IPv6网络中基于MF-DL的DDoS攻击快速防御机制

丑义凡[1)] 易 波[2)] 王兴伟[2)] 贾 杰[2)] 黄 敏[3)]

[1)](东北大学软件学院, 沈阳 110169)

[2)](东北大学计算机科学与工程学院, 沈阳 110169)

[3)](东北大学信息科学与工程学院, 沈阳 110819)

摘 要 当前,分布式拒绝服务(Distributed Denial of Service, DDoS)攻击是互联网面临的十分严峻的安全威胁之一. IPv6网络考虑了IPv4网络中的诸多安全问题,但它对DDoS攻击仍未能起到很好的防护作用. 针对IPv6网络中DDoS攻击的防御问题,本文设计了一种基于MF-DL (Membership Function and Deep Learning)的DDoS快速防御机制. 该防御机制以MF-DL检测机制为核心,辅以响应机制等实现对DDoS攻击的防御功能. 在检测机制中,首先使用基于隶属度函数的预检测方法,实现对网络流量数据的轻量级异常检测;接着通过基于深度学习方法中神经网络模型的深度检测,实现在异常发生后对流量进行高精度分类. 在响应机制中,利用Anti-Fre响应算法实现对请求访问的IP地址进行信誉等级划分,进而实现流量定向阻断并恢复系统性能. 最后,分别基于经典入侵检测数据集和校园网的模拟攻击数据集对本文提出的防御机制进行了实验. 结果显示,本文提出的防御机制相比于三种对比算法,检测准确率可提高6.2%,误报率和漏报率可降低6.75%、8.46%,且能够有效处理攻击并恢复部分系统性能.

关键词 DDoS攻击;IPv6网络;入侵检测;攻击防御机制;深度学习;隶属函数

中图法分类号 TP393 **DOI号** 10.11897/SP.J.1016.2021.02047

A Rapid Defense Mechanism Based on MF-DL for DDoS Attack in IPv6 Networks

CHOU Yi-Fan[1)] YI Bo[2)] WANG Xing-Wei[2)] JIA Jie[2)] HUANG Min[3)]

[1)](*Department of Software, Northeastern University, Shenyang* 110169)

[2)](*Department of Computer Science and Engineering, Northeastern University, Shenyang* 110169)

[3)](*Department of Information Science and Engineering, Northeastern University, Shenyang* 110819)

Abstract At present, the Distributed Denial of Service (DDoS) attack is still one of the most serious security threats to the Internet. The core of IPv6 networks is to solve the problem of IP address resource exhaustion. At the same time, IPv6 networks also have considered many security issues in IPv4 networks, such as the use of IPsec (Internet Protocol Security) protocol. However, IPv6 networks still follow the mechanism of data packets routing, which makes it still fail to play a good role in the protection against DDoS attacks. Aiming at the defense of DDoS attacks in IPv6 networks, this paper designs a fast defense mechanism based on MF-DL

收稿日期:2020-04-21;在线发布日期:2021-01-09. 本课题得到国家重点研发计划项目(2017YFB0801701)、国家自然科学基金(61872073,61772126)和辽宁省"兴辽英才计划"资助项目(XLYC1902010)资助. **丑义凡**,硕士研究生,主要研究领域为DDoS攻击防御、IPV6安全. E-mail: chouyf133@163.com. **易 波**,博士,讲师,主要研究领域为服务计算和路由. **王兴伟**(通信作者),博士,教授,国家杰出青年科学基金获得者,中国计算机学会(CCF)高级会员,主要研究领域为未来互联网、云计算和网络安全. E-mail: wangxw@mail.neu.edu.cn. **贾 杰**,博士,教授,主要研究领域为5G网络、物联网与大数据分析. **黄 敏**,博士,教授,主要研究领域为供应链物流管理、智能决策与调度优化.

(Membership Function and Deep Learning). The whole detection mechanism is divided into four parts: infrastructures, the traffic collector, the MF-DL detection mechanism, and the response mechanism. Among them, infrastructures as the basic equipment are the hardware basis of the defense mechanism. The traffic collector realizes the functions of traffic collection, filtering and processing. The MF-DL detection mechanism is the core of the defense mechanism to realize the specific detection function of DDoS attacks. The response mechanism complements the MF-DL detection mechanism, manages the blacklist according to the detection results and realizes the traffic filtering function. The MF-DL detection mechanism is divided into two parts: the MF (Membership Function) pre-detection algorithm and the DL (Deep Learning) deep detection algorithm. Based on the pre-detection model of entropy measurement and membership function, the MF pre-detection algorithm calculates the traffic scale and traffic chaos degree of current network traffic and realizes lightweight anomaly detection at the traffic volume level. When the MF pre-detection algorithm detects that the current network traffic scale is abnormal, it means that there is a suspected DDoS attack. So, the DL deep detection is carried out. The DL deep detection algorithm realizes misuse detection based on the neural network classification model of deep learning methods. After feature extraction of historical attack traffic, the traffic feature set is used to train the neural network, and the trained model is used for attack detection later. After each attack, the training set is updated and the neural network classification model is retrained. In the response mechanism, the Anti-Fre response algorithm realizes the classification of the reputation of the requested IP address. When an attack is detected, the reputation level of the traffic IP addresses can be adjusted to achieve the function of directional blocking of traffic and the recovery of system performance. Finally, experiments are carried out on the defense mechanism proposed in this paper based on the classic intrusion detection data set and the simulated attack data set of the campus network. The results show that compared with the three comparison algorithms, the defense mechanism proposed in this paper can increase the detection accuracy by 6.2%, and reduce the false alarm rate and false alarm rate by 6.75% and 8.46%, and the experimental verification of the system load proves that the defense mechanism proposed in this paper can effectively deal with attacks and restore system performance in a short time.

Keywords DDoS attack; IPv6 networks; intrusion detection; attack defense mechanism; deep learning; membership function

1 引 言

近年来,随着互联网规模的大幅增长,DDoS攻击的频率和范围不断增加,一般的大型商业网络公司和国家政府部门均成为了DDoS攻击者的目标.发起简单、效果显著等特性,使得DDoS攻击成为了目前网络安全领域迫切需要解决的威胁之一.

目前DDoS的主要攻击目标为目标主机的系统资源和带宽资源.针对协议和应用程序缺陷,攻击者将数据包发送到一些随机或指定的端口,使网络资源饱和,达到攻击的目的,并通过UDP泛洪、ICMP泛洪耗尽网络带宽.其他诸如SYN泛洪、SIP泛洪攻击则会耗尽受害者的系统资源(例如CPU,内存等).但随着服务器技术的提升,针对系统资源的DDoS攻击效果明显减弱.然而,由于网络基础架构本身的问题,针对网络带宽的攻击仍较为容易实现.而且在IP欺骗、网络放大器、反射器等技术的加持下,攻击效果得以大幅提升.

IPv6网络的出现并未对现有网络体系结构进行根本性的改变,基于数据报文路由的网络传输机理与IPv4网络仍然相同,这意味着类似于IPv4网络下的安全威胁依旧存在.即使在IPv6网络下,利用内置的IPsec协议可以防范例如反射型泛洪DDoS攻击,但是它的使用并不强制,一些直接型泛洪攻击仍然有效.针对IPv6网络的未知类型的DDoS攻击

随时都可能出现，让已有的防御机制猝不及防.

