抗 SSDF 攻击的一致性协作频谱感知方案

刘 全,高 俊,郭云玮,刘思洋
(海军工程大学通信工程系,湖北武汉 430033)

摘 要: 在分布式认知无线电网络中,一般很难找到合适的融合中心能够收集所有协作用户的感知信息,而且协作过程极可能遭到篡改感知数据(Spectrum Sensing Data Falsification,SSDF)攻击.鉴于此,该文提出了一种改进的一致性协作频谱感知方案.利用 Metropolis 迭代规则,各次用户仅依靠邻接点之间的局部信息交互即可实现感知协作,且无需网络的任何先验知识.为了抵抗潜在的三种 SSDF 攻击,该方案中引入了相应的抗攻击策略,使合法次用户能及时检测并拒绝恶意用户接入网络.仿真结果表明,改进方案能保证绝大多数合法次用户最终趋于状态一致,并分别做出正确决策;与现有的一致性方案相比,该方案能使协作感知在各种攻击场景中的稳健性明显增强.

关键词: 认知无线电网络;协作频谱感知;感知安全;一致性;篡改感知数据攻击
中图分类号: TN92 **文献标识码:** A **文章编号:** 0372-2112 (2011) 11-2643-05

Securing Consensus-Based Cooperative Spectrum Sensing Against Spectrum Sensing Data Falsification Attacks

LIU Quan, GAO Jun, GUO Yun-wei, LIU Si-yang
(*Department of Communication Engineering, Naval University of Engineering, Wuhan, Hubei* 430033, *China*)

Abstract: In distributed cognitive radio networks (CRNs), a common fusion centre is always not available to collect the sensing results from all cooperative users, and the sensing cooperation is likely to be disrupted by spectrum sensing data falsification (SSDF) attacks. Allowing for these factors, this paper proposes a modified consensus-based scheme for decentralized cooperative spectrum sensing(CSS). Utilizing the iteration rule based on Metropolis weight matrix, each secondary user (SU) can maintain cooperation with others only through the local information exchange in the neighborhood, without requiring any a priori knowledge of the whole network. To counter three potential attack models of SSDF, some anti-attack strategies are also introduced, by which the authentic SUs can identify and reject the malicious users quickly. As represented by the extensive simulation results, the proposed scheme can generally guarantee most authentic SUs to reach a consensus and make right decisions individually; also, it is proved to be much more robust against all potential SSDF attacks, compared with the existing consensus-based scheme.

Key words: cognitive radio networks; cooperative spectrum sensing; sensing security; consensus; spectrum sensing data falsification attack

1 引言

在现有授权网络的基础上,构建基于主-次分层接入共享模型的认知无线电网络(CRN),不仅能够完美地与现有静态频谱分配体制兼容,又能以低成本的代价获得频谱效率的大幅度提高[1].频谱感知是 CRN 中需要解决的首要问题,其主要目的是快速可靠地获取周围环境中的动态频谱信息,使各次用户(SU)在不干扰现有主用户的前提下,实现基于“伺机接入”方式的频谱共享[1].为了减少多径及阴影衰落等因素带来的不利影响,通常都需要多个次用户进行协作[2].现有的协作频谱感知(CSS)方案大部分都需要特定的基站或者融合中心收集所有协作用户的本地感知数据或决策,然后以某种规则进行融合并做出统一判决[3].但是在许多分布式网络中,这些基于信息融合的 CSS 方案并不实用,因为很难找到一个与所有协作用户都能进行信息交互的节点充当融合中心.针对此问题,文献[4]首次将一致性算法引入到 CSS 中,仅通过邻接点之间进行多次局部信息交互后就能使所有次用户状态趋于一致.

然而,和大多数信息融合式 CSS 方案一样,分布式 CSS 也面临着多种潜在的安全隐患.在物理层,伪装主用户攻击[5]是其将要面临的主要干扰形式.而在链路

收稿日期:2010-07-31;修回日期:2011-03-17
基金项目:国家 863 高技术研究发展计划(No.2009AAJ208,2009AAJ116)

层,CSS 的局部信息交互过程更容易受到敌方的攻击,而且这些攻击通常都是通过恶意篡改本地感知结果来实现的,故被统称为篡改感知数据 (SSDF)攻击[5].现有的 CSS 相关文献中很少涉及感知安全问题,仅有少数对信息融合式 CSS 方案的安全策略进行了讨论,典型的如文献[5,6];而专门针对分布式 CSS 感知安全问题的研究则更为少见,虽然文献[7]对此进行了一些初步探讨,但是其给出的抵抗策略难以抵抗多种 SSDF 攻击.

