文章编号:1001 - 893X(2011)03 - 0063 - 06

抗 SSDF 攻击的 EWSPRT 协作频谱感知方案*

刘 全,郭云玮,高 俊,刘思洋

(海军工程大学 通信工程系,武汉 430033)

摘 要:比较了认知无线电网络中几种典型的协作感知方案在篡改感知数据(SSDF)攻击条件下的感知性能,并提出了一种增强型加权序贯检测(EWSPRT)协作方案。在该方案中,各次用户首先通过能量检测得到2 bit本地决策,然后收集其它协作用户的感知结果进行决策融合和最终判决,并依据历史观测信息动态更新各协作用户的融合权重;利用改进的信任度更新算法能使恶意用户的融合权重更快地降低,从而有效地减少 SSDF 攻击对协作过程的影响。Monte - Carlo 仿真结果表明,与传统方案相比,EWSPRT 方案能够更有效地抵抗 SSDF 攻击。

关键词:认知无线电;协作频谱感知;篡改感知数据攻击;加权序贯检测

中图分类号:TN92 **文献标识码**:A doi:10.3969/j.issn.1001 - 893x.2011.03.015

Robust EWSPRT Cooperative Spectrum Sensing Scheme against SSDF Attacks

LIU Quan, GUO Yun-wei, GAO Jun, LIU Si-yang

(Department of Communication Engineering, Naval University of Engineering, Wuhan 430033, China)

Abstract: This paper compares the sensing performance of several typical cooperative spectrum sensing (CSS) strategies under spectrum sensing data falsification (SSDF) attack in cognitive radio networks, and presents a new CSS scheme named as enhanced weighted sequential probability ratio test (EWSPRT). In the proposed scheme, each secondary user (SU) firstly makes a two - bit local decision via energy detection, then collects the decisions from nearby cooperative users, and finally obtains a decision with some decision fusion rule. The modified rule for updating the credit level can reduce the fusion weight of those potential attackers as early as possible, which effectively decreases the negative impacts of SSDF attacks. As represented by the Monte - Carlo simulation results, the EWSPRT scheme has better robustness against SSDF attacks than the traditional schemes.

Key words: cognitive radio; cooperative spectrum sensing; spectrum sensing data falsification attack; weighted sequential probability ratio test

1 引 言

认知无线电(Cognitive Radio, CR)技术作为无线通信领域的“下一个大事件”,采用动态频谱接入方式实现非授权(次)用户对频谱空洞的“二次利用”[1],能够有效地提高频谱利用效率,从根本上缓解频谱资源的紧张局面。CR 技术需要解决的首要问题是如何快速而准确地获取周围环境中的动态频谱信息[1,2]。现有的频谱感知算法大部分是从经典的信号检测理论中移植过来的[2],其中研究和应用

* **收稿日期**:2010 - 12 - 28;**修回日期**:2011 - 02 - 18
基金项目:国家高技术研究发展计划(863 计划)项目(2009AAJ208, 2009AAJ116)
Foundation Item: The National High - tech R&D Program (863 Program) of China (No.2009AAJ208, 2009AAJ116)

最广的是能量检测,因为其具有简单易实现、成本低廉、无需任何先验知识等突出优点[3]。然而,在实际信道中,由于受到多径或阴影衰落等多方面因素的影响,单个次用户的频谱感知精度非常有限[2]。鉴于此,文献中提出了多种协作频谱感知(Cooperative Spectrum Sensing, CSS)方案,将多个次用户的本地感知决策或数据按照一定规则进行信息融合处理后做出最终判决,可有效地提高整体的感知性能[2,4]。但是,在现有的大多数协作感知方案中,次用户网络在获得协作增益的同时也面临着新的安全问题。由于协作控制信道的开放性,敌方或恶意攻击节点可以伪装成合法次用户向融合中心发送错误或者混乱的感知结果,从而影响最终的融合判决。由于这些攻击通常都是通过恶意篡改本地感知结果来实现的,所以被统称为篡改感知数据 (Spectrum Sensing Data Falsification, SSDF)攻击[5]。在现有文献中,专门针对 SSDF 攻击的协作感知方案并不多见,文献[6]提出了加权序贯检测(Weighted Sequential Probability Ratio Test, WSPRT)方案,依据各协作用户的历史决策信息将恶意节点的融合权重逐渐降低。文献[7,8]在此基础上进行了一些改进,给出了新的权值更新算法,进一步提高了检测性能,但这些文献中均没有考虑感知信道中阴影及衰落效应的影响。文献[9]则采用基于数据挖掘的异常节点检测算法直接将恶意节点剔除后再进行决策融合及判决。本文在这些文献的基础上,对 SSDF 攻击条件下的协作感知策略进行了深入研究,比较了 WSPRT 等几种典型协作感知方案在 SSDF 攻击条件下的感知性能,提出了一种基于2 bit决策融合的增强型加权序贯检测(Enhanced Weighted Sequential Probability Ratio Test, EWSPRT)方案,给出了改进的节点信任度更新方法,并在衰落信道条件下进行了仿真,证明了该方案抵抗 SSDF 攻击的有效性。