关于DDoS攻击检测问题常见的解决方案是通过网络状态的异常或流量变化的异常来判断是否发生攻击.一些研究者多是从流量的状态入手，例如在攻击发生时，通过网络流量的熵特性进行攻击检测[1].通过构建具有不同特征的熵向量，使用聚类分析算法对正常模式进行建模，然后从所创建的模型中检测出偏差；基于网络熵、协同聚类、信息增益比等方法对数据流量进行特征提取再进行检测分类被证明是效果较好的[2].

Geoffrey Hinton教授等人于2006年提出深度学习(Deep Learning)的概念[3].由于计算硬件的快速发展、算法的不断优化等原因，使得深度学习成为了从事聚类、分类模型应用的相关研究人员高度关注的话题，其技术优势得到广泛认可.在网络流量异常检测模型中，使用基于流量的统计特征和一般机器学习的检测算法，在小规模数据集和较少攻击向量的基础上检测效果较好，但仍依赖于人工对有效参数的总结和提取，在大规模数据集和特征参数较多的情况下，很难产生有效的分类和预测.而深度学习具有的多隐层核心，支持采用浅层特征参数表示复杂客体，在检测模型构建上可降低成本，同时保证较高的检测精度.

未来，我国会继续加速IPv6网络的商用发展，其广泛应用的时代终会到来，DDoS会继续存在于IPv6网络中危害网络安全.深度学习技术快速发展，其对特征学习的技术优势显而易见.在这样的背景下，本文设计并实现了IPv6网络中基于MF-DL的DDoS攻击快速防御机制.通过将核心功能MF-DL检测机制和响应机制结合，实现对DDoS攻击的快速防御功能.利用检测机制中的预检测算法进行可疑攻击感知，利用深度检测算法对攻击特征进行检测、识别和学习.在不干扰正常流量的处理与转发的情况下，对网络流量中已知类型和未知类型的DDoS攻击行为进行检测，并通过响应算法进行轻量级的处理，在一定程度上减缓攻击并恢复系统性能.

本文结构如下：第2部分简述DDoS攻击检测方面的研究现状；第3部分介绍DDoS攻击快速防御机制的系统框架；第4部分详细介绍基于MF-DL的防御机制的具体设计，包括检测机制、响应机制以及全局防御算法；第5部分详细阐述本文提出的快速防御机制的实验和性能评价；第6部分对本文工作进行了总结.

2　相关工作

当前，国内外DDoS攻击检测的研究从不同的检测思路入手，比如将流量特征与从网络流量数据获得的通信特征相结合，可以更加全面地描述网络状态和行为.根据这种思路Ye S等人提出了一种新的用于流量特征提取的动态度量方法，可以在异常检测中更好地分析网络行为[4].在流量特征提取的基础上，David J等人认为抽象网络数据报文的流级特征比单纯的包级特征更能体现攻击行为[5].而这种基于流级特征的思路也被Ahmed M E等人采用，包级检测侧重于快速生成普通配置文件，而流级检测在检测攻击流量方面起着重要作用，通过二者结合可以更好地检测DDoS攻击[6].

相关研究证明，在实时环境中利用深度学习的神经网络模型对已知和未知的攻击进行检测和缓解是完全可行的[7].Elejla O E等人的工作证明了IPv4网络中处理入侵检测领域问题而使用到的机器学习的算法效率是较好的，它能够提供高检测精度，并且部署更容易，成本更低[8].Chen Zhang等人提出的新型DDoS特征表示模型利用深度信念网络充分提取原始数据的特征信息，充分挖掘原始流量信息的多样性[9].相关工作也表明，深度学习方法可以用于对DDoS攻击的预测.例如Yuze S U等人提出了基于混合流量预测模型的检测算法，首先将原始流量去噪，恢复流量原本的混沌状态；再通过神经网络预测模型求得流量的变化趋势，进而判断是否出现了DDoS攻击[10].

关于IPv6网络中的DDoS防御，也有研究人员做了详细研究[11-12].IPv6中的多播地址提供了一种发起泛洪DoS攻击的简便方法[13]，基于IPv6的新功能包括发现最大路径传输单元、自动配置机制、地址解析等没有很好地处理请求主机和广告主机之间的信任.因此，恶意攻击者可以利用此漏洞发动许多类型的攻击(包括DoS和DDoS等)[14].而预防攻击的方法常基于阻止源地址欺骗，即防止地址窃取或对网络流量实施控制策略[15].

在国内，大多IPv6环境下的实验性应用都部署于高校之中，已通过实验验证了基于IPsec的IPv6校园网无法完全抵御DDoS攻击[16].Satrya G B等人在IPv6环境下根据源地址分析和网络流量分析设计了一种DDoS攻击检测原型[17]，并基于不同的测试场景验证其有效性.也有一些研究人员围绕

IPv6网络中主要的DDoS攻击类型-路由广播泛洪攻击进行了研究并取得了一定的成果[18]. 对于IPv6网络中易被利用而进行攻击的NDP(Neighbor Discovery Protocol)协议,虽然有针对性地提出SEND(Secure Neighbor Discovery)去避免对NDP的威胁,但是一些学者认为NDP和SEND的安全性问题依旧存在,而且基于协议的分析存在较大的局限性[19].

DDoS攻击防御问题中,不仅需要关注核心内容:攻击检测,也要关注于其他防御手段. Neupane R L等人则设计了名为Dolus的新型防御系统,用于减轻DDoS对云平台的影响[20]. 在第一阶段完成异常检测后,在第二阶段通过攻击特征向量来识别DDoS攻击事件,此后创建黑名单并刷新SaaS服务,将其作为低成本解决方案来清洗恶意流. Liu Z等人提出的防御机制,则通过允许用户定制业务逻辑的自利流量监管规则来阻止相关流量[21]. 一个良好的防御机制,既能在攻击出现前期及时准确地检测到攻击发生并定位攻击源,又能采取合理措施隔离或清洗流量、缓解甚至恢复网络状态,保证合法用户的业务需求[22].

综上所述,针对现有IPv4网络架构下的DDoS的防御问题,相关学者已经进行了大量工作,提出了许多检测算法或者防御架构,其中不乏被证明是效果较好的. 但IPv6因部署应用有限、实验环境较差等情况,对其DDoS攻击防御问题的研究仍停留在初级阶段. 与此同时,大量工作指出人工智能方法用于异常检测模型具有较好的前景,而且综合考虑结合多种防御策略才能带来较好的防御效果. 所以,现阶段将深度学习技术和传统检测算法相结合,用于解决IPv6网络环境下的DDoS攻击防御问题是具有实际意义的.

3 防御机制系统框架

IPv6网络中基于MF-DL的DDoS攻击快速防御机制的系统框架设计如图1所示. 整个框架分为四部分:基础设备、流量收集器、MF-DL检测机制、响应机制.

基础设备为IPv6网络拓扑中防御节点的路由器或三层交换机,该设备为流量收集器和防御机制提供底层的数据依赖(IP报文). 该设备的网络流量的前向流向为防御机制所监控的子网络.

流量收集器的功能是网络流量的收集以及流量统计特征的提取. 流量收集器部署于具有光纤网卡的服务器上,和交换机以及业务主机相连,通过基础设备配置端口镜像功能. 流量收集器获得流经基础设备的IP报文,通过tcpdump实现流量的采集和统计,得到防御系统中检测机制所需的流量统计参数,发送至业务服务器用于MF-DL机制检测攻击.

