命名数据网络中基于WEASEL算法的协同Interest包泛洪攻击检测方法

邢光林,黄英
(中南民族大学 计算机科学学院,武汉 430074)

摘 要 兴趣包泛洪攻击(IFA)是命名数据网络(NDN)中一种典型的分布式拒绝服务攻击,而协同兴趣包泛洪攻击(CIFA)在IFA的基础上改变了攻击模式并且得到了协同生产者的辅助,比IFA更具隐蔽性和危害性.借鉴时间序列分类思想,提出了一种基于WEASEL算法的CIFA检测方法,通过对网络流量时间序列进行预测分类来检测CIFA.仿真结果表明:所提方法可以有效检测CIFA,并在误报率和漏报率方面具有良好的效果.

关键词 命名数据网络;协同兴趣包泛洪攻击;WEASEL算法;时间序列分类
中图分类号 TP393 **文献标志码** A **文章编号** 1672-4321(2025)05-0647-07
doi:10.20056/j.cnki.ZNMDZK.20250510

WEASEL-based method to detect against Collusive Interest Flooding Attack in Named Data Network

XING Guanglin, HUANG Ying
(College of Computer Science, South-Central Minzu University, Wuhan 430074, China)

Abstract Interest Flooding Attack (IFA) is a typical distributed denial-of-service attack in Named Data Network (NDN), and Collusive Interest Flooding Attack (CIFA) changes the attack mode on the basis of IFA and is assisted by co-producers, which is more stealthy and harmful than IFA. Based on the idea of time series classification, a CIFA detection method based on WEASEL algorithm is proposed, which detects CIFA by predicting and classifying network traffic time series. The simulation results show that the proposed method can effectively detect CIFA and has good results in false alarm rate and missed alarm rate.

Keywords Named Data Network; Collusive Interest Flooding Attack; WEASEL algorithm; time series classification

信息中心网络(Information-Centric Networking, ICN)[1]作为未来互联网体系结构之一逐渐得到国内外众多研究学者的关注,其中命名数据网络(Named Data Networking, NDN)[2]因在信息交互、数据存储等方面具有的特点被认为是ICN中最具代表性的解决方案之一[3].

在NDN中,数据信息的内容名称作为数据交互的唯一标识,代替了IP协议中的地址信息.NDN中存在两种数据包,Interest包和Data包,当用户想获取特定数据时,首先生成一个含有待获取数据名称的Interest包并发送到网络中,经过NDN路由器的转发,到达拥有这个数据的路由器或内容服务器(内容生产者),内容生产者将相应数据封装在Data包中并原路返回至用户.NDN路由器内部有三种数据结构.分别是用于提供数据缓存功能的内容存储表CS、用于记录路由器接收并已经成功转发的Interest包信息的待定兴趣表PIT和用来记录请求包在路由器之间的转发规则的转发信息表FIB.

在NDN中存在一种分布式拒绝服务攻击,即兴趣包洪泛攻击(Interest Flooding Attack, IFA)[4]. 在

收稿日期 2024-03-03 **通信作者** 黄英,研究方向:命名数据网络与信息安全,E-mail:2021110284@mail.scuec.edu..cn
作者简介 邢光林(1972-),男,副教授,博士,研究方向:移动计算与分布式系统、信息安全,E-mail:glxing@scuec.edu.cn
基金项目 国家自然科学基金资助项目(62372479)

IFA中,攻击者通过不断向NDN中注入大量虚假Interest包从而导致PIT持续过载而不能为正常请求提供服务.使得NDN网络服务质量不能得到保障.为了增加攻击的隐蔽性,近年来,一种称为协同Interest包泛洪攻击(Collusive Interest Flooding Attack,CIFA)被提出,CIFA利用协同内容生产者辅助攻击,因而比IFA更加隐蔽,也更难被检测.在CIFA中,攻击者周期性发动攻击,并在攻击周期的短时间内创造大量的恶意Interest包注入网络,大量占用有限的PIT资源,当恶意Interest包的PIT条目即将到期时,协同内容生产者会生成相应的协同Data包,对恶意Interest包进行响应,释放占据的PIT空间.下一轮CIFA中,刚刚释放的空间将再次被填充,导致PIT间歇性过载,正常用户无法请求新的数据内容,从而使得网络服务质量下降,严重危害NDN网络安全.

