引用格式:宋铁成,吴俊,梁浩宇,等. 基于滑动窗口的协作频谱感知对抗拜占庭攻击[J]. 信息对抗技术,2024, 3(3):63-78.[SONG Tiecheng, WU Jun, LIANG Haoyu, et al. Sliding window-based cooperative spectrum sensing against Byzantine attack[J]. Information Countermeasure Technology, 2024, 3(3):63-78. (in Chinese)]

基于滑动窗口的协作频谱感知对抗拜占庭攻击

宋铁成[1*],吴 俊[2],梁浩宇[2],程之序[1]

(1. 东南大学信息科学与工程学院,江苏南京 210018; 2. 杭州电子科技大学通信工程学院, 浙江杭州 310018)

摘 要 认知无线电技术允许从用户动态地接入主要用户被授权的频谱,提高频谱利用率。协作频谱感知是认知无线电技术的一个重要组成部分,通过空间分集检测主用户信号。然而,由于认知无线网络的开放性,协作频谱感知过程可能会受到拜占庭攻击,恶意用户伪造有关主用户信号的状态信息,然后对主用户的通信造成干扰或自私地占用频谱资源,此外,协作频谱感知因多个从用户协作而需要更多的时间来检测主用户信号,因而将导致协作频谱感知的性能和效率进一步降低。针对上述问题,提出了基于滑动窗口的协作频谱感知方案,以减轻拜占庭攻击的负面影响,提高协作效率。在深入分析融合中心盲的问题的基础上,从恶意用户的角度出发,建立了一个随机拜占庭攻击模型来描述恶意行为。为了解决感知样本融合过程中的盲的问题,提出了一种交付评估机制,为基于滑动窗口的协作频谱感知奠定了坚实的基础,并在一个滑动窗口内进一步评估信誉值,以提高报告阶段的协作效率。仿真结果表明,无论恶意比例如何,基于滑动窗口的协作频谱感知在始终攻击的情况下只需要 6 个平均样本数就可以提供 100%的检测准确率,而在恶意比例超过 50%的随机攻击的情况下依然能够展现出显著的性能优势。

关键词 协作频谱感知;拜占庭攻击;交付评估机制;基于滑动窗口的权重分配;动态报告方式;序贯概率比检验

中图分类号 TN 929.5 **文章编号** 2097-163X(2024)03-0063-16

文献标志码 A **DOI** 10.12399/j.issn.2097-163x.2024.03.004

Sliding window-based cooperative spectrum sensing against Byzantine attack

SONG Tiecheng[1], WU Jun[2], LIANG Haoyu[2], CHENG Zhixu[1]

(1. School of Information Science and Engineering, Southeast University, Nanjing 210018, China;
2. School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract Cognitive radio (CR) allows secondary users (SUs) to dynamically access the spectrum resources being authorized by the primary user (PU) and improves the spectrum utilization. Cooperative spectrum sensing (CSS) is the key function of CR technology to detect the PU signal by spatial diversity. However, due to the openness of CR networks (CRNs), the CSS process may suffer from Byzantine attack, in which malicious users (MUs) falsify the state information about the PU and then cause the harmful interference to the PU's commu-

收稿日期:2023-06-16 **修回日期**:2023-09-01

通信作者:宋铁成,E-mail:songtc@seu.edu.cn

基金项目:国家自然科学基金资助项目(61771126);江苏省重点研发计划项目(BE2020084-2)

nication or selfishly occupy the spectrum resources. In addition, CSS requires more sensing times to detect the PU signal because of the cooperative paradigm, therefore further decreasing the cooperative performance and efficiency. In view of this, this paper proposed a sliding window-based CSS (SW-CSS) scheme to mitigate the negative impact of Byzantine attack and improve cooperative efficiency. To this end, on basis of in-depth analyses on the blind problem, this paper formulated a random Byzantine attack model from the malicious perspective to characterize the malicious behaviors. In order to solve the blind problem in the process of the sample fusion, this paper proposed a delivery evaluation mechanism to lay a solid foundation for SW-CSS. On the basis of this, this paper further evaluated the trust value (TrV) to improve the cooperative efficiency in the reporting stage. At last, simulation results show that regardless of the malicious ratio, SW-CSS only requires the average number of samples (ANS) 6 to provide with 100% detection accuracy in the presence of always attack while also provides with remarkable performance when the malicious ratio exceeds 50%.

Keywords cooperative spectrum sensing; Byzantine attack; delivery evaluation mechanism; sliding window-based weight allocation; dynamic reporting way; sequential probability ratio test

0 引言

认知无线通信技术在过去 10 年里快速发展，大部分可用的频谱资源已被分配给越来越多的应用设备，从而导致了频谱稀缺。然而，联邦通信委员会的研究表明，大部分频谱资源在时间和空间上都没有得到充分利用[1-2]。传统的静态频谱分配策略明显制约了无线通信的发展。

为了提高频谱利用率，缓解频谱资源稀缺问题，认知无线电技术被提出[3-4]，使得从用户能够动态地接入被分配给主用户的授权信道。由于无线传播的固有特性[5-6]，单个从用户检测到主用户信号不太准确，从而导致主用户状态的判决不准确。因而，协作频谱感知的框架应运而生，它通过利用空间分集实现协作增益，提高频谱感知性能[7-9]。但这种协作方式也为恶意用户发起拜占庭(Byzantine)攻击提供了条件(即恶意用户可能会篡改感知结果，将原本表示主用户的状态篡改成相反的状态，比如将主用户存在的状态篡改为主用户不存在的状态，或将主用户不存在的状态改为主用户存在的状态)。最后将篡改的结果报告给融合中心，破坏融合中心的协作过程[10-12]，对认知无线电网络造成负面影响。

1 相关工作和研究动机

高效协作频谱感知的数据融合设计已经得到了广泛的研究[13]。文献[14]提出了一种基于高阶统计量的频谱感知方法，其中估计了三阶累积量并将其应用于二进制假设性检验，该方法能够在极低信噪比环境下进行频谱感知；文献[15-16]提出并严格分析了认知无线电中的频谱感知方案，该方案基于电平触发采样和非均匀采样技术，该技术自然输出一位信息而不执行任何量化，并允许从用户异步与融合中心通信；文献[17-23]以序贯概率比检验为基础，从不同的角度提高检测器的性能、效率或与网络的适配度；文献[24]提出了一种在信道随时间变化的动态环境中用于协作频谱感知的自适应算法；文献[25]提出了序贯压缩频谱感知调度，该调度联合利用压缩感知和序贯周期检测技术来实现更准确和及时的宽带感知；文献[26]提出了每个认知节点对每个收集的观测向量采用多窗感知方法，并对多窗感知的结果进行截断序贯概率比检验。这些工作从序贯的角度提高了协作频谱感知的性能和效率，但忽略了认知无线电底层协议的开放性而受到拜占庭攻击的威胁问题。为了进一步应对认知无线网络中存在的拜占庭攻击，文献[27-28]提出了加权序贯概率比检验来确保协作频谱感知的鲁棒性；文献[29-31]提出了一系列基于序贯检验的概率拜占庭攻击识别和抑制算法。总体而言，这些方法通过在序贯检验过程中引入信誉机制来实现拜占庭识别。然而，在较长的频谱

感知观察期中，从用户必须实时更新、存储和计算信誉数据，增加了从用户的负担。

鉴于上述问题，文献[32]利用滑动窗口方案来帮助能量检测器在没有噪声影响的情况下估计精确的主用户功率；文献[33]提出了一种异步频谱感知框架，其中每个节点使用滑动窗口算法来分析频谱状态；文献[34]提出了一种用于低信噪比下的滑动窗口方法；文献[35]提出了一种滑动窗口全双工策略，允许在逐个样本的基础上进行判决；文献[36-38]提出了一种基于盖氏圆准则和指数检测器的检测策略，新的测试统计量由每个滑动感知窗口的盖氏圆准则和指数检测器测试统计量的加权形成。尽管这些基于滑动窗口的频谱感知方法有利于实现主用户信号检测的协同效率，但拜占庭攻击问题却被忽视了。与之前的工作不同，文献[39]应用了滑动窗口的异常值检测方案来抑制基于集中融合的认知无线电系统中的恶意用户。为了抵御这种拜占庭攻击，文献[40]提出了一种低复杂度的基于熵的可信度加权协作频谱感知方案，其中每个感知节点的权重是根据滑动窗口期间 2 个连续感知时隙内融合中心接收数据的不一致性来评估的。此外，文献[41]提出了一个基于贝叶斯推理的滑动窗口信任模型，以在没有任何攻击先验信息的情况下识别和剔除独立和协作的概率拜占庭攻击。毫无疑问，滑动窗口信任模型能够减轻从用户可信度的更新、计算和存储负担，但不能提高协作效率和性能，尤其是当恶意用户占多数时。

此外，近几年随着机器学习在通信领域的逐步应用，很多研究人员开始利用机器学习方法来抵抗协作频谱感知中的拜占庭攻击，比如，文献[42]提出了一种基于神经网络的聚类和数据可视化算法即自组织映射；文献[43-45]分别提出了支持向量机来抵抗概率的拜占庭攻击；文献[46-47]对机器学习在协作频谱感知中应用做了广泛的调研。但是机器学习在应对拜占庭攻击时仍然有一定的局限性，比如，需要大量的来自恶意用户的频谱感知数据作为训练序列，以至于协作频谱感知的效率低下，机器学习应对不同攻击策略的通用性不够等。

因此，在拜占庭攻击的情况下，要设计一种准确高效的协作频谱感知来检测主信号的存在与否仍然面临着诸多问题和重大挑战。为此，本文引入了一个随机拜占庭攻击模型来描述恶意频谱行为，并利用序贯检验的优势来提高多个从用户之间的协作效率。此外，本文在交付评估机制的帮助下检查了所有从用户的感知结果的可靠性，并提出了一种基于滑动窗口的权重分配和动态报告方法，以高效可靠地在融合中心做出全局判决。本文的主要贡献可概括为：1）提出了一个随机拜占庭攻击模型，其中恶意用户的攻击行为由一对随机攻击概率来描述。为了解决融合中心盲的问题，提出交付评估机制来检查结果的可靠性，而不是融合中心，目的是准确识别恶意用户；2）为了抑制拜占庭攻击，提出了一种基于滑动窗口的权重分配，并考虑了主用户检测的性能和效率；3）在滑动窗口中，每个从用户的信誉值根据交付评估机制进行分配和更新。考虑到恶意用户伪造的感知结果可能会为融合中心的全局判决传递一些可用信息，本文提出了一种动态报告方式，以进一步提高协作频谱感知在始终攻击策略下的效率。