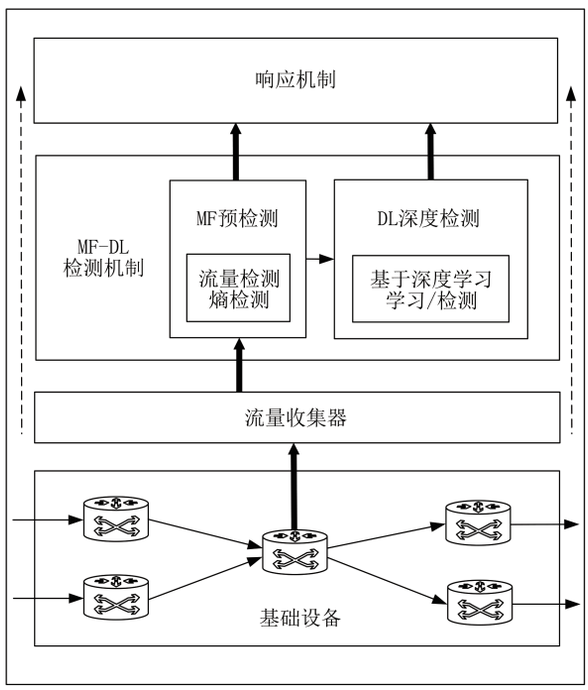

图1 系统框架

基于MF-DL的DDoS攻击快速防御机制的核心内容为MF-DL检测机制和响应机制. 其中,MF-DL检测机制主要分为MF预检测与DL深度检测. MF预检测对网络中的流量规模和趋势进行粗粒度的计算并保持实时检测,以便能够发现潜在的DDoS威胁. DL深度检测使用神经网络对网络中的流量进行高精度的分类. 由于神经网络的计算会花费大量的计算资源,为确保该机制能够做到快速响应与处理,因此,只有在MF预检测发现网络异常时,才会调用DL深度检测模块进行深度检测. 响应机制包括IP地址信用名单列表及Anti-Fre响应算法. IP地址信用名单列表对防御系统检测的DDoS攻击的流量中的IP地址进行记录. 在攻击期间,Anti-Fre响应算法会对IP地址信用等级进行实时维护,并生成流量黑名单用于阻断攻击流量.

4 基于MF-DL的快速防御机制

4.1 MF-DL检测机制

4.1.1 MF预检测算法

MF预检测的功能是对网络流量进行粗粒度的

异常检测，主要检测流量规模（流量大小）和混乱程度（流量熵值），二者是在DDoS攻击中变化最为显著的统计特征量. 在防御系统开启后，MF预检测一直处于守护线程的工作状态，在固定的时间间隔内循环计算统计特征参数，在发现网络流量异常时对系统发出预警，并调用DL深度检测对当前捕获的流量进行二次检测.

流量大小和流量熵值的定义如下：设t时刻所监控的子网络的实时流量大小为$T(t)$，在该监控节点的历史流量中，$T(t)$的平均值为$T_avg(t)$. 将详细流数据中的目的IP地址的熵值作为流量熵值，设为$E(t)$，相应的$E_avg(t)$为$E(t)$的历史平均值. 为了量化网络流量的变化程度，本文通过构造隶属函数变量U_T、U_E来表示流量规模和混乱程度.

$$U_T=\begin{cases}0 & T(t)\leqslant m\times T\_avg(t)\\ \dfrac{[T(t)-m\times T\_avg(t)]^2}{[n\times T\_avg(t)-m\times T\_avg(t)]^2} & m\times T\_avg(t)<T(t)\leqslant n\times T\_avg(t)\\ 1 & T(t)>n\times T\_avg(t)\end{cases}\tag{1}$$

U_T用于表示实时流量大小的程度，计算方式如公式（1）所示. 当t时刻的流量$T(t)\leqslant m\times T_avg(t)$时，判断当前流量属于小流量情况，即流量规模较小；当$n\times T_avg(t)\geqslant T(t)>m\times T_avg(t)$，通过$U_T$计算当前流量规模的程度值，所得结果用于后续检测计算；同理，当$T(t)>n\times T_avg(t)$，则认为当前为大流量情况. m、n通过对部署节点收集的历史流量数据进行概率分布统计得出：根据历史流量基于单位时刻的统计，求出一天中时刻t的平均值μ与标准差σ. 由于网络访问的随机性，根据标准正态函数的95%置信区间，求得上阈值$\mu+2.58\sigma$与下阈值$\mu-2.58\sigma$，m和n分别为上阈值和下阈值与平均值的比值.

U_E用于表示瞬时流量混乱的程度，计算方式如公式（2）所示. 当$E(t)>y\times E_avg(t)$时，则认为当前流量较为混乱，意味着流量的流向较为分散，属于正常情况；当$y\times E_avg(t)\geqslant E(t)>x\times E_avg(t)$时，计算当前网络的混乱程度值并用于后续检测的计算；同理，当$E(t)\leqslant x\times E_avg(t)$时，则认为流量混乱程度较低，流量的方向较为集中. 同m、n的计算方式相同，x、y通过对部署节点收集的历史流量数据进行概率分布统计得出.

$$U_E=\begin{cases}1 & E(t)\leqslant x\times E\_avg(t)\\ \dfrac{[E(t)-x\times E\_avg(t)]^2}{[y\times E\_avg(t)-x\times E\_avg(t)]^2} & x\times E\_avg(t)<E(t)\leqslant y\times E\_avg(t)\\ 0 & E(t)>y\times E\_avg(t)\end{cases}\tag{2}$$

MF预检测算法的流程如算法1所示，依次通过U_T和U_E等参数来判断当前网络是否出现网络异常，进而决定是否进入下一阶段的DL深度检测.

具体过程如下：首先，由U_T判断网络当前t时刻流量规模是否属于大流量，结果为0意味着不属于大流量则本次检测结束；结果为1则说明确定当前流量为大规模，启动DL深度检测算法；结果介于0和1之间则不确定是否为大流量，需进行下一步判断.

通过连续时间窗口的流量差值判断流量规模是否持续增加，若未持续增加则检测结束，若持续增加则继续计算U_E. U_E结果为0则说明当前网络并不混乱，则检测结束；结果为1则说明当前网络混乱程度低，疑似出现攻击则进行DL深度检测；结果介于0和1之间则继续计算熵值的变化趋势.

在连续时间窗口内，若熵值持续增大，则结束本次检测，若熵值持续减小则说明网络中混乱程度降低了，流量去向更集中，更有可能发生攻击，则进行DL深度检测.

算法1.　MF预检测算法

Input: traffic size $T(t-1)$, traffic size $T(t)$, average traffic $T\_avg\ (t)$, traffic IP entropy $E(t-1)$, traffic IP entropy $E(t)$, average IP entropy $E\_avg(t)$

Output: system policy state

BEGIN

1. Calculate $U_T(t)$, Initialize *state*=0;
2. **IF** $U_T(t)$=0 **THEN**
3. Break;
4. **ELSE IF** $U_T(t)$=1 **THEN**
5. start DL detection;
6. Break;
7. **ELSE** Calculate $T(t)-T(t-1)$
8. **IF** $T(t)-T(t-1)<0$ **THEN**
9. Break;

```
IF U_E(t)=0 THEN
    Break;
ELSE IF U_E(t)=1 THEN
    start DL detection;
    Break;
ELSE Calculate E(t)−E(t−1)
    IF E(t)−E(t−1)>0 THEN
        Break;
    ELSE start DL detection;
END
```

4.1.2 特征统计参数

当MF预检测发现网络中疑似出现攻击，则执行DL深度检测. 神经网络模型对历史流量特征的数据集进行训练，在DL深度检测开始后，将当前流量特征输入模型输出检测结果.

