



抵御 SSDF 攻击的维纳滤波器检测算法研究

吴孟礼, 陈跃斌, 吴海锋, 李 敏, 孙祥晟

(云南民族大学 电气信息工程学院, 昆明 650500)

摘 要: 针对认知无线网络中随机概率式频谱感知数据篡改(SSDF)的攻击, 利用基于最小均方误差建立的维纳滤波器对目标信号进行估计, 提出一种维纳滤波器检测(WFD)算法。基于梯度算法训练最优权重, 根据权重对训练数据加权融合并对融合结果取平均作为门限, 将训练得到的权重和门限与各认知用户发送的数据加权融合得出判决结果。仿真结果表明, 与传统的等增益合并算法相比, 在相同的信噪比下, WFD 算法的错误概率降低 20% 以上, 且受 SSDF 攻击的恶意用户所占比例、攻击概率和相对攻击强度等关键参数影响较小, 具有更好的鲁棒性。

关键词: 认知无线电; 频谱感知数据篡改; 最小均方误差; 维纳滤波器; 等增益合并

开放科学(资源服务)标志码(OSID):



中文引用格式: 吴孟礼, 陈跃斌, 吴海锋, 等. 抵御 SSDF 攻击的维纳滤波器检测算法研究[J]. 计算机工程, 2020, 46(11): 187-193.

英文引用格式: WU Mengli, CHEN Yuebin, WU Haifeng, et al. Research on wiener filter detection algorithm for resisting SSDF attacks[J]. Computer Engineering, 2020, 46(11): 187-193.

Research on Wiener Filter Detection Algorithm for Resisting SSDF Attacks

WU Mengli, CHEN Yuebin, WU Haifeng, LI Min, SUN Xiangsheng

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

[Abstract] To deal with the attacks of Spectrum Sensing Data Falsification (SSDF) in cognitive radio network, this paper proposes a Wiener Filter Detection (WFD) algorithm by using the Wiener filter based on the minimum Mean Square Error (MSE) to train the optimal weight and threshold for fusion decision. The algorithm uses the gradient algorithm to train the optimal weight, based on which the training data is weighted and fused, and the average of the fusion results is taken as the threshold. The weight obtained by training and the threshold are used to weight and fuse the data sent by each cognitive user to get the decision results. Simulation results show that compared with the traditional Equal Gain Combination (EGC) algorithm, the error probability of the WFD algorithm can be reduced by more than 20% under the same Signal-to-Noise Ratio (SNR). Also, the WFD algorithm has better robustness, and is less affected by the key parameters of SSDF attacks (including the proportion of malicious users, attack probability and relative attack intensity).

[Key words] Cognitive Radio (CR); Spectrum Sensing Data Falsification (SSDF); minimum Mean Square Error (MSE); Wiener filter; Equal Gain Combination (EGC)

DOI: 10.19678/j.issn.1000-3428.0055930

0 概述

随着人们对无线网络需求量的提高, 频谱资源变得十分紧缺。然而, 美国联邦通信委员会的研究结果表明, 固定频谱分配方式导致频谱利用率低下, 许多授权频段长期处于空闲状态, 没有得到有效

利用^[1]。

为解决频谱紧缺的危机, 认知无线电 (Cognitive Radio, CR) 应运而生。自从 ITOLA 博士提出 CR 概念以来^[2], 该技术得到了不断的研究和应用。CR 技术要求次级用户 (Second User, SU) 在不影响主用户 (Primary User, PU) 正常通信的前提下动态感知空闲

基金项目: 国家自然科学基金 (61762093)。

作者简介: 吴孟礼 (1991—), 男, 硕士研究生, 主研方向为认知无线网络安全; 陈跃斌 (通信作者)、吴海锋, 教授; 李 敏、孙祥晟, 硕士研究生。

收稿日期: 2019-09-05

修回日期: 2019-11-08

E-mail: 1049543669@qq.com

频谱^[3],并伺机接入空闲频段完成通信,一旦 PU 信号返回,SU 必须立即撤离并选择其他空闲信道完成通信,以避免对 PU 造成干扰。因此,频谱感知作为 CR 技术的首要环节,感知性能的优劣会对整个认知无线网络的性能产生重要的影响^[4]。

