



研究与开发

基于信任度的可变门限能量检测算法

肖洁, 陈跃斌, 陈楚天, 郑婷, 钱继武

(云南民族大学电气信息工程学院, 云南 昆明 650500)

摘要: 针对随机的概率式频谱感知数据篡改 (spectrum sensing data falsification, SSDF) 攻击, 提出基于信任度的可变门限能量检测算法。首先比较实际融合值与融合中心上、下边界值的关系, 更新可变门限, 且通过系统给定的虚警概率和漏检概率确定上、下边界值; 其次采用基于正确感知次数和总感知次数比值确定信任值的软融合方法。仿真结果表明, 与传统固定门限相比, 算法抵御攻击的同时不仅能够降低虚警概率和漏检概率, 同时可以提高系统检测概率。

关键词: 认知无线电; 能量检测; 概率式 SSDF 攻击; 可变门限

中图分类号: TN925

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018203

Variable threshold energy detection algorithm based on trust degree

XIAO Jie, CHEN Yuebin, CHEN Chutian, ZHENG Ting, QIAN Jiwu

School of Electrical and Information Technology, Yunnan Minzu University, Kunming 650500, China

Abstract: Aiming at stochastic probabilistic SSDF attacks, a variable threshold energy detection algorithm based on trust degree was proposed. Firstly, the variable threshold was updated by comparing the actual fusion value with the upper and lower boundary values of the fusion center. The upper and lower boundary values were determined through the given false alarm probability and missed probability. Secondly, a soft fusion method was used based on the ratio of correct perception times and the total number of times to update the trust value. Simulation results show that, compared with the traditional fixed threshold, the proposed algorithm can not only reduce the false alarm and missed detection probability, but also improve the detection probability of the system.

Key words: cognitive radio, energy detection, probabilistic spectrum sensing data falsification attack, variable threshold

1 引言

为了解决频谱资源紧缺问题, 认知无线电

(cognitive radio, CR) 技术被提出, 受到国内外研究学者的高度关注。CR 技术在不影响主用户 (primary user, PU) 正常工作的情况下动态感知

收稿日期: 2017-12-22; 修回日期: 2018-06-08

通信作者: 陈跃斌, cybuestc@sina.com

基金项目: 国家自然科学基金资助项目 (No.61261022); 云南民族大学创新团队项目

Foundation Items: The National Natural Science Foundation of China (No.61261022), Innovation Team Project of Yunnan Minzu University



空闲频谱^[1]。作为 CR 技术的首要环节——频谱感知,感知结果的好坏直接影响整个认知无线网络的性能。协作频谱感知通过融合多个认知用户 (cognitive user, CU) 的感知数据,提高频谱感知的精确性,消除单用户感知结果的不确定性和误差^[2]。但协作感知过程存在着诸多风险^[3-4],SSDF (spectrum sensing data falsification, 频谱感知数据篡改) 攻击是其中之一,即恶意用户 (malicious user, MU) 通过给融合中心 (fusion center, FC) 发送虚假的数据以致其做出错误的判决结果^[5-6]。

目前,抵御 SSDF 攻击的协作频谱感知方案较多。参考文献[7]分析 SSDF 攻击下协作频谱感知的性能限制问题并提出最优的攻击者跟踪策略,但未考虑最优策略的计算复杂度。参考文献[8]提出通过加权系数消除来自恶意用户的虚假信息,从而实现抑制恶意用户的协作检测技术,但此方法未考虑概率式 SSDF 攻击。参考文献[9]提出攻击意识的协作频谱感知方案抵御 SSDF 攻击,该方案对攻击强度进行评估,用硬判决准则得到使贝叶斯风险最小的 K 值,虽然分析了攻击强度,但未考虑概率式 SSDF 攻击。参考文献[10]提出基于改进的软融合能量检测算法抵御 SSDF 攻击方案,通过建立用户的历史服务质量信誉机制,并利用不同用户的平均信誉度合理分配权重,减少恶意用户对融合结果的影响,同样此方案也未考虑概率式 SSDF 攻击。参考文献[11]在参考文献[10]基础上针对概率式 SSDF 攻击采用协方差检测方法,基于改进的软融合方法中提出衰减因子,改善了低信噪比下的检测性能。参考文献[12]提出一种基于贝叶斯模型的协作频谱感知方案抵御 SSDF 攻击,通过比较融合值与固定门限的大小得到判决结果。虽然是抵御概率式 SSDF 攻击,但不能有效抵御攻击,原因是当恶意用户发动攻击时,融合值不断变化,系统需要门限为适应融合值的变化而变化,确保得到精确的判决结果,以有效抵御概率式 SSDF 攻击。

