DOI:10.13718/j.cnki.xsxb.2021.07.012

基于网络流量特征和自适应匹配追踪的 DDoS 检测①

孟伟东[1], 毕方明[2]

1. 盐城幼儿师范高等专科学校 大数据产业学院, 江苏 盐城 224005;
2. 中国矿业大学 计算机科学与技术学院, 江苏 徐州 221116

摘要: 针对低密度资源耗尽型分布式拒绝服务(Distributed Denial of Service, DDoS)攻击检测进行研究, 提出一种基于网络流量特征和自适应匹配追踪(Adaptive Matching Pursuit, AMP)的混合 DDoS 攻击检测算法. 该算法从包含原始网络数据包的数据集中提取网络数据包的属性, 生成特征向量, 然后使用 K-奇异值分解(K-Singular Value Decomposition, K-SVD)方法生成在 Frobenius 范数意义下具有最小残值的字典, 其次基于匹配追踪(Matching Pursuit, MP)算法根据每个时间窗口的残差向量生成异常指示值, 最后决策模块使用受训练的人工神经网络(Artificial Neural Network, ANN)生成警报. 实验结果表明: 对于所有流量类别(包括无攻击流量类别), 本文算法的性能均优于所对比的算法.

关 键 词: 分布式拒绝服务攻击; 自适应匹配追踪; 网络流量特征; 入侵检测系统

中图分类号: TP393 **文献标志码**: A **文章编号**: 1000-5471(2021)07-0090-07

分布式拒绝服务(Distributed Denial of Service, DDoS)攻击由于攻击签名不断变化而很难防御, 对各种业务和企业构成了严重威胁[1-2]. DDoS 攻击通过消耗目标的带宽、内存或 CPU 等资源, 使目标业务拒绝对外提供在线服务, DDoS 攻击检测问题是入侵检测系统领域中的一个经典问题[3-4]. 快速有效的网络流量识别和分类可以显著提高网络安全[5], 由于传输数据的大小不断增加以及应用程序的多样性, 必须通过流量分析进行流量优先级排序和诊断监控. 信息的多样性或传播对网络流量分类来讲是一个很大的挑战, 信息传播意味着每种类型的流量都可以具有独特的特征或统计属性[6-7].

匹配追踪(Matching Pursuit, MP)是一种稀疏信号表示方法, 通过迭代地将信号投影到从字典中选择的一组原子上, 找到信号的线性近似值[8-9]. 它可能给出一个次优的近似值, 当难以找到最佳正交解时, MP 是有用的. 入侵检测系统(Intrusion Detection System, IDS)用于检测 DDoS 攻击. 根据入侵检测技术的不同, 入侵检测方法被分为异常检测和误用检测两大类[10]. 误用检测方法使用攻击模式来识别入侵, 异常检测方法使用无攻击的网络流量模式来识别攻击[11]. 混合入侵检测结合了异常和误用检测方法, 对多个 DDoS 攻击类进行检测, 形成一种混合检测机制.

能够正确和快速地检测 DDoS 攻击是网络安全需要解决的关键技术. 近年来, 有关 DDoS 攻击检测系统的研究已取得若干成果. 文献[12]提出一种基于网络流量特征的动态性和相关性 DDoS 攻击检测算法. 该算法使用流量演化和动态算子考虑到流量数据包报头的相互关系, 利用流量数据包地址域和负载域的哈希函数区分正常和异常的流量状态. 文献[13]提出一种基于多级自动编码器特征学习的高效 DDoS 攻击检测技术, 该技术通过无监督方式学习多层次的浅层和深层自动编码器来对训练和测试数据进行编码, 用于

① 收稿日期: 2020-07-23
基金项目: 上海智能信息处理重点实验室开放项目(IIPL-2019-10).
作者简介: 孟伟东, 博士, 副教授, 主要从事大数据应用及数据挖掘研究.

特征再生，通过使用有效的多核学习算法组合多级特征来学习最终的统一检测模型. 文献[14]提出一种基于熵特征的 DDoS 攻击检测多分类器算法，该算法将序列特征选择和多层感知器相结合，可以有效地感知检测错误，然后根据最新数据重建检测器. 但是，该算法不能确保找到全局最优特征，且反馈机制可能会产生假阴性或假阳性反应.

