文章编号:1671-4598(2023)10-0285-06 DOI:10.16526/j.cnki.11—4762/tp.2023.10.043 中图分类号:TP393.4 文献标识码:A

基于流量特征的区域互联网攻击源IP地址检测

杨 波,徐胜超,毛明扬,陈 刚,王宏杰
(广州华商学院 数据科学学院,广州 511300)

摘要:当区域互联网受到攻击时,其流量会发生较为明显的变化,因此提出基于流量特征的区域互联网攻击源IP地址检测方法;采用NetFlow技术采集用户高速转发的IP数据流,得到网络流量数据;针对网络流量中突变数据,实施去除处理;通过最小冗余最大相关性,提取互联网的流量特征,以提高攻击源IP地址的检测精度;以流量特征的信息熵作为输入,结合极限学习机与k均值算法实现攻击流量检测并确定互联网攻击源IP地址;测试结果表明:在该方法的应用下,攻击源IP地址检测质量指数为0.97,由此说明该方法的检测准确性更高,检测质量更好。

关键词:流量特征;区域互联网;攻击源;IP地址检测;信息熵

IP Address Detection of Regional Internet Attack Sources Based on Traffic Characteristics

YANG Bo, XU Shengchao, MAO Mingyang, CHEN Gang, WANG Hongjie
(School of Data Science, Guangzhou HuaShang College, Guangzhou 511300, China)

Abstract: When regional internet is attacked, its traffic will undergo significant changes. Therefore, a regional internet attack source IP address detection method based on traffic characteristics is proposed. NetFlow technology is used to collect the high-speed IP data stream forwarded by users and obtain network traffic data. Removal processing for abrupt data is implemented in network traffic. By minimizing redundancy and maximizing correlation, the traffic characteristics of the Internet are extracted to improve the detection accuracy of the attack source IP address. With the information entropy of traffic characteristics as an input, combined with extreme learning machine and k-means algorithm, the attack traffic detection and determination of Internet attack source IP address are realized. The test results show that under the application of this method, the quality index of attack source IP address detection is 0.97, indicating that the detection accuracy and quality of the proposed method are better.

Keywords: flow characteristics; regional internet; attack source; IP address detection; information entropy

0 引言

随着经济发展的数字化转型和5G技术的发展,当前很多企业在云上部署业务,不仅业务更方便,同时大大减轻了企业的负担,这样就加快了经济的发展。利用“云”的方式来实现网络入侵检测、网络异常流量检测、负载均衡、物理主机资源充分利用、尽最大可能节省数据中心的能量消耗,符合国家节能减排的主要政策。

当数据上云后,能否很好地开展业务,云任务在复杂系统中的运行,在传输数据时是否会被窃取,延迟很高导致传输速度很慢等等问题,就是一直存在的。为了保证云网的安全稳定运行,减少入侵风险,如果我们将安全防护策略部署在云端,可以有效减低企业维护安全设备软硬件的人力物力资源,安全平台提供开放的接口标准,快速的实现零门槛的安全软件/硬件部署,实现企业网络安全防护。

为了实现满足云安全服务长期稳定可靠运行需求、监管合规、建设安全运营平台,实现云安全“可视”、“可控”。城域网区域互联网攻击源IP地址检测是云安全中的一个重要的研究方向[1]。目前,许多研究人员通过分析网络流量数据来检测互联网攻击源IP地址[2]。然而,传统的基于规则和特征的检测方法存在一定的局限性,比如需要事先定义规则或特征,并且对新型攻击的检测能力较弱。因此,基于机器学习和数据挖掘技术的检测方法逐渐成为研究热点[3]。

互联网攻击源检测在识别攻击和确保计算机网络安全方面发挥着重要作用。基于该问题,很多专家和学者依据各种算法提出了检测方法。例如文献[4]为了有效识别

收稿日期:2023-06-09; **修回日期**:2023-07-17。
基金项目:国家自然科学基金面上项目(61772221);广州华商学院校级导师制科研项目(2022HSDS23)。
作者简介:杨 波(1977-),男,硕士,副教授。
徐胜超(1980-),男,硕士,副教授。
陈 刚(1973-),男,硕士,副教授。
引用格式:杨 波,徐胜超,毛明扬,等.基于流量特征的区域互联网攻击源IP地址检测[J].计算机测量与控制,2023,31(10):285-290,298.