为了解决参考文献[12]中的问题,本文提出了一种基于信任度的可变门限策略 (variable threshold energy detection based on reputation, RVTED) 抵御概率式 SSDF 攻击。通过分析认知用户与以往提供感知数据的行为表现,将信任值看成正确感知次数与总感知次数的比值,给每个认知用户分配相应权值。首先攻击者发送概率式 SSDF 攻击,根据融合中心融合值的变化改变判决门限确保系统得到更精确的判决;其次在无攻击者的情况下,通过给定的较小的虚警概率和漏检概率分别得到融合值的上边界值和下边界值;最后通过比较真实融合值与上下边界值的大小关系进而确定系统门限大小,得到最终的判决结果。

2 系统模型和攻击问题

2.1 系统模型

存在多个恶意用户的协作频谱感知模型如图 1 所示,认知无线网络模型中存在一个 FC、一个 PU 和 M 个 CU。融合中心融合每个认知用户的本地感知结果并做出最终判决,判断 PU 是否工作。第 i 个认知用户的二元假设检验:

$$y_i(n) = \begin{cases} \eta_i(n), & H_0 \\ h_i s(n) + \eta_i(n), & H_1 \end{cases} \quad i = 1, 2, \dots, M \quad (1)$$

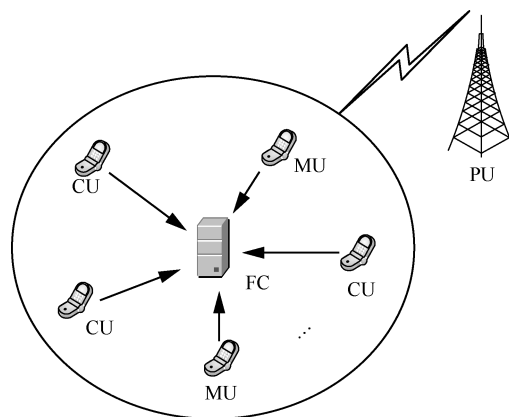


图 1 存在多个恶意用户的协作频谱感知模型

H_1 代表假设 PU 信号存在并占用频段, H_0 代表假设 PU 不存在频段空闲情况, n 表示采样的样

本数量, $y_i(n)$ 是第 i 个 CU 接收到的信号, h_i 是 PU 与第 i 个 CU 之间进行信号传输的信道增益, $s(n)$ 表示 PU 信号, $\eta_i(n)$ 是第 i 个 CU 服从均值为零、方差为 σ_i^2 的加性高斯白噪声。 $s(n)$ 和 $\eta_i(n)$ 是实信号且相互独立。

2.2 能量检测

能量检测是认知无线电技术最常用的频谱感知方法。因其不需知道 PU 的先验信息, 只需计算所有采样点的能量, 与预先设定的门限进行比较, 得到检测结果, 是目前最有效的检测未知信号的方法。

假设每个 CU 的本地能量检测采样样本为 N , 则第 i 个 CU 的本地能量检测统计量 Y_i 为:

$$Y_i = \frac{1}{N} \sum_{n=1}^N |y_i(n)|^2 \quad (2)$$

由中心极限定理, 当 N 足够大 ($N \geq 50$) 时, Y_i 近似服从高斯分布^[11]:

$$\begin{cases} H_0: Y_i \sim N(\sigma_i^2, 2\sigma_i^4/N) \\ H_1: Y_i \sim N((1+\gamma_i)\sigma_i^2, 2(2\gamma_i+1)\sigma_i^4/N) \end{cases} \quad (3)$$