1 相关工作

鉴于CIFA的危害,其检测与缓解方法已被NDN网络安全领域列为重点研究课题.COMPAGNO等人[5]提出了Poseidon方法来检测IFA,该方法通过监测路由器特定接口的Interest包满意度以及该接口在PIT中相应的条目数量来判断是否发生攻击.而在CIFA中协同生产者会对攻击者发出的恶意Interest包进行延迟响应,导致基于简单统计Interest包满意度或者PIT条目数的检测方法在CIFA中不能发挥良好的效果.XIN等人[6]通过监测内容请求的异常分布,提出了一种基于累积熵的新型IFA检测方法,通过分析Interest包名称的分布随机性来发现是否存在攻击.CHEN等人[7]利用Interest包的前缀分布情况设计了一种基于隔离林(IForest)算法的IFA检测机制.该机制通过多个指标来划分正常前缀和异常前缀,再根据PIT的占用率从异常前缀中检测到恶意前缀.霍红等人[8]在此基础上提出基于扩展隔离林算法的IFA检测机制,在异常前缀种类的检测上进行了改进.以上通过请求内容分布情况的检测方法受制于请求内容的种类和复杂度,而CIFA中攻击者请求的数据内容种类多而杂,因此,这些方法在CIFA检测上效果不太理想.

XIN等人[9]在2017年首次提出了CIFA的概念,并使用小波分析来检测CIFA.通过对网络流量状况进行小波变换转换进行检测,然而该方法容易造成误判漏判.SALAH等人[10]提出了一种针对CIFA的通用防御机制CoMon,通过设置监控路由器构成一种应用在NDN的协调框架,可以在早期使用少数路由器检测到并减轻攻击,然而该方法需要固定路由器的位置.CHENG等人[11]提出了非参数CUSUM算法,该算法对所涉及的流量进行实时统计分析,提出了一种利用所有名称前缀的平均响应时间值的缓解算法.该算法使用兴趣包和数据包之间的频繁差异作为识别攻击的指标.该方法可能具有一定局限性.LIU等人[12]提出了一种基于预测误差的CIFA检测方法,通过估计值和预测值之间的误差与设置阈值比较来判断网络状态.该方法缺少相应的防御措施.WU等人[13]提出了一种基于PIT空间管理的轻量级防御方案,采用基于滚动时间窗和置信区间相结合的方法来实现异常网络检测.该方案利用网络流量和PIT条目的相对状态来监控网络是否受到攻击.SHIGEYASU等人[14]提出使用PIT溢出状态、传入利率和缓存引用数三个阶段进行检测.通过计算中继路由器上的缓存引用数量来检测基于CIFA的安全攻击,该方法只在二叉树结构上进行了使用.

综上,由于CIFA只在攻击周期的攻击时间内进行短时间的快速攻击以及协同生产者辅助攻击的特点,CIFA的攻击更具隐蔽性,也更难检测.以往基于统计数据设置阈值的方式对于CIFA的检测存在局限,因此有必要从网络流量变化情况来判断网络状态.本文借鉴时间序列分类算法(Word ExtrAction for time SEries cLassification,WEASEL),提出一种基于WEASEL算法[15]的协同Interest包泛洪攻击检测方法(WEASEL based CIFA detection method,WCDM).该方法将网络流量视为一种时间序列,WCDM方法通过收集的正常和异常的网络流量时间序列数据,将提取的网络流量时间序列分类为正常或异常流量,然后预测网络状态并判断其是否正常,而异常流量代表着CIFA攻击.WCDM方法的实质是通过二分类进行攻击检测.实验通过异常检测率、误报率(False alarm rate,FAR)以及漏报率(Missed alarm rate,MAR)来衡量方法性能.实验结果表明,WCDM方法具有较好的性能,且在检测的FAR和MAR方面具有优势.