网络环境中大量网络流中未知的恶意攻击行为，提出了一种基于人工免疫网络与密度峰值（ADAID，artificial immune network and density peak）的检测方法，研究中引入了聚类标记算法和流异常检测算法，利用前者标记每个簇是否恶意，并将标记的簇视为检测器，利用后者识别攻击网络流量。文献［5］提出了一种基于人工神经网络的攻击检测方法，使用 NS2 网络模拟器收集网络流量并创建数据集，然后以此为输入，利用人工神经网络实现不同的 DoS 攻击检测。文献［6］提出了一种基于隐马尔可夫模型改进算法的攻击检测方法，研究中为了提高算法的学习能力和适应性，利用 Baum-Welch 算法改进隐马尔可夫模型，最后利用优化维特比算法检测攻击行为。文献［7］提出基于 XGBoost 回归分类器的网络攻击行为检测方法，该方法首先对 XGBoost 回归分类器的工作原理进行说明，采集网络运行中的各项数据，将采集的数据输入到 XGBoost 回归分类器中，实现分布式拒绝服务、网络钓鱼、跨站点脚本攻击的检测。文献［8］提出基于半监督学习的无线网络攻击行为检测方法，通过无监督学习模型栈式稀疏自编码器提取网络流量的新特征值向量与原始特征权重向量，将提取的两类向量输入到深度神经网络中进行迭代训练。采用 k-means 聚类方法对训练输出结果进行聚类处理，完成网络攻击的识别。

以上 5 种研究方法在攻击检测中都发挥了一定的作用，但是随着网络攻击朝着隐蔽性、复杂性、多步骤等方向发展，如果不考虑网络流量特征，则会降低攻击源的检测精度。针对上述问题，本文提出一种基于流量特征的区域互联网攻击源 IP 地址检测方法。

1 区域互联网攻击源 IP 地址检测

当下攻击方式具有很强的随机非线性、欺骗性、伪装性，使得要想准确定位攻击源 IP 地址困难[7]。面对这种情况，为了抵御恶意攻击者的恶意攻击，研究一种基于流量特征的区域互联网攻击源 IP 地址检测方法，检测方法的主要内容包括 IP 网络流量采集、IP 网络流量预处理、流量特征提取以及攻击源 IP 地址检测实现。下面针对上述步骤进行具体分析。

1.1 IP 网络流量采集

攻击源检测需要依据一定的数据来确定某一用户存在攻击行为，然后针对这一行为进行追踪，定位攻击源 IP 地址，完成攻击溯源[8]。从上述整个过程中可以看出依据数据是基础，后续所有检测步骤都是围绕该数据进行挖掘和分析，最终得出结果。基于此，依据数据的获取至关重要。依据数据类型主要有两种：一是互联网日志，二是网络流量[9]。在本研究中，选择后者作为基础。采集方法为 NetFlow 技术，采集具体过程如图 1 所示。

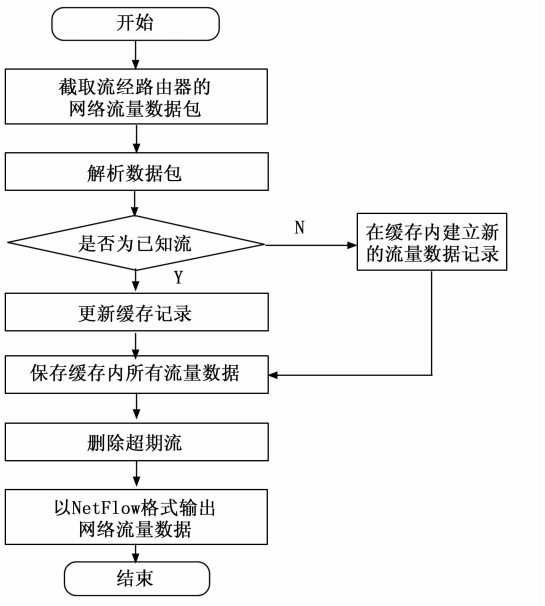

图 1 IP 网络流量采集流程

任何用户在进入互联网后，一切操作都会产生一定数据流量。数据流量会随着操作行为的不同而表现出差异性。基于此，只要把握住这种差异性就能反向观察用户行为，判断其是否存在攻击行为[10]。