特征统计参数提取主要包括网络流量中的五元组信息，为了补充网络中的其他信息，还在网络中提取了流速相关特征，并且在包头信息中提取了标志位相关特征来区分闪拥流量和攻击流量. DL检测中用于判断是否出现攻击的流特征统计参数如表1所示.

表1 攻击检测流量特征提取表

特征	描述
Source IP	源IP地址
Source Port	源端口
Destination IP	目的IP地址
Destination Port	目的端口
Protocol	传输协议
Total Fwd Packets	转发数据包总数
Total Backward Packets	返回数据包总数
Flow Packets/s	每秒传输包数
SYN Flag Count	SYN标志位
ACK Flag Count	ACK标志位
URG Flag Count	URG标志位
Down/Up Ratio	上传下载率
Average Packet Size	平均包大小
Avg Fwd Segment Size	平均前向转发部分包大小
Subflow Fwd Packets	子流前向转发包数
Subflow Fwd Bytes	子流前向转发字节数
Subflow Bwd Packets	子流反向转发包数
Subflow Bwd Bytes	子流反向转发字节数

4.1.3 DL深度检测

DL深度检测在MF预检测发现网络异常时进行确认检测，模块结构示意图如图2所示.

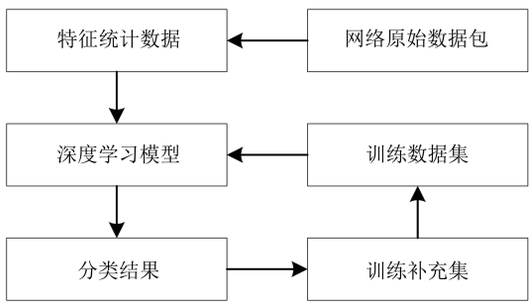

图2 DL深度检测模块结构示意图

首先，将流量采集器统计得到的特征值输入深度学习模型得到分类结果. 无论分类结果为正常还是为攻击，都在分类结束后将输入模型的数据作为补充数据重新对模型进行补充训练，以此保证模型在每次检测攻击后能够更新，在后续的检测过程中能够适应网络攻击的不断变化.

DNN网络结构采用层与层全连接的形式，以标准四层结构为例，如图3所示，第$l-1$层与第l层为全连接. 用于计算下一层输出的前向传播算法如公式(3)所示.

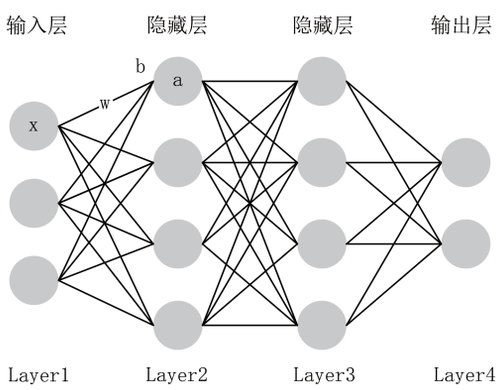

图3 DNN网络全连接结构图

其中，a^l表示第l层的n个神经元组成的向量，$\boldsymbol{a^{l-1}}$表示第$l-1$层的m个神经元组成的向量，W^l表示第$l-1$层和第l层神经元之间线性系数组成的$m*n$矩阵，b^l表示第l层的n个偏置量组成的向量. 其中，ϕ在输入层和隐藏层之间以及隐藏层彼此之间采用tanh激活函数，在隐藏层和输出层之间，ϕ采用softmax激活函数.

$$a^l=\phi\left(z^l\right)=\phi\left(W^l\boldsymbol{a}^{l-1}+b^l\right) \tag{3}$$

用于训练模型调整权重的反向传播算法如公式(4)所示，其中$\boldsymbol{W^{l+1}}$表示$l+1$层的系数矩阵，$\boldsymbol{z^l}$为第l层输出结果，$\boldsymbol{\delta^l}$表示第l层的损失函数(均方差)关于第l层输出$\boldsymbol{z^l}$的偏导数向量.

$$\boldsymbol{\delta^l}=\left(\boldsymbol{W^{l+1}}\right)^T\boldsymbol{\delta^{l+1}}\odot\phi'\left(\boldsymbol{z^l}\right) \tag{4}$$

关于DNN网络结构的设计，网络结构较为简单(层数较少、神经元个数较少)时则会出现无法学习到攻击流量中攻击IP的特殊形式，会降低识别的准确率，即普通流量行为和攻击流量并不能得到区分. 网络结构复杂(层数过大、神经元个数过多)，会导致过拟合的情况出现，在模型实际的学习过程中，微弱的波动也会被视为攻击，同样降低了攻击流量的识别率.

根据上述神经网络结构，参照DNN在分类问题上的具体应用、输入特征参数规模、数据集规模，本文所设计防御机制中DNN网络结构如下：共分为7层，分别是1个输入层(20个特征神经元)，5个隐藏层(分别包含32个神经元、64个神经元、64个神经元、128个神经元和64个神经元)，1个输出层(2个输出神经元，使用softmax分类器). 在隐藏层之间加入系数为0.25的dropout层，基于Tensorflow和Keras进行模型设计与构建，模型摘要如表2所示.

表2　模型摘要

Layer(type)	Output Shape	Param
dense_1(Dense)	(None, 20)	20
dense_2(Dense)	(None, 32)	672
dense_3(Dense)	(None, 64)	2112
dense_4(Dense)	(None, 128)	8320
dropout_1(Dropout)	(None, 128)	0
dense_5(Dense)	(None, 128)	16512
dropout_2(Dropout)	(None, 128)	0
dense_6(Dense)	(None, 64)	8256
dropout_3(Dropout)	(None, 64)	0
dense_7(Dense)	(None, 1)	65

4.2　响应机制

4.2.1　IP地址信用名单列表

响应机制维护一个IP地址信用名单列表. 该列表会在DL深度检测的结果和响应算法的共同作用下不断调整. 当检测机制执行一次检测结束后，确认该流量属于攻击流量时，系统保存该段流量的所有源IP并存储于IP地址信用名单列表，同时初始化所有IP的信誉等级为Level5.

IP地址信用名单列表结构如图4所示. 从Level0到Level5信用等级递增，Level0表示最低信用等级，Level5表示最高信用等级.

在后续的检测中，响应算法会根据检测结果，不断调整IP列表中的各个地址的信用等级.

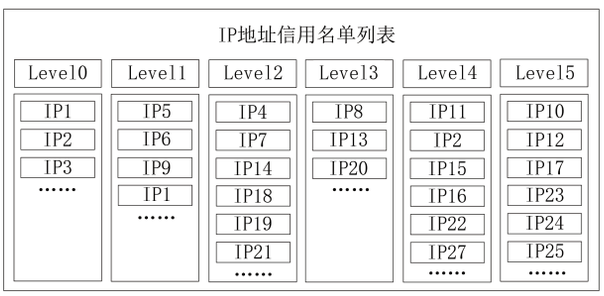

图4　IP地址信用名单列表示意图

4.2.2　Anti-Fre响应算法

响应算法根据检测结果及时对IP地址信用名单列表进行维护，调整各IP地址的信用等级，根据实时的检测结果生成黑名单列表，用于对攻击流量的拦截，及时减轻系统负载、恢复系统性能. 响应算法具体过程如算法2所示.