2 WCDM方法

WCDM方法是基于字典结构的时间序列分类

算法[16]，这类算法整体流程通常如下：首先将网络流量时间序列转换为符号序列，在网络流量时间序列上移动滑动窗口，并提取每个窗口的特征，随后将其输入机器学习分类器. WCDM方法的特点是基于具体数据集的类特征导出判别特征，采用不同的窗口长度. 这样可以尽可能避免特征在所有类别中都同样频繁，同时通过提取多个窗口长度的特征并将所有结果特征连接到一个特征向量中来保留序列的局部顺序，从而对时间序列模式的变化更加敏感，因而可以产生出更便于区别的特征集. 使用WCDM方法检测CIFA攻击是通过分析提取的网络流量特征，将攻击检测视为对网络流量特征进行分类，通过区分网络状态是属于“正常”类还是“异常”类，“异常”类代表着CIFA攻击，由此判断每个时刻的网络状态.

如图1所示，WCDM方法具体步骤如下：首先需要将网络流量时间序列转换为具有鉴别性的符号特征表示即图1中的Discriminative words. 将收集到的NDN网络流量时间序列原始数据转换生成时间序列的低维表示，原始数据中包含正常网络状态和CIFA攻击状态下的数据，比如以PIT占用率的使用情况为例，因为正常网络状态和CIFA攻击状态下的PIT占用率情况不同，初步得到的对应特征words也就不同；再将初步选取的特征words进行再次选取，以便从众多的特征中选出最具区分度的特征即图1中的Discriminative features，最后将选出的特征送入分类器达到攻击检测的目的. 通过在网络流量时间序列上移动滑动窗口Windowing进行特征提取，再将提取出来的各个不同长度的滑动窗口数据进行归一化，从归一化时间序列中提取的子序列完全模拟正态分布[17]. 然后对每一个归一化后的滑动窗口数据进行傅里叶变化(Fourier transform)，得到对应的傅里叶系数，其中傅里叶变化的公式为：

$$f(z_1)=\frac{1}{\sigma\sqrt{2\pi}}\cdot e^{\frac{-z_1^2}{2\sigma^2}}, \tag{1}$$

傅里叶系数公式为：

$$F(t)=\int f(x)\cdot e^{-itx}=e^{i\mu\sigma}\ e^{-\frac{1}{2}(\mu\sigma)^2}=e^{-\frac{1}{2}(\sigma t)^2}, \tag{2}$$

当$\mu=0$，$\sigma=1$时得到呈正态分布傅里叶系数，μ是归一化滑动窗口数据中各个数据的均值，σ是归一化滑动窗口数据中各个数据的标准差.