在采用软融合的集中式协作频谱感知^[5]认知无线网络中,研究人员已经对抵御 SSDF 攻击的方案进行了大量的研究。在融合方法的选择上,文献[6]对常见的 5 种融合准则算法进行了研究,指出由于软融合得到的数据更加完整,因此性能比硬融合更加优越,但文中没有对存在 SSDF 攻击的情况展开分析。文献[7]采用一种剥洋葱的方法抵御 SSDF 攻击,该算法能够提高检测性能,但提前条件是知道系统中是否存在恶意用户(Malicious User, MU)以及恶意用户的类型及数目。文献[8]研究了拜占庭防御算法,分析了互动博弈论视角下拜占庭攻击与防守的矛盾关系。当前国内外许多学者在研究抵御 SSDF 攻击的方案时,倾向于引入信誉机制来识别 MU。文献[9]提出一种基于信誉机制的协作频谱感知算法,融合中心(Fusion Center, FC)根据 SU 的历史表现实行奖惩,增加诚实用户(Honest User, HU)的信誉值,减少 MU 的信誉值。文献[10]提出一种基于信誉的聚类算法,该算法不需要提前了解 MU 的分布或对 MU 的完全识别,大幅降低了全局虚警概率。基于信誉值的融合方式是用信誉值决定 SU 的融合权重,这类算法的优点是当 MU 数量较少时,可以比较准确地识别出 MU,但当 MU 增加时,FC 的误判会惩罚 HU 而对 MU 进行奖励,并且还会对后续的融合产生影响,造成恶性循环。因此,基于信誉值的算法也容易受到恶意用户比例、攻击概率和相对攻击强度的影响。此外,信誉机制的算法需要储存各 SU 发送的数据,极大地增加了系统开销。文献[11-12]均采用基于最小均方误差的频谱感知算法,利用 LMS 算法估计信号的幅值,并直接将估计值作为检测统计量进行判决,但是该算法只适用于本地单用户检测,没有考虑存在攻击者的情况。

目前,多数融合算法都易受 SSDF 攻击的关键参数(恶意用户比例、攻击概率和相对攻击强度)的影响,并且融合权重的获取方法往往都是根据信噪比或者信誉值等单一的因素推导得出,不能全面地贴合 SU 发送数据的特征,或者是融合方式及其复杂因而对系统运算能力的要求极高。针对以上问题,本文将文献[11-12]基于最小均方误差的算法思想应用到集中式协作频谱感知中,提出一种维纳滤波器检测算法。利用基于最小均方误差建立的维纳滤波器对目标信号进行估计,本地检测采用简单的能量检测算法^[13]计算接收信号的能量值,FC 利用训练集数据对维纳滤波器进行训练得到收敛的权重,

运用训练出的权值对训练集中的数据加权融合得到融合结果,将多组融合结果的平均值作为判决门限。在测试阶段利用已生成的权重对各 SU 发送的能量值加权融合得到融合值,将融合值与判决门限比较得出最终判决结果。

1 系统模型和 SSDF 攻击

1.1 系统模型

在集中式协作频谱感知网络中,存在 1 个 FC 和多个 SU, SU 中多数是 HU, 小部分 SU 是 MU。本地 SU 接收到的信号观测值是一个二元假设检验模型:

$$x_i(m) = \begin{cases} \eta_i(m), & H_0 \\ h_i s(m) + \eta_i(m), & H_1 \end{cases} \quad (1)$$

其中, H_0 和 H_1 分别表示 PU 不存在和 PU 存在的情况, $\eta_i(m)$ 表示第 i 个 SU 在第 m 时刻所接收到的信号中的噪声, h_i 表示第 i 个 SU 的信道增益, 信道为块衰落信道(即在一个检测周分量, 且假设 $\eta_i(m)$ 是均值为 0、方差为 σ_i^2 的加性高斯白噪声期内信道增益保持不变), $s(m)$ 表示第 m 时刻 PU 发送的信号, $s(m)$ 与 $\eta_i(m)$ 相互独立, $x_i(m)$ 表示在 H_0 或 H_1 情况下第 i 个 SU 在第 m 时刻所接收到的信号。

各 SU 将感测到的结果发送至 FC, 一般在采用硬融合^[14]的网络中, 要求各 SU 发送 1 bit 的本地判决结果至 FC, 而在软融合^[15]的网络中, 要求各 SU 发送检测到的能量值。MU 为了引导 FC 误判, 故意发送偏离真实情况的检测数据至 FC。FC 接收各 SU 发送的感知结果, 采用特定的准则进行融合作出判决。存在 SSDF 攻击者的集中式频谱感知模型如图 1 所示。

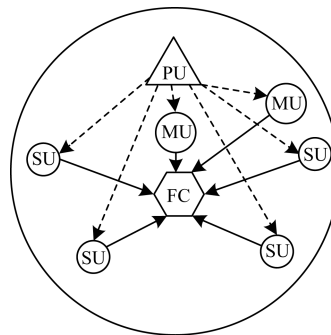


图 1 存在 SSDF 攻击者的集中式频谱感知模型

Fig.1 Centralized spectrum sensing model with SSDF attackers

1.2 本地能量检测

能量检测是一种常用的认知无线电频谱检测算法, 相比于其他检测算法, 该算法不仅简单, 而且不需要知道 PU 的先验信息, 只需计算在各采样点处观测信号的能量, 再与根据某一最佳准则确定的预设门限对比得出判决结果。由于能量检测算法简单快速又易于实现, 因此成为目前应用最广泛的一种盲检测方法。