本文旨在对一致性 CSS 方案进行改进,重点讨论如何抵抗三种潜在的 SSDF 攻击,并给出相应的抗攻击策略和具体的信息交互流程,最后通过仿真实验,与现有方案进行比较,证明所给改进方案的有效性.

2 系统模型

考虑一个分布式 CRN,N 个次用户按照上层协议分布在特定范围内,其中的某些节点可能被敌方控制而成为恶意用户,能够随时发动 SSDF 攻击.

2.1 一致性 CSS 方案

分布式 CSS 可看作是一个典型的多主体协作问题[8].为便于说明,本小节对文献[4]提出的一致性 CSS 方案进行简要介绍.首先将网络等效为一个连通图 $G=(V,E)$,其中 $V=\{1,2,\cdots,N\}$ 表示顶点(即所有次用户)集合;E 表示所有边(即次用户间的链路)集合[8].若以 $\boldsymbol{A}=\{a_{ij}\}$ 表示图的邻接矩阵,且 $a_{ij}\in\{0,1\}$,那么 $E=\{(i,j)\in V\times V, a_{ij}=1\}$,且次用户 $i(i\in[1,N])$的邻接点集合为 $Ne_i=\{j\in V\mid a_{ij}=1\}$,其度数是 $d_i=|Ne_i|$.图 1 给出了一致性的 CSS 方案的流程框图.整个 CSS 过程分为三步,各次用户首先分别以能量检测算法[9]进行本地感知,然后将检测结果作为初始状态 $x_i(0)$,与各自的邻接用户按照以下规则进行信息交互[4]:

$$x_i(k+1)=x_i(k)+\varepsilon\sum_{j\in Ne_i(k)}(x_j(k)-x_i(k)) \quad (1)$$

其中,k 表示迭代计数;$x_i(k)$和 $x_i(k+1)$分别表示第 i 个次用户在当前时刻和下一时刻的感知状态;ε 表示迭代的步进值,且必须满足

$$0<\varepsilon<1/\Delta,\Delta=\underset{l\in V}{\mathrm{Max}}\{d_l\}$$

受感知时间的限制,迭代次数必存在一定的上限,即 $k<T_c$.当 $k\geqslant T_c$ 时,各次用户终止信息交互,并分别根据各自的最终迭代状态做出最终决策 D_i,即

$$D_i=\begin{cases}1, & x_i(T_c)>\lambda_c\\ 0, & \text{otherwise}\end{cases} \quad (2)$$

其中,λ_c 表示统一设置的判决门限.

若不考虑任何潜在的 SSDF 攻击,而且给定的 T_c 足够宽裕,则所有次用户的最终状态都将趋于一致,并渐近收敛于初始平均值[8]:

$$x_i(T_c)\to x^*=\frac{1}{N}\sum_{i=1}^{N}x_i(0),\text{as } T_c\to\infty \quad (3)$$

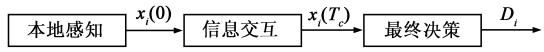

图1 基于一致性的协作感知方案

2.2 SSDF 攻击形式

在上述分布式 CSS 过程中,某些合法的协作次用户可能遭到敌方入侵或控制而成为恶意用户,继而通过篡改迭代状态而发动 SSDF 攻击,其攻击形式主要有以下三种[7]:(1)自私型攻击(Selfish Attack,SFA),主要是指恶意用户在信息交互过程中始终向邻接用户发送较高的感知状态(相对于邻接用户的检测门限),使邻接用户误以为当前信道被占用,从而使大量空闲频谱被浪费或被敌方侵占;(2)干扰型攻击(Interference Attack,IFA),即恶意用户始终发送相对较低的状态值,使其它用户盲目发射,造成对主用户的干扰;(3)混乱型攻击(Confusing Attack,CFA),是指恶意用户向外随机发送正常和恶意状态,使相邻用户的迭代过程发生紊乱,从而导致网络的状态始终无法趋于一致.