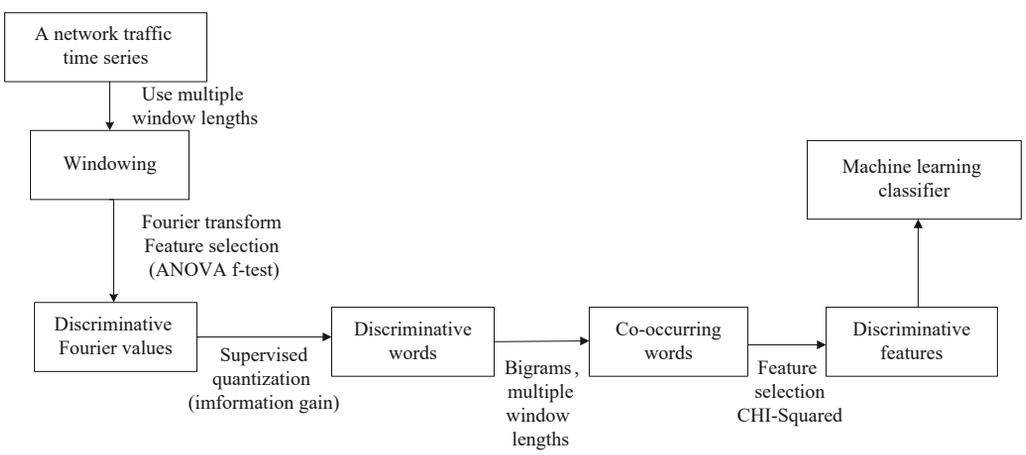

图1　WCDM方法步骤图

Fig. 1　WCDM method steps diagram

WCDM方法使用单向方差分析(Analysis of variance) F检验(ANOVA F)来选择最佳傅立叶系数，因为它适用于连续变量，单向ANOVA F检验[18]检验了两个或多个组在均值周围具有相同正态分布的假设. 最大的F值用作特征选择的一部分，即组平均值之间的巨大差异. 此步骤能使其分布能最好地将类标签分离在不相交的组中，再通过使用信息增益[19](Information gain)，使每个分区中的大多数值对应于同一个类标签. 应用量化步骤来为每个选定的实或虚傅里叶值找到最佳分割点，从而在每个分区中，大多数值对应于同一类. 值范围被划分为不相交的区域，称为区间. 每个区间都有一个符号. 落入区间的实值由其离散标签表示. 这会导致特征集不相交，便于区分.

将当前单个滑动窗口进行以上步骤将得到具有区分性的unigrams(一元分词)，将当前窗口与前一个窗口结合起来进行以上步骤将得到具有区分性的bigrams(二元分词)，它们将组成的Co-occurring words(共现词)并放入模式袋，再使用卡方($\chi 2$)检验来识别每个类中最相关的特征，以在训练

分类器之前将该特征空间减少到几百个特征.较大的χ2值意味着一个特征在特定类别中出现的频率更高.因此,需要保持那些χ2值高于阈值的特征.这突出了类之间的细微差别.所有其他特征都可以被认为是多余的,并被删除[16].提出特征后,我们可以使用分类器找到那些可以用来确定类标签的特征,区分特征进行流量分类.网络流量处于正常状态时,由于这个阶段时间序列相对平滑(即没有快速变化的模式或尖峰),所以几个子序列非常相似,很可能映射到同一个字符串.CIFA攻击时,即便是很小的攻击速度,但由于CIFA的恶意Interest包会尽可能长时间占据PIT条目的特点,在攻击周期内会周期性产生尖峰,此时提取出来的子序列就会产生新的字符串,我们以此来区分正常和异常流量.

3 仿真实验

本文以网状结构作为NDN的网络拓扑如图2所示,Interest包遵循最短路径的原则在NDN中进行信息交互.本次仿真实验中,设置两种类型的用户:合法用户与恶意用户,合法用户的数量为13,恶意用户的数量为4,NDN路由器数量为16.内容提供者数量为2,一个是正常内容提供者,另一个是协同内容提供者,也被认为是恶意生产者.其中正常内容提供者提供以"/normal/"为前缀的数据内容,协同内容提供者提供以"/evil/"为前缀的数据内容.实验参数如表1所示.