设每个 SU 在一个检测周期内的采样点数目为 M , 第 i 个 SU 在一个检测周期内的平均能量值用统计量 Y_i 来表示, 则有:

$$Y_i = \frac{1}{M} \sum_{m=1}^M |x_i(m)|^2 \quad (2)$$

在采用软融合的集中式协作频谱感知网络中, HU 只需要直接将检测到的能量值 Y_i 发送至 FC, 再由 FC 负责融合判决。MU 在计算出 Y_i 后, 并不是直接将 Y_i 发送至 FC, 而是以概率 P_a 对 Y_i 进行篡改, 篡改之后得到 Y_i' , 再将 Y_i' 发送至 FC, 以此来扰乱 FC 的判决。

当采样点数目 M 足够大 ($M \geq 45$) 时, Y_i 近似服从高斯分布^[16-17]:

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

其中, γ_i 表示第 i 个 SU 接收到的信号功率与噪声功率之比。

MU 除了需要计算出 Y_i 之外, 还需要对 PU 是否存在进行判决, 首先计算出门限值 λ_i , 再将 Y_i 与 λ_i 比较, 若 $\lambda_i < Y_i$ 则判决为 H_1 , 若 $\lambda_i \geq Y_i$ 则判决为 H_0 。

若第 i 个 SU 是 MU, 则本地门限根据最小错误概率准则^[18]进行设置, 错误概率定义如下:

$$P_{ei} = P(H_0)P_{fi} + P(H_1)P_{mi} \quad (4)$$

其中, P_{ei} 表示第 i 个 SU 的错误概率, $P(H_0)$ 和 $P(H_1)$ 分别表示 PU 不存在和存在的先验概率, P_{fi} 和 P_{mi} 分别为第 i 个 SU 的虚警概率和漏检概率。文献[19]详细推导了以最小错误概率准则设置门限的过程, 最终得出的本地判决门限为:

$$\lambda_i = \frac{\sigma^2}{2} \left(1 + \sqrt{(2\gamma_i + 1) \left[1 + \frac{4 \ln(\theta(2\gamma_i + 1))}{M\gamma_i} \right]} \right) \quad (5)$$

其中, θ 表示先验概率的比值为:

$$\theta = \frac{P(H_0)}{P(H_1)} \quad (6)$$

MU 作出本地判决, 判决结果用 d_i 表示为:

$$d_i = \begin{cases} -1, \lambda_i \geq Y_i \\ 1, \lambda_i < Y_i \end{cases} \quad (7)$$

MU 根据自己的判决结果 d_i 的不同来决定发动不同的攻击。设攻击强度为 Δ , 当 $d_i = -1$ 时, 表示 MU 认为信道空闲, 为了诱导 FC 误判, MU 将 Y_i 的值增大 Δ 之后再发送给 FC, 这样会使 FC 进行判决的虚警概率增大; 当 $d_i = 1$ 时, 表示 MU 判定 PU 存在, 为了诱导 FC 误判, MU 将 Y_i 的值减小 Δ 之后再发送给 FC, 这样会使 FC 的漏检概率增大。因为连续的攻击容易被识别出, 而间歇性的概率型攻击不容易被 FC 察觉, 所以 MU 发动攻击不是连续的, 而是以一定的概率 P_a 发动的。MU 篡改后的数据 Y_i'

可以表示为:

$$Y_i' = Y_i - \Delta d_i \quad (8)$$

其中, 攻击强度 Δ 与噪声功率 P_n 呈线性关系, 即:

$$\Delta = r_a P_n \quad (9)$$

其中, r_a 为相对攻击强度比例。

2 融合中心融合判决

2.1 维纳滤波器

本文使用的维纳滤波器结构如图 2 所示。

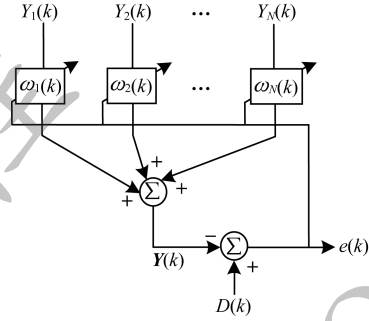


图 2 维纳滤波器结构

Fig.2 Structure of Wiener filter

设训练集总共有 K 组数据, SU 数目为 N , 则设置滤波器的阶数为 N 阶, 设输入观测向量为 $\mathbf{Y}(k) = [Y_1(k) \ Y_2(k) \ \dots \ Y_N(k)]^T$, 其中, $Y_i(k)$ ($i = 1, 2, \dots, N; k = 1, 2, \dots, K$) 表示训练集中的第 i 个 SU 在第 k 个检测周期的能量观测值, $\omega_i(k)$ ($i = 1, 2, \dots, N; k = 1, 2, \dots, K$) 表示第 i 个 SU 在第 k 个检测周期进行融合时的滤波器抽头系数 (权重), 设 $\mathbf{W}(k) = [\omega_1(k) \ \omega_2(k) \ \dots \ \omega_N(k)]^T$, 初始化 $\mathbf{W}(0)$ 为零向量; 采用梯度下降法对权值进行更新, 即:

$$\mathbf{W}(k+1) = \mathbf{W}(k) + \mu e(k) \mathbf{Y}(k) \quad (10)$$

其中, μ 为学习速率参数 (权值更新步长), 为保证算法收敛, μ 的取值有范围限制^[20]:

$$0 < \mu < \frac{1}{\lambda} \quad (11)$$

$$\lambda = \sum_{i=1}^N \sum_{k=1}^K E[Y_i^2(k)] \quad (12)$$

在实际计算时, 用下式来确定 μ 的值:

$$\mu = \left[\frac{1}{\alpha} \sum_{i=1}^N \sum_{k=1}^K Y_i^2(k) \right]^{-1} \quad (13)$$