2 系统模型

考虑一个分布式的认知无线电网络,假设 N 个次用户通过协作进行感知,其中有 N_a 个恶意用户,可随时向邻接点发动 SSDF 攻击。每个次用户可随机缓慢移动,同时具备本地感知和信息融合功能。各次用户首先独立地进行能量检测得到本地决策 $u_i(i\in[1,N])$,然后作为融合中心(Fusion Center, FC)收集邻近用户的感知结果进行决策融合并作出最终判决 u。

2.1 信道模型

主用户信号在感知信道中传输不仅会有路径损耗和噪声叠加,而且会发生多径或阴影衰落,通常可将实际信道的统计特性用接收信号的瞬时信噪比(dB 形式)描述[10]:

$$\gamma_{\mathrm{dB}}=\bar{\gamma}_{\mathrm{dB}}+Shadow_{\mathrm{dB}}+Fading_{\mathrm{dB}} \tag{1}$$

式中,$\bar{\gamma}_{\mathrm{dB}}$表示接收端的平均信噪比 $\bar{\gamma}$ 的 dB 形式,用于描述信号功率的路径损耗,本文采用 IEEE 802.22协议推荐的 HATA 模型[11]; $Shadow_{\mathrm{dB}}$和 $Fading_{\mathrm{dB}}$是两个随机变量,分别表示信道中的阴影衰落效应和多径衰落效应[10]。根据实际环境测试数据显示,阴影衰落信道的功率线性增益(相对 dB 而言)服从对数正态分布,则 $Shadow_{\mathrm{dB}}\sim N(0,\sigma_{\mathrm{dB}}^2)$,$\sigma_{\mathrm{dB}}$为功率发散因子[12];而多径衰落信道中,接收信号包络多数服从瑞利分布,其相应的线性信道增益服从指数分布[12]。若信道中同时存在阴影和多径衰落,则称为 Suzuki 信道[10],其瞬时信噪比的概率密度分布函数(PDF)可表示为[10]

$$f_\gamma(x)=\int_0^\infty \frac{1}{t^2}\frac{10}{\ln(10)}\frac{1}{\sqrt{2\pi}\sigma_{\mathrm{dB}}}\mathrm{e}^{\left(-\frac{x}{t}-\frac{(10\lg(t)-10\lg(\bar{\gamma}))}{2\sigma_{\mathrm{dB}}^2}\right)}\mathrm{d}t \tag{2}$$

常用的 AWGN 信道只考虑路径损耗,而不考虑多径衰落以及阴影效应的影响,其它衰落信道如 Log-normal Shadowing、Rayleigh 等,$f_\gamma(x)$ 均有所不同,其具体形式可参见文献[10]。

2.2 常用的协作感知方案

K-N 准则[12]:N 个协作用户上报的本地决策中至少有 K 个为'1'(即主用户存在),则决策融合的最终判决为'1'。特别地,当 K 取值为 1、$\lceil N/2\rceil$和 N 时,分别称为 OR、Majority 和 AND 融合准则。