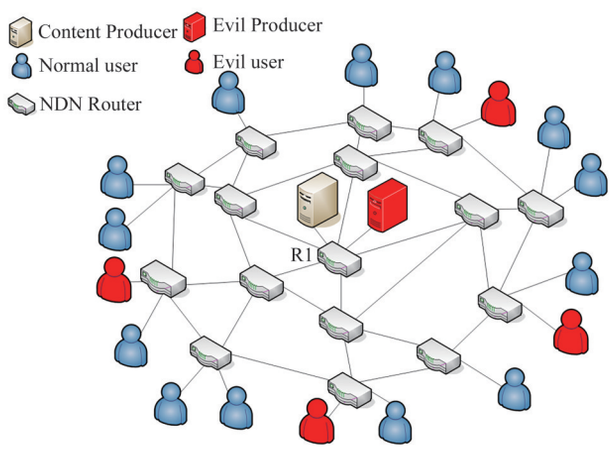

图2 网状拓扑图

Fig. 2 Mesh topology diagram

本文提取R1的网络流量来分析比较CIFA网络流量与正常网络流量.因为它最靠近服务器,处于信息交互的中心.本文的模拟实验持续200 s,正常用户的请求时间是0~200 s,CIFA攻击分别在第80 s和第160 s启动,持续40 s.其中攻击脉冲强度分别为5 packet/s、10 packet/s和50 packet/s,持续时间为1 s,攻击周期为5 s.因为PIT占用率在正常网络状态下的变化趋势与在CIFA攻击下的变化趋势具有极大不同,本文提取网络流量时间序列的PIT占用率这个特征进行分析.正常用户发送Interest包的速率为50 packet/s,在第20 s时用户将以100 packet/s的速率发送Interest包,以模拟正常情况下流量波动的情况.攻击检测周期设置为100 ms,每一跳包的传输时间是10 ms.PIT条目的生存周期为4 s,容量为200 entries.

表1 仿真实验参数

Tab. 1 Simulation experiment parameters

参数	取值
仿真时间	200 s
攻击检测周期	10 ms
用户发送Interest包的速率	50 packet/s
CIFA攻击者发送Interest包的速率	50 packet/s
每一跳包的传输时间	10 ms
PIT条目生存周期	4 s
PIT容量	200 entries

本实验设定模拟的数据请求遵循Zipf分布.从图3中可以看出,正常流量波动时,PIT占用率将会有一定程度的上涨.这是因为流量波动大都是由于对同一资源的大量请求引起的,NDN中有路由缓存机制,所以使PIT占用率产生一定的波动,但正常流量波动带来的PIT占用率的变化规律明显不同于CIFA攻击.CIFA攻击会使时间序列的表现模式出现快速变化,且因其周期性发动攻击的特点,PIT占用率的变化上呈现出一种规律性变化,因为CIFA会尽可能长时间的占据PIT条目的特性,使得即使是5 packet/s的攻击速率,也会使PIT占用率出现明显不同于正常时的变化趋势.从图3中我们可以看出,当攻击速率越大,这种变化趋势就越明显.基于以上特点,提出使用WCDM方法来检测CIFA.WCDM方法对网络流量的PIT占用率提取特征,当攻击速率越大,经过算法提出出来的特征表现将明显区别于正常状态,也越容易被算法发现提取记录.

本实验将对PIT占用率,Interest包满意度的网络流量时间序列进行提取,将网络流量时间序列数据分为训练集和测试集,使用WCDM方法进行分类.通过生成的直方图分布可以确定网络流量时间序列数据之间的结构相似性,以此判断该时刻是否