其中, $\alpha > 1$, α 越大收敛速度越慢, 越小收敛速度越快, 但当 α 越小时, 过渡过程的振荡越大^[21], 因此, 为保证算法收敛且不产生剧烈振荡, α 的取值应大于 1, 但 α 的取值也不宜太大, 否则收敛速度较慢, 在仿真过程中, 经过多次实验发现, 当 α 的值取 10 时, 算法就能快速收敛并且权值振荡较小。 $e(k)$ 为第 k 次迭代时的瞬时误差为:

$$e(k) = D(k) - \mathbf{W}^T(k) \mathbf{Y}(k) \quad (14)$$

其中, $D(k)$ 是第 k 次迭代的需求值, 在 H_1 下 $D(k)$

的取值为接收信号的功率 P , 在 H_0 下 $D(k)$ 取为 $-P$ 。

$$P = P_s + P_n \quad (15)$$

其中, P_s 表示主用户的功率, P_n 表示噪声功率。

经过 K 次迭代后, 得到最终的权重值 \mathbf{W} , 即:

$$\mathbf{W} = \mathbf{W}(K+1) \quad (16)$$

2.2 软融合

融合中心接收各 SU 发送的能量值 Y_i , 再对 Y_i 加权求和, 可以表示为:

$$Z = \sum_{i=1}^N \omega_i Y_i \quad (17)$$

其中, Z 表示最终融合值, ω_i 表示第 i 个 SU 的权重。

不同的软融合方法的差别主要在于权重的赋值方式不同。在等增益算法中, 各 SU 的权重相等:

$$\omega_1 = \omega_2 = \cdots = \omega_N = \frac{1}{N} \quad (18)$$

可见, EGC 算法的本质是求 SU 发送的能量值的均值, 即利用数据的一阶矩进行判决。由于对所有 SU 平等对待, 因此当存在 MU 时, MU 发送的数据偏离真实值会使统计量 Z 的均值发生偏移, 导致错误率增加。

在最大比合并 (Maximal Ratio Combination, MRC) 融合算法中, 权重系数由各 SU 的信噪比决定, 信噪比越大分配的权值越大:

$$\omega_i = \frac{\text{SNR}_i}{\sqrt{\sum_{k=1}^N \text{SNR}_k^2}} \quad (19)$$

在 MRC 融合算法中, ω_i 仅与 SNR_i 有关, 若不存在 MU 或 MU 数量较少时, 该算法可以获得较好的效果, 但当 MU 数量较多时, 由于 MU 的信噪比也可能较高, 会导致该算法性能急剧下降。

为使权重值不单独依赖于 SU 的数量 N 或者 SU 的信噪比, 而是直接由 SU 发送的能量值本身的特征决定, 在本文的算法中, 权重值由训练产生, 即预先给定 K 组能量观测值以及对应的 K 个需求值 $D(k)$ ($k=1, 2, \dots, K$), 将训练数据送入维纳滤波器进行训练, 当给出的训练数据的容量 K 足够大时, 权值 ω_i 收敛, 得到式 (16) 中的权向量 $\mathbf{W} = [\omega_1, \omega_2, \dots, \omega_N]^T$, 再将训练得到的权重代入式 (17) 求得融合值 Z 。相比前两种融合准则, 本文获取加权系数 ω_i 的途径不再是由单一因素决定, 而是由训练得出的建立在最小均方误差基础上的最优权重值。

2.3 软判决

将融合值 Z 与融合中心门限 Th 比较, 得出最终的判决结果。在传统的算法中, Th 是在给定的虚警概率的条件下利用纽曼-皮尔逊准则^[21]或者最小错误概率准则获得, 使得门限受到噪声功率的影响非常大, 并且由于若要准确地知道是否存在攻击及攻

击的强度非常困难, 因此在使用纽曼-皮尔逊准则或者最小错误概率准则设定门限时, 通常是假定在无攻击的条件下推导得出的, 一旦当 MU 发起攻击时, 融合值 Z 发生偏移, 就会造成错误率上升。

本文获得 Th 的方法是用训练出的权重来对训练集中的 K 组能量观测值分别加权融合, 再将融合的结果取平均作为门限, 即:

$$\text{Th} = \frac{1}{K} \sum_{k=1}^K \mathbf{W}^T \mathbf{Y}(k) \quad (20)$$

判决的结果为:

$$D_{fc} = \begin{cases} -1, & \text{Th} \geq Z \\ 1, & \text{Th} < Z \end{cases} \quad (21)$$

