

面向拜占庭攻击的认知用户分类

尹拓凯^{1*}, 岳文静¹, 陈志²

(1. 南京邮电大学 通信与信息工程学院, 江苏 南京 210000;

2. 南京邮电大学 计算机学院, 江苏 南京 210000)

摘要: 万物互联的蓬勃发展使得承载业务的无线资源日益短缺, 认知无线电技术是具有广大前景的技术。而作为实现认知无线电的基础环节的频谱感知却面临特有的安全威胁, 其中拜占庭攻击伪造频谱感知数据, 利用认知网络的开放性和合作机制, 恶意篡改上传数据, 致使融合中心做出错误判断, 造成频谱资源损失。因此, 针对拜占庭攻击下的安全问题, 该文提出了基于图神经网络的异常度检测, 依据图神经网络得到数据异常程度, 结合全局判决与邻居用户冲突程度建立异常度模型。首先, 介绍了认知网络频谱感知的相关原理; 接着, 展示了认知网络的模型, 并对拜占庭攻击做了简单的概括。研究结果表明, 该算法在拜占庭攻击中取得优异的识别性能, 不仅降低了正常用户的误判概率, 同时提高了恶意用户的检测概率。

关键词: 认知无线电; 图神经网络; 拜占庭攻击; 恶意用户; 无线通信

中图分类号: TP309; TN925

文献标识码: A

文章编号: 1673-629X(2023)04-0102-06

doi: 10.3969/j.issn.1673-629X.2023.04.015

Cognitive User Classification for Byzantine Attack

YIN Tuo-kai^{1*}, YUE Wen-jing¹, CHEN Zhi²

(1. School of Communication & Information Engineering, Nanjing University of Posts &

Telecommunications, Nanjing 210000, China;

2. School of Computer, Nanjing University of Posts & Telecommunications, Nanjing 210000, China)

Abstract: The vigorous development of the Internet of things makes the wireless resources carrying services increasingly scarce. Cognitive radio technology is a technology with broad prospects. Spectrum sensing, as the basic link of cognitive radio, faces a unique security threat. Byzantine forges spectrum sensing data and maliciously tampers with the uploaded data by using the openness and cooperation mechanism of cognitive network, resulting in the wrong judgment of fusion center FC and the loss of spectrum resources. Therefore, aiming at the security problem under Byzantine attack, we propose a reputation detection based on graph neural network, obtain the degree of data abnormality according to graph neural network, and establish a reputation model combined with the degree of conflict between global judgment and neighbor users. Firstly, we introduce the relevant principles of spectrum sensing in cognitive network, then show the model of cognitive network, and briefly summarize the Byzantine attack. The results show that the proposed algorithm achieves excellent recognition performance in Byzantine attack, which not only reduces the false positive rate, but also improves the real rate.

Key words: cognitive radio; graph neural network; Byzantine attack; malicious user; wireless communication

0 引言

近年来由于无线电设备的急剧增加和频谱的静态管理, 造成无线电可用频谱的短缺^[1], 解决问题的方法之一是使用认知无线电技术^[2]。认知无线网络可以在不影响主用户的情况下使用闲置资源, 对频段进行授权, 提高频谱资源的利用率, 满足更多无线用户的需求。认知无线网络本质上是一种具有认知特性的无线

通信网络, 目的是解决无线频谱资源稀缺的问题。认知网络可以观察周围的无线网络环境, 并利用环境感知来获取相关的频谱使用信息, 对获取的信息进行处理和学习, 用于决策, 动态访问可用频谱, 最终重构网络, 适应动态认知无线网络环境, 最大化使用频谱^[3]。认知无线网络中的用户称为认知用户, 认知用户借用原本属于主用户的信道, 所以, 一旦主用户使用认知用

收稿日期: 2022-04-30

修回日期: 2022-08-31

基金项目: 江苏省重点研发计划(社会发展)项目(BE2019739); 中兴通讯产学研合作基金项目(2021外381)