2　系统模型

为了减轻拜占庭攻击对协作频谱感知的负面影响，本文从恶意用户的角度提出了一个随机攻击模型来描述协作频谱感知过程中的攻击行为。

2.1　本地频谱感知模型

假设 1 个集中式认知无线电网络包括 1 个主用户，N 个从用户，包括诚实用户和恶意用户（恶意用户百分比为 ρ），以及 1 个融合中心，则这种认知无线电网络的周期频谱感知帧由感知时隙、报告时隙和传输时隙组成，在报告时隙后是否跟入传输时隙，取决于全局判决的结果，如图 1 所示。在被允许访问主用户的信道之前，每个从用户需要通过感知时隙处的本地频谱感知技术来检测主用户信号。具体而言，在没有任何主用户信号先验信息的情况下，能量检测是最常用的低复杂度的频谱感知技术[48]。假设 H_0 和 H_1 分别表示主用户的不存在和存在，$h_i(k)$ 表示在第 k 个感知时隙处的第 i 个从用户的信道增益。在具有均值为 0 和方差 σ_u^2 的圆对称复高斯的噪声信号 $n_i(t)$ 下，第 i 个从用户接收机的接收信号可以表示为：

$$y_i(t)=\begin{cases}n_i(t), & \mathrm{H}_0\\ h_i(k)s(t)+n_i(t), & \mathrm{H}_1\end{cases} \tag{1}$$

式中，$s(t)$为主用户的复相移键控信号。假设$s(t)$和$n_i(t)$相互独立，根据能量检测，能量值$r_i(k)$为：

$$r_i(k)=\sum_{t=1}^{M}|y_i(t)|^2=\begin{cases}\sum_{t=1}^{M}|n_i(t)|^2, & \mathrm{H}_0\\ \sum_{t=1}^{M}|h_i(k)s(t)+n_i(t)|^2, & \mathrm{H}_1\end{cases} \tag{2}$$

式中，$M=\tau f_s$是信号采样数，τ是可用的感知时间，接收信号的采样频率为f_s。根据中心极限定理，$r_i(k)$近似为高斯分布，即：

$$r_i(k)\sim\begin{cases}N(M\sigma_u^2,2M\sigma_u^4), & \mathrm{H}_0\\ N(M(\gamma_i+1)\sigma_u^2,2M(\gamma_i+1)^2\sigma_u^4), & \mathrm{H}_1\end{cases} \tag{3}$$

式中，γ_i是第i个从用户测量的主用户的平均信噪比。

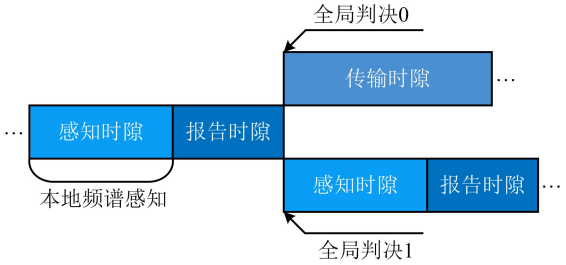


图 1 频谱感知帧结构

Fig. 1 Spectrum sensing frame structure

由于$r_i(k)$遵循高斯分布，用马坎函数$Q(\cdot)$来表示第i个从用户的本地频谱感知性能，即本地虚警概率$P_{\mathrm{f},i}$和本地检测概率$P_{\mathrm{d},i}$。在能量检测阈值为λ的情况下，$P_{\mathrm{f},i}$和$P_{\mathrm{d},i}$可以表示为[49]：

$$P_{\mathrm{f},i}=P(S_i=1\mid\mathrm{H}_0)=Q\left(\left(\frac{\lambda}{\sigma_u^2}-1\right)\sqrt{\tau f_s}\right) \tag{4}$$

$$P_{\mathrm{d},i}=P(S_i=1\mid\mathrm{H}_1)=Q\left(\left(\frac{\lambda}{\sigma_u^2}-\gamma_i-1\right)\sqrt{\frac{\tau f_s}{2\gamma_i+1}}\right) \tag{5}$$

式中，S_i为感知结果。$P_{\mathrm{m},i}=1-P_{\mathrm{d},i}$为本地漏检概率。

2.2 协作频谱感知模型

在本地频谱感知中，每个从用户根据能量检测分别做出关于主用户信号状态的二进制本地感知结果。此外，感知结果通过协作频谱感知中的自由误差控制信道由从用户提交给融合中心，然后融合中心通过特定的融合规则负责全局判决，并决定是否允许从用户接入该信道，如图 2 所示。

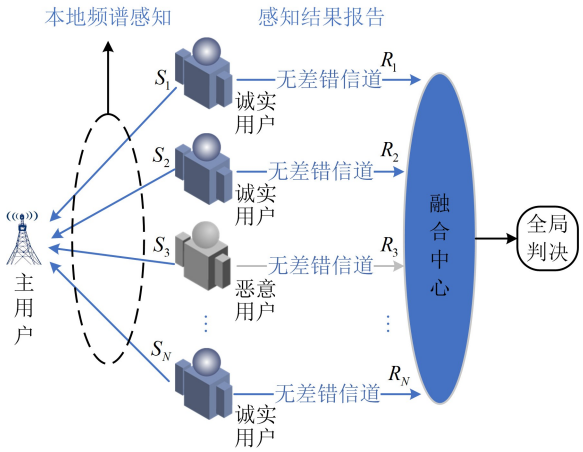


图 2 拜占庭攻击下的协作频谱感知

Fig. 2 CSS in the presence of Byzantine attack

然而，由于认知无线电网络的开放性，协作的方式容易受到恶意用户的影响。恶意用户利用协作机会参与协作频谱感知，然后误导融合中心进行错误的全局判决。在拜占庭攻击过程中，恶意用户会根据感知主用户是否存在的结果，来决定如何向融合中心发送报告。一种情况是：若恶意用户检测到主用户存在，此时感知判决结果为 1，但最终会概率性地向融合中心报告 0，且结果 1 篡改为 0 的概率为β（即攻击概率为β）；另一种情况是：若恶意用户检测到主用户不存在，此时感知判决结果为 0，但最终会概率性地向融合中心报告 1，且结果篡改为 1 的概率为α（即攻击概率α）。鉴于此，拜占庭攻击问题应被重视以实现协同增益和安全[50]。

2.3 拜占庭攻击模型

根据本地频谱感知模型，每个从用户根据本地频谱感知性能生成感知结果。在此基础上，恶意用户可以采取多种攻击策略来实现拜占庭的攻击。目前，认知无线电网络中有 3 种常见的拜占庭攻击类型：1）始终为“否”。恶意用户总是向融合中心提交 0，而不管原始的感知结果如何，从而自私地占用信道；2）始终为“是”。恶意用户无论原始感知结果如何，始终向融合中心提交 1，从而对主用户造成有害干扰；3）始终为“错误”。恶

意用户总是向融合中心提交与原始感知结果相反的感知结果。这种始终攻击的策略容易被许多拜占庭识别算法识别和抑制。

为了提高协作频谱感知进程的安全性，本文提出了一种随机拜占庭攻击模型，其中恶意用户动态调整攻击参数以实现各种攻击策略，如图 3 所示。在恶意用户产生二进制感知结果，即 0 或 1 之后，感知结果可能被篡改。例如，感知结果 0 以概率 α 翻转为 1，而感知结果 1 以概率 β 翻转为 0。换句话说，一对翻转概率 α 和 β 可以被视为攻击概率，于是，拜占庭攻击模型可以被描述为：

$$\begin{cases}\alpha = P(R_i = 1 \mid S_i = 0) \\ \beta = P(R_i = 0 \mid S_i = 1)\end{cases} \tag{6}$$

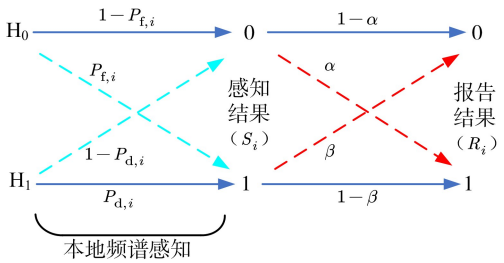


图 3　随机拜占庭攻击模型

Fig. 3　Random Byzantine attack model

遵循上述随机拜占庭攻击模型，恶意用户也能轻易实现始终攻击的策略，即 $(\alpha,\beta)=(0,1)$ 对应于始终“否”攻击，$(\alpha,\beta)=(1,0)$ 对应于始终“是”攻击，$(\alpha,\beta)=(1,1)$ 对应于始终“错误”攻击。此外，恶意用户可以根据自身的安全风险将其攻击概率在 0 与 1 之间随时调整。相较于传统的 3 种始终攻击策略，上述所提出的随机拜占庭攻击策略更加灵活多变（可以演变出各种攻击策略），且向下兼容 3 种始终攻击策略，恶意用户采取该攻击模型，更不易被识别，故而对融合中心所采取的拜占庭防御策略提出了更高的要求和挑战。

根据本地频谱感知的性能和所提出的攻击模型，恶意用户的虚警概率和检测概率可以表示为：

$$\begin{aligned}\widetilde{P}_{\mathrm{f},i} &= P(R_i = 1 \mid \mathrm{H}_0) \\ &= (1 - P_{\mathrm{f},i})\alpha + P_{\mathrm{f},i}(1-\beta)\end{aligned} \tag{7}$$

$$\begin{aligned}\widetilde{P}_{\mathrm{d},i} &= P(R_i = 1 \mid \mathrm{H}_1) \\ &= (1 - P_{\mathrm{d},i})\alpha + P_{\mathrm{d},i}(1-\beta)\end{aligned} \tag{8}$$