算法2.　Anti-Fre响应算法

Input: IP addresses set, G

Output: Level0 IP addresses set, L

BEGIN

1. For each IP from U as IP_i, i=1,2,3,…, DO
2. IF the counter of IP_i is 12t, THEN
3. increase the level of IP_i;
4. the counter of IP_i ←0;
5. ELSE
6. increase the count of IP_i;
7. For each IP from G as IP_j, j=1,2,3,…, DO
8. IF $IP_j \in U$, THEN
9. IF the level of IP_j is 0, THEN
10. the counter of IP_j ←0;
11. continue;
12. ELSE
13. decrease the level of IP_j;
14. the counter of IP_j ←0;
15. ELSE
16. $IP_j \rightarrow U$
17. the counter of IP_j ←0;
18. the level of IP_j ←5;
19. For each IP from U as IP_m, m=1,2,3,…, DO
20. IF the level of IP_m is 0, THEN
21. $L \leftarrow IP_m$;
22. RETURN L

END

集合U中包含被检测的目标为攻击流量的所有IP地址、对应IP的计数器及其级别，集合G为检测机制输出的攻击IP地址集合. 在防御机制首次检测到攻击发生后，DL深度检测算法进行周

期性的流量检测.DL检测的时间间隔过长,会影响检测到攻击的速度,太短则会导致聚合的数据具有较高的随机性,降低准确率.因此,鉴于MF预检测阶段的统计特征采用间隔为g的平均统计量,此处DL检测算法每$g/4$执行一次检测,生成结果G.

对于IP地址信用名单列表的自动维护流程如下:假定某一IP在时间t min内未再出现于攻击流量中,即counter大于等于$12t$,则此IP信用等级加1,并重置计数器.

从检测模块输入的集合G的具体操作分为两种情况:当集合G中的IP地址未出现于U中,则将此IP添加到U中并初始化;当G中IP已经存在于U中时,则该地址的信用等级减1并重置计数器(0为信用最低等级).

响应算法的每次执行都将信用等级为0的IP地址集合输出,作为黑名单列表发送给防火墙用于流量拦截.

4.3 全局防御算法

4.3.1 系统策略

在防御机制运行中,如表3所示将整个系统分为四种状态,包括:稳定状态、预警状态、防护状态和紧急状态.

表3 响应策略

系统状态	响应措施
稳定状态*state*=1	防御机制:初始化各模块、启动MF预检测
预警状态*state*=2	防御机制:启动DL深度检测 管理员:指定链路分流、增加等待队列长度
防护状态*state*=3	管理员:下发防护通知、限制接收速率
紧急状态*state*=4	防御机制:启动响应机制 管理员:调整业务能力

每种状态的响应措施对应防御机制自身的检测、响应等操作,以及对网络管理员的建议操作.

稳定状态下,防御机制正常运行,MF预检测处于工作状态.

预警状态下,系统调用DL深度检测模块,并且系统会发出警告,建议网络管理员对网络进行链路分流、增加等待队列长度等操作.

防护状态下,防御系统认为此时网络比较拥堵,可能会对系统负载产生较大压力,建议网络管理员限制接受速率.

紧急状态下,系统会立刻启用响应机制进行流量拦截,同时提醒网络管理员要做好对应的攻击冲击准备.

4.3.2 算法流程

全局防御算法主要以MF-DL检测机制为核心实现攻击检测,并辅以轻量级的响应机制来完成对攻击的缓解处理,通过这两个子机制的合作完成对DDoS攻击的防御.系统策略贯穿防御算法的始终,不但明确防御机制的具体操作,也为网络管理员提供操作建议,增强防御攻击的效果.全局防御算法流程如算法3所示.

算法3. 全局防御算法

```
BEGIN
1.  Initialize the defense system;
2.  Collect traffic information;
3.  a = Real-time monitoring = 1;
4.  DO
5.      state = 1;
6.      Perform MF pre-detection, get the result, state;
7.      IF state = 2 THEN
8.          Calculate characteristic parameters;
9.          Perform DL detection, get the result, attack;
10.         IF attack = 1 THEN
11.             state = 4;
12.             Perform response mechanism;
13.         ELSE state = 3;
14.     ELSE continue;
15.     IF system is over THEN
16.         a = 0;
17. WHILE a = 1
END
```

首先初始化防御机制,流量收集器从基础设备的镜像流量中获取网络流量数据包信息,并对流量数据包进行统计,获取当前网络流量信息.接着开启防御机制,设置当前系统策略为1,依次计算并判断MF预检测的相关参数.MF预检测机制属于轻量级检测,根据网络流量的统计信息对网络状态进行实时监测,当发现流量异常疑似出现攻击时,更改系统策略状态为2,并启动DL深度检测并继续检测.DL深度检测检测到攻击时,更改系统策略为4并启动响应机制对攻击流量进行隔断.DL深度检测未确认攻击则更改系统策略状态为3.通过本文所提出的防御机制的收集、检测、响应一系列操作,完成对DDoS攻击的快速防御.

5　性能评价

5.1　评价指标

本文选择检测效率、响应效率为评价指标对系统进行了评价.

5.1.1　检测效率

检测过程是一个二分类问题的判断过程，因此系统的检测结果具体分类如表4所示.

表4　检测结果分类

实际流量	当检测为正常	当检测为攻击
正常	真阴	假阳
攻击	假阴	真阳

检测系统的效率可以从三个方面进行描述，分别是准确率、误报率、漏报率.

系统的检测准确率指的是在实际检测过程中，流量检测结果是正确的占比. 准确率的计算公式如公式(5)所示.

$$准确率=\frac{真阳+真阴}{正常+攻击}\times 100\% \tag{5}$$

系统的误报率指被检测为攻击的流量中非攻击流量的占比. 误报率的计算公式如公式(6)所示.

$$误报率=\frac{假阳}{假阳+真阳}\times 100\% \tag{6}$$

系统的漏报率指的是被检测为正常的流量中实际上是攻击流量的占比. 漏报率的计算公式如公式(7)所示.

$$漏报率=\frac{假阴}{真阴+假阴}\times 100\% \tag{7}$$

5.1.2　响应效率

本文所设计的快速防御机制，不但能检测攻击流量，也能在发现攻击流量后通过响应算法及时处理攻击流量从而降低系统负载. 因此，防御系统主机的CPU占用率和网络负载率(根据本文实验环境此指标应为网卡利用率)被用于观察响应机制的具体指标.

5.2　对比算法

由于已有的防御机制都注重于攻击检测，对攻击的响应处理参差不齐，而且检测效率可以得到量化指标. 因此本文为实现公平对比，与对比算法的实验对比仅仅体现在检测算法的准确率、误报率和漏报率上.

经典的基于熵和聚类的算法是通过选取流的特征字段，通过计算各字段的熵值来完成对流量的分类. 比如通过提取Netflow的五个特征字段(目的地址、目的端口、源地址、包大小等级和流持续时间)的值，分别计算各字段的熵值并且使用K-means方法对熵值进行聚类建模，得到训练后的模型用于对流进行分类，进而可以检测是否出现DDoS攻击[23].