3 改进的一致性 CSS 方案

显然,当网络中存在 SSDF 攻击时,一致性 CSS 方案的平均收敛性将被破坏,所有次用户的状态都将一致趋于错误或根本无法收敛,究其根本原因在于该方案中没有引入任何抗攻击策略.此外各次用户需预知网络的最大度数等先验知识,而这在实际中非常困难.针对这两个问题,本节对一致性 CSS 方案进行了改进.

3.1 本地能量检测

根据 Urkowitz 能量检测理论[9],接收信号经过 A/D 采样和带通滤波后,在观察时间段 T,检测带宽 W 内的能量检测过程可建模为:

$$Y_i=\begin{cases}\dfrac{1}{\delta_i^2}\displaystyle\sum_{n=1}^{2m}w_i^2(n), & H_0\\ \dfrac{1}{\delta_i^2}\displaystyle\sum_{n=1}^{2m}(h_i(n)s(n)+w_i(n))^2, & H_1\end{cases} \quad (4)$$

其中,Y_i 是归一化的累计能量值;δ_i^2 表示噪声平均功率;$m=TW$ 称为时间带宽积;$s(n)$,$w_i(n)$,$h_i(n)$分别表示采样后的主用户信号,加性高斯白噪声,感知信道增益.由式(4)可推导出 Y_i 服从卡方分布[9]:

$$Y_i\sim\begin{cases}\chi_{2m}^2, & H_0\\ \chi_{2m}^2(2m\gamma_i), & H_1\end{cases} \quad (5)$$

其中,$\gamma_i=P/\delta_i^2$ 表示检测端的信噪比;而 P 表示接收到的主信号功率.

3.2 信息交互

一旦各次用户之间的链路建立,则按照以下流程

进行感知信息交互迭代:

①对 $\forall i\in[1,N]$,初始化 $x_i(0)=Y_i$, $k=0$.

②更新 $Ne_i(k)$ 和 $d_i(k)$. 记录各邻接点报告状态:$R_{ij}(k)=x_j(k)$, $j\in Ne_i(k)$,并缓存 $2L$ 级.

③求出次用户 i 邻接区域内的平均值:

$$u_i(k)=\frac{x_i(k)+\sum_{j\in Ne_i(k)}x_j(k)}{1+d_i(k)} \tag{6}$$

④找出偏离 $u_i(k)$最远的邻接点,并将其记录作为发动 SFA 或 IFA 攻击的可疑用户:

$$j_0=\arg\max_{j\in Ne_i(k)}\{x_j(k)-u_i(k)\} \tag{7}$$

⑤计算 i 及所有非可疑邻接点的平均值:

$$u_i'(k)=\frac{x_i(k)+\sum_{j\in Ne_i(k)}x_j(k)-x_{j_0}(k)}{d_i(k)} \tag{8}$$

⑥如果 $(u_i(k)-\lambda_c)(u_i'(k)-\lambda_c)<0$,则将 j_0 从用户 i 的邻接点集合中彻底剔除,即:

$$Ne_i(k)=Ne_i(k)/j_0 \tag{9}$$

⑦如果 $k\geqslant 2L$ 且 $\mathrm{mod}(k,L)=0$,则对于 $\forall j\in Ne_i(k)$,计算其报给 i 的最近 L 次以及过去 L 次状态的标准差:

$$a=\sqrt{\frac{1}{L}\sum_{l=0}^{L-1}\left(R_{ij}(k-l)-\frac{1}{L}\sum_{n=0}^{L}R_{ij}(k-n)\right)^2} \tag{10}$$

$$b=\sqrt{\frac{1}{L}\sum_{l=L}^{2L-1}\left(R_{ij}(k-l)-\frac{1}{L}\sum_{n=L}^{2L-1}R_{ij}(k-n)\right)^2} \tag{11}$$

⑧遍历用户 i 所有的邻接点,如果对于 $j_1\in Ne_i(k)$,存在 $a\geqslant b$,那么,j_1将被当成 CFA 攻击节点从 i 的邻接点集合中剔除,即

$$Ne_i(k)=Ne_i(k)/j_1 \tag{12}$$

这是因为,合法次用户的感知状态将随着迭代次数的增多而逐渐趋向初始平均值,故对 i 来说,合法邻接用户上报的状态值的波动性将越来越小. 而那些发动 CFA 攻击的邻接用户,由于其上报给 i 的感知状态是随机变化的,所以其状态波动性肯定不是逐渐减小的. 利用这一明显的区别,可以将 CFA 攻击用户剔除.