其中，漏检概率 $\widetilde{P}_{\mathrm{m},i} = 1 - \widetilde{P}_{\mathrm{d},i}$。

3　问题分析

3.1　盲的问题

恶意用户可通过拜占庭攻击使融合中心完全盲，这意味着融合中心无法通过从用户的感知结果传达准确的主用户状态信息。因此，融合中心处主用户信号的检测性能并不比随机猜测好。换句话说，从贝叶斯的角度来看，报告结果与主用户状态无关。因此，融合中心的盲场景可以描述为：

$$P(\boldsymbol{R} \mid \mathrm{H}_0) = P(\boldsymbol{R} \mid \mathrm{H}_1) \tag{9}$$

式中，$\boldsymbol{R} = [R_1, R_2, \cdots, R_N]$ 是报告结果向量。

假设每个从用户的虚警概率和漏检概率是相同的，也即 P_{f} 和 P_{m}（$P_{\mathrm{f},i} = P_{\mathrm{f}}$ 且 $P_{\mathrm{m},i} = P_{\mathrm{m}}$）。当每个恶意用户采用相同的攻击概率 α 和 β 时，式(9)的盲的条件可以进一步表示为：

$$\begin{aligned}&\rho(\alpha(P_{\mathrm{f}} + P_{\mathrm{m}} - 1) + (1-\beta)(1 - P_{\mathrm{f}} - P_{\mathrm{m}})) \\ &\quad + (1-\rho)(1 - P_{\mathrm{f}} - P_{\mathrm{m}}) = 0\end{aligned} \tag{10}$$

因此，根据式(10)可得：

$$\rho = \frac{1}{\alpha + \beta} \tag{11}$$

根据上述结果，可以得出结论，恶意用户比例 $\rho \geqslant 1/(\alpha+\beta)$ 是恶意用户使融合中心盲的关键条件，即当恶意用户采用始终“错误”攻击时，$\rho = 50\%$ 可以使 $(\alpha,\beta)=(1,1)$。此时，在融合中心处对主用户信号的检测性能并不比随机猜测好。

3.2　多数准则

在拜占庭攻击面前，有 2 种类型的数据融合规则可以在融合中心上做出全局判决，即判决规则和假设性检验。多数规则是最具代表性的判决规则之一，例如，当报告结果 1 的数量超过报告结果总数的 1/2 时，融合中心接受 H_1，否则接受 H_0。也就是说，在多数规则中，融合中心需要收集所有从用户的报告结果，但不具有拜占庭防御能力（只有融合中心在恶意比例较低时有效）。

3.3　加权序贯概率比检验

与多数规则或其他融合规则相比，一系列假设性检验需要先验信息，但序贯概率比检验和贝叶斯检测除了加权序贯概率比检验之外也不具备拜占庭防御能力。本节简要介绍一个经典的加权序贯概率比检验，以展示协作频谱感知的性能和效率，包括序贯似然比计算和权重分配，其

中序贯是一种数据融合规则的方式，如图 4 所示。相较于普通投票准则（多数准则），序贯准则不需要依靠全部的报告样本来做出最终的全局判决。从用户按照顺序向融合中心发送感知报告，融合中心序贯地接收这些报告，一旦报告中的信息达到预设的阈值，融合中心便会中断这次数据融合，立即做出全局判决，这便是序贯准则。由于不需要全部的从用户发送报告来进行数据融合，序贯准则可以有效地减少从用户报告数量，可以实现更高效的协作频谱感知。

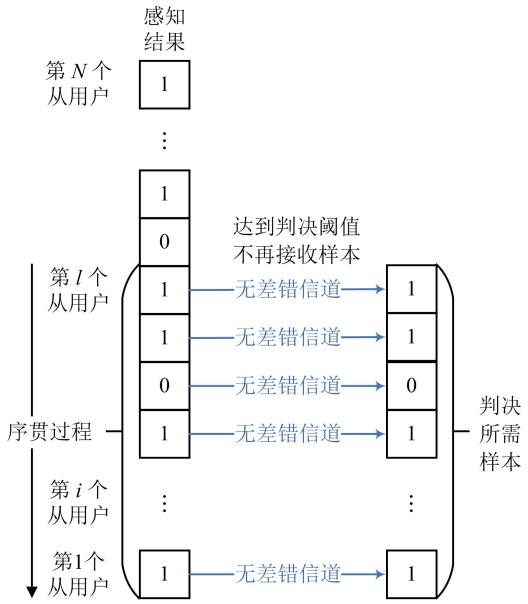


图 4 广义序贯过程

Fig. 4 Generalized sequential process

为了提高协作频谱感知的效率，通常采用序贯的思想进行感知数据融合。报告结果按序贯计算为序贯概率比检验中的似然比，一旦满足判决条件，则终止序贯过程。例如，在第 k 个感知时隙的似然比计算可以被描述为：

$$\begin{aligned} L_l(k) &= \prod_{i=1}^{l}\left(\frac{P(R_i(k)\mid \mathrm{H}_1)}{P(R_i(k)\mid \mathrm{H}_0)}\right) \\ &= \prod_{i=1}^{l}\left(\left[\frac{P(R_i(k)=1\mid \mathrm{H}_1)}{P(R_i(k)=1\mid \mathrm{H}_0)}\right]^{R_i(k)}\right. \\ &\quad \left.\cdot\left[\frac{P(R_i(k)=0\mid \mathrm{H}_1)}{P(R_i(k)=0\mid \mathrm{H}_0)}\right]^{1-R_i(k)}\right) \end{aligned} \tag{12}$$

式中，$l\in(0,N]$ 是融合中心做出全局判决所需的样本数，$R_i(k)$ 是第 i 个从用户在第 k 个感知时隙的报告结果。来自从用户的报告结果被计算为融合中心处累积的似然比，直到融合中心根据一对判决阈值 λ_{U} 和 λ_{L} 对主用户状态做出全局判决。然后，判决过程可以表示为：

$$\begin{cases} L_l(k)\geqslant\lambda_{\mathrm{U}}, & \text{接受 } \mathrm{H}_1 \\ L_l(k)\leqslant\lambda_{\mathrm{L}}, & \text{接受 } \mathrm{H}_0 \\ \lambda_{\mathrm{L}}<L_l(k)<\lambda_{\mathrm{U}}, & \text{采用下一个采样} \end{cases} \tag{13}$$

式中，下判决阈值 λ_{L} 和上判决阈值 λ_{U} 的计算公式为：

$$\lambda_{\mathrm{L}}=\frac{1-\overline{P}_{\mathrm{f}}}{\overline{P}_{\mathrm{m}}},\lambda_{\mathrm{U}}=\frac{\overline{P}_{\mathrm{f}}}{1-\overline{P}_{\mathrm{m}}} \tag{14}$$

式中，$\overline{P}_{\mathrm{f}}$ 是可容忍虚警概率，而 $\overline{P}_{\mathrm{m}}$ 表示可容忍漏检概率。

尽管序贯概率比检验有利于协作频谱感知显著减少平均样本数，但在面临拜占庭攻击时，其性能并不令人满意。

由于序贯概率比检验的序贯过程是随机的，拜占庭的识别和抑制不能通过似然比来实现。因此，基于信誉值的权重分配被集成到似然比计算中。为此，根据融合中心的全局判决与报告结果之间的一致性，为每个从用户分配一个信誉值。在第 k 个感知时隙之后，第 i 个从用户的信誉值表示为：

$$T_i(k)=T_i(k-1)+(-1)^{R_i(k)+d(k)} \tag{15}$$

式中，$d(k)$ 表示融合中心的全局判决。随后，第 i 个从用户与其信誉值相关的权重可以表示为：

$$w_i(k)=\begin{cases} 0, & T_i(k)\leqslant -g \\ \dfrac{T_i(k)+g}{\max\ T(k)+g}, & T_i(k)>-g \end{cases} \tag{16}$$

式中，$T(k)$ 表示在第 k 个感知时隙处的所有从用户的信誉值的集合，且 $g=5$。当权重被引入似然比计算中时，可得：

$$L_l(k)=\prod_{i=1}^{l}\left(\frac{P(R_i(k)\mid \mathrm{H}_1)}{P(R_i(k)\mid \mathrm{H}_0)}\right)^{w_i(k)} \tag{17}$$

最后，融合中心对第 $k+1$ 个感知时隙处的主用户状态做出全局决定（假设每个从用户的权重在第 1 个感知隙处为 1）。

4 基于滑动窗口的协作频谱感知

通过对加权序贯概率比检验的简单介绍，可以很容易地解决上述始终攻击策略。然而，关于协作频谱感知的性能和效率仍有许多问题需要解决，特别是在随机拜占庭攻击的情况下。首先，拜占庭攻击可能使融合中心盲，因为除了始终“错误”攻击之外，恶意用户仍可以通过适当的

攻击参数满足盲的条件($\rho \geqslant 1/(\alpha+\beta)$)。一旦拜占庭攻击使融合中心盲，式(15)的信誉值更新机制将错误识别恶意用户，从而破坏感知过程；其次，在融合中心通过特定的融合规则识别出恶意用户，将立即删除恶意用户。这种武断的方式对于被误认为是恶意用户的诚实用户来说显然是极端的，不利于鼓励恶意用户恢复正常的频谱感知行为。事实上，在深入分析拜占庭攻击的特点后，融合中心可以从恶意用户的报告结果中挖掘出有利于做出准确全局判决的感知信息；最后，除了协作频谱感知性能外，还应考虑协作频谱感知效率，因为在大型认知无线电网络中，协作的通信开销往往很大。序贯概率比检验的序贯优势可以减少样本数，但其随机性或拜占庭攻击的负面影响使样本数不确定。基于以上分析，本文提出基于滑动窗口的协作频谱感知策略，以提高协作频谱感知抵御拜占庭随机攻击的性能和效率，具体包括交付评估机制、基于滑动窗口的权重分配和动态报告方式。完整的基于滑动窗口的协作频谱感知融合规则如图 5 所示。

