting its own strategy.

Keywords: Cognitive Radio; cooperative spectrum sensing; Spectrum Sensing Data Falsification attack; game theory

由于可以有效缓解无线频谱资源短缺问题，认知无线电(Cognitive Radio，CR)技术[1]得到了广泛研究。频谱感知是 CR 技术实现的首要环节，它负责确定可能被 CR 用户使用的频谱资源，频谱感知性能的好坏将直接关系到 CR 系统的性能。单个 CR 用户容易受到阴影衰落和多径效应的影响，感知性能较差且可能导致“隐藏终端问题”[2]。多个 CR 用户以合作的方式进行频谱感知可以克服单用户频谱感知的不足[3]，但是也容易受到各种安全威胁[4]，比如感知数据错误化(SSDF)攻击。

在存在数据融合中心的合作频谱感知系统中，数据融合中心负责收集 CR 用户的频谱感知数据并做出频谱是否可用的判断[5-6]；而 SSDF 攻击者通过向数据融合中心发送错误化的频谱感知结果，干扰其对频谱使用情况做出正确判断。目前 SSDF 攻击是合作频谱感知安全领域研究的热点问题，J.M.Park 等人利用序贯检测和 CR 用户置信度相结合的方法来对抗 SSDF 攻击[7]。文献[8]通过分析 CR 用户的历史行为来计算 CR 用户的可信度，并在此基础上构建了一套可以对抗 SSDF 攻击的合作频谱感知方法。文献[9]从攻击收益的角度考察了 SSDF 攻击者的行为，并通过对置信度门限的控制使得 SSDF 攻击者失去发起攻击的兴趣。文献[10]指出可以在介质访问控制(Media Access Control，MAC)层设计中加入认证方案来对抗 SSDF 攻击问题。文献[11]和文献[12]则研究了如何对抗多个 SSDF 攻击者同时发起攻击。博弈论适合于分析利益相关方的斗争与合作问题，但目前其在 CR 领域的

收稿日期：2015-09-12；**修回日期：**2015-11-05
基金项目：国家自然科学基金资助项目(61371169)
***通信作者：**张小飞 email:zhangxiaofei@nuaa.edu.cn

应用集中在频谱资源分配[13-16]等方面，在合作频谱感知安全问题中的应用还比较少。文献[17]提出了一种基于随机零和博弈的抗 Jamming 攻击的合作频谱感知方法。文献[18]分析了拜占庭攻击者和数据融合中心的博弈过程和最优策略。文献[19]构建了数据融合中心与恶意 CR 用户之间的博弈模型，并提出了一种基于信誉的数据融合方法来对抗恶意 CR 用户的攻击。

本文将博弈论引入了认知无线电合作频谱感知中的 SSDF 问题，利用博弈论的思想分析了各利益相关方的最佳策略，并分析了 SSDF 攻击者的攻击收益折现率和攻击被发现的概率对博弈均衡的影响。

1　系统模型

1.1 感知模型

考虑由 1 个数据融合中心和 K–1 个诚实的 CR 用户组成的 CR 网络，在这个 CR 网络中，所有 CR 用户都对同一主用户频段的信号进行频谱感知，并将感知结果发送给数据融合中心，由数据融合中心判决该频段上主用户信号是否存在；有 1 个新的 CR 用户(记为第 K 个 CR 用户)加入了该合作频谱感知网络，此 CR 用户是 1 个 SSDF 攻击者，其攻击方法是在感知到主用户信号存在时依然报告主用户信号不存在的感知数据。

所有的 CR 用户(包括 SSDF 攻击者)采用能量检测方法[20]对主用户信号进行感知，每个 CR 用户在 1 个感知周期内采样 N 次。根据中心极限定理[21]，当 N 足够大时，CR 用户的本地感知结果近似地服从正态分布。对于诚实 CR 用户和未发起攻击时的 SSDF 攻击者而言，其感知结果正态分布的期望值和方差分别是：

$$E(X_i)=\begin{cases} N\sigma_i^2 & H_0 \\ (N+\lambda_i)\sigma_i^2 & H_1 \end{cases} \qquad Var(X_i)=\begin{cases} 2N\sigma_i^4 & H_0 \\ 2(N+2\lambda_i)\sigma_i^4 & H_1 \end{cases} \tag{1}$$