1.2 IP 网络流量突变预处理

网络流量数据具有一定的突变性特征，该特征主要是用户设备和互联网连接异常造成的，这种流量数据的存在很容易与攻击用户所产生的流量数据混淆，二者十分相似，因此会干扰检测结果准确性[11]。面对这种现象，需要找出其中的突变网络流量数据，提高 IP 网络流量数据质量。具体过程如下：

步骤 1：输入 IP 网络流量数据；

步骤 2：通过互补聚合经验模态分解（CEEMDAN，complete EEMD with adaptive noise）方法对 IP 网络流量数据分解，得到 k 个子序列 IP 网络流量，记为 $S=\{s_i \mid i=1, 2, \ldots, k\}$。

步骤 3：计算 S 中每个子序列的分散熵，记为 b_i；

步骤 4：将求得的 k 个分散熵值归一化处理，记为 $\hat{b}_i$；

步骤 5：将相邻两个子序列的 $\hat{b}_i$ 相减，然后取绝对值，记为 c_i。

步骤 6：将 c_i 与设定的均值变化率阈值 T 进行对比。当 $c_i \geqslant T$ 时，将第 i 个子序列归入去突变模态集合；否则将第 i 个子序列归入保留模态集合。

步骤 7：参照根据 CEEMDAN 的分解规律，将去突变模态集合中的子序列 IP 网络流量划分为高、中、低频三类。

步骤 8：对其中的高频部分进行舍弃，对其中相对中频子模态利用小波阈值方法去除突变网络流量数据，低频部分则保持不变，不进行任何处理[12]。

步骤 9：将低频部分与去除突变后的低频部分进行重构，完成 IP 网络流量突变预处理。

经过上述流程，完成 IP 网络流量突变预处理，避免了突变流量数据带来的干扰[13]。

IP 网络流量突变预处理流程如图 2 所示。

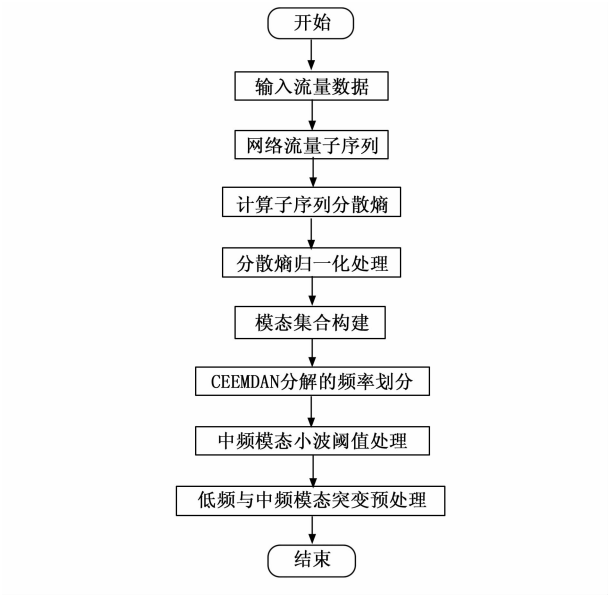

图 2　IP 网络流量突变预处理

1.3　流量特征提取

根据 1.2 节中的处理结果，本节正式进入数据分析环节。IP 网络流量中包含了很多特征参数，如表 1 所示。

表 1　IP 网络流量数据特征参数表

类别	特征参数
流量大小	总报文数
	总字节数
流的数目	总的 TCP 流的数量
	总的 UDP 流的数量
端口的数目	总的使用的端口的数量
TCP 连接数	TCP 连接数
跳变报文的数量	发生跳变的报文的比例
IP 地址数	通信的总 IP 地址数
上下行流量差异	上下行流量的字节数差值比例
	上下行流量的报文数差值比例
网络空闲时间	空闲时间比例
	最大空闲时间
DNS 报文的数量	总发送 DNS 请求报文的数量
HTTP 和 HTTPS 报文的数量	总 HTTP 报文和 HTTPS 报文的数量
访问网站的数量	总的访问网站的数量
TCP 或 UDP 使用情况	TCP 与 UDP 报文数差值比例
	TCP 与 UDP 字节数差值比例