由于 ω_i 由训练得出, 并且权值并不依赖于噪声功率, 而是直接依赖于各 SU 发送的数据, 因此 Th 也是直接依赖于各 SU 发送的数据的最优门限。

2.4 WFD 算法

WFD 算法流程如下:

1) 初始化权向量: $\mathbf{W}(0) = 0$; 确定步长因子

$$\mu = \mu = \left[\frac{1}{\alpha} \sum_{i=1}^N \sum_{k=1}^K Y_i^2(k) \right]^{-1}, \alpha = 10。$$

2) 计算瞬时误差: $e(k) = D(k) - \mathbf{W}^T(k) \mathbf{Y}(k)$ 。

3) 更新权向量: $\mathbf{W}(k+1) = \mathbf{W}(k) + \mu e(k) \mathbf{Y}(k)$ 。

4) 重复步骤 2、步骤 3 直到权向量收敛 (默认训练集长度 K 足够大, 当训练 K 次后权向量收敛于 \mathbf{W})。

5) 求判决门限: $\text{Th} = \frac{1}{K} \sum_{k=1}^K \mathbf{W}^T \mathbf{Y}(k)$ 。

6) 引入测试集, 使用训练得到的权值 \mathbf{W} 和门限 Th 对测试集进行软判决:

$$D_{fc} = \begin{cases} 1, & \text{Th} \leq \mathbf{W}^T \mathbf{Y}_{\text{test}} \\ -1, & \text{Th} > \mathbf{W}^T \mathbf{Y}_{\text{test}} \end{cases}$$

其中, \mathbf{Y}_{test} 是各 SU 向 FC 发送的能量值组成的向量。

3 仿真结果与分析

本文将传统的抵御 SSDF 的 EGC 与本文提出的 WFD 算法作对比分析。设定的信道环境为: 主用户与 SU 之间的信道存在瑞利衰落和均值为零的加性高斯白噪声, 信噪比范围设定为 $-20 \text{ dB} \sim -5 \text{ dB}$, 网络模型中存在 1 个 PU 和 1 个 FC, 先验概率 $P(H_0) = P(H_1) = 0.5$, SU 总数目为 $N = 50$, MU 占 SU 总数目的比例为 rm , MU 发起攻击的概率为 P_a , 相对攻击强度比例为 r_a , 仿真采用 BPSK 数字信号作为信号源, 训练样本为 10 000 组数据。本文以全局错误概率 P_e 作为性能指标, 采用蒙特卡洛方法进行仿真, 蒙特卡洛次数为 20 000 次。

体现随机概率型 SSDF 攻击的主要参数有恶意用户比例 rm 、发动攻击的概率 P_a 以及相对攻击强度 r_a , 因此, 仿真中主要分析当这 3 个参数变化时 EGC

和 WFD 全局错误概率的变化。当 rm 、 P_a 、 r_a 三者中的任意一个参数增大时,都会使网络承受的总攻击量增大,对于 EGC 算法来说,由于分配给每个 SU 的权值 ω_i 相等, rm 、 P_a 、 r_a 增大意味着由攻击引起的最终融合值 Z 相对真实情况的偏移量越大,因此,造成的错误概率会增加;对 WFD 算法而言,由于 ω_i 是由训练集训练得出的,因此即便 rm 、 P_a 、 r_a 增大,在训练过程中也会使 MU 的权值减小,使 HU 的权值增大,从而使得 Z 值几乎不会发生偏移。WFD 算法门限设置与 EGC 不同,EGC 是按无攻击的情况设置的固定门限,而 WFD 是由训练出的权重与训练集融合结果的平均值得到,当 rm 、 P_a 、 r_a 变化时,WFD 的门限也会自动适应以达到最佳,因此,WFD 能获得更低的错误概率。

图3所示为当 $P_a = 0.7$ 、 $r_a = 0.6$ 以及 MU 所占的比例分别为 $rm = 0.1$ 、 $rm = 0.2$ 、 $rm = 0.3$ 时,EGC 和 WFD 算法的全局错误概率 P_e 随信噪比 SNR 变化的曲线。

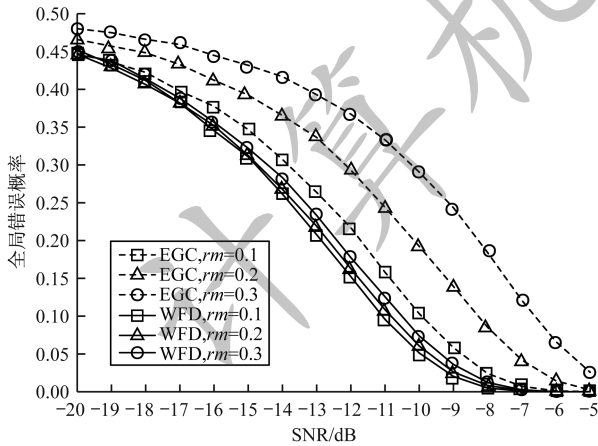


图3 EGC 算法与 WFD 算法在不同恶意用户比例下全局错误概率随信噪比的变化曲线

Fig.3 Curve of global error probability of EGC algorithm and WFD algorithm changing with SNR under different malicious user proportions