式中：X_i 表示第 i 个 CR 用户的感知结果；$\lambda_i=N\mu_i$；σ_i^2 和 μ_i 分别表示第 i 个 CR 用户的噪声方差和本地信噪比(Signal to Noise Ratio, SNR)值；用 H_0 表示目标频段无主用户信号的假设，而用 H_1 表示目标频段主用户信号存在的假设。不失一般性，假设不同 CR 用户的地理位置各不相同且感知结果互不相关。

对于发起攻击时的 SSDF 攻击者，其感知结果正态分布的期望值和方差分别是：

$$E(X_K)=\begin{cases} (N+\lambda_K)\sigma_K^2 & H_0 \\ (N+\lambda_K)\sigma_K^2 & H_1 \end{cases} \qquad Var(X_K)=\begin{cases} 2(N+2\lambda_K)\sigma_K^4 & H_0 \\ 2(N+2\lambda_K)\sigma_K^4 & H_1 \end{cases} \tag{2}$$

数据融合中心采用传统的等增益融合(Equal Gain Combination，EGC)方式对各个 CR 用户的感知结果进行融合，则在数据融合中心不采纳新加入的 SSDF 攻击者的感知数据时，融合结果 $X_c(K–1)$的期望值和方差满足：

$$E\left[X_c(K-1)\right]=\begin{cases} \dfrac{1}{K-1}\displaystyle\sum_{i=1}^{K-1}N\sigma_i^2 & H_0 \\ \dfrac{1}{K-1}\displaystyle\sum_{i=1}^{K-1}(N+\lambda_i)\sigma_i^2 & H_1 \end{cases} \qquad Var\left[X_c(K-1)\right]=\begin{cases} \displaystyle\sum_{i=1}^{K-1}\frac{2N\sigma_i^4}{(K-1)^2} & H_0 \\ \displaystyle\sum_{i=1}^{K-1}\frac{2(N+2\lambda_i)\sigma_i^4}{(K-1)^2} & H_1 \end{cases} \tag{3}$$

当数据融合中心采纳 SSDF 攻击者的感知数据且 SSDF 攻击者未发起攻击时，融合结果 $X_c(K)$的期望值和方差的计算方法与式(3)相同；而当数据融合中心采纳 SSDF 攻击者的感知数据且 SSDF 攻击者发起攻击时，融合结果 $X_c'(K)$ 的期望值和方差满足：

$$E\left[X_c'(K)\right]=\begin{cases} \dfrac{1}{K}\displaystyle\sum_{i=1}^{K}N\sigma_i^2 & H_0 \\ \dfrac{1}{K}\left[N\sigma_K^2+\displaystyle\sum_{i=1}^{K-1}(N+\lambda_i)\sigma_i^2\right] & H_1 \end{cases} \qquad Var\left[X_c'(K)\right]=\begin{cases} \displaystyle\sum_{i=1}^{K}\frac{2N\sigma_i^4}{K^2} & H_0 \\ \dfrac{2N\sigma_K^4}{K^2}+\displaystyle\sum_{i=1}^{K-1}\frac{2(N+2\lambda_i)\sigma_i^4}{K^2} & H_1 \end{cases} \tag{4}$$

得出融合结果后，数据融合中心作出以下判断：

$$X_c \underset{H_0}{\overset{H_1}{\gtrless}} \gamma_c \tag{5}$$

采用 Neyman-Pearson 准则，判决门限 γ_c 可以由指定的虚警概率得出，进而检测概率可由此门限 γ_c 计算得出：

$$P_f=Q\left[\frac{\gamma_c-E(X_c\mid H_0)}{\sqrt{Var(X_c\mid H_0)}}\right] \qquad P_d=Q\left[\frac{\gamma_c-E(X_c\mid H_1)}{\sqrt{Var(X_c\mid H_1)}}\right] \tag{6}$$

由上分析可知，在数据融合中心不采纳 SSDF 攻击者感知数据、数据融合中心采纳 SSDF 攻击者感知数据但 SSDF 攻击者未发起攻击、数据融合中心采纳 SSDF 攻击者感知数据且 SSDF 攻击者发起攻击 3 种情况下，可以得出 3 个不同的检测概率，分别记为 $P_{\mathrm{d}}(K-1)$, $P_{\mathrm{d}}(K)$ 和 $P'_{\mathrm{d}}(K)$。

