



协作频谱感知中抗 SSDF 攻击的 认知用户不确定性行为评估

冯景瑜, 李金龙, 卢光跃

(西安邮电大学通信与信息工程学院 西安 710061)

摘要: 针对认知用户的协作感知行为不确定性, 提出一种基于 D-S 证据理论的信任评估机制——HardGuard, 为硬判决融合算法提供保护, 使其成为具有抑制频谱感知数据伪造 (SSDF) 攻击能力的可信协作频谱感知算法。HardGuard 采取感知数据预处理措施, 在融合之前有效过滤虚假感知数据, 规避了恶意用户的影响。仿真结果表明, HardGuard 能使硬判决融合算法面对 SSDF 攻击时保持较好的感知性能。

关键词: 协作频谱感知; 硬判决融合; SSDF 攻击; 信任

doi: 10.11959/j.issn.1000-0801.2015025

Evaluating Uncertainty Behaviors of Cognitive Users Against SSDF Attack for Cooperative Spectrum Sensing

Feng Jingyu, Li Jinlong, Lu Guangyue

(Institute of Communication Engineering, Xi'an University Posts & Telecommunications, Xi'an 710061, China)

Abstract: Aiming at the uncertainty behaviors of cognitive users, an evaluation mechanism based on D-S theory, called HardGuard, was proposed to guard the hard-decision fusion schemes. Before fusing data, HardGuard will filter out false sensing data to avoid the impact of malicious users. The simulation results show that HardGuard is effective in suppressing spectrum sensing data falsification attack, and it can ensure the better sensing performance for the hard-decision schemes.

Key words: cooperative spectrum sensing, hard decision fusion, SSDF attack, trust

1 引言

随着无线通信业务的迅速发展以及物联网、移动互联网的广泛应用, 频谱资源日益紧缺。认知无线电技术^[1]通过赋予未授权用户 (也称认知用户) 频谱感知功能来寻找可

用的频谱资源, 并在授权用户 (也称主用户 (primary user, PU)) 的可用频谱资源空闲时进行动态接入, 缓解了频谱资源稀缺与日益增长的无线接入需求之间的矛盾, 成为下一代无线通信发展的关键技术之一。

协作频谱感知是认知无线电技术的首要环节, 感知性

收稿日期: 2014-11-01; 修回日期: 2015-01-04

基金项目: 国家自然科学基金资助项目 (No.61301091), 中国博士后科学基金项目 (No.2013M541013), 陕西省自然科学基金基础研究计划项目 (No.2014JQ8321), 陕西省教育厅专项科研计划项目 (No.14JK1681)

Foundation Items: The National Science Foundation of China (No.61301091), The China Postdoctoral Science Foundation (No.2013M541013), The National Science Foundation of Shaanxi Province (No.2014JQ8321), The Science Foundation of Shaanxi Provincial Education Office (No.14JK1681)



能的好坏会影响到整个认知无线电系统的性能。所谓协作频谱感知,就是通过对多个认知用户感知信息的融合来消除单个用户感知的不确定性和“终端隐藏”问题,共同协商确定主用户频谱资源的使用情况,达到更好的感知性能^[2]。在众多的协作频谱感知策略中,由于硬判决融合算法具有较低的通信负载且易于实现,得到了研究者和业界的广泛关注^[3]。然而,已有的“OR”、“AND”、“Majority”3种硬判决融合算法^[4]默认所有的认知用户都是可信的,不加筛选地融合各个认知用户发送的感知数据,为恶意用户带来了可乘之机。恶意用户通过实施频谱感知数据伪造(spectrum sensing data falsification, SSDF)攻击,使得硬判决融合算法不能根据外界环境得出正确的频谱感知决策^[5]。

在 SSDF 攻击的抑制方法研究方面,目前倾向于信任评估机制。而信任评估机制适用于协作频谱感知的主要原因在于,凡是涉及分布式协作的行为活动都会存在信任问题,频谱协作感知正是一种典型的分布式协作活动^[6]。参考文献[7]使用 Beta 系统提出了一个协作频谱感知环境下的信任模型,解决恶意用户的策略性攻击问题。参考文献[8]利用认知循环建立信任模型来保障协作频谱感知的安全性。参考文献[9]分析了存在 SSDF 攻击时协作频谱感知硬判决融合算法的性能,提出了一种基于信任加权的协作频谱感知算法。这些方法的共同点是认为恶意用户的 SSDF 攻击行为是可预测的,因此可以依据各个认知用户的历史感知行为评估其可信情况,达到检测恶意用户的目的。但是,主用户的可用频谱资源出现情况是随机的,并且恶意用户为了规避检测也会偶尔发送正确的感知数据,因而恶意用户的 SSDF 攻击行为存在着不确定性,有时是不可预测的。