从图3可以看出,随着信噪比的增加,两种算法的 P_e 都在减小。两种算法在 $rm = 0.1$ 时 P_e 最小,在 $rm = 0.3$ 时最大,说明随着 rm 增加, P_e 会随之增大。当信噪比低至 -20 dB 时,通信环境十分恶劣,两种算法的 P_e 相差较小且都比较高,当信噪比增大到 -5 dB 时,通信环境相对较好,两种算法的 P_e 相差较小且都比较低。若固定 $P_e = 0.1$,当 $rm = 0.1$ 时 EGC 算法需要信噪比达到 -10 dB,而 WFD 算法只需 -11 dB,WFD 相对于 EGC 算法对信噪比的要求降低了 1 dB。当 $rm = 0.2$ 和 $rm = 0.3$ 时,WFD 相对于 EGC 算法对信噪比的要求分别大约降低了 2.7 dB 和 4 dB;类似地,若固定 $SNR = -10$ dB,当

$rm = 0.1$ 时,EGC 算法的 $P_e = 0.11$,WFD 的 $P_e = 0.05$,错误率降低了 6% ,当 $rm = 0.2$ 和 $rm = 0.3$ 时,WFD 比 EGC 算法的错误率分别降低了 13% 和 21% 。

图4所示为当 $rm = 0.3$ 、 $r_a = 0.6$ 以及攻击概率分别为 $P_a = 0.3$ 、 $P_a = 0.6$ 、 $P_a = 0.9$ 时,EGC 和 WFD 算法的全局错误概率 P_e 随信噪比 SNR 变化的曲线。

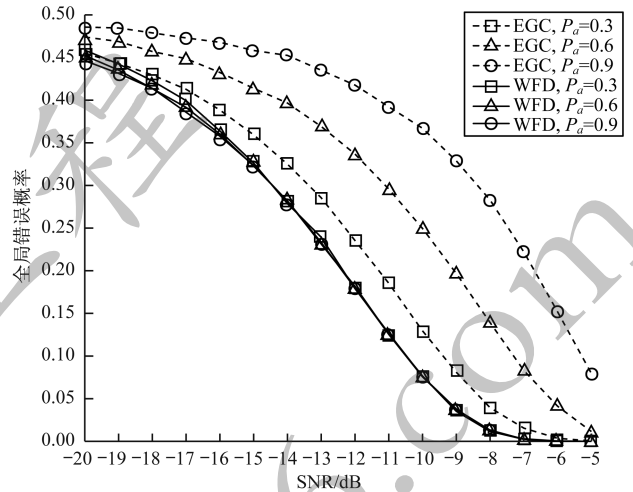


图4 EGC 算法与 WFD 算法在不同攻击概率下全局错误概率随信噪比的变化曲线

Fig.4 Curve of global error probability of EGC algorithm and WFD algorithm changing with SNR under different attack proportions

从图4可以看出,随着 SNR 的增加,两种算法的 P_e 都在降低。两种算法在 $P_a = 0.3$ 时 P_e 最小,在 $P_a = 0.9$ 时最大,说明随着攻击概率的增加, P_e 会随之增大。与图3中的情况类似,在 SNR 极低或较高时,WFD 与 EGC 算法的性能比较接近,但不同的是在改变 P_a 的值时,WFD 的性能曲线几乎没有改变,而 EGC 算法受 P_a 的影响却极其严重,例如,当需要达到的 P_e 为 0.1 时,EGC 算法所需的信噪比分别为 -9.5 dB、 -7.4 dB 和 -5.4 dB,而 WFD 算法所需的信噪比恒为 -10.5 dB,WFD 比 EGC 对信噪比的需求分别降低了 1 dB、 3.1 dB 和 5.1 dB,在相同的错误概率需求下,WFD 比 EGC 算法要求的信噪比更低。若固定 $SNR = -10$ dB,无论 P_a 取何值,WFD 算法的 P_e 总能稳定在 0.08 左右,而 EGC 算法在 $P_a = 0.3$ 、 $P_a = 0.6$ 、 $P_a = 0.9$ 的 P_e 却分别达到了 0.13 、 0.25 、 0.37 ,WFD 比 EGC 的错误率分别降低了 5% 、 17% 和 29% ,因此在相同信噪比下,WFD 算法能够比 EGC 算法获得更低的全局错误概率。

图5所示为当 $rm = 0.3$ 、 $P_a = 0.6$ 以及相对攻击强度分别为 $r_a = 0.4$ 、 $r_a = 0.6$ 、 $r_a = 0.8$ 时,EGC 和 WFD 算法的 P_e 随信噪比 SNR 变化的曲线。