从表 1 中可以看出，IP 网络流量中特征参数有很多，虽然都可以用于最后的攻击源检测，但是过多的特征参数不仅会大大增加后期检测工作的计算量，而且对提高检测精度并没有太大的帮助[14]。针对这种情况，只要从上述表 1 中选出 N 个最优特征参数就可以。在这里 N 取值 4[15]。通过计算最小冗余最大相关性，选取排名前 4 的特征参数，具体选取流程如下：

步骤 1：计算第 i 个特征参数 p_i 与类别 Q 之间，特征参数 p_i 和 p_j 之间的互信息值，记为 $R(p_i,Q)$、$W(p_i,p_j)$。

步骤 2：计算 $R(p_i,Q)$、$W(p_i,p_j)$ 的平均值，公式如下：

$$\begin{cases}\overline{R}(p_i,Q)=\dfrac{\sum\limits_{p_i\in P}R(p_i,Q)}{P}\\ \overline{W}(p_i,p_j)=\dfrac{\sum\limits_{p_i,p_j\in P}W(p_i,p_j)}{P}\end{cases}\tag{1}$$

式中，P 代表特征数量。

步骤 3：计算最小冗余最大相关性。计算公式如下：

$$G_i=\max_P\left[\overline{R}(p_i,Q)-\frac{\sum\limits_{p_i,p_j\in P}W(p_i,p_j)}{P^2}\right]\tag{2}$$

式中，G_i 代表第 i 个特征参数的最小冗余最大相关性。

步骤 4：按照从大到小的顺序排列 G_i。

步骤 5：选取 G_i 值排前 4 的特征参数作为选取结果。

计算 4 个流量特征的信息熵值，统一参数值[16]。熵值计算公式如下：

$$H_i=-\sum_{i=1}^{4}G_i\log g(G_i)\tag{3}$$

式中，H_i 代表第 i 个网络流量特征的熵值；$g(G_i)$ 代表 G_i 出现的概率。

经过上述过程，完成了流量特征的选择工作，为攻击源 IP 地址的精准检测奠定基础。

1.4　攻击源 IP 地址检测实现

攻击源 IP 地址检测是本研究的最后一部分，该部分的工作主要分为两步：攻击流量检测和攻击源 IP 地址定位[17]。下面将对这两个步骤进行具体分析与研究。

1.4.1　攻击流量检测

攻击流量检测是指基于网络流量数据特征判断是否存在攻击流量[18]。结合极限学习机与 k 均值算法来构建攻击流量监测模型，攻击流量监测模型的结构如图 3 所示。

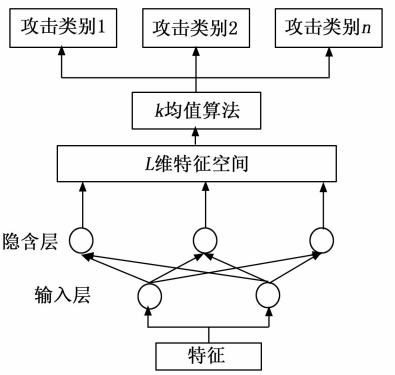

图 3　攻击检测模型

为了进一步攻击流量检测的精度，基于极限学习机和 k 均值算法进行攻击流量检测。首先利用 k 均值算法对原始数据进行聚类分析，将数据划分为不同的簇；然后，将每个簇的数据作为输入，利用极限学习机算法进行分类预测。通过不断迭代优化，可以得到一个精度较高的分类模型，用于对未知数据进行分类识别。其具体流程如下：