本文引入 D-S 证据理论研究协作频谱感知中的信任评估机制——HardGuard,为硬判决融合算法提供抑制 SSDF 攻击的保护。HardGuard 对认知用户从事协作频谱感知时的不确定性行为进行建模,利用证据信息设计基本信度分配函数计算多维度信任,并根据 D-S 证据合成规则融合多维信任,实现对认知用户可信性的综合评估。在此基础上,HardGuard 采取数据预处理措施,过滤恶意用户的虚假感知数据,只允许可信的认知用户参与硬判决融合,从而提高了硬判决融合算法的安全性能,有效规避了恶意用户的 SSDF 攻击。

2 协作频谱感知的系统模型

协作频谱感知中的认知用户通常分为两种类型:请求感知用户(request sensing user, RSU)和协作感知用户

(cooperative sensing user, CSU)。这两种类型的划分是相对的,不是绝对的。当某个认知用户由于阴影效应、多径衰落和“终端隐藏”等因素的存在,无法独自得出关于主用户频谱状态的感知决策时,就会请求协作频谱感知,此时该用户就是 RSU;当该用户参与别的认知用户发起的协作频谱感知时,就是 CSU。

多个 CSU 参与协作频谱感知时,每个 CSU 首先根据能量检测判断授权频段上 PU 信号的能量水平,得出局部感知数据。假设 $s(t)$ 表示 PU 信号, $n(t)$ 表示授权频段上的加性高斯白噪声, $h(t)$ 为授权频段上的信道增益, $y(t)$ 表示每个 CSU 的接收信号,能量检测可以描述为二元假设检验问题^[10],如式(1)所示:

$$y(t) = \begin{cases} n(t), & H_0 \\ h(t)s(t) + n(t), & H_1 \end{cases} \quad (1)$$

当 $y(t) > \lambda$ (λ 为能量检测的判决门限)时判决为 H_1 ,即 PU 信号存在;否则,判决为 H_0 ,即 PU 信号不存在。因此,在硬判决融合中,每个 CSU 的局部感知数据可以表示为只包含 1 bit 的判决信息,即:

$$d_i = \begin{cases} 0, & H_0 \\ 1, & H_1 \end{cases} \quad (2)$$

以第 i 个协作频谱感知用户 CSU_i 为例,“0”表示 CSU_i 认为 PU 的可用频谱状态为空闲,“1”表示 CSU_i 认为 PU 的可用频谱状态为繁忙。

之后,每个 CSU 将各自的局部感知数据发送给融合中心(fusion center, FC)进行硬判决融合,得出最终的感知决策。现有硬判决融合算法“OR”、“AND”和“Majority”的特点如下^[4]。

- “OR”: 一个以上的 CSU 认为 PU 的频谱状态为繁忙时,FC 判决 PU 的授权频段不可用。“OR”的优点在于能最大程度地避免对 PU 的干扰,这是因为只有所有的 CSU 都认为 PU 的频谱状态为空闲时,FC 才判决 PU 的授权频段可用。
- “AND”: 所有的 CSU 都认为 PU 的频谱状态为繁忙时,FC 判决 PU 的授权频段不可用。“AND”的优点在于能最大程度地利用 PU 频谱,这是因为只有一个以上的 CSU 认为 PU 的频谱状态为空闲时,FC 判决 PU 的授权频段可用。
- “Majority”: 与“OR”和“AND”相比,“Majority”的使用更为灵活。只需要超过多数的 CSU 认为 PU 的频谱状态为空闲或繁忙时,FC 就能判决出 PU 的授权频段可用或不可用。

通常,融合算法的性能主要体现为较高的检测概率(感知结果与 PU 实际频谱状态相符的概率)和较低的虚警概率(PU 频谱空闲存在却被误判为繁忙的概率)。假设共有 n 个 CSU 参与协作频谱感知,每个 CSU 的感知性能用检测概率 P_d 和虚警概率 P_f 衡量,则硬判决融合算法的检测概率 Q_d 和虚警概率 Q_f 分别为^[11]:

$$Q_d = \text{Prob}(H_1|H_1) = \sum_{l=k}^n \binom{n}{l} P_d^l (1-P_d)^{n-l} \quad (3)$$

$$Q_f = \text{Prob}(H_1|H_0) = \sum_{l=k}^n \binom{n}{l} P_f^l (1-P_f)^{n-l}$$

式(3)中,当 $k=1$ 时,表示“OR”的感知性能;当 $k=n$ 时,表示“AND”的感知性能;当 $k \geq n/2$ 时,表示“Majority”的感知性能。