作者简介: 尹拓凯(1996-), 男, 通讯作者, 研究方向为认知无线电、恶意用户检测; 岳文静(1982-), 女, 副教授, 研究方向为认知无线网络、移动物联网、数据挖掘。

户占用的信道,认知用户必须立即退出信道,同时寻找其他可用的信道。

认知无线电包含多个方面的技术,其中频谱感知^[4]是认知无线电用户等待机会使用主用户频谱,传输数据的关键技术。同时由于设备故障、信道阴影衰落、噪声等原因,单个认知用户经常误判主用户占用信道情况。不过认知用户间的协同频谱感知^[4]可以解决上述问题,有效提高频谱观测的效率和可靠性。协作感知虽然提高了感知的精度,但是将系统暴露在可能的恶意用户的危险中:不进行任何感知操作,随机报告感知结果,从而节省时间和能量;或者向融合中心报告信道忙,使融合中心做出错误判断,达到占用频谱的目的,或者对网络发起拒绝服务攻击^[5]。

在协同频谱感知过程中,为了减少恶意用户对最终决策的影响,提出了一种可行的方法是首先识别恶意用户,然后禁止它们参与频谱感知和最终数据融合。从现有文献中使用的理论和方法来看,恶意用户检测方法主要包括以下三类:基于信誉的去除低信誉用户的检测方法^[6]、基于异常统计行为检测离群点的检测方法^[7]、基于聚类 and 机器学习的检测方法^[8]。

基于信誉的拜占庭攻击检测方法原理简单,易于应用,在大量文献中均有大量研究结果。该方法的核心思想是根据可靠的参考信息更新每个感知节点的信誉,一旦信誉值超过给定的阈值,该节点就被判断为诚实节点或恶意节点。在文献[9]中引入贝塔信誉模型,根据认知传感器节点的历史感知行为为其分配信誉值,并根据所提交的观测数据对协同传感器节点进行评估,给出合理的权重值,以提高感知结果的准确性;文献[10]中的作者利用认知用户在前一个感知时期的局部感知结果的历史来识别攻击者。首先,利用极大似然法估计正常认知用户的分布参数,然后,采用自适应组合规则对加权系数进行调整。文献[11]中提出了一种基于认知用户声誉的防卫拜占庭攻击的方法。在每个频谱感知周期中,每个认知用户的信誉都会根据他们在前一个感知周期中的行为进行更新,然后,融合中心根据用户的声誉对用户进行分类。

基于异常统计行为检测离群点的检测方法,如果部分认知用户的感知结果异于同一认知网络中大部分认知用户的感知结果,那么这小部分认知用户会被判定为恶意用户。在文献[12]中作者提出了一个信任感知的一致性分布式合作频谱感知(DCSS)方案来抵抗拜占庭攻击。该方案要求每个节点不断更新相邻节点的信任评分。信任分数用来表示节点可以信任的程度,以及它的本地决策是否可以用于全局决策中。它们能够检测邻居的可信程度,并将其报告与下一次更新中的正常报告隔离开来,这有助于实现更好的感知

结果。在文献[13]中提出了共轭先验检测方案,以减轻在认知无线电环境中可能存在的拜占庭攻击。该方案将恶意用户产生的虚假感知结果与正常感知结果隔离开来。该方案将来自认知用户的传感报告作为随机变量处理,然后通过共轭先验方法考虑随机变量的概率密度。共轭先验检测还可以隔离任何行为不端的认知用户收到的虚假感知报告。当感知结果被判定为恶意攻击,感知结果不会用于最终决策中。