目前，已经提出的基于深度学习的检测算法则不需要人工的高级特征提取，可以利用神经网络的各层神经元自动提取特征用于分类. 例如从ISCX2012数据集中提取20个网络流量字段(tcp.dstport、icmp.length、frame.protocols等)进行检测，通过4种不同的深度学习网络模型对其训练，得到各模型的检测结果[24]. 该文中所使用的模型都是基于LSTM设计，且实验结果证明基础的LSTM模型的检测结果在多数情况下综合性能优于改进的GRU、CNNLSTM等模型. 鉴于实验还原难度，采用文中的LSTM模型来进行对比试验，其中模型的具体结构为：4层LSTM层，每层64个神经元，采用tanh激活函数；后接两个全连接层，每层128个神经元，采用relu激活函数；最后在输出层使用sigmoid激活函数进行分类.

并且为了验证MF预检测模块对整个防御机制的检测精度和检测速度的有效提高，在对比算法中增加了使用纯DL检测算法的内容，二者的实验对比结果可以体现MF预检测模块在攻击检测方面的成效. 而单纯基于DL检测算法的方法和上文提到的基于深度学习的对比算法相类似，不同的是，DL检测算法的特征参数不同，且模型结构较为简单.

5.3　实验环境和数据集

本文设计的IPv6网络中基于MF-DL的DDoS攻击快速防御机制基于Python3、Tensorflow和Keras框架实现.

本文通过两部分实验对MF-DL检测机制的性能进行评价，这是因为截止到目前，仍未出现已公开且权威的IPv6下的DDoS攻击数据集，相关研究工作大多采用本地实验拓扑的模拟数据，由于隐私问题这些数据集并不公开或缺少必要信息. 因此，第一部分实验采用加拿大网络研究所的入侵检测数据集CICIDS2017[25]来完成检测部分的实验以及完成与对比算法的性能对比. 由于该数据集是以IPv4报文为基础进行统计，而且除了IP地址字段，其他特征字段的统计量无关乎IP报文版本格式，因此只修改IP字段即可. 通过批量处理原数据集，将IPv4地址嵌入IPv6格式(例如："192.168.0.1"经过完全填充后得到地址"::FFFF:192.168.0.1")来进行后续

实验.关于此做法的有效性论述如下:首先,在该数据集的生成过程中,研究人员是通过若干不同网段的攻击流量来实现DDoS攻击中的分布式攻击效果的,而IPv6地址长度虽然增加,地址差异更大,但对于不同地址间的区别性是一致的.在本文所提出的检测机制中,并不是通过IPv6的地址字段的具体内容来进行攻击检测,而是根据关联于地址的数据流的统计信息进行检测.换言之,本文的检测机制是将IP地址作为一个参与者的身份标识,而检测机制关注的更多是参与者的行为.

该数据集包括从2017年7月3日上午9点开始,到2017年7月7日下午5点结束共计5天捕获的数据,其中包括例如周一的一些正常流量以及例如周五DDoS泛洪和低速攻击的攻击流量.将这部分数据集以固定的时间窗口大小从早到晚输入机制中来模拟实时攻击时出现的网络情况,用以对本文提出的机制和两种对比算法进行性能测试.

第二部分实验通过在校园网内(外网不完全支持IPv6)模拟小型DDoS攻击(资源占用型泛洪攻击)来测试防御机制的检测和响应性能.参考数据集CICIDS2017的拓扑结构,模拟攻击的实验拓扑如图5所示,将9个网段的20台主机预装网络流量压力软件hyenaeFE并关闭防火墙模拟多用户的流量访问,每台主机生成固定20个同网段IP的数据包.其中,9个网段上分布不同的攻击主机、正常访问主机和被攻击主机,且不同网段之间具有不同的层次关系.以上结构可以保证被攻击主机在系统主机的监测范围内,同时流经系统主机的流量的IP分布足够的分散、流量规模(攻击流量及正常访问流量)相对于被攻击主机足够大,且保证了模拟攻击效果符合本文所提出的防御机制的应用环境.

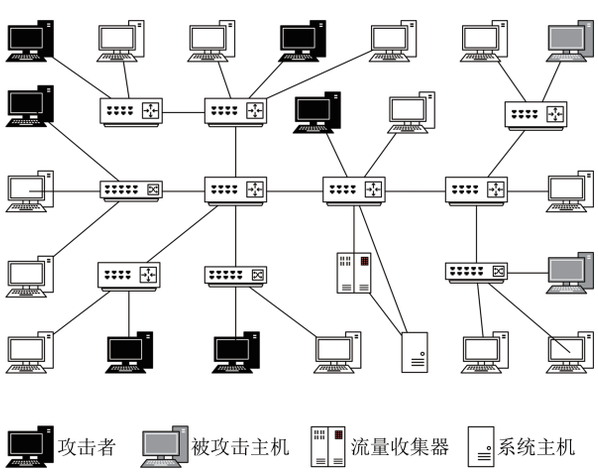

图5 本地模拟数据拓扑结构

在前期背景流量的采集中,模拟正常访问的随机和小规模发包行为.模拟攻击时,攻击主机同时对被攻击主机发送大量TCP和UDP包.通过受攻击本地主机网卡处理能力的限制来模拟资源耗尽型的DDoS泛洪攻击,在20分钟的攻击时间内,来自不同网段的120个模拟攻击主机地址通过间接发包共发出约1.6亿条流量信息.通过此部分测试完成对本机制提出的响应算法可以有效处理DDoS攻击的验证.

5.4 性能测试与分析

5.4.1 检测准确率

检测准确率的实验结果如表5所示,实验结果曲线图如图6所示.

表5 检测准确率

实验次数	MF-DL算法	熵聚类	深度学习	DL算法
1	0.934	0.885	0.92	0.904
2	0.962	0.862	0.822	0.882
3	0.933	0.879	0.947	0.917
4	0.951	0.907	0.911	0.905
5	0.967	0.881	0.95	0.845
6	0.894	0.854	0.885	0.883
7	0.928	0.868	0.934	0.868
8	0.952	0.853	0.887	0.921
9	0.946	0.905	0.914	0.889
10	0.925	0.882	0.893	0.878

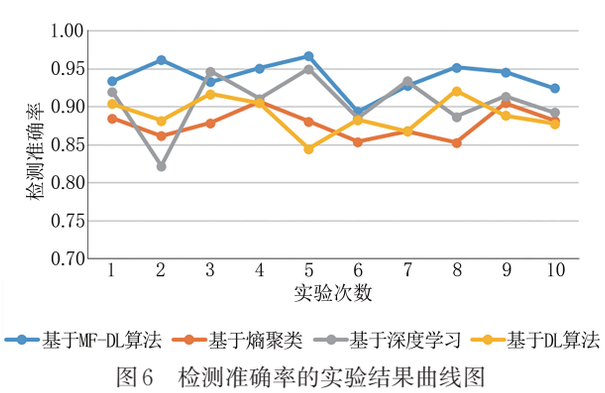

图6 检测准确率的实验结果曲线图

其中,横坐标表示实验次数(共计10次试验),纵坐标表示检测准确率.从图中可以看出,本文提出的基于MF-DL的DDoS攻击快速防御机制的检测准确率在多次实验结果中,平均可达到93.9%.通过对原文算法进行代码还原而实现的基于熵和聚类的方法平均准确率可达87.7%,基于深度学习的检测方法可达90.6%,而单纯基于DL检测算法的平均准确率为88.9%.本文所提出的方法的检测准确率要明显高于对比算法.