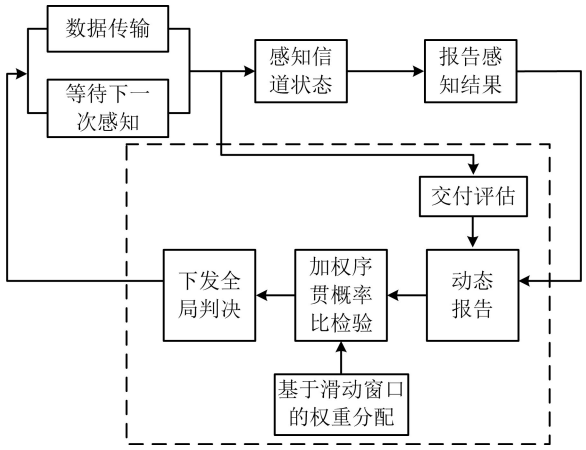


图 5　基于滑动窗口的协作频谱感知框图

Fig. 5　Block diagram of SW-CSS

4.1　交付评估机制

融合中心的全局判决通常用于评估每个从用户的信誉值，并生成权重，为感知信息融合做准备。如前所述，信誉值评估总是受到盲的问题的影响，鉴于此，可靠的信誉值评估机制变得至关重要，因此，本节通过观察信道中的数据传输状态来确定全局判决的正确性，并利用该消息来评估从用户报告结果的正确性。众所周知，关于主用户的状态有 4 种情况，如图 6 所示。根据接收到的报告结果，一方面，当融合中心的全局判决为 0 时，则允许从用户根据全局判决 0 接入信道以正常发送数据，如果全局判决为真，则不会对主用户造成干扰；如果全局判决为假，即主用户仍在使用该信道，则毫无疑问，从用户接入该信道后，对主用户的网络存在过度干扰或主用户/从用户数据传输失败；另一方面，当融合中心的全局判决为 1 时，则根据全局判决 1 禁止所有从用户接入信道，如果全局判决为真，则从用户需要继续频谱感知；如果全局判决为假，则存在自私地占用信道的恶意用户，而主用户不使用该信道。

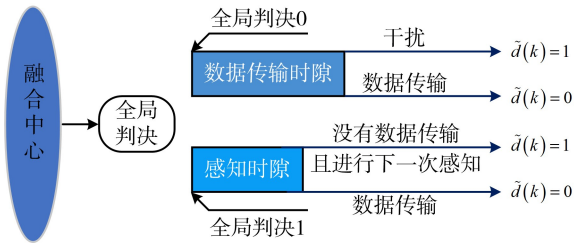


图 6　交付评估机制

Fig. 6　Delivery evaluation mechanism

根据上述频谱感知过程，融合中心可以在做出全局判决后通过观察信道中的数据传输情况来确定全局判决是否正确，因为全局判决可能会被恶意用户篡改。因此，从用户的信誉值可以根据交付评估机制进行更新为：

$$T_i(k)=T_i(k-1)+(-1)^{R_i(k)+\tilde{d}(k)} \tag{18}$$

式中，$\tilde{d}(k)$是根据第 k 个频谱感知帧结束后交付评估机制的信道状态。

由于融合中心需要通过可靠的标准检验来自从用户的本地判决的可靠性，所以这个检验的标准必须非常可靠且不受恶意用户的数量和攻击策略的影响。由于很多研究常常采用全局判决作为这一标准来检验本地判决的可靠性，一旦全局判决不再可靠(比如盲的问题)，此时依旧将其作为检验标准，并作为更新从用户信誉值甚至权重的依据，则会出现恶意用户误判的情况。相较之下，本文所提出的交付评估机制并不依赖于全局判决，而是在全局判决结束后，融合中心通过观察信道中数据传输情况，来检查全局判决的正确与否，这种方式不受拜占庭攻击的影响，进而为信誉值的更新和下一频谱感知帧的权重提供可靠的保障。

4.2　基于滑动窗口的权重分配

融合中心通常使用历史报告结果的一致性

来评估当前报告结果的可靠性。随着感知次数的增加和时间的推移，过去时间较长的报告结果对当前感知时隙的信誉值或权重计算的价值越来越低。更重要的是，恶意用户可以利用长的感知观察期来提高自身的隐蔽性，这不利于对恶意用户的鉴别。然而，一定的感知观察期将鼓励理性的恶意用户恢复正常的频谱感知行为。因此，本节提出了一种基于滑动窗口的权重分配。

如图 7 所示，在每一次频谱感知帧结束后，融合中心仅考察某个用户在滑动窗口内每个从用户报告结果的一致性，以计算信誉值和权重。通过滑动窗口，最大信誉值被作为设计权重分配的标准，第 i 个从用户的权重可以表示为：

$$w_{i,W}(k)=\frac{T_{i,W}(k)}{\max\ T_W(k)} \tag{19}$$

式中，$T_{i,W}(k)$是滑动窗口内的第 i 个从用户的信誉值，$T_W(k)$是滑动窗口内所有从用户信誉值的集合。需要注意的是，在计算权重的过程中，如果 $k\leqslant W$，则 $T_{i,W}(k)=T_i(k)$；如果 $k>W$，则 $T_{i,W}(k)=T_i(k)-T_i(k-W)$。

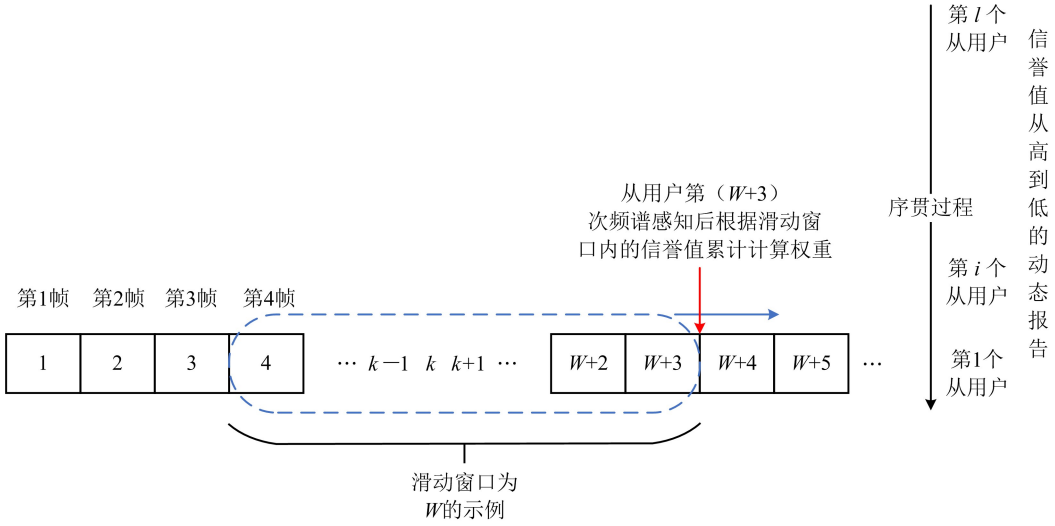


图 7 基于滑动窗口的权重分配

Fig. 7 Sliding window-based weight allocation

有交付评估机制的保障，诚实用户能够被准确地赋予更高的信誉值，同时恶意用户也被准确地赋予更低的信誉值，结合式(19)的权重分配，来自诚实用户的可靠感知结果能够被分配更高的权重，在序贯检验的过程中能够对全局判决发挥更积极的作用。换言之，诚实用户的感知结果很容易快速满足序贯检验的判决条件，在这种情况下，即便恶意用户有一定的信誉值和其感知结果有一定的权重(攻击概率较小时)，但没有机会参与协作频谱感知。但值得一提的是，一个过大或过小的滑动窗口都不利于协作频谱感知。一方面，大的滑动窗口不仅使频谱感知效率降低，而且有利于恶意用户的隐藏；另一方面，由于无线传播的影响，小的滑动窗口将增加诚实用户被识别为恶意用户的可能性。因此，合适的滑动窗口才能满足认知无线电网络的要求。

4.3 动态报告方式

在将滑动窗口应用于权重分配以提高感知观察期中的协作效率之后，接下来要考虑的是融合中心如何在每个感知时隙实现从用户之间的高效协作。在传统的序贯检验(即序贯概率比检验、加权序贯概率比检验等)中，每个从用户序贯随机地向融合中心报告自己的感知结果，并将其计算为累积的似然比。然而，这种报告方式容易受到拜占庭攻击的影响，因为即便是恶意用户信誉值低，其感知结果的权重也比较低，但有可能先于诚实用户被计算到序贯检验中。如此一来，恶意用户依然对协作频谱感知有一定的负面影响，而且样本数也不可控。因此，设计一种新的报告方式来保证协作频谱感知的效率变得至关重要。

动态报告方式将报告结果的信誉值进行排序来从高到低地计算其似然比。由于序贯融合准则对报告的顺序非常敏感，而本文提出的对报告按照信誉值动态排序的方法，可以有效地将可靠报告放在靠前的位置进行数据融合。由于信

誉值是随着感知时隙前进实时更新，所以每次数据融合前都会进行一次排序。下面对动态报告方式进行详细说明。

在滑动窗口内，从用户表现出信誉值的差异，在似然比累积的计算过程中，具有高信誉值的从用户的报告结果将被优先进行计算似然比。也就是说，按照信誉值降序，报告结果依次通过个体权重累积的似然比进行计算，直到融合中心根据 λ_{L} 和 λ_{U} 做出全局判决。在融合中心做出全局判决后，融合中心不需要其他报告结果。这种信誉值优先报告方法确保了可靠的报告结果，在全局判决中发挥积极作用。更重要的是，原本诚实用户的可靠感知结果通过较大的权重就能够发挥更大作用，相较于随机报告方式，信誉值优先的方式，进一步保证了可靠感知结果优先权，加速全局判决的完成，降低信誉度的从用户甚至恶意用户的负面影响。