基于聚类和机器学习的检测方法,在认知网络中应用人工智能和机器学习方法的概念是必不可少的,因为认知网络是一个动态系统,可以学习和适应环境,以修改其无线电参数。例如,认知用户可以通过与周围环境相互作用、做出选择和更新其模型来从环境中学习,以便在未来的决策和预测中达到更好的准确性。近年来,利用机器学习技术提高频谱使用性能的思想由于其相对于传统方法的高效性而引起了人们的广泛关注,并引发了该领域的各种研究。机器学习算法学习输入数据集中的例子的特征,这些例子的类属性已知,并利用这种学习对新的观测值进行分类。另一个优点是分类模型的训练,这是计算密集型,但可以离线完成,只要数据集可以离线提供。拜占庭攻击者在发动攻击时,发送给融合中心的报告中总会留下篡改的痕迹,这些痕迹可以转换为输入特征并应用学习算法来学习。一旦学习完成,就可以检测到攻击者的攻击痕迹。在文献[14]中提出了一种使用改进支持向量机分类器的独特方法,称为两阶段支持向量机,旨在提高协作频谱感知的性能。将认知用户感知主用户能量水平的向量被视为特征向量,并在训练和测试阶段输入分类器。二元报告和连续报告的通用报告网络之间存在一定的差别,这两种报告网络中用于分类的数据分析相距甚远。例如,在连续报告中报告感应能量值的情况下,攻击者通常会在发送给融合中心之前增加或减少能量值。这个能量值范围很广,通常被视为一个重要的输入特性,它揭示了攻击者的遗留的痕迹。因此,可以根据已有数据集训练分类器。然后,由于攻击者会在连续报告中留下攻击痕迹,两阶段支持向量机就能根据特征向量判断信道是否可用。

1 系统模型

本小节建立了认知网络模型,并介绍了拜占庭攻击的相关情况。

1.1 认知网络模型

图1是一个认知无线网络中的协作频谱感知模型。PU代表主用户,FC代表融合中心。HU代表认知网络中的诚实用户,MU代表认知网络中的恶意用户,两者从属于认知用户。

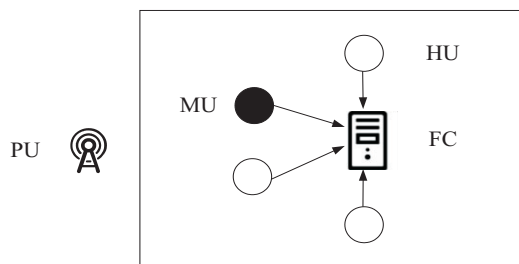


图1 认知网络模型

该文采用集中式协作频谱感知^[15],需要一个理想的节点作为融合中心来控制所有的合作感知过程。在集中式协作感知中,融合中心选择一个信道作为当前感知周期的感知信道,然后允许所有参与协作的认知用户对感知信道进行频谱感知,并将认知用户本身的频谱感知结果发送给融合中心。最后,融合中心对接收到的所有本地感知结果进行融合,通过一定的数据融合规则融合得到决策结果,判断主用户是否在使用信道,并将决策结果发送给参与协作的所有认知用户,认知用户根据判决结果知晓主用户的状态。

授权频段主用户优先使用,只有当主用户不使用该频段时,认知用户才有机会访问该频段。

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

用 $s(t)$ 表示主用户信号, $n(t)$ 表示加性高斯白噪声。 H_0 表示主用户未使用授权频段, H_1 表示主用户在使用频段。

在目前所有的频谱感知算法中,能量检测^[16]方法是一种复杂度较低、比较容易实现的感知算法,而且这种检测方法不需要主用户信号的先验信息,具有很大的优势。

在每个时隙, SU 首先使用能量检测进行频谱感知,分析主用户是否在使用授权频段。因此,第 i 个认知用户 SU_i 的能量感知结果可表示为:

$$T_i = \frac{1}{L} \sum_{k=1}^L |y_i(k)|^2 \quad (2)$$

将能量检测得到的结果与判决阈值 γ 比较:

$$o_i = \begin{cases} -1, & T_i < \gamma \\ 1, & T_i \geq \gamma \end{cases} \quad (3)$$