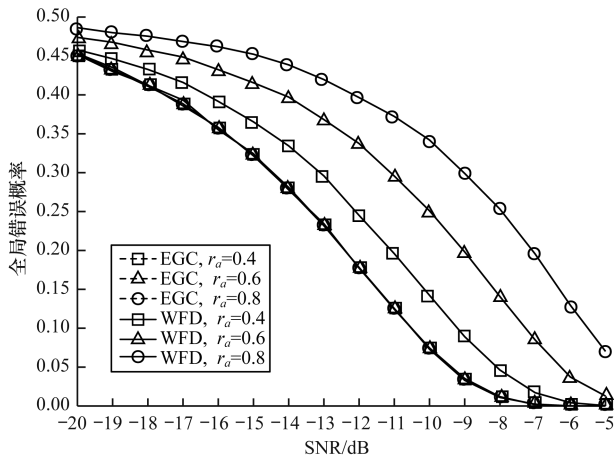


图5 EGC算法与WFD算法在不同相对攻击强度下全局错误概率随信噪比的变化曲线

Fig.5 Curve of global error probability of EGC algorithm and WFD algorithm changing with SNR under different relative attack intensity

从图5可以看出,随着SNR的增加,WFD和EGC算法的 P_e 都在降低。两种算法在 $r_a = 0.4$ 时 P_e 最小,在 $r_a = 0.8$ 时最大,说明随着相对攻击强度的增加, P_e 会随之增大。当需要达到的 P_e 为0.1时,EGC算法所需的信噪比分别为-9.3 dB、-7.3 dB和-5.5 dB,而WFD算法所需的信噪比恒为-10.5 dB,WFD比EGC对信噪比的需求分别降低了1.2 dB、3.2 dB和5 dB,在相同的错误概率需求下,WFD比EGC算法要求的信噪比更低。若固定SNR = -10 dB,无论 P_a 取何值,WFD算法的 P_e 总能稳定在0.07左右,而EGC算法在 $r_a = 0.4$ 、 $r_a = 0.6$ 、 $r_a = 0.8$ 的 P_e 却分别达到了0.14、0.25、0.34,WFD比EGC的错误率分别降低了7%、18%和27%,因此可以看出,当固定SNR时,随着 r_a 的增大,EGC和WFD算法的错误概率之差也在不断增大;当固定所需 P_e 时,随着 r_a 的增大,EGC比WFD算法所需的SNR也在不断增大。

从图3~图5可以发现,随着 rm 、 P_a 、 r_a 中的某一个参数改变时,EGC的性能都受到了较大的影响,而对WFD的性能曲线影响却不大,尤其是在图4和图5中,当 P_a 或 r_a 改变时,WFD的性能曲线仍然几乎重叠在一起,这说明WFD算法在面对SSDF攻击时具有更好的鲁棒性,同时,在固定了 rm 、 P_a 、 r_a 以及SNR后,WFD总是能比EGC算法获得更低的错误概率,在最佳情况下($rm = 0.3$ 、 $r_a = 0.6$ 、 $P_a = 0.9$ 、SNR = -10 dB,见图4),WFD比EGC的错误率降低29%,说明WFD算法对SSDF攻击抵御能力更强,这与前文的分析一致。

4 结束语

针对概率式的SSDF攻击,本文提出一种抵御SSDF攻击的维纳滤波器检测算法,将训练出的权重

与训练集加权融合产生融合门限。实验结果表明,与传统的EGC算法相比,WFD算法具有更强的稳健性且能有效降低错误概率,对抵御SSDF攻击更有效。本文假定了所有SU均处于相同的无线通信环境中(同质场景),下一步将研究贴近于真实的无线通信环境,即各SU的信噪比均不一定相同(非同质环境),采用机器学习的方法对用户进行分类,识别出攻击者并将其发送的数据屏蔽,运用HU的数据进行融合得出更精确的判决结果。