其中, γ_i 代表第 i 个认知用户接收信噪比。

根据式 (3), 第 i 个 CU 的本地检测概率 $p_d(i)$ 、本地虚警概率 $p_f(i)$ 为:

$$p_d(i) = \Pr(Y_i \geq \lambda_i / H_1) = Q\left(\left(\frac{\lambda_i}{\sigma_i^2} - \gamma_i - 1\right) \sqrt{\frac{N}{4\gamma_i + 2}}\right) \quad (4)$$

$$p_f(i) = \Pr(Y_i \geq \lambda_i / H_0) = Q\left(\left(\frac{\lambda_i}{\sigma_i^2} - 1\right) \sqrt{\frac{N}{2}}\right) \quad (5)$$

其中, λ_i 是第 i 个 CU 的本地判决门限, $Q(x)$ 为互

补误差函数, 且 $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt$ 。

采用纽曼皮尔逊准则, 推导式 (5) 得到本地判决门限 λ_i :

$$\lambda_i = (Q^{-1}(p_f(i)) \cdot \sqrt{N/2} + 1) \sigma_i^2 \quad (6)$$

2.3 概率式 SSDF 攻击过程

假设恶意用户的攻击强度 Δ (偏离本地感知能量的值)、攻击概率 p_a , 第 i 个 CU 本地判决结果为 d_i 。协作频谱感知过程, 每个 MU 以概率 p_a

发送 SSDF 攻击导致融合中心做出错误的判决结果。具体情况如下^[9]:

(1) 当 MU 不发送攻击, MU 将发送正确的能量值 Y_i 和本地判决结果 d_i 到融合中心;

(2) 当存在 PU 信号占用频段的情况下 ($Y_i > \lambda_i$), MU 以概率 p_a 发送 “0” 攻击, MU 将发送虚假的能量值 $Y_i - \Delta$ 代替 Y_i 和本地判决结果 d_i 到融合中心;

(3) 当不存在 PU 信号频段空闲的情况下 ($Y_i < \lambda_i$), MU 以概率 p_a 发送 “1” 攻击, MU 将发送虚假的能量值 $Y_i + \Delta$ 代替 Y_i 和本地判决结果 d_i 到融合中心。

因此第 i 个 CU 发送到融合中心的真实本地感知数据 Z_i 为:

$$Z_i = \begin{cases} Y_i, & \text{无攻击} \\ Y_i - \Delta, & \text{“0” 攻击} \\ Y_i + \Delta, & \text{“1” 攻击} \end{cases} \quad (7)$$

融合中心采用线性加权融合认知用户的本地感知数据, 融合中心值为:

$$Z_c = \sum_{i=1}^M w_i \cdot Z_i \quad (8)$$

其中, w_i 是第 i 个 CU 的本地感知能量的加权系数且 $\sum_{i=1}^M w_i = 1$ 。

3 基于可变门限策略抵御 SSDF 攻击

3.1 MU 不发送攻击

Z_c 是 MU 不发动攻击时融合中心的值, 由于 Z_i 服从高斯分布, 则根据式 (7)、式 (8), Z_c 也服从高斯分布:

$$\begin{cases} H_0: Z_c \sim N\left(\sum_{i=1}^M w_i \sigma_i^2, 2 \sum_{i=1}^M w_i^2 \sigma_i^4 / N\right) \\ H_1: Z_c \sim N\left(\sum_{i=1}^M w_i (1+\gamma_i) \sigma_i^2, 2 \sum_{i=1}^M w_i^2 (1+2\gamma_i) \sigma_i^4 / N\right) \end{cases} \quad (9)$$

由式 (7) ~ 式 (9), MU 不发动攻击时的全局虚警概率 p_f 和全局漏检概率 p_m 为:



$$p_f = \Pr(Z_c \geq \lambda_c / H_0) = Q \left(\frac{\lambda_c - \sum_{i=1}^M w_i \sigma_i^2}{\sqrt{2 \sum_{i=1}^M w_i^2 \sigma_i^4 / N}} \right) \quad (10)$$

$$p_m = \Pr(Z_c > \lambda_c / H_1) = 1 - Q \left(\frac{\lambda_c - \sum_{i=1}^M w_i (1 + \gamma_i) \sigma_i^2}{\sqrt{2 \sum_{i=1}^M w_i^2 (1 + 2\gamma_i) \sigma_i^4 / N}} \right) \quad (11)$$