检测准确率的实验结果分析如下：基于熵和聚类的方法由于模型仅限于对五种流量熵值进行聚类建模，导致模型对流量特征的学习过于局限. 虽然在明显攻击中可以快速检测出，但对不明显的低速攻击和其他异常情况的感知并不足够，所以准确率较低.

基于深度学习的检测方法在不同的实验中检测准确率波动较大，并且单纯基于DL算法的对比实验体现了和基于深度学习相似的实验结果曲线. 经分析得出，由于单纯神经网络模型对流量进行学习时，流量具有极大随机性，难以捕捉最为合适的特征集合，所以在训练集和测试集划分不同的情况下，模型可能会出现过拟合和欠拟合的情况，从而导致检测结果具有较大波动性. 即使基于纯DL算法的检测方法利用了流量的统计特征，但也无法避免.

而本文所提出的方法，通过MF预检测可以规避一些不需要输入模型的正常流量，从而避免过多的无效流量干扰攻击特征流量的建模过程，让后续DL检测使用的神经网络模型可以更加精准地建模. 因此本文提出的检测机制的检测准确率更稳定一些，且效果稍优于另两种对比方法，也优于单独使用DL检测算法.

误报率和漏报率的试验结果如表6、表7所示，实验结果曲线图如图7、8所示.

表6　检测误报率

实验次数	MF-DL算法	熵聚类	深度学习	DL算法
1	0.04	0.08	0.102	0.095
2	0.021	0.085	0.094	0.085
3	0.0371	0.077	0.086	0.091
4	0.0423	0.071	0.112	0.104
5	0.015	0.08	0.134	0.108
6	0.02	0.09	0.1	0.092
7	0.031	0.095	0.098	0.093
8	0.034	0.068	0.101	0.104
9	0.0411	0.072	0.088	0.082
10	0.038	0.081	0.08	0.086

图7和图8的横坐标表示实验次数，纵坐标分别表示误报率和漏报率.

从图中可以看出，无论是误报率还是漏报率，本文提出的基于MF-DL的快速防御机制在检测误报率和漏报率都要优于对比方法，误报率和漏报率平均能达到3.2%和8.28%，而基于熵和聚类方法的误报率和漏报率是7.99%和16.74%，基于深度学习的方法能够达到9.95%和10.7%，单纯基于DL算法的方法为9.4%和10.9%. 从对比算法的实验结果的比较中得出如下结论：基于熵和聚类方法的模型对攻击行为的描述能力不足导致较高的漏报率；而基于深度学习的神经网络模型的方法和单纯基于DL检测算法的方法由于所有数据不经筛选进行训练导致模型表达不够稳定，具有较高的偶然性.

表7　检测漏报率

实验次数	MF-DL算法	熵聚类	深度学习	DL算法
1	0.09	0.172	0.102	0.115
2	0.077	0.144	0.113	0.106
3	0.091	0.166	0.103	0.12
4	0.084	0.162	0.121	0.131
5	0.073	0.184	0.109	0.095
6	0.08	0.17	0.116	0.121
7	0.092	0.152	0.102	0.107
8	0.086	0.169	0.115	0.091
9	0.076	0.177	0.104	0.108
10	0.079	0.178	0.092	0.101

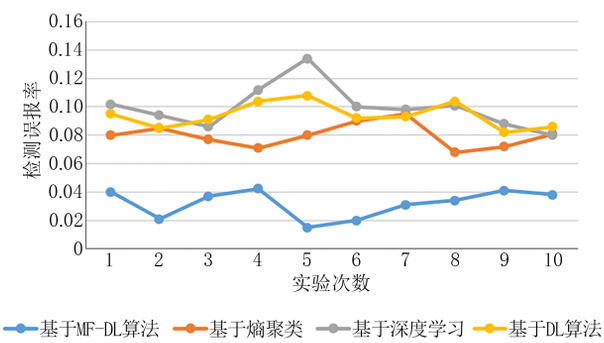

图7　检测误报率的实验结果曲线图

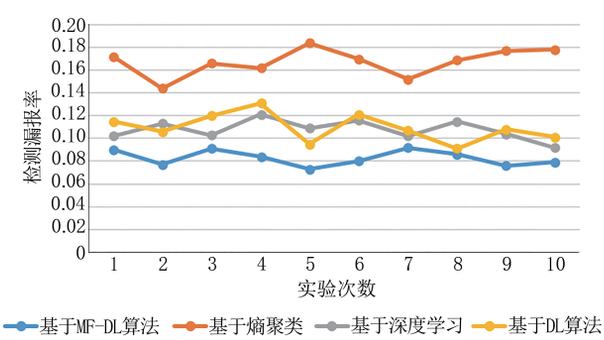

图8　检测漏报率的实验结果曲线图

因此，当在训练集的学习中，由于训练集的偶然性，神经网络模型将非重点特征进行了重点学习，就会出现略微过拟合的情况从而导致高误报率. 而本文提出的方法很好地结合了二者的优点，通过预检测来提高防御系统对流量体积异常的敏感度，降低漏报率；又通过深度检测来确定当前流量的详细统计信息与正常情况不同进而确定攻击的发生，降低

误报率.因此,本文提出的快速检测机制在DDoS攻击检测中具有较为明显的优势.

5.4.2 响应效率

CPU的占用率和网卡的占用率是验证快速防御机制性能的重要指标.通过第二部分的模拟攻击测试,分别在关闭响应机制和开启响应机制状态下进行实验.实验结果如图9和图10所示,横坐标表示实验进行的时间(攻击发起时间),纵坐标表示CPU或NIC的占用率.

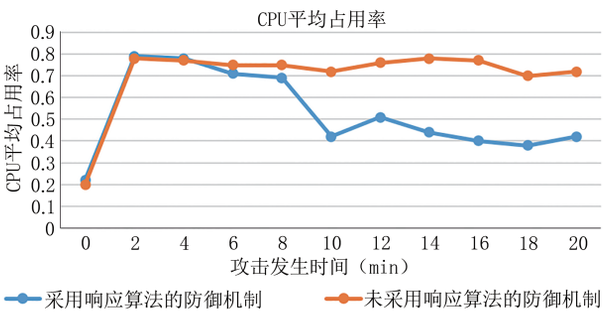

图9 CPU占用率的实验结果

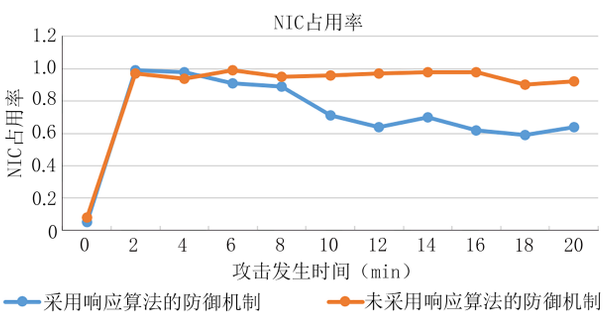

图10 NIC占用率的实验结果

在开启响应机制的状态下,实验进行到4 min之后CPU和网卡的占用率都有持续的下降,实验在进行到10分钟左右的时候趋于稳定.通过实验分析,检测到攻击流量时通过拦截黑名单IP地址的访问流量,可以有效降低网卡的负载情况,进而也降低CPU的负载情况.在实验中虽然不是对所有的攻击流量都能做到完全拦截,但可以对部分泛洪攻击流量进行处理,有效降低系统的资源开销.实验结果证明了本文提出的机制的快速防御效果是优异的.