步骤 1：设定攻击流量检测模型的相关参数。

步骤 2：构建极限学习机。

步骤 3：确定 K-Mean 算法中的近邻数。

步骤 4：输入训练样本到极限学习机当中，经过三层处理，在映射函数的帮助下，将网络流量特征训练样本（信息熵）映射到 L 维特征空间中[19]。

步骤 5：执行 k 均值算法检测流程。具体如下：

1）从 L 维特征空间中选取初始聚类中心，选取数量为 M。

2）计算其余所有特征矢量与 M 个初始聚类中心之间的加权距离 D，计算公式如下：

$$D=\left[\sum_{i=1}^{N}w_i(H_i-O_j)^2\right]^{1/2},j=1,2,\ldots,M \quad (4)$$

式中，O_j 表示第 j 个聚类中心；N 表示特征数，这里取值 4；w_i 表示特征对应的权值，取值一般在 0～1 之间，由于本研究有 4 个特征参数，这 4 个特征参数合计需要等于 1。

3）根据 D 将特征矢量分配到某一类。在这里主要是指两类，一类为正常，一类为攻击。

4）更新聚类中心。

5）中心是否发生变化？若发生，回到步骤 2）；否则，停止并输出检测结果[20-23]。

1.4.2 攻击源 IP 地址定位

在完成攻击流量检测之后，进行攻击源 IP 地址定位。具体过程如下：

步骤 1：通过水印添加器在检测出来的攻击流量中嵌入水印。水印添加器可以直接在攻击流量中嵌入目标水印，不需要额外进行操作，可以在确保水印嵌入可靠性的基础上，提高水印嵌入的效率[24-27]。水印添加器添加水印的流程如图 4 所示。

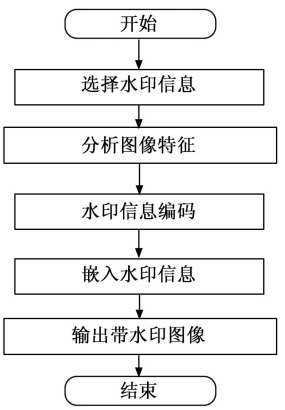

图 4 水印添加器添加水印的流程图

步骤 2：依据嵌入的水印得到一条从发送端到终点站的流量传输路径。

步骤 3：对路径进行追踪并实时提交提交本机（IP，检测时间戳，水印参数名）。

步骤 4：通过定位到的用户服务器的 IP 地址，可以实施防御策略，以击退攻击并保护网络安全。

2 实验与性能分析

为保证本文检测方法的实际应用效果，在设置的算例下，进行攻击源 IP 地址检测测试。为进一步凸显该方法性能，与基于 ADAID、人工神经网络、改进隐马尔可夫模型的检测方法应用结果进行对比。

2.1 实验环境

实验采用某个区域互联网作为模拟测试环境，通过极限学习进行预测建模，再采用均值算法对数据进行挖掘，并最终通过水印添加器对其进行数字版权和内容安全保护。在该环境中，共有 1153 个网络用户，其中 321 个用户为网络攻击用户，其余用户为合法上网用户。

2.1.1 实验参数设置

K-mean 算法的参数设置如表 2 所示。

表 2 K-mean 算法的参数设置

参数	数值
K 值	4
初始聚类中心	根据数据分布选择
距离度量	欧氏距离
迭代终止条件	最大迭代次数、聚类中心变化小于阈值
初始化方式	Forgy 算法
阈值	50