联合似然比检测(LRT)[6]:H_0 和 H_1 分别表示主用户信号不存在和存在的假设,P_0 和 P_1 分别为 H_0 和 H_1 发生的先验概率,C_{10}表示虚警代价,C_{01}表示漏检代价,C_{00}和 C_{11}表示正确检测的代价,则联合似然比 L_N 可表示为

$$L_N=\prod_{i=0}^{N}\frac{P[u_i|H_1]}{P[u_i|H_0]} \tag{3}$$

将其与设定的门限值 λ_N 进行比较,$L_N>\lambda_N$ 时,判决 $u=1$,反之 $u=0$。根据文献[6],若采用 Bayesian 判决准则,则 $\lambda_N=\frac{P_0(C_{01}-C_{00})}{P_1(C_{01}-C_{11})}$;若采用 Neyman-Pear-

son 准则,则应最小化漏检概率以确定 λ_N 值。

2.3 SSDF 攻击

恶意节点通过故意篡改感知数据发动 SSDF 攻击,主要有以下 4 种可能形式[4, 5, 9, 13]:

(1)反向型攻击(Reversed Attack,REA),即始终发送与实际感知结果相反的决策;

(2)自私型攻击(Selfish Attack, SFA),主要是指恶意用户始终向邻接点发送决策'1',使其它用户误以为当前信道被占用,从而使大量空闲频谱资源被浪费或被敌方侵占;

(3)干扰型攻击(Interference Attack, IFA),即恶意用户在信息交互过程中始终发送'0',使其它用户误以为信道空闲而盲目发射造成对主用户干扰;

(4)混乱型攻击(Confusing Attack, CFA),恶意用户随机发送感知结果,时对时错,造成邻接点的决策融合混乱。

3 WSPRT 协作方案

为了抵抗 SSDF 攻击,文献[6]提出了 WSPRT 协作方案。该方案在传统的序贯检测(SPRT)[6]基础上,为每个协作节点引入信任度 r_i,对应的融合权重为 w_i,则检测统计量为[6]

$$S_n = \prod_{i=0}^{n}\left(\frac{P[u_i \mid H_1]}{P[u_i \mid H_0]}\right)^{w_i} \tag{4}$$

然后,按以下规则进行最终判决[6]:

$$\begin{cases} S_n \geqslant \lambda_1, \text{判决 } \mu = 1 \\ S_n \leqslant \lambda_0, \text{判决 } \mu = 0 \\ \lambda_0 \leqslant S_n \leqslant \lambda_1, \text{待进一步判断} \end{cases} \tag{5}$$

式中,n 为融合的本地决策个数,判决门限值 λ_1 和 λ_0 分别由系统所需的虚警概率 Q_f 和漏检概率 Q_m 确定[6]:

$$\lambda_1 = \frac{1-Q_m}{Q_f}, \lambda_0 = \frac{Q_m}{1-Q_f} \tag{6}$$

当 $w_i = 1$ 时,WSPRT 与传统的 SPRT 相同。每判决一次,则 FC 根据当前各节点的本地决策 u_i 与最终决策 u 的比较结果,更新其信任度 r_i: $r_i = r_i + (-1)^{u_i - u}$,并调整各节点的融合权重 w_i[6]:

$$w_i = \begin{cases} 0, & r_i \leqslant g \\ \dfrac{r_i - g}{\max(r_i) - g}, & r_i > g \end{cases} \tag{7}$$

式中,g 为调节 r_i 的特定门限值[6]。当 $r_i \leqslant g$ 时,则可将该节点判定为恶意节点,其融合权重为 0,这样就可以避免协作过程遭到 SSDF 攻击。

4 EWSPRT 协作感知方案

在 WSPRT 方案中,各次用户的接收信号功率 P_{r_i} 分别与本地检测门限 Λ 进行比较,作出1 bit的本地决策 u_i,即'0'或'1',且 Λ 由接收机灵敏度和背景噪声来确定[8]。为了保留更多的本地检测信息,在 EWSPRT 方案中,拟采用 M bit 的本地决策,考虑到协作开销和控制信道带宽的限制,以下选择2 bit ($M=2$)决策进行分析。引入本地检测门限值系数 $a(a>1)$,则得到 $a\Lambda$、Λ、Λ/a 3 个本地检测门限,将接收信号功率划分为 4 档,并由此作出2 bit本地决策:

$$u_i = \begin{cases} 11, & P_{ri} \geqslant a\Lambda \\ 10, & \Lambda \leqslant P_{ri} < a\Lambda \\ 01, & \Lambda/a \leqslant P_{ri} < \Lambda \\ 00, & P_{ri} < \Lambda/a \end{cases} \tag{8}$$