1.2 博弈模型

此 CR 网络所有参与者分为 2 个利益方：K–1 个诚实的 CR 用户及数据融合中心为一个利益方，其希望提升合作频谱感知的检测性能；SSDF 攻击者为另一个利益方，其希望降低合作频谱感知的检测性能。

为方便描述，以下在讨论 2 个利益方博弈时，用数据融合中心代表 K–1 个诚实的 CR 用户及数据融合中心，则本文描述的合作频谱感知过程可视为数据融合中心与 SSDF 攻击者的两方博弈过程，该博弈的模型描述如下：

1) 参与者：参与者 1(数据融合中心)和参与者 2(SSDF 攻击者)，记为博弈参与者集合 $j\in J, J=\{1,2\}$；

2) 策略空间：数据融合中心的策略空间 $\boldsymbol{r}_1=${采纳数据，不采纳数据}，SSDF 攻击者的策略空间 $\boldsymbol{r}_2=${攻击，不攻击}；

3) 收益函数：数据融合中心的收益为其检测概率的上升值，记为 U_1，SSDF 攻击者的收益为数据融合中心检测概率的下降值减去其攻击的开销，记为 U_2。

此博弈可用图 1 的策略矩阵描述：C 代表攻击者发起攻击的开销，$[P_{\mathrm{d}}(K-1)-P'_{\mathrm{d}}(K)]$是指由于 SSDF 攻击者发起攻击而数据融合中心采纳其数据后检测概率的下降值，而$[P_{\mathrm{d}}(K)-P_{\mathrm{d}}(K-1)]$则表示 SSDF 攻击者未发起攻击从而发送真实感知数据给数据融合中心且数据融合中心采纳其数据后检测概率的上升值。在以下讨论中，假定 $P_{\mathrm{d}}(K)$, $P_{\mathrm{d}}(K-1)$和 $P'_{\mathrm{d}}(K)$满足 $P_{\mathrm{d}}(K)>P_{\mathrm{d}}(K-1)>P'_{\mathrm{d}}(K)$，即 K–1 个诚实的 CR 用户的合作感知性能弱于 K 个诚实的 CR 用户的合作感知性能，但是强于 K–1 个诚实的 CR 用户和 1 个 SSDF 攻击者的合作频谱感知性能。

		SSDF attacker (2)	
		attack	not attack
data fusion center (1)	adopt	$P'_{\mathrm{d}}(K)-P_{\mathrm{d}}(K-1)$, $P_{\mathrm{d}}(K-1)-P'_{\mathrm{d}}(K)-C$	$P_{\mathrm{d}}(K)-P_{\mathrm{d}}(K-1)$, $P_{\mathrm{d}}(K-1)-P_{\mathrm{d}}(K)$
	not adopt	0, $-C$	0,0

Fig.1 SSDF attacker and fusion center's game

图 1 SSDF 攻击者与数据融合中心的博弈

上述博弈模型是一个较为简化的完全信息博弈模型。在实际场景中，博弈双方尤其是 SSDF 攻击者的完全决策信息是更加复杂且难以获取的，但认知无线网络可通过对各个 CR 用户的信道衰落、噪声等环境因素及各个 CR 用户的行为进行有效监测，并辅以强力的惩罚手段来吓阻 SSDF 攻击者采取其他的策略，同时数据融合中心的策略一般对各个 CR 用户是公开的，因此用上述完全信息博弈模型分析认知无线网络合作频谱感知中 SSDF 攻击有一定的实际意义。

1.3 SSDF 攻击者收益

由图 1 可知，攻击者发起攻击的开销 C 是博弈的关键影响因素之一。对于不同的攻击者而言，其攻击开销 C 不同。考虑一种极端情况：SSDF 攻击者完全不顾及攻击开销，即 C=0，则无论数据融合中心的策略如何，攻击都是 SSDF 攻击者的弱优势策略，因此在此极端情况下的弱占优策略均衡为：SSDF 攻击者发起攻击，而数据融合中心不采纳新加入 CR 用户的数据。考虑另一种极端情况，若 SSDF 攻击者攻击的开销为 ∞，则不攻击是 SSDF 的严格优势策略，则在此极端情况下有严格占优策略均衡：SSDF 攻击者不发起攻击，而数据融合中心采纳新加入 CR 用户的数据。