极限学习机方法的参数设置如表 3 所示。

表 3 极限学习机方法的参数设置

参数	数值
隐含层神经元数/个	100
激活函数	relu
正则化参数	0.001
权重初始化方式	随机初始化
学习率/%	0.01

2.1.2 实验软件与硬件设置

1）软件设置：

（1）操作系统：选择 Windows10 的操作系统。

（2）网络安全软件：安装防火墙、入侵检测系统（IDS）网络安全软件来保护实验环境。

（3）流量分析工具：使用 Wireshark 工具对流量进行抓取和分析。

（4）信息采集：在网络用户的终端设备内安装 NetFlow 软件，采集这些用户为期 30 天的网络流量数据。

2）硬件设置：

（1）网络设备：交换机、路由器等用于构建实验网络环境，并保证流量传输的稳定。

（2）流量生成工具：使用流量生成器模拟的攻击流量，用于实验测试。

实验共计 3 000 多条记录，每条记录包含 3 个特征和 1 个类别标签。以其中 1 条流量数据为例，数据样本如图 5 所示。

对于网络流量中的每条正常流量数据和攻击流量数据，

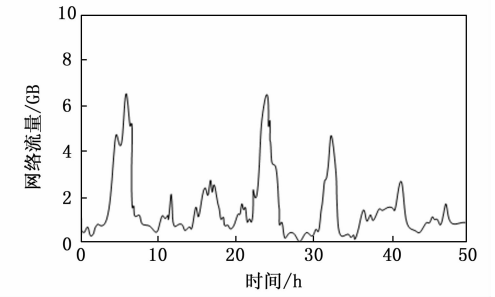

图 5　网络流量示例

根据已知的攻击类型对数据包进行匹配和标记。每条流量数据将被标记为攻击包或非攻击包。为了消除数据偏差，在要输入数据来训练检测模型时，将所有攻击数据包与随机数目的合法数据包混合，然后重新采样以获得训练模型的输入数据。

2.2　相关性测试结果

为了从较多的流量特征参数中，选取出与攻击源 IP 地址检测最为相关的特征，并减少后续的计算量，通过最小冗余最大相关性 G_i 来进行流量特征参数的选择。最小冗余最大相关性 G_i 的计算结果如表 4 所示。

表 4　网络流量数据特征参数的最小冗余最大相关性表

特征参数	最小冗余最大相关性
总报文数	9.822 2
总字节数	9.210 7
总的 TCP 流的数量	8.652 2
总的 UDP 流的数量	8.846 5
总的使用的端口的数量	7.652 4
TCP 连接数	9.742 4
发生跳变的报文的比例	9.688 2
通信的总 IP 地址数	8.621 5
上下行流量的字节数差值比例	7.664 5
上下行流量的报文数差值比例	7.412 2
空闲时间比例	9.625 2
最大空闲时间	8.124 2
总发送 DNS 请求报文的数量	9.044 4
总 HTTP 报文和 HTTPS 报文的数量	8.913 2
总的访问网站的数量	8.365 4
TCP 与 UDP 报文数差值比例	7.852 2
TCP 与 UDP 字节数差值比例	8.045 2

从表 4 中可以看出，结合本文方法的优点，可以对选出的 4 个流量特征进行丰富。以下是一个具体的描述：根据最小冗余最大相关性的排序结果，本文选择了总报文数、TCP 连接数、发生跳变的报文的比例以及空闲时间比例作为关键的流量特征。这四个特征的选择是基于本文方法的优点来进行的。首先，总报文数作为一个基本的统计特征，可以提供关于流量负载的整体信息。它能够反映网络中数据包的总体流量情况；其次，TCP 连接数是一个重要的指标，用于衡量潜在的攻击行为。攻击者通常会引发大量的非正常或恶意的 TCP 连接，因此监测和分析 TCP 连接数可以有效检测和识别攻击行为；第三，发生跳变的报文比例是一个针对网络流量异常变化的特征。异常的报文跳变可能表示网络中出现了异常事件或攻击行为。通过监测和分析该比例，可以快速发现网络中的可疑活动；最后，空闲时间比例是一个与网络利用率和活动程度相关的特征。攻击者可能会利用网络的空闲时间来进行攻击，因此监测和分析空闲时间比例可以帮助识别潜在的攻击行为。通过选取这四个流量特征，可以充分利用最小冗余最大相关性的方法，在保持簇间相关性最小且簇内相关性最大的同时，捕获到网络流量数据中的关键信息，从而提高攻击源 IP 地址检测的准确性和效果。