融合中心通过融合技术对认知用户发送的数据进行融合,得到关于主用户存在的全局判断结果。该文采用硬融合技术,认知用户对主用户的状态做出硬决策,即二进制决策,1 或 -1 表示主用户存在与否,并将认知用户本地决策结果独立发送给融合中心。融合中心将每个认知用户的二进制判断结果按照一定规则进行融合,以获得全局判断结果(主用户在当前信道中的占用状态),并将全局判断结果发送给每个认知用户。硬融合技术只需要少量带宽,复杂度低,易于实

现。目前,许多协作频谱感知场景都使用了硬融合技术。

该文采用硬融合技术中的 K 秩准则, K 秩准则是指在参与感知的 N 个感知节点中,如果有大于等于 K 个节点上报频段繁忙的感知结果,则最终判决结果为信道繁忙,反之,则信道空闲。每个认知用户得到本地决策结果后,会通过公共信道上报融合中心。融合中心利用融合准则得到融合决策结果,根据 K 秩准则决定频谱状态,该结果表示通道处于空闲和被占用状态。

信道状态计算方式如下:

$$J(t) = \begin{cases} H_1, & \sum_{n=1}^N (o_i(t) = 1) \geq \beta \\ H_0, & \text{otherwise} \end{cases} \quad (4)$$

式中, $o_i(t)$ 表示 SU_i 在 t 时刻的上报数据, β 指全局判决的阈值。

1.2 拜占庭攻击模型

可以对拜占庭攻击^[17]进行三个方面的分析,一是恶意用户是否以恒定概率攻击认知网络,按照攻击概率,拜占庭攻击主要分为概率攻击和非概率攻击。所谓的概率攻击,换句话说,恶意用户攻击的概率总是相同的。从恶意用户的角度来看,这样的攻击可以获得更好的攻击效果。检测系统可以通过观察攻击对象的数据来判断攻击概率。因此,很容易检测到概率攻击。所谓非概率攻击,是指恶意用户不以相同的概率发起攻击,而是自适应地选择合适的概率发起间歇性攻击。当恶意用户发起这种攻击时,他们不容易被检测系统识别,攻击效果不如恒定概率攻击好。

二是恶意用户攻击的认知网络属于集中式网络还是分布式网络,认知网络主要分为两种场景,一种是集中式,另一种是分布式。在集中式场景下,每个认知用户都会将自身的感知结果送到融合中心,融合中心统一决策,根据一定的恶意用户识别机制纠正恶意用户的影响。在分布式场景中,恶意用户可以向其邻居用户发送篡改的感知结果,如恶意用户判断主用户存在反而告知邻居用户主用户不存在,误导邻居用户做出错误的决定,相较于集中式场景,难以识别恶意用户。因此,在这种情况下,恶意用户变得更加难以检测,认知网络的可靠性大大降低。

三是恶意用户之间是合作攻击,还是分别独立攻击认知网络。独立攻击是指恶意用户独立发起的攻击。恶意用户之间没有信息交互,攻击性能较弱。很容易被防御系统识别。合作攻击,即恶意用户之间相互交换信息和合作的行为。当恶意用户发起协同攻击时,制定相同的攻击策略是非常重要的。它增加了攻击强度,不容易被入侵防御系统识别,大大增加了攻击

成功的概率。相比之下,合作攻击对整个认知网络的伤害更大,攻击方式更灵活,防御难度更大。

此外,从攻击规模来看,拜占庭攻击主要分为大规模攻击和小规模攻击。当网络中恶意用户越多,对整个认知系统的危害越大,攻击性能越好,攻击难度越大。当恶意用户数量达到一定数量时,整个系统将瘫痪。不过大规模攻击代价高昂。