将各次用户的融合权重首先初始化为 1,并由式(6)确定 λ_1、λ_0,然后按式(4)计算检测统计量 S_n,若 $S_n \geqslant \lambda_1$,最终判决 $u=1$;若 $S_n \leqslant \lambda_0$,则 $u=0$;若 $\lambda_0 < S_n < \lambda_1$,则转入下一次检测。每完成一次最终判决,则计算各节点的本地决策 u_i 与 u 之间的距离,并用 du_i 表示,具体计算方法略。根据 du_i,调整各节点的信任度 r_i,其调整增量 Δr_i 按以下线性规则得到:

$$\Delta r_i = (-2) \times du_i/(2^M - 1) + 1 \tag{9}$$

式(9)利用的是距离 du_i 与信任值 r_i 之间的线性关系进行更新。为使信任值更新得更快,可构建非线性关系,对感知结果与最终决策偏差较大的节点进行一定的惩罚,从而减少算法的循环次数,尽可能降低恶意攻击造成的影响。例如,采用以下非线性规则使 r_i 的调整增量为

$$\Delta r_i = 2 \times (du_i - (2^M - 1))^2/(2^M - 1)^2 - 1 \tag{10}$$

根据以上分析,下面给出 EWSPRT 的算法流程:

步骤 1　建立节点随机移动模型;

步骤 2　对于所有节点 j,$j \in [1, N]$,$r_j = 0$;

步骤 3　对于每个可与 j 进行协作的节点 $i \in [1, m]$;

步骤 4　初始化 $S_n = 1$;

步骤 5 根据门限值 Λ 及系数 a,得到本地决策 u_i;

步骤 6 由式(4)计算决策统计量 S_n;

步骤 7 如果 $\lambda_0 < S_n < \lambda_1$, $i \leftarrow (i+1) \bmod (m+1)$,转到步骤 5;

步骤 8 如果 $S_n \geqslant \lambda_1$,判决 $u=1$,转到步骤 10;

步骤 9 如果 $S_n \leqslant \lambda_0$,判决 $u=0$;

步骤 10 对每个节点 i,据表 1 求 du_i,由式(9)或式(10)计算 Δr_i;

步骤 11 $r_i \leftarrow r_i + \Delta r_i$。

5 性能分析与仿真

在一个2 400 m × 2 400 m的正方形 Ad Hoc CR 网络中,以试验节点作为原点,以发射端所在方向作为横轴,建立坐标系,如图 1 所示,网络中有 N 个次用户进行协作感知,其中 N_a 个被敌方控制而成为恶意用户,可随时发动 SSDF 攻击。每个节点都是随机移动的,移动的最大速度为 $V_{\max}$(m/s),节点信息的最大传输距离为 $d_{\max}$(m),发射端为无线电发射塔,塔高为 h_b(m),发射功率为 P_t(kW),发射频率为 f_c(MHz),空闲先验概率为 P_0,发射塔与试验节点的距离为 D_0,用户接收天线高度为 h_m(m)。假设接收机的检测灵敏度为 -94 dBm,噪声服从(-106, 11.8)的正态分布,各个用户与发射塔之间距离为 D_i(m),每次检测的时间间隔为 T(s)。

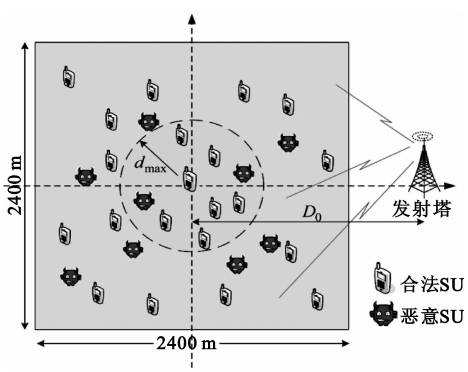

图 1 系统模型示意图

Fig.1 Illustration of the system model

根据 IEEE 802.22 协议给出的 HATA 模型,以农村环境为例,计算各节点路径损耗 L_{po_i}(dBm)[11]:

$$L_{po_i} = 69.55 + 26.16 \times \lg f_c - 13.82 \times \lg h_b - ((1.1 \times \lg f_c - 0.7) \times h_m - (1.56 \times \lg f_c - 0.8)) + (44.9 - 6.55 \times \lg h_b) \times \lg(D_i) - 4.78 \times (\lg f_c)^2 + 18.33 \times \lg f_c - 40.98 \quad (11)$$