⑨采用 Metropolis 迭代规则更新状态值[8]:

$$\boldsymbol{X}(k+1)=\boldsymbol{W}(k)\boldsymbol{X}(k) \tag{13}$$

其中 $\boldsymbol{X}(k)=\{x_1(k),x_2(k),\cdots,x_N(k)\}$; $\boldsymbol{W}(k)$被称为 Metropolis 权重矩阵[8],其元素定义如下:

$$W_{ij}(k)=\begin{cases}\dfrac{1}{1+\max\{d_i(k),d_j(k)\}}, & \text{if } j\in Ne_i(k)\\ 1-\sum_{n\in Ne_i(k)}W_{in}(k), & \text{if } i=j\\ 0, & \text{otherwise}\end{cases} \tag{14}$$

⑩更新迭代次数:$k=k+1$;如果 $k\geqslant T_c$,则停止迭代并进入最终判决;否则从②继续迭代.

显然,按照 Metropolis 迭代规则,各次用户无需网络的任何先验知识,只需根据其自身和邻接点的状态进行更新,因此该规则比式(1)的规则更适用于大型的分布式网络中. 在不考虑攻击的条件下,整个网络可等效为非时变图,根据文献[8]的推导可知,该规则同样能保证所有次用户的状态最终趋于平均一致[8]:

$$x_i(k)\to x^*=\sum_{i=1}^{N}Y_i,\quad \text{as}\quad k\to\infty \tag{15}$$

然而,在攻击条件下,为了抵御 SSDF 攻击而引入安全策略后,各次用户的邻接点集合在信息交互过程中将不断变化,网络应等效为一个动态的有向图. 将所有合法次用户构成的动态子图记为 $G_a(k)=(V_a,E_a(k)$,其中 V_a 和 $E_a(k)$分别表示合法次用户顶点集合以及边集合,则根据文献[10]的结论,只要在足够多次迭代过程中所形成的一系列子图的集合:

$$U_{k=n}^{n+T-1}G_a(k)=\{G_a(n),G_a(n+1),\cdots,G_a(n+T-1)\}$$

能够保证强连通(即具有生成树),则所有合法次用户的一致收敛特性仍可以得到保证. 但是,在恶意用户被剔除之前,部分合法次用户不可避免地已受到一些影响,而且由于受到迭代次数的限制,在少数情况下,个别合法次用户的状态将偏离其它大部分用户,甚至有可能也被错当成攻击用户而逐出网络. 因此,网络的最终收敛状态与平均一致性存在一定的偏差,即:

$$x_a^*=\frac{1}{N_a}\sum_{h\in V_a}x_h(0)+\theta=\frac{1}{N_a}\sum_{h\in V_a}Y_h+\theta \tag{16}$$

其中,h 是合法次用户编号; x_a^* 为网络的最终收敛状态; N_a 为合法次用户个数; θ 是由迭代次数限制和攻击的部分影响而引入的随机偏差量.