3 HardGuard——保护硬判决融合算法

针对认知用户从事协作频谱感知时的行为不确定性,引入 D-S 证据理论研究协作频谱感知中的信任评估机制——HardGuard,帮助 FC 在硬判决融合时规避恶意用户的 SSDF 攻击。

3.1 基本结构

HardGuard 采取模块化设计思想。如图 1 所示,FC 收到 CSU 的局部感知数据后,触发 HardGuard。首先,运行数据预处理模块识别恶意用户并过滤其虚假的感知数据。接着,将过滤后的感知数据输入可信数据融合模块进行硬判决融合,得出最终的感知决策。RSU 确定 PU 的实际频谱状态后,发送反馈信息给信任数据库(trust database, TD),由其负责调用 D-S 证据理论信任评估引擎,实时更新每个 CSU 的信任值。同时,TD 数据库为数据预处理模块提供

CSU 信任值的实时查询,支撑该模块的恶意用户识别功能。HardGuard 的核心功能模块是基于 D-S 证据理论的信任评估引擎,从协作频谱感知的角度评估认知用户的不确定行为,也就是评估 CSU 的行为可信性。

3.2 基于 D-S 证据理论的信任评估

D-S 证据理论^[12]是建立在非空有限域 Θ 上的不确定性数学理论,以简单的推理形式,可对相互重叠、非互不相容的命题进行证据组合并得到较好的结果,比传统的概率能更好地把握问题的未知性与不确定性,是比概率论更弱的公理系统。 Θ 称为辨识框架,表示有限个状态 $\{\theta_1, \theta_2, \dots, \theta_n\}$,而系统状态为 Θ 的一个子集,即 Θ 的幂集 2^Θ 的一个元素。本文仅考虑 $\Theta = \{T, \neg T\}$,其中 T 表示信任, $\neg T$ 表示不信任。 $2^\Theta = \{\emptyset, \{T\}, \{\neg T\}, \{T, \neg T\}\}$,其中 $\{T\}$ 表示某个 CSU 处于可信状态, $\{\neg T\}$ 表示某个 CSU 处于不可信状态, $\{T, \neg T\}$ 表示某个 CSU 处于哪个状态具有不确定性。

运用 D-S 证据理论进行信任评估时,首先需要定义证据信息支持某个 CSU 可信性状态的概率,称为基本信度分配函数。

定义 1 基本信度分配函数:从 Θ 的幂集到 $[0, 1]$ 的映射,定义为:

$$m: 2^\Theta \rightarrow [0, 1], m(\emptyset) = 0, \sum_{X \in 2^\Theta} m(X) = 1 \quad (4)$$

支持一个 CSU 可信性状态的证据信息来源于 RSU 判断出主用户的实际频谱状态后,发送给 FC 的反馈信息。由于一个 CSU 通常会在不同时段参与多个 RSU 发起的协作频谱感知,因而证据信息是多维的,也就存在多个基本信度分配函数进行某个 CSU 的多维信任评估。