其中, λ_c 为融合中心的判决门限。采用纽曼皮尔逊准则, 由式 (10) 推导融合中心的判决门限 λ_c :

$$\lambda_c = Q^{-1}(p_f) \cdot \sqrt{2 \sum_{i=1}^M w_i^2 \sigma_i^4 / N} + \sum_{i=1}^M w_i \sigma_i^2 \quad (12)$$

3.2 MU 以概率 p_a 发送攻击

假设环境中 MU 的数量为 J ($J \leq M/2$), 当 MU 发送攻击时, 方式有 2 种: PU 占用频段时以概率 p_a 发送“0”攻击; PU 不占用频段时以概率 p_a 发送“1”攻击, 由式 (7)、式 (8) 知 MU 发动攻击时的融合中心值为:

$$Z'_c = \sum_{i=1}^M w_i Y_i \pm \sum_{i=1}^J w_i \Delta \quad (13)$$

其中, Z'_c 表示 MU 发动攻击时的融合中心值。由于 $\sum_{i=1}^M w_i = 1$ 且 $J \leq M/2$, 可知:

$$Z'_c = \begin{cases} \sum_{i=1}^M w_i Y_i + \sum_{i=1}^J w_i \Delta, & H_0 \\ \sum_{i=1}^M w_i Y_i - \sum_{i=1}^J w_i \Delta, & H_1 \end{cases} \quad (14)$$

同样地, Z'_c 也服从高斯分布, 如式 (15):

$$\begin{cases} H_0: Z'_c \sim N \left(\sum_{i=1}^M w_i \sigma_i^2 + \sum_{i=1}^J w_i \Delta, 2 \sum_{i=1}^M w_i^2 \sigma_i^4 / N \right) \\ H_1: Z'_c \sim N \left(\sum_{i=1}^M w_i (1 + \gamma_i) \sigma_i^2 - \sum_{i=1}^J w_i \Delta, 2 \sum_{i=1}^M w_i^2 (1 + 2\gamma_i) \sigma_i^4 / N \right) \end{cases} \quad (15)$$

根据式 (15) 知, 在 H_0 情况下发送“1”攻击, $Z'_c > Z_c$ 需使式 (12) 中的门限 λ_c 升高得到精确的判决结果; 在 H_1 情况下发送“0”攻击, $Z'_c < Z_c$ 需使式 (12) 中的门限 λ_c 降低得到精确的判决结果。门限 λ_c 需随着发起攻击时融合中心值的变化

而发生移动, 可变门限 λ'_c 为:

$$\lambda'_c = \begin{cases} \lambda_c + \sum_{i=1}^J w_i \Delta, & H_0 \\ \lambda_c - \sum_{i=1}^J w_i \Delta, & H_1 \end{cases} \quad (16)$$

为了确定门限 λ'_c 具体取值, 假设 Z_H 和 Z_L 分别表示融合中心统计能量的上边界值和下边界值。如图 2 所示, 令 $p_f = p(Z_c \geq Z_H | H_0) = 0.05$ 或者 $p_m = p(Z_c \leq Z_L | H_1) = 0.05$, 由式 (10)、式 (11) 推导 Z_H 、 Z_L , 得到式 (17):

$$\begin{cases} Z_H = Q^{-1}(0.05) \cdot \sqrt{2 \sum_{i=1}^M w_i^2 \sigma_i^4 / N} + \sum_{i=1}^M w_i \sigma_i^2 \\ Z_L = Q^{-1}(1 - 0.05) \cdot \sqrt{2 \sum_{i=1}^M w_i^2 (1 + 2\gamma_i) \sigma_i^4 / N} + \sum_{i=1}^M w_i (1 + \gamma_i) \sigma_i^2 \end{cases} \quad (17)$$

通过比较 Z_c 和上下边界值的大小, 确定门限的 λ'_c 取值:

$$\lambda'_c = \begin{cases} \lambda_c + \sum_{i=1}^J w_i \Delta, & H_0, Z_c > Z_H \\ \lambda_c - \sum_{i=1}^J w_i \Delta, & H_1, Z_c < Z_L \end{cases} \quad (18)$$