参考文献

- [1] Federal Communications Commission. Spectrum policy task force report [EB/OL]. [2019-07-20]. <http://dx.doi.org/Publication>.
- [2] MITOLA J, MAGUIRE G Q. Cognitive radio: making software radios more personal [J]. IEEE Personal Communications, 1999, 6(4): 13-18.
- [3] YANG J X, CHEN Y B, SHI W G, et al. Cooperative spectrum sensing against attacks in cognitive radio networks [C]//Proceedings of 2014 IEEE International Conference on Information and Automation. Piscataway, USA: IEEE Press, 2014: 71-75.
- [4] PEI Qingqi, LI Hongning, ZHAO Hongyang, et al. Security in cognitive radio networks [J]. Journal on Communications, 2013, 33(1): 144-158. (in Chinese) 裴庆祺, 李红宁, 赵弘洋, 等. 认知无线网络安全综述[J]. 通信学报, 2013, 33(1): 144-158.
- [5] FENG Jingyu, LI Jinlong, LU Guangyue. Evaluating uncertainty behaviors of cognitive users against SSDF attack for cooperative spectrum sensing [J]. Telecommunications Science, 2015, 31(2): 97-102. (in Chinese) 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.
- [6] CHU Yuzhi, ZHENG Baoyu, JI Wei. Data fusion schemes based on cooperative spectrum sensing [J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2010, 30(3): 39-45. (in Chinese) 褚御芝, 郑宝玉, 季薇. 协同频谱感知中的融合策略[J]. 南京邮电大学学报(自然科学版), 2010, 30(3): 39-45.
- [7] WANG Wenkai, LI Husheng, SUN Yan, et al. Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks [J]. EURASIP Journal on Advances in Signal Processing, 2010, 22(11): 40-54.
- [8] ZHANG Linyuan, DING Guoru, WU Qihui, et al. Byzantine attack and defense in cognitive radio networks: a survey [J]. IEEE Communication Surveys & Tutorials, 2015, 17(3): 1342-1363.
- [9] PENG Deming, HU Gang, XU Ming. Trust model-based secure cooperative sensing techniques for cognitive radio networks [C]//Proceedings of the 20th IEEE International Conference on Networks. Washington D. C., USA: IEEE Press, 2011: 1-6.
- [10] HYDER C S, GREBUR B, LI X, et al. ARC: adaptive reputation based clustering against spectrum sensing data falsification attacks [J]. IEEE Transactions on Mobile Computing, 2014, 13(8): 1707-1719.

- [11] WANG Fan, LU Guangyue. Spectrum sensing method using LMS [J]. Journal of Signal Processing, 2016, 32(5):543-549. (in Chinese)
王凡,卢光跃. 利用 LMS 的频谱感知算法[J]. 信号处理, 2016, 32(5):543-549.
- [12] GUO Wenxiang, YU Zhiyong, SUN Yamin. Research on spectrum sensing algorithm based on LMS [J]. Computer Simulation, 2019, 36(2):241-244. (in Chinese)
郭文祥,余志勇,孙亚民. 基于 LMS 的频谱感知算法研究[J]. 计算机仿真, 2019, 36(2):241-244
- [13] URKRWITZ H. Energy detection of unknown deterministic signals [J]. Proceedings of the IEEE, 1967, 55(4):523-531.
- [14] JIANG Xiaolin. Double threshold collaborative spectrum sensing algorithm based on energy sensing [J]. Journal of Heilongjiang University of Science and Technology, 2016, 26(1):75-79. (in Chinese)
江晓林. 基于能量检测的双门限协作频谱感知算法[J]. 黑龙江科技大学学报, 2016, 26(1):75-79.
- [15] CHU Guangqian, CAO Yan, ZHONG Linghui. Analysis of cognitive radio soft fusion algorithm based on cooperative spectrum detection [J]. Science & Technology Information, 2014, 12(25):3-4. (in Chinese)
初广前,曹燕,钟凌惠. 浅析基于协作频谱检测的认知无线电软融合算法[J]. 科技咨询, 2014, 12(25):3-4.
- [16] XU Quanzhi, LÜ Shu. Probability Theory and Mathematical Statistics [M]. 2nd ed. Beijing: Higher Education Press, 2010. (in Chinese)
徐全智,吕恕. 概率论与数理统计[M]. 2版. 北京:高等教育出版社, 2010.
- [17] PENG Ting, CHEN Yuebin, XIAO Jie, et al. Improved soft fusion-based cooperative spectrum sensing defense against SSDF attacks [C]//Proceedings of IEEE International Conference on Computer Information and Telecommunication System. Washington D. C., USA: IEEE Press, 2016:134-138.
- [18] ZHANG Mingyou, LÜ Ming. Signal detection and estimation [M]. 2nd ed. Beijing: Publishing House of Electronics Industry, 2005. (in Chinese)
张明友,吕明. 信号检测与估计[M]. 2版. 北京:电子工业出版社, 2005.
- [19] WEN Kai, JIANG Laiying. Optimization algorithm with dynamic double-threshold cooperative spectrum sensing based on difference of sensing channel [J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science), 2017, 37(1):41-46. (in Chinese)
文凯,姜赖赢. 基于感知信道差异性的动态双门限协作频谱感知优化算法[J]. 南京邮电大学学报(自然科学版), 2017, 37(1):41-46.
- [20] GONG Yaohuan. Adaptive filtering—time-domain adaptive filtering and smart antenna [M]. 2nd ed. Beijing: Publishing House of Electronics Industry, 2003. (in Chinese)
龚耀寰. 自适应滤波——时域自适应滤波和智能天线[M]. 2版. 北京:电子工业出版社, 2003.
- [21] XIAO Jie, CHEN Yuebin, CHEN Chutian, et al. Variable threshold energy detection algorithm based on trust degree [J]. Telecommunications Science, 2018, 34(8):129-135. (in Chinese)
肖洁,陈跃斌,陈楚天,等. 基于信任度的可变门限能量检测算法[J]. 电信科学, 2018, 34(8):129-135.

编辑 索书志