综上所述，本节提出的基于滑动窗口的协作频谱感知策略的整个过程由交付评估机制、基于滑动窗口的权重分配和动态报告方式组成，如算法 1 所示。

算法 1　基于滑动窗口的协作频谱感知

1. 初始化 $T_i(1)=0$，$w_{i,W}(1)=1$，$i=1,\cdots,N$
2. for k to 感知次数 do
3. if $k\leqslant W$ then
4. 按降序对所有从用户的信誉值进行排序
5. 根据信誉值对从用户的报告结果进行降序排序
6. $L_l(k)=1$
7. for $i=1$ to N do
8. if $R_i(k)=1$ or 0 then
9. 权重分配 $w_{i,W}(k)$通过式(19)算出
10. 更新

$$L_l(k)=L_l(k)\cdot\left(\frac{P(R_i(k)\mid \mathrm{H}_1)}{P(R_i(k)\mid \mathrm{H}_0)}\right)^{w_{i,W}(k)}$$

$$=L_l(k)\cdot\left[\frac{P(R_i(k)=1\mid \mathrm{H}_1)}{P(R_i(k)=1\mid \mathrm{H}_0)}\right]^{R_i(k)w_{i,W}(k)}\cdot\left[\frac{P(R_i(k)=0\mid \mathrm{H}_1)}{P(R_i(k)=0\mid \mathrm{H}_0)}\right]^{(1-R_i(k))w_{i,W}(k)}$$

11. end if
12. if $L_l(k)\geqslant\lambda_{\mathrm{U}}$ then
13. 接受 H_1，break
14. else if $L_l(k)\leqslant\lambda_{\mathrm{L}}$ then
15. 接受 H_0，break
16. else
17. continue
18. end if
19. end for
20. else
21. 从 k 到 $k-W$ 计算权重 $w_{i,W}(k)$，其他过程与情况 $k\leqslant W$ 相同
22. end if
23. 根据交付评估机制更新 $T_i(k)=T_i(k-1)+(-1)^{R_i(k)+\delta(k)}$
24. 更新权重分配 $w_{i,W}(k+1)$
25. end for

5　仿真结果

本节对多数规则、贝叶斯检测、序贯概率比检验、加权序贯概率比检验和本文提出的基于滑动窗口的协作频谱感知策略的协作频谱感知性能和效率进行了比较和分析。为此，通过全局错误概率和平均样本数来评估协作频谱感知的性能和效率，其中全局错误概率为：

$$Q_{\mathrm{e}}=P_{\mathrm{H}_0}Q_{\mathrm{f}}+P_{\mathrm{H}_1}Q_{\mathrm{m}} \tag{20}$$

式中，P_{H_0} 和 P_{H_1} 分别是 H_0 和 H_1 的概率，Q_{f} 和 Q_{m} 分别是全局虚警概率和漏检测概率，平均样本数是融合中心在感知观察期（2×10^4 个帧）内做出全局判决所需的平均样本量。为了建立一个公平的仿真环境，在考虑平均样本数时，我们只对序贯概率比检验、加权序贯概率比检验和基于滑动窗口的协作频谱感知 3 种数据融合规则进行比较，因为多数准则和贝叶斯检测都是全样本融合规则，需要所有从用户的判决样本数，即参与协作频谱感知的从用户数量 N。

仿真参数设置如下：参与协作频谱感知的从用户数量 N 为 100。此外，假设主用户存在的概率 $P_{\mathrm{H}_1}=0.3$，不存在的概率 $P_{\mathrm{H}_0}=0.7$[49]。可容忍的虚警概率 $\overline{P}_{\mathrm{f}}$ 和漏检概率 $\overline{P}_{\mathrm{m}}$ 分别设置为 10^{-3} 和 10^{-4}[51-52]。恶意比例 ρ 在(0～90)%之间变化，假设每个帧持续时间为 100 ms，贝叶斯检测阈值 λ_{Bayes} 为 2.3[51]，其中虚警成本和漏检成本为 1，正确检测成本则均为 0。通过多次实验，滑动窗口的大小设置为 50，更加准确的滑动窗口大小还需要结合网络环境（比如主用户的活动状态）和拜占庭攻击策略进一步分析和研究。

5.1　始终攻击

由于始终攻击是协作频谱感知中经常考虑的攻击策略，因此当假设本地检测概率 P_{d} 和本地虚警概率 P_{f} 分别为 0.9 和 0.1 时，错误概率和平均样本数如图 8～9 所示。

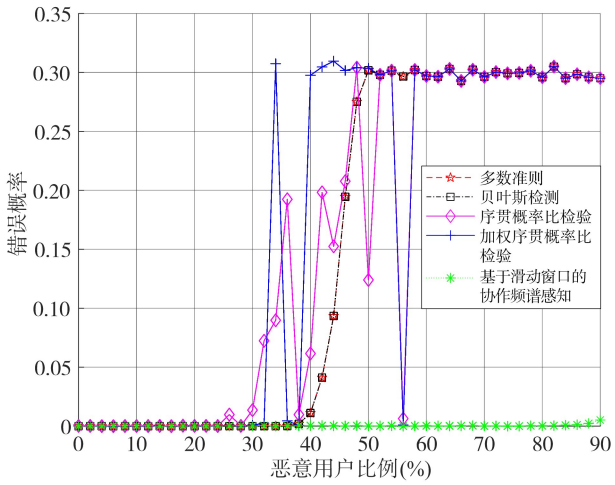


图 8 始终“否”攻击下基于滑动窗口的协作频谱感知策略与其他融合策略的错误概率

Fig. 8 The error probability of SW-CSS and other fusion rules in the presence of AN attack

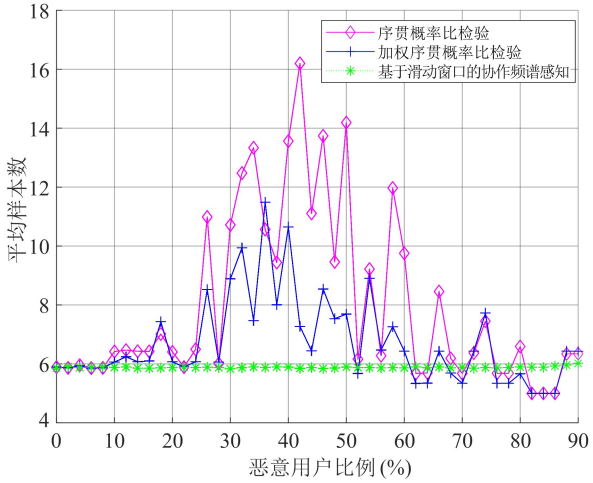


图 9 始终“否”攻击下基于滑动窗口的协作频谱感知策略与其他融合策略的平均样本数

Fig. 9 ANS of SW-CSS and other fusion rules in the presence of AN attack

如图 8 所示，当恶意用户比例小于 30%时，协作频谱感知的所有数据融合规则都能提供显著的主用户信号检测准确率，这是因为恶意用户较少时，其负面影响对于协作系统来说较小，融合中心依然能做出准确的全局判决。但随着恶意用户比例的增加，序贯概率比检验的错误概率开始抖动式增加，然后加权序贯概率比检验的错误概率也剧烈抖动和增加。与序贯概率比检验和加权序贯概率比检验相比，多数规则和贝叶斯检测的错误概率直到恶意比例大于 40%才开始增大，并且由于它们是全样本的融合规则，所以即使是性能开始下降，也恶化的较为平滑。显然，不同于多数规则和贝叶斯检测，在拜占庭攻击的随机性和似然比计算的共同影响下，序贯概率比检验和加权序贯概率比检验的错误概率波动很大，由于是非全样本的序贯方式，序贯概率比检验和加权序贯概率比检验在接受下一个判决样本时并不能确定是来自恶意用户还是诚实用户，以至于其恶化的性能无法跟多数规则和贝叶斯检测一样平滑。但加权序贯概率比检验通过降低恶意用户的判决权重，在一定程度上抑制了始终“否”攻击。当恶意用户呈现大多数时，除了本文提出的基于滑动窗口的协作频谱感知策略能够提供几乎 100%准确性之外，其他 4 种融合规则在始终“否”攻击下的错误概率保持在 0.3。这是因为在大规模始终“否”攻击的情况下，恶意用户总是对融合中心宣称主用户不存在，以至于漏检概率为 0，虚警概率则为 1，考虑主用户存在的概率为 0.3。根据式(20)可知，最终这 4 种融合规则的错误概率保持在 0.3。

同时，在始终“否”攻击的情况下，图 9 说明了 3 种融合规则(序贯概率比检验、加权序贯概率比检验和基于滑动窗口的协作频谱感知)的平均样本数。可以看出，序贯概率比检验和加权序贯概率比检验的平均样本数都是先抖动式增加后抖动式减少，并且序贯概率比检验所需的样本总是多于加权序贯概率比检验所需的样本(由于加权序贯概率比检验将每个从用户的信誉值集成到似然比中，在恶意用户比较低时，能一定程度上抑制拜占庭攻击，可以尽可能接受诚实用户的判决样本，因此使融合中心能够比序贯概率比检验更快、更准确地做出全局判决)。毫无疑问，序贯概率比检验对于拜占庭攻击没有任何抵抗能力(恶意用户较少时可以保证性能，但这不是本身的优势或特点所带来的，其他融合规则也可以)，一旦恶意用户逐渐增多，不仅性能受影响，且因无法立即做出全局判决，所需要的样本也增多。显然，序贯概率比检验和加权序贯概率比检验下的全局判决并没有完全被影响，但在拜占庭攻击的情况下，融合中心需要更多的样本来做出全局判决。一旦全局判决完全翻转，随着恶意用户的增加，融合中心就不需要更多的样本。相比之下，基于滑动窗口的协作频谱感知策略从始至终只需要 6 个样本便能够提供稳定而显著的检测性能。