在实际情况中，SSDF 攻击者的攻击开销一般在 0 至 ∞ 之间，此时本博弈无纯策略博弈均衡点。考虑如下场景：在 SSDF 攻击者发起攻击时，有 θ 的概率被数据融合中心发现$(0<\theta<1)$，且被发现后其数据再也不会被采纳，从而无法再获得攻击收益。假设 SSDF 攻击者收益的折现率为 $\varepsilon(0<\varepsilon<1)$，折现率是指 SSDF 攻击者在下一个感知周期发起攻击获得的收益折合成当前收益的比率。不考虑其他攻击开销，则 C 满足以下等式：

$$C=\theta\{[P_{\mathrm{d}}(K-1)-P'_{\mathrm{d}}(K)-C]\varepsilon+[P_{\mathrm{d}}(K-1)-P'_{\mathrm{d}}(K)-C]\varepsilon^2+[P_{\mathrm{d}}(K-1)-P'_{\mathrm{d}}(K)-C]\varepsilon^3\cdots\} \tag{7}$$

可知：

$$C=\frac{\theta\varepsilon}{\theta\varepsilon+(1-\varepsilon)}\left[P_{\mathrm{d}}(K-1)-P'_{\mathrm{d}}(K)\right] \tag{8}$$

2　纳什均衡

定义 1：纳什均衡被定义为：

$$U_j(\boldsymbol{r}_j^*,\boldsymbol{r}_{-j})\geqslant U_j(\boldsymbol{r}_j',\boldsymbol{r}_{-j}),\forall j,\forall \boldsymbol{r}_j'\in\boldsymbol{r}_j \tag{9}$$

即对于一博弈方的行为，没有其他博弈方能够通过单独改变行为而获得更大的收益。如果 1 个博弈方在任何情况下都采用 1 个策略，则该策略为纯策略。按照定义 1，在 $P_d(K)>P_d(K-1)$的条件下，图 1 所示的博弈无纯策略纳什均衡解。

定义 2：混合策略纳什均衡被定义为：

$$\sum_{r_{-j}\in\boldsymbol{r}_{-j}} p(r_j,r_{-j})\left[U_j(r_j',r_{-j})-U_j(r_j,r_{-j})\right]\leqslant 0,\forall r_j'\in\boldsymbol{r}_j \tag{10}$$

式中 p 为 1 个概率分布，表示各个博弈方采用各个策略的概率。

定理 1：在有限个参与者的标准式博弈中，若每个参与者的策略空间中的纯策略是有限个数的，则博弈至少存在 1 个纳什均衡(纯策略或混合策略)。

由定理 1 可知，图 1 的博弈必然存在 1 个混合策略纳什均衡解。用 w_1 表示数据融合中心采纳 SSDF 攻击者数据的概率，用 w_2 表示 SSDF 用户发起攻击的概率，则在概率$\{w_1,w_2\}$下，数据融合中心和 SSDF 攻击者的收益函数分别为：

$$U_1=w_1w_2[P'_d(K)-P_d(K-1)]+w_1(1-w_2)[P_d(K)-P_d(K-1)] \tag{11}$$

$$U_2=w_1w_2[P_d(K-1)-P'_d(K)-C]+w_1(1-w_2)[P_d(K-1)-P_d(K)]+(1-w_1)w_2(-C) \tag{12}$$

C 用式(8)代替，采用微分法求解博弈均衡点，由 $\frac{\partial U_1}{\partial w_1}=0$ 和 $\frac{\partial U_2}{\partial w_2}=0$ 可知：