则节点的接收功率 $P_{r_{i\_\mathrm{dBm}}} = P_{t\_\mathrm{dBm}} - L_{po_i}$,其中 P_{t_dBm}和 $P_{r_{i_\mathrm{dBm}}}$分别为 P_t 和 P_{r_i}的 dBm 表示形式。

以第一种 SSDF 攻击模式为例,对 EWSPRT 方案下的协作感知性能进行 Monte-Carlo 仿真,仿真次数为50 000。协作感知性能可由错误检测概率 $Q_e = Q_f + Q_m$ 表示,Q_e 越小,则表示检测性能越好。

图 2 比较了几种协作感知方案在 AWGN 信道下的感知性能。主要仿真参数设置为:$N=600$, N_a 取值从 0 到 200, $d_{\max}=300$, $D_0=10\,000$, $P_t=200$, $h_b=100$, $h_m=1$, $f_c=617$, $C_{00}=C_{11}=0$, $C_{10}=1$, $C_{01}=10$, $P_0=0.8$, $Q_m=10^{-5}$, $Q_f=10^{-6}$, $v=10$, $T=30$。从图中可以看出,OR - CSS 和 AND - CSS 的错误检测概率很高,而 MAJ - CSS、LRT 以及 WSPRT 3 种方案下的错误检测概率相对较低,但随着恶意节点数量 N_a 的增加,三者的感知性能均有一定的恶化趋势。调整参数,继续对这 3 种方案进行多次仿真比较发现,在信噪比较低的情况下,即使恶意用户较少,MAJ - CSS 的感知性能也不理想;LRT 虽然在低信噪比时仍有较好的性能,但随着恶意用户增多,其性能下降较 WSPRT 更明显,而且较大的控制带宽及较长的感知时间需求限制了该方案的实际应用[6]。相比之下,WSPRT 的最大优势在于:通过多次权重更新,能使恶意用户的影响趋近最小,因此,在恶意用户数量较多时仍具有较好的感知性能,且一旦超过门限即进行最终判决,其感知速度明显较 LRT 更快。

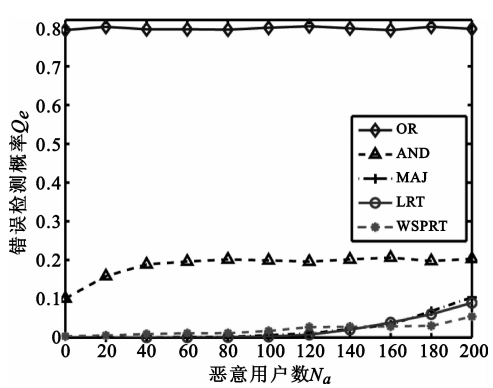

图 2 SSDF 攻击下几种协作感知方案的性能比较

Fig.2 Performance comparison of several CSS schemes under SSDF attacks

图 3 和图 4 分别给出了 LRT 和 WSPRT 两种方案在几种典型的衰落信道环境(AWGN、Rayleigh 和 Suzuki)中的协作感知性能随恶意用户数量的变化情况,其中 $\sigma_{dB}=6$。从图中不难发现,多径及阴影衰落效应对协作感知性能有明显的负面影响。

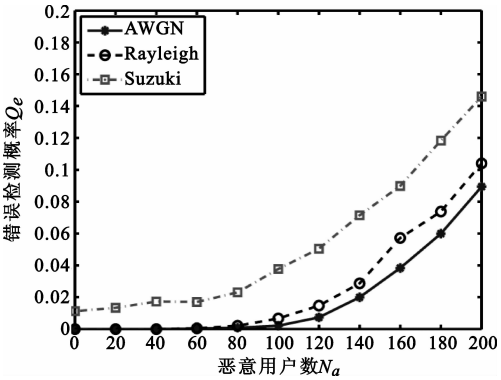

图 3　LRT 方案在不同衰落信道下的性能
Fig.3 Performance of the LRT scheme under different fading channels