与始终“否”攻击的仿真结果类似，始终“是”攻击的仿真效果如图 10 和图 11 所示。无论是错误概率还是平均样本数，在始终“是”攻击下，几种融合规则与始终“否”有相似的特征。当恶意用户占多数时，除了基于滑动窗口的协作频谱感知策略之外，其他 4 个融合规则在始终“是”攻击下的错误概率保持在 0.7，这是因为在大规模始终“是”攻击的情况下，恶意用户总是对融合中心宣称主用户存在，以至于漏检概率为 1，虚警概率则为 0，考虑主用户存在的概率为 0.3。根据式(20)可知，最终这 4 种融合规则的错误概率保持在 0.7。基于滑动窗口的协作频谱感知策略仍然只需要 6 个样本，就可以提供稳定而显著的检测性能。总之，始终“是”攻击的仿真结果再次证实了所提出的基于滑动窗口的协作频谱感知策略的高性能和高效性。

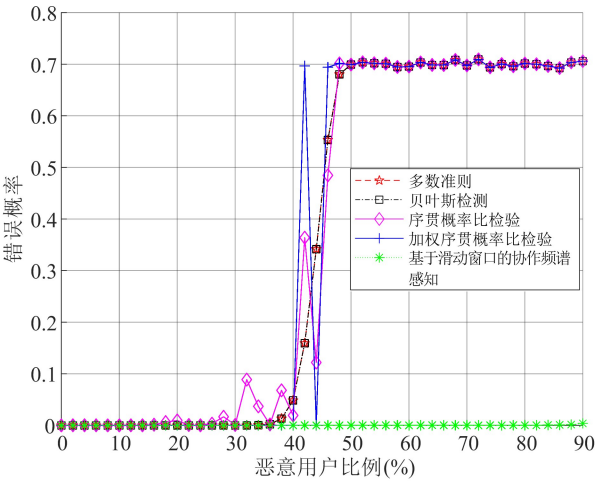


图 10　始终“是”攻击下基于滑动窗口的协作频谱感知策略与其他融合规则的错误概率

Fig. 10　The error probability of SW-CSS and other fusion rules in the presence AY attack

与独立的始终“否”和“是”攻击相比，始终“错误”攻击对协作频谱感知的负面影响更大，因为无论恶意比例如何，始终“是”和始终“否”攻击都不能使融合中心盲。因此在图 12 和 13 中展示了在始终“错误”攻击的情况下几种融合规则的错误概率和平均样本数。与始终“是”和“否”攻击不同，当恶意比例 $\rho \geqslant 50\%$ 时，除基于滑动窗口的协作频谱感知外，其他 4 种融合规则的错误概率均为 50%，而序贯概率比检验和加权序贯概率比检验的平均样本数也最大。毫无疑问，融合中心此时是盲的，其错误概率也随着恶意用户比例的进一步增加而降低，直至 100%。

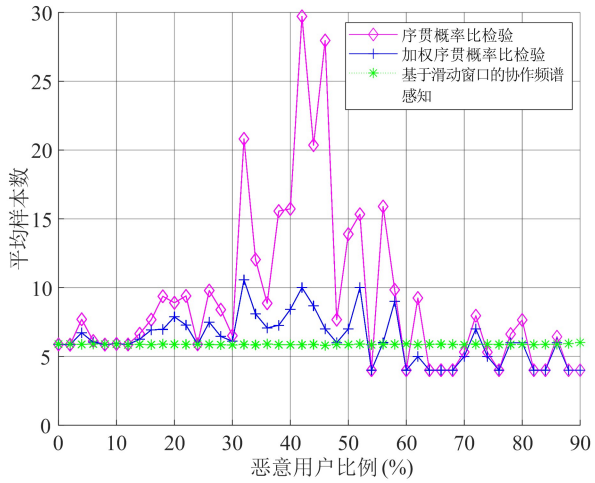


图 11　始终“是”攻击下基于滑动窗口的协作频谱感知策略与其他融合规则的平均样本数

Fig. 11　ANS of SW-CSS and other fusion rules in the presence AY attack

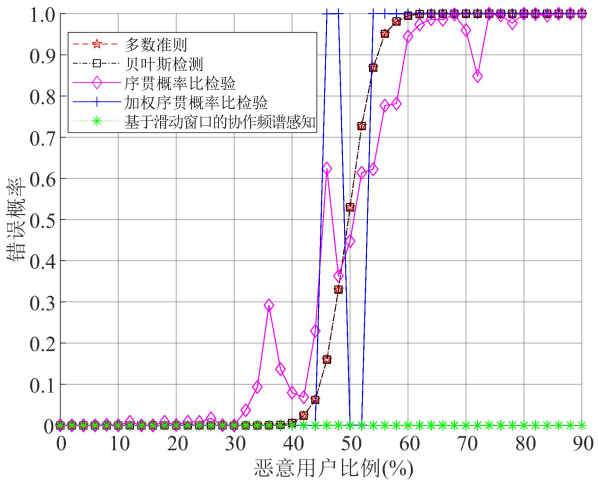


图 12　始终“错误”攻击下基于滑动窗口的协作频谱感知策略与其他融合规则的错误概率

Fig. 12　The error probability of SW-CSS and other fusion rules in the presence of AF attack

从以上结果可以看出，对拜占庭攻击没有抵抗能力的融合规则(如多数准则、贝叶斯准则和序贯概率比检验)，在恶意用户比例较小的情况下，也能够保证可观的协作频谱感知性能，少量的被篡改的频谱感知数据可以被协作系统所淹没。而当恶意用户比例进一步增加时，具备一定抵抗能力的加权序贯概率比检验能保证一定的性能和效率，对于始终攻击也能做出识别，比如 3 种始终攻击策略下的恶意比例较小时，可见始终攻击是一种容易识别的攻击策略，这种性能和效率完全依赖融合中心所做出的全局判决的可

靠性，因为需要全局判决去衡量本地感知结果的可靠性。但一旦恶意比例超过 50%，如在始终“错误”攻击下，它仍然会对错误概率和平均样本数产生显著影响，因为融合中心的全局判决不再可靠了，在全局判决来衡量本地感知结果的基础上，任何权重分配方案和报告方式都无法保证协作频谱感知的性能和效率。而本文提出的协作频谱感知方案在交付评估机制的影响下，很容易识别此类攻击策略，更重要的是，它还解决了盲的问题（比如在始终“错误”攻击下恶意用户比例超过 50%）。因为交付评估机制有别于传统的本地感知结果的评估机制，独立于全局判决。当一个频谱感知帧结束后，交付评估机制只需要根据融合中心监测信道中的数据传输情况，来后验地（因为传统的评估机制只需要融合中心做出全局判决后，就能立即评估从用户感知结果的可靠性，为下一次从用户的感知分配权重）确认本次全局判决是否可靠，利用此信息就能准确地判定本地感知结果是否准确，进而计算滑动窗口内的权重分配。在此基础上，借助动态的报告方式，在序贯的过程中，信誉值高的从用户可以优先计算（如似然比计算），进一步实现了主用户信号的快速检测，提高协作频谱感知的效率。

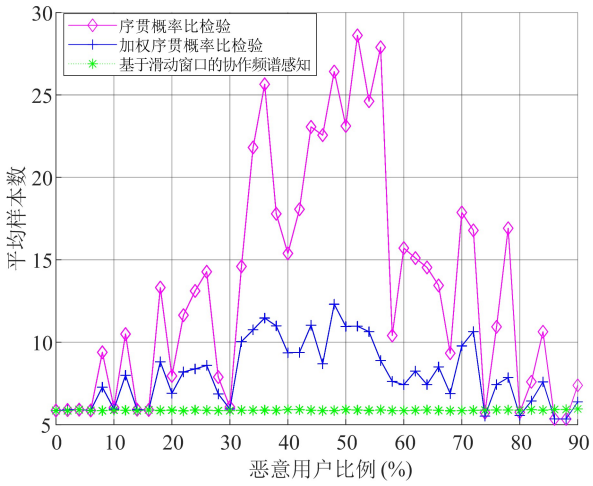


图 13 始终“错误”攻击下基于滑动窗口的协作频谱感知策略与其他融合规则的平均样本数

Fig. 13 ANS of SW-CSS and other fusion rules in the presence of AF attack

5.2 随机攻击

前一小节验证了所提策略在错误概率和平均样本数方面的优越性，这表明所提出的策略的高性能和高效率。与始终攻击相比，随机攻击对协作频谱感知的影响较小，但也更难被识别和抑制。接下来，仿真在随机攻击下进一步考虑了 5 种融合规则的错误概率和平均样本数。为此，假设攻击概率(α,β)分别为$(0.5,0.5)$和$(0.8,0.8)$。

图 14 和图 15 分别显示了$(\alpha,\beta)=(0.5,0.5)$时的错误概率和平均样本数。在这种情况下，除非恶意用户比例为 100%，否则拜占庭攻击不会使融合中心盲。因此，从图 14 中可以观察到，在恶意用户百分比超过 20%后，尽管攻击概率很小，但是融合中心序贯的接受恶意用户的判决样本是随机的，由于没有权重分配方案的抑制作用且并非全样本规则，导致序贯概率比检验的错误概率抖动。在恶意用户比例超过 70%后，多数规则和贝叶斯检测都开始下降，显然较低的攻击概率可以容忍更多的恶意用户，而加权序贯概率比检验和基于滑动窗口的协作频谱感知策略在恶意用户比例超出 86%后才开始下降，可见这种无法使融合中心盲且适度的攻击，加权序贯概率比检验也能抵抗，因为融合中心的全局判决依旧可以保持准则，基于滑动窗口的协作频谱感知策略亦然。

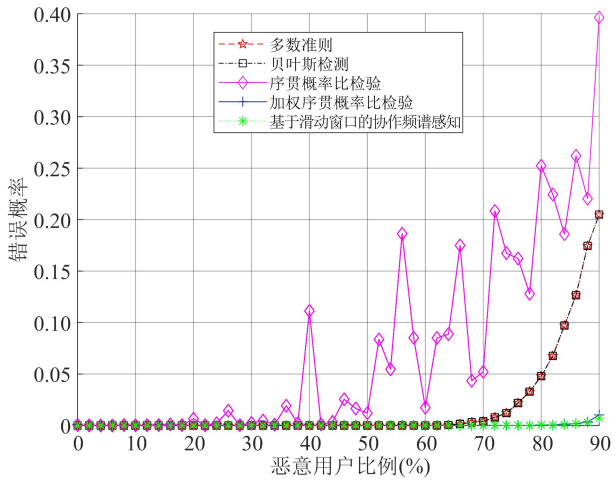


图 14 随机攻击$(\alpha,\beta)=(0.5,0.5)$下基于滑动窗口的协作频谱感知策略与其他融合规则的错误概率

Fig. 14 The error probability of SW-CSS and other fusion abilityofrules in the presence of random attack$(\alpha,\beta)=(0.5,0.5)$