文中拜占庭攻击使用独立攻击,集中式场景。假设恶意用户以恒定概率翻转发送的能量值,并发送至融合中心。每个恶意用户以概率 P 进行拜占庭攻击。

因此,恶意用户发送到融合中心的本地感知数据如图2所示。

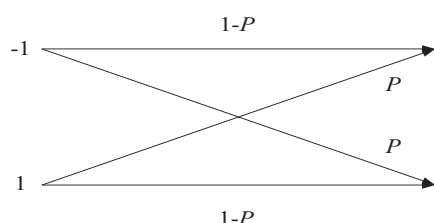


图2 恶意攻击转移概率

在该文设定的认知网络中,诚实用户正常地发送感知结果,而恶意用户如图2所示,感知结果会按照一定规律进行翻转,例如,当恶意用户感知结果为-1时,有 $1 - P$ 的可能正常发送,有 P 的可能翻转感知结果,发送错误信息给融合中心,促使融合中心做出错误判决,干扰认知网络正常运转。

2 基于图神经网络的恶意用户识别算法

结合图神经网络和异常度模型,设计了一种区分诚实用户与恶意用户的方案。首先,认知用户通过能量感知做出判决,然后,上传本地感知结果至融合中心。假设融合中心已经知道认知用户的位置信息,这些信息可以通过地理位置数据库^[18]获得。融合中心通过节点的上传信息,计算出认知用户的异常度,同时得出频谱的判决结果。

2.1 图神经网络

图神经网络^[19]的概念是由 Gori 等人在 2005 年首次提出的。图神经网络是一种用于对图结构数据进行高效建模的深度学习框架。它聚合邻域节点信息,利用神经网络学习和更新节点聚合信息。目前,图神经网络已应用于知识地图、推荐系统、计算机视觉、自然语言处理、社交网络等研究领域,并解决了许多相关问题。

图神经网络是图与神经网络的组合。图由节点和边组成,图的大小是任意的,图的拓扑结构复杂,没有像图像一样的空间局部性,同时图没有固定的节点顺序,或者说没有一个参考节点。

图是一种数据结构,它对一组对象及其结构布局进行建模,其中对象用作节点,邻接处用作边。图具有很强的表达能力,但其复杂性是显而易见的。因此,如何训练图,对一些机器学习算法带来了巨大的挑战。这是因为数据不规则。每个图都有数量可变的无序节点,并且图中的每个节点都有不同数量的相邻节点,这导致了一些重要的操作(例如卷积),这些操作在易于在普通图像中计算,但无法直接应用于图结构。

同时,现有机器学习算法之一的核心假设是实例相互独立。然而,图数据并非如此。图中的每个实例(节点)都通过一些复杂的连接信息,这些信息与其他实例相关,相互依存。

传统的深度学习模型,如卷积神经网络和递归神经网络。生成对抗网络,通常作用于欧几里得数据(包括图像、文本、语音序列、视频)。然而,面对某些场景下产生的非结构化数据,如图结构数据,传统的深度学习网络不能很好地对这种结构化数据建模。例如,普通神经网络(如卷积神经网络)无法正确处理图的输入,因为图中没有自然节点顺序。为了完整地呈现图,卷积神经网络需要遍历所有可能的序列作为模型的输入,对于一个图来说,这是完全没有必要的。为了解决这个问题,图神经网络在图的每个节点上分别传播,忽略节点的输入顺序。换句话说,图神经网络的输出完全没必要考虑节点的输入顺序。

图中的边表示两个节点之间的关联信息。在卷积神经网络中,关联信息并不能很好地表现出来,只能作为节点特征输入。然而,图神经网络可以依据图的特殊结构传播,而不是作为特征的一部分。一般来说,图神经网络通过相邻节点状态的加权和来更新节点的隐藏状态。

人脑的推理过程基于从日常经验中提取的图形。标准神经网络已经证明了其通过学习数据分布来生成合成图像和文档的能力,但它们仍然无法从大量实验数据中学习推理图。

在文献[20]中,使用结构与属性自编码器重构数据,发掘数据中的异常值,首先使用结构编码器将节点每个时隙的判决转为低维潜在表示,如公式(5)所示:

$$\tilde{\mathbf{Z}}^v = \sigma(\mathbf{X}\mathbf{W}^{v(1)} + \mathbf{b}^{v(1)}) \quad (5)$$