6 结束语

针对IPv6网络环境下的DDoS攻击防御问题,本文提出了一种基于MF-DL的DDoS攻击快速防御机制.此防御机制主要基于MF-DL检测机制和响应机制实现防御功能.MF-DL检测机制以流量隶属函数和深度学习两种技术为核心实现对网络异常的实时监测和对发生异常后的DDoS攻击检测.响应机制则在发生攻击时通过IP管理实现轻量级的处理来降低网络负载.本文对提出的机制进行了系统实现,选择了国外的经典数据集进行实验.结果证明,本文设计的防御机制相比于经典的算法在平均检测的准确率、误报率和漏报率方面都有所提高,而实际的响应效果也十分明显.

致 谢 感谢匿名审稿专家和计算机学报编辑们对本文提出的宝贵意见和建议!

参 考 文 献

[1] Qin X, Xu T, Wang C. DDoS attack detection using flow entropy and clustering technique//Proceedings of the 2015 11th International Conference on Computational Intelligence and Security (CIS). Shenzhen, China, 2015: 412-415

[2] Idhammad M, Afdel K, Belouch M. Semi-supervised machine learning approach for DDoS detection. Applied Intelligence, 2018, 48(10): 3193-3208

[3] Hinton G E, Osindero S, Teh Y W. A fast learning algorithm for deep belief nets. Neural computation, 2006, 18(7): 1527-1554

[4] Ye X, Chen X, Liu D, et al. Notice of Retraction: Efficient feature extraction using apache spark for network behavior anomaly detection. Tsinghua Science and Technology, 2018, 23(5): 561-573

[5] David J, Thomas C. Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic. Computers & Security, 2019, 82: 284-295

[6] Ahmed M E, Ullah S, Kim H. Statistical Application Fingerprinting for DDoS Attack Mitigation. IEEE Transactions on Information Forensics and Security, 2018, 14(6): 1471-1484

[7] Saied A, Overill R E, Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing, 2016, 172: 385-393

[8] Elejla O E, Belaton B, Anbar M, et al. Intrusion detection systems of ICMPv6-based DDoS attacks. Neural Computing and Applications, 2018, 30(1): 45-56

[9] Chen Zhang, Jieren Cheng, Xiangyan Tang, Victor S. Sheng, Zhe Dong and Junqi Li: Novel DDoS Feature Representation Model Combining Deep Belief Network and Canonical Correlation Analysis, Computers, Materials & Continua, 2019, 61(2): 657-675

[10] Yuze S U, Xiangru M, Qingwei M, et al. DDoS Attack Detection Algorithm Based on Hybrid Traffic Prediction Model//Proceedings of the 2018 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). Qingdao, China, 2018: 1-5

[11] Gao J, Chen Y. Detecting DOS/DDOS Attacks Under Ipv6// Proceedings of the 2012 International Conference on Cybernetics and Informatics. Chongqing, China, 2014: 847-855

[12] Sun Y, Zhang C, Meng S, et al. Modified deterministic packet marking for DDoS attack traceback in IPv6 network// Proceedings of the 2011 IEEE 11th International Conference on Computer and Information Technology. Paphos, Cyprus, 2011: 245-248

[13] E. Durdağı and A. Buldu. IPV4/IPV6 security and threat comparisons. Procedia-Social and Behavioral Sciences, 2010, 2 (2):5285-5291

[14] P. Nikander, J. Kempf, and E. Nordmark, "IPv6 neighbor discovery (nd) trust models and threats," 2004. Request for Comments 3756. Available: https://www.ietf.org/rfc/rfc3756.txt. Last accessed on 2015 November

[15] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, 2004,34(2): 39-53

[16] Hui W, Sun Y, Liu J, et al. DDoS/DoS attacks and safety analysis of IPv6 campus network: Security research under IPv6 campus network//Proceedings of the 2011 International Conference on Internet Technology and Applications. Wuhan, China, 2011: 1-4

[17] Satrya G B, Chandra R L, Yulianto F A. The detection of ddos flooding attack using hybrid analysis in ipv6 networks// Proceedings of the 2015 3rd International Conference on Information and Communication Technology (ICoICT). Nusa Dua, Bali, 2015: 240-244

[18] Aleesa A M, Hassan R. A proposed technique to detect DDoS attack on IPv6 web applications//Proceedings of the 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC). Waknaghat, India, 2016: 118-121

[19] Zhang T, Wang Z. Research on ipv6 neighbor discovery protocol (ndp) security//Proceedings of the 2016 2nd IEEE International Conference on Computer and Communications (ICCC). Chengdu, China, 2016: 2032-2035

[20] Neupane R L, Neely T, Calyam P, et al. Intelligent defense using pretense against targeted attacks in cloud platforms. Future Generation Computer Systems, 2019, 93: 609-626

[21] Liu Z, Cao Y, Zhu M, et al. Umbrella: Enabling ISPs to offer readily deployable and privacy-preserving DDoS prevention services. IEEE Transactions on Information Forensics and Security, 2018, 14(4): 1098-1108

[22] Khalaf B A, Mostafa S A, Mustapha A, et al. Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods. IEEE Access, 2019: 51691-51713

[23] Qin X, Xu T, Wang C. DDoS attack detection using flow entropy and clustering technique//Proceedings of the 2015 11th International Conference on Computational Intelligence and Security (CIS). Shenzhen, China, 2015: 412-415

[24] Yuan X, Li C, Li X. DeepDefense: identifying DDoS attack via deep learning//Proceedings of the 2017 IEEE International Conference on Smart Computing (SMARTCOMP). Hong Kong, China, 2017: 1-8

[25] Sharafaldin I, Lashkari A H, Ghorbani A A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization//Proceedings of the 4th International Conference on Information Systems Security and Privacy. Funchal ,Portugal, 2018: 108-116

CHOU Yi-Fan, M. S. candidate. His current research interests include DDoS attacks detection and IPv6 security.

YI Bo, Ph. D., lecture, His current research interest includes service computing and routing.

WANG Xing-Wei, Ph. D., professor. His current research interests include future Internet, cloud computing, and cyber-security.

JIA Jie, Ph. D., professor. Her current research interests include 5G network, IoT, and big data analysis.

HUANG Min, Ph. D., professor. Her current research interests include supply chain logistics management, intelligent decision and scheduling optimization.

Background

This paper mainly studies the detection of DDoS attacks in IPv6 networks. In the field of DDoS attack detection, there have been many targeted solutions, such as detection algorithms, architecture, mechanisms, and so on. However, DDoS attacks are still unavoidable. At present, DDoS is still one of the major security threats in the Internet world. As a traditional IP network, IPv6 networks can not avoid DDoS attacks from the network architecture. Many solutions to DDoS attack detection problems have been proposed by domestic and foreign-related staff, which proves that feature extraction can abstract the importance of network traffic state, machine learning and big data detection methods are available and effective. In this paper, a detection mechanism based on MF-DL is designed, and a complete detection framework and process are proposed. The proposed detection mechanism is implemented based on the CERNET2 network. The neural network is trained with the existing open-source datasets. The results show that the proposed detection mechanism is effective and the detection effect is better than the traditional methods. This topic belongs to the 13th Five-Year Key R&D Program "IPv6 Address-Driven Network Security Management System and Its Mechanism Research". The specific research topic is "Fast Defense and Traceback of DDoS Attacks in IPv6 Networks", which aims to solve the problem of DDoS Attacks in IPv6 Networks.