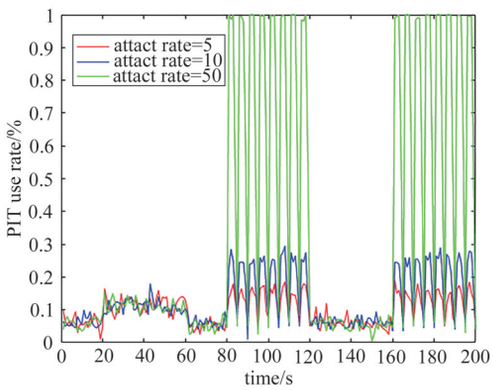

图3　PIT占用率变化趋势图

Fig. 3　PIT occupancy rate trend dhart

正在被攻击. 以PIT占用率网络流量时间序列为例，从图3可以看出，攻击状态下的PIT占用率变化趋势明显区别于正常状态下，这是因为CIFA攻击会导致原本平稳的时间序列数据发生快速变化，从而产生易于区分的特征. 图4的(a)、(b)中展示了使用不同窗口长度所捕捉到的特征. 所描述的数据集包含两个类：0类和1类，0类代表正常网络状态，1类代表攻击状态. 以攻击速率为5 packet/s的情况为例，横轴为算法提取的特征名，纵轴为该特征出现的频次. 网络流量时间序列的PIT占用率在正常状态与异常状态被算法捕捉出来的各项特征不同，在各项特征上也有着不同的频次表现. 从图中可以看出，两类特征的区别较为明显，图4(a)显示“5aab abb”是0类pit占用率正常情况下的特征，“15aab”是1类攻击时的特征. 特征“5aab”和“5aab aab”两类都有出现，但明显攻击时出现的频次要高于正常情况. 因为WEASEL是基于具体数据集的类特征导出判别特征，所以不同攻击速率所产生的数据集经过算法处理后会生成不同的特征表现. 从图3中可以看出，攻击速率为50 packet/s时PIT占用率波动程度大于攻击速率为5 packet/s，从图4中可以看到经算法处理后的正常状态与攻击状态时的特征表现. 在图4(b)中，因为攻击速率达到50 packet/s，虽与正常用户请求速率等同，但为CIFA中攻击Interest包被协同内容提供者延迟满足的特点，PIT占用率的变化十分明显，攻击时会占据PIT的大部分条目空间. 经过WEASEL处理后，两类的特征十分明显，便于区分. 例如特征“5 aaa aab”是0类特征，“5 baa”是1类特征，特征“5 aaa aaa”虽然0类和1类都有，但从图中明显能发现1类的频次达到了7，而0类的频次为2，另外特征“15 aaa”两类的频次均为1.

综上所述，经过算法处理后正常状态与异常状态两个类的特征明显不同，便于分类器分类，因而该算法在CIFA的检测上具有一个良好的效果.

为了验证WCDM方法的有效性，本文将此方法与其他三个具有代表性的防御方法进行比较，这三种方法分别为：小波分析(Wavelet Analysis)[8]、隔离林(IForest)[7]、基于累积熵和相对熵的IFA防御方法[6]. WCDM方法通过提取的特征把网络流量分为两类，针对此次数据集，以PIT占用率该特征作为输

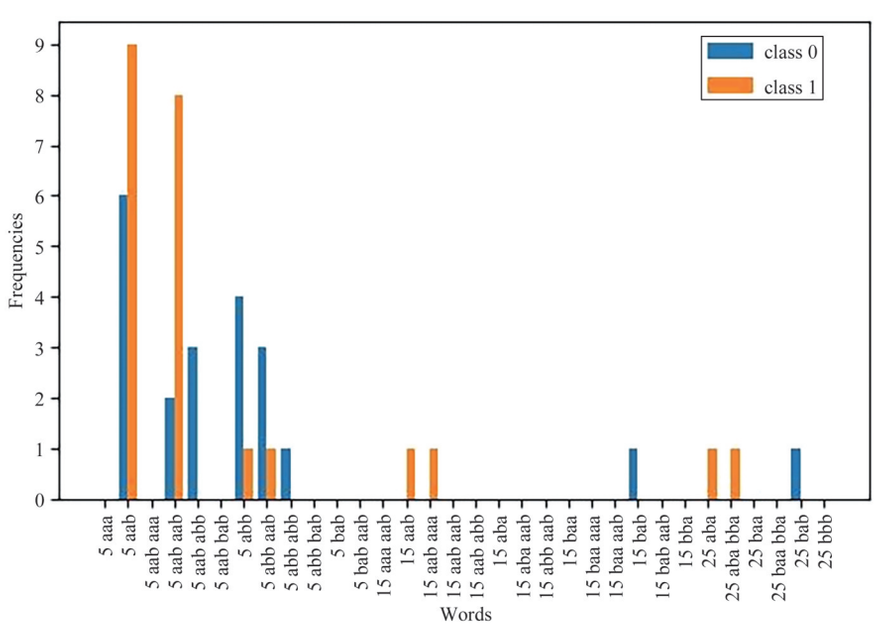

图4(a)　攻击速率为5packet/s时使用WCDM方法提取的PIT占用率

Fig. 4(a) The PIT occupancy rate extracted using the WCDM method when the attack rate is 5 packets/s