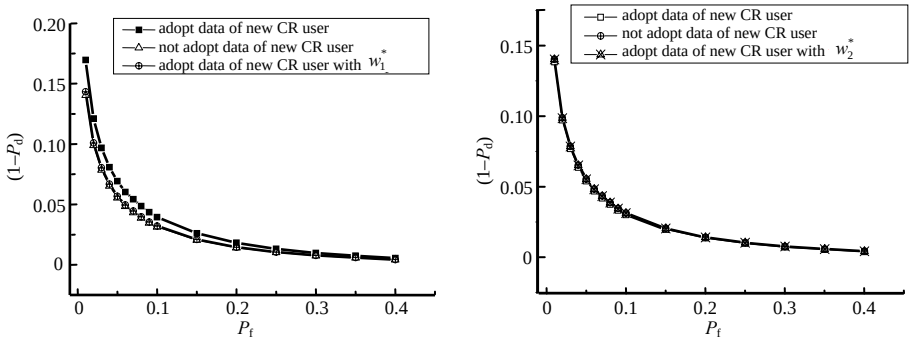
$$w_1^*=\frac{\theta\varepsilon}{\theta\varepsilon+(1-\varepsilon)}\cdot\frac{P_d(K-1)-P_d'(K)}{P_d(K)-P_d'(K)},\quad w_2^*=\frac{P_d(K)-P_d(K-1)}{P_d(K)-P_d'(K)} \tag{13}$$

由定义 2 可知，在 $P_d(K)>P_d(K-1)>P'_d(K)$, $0<\theta<1$ 和 $0<\varepsilon<1$ 条件下，$\{w_1^*,w_2^*\}$即为本博弈的混合策略均衡解。

3　仿真与分析

3.1　数据融合中心均衡策略性能分析

设 K=10，即此 CR 网络包括 9 个诚实的 CR 用户和 1 个新进入的 SSDF 攻击者。为简化仿真，假设所有 CR 用户和 SSDF 攻击者所处环境的 SNR 值都是–4 dB，且噪声方差 $\sigma_i^2=1(i=1,2,3,\cdots,K)$，同时假设所有 CR 用户和 SSDF 攻击者在每个感知周期内采样 20 次，SSDF 发起攻击时被数据融合中心发现的概率 θ 为 0.1，SSDF 攻击者收益的折现率 ε 为 0.7。图 2(a)和图 2(b)对比了在数据融合中心分别采取完全不采纳新加入 CR 用户的数据、完全采纳新加入 CR 用户的数据和以式(13)的比率采用新加入 CR 用户的数据 3 种策略情况下，当 SSDF 攻击者一直发起攻击时和以式(13)的概率发起攻击时的漏检概率对比。



(a) comparison of the miss detection performance among 3 strategies when the SSDF attacker attacks all the time

(b) comparison of the miss detection performance between 3 strategies when the SSDF attacker attacks with the probability presented in this paper

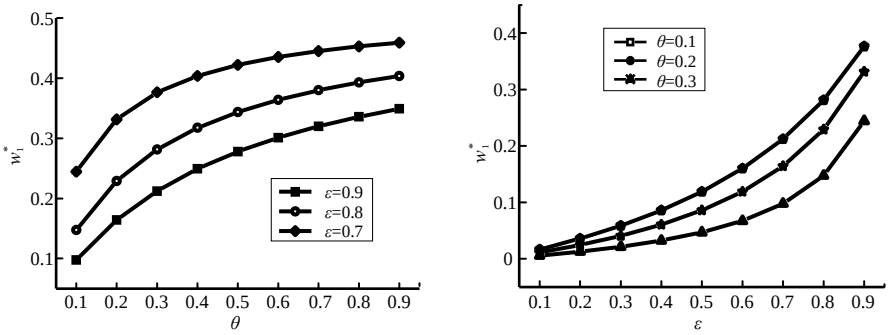
Fig.2 Comparison of the miss detection performance among 3 strategies when the SSDF attacker attacks all the time and with the probability presented in this paper

图 2　三种融合策略的漏检概率比对

由图 2(a)可知，当存在 SSDF 攻击者一直发起攻击时，完全信任新加入 CR 用户的数据是不合适的，而以式(13)的比率采纳新加入 CR 用户的数据所达到的检测性能则与完全不采纳新加入 CR 用户数据的方案相当。由图 2(b)可知，当 SSDF 攻击者以本文所述的 w_2^* 的概率发起攻击时，数据融合中心采用 3 种策略的检测性能相当，即此时数据融合中心无法通过策略的选择来提升自身的感知性能，此结论与定义 2 相吻合。