3.3　最终判决

当各合法次用户的信息交互终止后,分别与检测门限比较做出最终判决,即

$$D_h=\begin{cases}1, & x_h(T_c)>\lambda_c\\ 0, & \text{其它}\end{cases},\quad \text{for}\quad \forall h\in V_a \tag{17}$$

理论上,若迭代次数足够多,抗攻击策略足够稳健,则最终的随机偏差量 θ 非常小,故

$$x_a^*\approx\frac{1}{N_a}\sum_{h\in V_a}x_h(0)=\frac{1}{N_a}\sum_{h\in V_a}Y_h=\frac{1}{N_a}Y_0 \tag{18}$$

其中,Y_0 表示所有合法次用户的初始感知状态之和,这与常用的等增益合并 CSS 方案[11]是等效的. 由式(5)推导得到 Y_0 服从以下分布[12]

$$Y_0=\sum_{h\in V_a}Y_h\sim\begin{cases}\chi^2_{2mN_a}, & H_0\\ \chi^2_{2mN_a}\left(2m\sum_{h\in V_a}\gamma_h\right), & H_1\end{cases} \tag{19}$$

故,联合虚警概率 Q_f 和漏检概率 Q_m 分别为[12]:

$$Q_f=P\{x_a^*>\lambda_c\mid H_0\}=P\Big\{\sum_{j\in V_a}Y_j>N_a\lambda_c\mid H_0\Big\}$$

$$= 1 - \Gamma\left(\frac{N_a\lambda_c}{2}, mN_a\right) \tag{20}$$

$$Q_m = P\{x_a^* \leqslant \lambda_c \mid H_1\} = P\left\{\sum_{j\in V_a} Y_j \leqslant N_a\lambda_c \mid H_1\right\}$$

$$= 1 - \int_{\gamma_0} Q\left(\sqrt{2m\gamma_0}, \sqrt{N_a\lambda_c}, mN_a\right) f_{\gamma_0}(x) \tag{21}$$

其中，γ_0 是所有合法次用户的平均信噪比之和；$f_{\gamma_0}(\cdot)$ 是 γ_0 的概率密度函数；$Q(\cdot,\cdot,\cdot)$ 和 $\Gamma(\cdot,\cdot)$ 分别是 Marcum Q 函数和非完全 gamma 函数[13].

考虑到迭代次数的限制，以及攻击的部分影响，改进方案不可能始终保证平均收敛，故其实际性能与上述理想性能之间存在一定的差距，式(20)和式(21)可作为此类基于一致性算法 CSS 方案的 CROC 特性[12]的理论下限.

4 仿真及讨论

本节通过仿真实验对改进方案的有效性进行验证，并与文献[4]给出的基本方案(见 2.1 节)进行对比. 以图 2 所示的拓扑结构为例，该分布式 CRN 由 16 个次用户 5u、42 条链路组成，其中第 7 个和第 12 个次用户是潜在的恶意用户，二者可随时发动任意形式的 SSDF 攻击. 假设各次用户的感知信道为独立同分布的 Suzuki 衰落信道[14]，功率发散因子为 $\sigma_{\mathrm{dB}} = 8\mathrm{dB}$. 各用户处本地能量检测的时间带宽积都设置为 $m = 20$，平均 SNR 分别在 0 ~ 5dB 范围内均匀分布，信息交互的最大迭代次数为 100，本地感知的初始结果直接按式(5)产生.

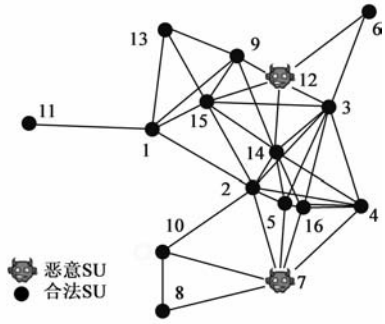

图2 分布式CRN的拓扑结构

以下针对次用户 12 的 4 种不同攻击场景，对改进的 CSS 方案分别进行了 100000 次仿真. 考虑到迭代次数有限，且个别次用户不可避免地会受到攻击的一些影响，此处将网络收敛定义适当放宽，规定 90%(含)以上合法次用户最终趋于一致(容差范围 $\leqslant$0.1dB)的情况即为收敛. 表 1 列出了基本方案和改进方案分别在不同场景中进行多次实验后统计的收敛比例，其中，$L = 10$，$\lambda_c = 48$(由式(20)计算得到).

在无攻击场景中，恶意用户与合法次用户没有区别. 图 3(a)给出了该场景中两种方案进行某次仿真时的信息交互过程，从图中可看出，两种方案都能使次用户的感知状态逐渐趋于一致. 由表 1 的统计数据可知，当网络中无攻击时，两种方案基本都能保证绝大多数的次用户收敛；由于改进方案中加入了一些抵抗攻击策略，少数实验中可能会将 2 个以上的合法次用户误当成恶意节点逐出网络，所以收敛率稍低一些.