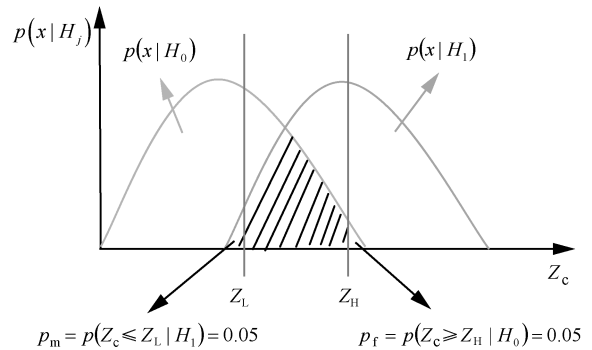


图2 二元信号能量检测的能量值与判决概率分布

4 基于信任值的软融合方法抵御 SSDF 攻击

每个 CU 的信任值与其以往提供感知数据的行为表现有关, 过去经常提供正确的感知数据使其信任值升高, 错误的感知数据使信任值降低^[13]。

因此, 每个认知用户的信任值被看成正确感知次数与感知总数的比值。用二元假设表示第 i 个 CU 本地感知判决结果 d_i 为:

$$d_i = \begin{cases} 0, & H_0 \\ 1, & H_1 \end{cases} \quad (19)$$

其中, “1” 和 “0” 表示 PU 信号存在并占用频段或者不存在频段空闲的判决结果。 d_{FC} 表示融合中心的判决结果, 根据 CU 和 FC 所做判决结果见表 1。

表 1 K 次采样 M 个认知用户与融合中心的判决分布

采样数	CU ₁	CU ₂	...	CU _i	...	CU _M	FC
1	d_1	d_2	...	d_i	...	d_M	d_{FC}
2	d_1	d_2	...	d_i	...	d_M	d_{FC}
...	...	...	...	...	...	...	...
K	d_1	d_2	...	d_i	...	d_M	d_{FC}

由表 1 可知, 第 i 个 CU 的信任度 R_i 为:

$$R_i = \frac{C_i}{S_i}, \quad S_i \neq 0 \quad (20)$$

其中, C_i 表示在 K 次采样中的正确感知次数, S_i 是总感知次数。

很明显, 当认知用户提供较大的信任值时, 其在数据融合过程中就要占较大比重来改善协作频谱感知的性能。因此第 j 个 CU 分配的加权系数为:

$$w_j = R_j / \sum_{i=1}^M R_i, \quad j = 1, 2, \dots, M \quad (21)$$

总的来说, 根据式 (10) 和式 (11), 由 Q 函数的性质知: p_f 是门限的单调递减函数, p_m 是门限的单调递增函数。由式 (18) 可知, SSDF 攻击者发送攻击时, 本文提出的可变门限下的全局虚警概率 p_f 和漏检概率 p_m 的变化为:

$$\begin{cases} p_f(\lambda'_c) < p_f(\lambda_c), H_0, \text{以概率 } p_a \text{ 发送“1”攻击} \\ p_m(\lambda'_c) < p_m(\lambda_c), H_1, \text{以概率 } p_a \text{ 发送“0”攻击} \end{cases} \quad (22)$$

5 仿真结果及分析

本文给出抵御 SSDF 攻击的等增益固定门限

算法以及本文提出的基于信任度的可变门限算法的仿真性能分析。考虑信道中存在加性高斯白噪声, 且假设在真实的无线通信环境中, 即实际存在的攻击者的所占比例少于正常认知用户所占比例。本文采用蒙特卡洛方法进行仿真, 蒙特卡洛次数为 10 000, 假设网络模型中存在一个 PU、一个 FC, 认知用户数量 $M = 10$, 采样点数为 N 。系统中 MU 发起攻击的概率 $p_a = 0.8$, 攻击强度 Δ , 其攻击过程描述如下: 在主用户存在的情况下以概率 $p_a = 0.8$ 发送 “0” 攻击; 主用户不存在的情况下以概率 $p_a = 0.8$ 发送 “1” 攻击。仿真实验采用 BPSK 数字信号作为信号源, 对 BPSK 进行采样, 且加性高斯白噪声服从均值为零、方差为 $\sigma_i^2 (i = 1, 2, \dots, M)$ 的高斯分布。