在研究了现有 DDoS 攻击检测的基础上，为了有效检测低密度资源耗尽型 DDoS 攻击，本文提出一种基于网络流量特征和自适应匹配追踪(Adaptive Matching Pursuit，AMP)的混合 DDoS 攻击检测算法. 该算法同时利用网络流量的多种特征，使用 K-奇异值分解(K-Singular Value Decomposition，K-SVD)方法从网络流量的参数中生成在 Frobenius 范数意义下具有最小残值的字典，为网络流量增加适应性. 基于 MP 算法根据每个时间窗口的残差向量生成异常指示值，将从字典中获得的异常指示值与智能决策机制结合进行 DDoS 攻击检测. 实验结果表明，在具有多个攻击的混合入侵检测系统中，本文方法的检测率高于 99%，可以有效检测低密度的资源耗尽型 DDoS 攻击.

1　基于网络流量特征和 AMP 的混合 DDoS 攻击检测

本文提出的 DDoS 攻击检测算法使用 MP 算法为每个字典生成异常指示值，利用训练数据得到的异常指示向量对决策模块进行训练，决策模块利用训练好的神经网络生成报警. 具体流程如图 1 所示.

1.1　网络流量特征生成

特征生成模块从网络流量数据中提取网络数据包的属性. 遍及网络的数据具有各种属性，包括源目标互连网协议地址(IP 地址)、传输控制协议(TCP)标志、源/目标端口、流量信息，这种多样性导致了高维属性空间. 属性多样性示例包括流量信息、路由器简单网络管理协议的管理信息库变量、TCP 报头信息、基于熵的特性. 关于属性的挑战之一是从各种属性中找到代表不同类型 DDoS 攻击的最佳特性集. 此外，在 DDoS 攻击下，多个流量属性会同时发生变化.

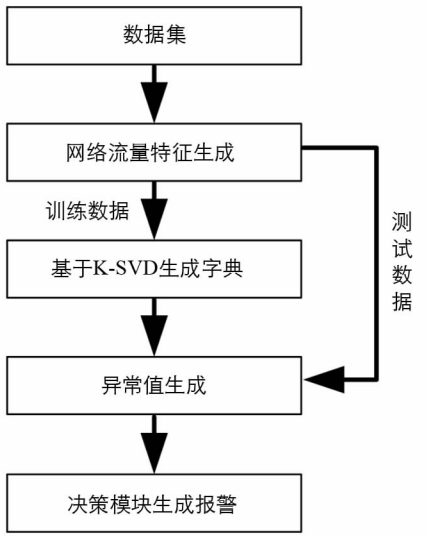


图 1　DDoS 攻击检测流程图

在特征生成阶段，本文从包含原始网络数据包的数据集中提取数字流量属性. 首先将网络流量划分为等距的时间窗口，然后在时间窗口中统计网络包的一些特定属性，形成定义的属性向量.

本文以流量属性和特征向量两种不同的方式处理网络流量. 一维属性向量受到 DDoS 攻击的影响是多种多样的，DDoS 攻击对属性的影响随攻击强度/类型、受害网络的大小和攻击 IP 地址的变化而变化. 从网络流量中得到 16 种不同的流量属性. 本研究中使用的属性是根据其揭示 DDoS 攻击特性的潜力来选择的.

基于包的属性是通过计算网络流量中数据包的特征来获得的，生成这些属性时不考虑流信息. 基于数据包的属性是同步(SYN)，重置(RST)，确认(ACK)，传输控制协议(TCP)，用户数据报协议(UDP)和因特网控制消息协议(ICMP)数据包的数量，这些是根据包头信息来计算的.

业务流的特征是具有相同的源/目标 IP 地址和源/目标端口等公共属性的数据包序列. 在这项工作中，通过考虑网络包的源/目标 IP 地址对和源/目标 TCP 端口对来创建网络流. 本文中使用的基于流的属性向量是流的数量、每个流的包数、每个流的数据量以及每个流的 TCP，UDP，ICMP 包数. 当计算平均包大小时，数据为包的有效载荷的长度.

为了同时捕捉 DDoS 攻击对不同流量属性的影响，本文将时间窗口的正常流量和攻击流量属性建模为属性向量. 特征向量由归一化属性向量生成. 从训练数据集中得到的特征向量根据其属于正常流量还是攻

击流量，将其分为多个类.

1.2 根据训练数据生成字典

本节从训练数据集中每个网络类生成一个单独的字典. 根据训练数据中特征向量的攻击样本，生成误用字典；从训练数据中特征向量的无攻击样本中，生成异常字典.