对于 CSU_i ,其在协作频谱感知活动中产生的多维证据

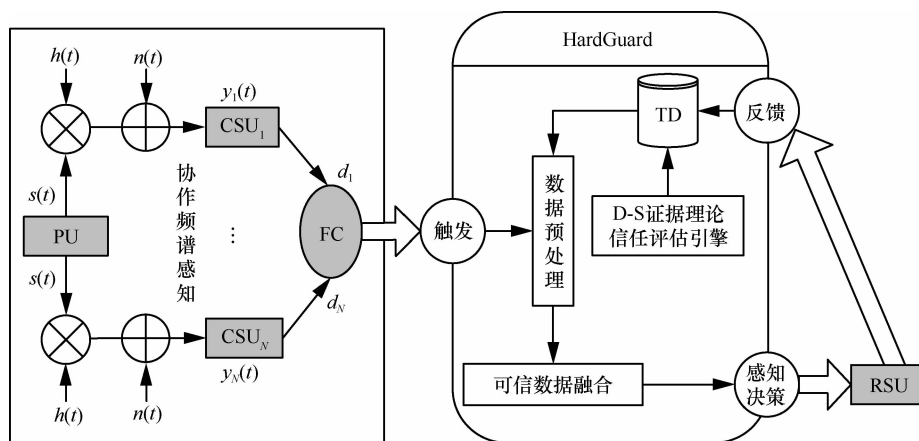


图 1 协作频谱感知中的 HardGuard 结构



信息可以描述为 $\{E_{i1}, \dots, E_{ki}, \dots, E_{im}\}$ 。其中, N 为证据维数, $E_{ki}=(s_{ki}, c_{ki}, u_{ki})$,分别代表来自于RSU k 的3种证据信息:“肯定”次数、“抱怨”次数和“不确定”次数。这3种证据信息是对RSU确定PU实际频谱状态后的历史经验反馈,“肯定”表示RSU使用PU的频谱后发现与FC提供的最终感知决策一致,“抱怨”则表示不一致。“不确定”表示RSU不能根据FC提供的最终感知决策做出是否使用PU频谱的决定。

根据证据信息,RSU k 关于CSU i 的基本信度分配函数可设计为:

$$m_{ki}(X) = \frac{e_{ki}}{s_{ki} + c_{ki} + u_{ki}} \quad (5)$$

显然, $0 \leq m_{ki} \leq 1$ 。当 $X=\{T\}$ 时, $e_{ki}=s_{ki}$;当 $X=\{\neg T\}$ 时, $e_{ki}=c_{ki}$;当 $X=\{T, \neg T\}$ 时, $e_{ki}=u_{ki}$ 。

以此类推,可得到关于CSU i 的 N 个基本信度分配函数。这些基本信度分配函数只是刻画出CSU i 的 N 维度信任,需要一个数值综合反映CSU i 的可信性。D-S证据理论提供了Dempster合并规则^[2]以合并多维信任。应用此合并规则的前提是被合并的证据必须是独立的。本文通过提取不同RSU的反馈信息来计算基本信度分配函数,因此它们之间满足彼此独立。

定义2 综合信任值:对某个CSU可信性的综合反映。对于CSU i ,通过 N 维度信任的融合得出综合信任值为:

$$TV_i = m_{i1}(T) \oplus m_{i2}(T) \oplus \dots \oplus m_{iN}(T) \\ = K^{-1} \sum_{\cap X_k = T} m_{i1}(X_1) m_{i2}(X_2) \dots m_{iN}(X_N) \quad (6)$$

其中, K 为归一化因子, $K = \sum_{\cap X_k = T} m_{i1}(X_1) m_{i2}(X_2) \dots m_{iN}(X_N)$ 。

3.3 HardGuard的算法实现

在HardGuard的模块化实现过程中,实施其对硬判决融合算法的保护主要有3个方面的工作:数据预处理、可信数据融合和RSU反馈信息。

3.3.1 数据预处理

防御SSDF攻击的关键在于剥夺恶意用户参与感知数据融合的机会,减少其对硬判决融合的影响。根据信任阈值 δ ,可由下面的数据预处理算法将感知数据集 Ψ 分解为 Ψ_r 和 Ψ_f ,其中 Ψ_r 为真实感知数据集, Ψ_f 为伪造感知数据集。

算法1 数据预处理算法

输入: Ψ
输出: Ψ_r
初始化 $\Psi_r = \Psi_f = \emptyset$;
for $i \in \Psi$ do
 计算 TV_i ;
 if $(TV_i < \delta)$ then
 i 是恶意用户;
 $\Psi_f \leftarrow i$;
 else
 $\Psi_r \leftarrow i$;
 end if
end for

3.3.2 可信数据融合

过滤掉恶意用户的虚假感知数据后,根据 Ψ_r 数据集集中全1的数据个数 L ,在 Ψ_r 数据集上执行硬判决融合算法(见算法2),得出最终感知决策 d 。

算法2 硬判决融合算法

输入: $|\Psi_r|, L$
输出: d
(1)“OR”
 if $(L \geq 1)$ then
 $d=1$;
 else
 $d=0$;
 end if
(2)“AND”
 if $(L=|\Psi_r|)$ then
 $d=1$;
 else
 $d=0$;
 end if
(3)“Majority”
 if $(L \geq |\Psi_r|/2)$ then
 $d=1$;
 else
 $d=0$;
 end if