表 1 不同攻击场景下的网络状态收敛率

攻击场景	无攻击	SFA	IFA	CFA
基本方案	100%	0%	0%	0%
改进方案	97.2%	90.1%	87.7%	90.4%

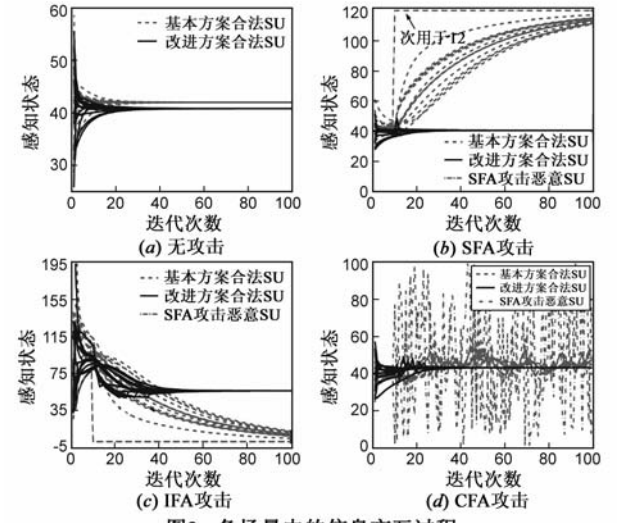

图3 各场景中的信息交互过程

在 SFA 攻击场景中，假设用户 12 在 H_0 条件下于第 10 次迭代时，开始持续向周围用户发送偏高的感知状态‘120’. 图 3(b)绘出了两种方案在某次仿真时的信息交互过程，显然，基本方案对 SFA 攻击毫无抵抗能力，所有合法次用户的状态均朝着错误状态移动；相反，改进方案能很快发现并及时剔除用户 12，并能使绝大多数合法次用户迅速一致趋于正确状态. 类似地，在 IFA 攻击场景中，用户 12 将在 H_1 条件下始终发送很低的感知状态‘1’，而在 CFA 攻击场景中它将一直发送[0,100]区间内的随机状态值. 图 3(c)和图 3(d)分别给出了这两种方案在 IFA 和 CFA 攻击场景中进行某次仿真时的信息交互过程. 从两图中不难发现，改进方案能有效保护合法次用户不受 IFA 和 CFA 攻击的影响.

图 3 和表 1 中的结果充分说明，改进方案在以上 4 种场景中均能使绝大多数合法次用户最终状态趋于一致，而基本方案在任意一种 SSDF 攻击条件下几乎都无法收敛，尤其在 CFA 攻击条件下，即使迭代次数足够多，各次用户的状态也始终无法趋于一致.

为了进一步说明改进方案在抵抗 SSDF 攻击方面的优势，本文还对比了这两种方案在各种攻击场景中的协作感知性能. 以 SFA 攻击场景为例，图 4 给出了当 CRN 面临 0-2 个 SFA 攻击时，这两种方案分别进行 100000 次仿真得到的 CROC(Q_m-Q_f)曲线. 为便于对比，图中还依据式(21)和(20)给出了相应的理论下限值. 从

图 4 中可以看出:(1)改进方案在无攻击条件下的 CROC 性能与理想下限的差距较小,而在有攻击条件下,由于某些合法节点不可避免地受到攻击的部分影响,它的 CROC 特性与理论下限值相比确实存在一定的差距;(2)虽然基本方案的 CROC 性能在无攻击条件下与理论下限曲线基本一致,但是它在 SFA 攻击条件下的 Q_m 和 Q_f 分别恒等于 0 和 1,即基本无抵抗能力.类似地,在 IFA 攻击和 CFA 攻击场景中的仿真均能得到与此相近的结果.可见,基本方案的协作检测性能只有在无攻击条件下才略优于改进方案,只要网络中存在任意一种 SSDF 攻击,基本方案就将完全失效;而改进方案的检测性能随着恶意用户数量的增多,并未发生太大变化,其抗攻击能力明显优于基本方案.