图 3 给出采样数 $M = 50$, 信噪比 $\text{SNR} = -5$ dB, 存在 2 个 MU, 攻击概率攻击 $p_a = 80\%$, 强度 $\Delta = 0.5$ 时, 两种方案下得到的虚警概率随着给定虚警概率的变化曲线。本文提出的基于信任度的可变门限算法的全局虚警概率明显低于等增益算法。概率式 SSDF 攻击的存在, 导致 CU 发送至融合中心的感知数据的能量值发生较大偏移, 融合中心进行数据融合得到相对较高的 p_f 。因为在 PU 不占用频段, MU 发动攻击导致融合中心的能量统计值升高, 本文算法通过提高门限降低系统的虚警概率 p_f 。图 3 给出的攻击强度为 0.5, 相对较小, 当给定虚警概率 $p_f = 0.1$, 两种算法的虚警概率依次为 0.3、0.06。相比较得到, 本文算法得到较低的虚警概率。

图 4 是采样数 $M = 50$, 信噪比 $\text{SNR} = -5$ dB, 存在 2 个 MU, 攻击概率攻击 $p_a = 80\%$, 强度 $\Delta = 0.5$ 、1、2 时, 本文提出可变门限算法的全局虚警概率 p_f 随着给定虚警概率的变化曲线。从图 4 可以看出, 随着攻击强度的增加, 全局虚警概率 p_f 随之增加, 但增幅较小, 即使是在攻击强度 $\Delta = 2$ 的强攻击下, 本文算法依然可以得到较低的虚警概率。

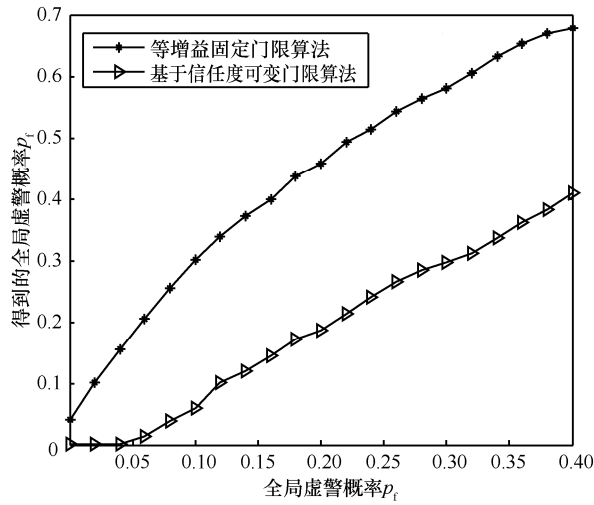
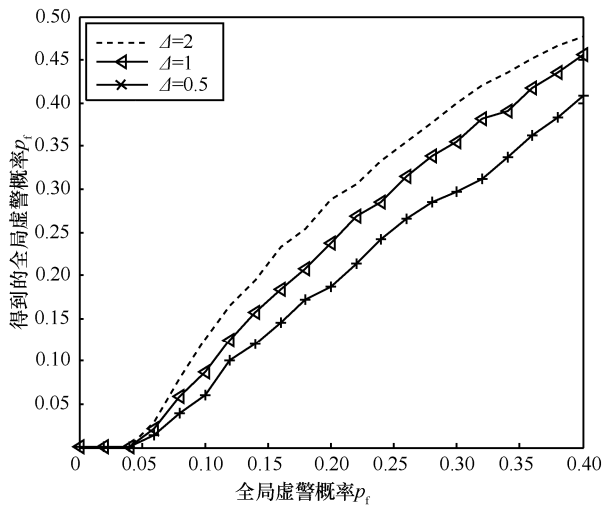
图3 不同方案下随 p_f 变化的虚警概率曲线图4 不同攻击强度下基于信任度的可变门限算法随 p_f 变化的虚警概率曲线

图5描述了采样数 $M=50$ ，信噪比 $\text{SNR} = -5 \text{ dB}$ ，存在2个MU，攻击概率攻击 $p_a = 80\%$ ，强度 $\Delta=2$ 时，两种算法的全局漏检概率 p_m 随给定虚警概率的变化曲线。由图5可知，两种算法的漏检概率都随着虚警概率的增加而降低，同种条件下可变门限算法比等增益固定门限算法的漏检概率降低较快，尤其是虚警概率 p_f 较低的情况下，在 $p_f = 0.1$ ，两种算法的漏检概率分别为0.0725、0.0085。其主要原因是PU工作的情况下，攻击者发送恶意攻击导致融合中心的统计量变小，本文算法通过降低可变门限值导致判决为“0”的情况有所减少进而得到较低的漏检概率 p_m 。