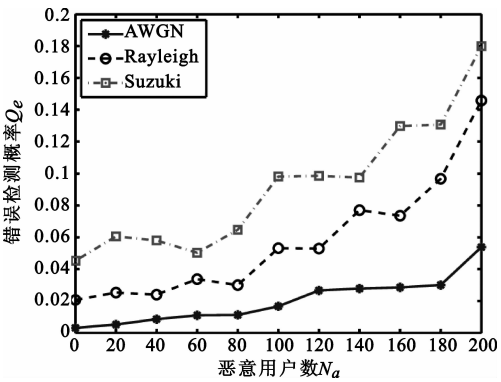

图 4　WSPRT 方案在不同衰落信道下的性能
Fig.4 Performance of the WSPRT scheme under different fading channels

图 5 比较了在 Suzuki 信道下传统 WSPRT 方案和本文给出的 EWSPRT 方案的协作感知性能,其中 EWSPRT－1 和 EWSPRT－2 分别对应信任度 r_i 的线性增量和非线性增量两种不同的规则,$\sigma_{dB}=6$, $a=10$。从该图的结果可以看出,两种规则下 EWSPRT 的错误检测概率均明显低于 WSPRT 方案,这说明 EWSPRT 可以更有效地抵抗 SSDF 攻击。此外,在 EWSPRT 方案中采用非线性规则更新节点信任度,比普通的线性规则所获得的性能更优,这是因为在非线性规则下,恶意节点的融合权重被及早地降低,则 SSDF 攻击对整体的感知性能影响自然就更小。

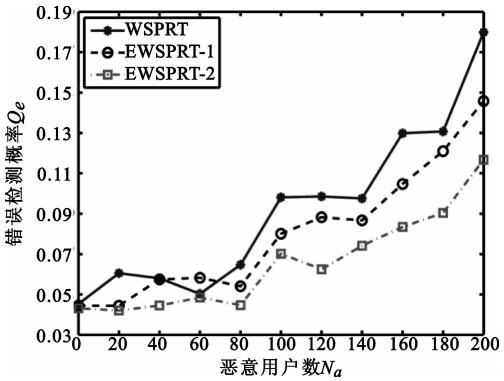

图 5　EWSPRT 与传统 WSPRT 的性能比较
Fig.5 Performance comparison between EWSPRT and WSPRT schemes

6　结　论

本文提出了一种基于 2 bit 决策融合的增强型加权序贯检测(EWSPRT)协作频谱感知方案,对次用户信任度的更新算法进行了改进,并在 SSDF 攻击条件下,比较了 K－N、LRT 以及 WSPRT 3 种常用方案在不同衰落信道环境中的感知性能,归纳了其各自的优缺点及适用范围。Monte－Carlo 仿真结果表明,EWSPRT 方案与传统的 WSPRT 方案相比,能够更有效地抵抗 SSDF 攻击,且采用非线性规则更新节点的信任度能进一步提升其感知性能。

参考文献:

[1] ZENG Y, LIANG Y, HOANG A T, et al. A review on spectrum sensing for cognitive radio: challenges and solutions[J/OL]. EURASIP Journal on Advances in Signal Processing, 2010, 2010: 1－15[2010－12－28]. http://www.hindawi.com/journals/asp/2010/381465/.

[2] YUCEK T, ARSLAN H. A survey of spectrum sensing algorithms for cognitive radio applications[J]. IEEE Communications Surveys & Tutorials, 2009, 11(1): 116－130.

[3] URKOWITZ H. Energy detection of unknown deterministic signals[J]. Proceedings of the IEEE, 1967, 55(4): 523－531.

[4] WANG W, LI H, SUN Y L, et al. Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks[J/OL]. EURASIP Journal on Advances in Signal Processing, 2010, 2010: 1－15[2010－12－28]. http://www.hindawi.com/journals/asp/2010/6957501/.

[5] CHEN R, PARK J, HOU Y T, et al. Toward secure distributed spectrum sensing in cognitive radio networks[J]. IEEE Communications Magazine, 2008, 46(4): 50－55.