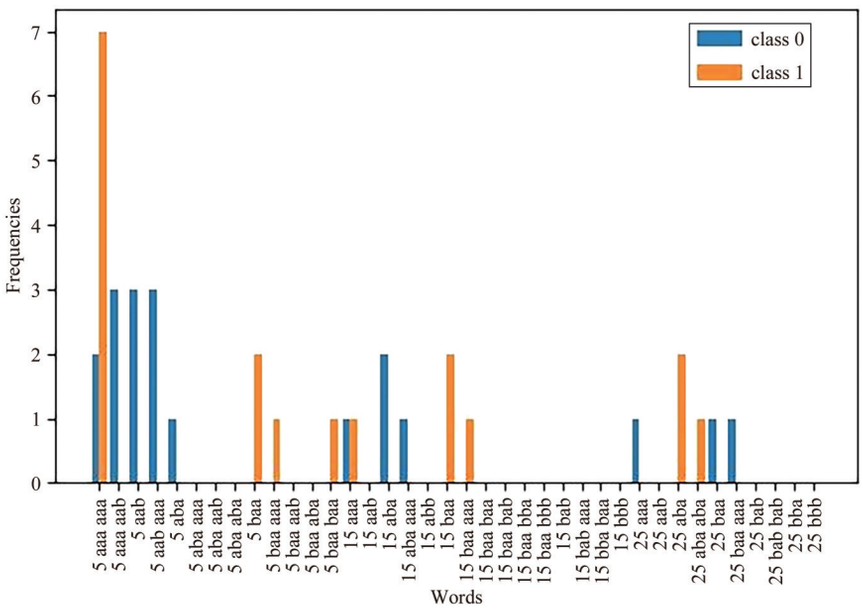

图4(b) 攻击速率为50 packet/s时使用WCDM方法提取的PIT占用率

Fig. 4(b) The PIT occupancy rate extracted using the WCDM method when the attack rate is 50 packets/s

入,比较结果如表2所示,WCDM方法的检测率是98.73%,高于其他三种检测算法.此外,WCDM方法还具有一个较小的FAR是0.82%和MAR是1.27%.进一步证明了WCDM方法在CIFA检测方面具有更好的检测性能.其中小波分析的检测效果最好,为87.23%,但同时有着较高的漏报率和误报率,而IForest和累积熵的方法检测效果不理想,在检测的FAR和MAR方面会产生较大的误差.这是因为CIFA的协同内容生产者辅助攻击,会对恶意兴趣包延时响应,从而导致单纯基于数值统计的方法不再具有良好效果.

表2 实验结果与小波变化、IF、基于累积熵的比较

Tab. 2 Comparison of the experimental results of WCDM of wavelet analysis, IForest, and the method based on cumulative impurity /%

Algorithm	WEASEL algorithm	Wavelet Analysis	IForest	Cumulative Impurity
Detection rate	98.73	87.23	54.38	51.2
FAR	0.82	14.59	37.42	33.5
MAR	1.27	12.57	34.89	32.29

4 结语

本文提出了基于WEASEL算法的CIFA检测方法——WCDM,该方法引入时间序列分类的思想,通过训练学习网络流量时间序列数据的特点,将网络流量时间序列数据分为正常网络流量状态以及CIFA攻击状态,以分类的方式进行攻击检测,再通过检测率,漏报率和误报率检测分类的正确性.并通过仿真实验证明了该方法的有效性.在未来的工作中,计划在更加复杂的攻击情况下开展研究.