为了得到字典，本文使用了迭代优化算法 K-SVD. K-SVD 是一种广义 K-均值聚类算法，在字典生成过程中，根据训练的特征集生成由 K 个原子组成的字典. 本文通过实验确定词典大小，根据从训练数据集中获得的特征向量构造矩阵 $\boldsymbol{Y}$. K-SVD 算法的目标函数为

$$\min_{D,\,x} \| \boldsymbol{Y} - Dx \|_F^2 \, subject\ to\ \forall i,\ \| x_i \|_0 \leqslant \varepsilon \tag{1}$$

其中，$\| \cdot \|_F^2$ 是 Frobenius 范数，$\| \cdot \|_0$ 是向量的 L_0 范数，D 为冗余字典，x 为稀疏系数，ε 为稀疏约束项. K-SVD 算法的目标是使用给定的数据集生成在 Frobenius 范数意义下最小残值的字典. 训练数据集可以包含不同的流量类别，如无攻击流量类和各种类型的攻击. 对于每个流量类，都会创建一个单独的字典. 使用特定业务量类别的字典获得残差的 Frobenius 范数对于属于相同类别的向量具有较小的值. 同样，不同流量类的向量会产生更高的范数.

1.3 基于时间窗口的残差生成异常值

对于每个时间窗口，在警报生成阶段，使用与每个网络类对应的字典计算异常指示值. 对于测试数据集中的每个时间窗口，利用特征生成模块获取特征向量. 这些特征向量由 MP 算法和字典进行分解，异常指示值根据产生的残差向量计算.

MP 算法在冗余字典 $D = \alpha_1, \alpha_2, \cdots, \alpha_K \subseteq H$ 上分解 Hilbert 空间中的任意向量 $y \in H$，其中 $\alpha_1 \in H$ 是字典中的一个原子，i 为原子的指数，$x \in {}_i{}^K$ 包含 y 的表示系数.

第一步要实现信号 y 的最佳稀疏分解，必须找到与信号 y 内积最高的原子 α，第一残差 r 等于整个信号 $r_0 = y$. 为了使残差 r_1 的能量最小，该算法从找到给出最大投影 y 的 α_0 开始.

$$\alpha_0 = \arg\max\langle y, \alpha_i \rangle \tag{2}$$

通过从 y 减去 α_0 乘以投影大小 c_0 的量来更新残差

$$y_1 = y - c_0\alpha_0 \tag{3}$$

式(3)中 $c_0 = \langle y, \alpha_0 \rangle$ 称为 α_0 的系数，该过程通过将 r 投影到字典原子上并更新 r_{i+1} 来迭代. 经过 m 次迭代后，y 可以表示为

$$y = \sum_{i=0}^{m-1} c_i\alpha_i - r_m \tag{4}$$

残差可以写为

$$r_m = y - Dx \tag{5}$$

在以下情况下，也可保留能量守恒

$$\| y \|^2 = \sum_{i=0}^{m-1} \| c_i \|^2 + \| r_m \|^2 \tag{6}$$

根据产生的残差向量计算异常指示值

$$\psi_i = \| r_i \|^2 \tag{7}$$

式(7)中 ψ_i 为第 i 个时间间隔的异常指示值，$\| \cdot \|^2$ 为向量的 L_2 范数，报警是通过对异常指示向量 ψ 应用一个阈值而产生的.

异常指示向量根据字典类型进行不同的评估. 如果使用异常字典，则预期异常值在受到攻击时会增加. 当使用误用字典时，预期异常指示值在受到攻击时会降低. 同样的方法适用于误用字典和合法流量. 由于 K-SVD 算法生成字典给出的残差范数最小，且具有最大数量的非零元素，因此这种行为是 K-SVD 算法目标函数的结果.

1.4 决策模块生成报警

本文采用人工神经网络(Artificial Neural Network，ANN)作为决策机制，决策模块通过受训练的

ANN 利用异常指示值生成报警. ANN 是大量相互关联的处理单元(节点)的组合，这些处理单元(节点)展示了利用数据训练模式中信息学习和分类数据的能力. 人工神经网络是一种有监督的分类算法，需要训练.

训练神经网络包括调整权值和网络偏差，以优化网络性能. 本文使用前馈神经网络和均方误差作为性能函数.

$$e_{mse} = \frac{1}{N}\sum_{i=1}^{N}(t_i - a_i)^2 \tag{8}$$

式(8)中 a 是神经网络的输出，N 是样本量，t 是目标输出.

神经网络中使用的传递函数为双曲正切 S 型传递函数，计算为

$$t(x) = \frac{2}{1+\exp(-2^x)} - 1 \tag{9}$$

本文所用的 ANN 在隐藏层有 20 个节点，在 3 个流量类中使用的输出层有 3 个神经元，在 2 个流量类检测中实验的输出层有 2 个神经元.

AMP 方法为每个字典生成一个异常指示符值. 因此对于包含 2 个流量类的数据集，AMP 方法生成 2 个异常指示向量，采用 2 种输入方式. 同样，对于包含 3 个流量类的数据集，AMP 方法生成 3 个异常指示向量，采用 3 种输入方式.