3.2 不同 θ 和不同 ε 对均衡的影响

由式(13)可知，不同的 SSDF 攻击被发现概率 θ 和不同的 SSDF 攻击收益折现率 ε 都会影响数据融合中心的策略。依然设置 K=10，即包括 9 个诚实 CR 用户和 1 个新加入的 SSDF 攻击者，且假设所有 CR 用户和 SSDF 攻击者所处环境的 SNR 值、噪声方差和采样次数也与 3.1 节相同。图 3 反映了在以上条件下，当要求虚警概率 P_f 为 0.01 时，ε 等于 0.7,0.8,0.9 和 θ 等于 0.1,0.2,0.3 时，数据融合中心采纳新加入 CR 用户数据的概率：由图 3(a)和图 3(b)可见，在相同的 θ 下，折现率 ε 越大，即 SSDF 攻击者越在意未来的攻击收益，则数据融合中心可以更高的概率采纳新加入 CR 用户的数据；在相同的 ε 下，数据融合中心发现 SSDF 攻击的能力越强，即 θ 越大，则数据融合中心也可以更高的概率采纳新加入 CR 用户的数据。



(a) effects of different θ on fusion center's strategy (b) effects of different ε on fusion center's strategy

Fig.3 Effects of different θ(Fig.a) and different ε(Fig. b) on fusion center's strategy

图 3 不同的 θ 和不同的 ε 对数据融合中心策略的影响

4 结论

合作频谱感知可以有效避免单用户频谱感知的弱点，但是其容易受到 SSDF 等攻击的威胁，所以数据融合中心需要考虑新加入 CR 用户是 SSDF 攻击者情况下的策略。本文利用博弈论分析了 SSDF 攻击者和数据融合中心的最佳策略，并考虑了 SSDF 攻击者收益折现率与数据融合中心发现 SSDF 攻击者的能力对该博弈均衡的影响。仿真结果表明，数据融合中心以特定的比率采纳新加入 CR 用户感知数据的比率，在遭受到 SSDF 攻击时能保持较好的感知性能；同时，SSDF 攻击者越在意未来的攻击收益，或数据融合中心发现 SSDF 攻击者的能力越强，则数据融合中心越可以提升采纳新加入 CR 用户感知数据的比率。

参考文献：

[1] MITLOA J,MAGUIRE Jr G Q. Cognitive radio: making software radios more personal[J]. IEEE Personal Communications, 1999,6(4):13–18.

[2] AKYILDIZ I F,LEE W Y,VURAN M C,et al. A survey on spectrum management in cognitive radio networks[J]. IEEE Communications Magazine, 2008,46(4):40–48.

[3] GANESAN G,LI Y. Cooperative spectrum sensing in cognitive radio networks[C]// 2005 First IEEE International Symposium New Frontiers in Dynamic Spectrum Access Networks. Baltimore,MD,USA:IEEE, 2005:137–143.

[4] CHEN R,PPARK J M. Ensuring trustworthy spectrum sensing in cognitive radio networks[C]// 2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks. [S.l.]:IEEE, 2006:110–119.

[5] PEH E,LIANG Y C. Optimization for cooperative sensing in cognitive radio networks[C]// 2007 IEEE Wireless Communications and Networking Conference. Washington,DC,USA:IEEE, 2007:27–32.

[6] CHEN H,WU W,XIE L. Cooperative spectrum sensing scheme with light communication overhead in cognitive radio networks[C]// 2010 IEEE 21st International Symposium on Personal Indoor and Mobile Radio Communications(PIMRC). [S.l.]:IEEE, 2010:1539–1543.

[7] CHEN R,PARK J M,BIAN K. Robust distributed spectrum sensing in cognitive radio networks[C]// 2008 The 27th Conference on Computer Communications. [S.l.]:IEEE, 2008:1–7.

[8] FENG J,ZHANG Y,LU G,et al. Defend against collusive SSDF attack using trust in cooperative spectrum sensing environment[C]// 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. [S.l.]:IEEE, 2013:1656–1661.