同时计算节点对邻居节点的重要性,称为注意力机制:

$$e_{i,j} = \text{attn}(\tilde{\mathbf{Z}}_i^v, \tilde{\mathbf{Z}}_j^v) = \sigma(\mathbf{a}^T \cdot [\mathbf{W}^{v(2)} \tilde{\mathbf{Z}}_i^v \parallel \mathbf{W}^{v(2)} \tilde{\mathbf{Z}}_j^v]) \quad (6)$$

通过 softmax 函数进行归一化:

$$\gamma_{i,j} = \frac{\exp(e_{i,j})}{\sum_{k \in N_i} \exp(e_{i,k})} \quad (7)$$

式中, \mathbf{W} 与 \mathbf{b} 分别是权重与偏置矩阵, \mathbf{X} 是认知网络节点每个时隙的判决, $\sigma(\square)$ 是激活函数。

最后结构编码器的嵌入表示由加权获得:

$$\mathbf{Z}_i^v = \sum_{k \in N_i} \gamma_{i,k} \cdot \tilde{\mathbf{Z}}_k^v \quad (8)$$

通过 Sigmoid 函数获取原始网络结构数据经编码器重构的输出:

$$\tilde{\mathbf{A}} = \text{Sigmoid}(\mathbf{Z}^v (\mathbf{Z}^v)^T) \quad (9)$$

神经网络的训练目标是 minimized 网络结构重建误差 rec :

$$\text{rec} = \|\mathbf{A} - \tilde{\mathbf{A}}\|_F^2 \quad (10)$$

式中, \mathbf{A} 是原始网络结构数据, $\tilde{\mathbf{A}}$ 是重构后得到的网络结构数据。

2.2 方案模型

对神经网络训练得到的重构误差进行极大极小归一化:

$$\tilde{S} = \frac{\text{rec} - \min(\text{rec})}{\max(\text{rec}) - \min(\text{rec})} \quad (11)$$

$$S = \begin{cases} 1, & \tilde{S} > \lambda \\ 0, & \text{otherwise} \end{cases} \quad (12)$$

设立恶意用户集合, 对异常度超过阈值的移入集合。

再结合每个节点在各个时隙与全局决策的匹配程度判断两者间的冲突程度:

$$\tilde{d} = \frac{R + 1}{T + R - 2} \quad (13)$$

$$d = \frac{\arctan(\tilde{d}) * 2}{\pi} \quad (14)$$

$$c = r \times (1 - w) + (1 - r) \times d \quad (15)$$

对冲突程度较严重的认知用户 SU_i , 分析其邻居用户的恶意用户占比, 对恶意用户占比超过一半的, 移出恶意用户集合, 小于一半的维持原有判断。

2.3 方案流程

基于图神经网络的异常度模型恶意用户识别方案:

输入: 认知网络 N , 认知用户 T 个时隙的上报值 F 。

输出: 恶意用户集合。

(1) F 、 N 输入图神经网络计算得到重构误差 rec , 并由式(10)计算;

(2) 融合中心经过 Majority rule 做出全局判决;

(3) 计算每个认知用户上传值与全局判决相同的次数, 根据式(14)计算 d ;

(4) 根据式(15)计算初步判决与全局匹配程度 d 的冲突程度;

(5) 对冲突程度较大的用户, 查看邻居用户的情况, 依据实际情况移入移出恶意用户集合。

3 仿真与分析

假设一片 $1\,000\text{ m} \times 1\,000\text{ m}$ 正方形区域, 存在 1 个融合中心, 1 个主用户, 50 个认知用户, 其中存在若干恶意用户。认知用户间距离小于 400 m 判定为邻居用户, 每个认知用户采用能量检测做出本地判决, 判决以 $-1, 1$ 形式上传至融合中心。