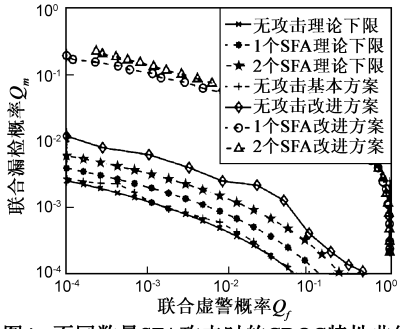

图4　不同数量SFA攻击时的CROC特性曲线

5　结论

本文重点研究了分布式 CSS 中的安全问题,在一致性 CSS 方案的基础上进行了两方面改进:一是利用基于 Metropolis 权重矩阵的迭代规则替代了通用的迭代算法;二是在信息交互规则中引入了抵抗 SSDF 攻击的策略.仿真结果表明,改进方案的收敛特性和感知性能虽然在无攻击条件下比现有方案稍逊一些,但是在任意一种 SSDF 攻击场景中,其稳健性明显增强.

参考文献

[1] Zhao Q, Sadler B M. A survey of dynamic spectrum access [J]. IEEE Signal Processing Magazine, 2007, 24(3): 79 – 89.

[2] 朱佳,郑宝玉,邹玉龙.基于最佳中继选择的协作频谱感知方案研究[J].电子学报,2010,38(1):92 – 98.
Zhu Jia, Zheng Bao-Yu, Zou Yu-Long. Cooperative spectrum sensing in multiuser cognitive radio networks with best relay selection[J]. Acta Electronica Sinica, 2010, 38(1): 92 – 98. (in Chinese)

[3] Shen B, Ullah S, Kwak K. Deflection coefficient maximization criterion based optimal cooperative spectrum sensing[J]. AEU - International Journal of Electronics and Communications, 2010, 64(9): 819 – 827.

[4] Li Z, Yu F R, Huang M. A cooperative spectrum sensing consensus scheme in cognitive radios[A]. INFOCOM[C]. Leblon: IEEE, 2009. 2546 – 2550.

[5] Chen R, Park J, Bian K. Robust distributed spectrum sensing in cognitive radio networks[A]. INFOCOM[C]. Phoenix: IEEE, 2008. 31 – 35.

[6] Li H, Han Z. Catching attacker(s): for collaborative spectrum sensing in cognitive radio systems: an abnormality detection approach[A]. DySPAN[C]. Singapore: IEEE, 2010. 1 – 12.

[7] Yu F R, Tang H, Huang M, et al. Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios[A]. MILCOM[C]. Boston: IEEE, 2009. 1 – 7.

[8] Lin X, Boyd S, Lall S. A scheme for robust distributed sensor fusion based on average consensus[A]. 4th IPSN[C]. Los Angeles: IEEE, 2005. 63 – 70.

[9] Urkowitz H. Energy detection of unknown deterministic signals [J]. Proceedings of the IEEE, 1967, 55(4): 523 – 531.

[10] Ren W, Beard R W. Consensus seeking in multiagent systems under dynamically changing interaction topologies[J]. IEEE Trans on Automatic Control, 2005: 655 – 661.

[11] Digham F F, Alouini M, Simon M K. On the energy detection of unknown signals over fading channels[A]. ICC[C]. Alaska: IEEE, 2003. 3575 – 3579.

[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] Abramowitz M, Stegun I A. Handbook of Mathematical Functions, National Bureau of Standards, Applied Math. Series #55[M]. New York: Dover Publications, 1965.

[14] Kyperountas S, Correal N, Shi Q, et al. Performance analysis of cooperative spectrum sensing in suzuki fading channels [A]. 2nd CrownCom[C]. Orlando: IEEE, 2007. 428 – 432.

作者简介

刘　全　男,1985 年生于江西萍乡,海军工程大学博士生,研究方向:认知无线电链路层关键技术,多抽样率信号处理理论及应用.
E-mail: liuquan.hjgc@gmail.com

高　俊　男,1957 年生于江苏泰州,海军工程大学教授,博导,主要研究方向:软件无线电,数字通信理论与技术.
E-mail: gaojunnj@163.com