[6] CHEN R, PARK J, BIAN K. Robust distributed spectrum sensing in cognitive radio networks[C]// Proceedings of

IEEE Communications Society Conference on Computer Communications. Phoenix, AZ, USA: IEEE, 2008: 31 – 35.

[7] HU F, WANG S, CHENG Z. Secure cooperative spectrum sensing for cognitive radio networks[C]// Proceedings of 2009 IEEE Military Communications Conference. Boston, MA, US: IEEE, 2009: 1 – 5.

[8] ZHU F, SEO S W. Enhanced robust cooperative spectrum sensing in cognitive radio[J]. Journal of Communications and Networks, 2009, 11(2): 122 – 133.

[9] LI H, HAN Z. Catching attacker(s): for collaborative spectrum sensing in cognitive radio systems: an abnormality detection approach[C]// Proceedings of 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum. Singapore: IEEE, 2010: 1 – 12.

[10] KYPEROUNTAS S, CORREAL N, SHI Q, et al. Performance analysis of cooperative spectrum sensing in suzuki fading channels[C]//Proceedings of the 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications. Orlando, USA: IEEE, 2007: 428 – 432.

[11] RAPPAPORT T S. Wireless communication: principles and practice[M]. New York: Prentice Hall, 1996.

[12] GHASEMI A, SOUSA E S. Opportunistic spectrum access in fading channels through collaborative sensing[J]. Journal of Communications, 2007, 2(2): 71 – 82.

[13] YU F R, TANG H, HUANG M, et al. Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios[C]//Proceedings of 2009 IEEE Military Communications Conference. Boston, MA, USA: IEEE, 2009: 1 – 7.

作者简介:

刘 全(1985 –),男,江西萍乡人,2006 年于海军工程大学获工学学士学位,现为博士研究生,主要研究方向为认知无线电网络链路层关键技术、多抽样率信号处理;

LIU Quan was born in Pingxiang, Jiangxi Province, in 1985. He received the B.S. degree in Naval University of Engineering in 2006. He is currently working towards the Ph.D. degree. His research interests include cognitive radio systems and multirate signal processing.

Email: liuquan.hjgc@gmail.com, alex – hjgc@163.com

郭云玮(1983 –),男,江西新余人,2004 年于海军工程大学获工学学士学位,现为硕士研究生,主要研究方向为认知无线电频谱感知技术;

GUO Yun – wei was born in Xinyu, Jiangxi Province, in 1983. He received the B.S. degree in Naval University of Engineering in 2004. He is now a graduate student. His research direction is spectrum sensing in cognitive radio.

高 俊(1957 –),男,江苏泰州人,1982 年于海军电子工程学院获工学学士学位,1989 年于北京理工大学获工学博士学位,现为教授、博士生导师,主要研究方向为软件无线电、数字通信理论与技术;

GAO Jun was born in Taizhou, Jiangsu Province, in 1957. He received the B.S. degree in Naval Electronic College of Engineering, the Ph.D. degree in Beijing Institute of Technology in 1982 and 1989, respectively. He is now a professor and also the Ph.D. supervisor. His research interests include digital communications and software radio systems.

刘思洋(1986 –),男,黑龙江哈尔滨人,2009 年于哈尔滨工程大学获工学学士学位,现为硕士研究生,主要研究方向为认知无线电网络。

LIU Si-yang was born in Harbin, Heilongjiang Province, in 1986. He received the B.S. degree in Harbin University of Engineering in 2009. He is now a graduate student. His research direction is cognitive radio networks.

本刊加入“万方数据 – 数字化期刊群”等数据库的声明

为了适应我国信息化建设的需要,扩大作者学术交流渠道,实现科技期刊编辑、出版发行工作的电子化,推进科技信息交流的网络化进程,本刊现已加入“万方数据 – 数字化期刊群”、“中国学术期刊(光盘版)”、“中国期刊全文数据库”、“中国学术期刊网”、“中文科技期刊数据库”、“中国期刊网”等本刊目次页上著录的数据库,本刊录用发表的论文,将由编辑部统一纳入上述数据库,进入因特网或光盘提供信息服务。本刊所付稿酬已包含著作权使用费和刊物内容上网服务报酬,不再另付。凡有不同意者,请事先声明,本刊将作适当处理。

《电讯技术》编辑部