[9] WU W,ZHANG X F,CHEN X M. A SSDF–Attack–Exclusion cooperative spectrum sensing scheme in cognitive radio networks[J]// Applied Mechanics and Materials, 2014,556–562:5219–5222.

[10] NGUYEN–THABH N,NGUYEN V T. Medium access control design for cognitive radio networks:a survey[J]. IEICE Transactions on Communications, 2014,97(2):359–374.

[11] LIU B,WANG M,ZHANG C,et al. Robust sensor selection for collaborative spectrum sensing with attacks under correlated shadowing[C]// 2014 IEEE International Conference on Communications Workshops(ICC). [S.l.]:IEEE, 2014:279–284.

[12] HYDER C S,GREBUR B,XIAI L,et al. ARC:adaptive reputation based clustering against spectrum sensing data falsification attacks[J]. IEEE Transactions on Mobile Computing, 2014,13(8):1707–1719.
[13] NI Q,ZATAKOVITIS C C. Nash bargaining game theoretic scheduling for joint channel and power allocation in cognitive radio systems[J]. IEEE Journal on Selected Areas in Communications, 2012,30(1):70–81.
[14] ELMACHKOUR M,DAHA I,SABIR E,et al. Green opportunistic access for cognitive radio networks:a minority game approach[C]// 2014 IEEE International Conference on Communications(ICC). [S.l.]:IEEE, 2014:5372–5377.
[15] SHARMA A,HASTIR V,SAINI D S. Transmit power optimization in cognitive radio networks using game theoretic approach[C]// 2014 International Conference on Signal Propagation and Computer Technology(ICSPCT). [S.l.]:IEEE, 2014:312–316.
[16] 张齐新,杨涛,冯辉,等. 车联网中基于分布式博弈的移动网关选取算法[J]. 太赫兹科学与电子信息学报, 2015,13(1):94–100. (ZHANG Qixin,YANG Tao,FENG Hui,et al. A distributed game theoretic approach for dynamic gateway selection in VANETs[J]. Journal of Terahertz Science and Electronic Information Technology, 2015,13(1):94–100.)
[17] LIU K J R,WANG B. Cognitive Radio Networking and Security:A Game-theoretic View[M]. New York,NY,USA:Cambridge University Press, 2010.
[18] VEGY M K. Study of Byzantine attacks and countermeasures in spectrum sensing[D]. Oklahoma:Oklahoma State University, 2014.
[19] WANG J,CHEN I R. Trust-based data fusion mechanism design in cognitive radio networks[C]// 2014 IEEE Conference on Communications and Network Security(CNS). [S.l.]:IEEE, 2014:53–59.
[20] KAY S M. Fundamentals of Statistical Signal Processing:Detection Theory[M]. 2nd ed. New Jersey,US:PTR Prentice Hall, 1998.
[21] GNEDENKO B V,KOLMOGOROV A N,DOOB J L,et al. Limit Distributions for Sums of Independent Random Variables[M]. Massachusetts:Addison–Wesley, 1968.

作者简介:

吴　伟(1986–),男,湖北省汉川市人,在读博士研究生,主要研究方向为认知无线电网络中的频谱感知问题.email:39834290@qq.com.

张小飞(1977–),男,江苏省淮安市人,教授,博士生导师,主要研究方向为数字通信、通信信号处理、阵列信号处理、雷达信号处理.email:zhangxiaofei@nuaa.edu.cn.

(上接第 865 页)

[11] NEILSEN M A,CHUANG I L. Quantum Computation and Quantum Information[M]. Cambridge:Cambridge University Press, 2000.
[12] HOUSHMAND M,HOSSEINI-KHAYAT S. Minimal-memory realization of pearl-necklace encoders of general quantum convolutional codes[J]. Physical Review A, 2010,83(2):782–787.
[13] HOUSHMAND M,HOSSEINI-KHATAT S,WILDE M M. Minimal-memory requirements for pearl-necklace encoders of quantum convolutional codes[J]. IEEE Trans. Computers, 2012,61(3):299–312.

作者简介:

邱鹏辉(1993–),男,福建省三明市人,在读博士研究生,主要研究方向为量子通信与量子编码.email:qphfj@163.com.

陈晓光(1964–),男,安徽省五河县人,博士,副教授,主要研究方向为无线通信与量子通信.