采用以下两个指标(检测概率和误判概率)进行评估, 检测概率是指正确检测到恶意用户的概率, 误判概率是指诚实用户被错误地检测为恶意用户的概率。检测概率越大, 误判概率越低, 则效果越好。

文献[21]中提出了一种方法, 利用节点间相关性的差异区分正常节点与恶意节点。记为方案 1。

图 3 是在恶意用户占比 10% 情况下的仿真结果。

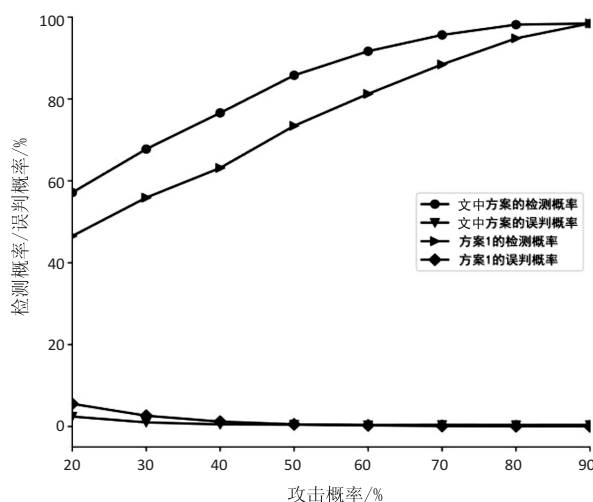


图 3 不同攻击概率下恶意用户占比 10% 的检测率与误判率

随着固定比例恶意用户攻击概率的增加, 恶意用户的检测概率在不断提高, 误判概率不断减小。这是因为恶意用户在提高自身攻击频次的同时, 其与正常用户的差异不断地扩大, 更容易被检测出来。与方案 1 对比, 在恶意用户占比 10% 的情况下, 文中方案的检测概率与方案 1 相比提高了 10% 左右。误判概率在低攻击概率下优于方案 1, 随着攻击概率的提高, 恶意用户更容易被检测出来, 两者差距缩小。

图 4 是在恶意用户占比 20% 情况下的仿真结果。

从图 4 中可知, 文中方案的仿真结果相对稳定, 并未因为恶意用户占比提高而恶化, 与恶意用户占比 10% 情况的差距不大。与恶意用户占比 10% 的情况对比, 方案 1 在恶意用户占比 20% 的情况下, 检测概率显著下降, 误判概率提高。显而易见, 文中方案在检测概率与误判概率两方面有较明显的优势。

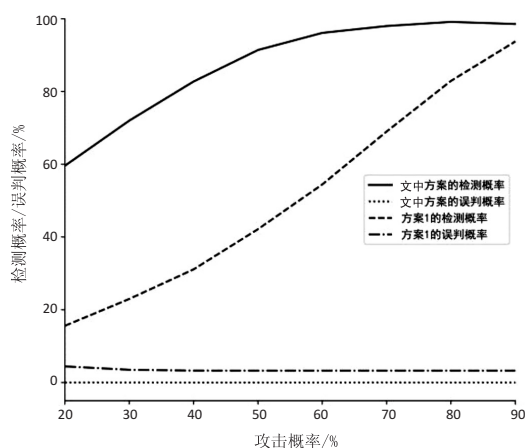


图4 不同攻击概率下恶意用户占比20%的检测率与误判率

4 结束语

针对随机拜占庭攻击,提出了一种基于图神经网络的异常值算法。在该方案中,依据恶意用户区别于其他正常用户的特点,使得恶意用户攻击发生之后,恶意用户的异常程度高于诚实用户而被区分开来,再结合本地判决与全局判决的匹配次数,进一步区分诚实用户与恶意用户。

参考文献:

- [1] AL-FUQAHA A, GUIZANI M, MOHAMMADI M, et al. Internet of things: a survey on enabling technologies, protocols, and applications [J]. IEEE Communications Surveys Tutorials, 2015, 17(4): 2347–2376.
- [2] RAWAT P, SINGH K D, BONNIN J M. Cognitive radio for M2M and Internet of things: a survey [J]. Computer Communications, 2016, 94: 1–29.
- [3] 聂慧峰, 徐声海. 认知无线电中的协作频谱感知技术[J]. 电子技术应用, 2020, 46(5): 63–67.
- [4] 倪水平, 常慧刚. 认知无线网络多用户智能协作频谱感知算法[J]. 测控技术, 2018, 37(4): 82–87.
- [5] 杨衍玥. 对认知无线网络的安全建议[J]. 中国无线电, 2018(8): 36–40.
- [6] SUN Z, XU Z, CHEN Z, et al. Reputation-based spectrum sensing strategy selection in cognitive radio ad hoc networks [J]. Sensors, 2018, 18(12): 4377.
- [7] RAJKUMARI R, MARCHANG N. Secure non-consensus based spectrum sensing in non-centralized cognitive radio networks [J]. IEEE Sensors Journal, 2018, 18(9): 3883–3890.
- [8] TAGGU A, MARCHANG N. Detecting byzantine attacks in cognitive radio networks: a two-layered approach using hidden Markov model and machine learning [J]. Pervasive and Mobile Computing, 2021, 77: 101461.
- [9] LUO X. Secure cooperative spectrum sensing strategy based on reputation mechanism for cognitive wireless sensor networks [J]. IEEE Access, 2020, 8: 131361–131369.
- [10] CHEN H, ZHOU M, XIE L, et al. Cooperative Spectrum sensing with m-ary quantized data in cognitive radio networks under SSDF attacks [J]. IEEE Transactions on Wireless Communications, 2017, 16(8): 5244–5257.
- [11] AL-MATHEHAJI Y, BOUSSAKTA S, JOHNSTON M, et al. Defeating SSDF attacks with trusted nodes assistance in cognitive radio networks [J]. IEEE Sensors Letters, 2017, 1(4): 1–4.
- [12] LIMBASIYA T, DAS D, YADAV R N. A reputation-based trust management model in multi-hop cognitive radio networks [J]. Recent Findings in Intelligent Computing Techniques, 2018, 708: 183–192.
- [13] CHEN C, SONG M, XIN C. CoPD: a conjugate prior based detection scheme to countermeasure spectrum sensing data falsification attacks in cognitive radio networks [J]. Wireless Networks, 2014, 20(8): 2521–2528.
- [14] GHAZIZADEH E, ABBASI-MOGHADAM D, NEZAM-ABADI-POUR H. An enhanced two-phase SVM algorithm for cooperative spectrum sensing in cognitive radio networks [J]. International Journal of Communication Systems, 2019, 32(2): e3856.
- [15] 吕玉静, 宋志群, 刘玉涛. 单天线认知无线电中的协作频谱感知和无线能量传输 [J]. 计算机测量与控制, 2019, 27(11): 193–196.
- [16] 刘乐. 基于能量检测的认知无线电频谱感知算法研究 [J]. 物联网技术, 2019, 9(5): 15–17.
- [17] 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.
- [18] GHAZNAVI M, JAMSHIDI A. A low complexity cluster based data fusion to defense against SSDF attack in cognitive radio networks [J]. Computer Communications, 2019, 138: 106–114.
- [19] 马帅, 刘建伟, 左信. 图神经网络综述 [J]. 计算机研究与发展, 2022, 59(1): 47–80.
- [20] FAN Haoyi. Anomalydae: dual autoencoder for anomaly detection on attributed networks [C]//ICASSP 2020 – 2020 IEEE international conference on acoustics, speech and signal processing (ICASSP). Spain: IEEE, 2020: 5685–5689.
- [21] KHAN M S, FAISAL M, KIM S M, et al. A correlation-based sensing scheme for outlier detection in cognitive radio networks [J]. Applied Sciences, 2021, 11(5): 2362.