3.3.3 RSU反馈信息

每次协作频谱感知结束后,RSU k 需要向FC发送关于

PU 实际频谱状态的反馈信息 f_k , 以完成对本次协作频谱感知所有参与成员 Φ 的证据信息 E 的更新, 见算法 3。反馈信息存在 3 种状态: $f_k=1$, 表示对本次协作频谱感知的“肯定”; $f_k=0$, 表示“抱怨”; $f_k=-1$, 表示“不确定”。

算法 3 RSU 反馈算法

```
输入:  $f_k$ 
输出:  $E$ 
(1)  $f_k = 1$ 
for  $i \in \Phi$  do
    if ( $d_i=d$ ) then
         $s_{ki}++$ ;
    else
         $c_{ki}++$ ;
    end if
end for
(2)  $f_k = 0$ 
for  $i \in \Phi$  do
    if ( $d_i=d$ ) then
         $c_{ki}++$ ;
    else
         $s_{ki}++$ ;
    end if
end for
(3)  $f_k = -1$ 
for  $i \in \Phi$  do
     $u_{ki}++$ ;
end for
```

4 仿真结果及分析

采用蒙特卡洛仿真法, 在 MATLAB 平台上验证 HardGuard 的性能。设置认知用户数量为 30 个, 主用户数量为 3 个。其中, 认知用户中恶意用户比例为 50%, 每个恶意用户以 80% 的概率提交伪造的感知数据。仿真参数设置见表 1。

表 1 仿真环境参数设置

参数	描述	缺省值
count	蒙特卡洛次数	5 000
f_s	采样频率	1 kHz
τ	时间带宽积	50
SNR	信噪比	-8 dB
δ	信任阈值	0.6

协作频谱感知算法的性能主要体现为较高的检测率和较低的虚警率^[13]。图 2 和图 3 分别为能量检测判决门限值在 [4, 9] 内波动时的检测率和虚警率仿真情况, 并与 SensingGuard^[7]和无信任评估机制保护情况下的“OR”、“AND”和“Majority”进行对比。

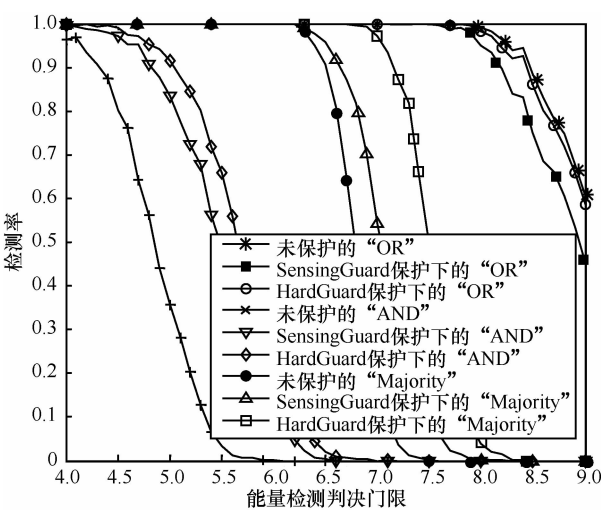


图 2 不同能量检测判决门限值下的检测率

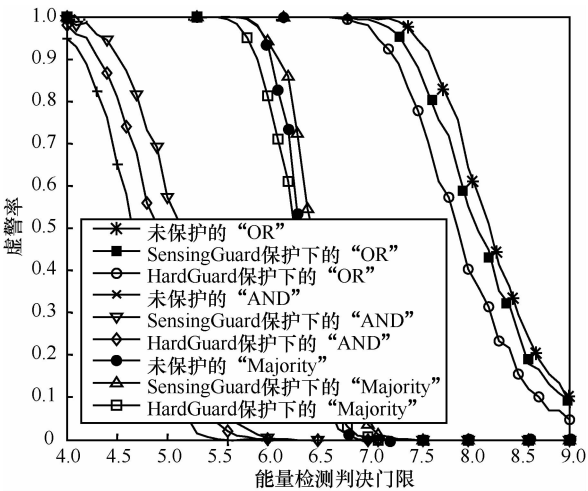


图 3 不同能量检测判决门限值下的虚警率

由图 2 可知, SSDF 攻击对“AND”的威胁主要在于降低检测率上。这是因为若有一个恶意用户伪造局部感知数据“0”, “AND”就会误判 PU 信号不存在。从仿真对比结果可以看出, 受 HardGuard 保护的“AND”和“Majority”的检测率高于未保护的“AND”和“Majority”的检测率, 而 SensingGuard 忽略了认知用户的不确定行为存在, 因而其保护的“AND”和“Majority”的检测率略低于 HardGuard 的检测率。但是 HardGuard 和 SensingGuard 对“OR”的作用不明显, 这是因为只需要一个以上的 CSU 发送局部感