2.3　特征信息熵的测试结果

针对选出四个最优网络流量特征，计算每条网络流量数据的信息熵。随机选取 10 条作为示例，其信息熵统计结果如表 5 所示。

表 5　特征信息熵示例表

序号	总报文数	TCP 连接数	发生跳变的报文的比例	空闲时间比例
4	0.864 2	1.745 2	0.222 2	0.084 2
87	1.897 6	1.522 2	0.287 6	0.045 6
162	1.048 8	2.522 2	0.845 6	0.041 2
352	2.852 2	0.987 4	0.184 3	0.087 5
378	1.086 4	0.344 1	0.452 2	0.045 5
421	3.874 5	1.226 5	0.872 2	0.089 7
569	1.046 5	1.987 6	0.453 2	0.038 4
721	2.819 4	2.465 5	0.345 2	0.074 2
784	2.087 8	4.845 2	0.722 2	0.032 2
907	1.774 5	2.870 0	0.428 4	0.387 4

分析表 5 可知，信息熵越高表示流量数据中的不确定性和复杂性越大。通过计算信息熵，可以量化每条流量数据的信息量大小，从而更好地理解其在整体数据集中的重要程度。根据实验结果，观察到不同流量数据的信息熵有所差异。这意味着某些网络流量数据可能包含更多的信息，对于识别攻击源 IP 地址具有更高的潜力。通过进一步分析和挖掘这些高信息熵的流量数据，可以更好地理解网络中的异常行为，并提高对潜在攻击的检测能力。通过计算选定网络流量特征的信息熵，可以更深入地了解流量数据的信息量，并为后续的攻击源 IP 地址检测工作提供有价值的参考

2.4　检测质量实验对比分析

应用本文方法、基于 ADAID 的检测方法、基于人工神经网络的检测方法、基于改进隐马尔可夫模型的检测方法进行互联网攻击源 IP 地址检测。根据计算结果，计算检测质量指数，公式如下：

$$J=\frac{\frac{X}{Z}\cdot\frac{Y}{U}}{\left|\frac{X}{Z}-\frac{X}{Z}\cdot\frac{Y}{U}+\frac{Y}{U}\right|} \tag{5}$$

式中，Y 代表正确检测出来的攻击源 IP 地址数；J 代表检测质量指数；U 代表用户 IP 地址总数；X、Z 代表方法检测出来和实际攻击源 IP 地址数目。当 J 越大，认为检测准确性越高。结果如图 6 所示。

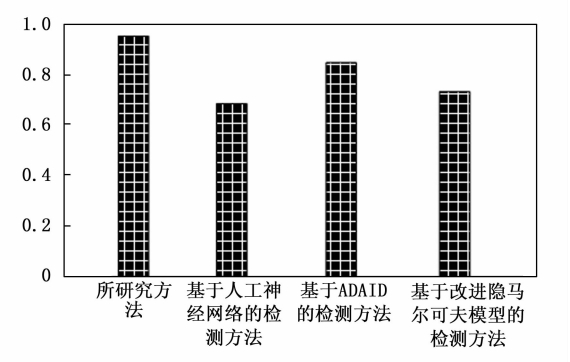

图 6 检测质量指数对比图

从图 6 中可以看出，基于 ADAID 的检测方法的质量指数为 0.83，基于人工神经网络的检测方法的质量指数为 0.65，基于改进隐马尔可夫模型的检测方法的矢量指数为 0.68，均低于本文方法。本文方法的检测质量指数为 0.97，说明本文方法的检测准确性更高。本文方法具有较高的检测质量指数的原因在于采用了 NetFlow 技术对区域互联网中的 IP 数据流进行采集，并在最小冗余最大相关性的约束下提取了流量特征。将流量特征的信息熵输入到极限学习机中，通过 k 均值算法确定互联网攻击源的 IP 地址。

3 结束语

为了能够有效阻止攻击，保护数据安全，进行基于流量特征的区域互联网攻击源 IP 地址检测研究。该研究以访问用户的流量数据为基础，通过提取流量特征，利用检测模型实现攻击流量检测，确定攻击地址，为防御策略提供了重要的参考。在未来的工作中将尝试在具有真实网络流量的网络环境中实施此方法，进一步验证方法的有效性。

参考文献：

[1] KUMAR V S, KHANNA M R, SARAVANAN R. Security concerns and remedial measures in MANETs using intrusion detection [J]. ECS transactions, 2022, 107 (1): 1459 - 1466.