参 考 文 献

[1] 孙彦斌, 张宇, 张宏莉. 信息中心网络体系结构研究综述[J]. 电子学报, 2016, 44(8): 2009-2017.

[2] SAXENA D, RAYCHOUDHURY V, SURI N, et al. Named data networking: A survey[J]. Computer Science Review, 2016, 19: 15-55.

[3] 吴超, 张尧学, 周悦芝, 等. 信息中心网络发展研究综述[J]. 计算机学报, 2015, 38(3): 455-471.

[4] JACOBSON V, SMETTERS D K, THORNTON J D, et al. Networking named content[C]//Proceedings of the 5th international conference on Emerging networking experiments and technologies. Rome:ACM, 2009: 1-12.

[5] COMPAGNO A, CONTI M, GASTI P, et al. *Poseidon*: Mitigating interest flooding DDoS attacks in Named Data Networking[C]//38th Annual IEEE Conference on Local Computer Networks. Sydney:IEEE, 2013: 630-638.

[6] XIN Y, LI Y, WANG W, et al. A novel interest flooding

attacks detection and countermeasure scheme in NDN [C]//2016 IEEE Global Communications Conference (GLOBECOM). Washington: IEEE, 2016: 1-7.

[7] XING G, CHEN J, HOU R, et al. Isolation forest-based mechanism to defend against interest flooding attacks in named data networking [J]. IEEE Communications Magazine, 2021, 59(3): 98-103.

[8] 邢光林，霍红，侯睿. 命名数据网络中基于增强隔离林的Interest包洪泛攻击检测方法[J]. 中南民族大学学报(自然科学版)，2023，42(4)：477-481.

[9] XIN Y, LI Y, WANG W, et al. Detection of collusive interest flooding attacks in named data networking using wavelet analysis[C]//MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM). Baltimore: IEEE, 2017: 557-562.

[10] SALAH H, STRUFE T. Evaluating and mitigating a Collusive version of the Interest Flooding Attack in NDN [C]//2016 IEEE Symposium on Computers and Communication (ISCC). Messina: IEEE, 2016: 938-945.

[11] CHENG G, ZHAO L, HU X, et al. Detecting and mitigating A sophisticated interest flooding attack in NDN from the network-wide view[C]//2019 IEEE First International Workshop on Network Meets Intelligent Computations (NMIC). Dallas: IEEE, 2019: 7-12.

[12] LIU L, FENG W, WU Z, et al. The detection method of collusive interest flooding attacks based on prediction error in NDN[J]. IEEE Access, 2020, 8: 128005-128017.

[13] WU Z, FENG W, YUE M, et al. Mitigation measures of collusive interest flooding attacks in named data networking[J]. Computers & Security, 2020, 97: 101971.

[14] SHIGEYASU T, SONODA A. Detection and mitigation of collusive interest flooding attack on content centric networking[J]. International Journal of Grid and Utility Computing, 2020, 11(1): 21-29.

[15] SCHÄFER P, LESER U. Fast and accurate time series classification with WEASEL [C]//Proceedings of the 2017 ACM on Conference on Information and Knowledge Management. Singapore: ACM, 2017: 637-646.

[16] ISMAIL FAWAZ H, FORESTIER G, WEBER J, et al. Deep learning for time series classification: A review[J]. Data Mining and Knowledge Discovery, 2019, 33(4): 917-963.

[17] LIN J, KEOGH E, LONARDI S, et al. A symbolic representation of time series, with implications for streaming algorithms[C]//Proceedings of the 8th ACM SIGMOD workshop on Research issues in data mining and knowledge discovery. San Diego: ACM, 2003: 2-11.

[18] LOWRY R. Concepts and applications of inferential statistics [J/OL]. (2014-05-05) [2024-02-21] http://vassarstats.net/textbook/ch14pt1.html.

[19] QUINLAN J R. Induction of decision trees[J]. Machine Learning, 1986, 1(1): 81-106.

（责编&校对　雷建云）