随机攻击$(\alpha,\beta)=(0.5,0.5)$下的样本数量如图 15 所示。在此攻击策略下的样本数量有别于此前始终攻击，在恶意比例小于 50%时，序贯概率比检验和加权序贯概率比检验的样本数小幅抖动增加，加上攻击概率相对较小的因素叠

加，所以拜占庭攻击对于序贯概率比检验和加权序贯概率比检验的负面影响较小。但是随着恶意用户进一步增多，它们的样本数也进一步抖动，且加权序贯概率比检验抖动更大。很明显，增加的恶意用户已经使得序贯概率比检验的错误概率恶化更严重，因而并不需要样本数来满足似然比上下阈值的判决条件，而加权序贯概率比检验恶意错误概率依然很低，但是在拜占庭攻击的影响下，需要更多样本数量来满足似然比上下阈值的判决条件，提供相对准确的检测。

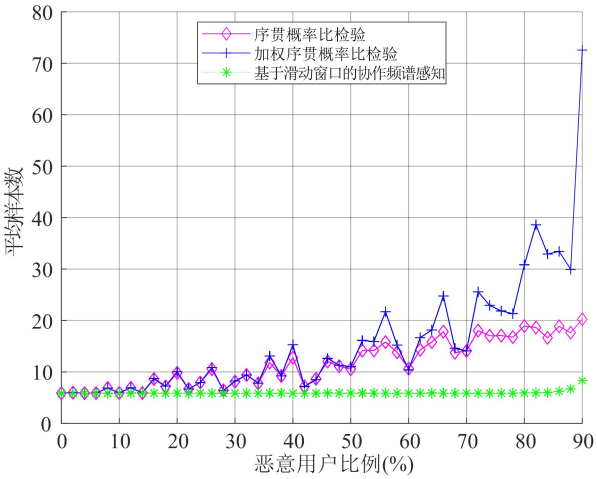


图 15　随机攻击$(\alpha,\beta)=(0.5,0.5)$下基于滑动窗口的协作频谱感知策略与其他融合规则的样本数

Fig. 15　ANS of SW-CSS and other fusion rules in the presence of random attack $(\alpha,\beta)=(0.5,0.5)$

与$(\alpha,\beta)=(0.5,0.5)$的仿真结果不同，图 16 和图 17 中在$(\alpha,\beta)=(0.8,0.8)$下关于错误概率和平均样本数的仿真结果与始终“错误”攻击更相似。$(\alpha,\beta)=(0.8,0.8)$和$(\alpha,\beta)=(0.5,0.5)$之间的最大差异是抖动中心（误差概率接近50%，而此时平均样本数的抖动最大）从$\rho=50\%$移动到$\rho=60\%$左右。其结果满足$\rho\geqslant 1/(\alpha+\beta)$，这会导致此时误差概率和平均样本数的急剧增加。

总之，无论是始终攻击还是随机攻击，交付评估机制都可以为协作频谱感知系统提供本地感知信息的稳健度量，并为高性能提供强大的保证。基于滑动窗口的权重分配和动态报告方式促使融合中心快速做出准确的判决。具体来说，在频谱感知观察期，适当的滑动窗口不仅可以抵抗潜在的恶意用户（如果在没有滑动窗口限制的情况下，恶意用户会有更多的活动空间，例如，可以动态调整攻击策略以确保一定水平的信誉值），还可以减少本地存储的负担。

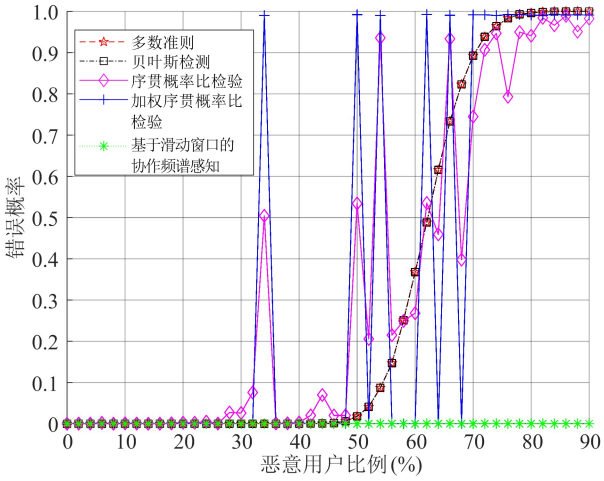


图 16　随机攻击$(\alpha,\beta)=(0.8,0.8)$下基于滑动窗口的协作频谱感知策略与其他融合规则的错误概率

Fig. 16　The error probability of SW-CSS and other fusion rules in the presence of random attack $(\alpha,\beta)=(0.8,0.8)$

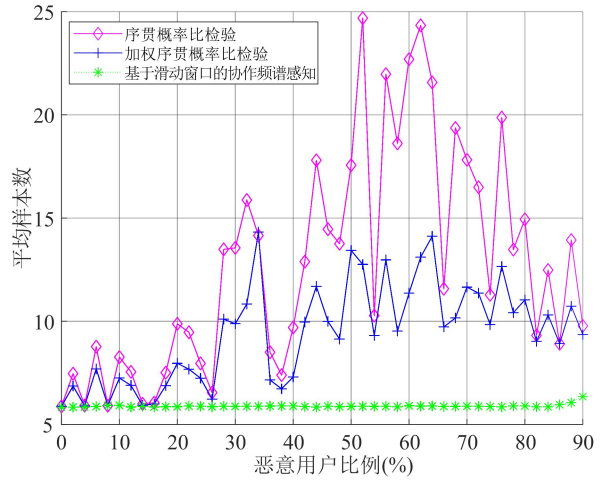


图 17　随机攻击$(\alpha,\beta)=(0.8,0.8)$下基于滑动窗口的协作频谱感知策略与其他融合规则的样本数

Fig. 17　ANS of SW-CSS and other fusion rules in the presence of random attack $(\alpha,\beta)=(0.8,0.8)$

6　结束语

本文提出了一种在认知无线电网络中存在拜占庭攻击的情况下基于滑动窗口的协作频谱感知策略。首先，简要分析了拜占庭攻击下的协作频谱感知，包括盲的问题、序贯检验；其次，提出了交付评估机制而不是全局判决来衡量从用户报告结果的准确性，并将其作为信誉值更新的方案；再次，基于滑动窗口的权重分配设计不仅提高了协作效率，而且鼓励了恶意用户的正常频

谱感知行为；最后，通过动态报告的方式来衡量协作的绩效和效率。仿真结果表明，本文提出的基于滑动窗口的协作频谱感知策略在错误概率和平均样本数方面的优势是明显的，这证明了所提出的策略在大规模拜占庭攻击中的高性能和高效性。

未来的研究仍有许多问题有待探索，例如分析融合中心和共谋的拜占庭攻击以博弈的方式优化其自身效益的场景，研究在分布式数据融合中使频谱感知性能最大化的最优策略等。

参 考 文 献

[1] JAIN S, YADAV A K, KUMAR R, et al. Cooperative spectrum sensing in cognitive radio networks: a systematic review[J]. Recent Advances in Computer Science and Communications, 2023, 16(4): 2-32.

[2] 吴俊. 协作频谱感知安全策略的研究[D]. 南京：东南大学, 2018.
WU Jun. Research on cooperative spectrum sensing security strategy[D]. Nanjing: Southeast University, 2018. (in Chinese)

[3] MITOLA J. Cognitive radio architecture evolution[J]. Proceedings of the IEEE, 2009, 97(4): 626-641.

[4] 卢俊峰. 认知无线电网络能效优化功率分配算法研究[D]. 成都：电子科技大学, 2022.
LU Junfeng. Energy-efficient power allocation algorithm in cognitive radio networks[D]. Chengdu: University of Electronic Science and Technology of China, 2022. (in Chinese)

[5] NAIR R G, NARAYANAN K. Cooperative spectrum sensing in cognitive radio networks using machine learning techniques[J]. Applied Nanoscience, 2023, 13: 2353-2363.

[6] 付元华. 高效安全协作频谱感知技术研究[D]. 成都：电子科技大学, 2020.
FU Yuanhua. Research on highly-efficient and secure cooperative spectrum sensing techniques[D]. Chengdu: University of Electronic Science and Technology of China, 2020. (in Chinese)

[7] ZHAO Q, SWAMI A. A survey of dynamic spectrum access: signal processing and networking perspectives[C]//Proceedings of 2007 IEEE International Conference on Acoustics, Speech and Signal Processing. [S. l.]: IEEE, 2007: 1349-1352.

[8] KYPEROUNTAS S, CORREAL N, SHI Q C, 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. [S. l.]: IEEE, 2007: 428-432.

[9] SHRIVASTAVA S, RAJESH A, BORA P K, et al. A survey on security issues in cognitive radio based cooperative sensing[J]. IET Communications, 2021, 15(7): 875-905.

[10] HE X F, DAI H Y, NING P. A Byzantine attack defender in cognitive radio networks: the conditional frequency check[J]. IEEE Transactions on Wireless Communications, 2013, 12(5): 2512-2523.

[11] 唐薇. 面向拜占庭攻击的认知无线电频谱感知算法研究[D]. 北京：北京交通大学, 2020.
TANG Wei. Research on approaches of spectrum sensing in the presence of Byzantine attack for cognitive radio[D]. Beijing: Beijing Jiaotong University, 2020. (in Chinese)

[12] LUO Z P, ZHAO S Q, LU Z, et al. When attackers meet AI: learning-empowered attacks in cooperative spectrum sensing[J]. IEEE Transactions on Mobile Computing, 2022, 21(5): 1892-1908.