[2] DONG R H, YAN H H, ZHANG Q Y. An intrusion detection model for wireless sensor network based on information gain ratio and bagging algorithm [J]. International Journal of Network Security, 2020, 22 (2): 218 - 230.

[3] YAO H, LI C, SUN P. Using parametric t-distributed stochastic neighbor embedding combined with hierarchical neural network for network intrusion detection [J]. International Journal of Network Security, 2020, 22 (2): 265 - 274.

[4] SHI Y, SHEN H. Anomaly detection for network flow using immune network and density peak [J]. International Journal of Network Security, 2020, 22 (2): 337 - 346.

[5] HUSSAIN M, REN J, AKRAM A. Classification of DoS attacks in wireless sensor network with artificial neural network [J]. International Journal of Network Security, 2020, 22 (3): 542 - 549.

[6] ZHAO D, WANG H, GENG S. Compound attack prediction method based on improved algorithm of hidden Markov model [J]. Journal of Web Engineering, 2020, 19 (7/8): 1213 - 1237.

[7] RAGHUNATH K M K, KUMAR V V, VENKATESAN M, et al. XGBoost regression classifier (XRC) model for cyber attack detection and classification using inception V4 [J]. Journal of Web Engineering, 2022, 21 (4): 1295 - 1321.

[8] 王 婷，王 娜，崔运鹏，等. 基于半监督学习的无线网络攻击行为检测优化方法 [J]. 计算机研究与发展，2020，57 (4)：791 - 802.

[9] 展 鹏，陈 琳，曹鲁慧，等. 基于特征符号表示的网络异常流量检测算法 [J]. 浙江大学学报 (工学版)，2020，54 (7)：1281 - 1288.

[10] ZHAO X, HUANG G, MOUSOLI R. A multi-threading solution to multimedia traffic in NIDS based on hybrid genetic algorithm [J]. International Journal of Network Security, 2020, 22 (3): 427 - 436.

[11] CHEN Y, CHEN Y. A network flow correlation method based on chaos theory and principal component analysis [J]. International Journal of Network Security, 2020, 22 (2): 242 - 249.

[12] GAYATHRI M, MALATHY C. A deep learning framework for intrusion detection and multimodal biometric image authentication [J]. Journal of Mobile Multimedia, 2022, 18 (2): 393 - 419.

[13] MO L, ZHOU Y. Small area purification and recognition of network intrusion signals based on the second-order matching filter detection [J]. International Journal of Internet Protocol Technology, 2022, 15 (1): 1 - 7.

[14] WANG Y, JIANG Y, LAN J. Intrusion detection using few-shot learning based on triplet graph convolutional network [J]. Journal of Web Engineering, 2021, 20 (5): 1527 - 1552.

[15] REKHA P M, SHAHAPURE N H, PUNITHA M, et al. Water moth search algorithm-based deep training for intrusion detection in IoT [J]. Journal of Web Engineering, 2021, 20 (6): 1781 - 1811.

[16] CHEN J, CHEN Y, ZHENG H, et al. MGA: momentum gradient attack on network [J]. IEEE Transactions on Computational Social Systems, 22021, 8 (1): 99 - 109.

[17] MANOKARAN J, VAIRAVEL G. An empirical comparison of machine learning algorithms for attack detection in internet of things edge [J]. ECS Transactions, 2022, 107 (1): 2403 - 2417.

[18] LI L, YANG H, XIA Y, et al. Attack detection and distributed filtering for state-saturated systems under deception attack [J]. IEEE Transactions on Control of Network Systems, 2021, 8 (4): 1918 - 1929.

(下转第 298 页)