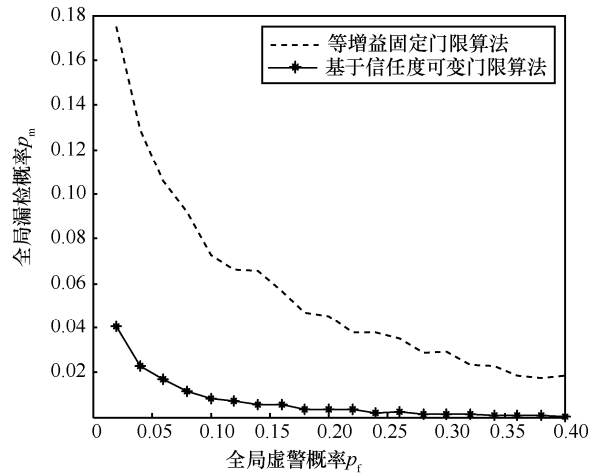
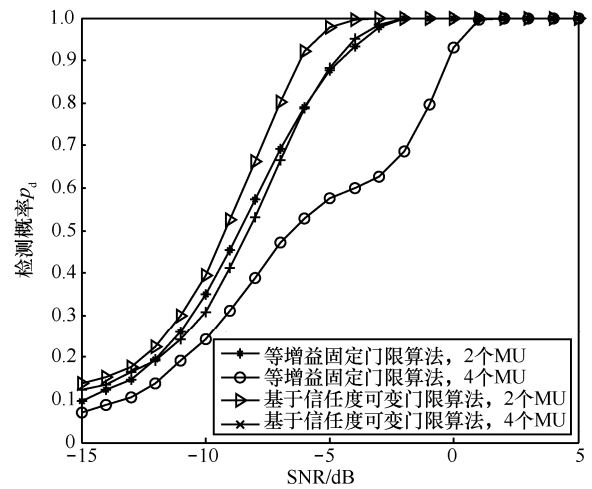
图5 不同方案下随 p_f 变化的漏检概率曲线图6 不同方案下随信噪比变化的检测概率 p_d 的曲线

图6给出采样数 $M=50$ ，攻击概率攻击 $p_a = 80\%$ ，攻击强度为最大攻击强度即信号与噪声的总能量且 $p_f = 0.05$ ，MU数量分别为2个和4个时，两种算法系统检测概率 p_d 随信噪比的变化。从图6知，随着信噪比的增加两种算法的检测概率都上升，在攻击者数量一样的情况下本文优化算法比等增益固定门限算法的检测概率要高且能较快达到1。在 $\text{SNR} = -10 \text{ dB}$ ，攻击者数量为4时，两种算法的检测概率分别为0.2417、0.3075，检测性能提高了27%。

6 结束语

本文针对概率式SSDF攻击，提出基于信任

度的可变门限能量检测协作频谱感知算法。本算法的门限值不再是固定不变的,而是随着恶意用户发动攻击的情况发生变化,其过程是通过比较融合中心真实值与上下边界值的大小决定门限增大或减小,然后将实际融合中心值与变化过的门限进行比较,得到最终判决。算法中的信任度主要依据以往提供感知数据的行为表现进行更新,将正确感知次数与总感知次数的比值看成信任度,合理分配权重。仿真结果表明,该算法与传统算法相比,能有效抵御 SSDF 攻击,在降低漏检概率和虚警概率的同时提高了系统的检测概率。

参考文献:

- [1] YANG J X, CHEN Y B, SHI W G, et al. Cooperative spectrum sensing against attacks in cognitive radio networks [C]// 2014 IEEE International Conference on Information and Automation (ICIA), July 26-31, 2014, Hulun Buir, China. Piscataway: IEEE Press, 2014: 71-75.
- [2] 冯景瑜, 李金龙, 卢光跃. 协作频谱感知中抗 SSDF 攻击的认知用户不确定性行为评估[J]. 电信科学, 2015, 31(2): 97-102.
FENG J Y, LI J L, LU G Y. Evaluating uncertainty behaviors of cognitive users against SSDF attack for cooperative spectrum sensing[J]. Telecommunications Science, 2015, 31(2): 97-102.
- [3] 裴庆祺, 李红宁, 赵弘洋. 认知无线电网络安全综述[J]. 通信学报, 2013, 34(1): 144-158.
PEI Q Q, LI H N, ZHAO H Y, et al. Security in cognitive radio networks[J]. Journal of communication, 2013, 34(1): 144-158.
- [4] XIAO J, CHEN Y B, XING C X, et al. An optimized scheme to resist primary user emulation attacks[C]// The 2016 International Conference on Communications, Information Management and Network Security(CIMNS2016), Sept 25-26, 2016, Shanghai, China. [S.l.:s.n.], 2016: 176-180.
- [5] 卢光跃, 苏杭. 分布式协作认知无线电 SSDF 攻击的防御策略综述[J]. 电信科学, 2017, 33(1): 95-105.
LU G Y, SU H. Survey on SSDF attack and defense for distributed cooperative cognitive radio[J]. Telecommunications Science, 2017, 33(1): 95-105.
- [6] 冯景瑜. 协作频谱感知中的 SSDF 攻击及其对策研究[J]. 电信科学, 2014, 1(11): 67-72.
FENG J Y. Research on SSDF attack and defense for cooperative spectrum sensing[J]. Telecommunications Science, 2014, 1(11): 67-72.
- [7] RAWAT A S, ANAND P, CHEN H, et al. Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks[J]. IEEE Transactions on Signal Processing, 2011, 59(2): 774-786.
- [8] ZHAO T, ZHAO Y. A new cooperative detection technique with malicious user suppression[C]// IEEE ICC2009, June 14-18, 2009, Dresden, Germany. Piscataway: IEEE Press, 2009: 1-5.
- [9] SHARIFI A A, NIYA M J M. Defense against SSDF attack in cognitive radio networks: attack-aware collaborative spectrum sensing approach[J]. IEEE Communications Letters, 2016, 20(1): 93-96.
- [10] PENG T, CHEN Y B, XIAO J, et al. Improved soft fusion-based cooperative spectrum sensing defense against SSDF attacks[C]// IEEE International Conference on Computer Information and Telecommunication System(CITS 2016), July 6-8, 2016, Kunming, China. Piscataway: IEEE Press, 2016: 134-138.
- [11] YANG Z L, CHEN Y B, XING C X, et al. Improved reputation of soft fusion based on cooperative spectrum sensing defence SSDF attacks[C]//The 2016 International Conference on Communications, Information Management and Network Security(CIMNS2016), Oct 22-23, 2016, Beijing, China. [S.l.:s.n.], 2016: 181-185.
- [12] ZHOU M, SHEN J, CHEN H, et al. A cooperative spectrum sensing strategy based on the Bayesian reputation model in cognitive radio networks[C]//2013 IEEE Wireless Communication and Networking Conference(WCNC 2013), April 7-10, 2013, Shanghai, China. Piscataway: IEEE Press, 2013: 614-619.
- [13] FENG J Y, ZHANG Y Q, LU G Y, et al. Defend against collusive SSDF attack using trust in cooperative spectrum sensing environment[C]// IEEE International Conference on Trust, Security and Privacy in Computing and Communication, Oct 19-20, 2014, Beijing, China. Piscataway: IEEE Press, 2014: 1656-1661.

作者简介



肖洁(1992-), 女, 云南民族大学硕士生, 主要研究方向为认知无线电网络安全、频谱感知数据篡改(SSDF)攻击。

陈跃斌(1963-), 男, 云南民族大学教授、硕士生导师, 主要研究方向为认知无线电、协作频谱感知和认知无线电网络安全。

陈楚天(1991-), 男, 云南民族大学硕士生, 主要研究方向为认知无线电网络安全、频谱检测。

郑婷(1992-), 女, 云南民族大学硕士生, 主要研究方向为认知无线电网络安全、恶意模拟主用户(PUEA)攻击。

钱继武(1990-), 男, 云南民族大学硕士生, 主要研究方向为认知无线电网络安全、频谱感知。