知数据“1”,“OR”就判决 PU 频谱繁忙,从而能保障较高的检测率。

由图 3 可知,受 HardGuard 保护的“OR”和“Majority”的虚警率低于未保护的“OR”和“Majority”的虚警率,并略低于 SensingGuard 保护下的“OR”和“Majority”的虚警率。从图 3 也可以看出,HardGuard 和 SensingGuard 对“AND”的保护作用不大。这是因为在抬高虚警率方面,SSDF 攻击对“AND”的威胁有限,只有当所有的 CSU 发送局部感知数据“1”时,“AND”才会判决 PU 频谱繁忙,从而能避免虚警率的抬高。

5 结束语

本文针对 3 种常用的“OR”、“AND”、“Majority”硬判决融合算法在抑制 SSDF 攻击时的脆弱性,提出了一种基于 D-S 证据理论的信任评估机制——HardGuard,帮助 FC 在硬判决融合时规避恶意用户的虚假感知数据影响,并给出了 HardGuard 的实现算法。仿真结果表明,HardGuard 能使硬判决融合算法在面对 SSDF 攻击时保持较好的感知性能,提高了协作频谱感知的安全性。

参考文献

- Mitola J, Maguire G. Cognitive radio: making software radios more personal. *IEEE Personal Communications*, 1999, 6(4)
- Akyildiz I F, Lo B F, Balakrishnan R. Cooperative spectrum sensing in cognitive radio networks: a survey. *Physical Communication*, 2011, 4(1)
- Blasco M J, Rifù-Pous H, Garrigues C. Review of robust cooperative spectrum sensing techniques for cognitive radio networks. *Wireless Personal Communications*, 2012, 67(2)
- Shen J, Liu S, Zeng L, Xie G, *et al.* Optimisation of cooperative spectrum sensing in cognitive radio network. *IET Communications*, 2009, 3(7)
- Chen R L, Park J M, Hou Y T. Toward secure distributed spectrum sensing in cognitive radio networks. *IEEE Communications Magazine*, 2008, 46(4)
- 冯景瑜. 协作频谱感知中的 SSDF 攻击及其对策研究. *电信科学*, 2014, 30(1)
Feng J Y. Research on SSDF attack and defense for cooperative spectrum sensing. *Telecommunications Science*, 2014, 30(1)
- Feng J Y, Zhang Y Q, Lu G Y, *et al.* Securing cooperative spectrum sensing against rational SSDF attack in cognitive radio networks. *KSH Transactions on Internet and Information Systems*, 2014, 8(1)
- Pei Q Q, Yuan B B, Li L, *et al.* A sensing and etiquette reputation-based trust management for centralized cognitive radio networks. *Neurocomputing*, 2013, 101(4)
- 闫琦, 杨家玮, 张雯. 认知无线网络中安全的合作频谱感知. *北京邮电大学学报*, 2011, 34(2)
Yan Q, Yang J W, Zhang W. The sensing of the secure cooperative spectrum in cognitive radio networks. *Journal of Beijing University of Posts and Telecommunications*, 2011, 34(2)
- Akyildiz I F, Lee W Y, Chowdhury K R. CRAHNS: cognitive radio ad hoc networks. *Ad Hoc Networks*, 2009, 7(5)
- Zhang W, Ranjan K, Mallik. Cooperative spectrum sensing optimization in cognitive radio networks. *Proceedings of the IEEE International Conference on Communications*, Beijing, China, 2008
- Sentz K, Ferson S. Combination of Evidence in Dempster-Shafer Theory. Sandia National Labs: Technical Report SAND2002-0835, 2002
- Ahsant B, Viswanathan Odoni R. *Advancement in Sensing Technology*. Berlin: Springer-Verlag, 2013

[作者简介]



冯景瑜,男,博士,西安邮电大学通信与信息工程学院讲师,中国科学院大学在站博士后,主要研究方向为无线通信安全、认知无线电、协作频谱感知等。



李金龙,男,西安邮电大学通信与信息工程学院硕士生,主要研究方向为无线通信网络、协作频谱感知等。



卢光跃,男,博士,西安邮电大学通信与信息工程学院教授、博士生导师,主要研究方向为通信信号处理、认知无线电、协作频谱感知等。