[13] 钱小敏. 认知无线电系统中协作频谱感知关键技术研究[D]. 成都：西南交通大学, 2021.
QIAN Xiaomin. Research on key techniques of cooperative spectrum sensing in cognitive radio systems[D]. Chengdu: Southwest Jiaotong University, 2021. (in Chinese)

[14] HSIEH H Y, CHANG H K, KU M L. Higher-order statistics based sequential spectrum sensing for cognitive radio[C]//Proceedings of the 11th International Conference on ITS Telecommunications. [S. l.]: IEEE, 2011: 696-701.

[15] YILMAZ Y, MOUSTAKIDES G V, WANG X D. Cooperative sequential spectrum sensing based on level-triggered sampling[J]. IEEE Transactions on Signal Processing, 2012, 60(9): 4509-4524.

[16] YILMAZ Y, GUO Z Y, WANG X D. Sequential joint spectrum sensing and channel estimation for dynamic spectrum access[J]. IEEE Journal on Selected Areas in Communications, 2014, 32(11): 2000-2012.

[17] SHEI Y, SU Y T. A sequential test based cooperative spectrum sensing scheme for cognitive radios[C]//Proceedings of the 19th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. [S. l.]: IEEE, 2008: 943-947.

[18] GUO J M, ZHONG G H, QU D M, et al. Multi-slot spectrum sensing with backward SPRT in cognitive radio networks[C]//Proceedings of 2009 International Conference on Wireless Communications & Signal Processing. [S. l.]: IEEE, 2009: 650-654.

[19] XIN Y, ZHANG H H, RANGARAJAN S. SSCT: a simple sequential spectrum sensing scheme for cognitive radio[C]//Proceedings of 2009 IEEE Global Tele-

communications Conference. [S. l.]: IEEE, 2009: 4179-4184.

[20] HAGHIGHI K, SVENSSON A, AGRELL E. Wideband sequential spectrum sensing with varying thresholds[C]//Proceedings of 2010 IEEE Global Telecommunications Conference. [S. l.]: IEEE, 2010: 6926-6930.

[21] SREEDHARAN J K, SHARMA V. A novel algorithm for cooperative distributed sequential spectrum sensing in cognitive radio[C]//Proceedings of 2011 IEEE Wireless Communications and Networking Conference. [S. l.]: IEEE, 2011: 1881-1886.

[22] LI Q W, LI Z. A novel sequential spectrum sensing method in cognitive radio using suprathreshold stochastic resonance[J]. IEEE Transactions on Vehicular Technology, 2014, 63(4): 1717-1725.

[23] DWIVEDI S, KOTA A, JAGANNATHAM A K. Optimal bartlett detector based SPRT for spectrum sensing in multi-antenna cognitive radio systems[J]. IEEE Signal Processing Letters, 2015, 22(9): 1409-1413.

[24] PEREZ J, SANTAMARIA I, VIA J. Adaptive EM-based algorithm for cooperative spectrum sensing in mobile environments[C]//Proceedings of 2018 IEEE Statistical Signal Processing Workshop. [S. l.]: IEEE, 2018: 732-736.

[25] ZHAO J, LIU Q, WANG X, et al. Scheduled sequential compressed spectrum sensing for wideband cognitive radios[J]. IEEE Transactions on Mobile Computing, 2018, 17(4): 913-926.

[26] GAO S H, ZHANG N B, KANG G X. Improved cooperative spectrum sensing scheme using truncated SPRT in internet of things[C]//Proceedings of the 2nd IEEE International Conference on Electronic Information and Communication Technology. [S. l.]: IEEE, 2019: 89-93.

[27] CHEN R L, PARK J M, BIAN K G. Robust distributed spectrum sensing in cognitive radio networks [C]//Proceedings of the 27th IEEE Conference on Computer Communications. [S. l.]: IEEE, 2008: 31-35.

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

[29] WU J, SONG T C, YU Y, et al. Sequential cooperative spectrum sensing in the presence of dynamic Byzantine attack for mobile networks[J]. PLoS One, 2018, 13(7): e0199546.

[30] WU J, SONG T C, YU Y, et al. Reuse of Byzantine data in cooperative spectrum sensing using sequential detection[J]. IET Communications, 2019, 14(2): 251-261.

[31] WU J, YU Y, SONG T C, et al. Sequential 0/1 for cooperative spectrum sensing in the presence of strategic Byzantine attack[J]. IEEE Wireless Communications Letters, 2019, 8(2): 500-503.

[32] KIM Y M, ZHENG G B, SOHN S H, et al. An alternative energy detection using sliding window for cognitive radio system[C]//Proceedings of the 10th International Conference on Advanced Communication Technology. [S. l.]: IEEE, 2008: 481-485.

[33] SONG C Q, ZHANG Q. Sliding-window algorithm for asynchronous cooperative sensing in wireless cognitive networks[C]//Proceedings of 2008 IEEE International Conference on Communications. [S. l.]: IEEE, 2008: 3432-3436.

[34] TIAN X, TIAN Z, BLASCH E, et al. Sliding window energy detection for spectrum sensing under low SNR conditions[J]. Wireless Communications and Mobile Computing, 2016, 16(12): 1437-1663.

[35] AFISIADIS O, AUSTIN A C M, BALATSOUKAS-STIMMING A, et al. Sliding window spectrum sensing for full-duplex cognitive radios with low access-latency[C]//Proceedings of the 83rd IEEE Vehicular Technology Conference. [S. l.]: IEEE, 2016: 898-902.

[36] GUIMARÃES D A, LIM C H. Sliding-window-based detection for spectrum sensing in radar bands[J]. IEEE Communications Letters, 2018, 22(7): 1418-1421.

[37] GUIMARÃES D A, LIM C H. Hybrid sliding-window based detector for spectrum sensing in radar bands[J]. Journal of Communication and Information Systems, 2019, 34(1): 192-200.

[38] NOH J, KWON Y, LEE J, et al. Adaptive-sliding-window-based detection for noncooperative spectrum sensing in radar band[J]. IEEE Systems Journal, 2022, 16(3): 3878-3881.

[39] SHRIVASTAVA S, RAJESHA, BORA P K. Sliding window Dixon's tests for malicious users' suppression in a cooperative spectrum sensing system[J]. IET Communications, 2014, 8(7): 1065-1071.

[40] FU Y H, HE Z M. Entropy-based weighted decision combining for collaborative spectrum sensing over Byzantine attack[J]. IEEE Wireless Communications Letters, 2019, 8(6): 1528-1532.

[41] FU Y H, HE Z M. Bayesian-inference-based sliding window trust model against probabilistic SSDF attack in cognitive radio networks[J]. IEEE Systems Journal, 2020, 14(2): 1764-1775.

[42] CHENG Z X, SONG T C, ZHANG J, et al. Self-organizing map-based scheme against probabilistic SSDF attack in cognitive radio networks[C]//Proceedings of the 9th International Conference on Wireless Commu-

nications and Signal Processing. [S. l. : s. n.], 2017: 1-6.

[43] ZHU H C, SONG T C, WU J, et al. Cooperative spectrum sensing algorithm based on support vector machine against SSDF attack[C]//Proceedings of 2018 IEEE International Conference on Communications Workshops. [S. l. : s. n.], 2018: 1-6.

[44] CHEN Z, WU J, BAO J R. Semi-supervised learning-enabled two-stage framework for cooperative spectrum sensing against SSDF attack[C]//Proceedings of 2022 IEEE Wireless Communications and Networking Conference. [S. l.]: IEEE, 2022: 554-559.

[45] ZHANG Z X, WU J, GAN J P, et al. Support vector machine process against probabilistic Byzantine attack for cooperative spectrum sensing in CRNs[C]//Proceedings of the 8th International Conference on Machine Learning Technologies. [S. l. : s. n.], 2023: 269-276.

[46] THILINA K M, CHOI K W, SAQUIB N, et al. Machine learning techniques for cooperative spectrum sensing in cognitive radio networks[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(11): 2209-2221.

[47] JANU D, SINGH K, KUMAR S. Machine learning for cooperative spectrum sensing and sharing: a survey [J]. Transactions on Emerging Telecommunications Technologies, 2022, 33(1): e4352.

[48] WANG W K, LI H S, SUN Y, et al. Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks[J]. Eurasip Journal on Advances in Signal Processing, 2010, 2010 (1): 695750.

[49] LIANG Y C, ZENG Y H, PEH E C Y, et al. Sensing-throughput tradeoff for cognitive radio networks [J]. IEEE Transactions on Wireless Communications, 2008, 7(4): 1326-1337.

[50] 郭照人. 无线传感器网络中的安全数据聚合方法研究[D]. 成都: 电子科技大学, 2021.
GUO Zhaoren. Research on secure data aggregation in wireless sensor networks[D]. Chengdu: University of Electronic Science and Technology of China, 2021. (in Chinese)

[51] CHEN R L, JERRY P J M, BIAN K G. Robustness against Byzantine failures in distributed spectrum sensing[J]. Computer Communications, 2012, 35(17): 2115-2124.

[52] MA L P, HAN X F, SHEN C C. Dynamic open spectrum sharing MAC protocol for wireless ad hoc networks[C]//Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks. [S. l.]: IEEE, 2005: 203-213.

作 者 简 介

宋铁成

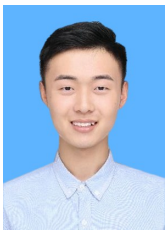
男,1967 年生,博士,教授,博士研究生导师,研究方向为移动通信理论与技术、认知无线电、物联网和泛在异构网络

E-mail: songtc@seu.edu.cn

吴 俊

男,1988 年生,博士,讲师,研究方向为认知无线电技术、无线传感器网络、无人机网络、车联网

E-mail: wojames2011@163.com



梁浩宇

男,1998 年生,硕士研究生,研究方向为认知无线电技术、无线传感器网络、无人机网络、车联网

E-mail: a15305620516@163.com

程之序

男,1993 年生,博士研究生,研究方向为移动通信理论与技术、认知无线电、物联网和泛在异构网络

E-mail: chengzhixu@hdu.edu.cn

责任编辑 钱 静