基于 AMP 的 DDoS 攻击检测需要使用训练数据集进行训练. 训练有两个阶段，分别对应于字典生成和决策模块中的 ANN 训练. 最初，为每个网络类生成一个单独的字典，利用训练数据得到的异常指示向量对决策模块进行训练.

对于每个时间窗口，在报警生成阶段，使用与每个网络类对应的字典计算异常指示值. 决策模块通过受过训练的 ANN 利用异常指示值生成报警.

2　实验结果与分析

为了评估本文算法的性能，所有实验均在 2.30 GHz 处理器、64 GB RAM 和 64 位 Windows 7 操作系统进行，所有测试均是在 MATLAB R2016a 环境下实现. 选取 BOUN-DDoS 数据集[8] 进行实验，BOUN DDoS 数据集是一种新的在线数据集，包含多种不同强度的低密度 DDoS 攻击，这些攻击在后台攻击免费流量. BOUN DDoS 数据集还包含各种类型的合法流量、SYN Flood 和 UDP Flood 攻击. 这些数据集分为训练和测试两个子集，训练数据集包含整个数据集的 30%，而测试数据集包含 70%. 将测试结果与匹配追踪平均投影(Matching Pursuit Mean Projection，MPMP)[15] 和小波(Wavelet)变换[16] 进行分析比较，两者均用于 DDoS 攻击检测.

2.1　评价指标

为了评价算法的性能指标，采用检测率(Ture Positive Rate，TPR)、受试者工作特性(Receiver Operating Characteristic curve，ROC)曲线、ROC 曲线下面积(Area Under Curve，AUC)和准确度(Accuracy，Acc)4 种不同的评价检测指标. 这些指标由正确识别的样本数和检测器漏检的样本数来计算.

$$TPR = \frac{TP}{TP+FN} \times 100\% \tag{10}$$

$$Acc = \frac{TP+TN}{TP+FP+TN+FN} \times 100\% \tag{11}$$

式(10)、式(11)中真阳性(True Positive，TP)表示攻击样本经过正确分类后被判为攻击样本；真阴性(True Negative，TN)表示正常流量经过正确分类后被判为无攻击样本；假阳性(False Positive，FP)表示正常流量经过错误分类后被判为攻击样本；假阴性(False Negative，FN)表示攻击流量经过错误分类之后被判为无攻击样本.

这些指标无法找到检测系统的最佳工作点. 因此，本文采用入侵检测能力(Capability of Intrusion Detection，CID)度量来寻找最佳操作点. CID 参数考虑了评估指标的所有方面以及这些指标的细微变化，

包括TPR、正预测值、负预测值和基准率. 较高的CID值意味着IDS具有更好的、准确分类输入事件的能力. 选择ROC曲线中给出最大CID值的点来比较检测性能，根据最高CID值选择结果部分性能指标的操作点.

设 X 表示IDS输入的随机变量，Y 表示IDS输出的随机变量. 随机变量 X 的输入熵定义为

$$H(X) = -\sum_{x\in X} p(x)\log(p(x)) \tag{12}$$

式(12)中 $p(x)$ 表示变量 x 的概率.

随机变量 X 和 Y 之间的互信息定义为

$$I(X;Y) = \sum_{x\in X}\sum_{y\in Y} p(x,y)\log\frac{p(x,y)}{p(x)p(y)} \tag{13}$$

式(13)中，$p(y)$ 表示变量 y 的概率，$p(x,y)$ 表示变量 x 和 y 同时发生的概率.

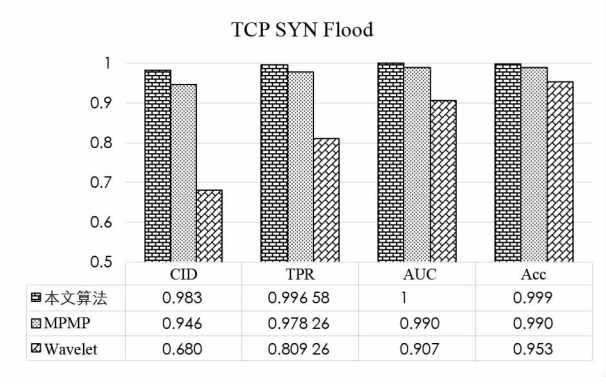
利用以上方程，可以将CID计算为

$$CID = \frac{I(X;Y)}{H(X)} \tag{14}$$

互信息通过了解IDS的输出来衡量输入不确定性的降低，此互信息用输入熵 $H(X)$ 归一化. 因此，CID是给定IDS输出的IDS输入不确定度降低的比率，其值范围为[0，1].

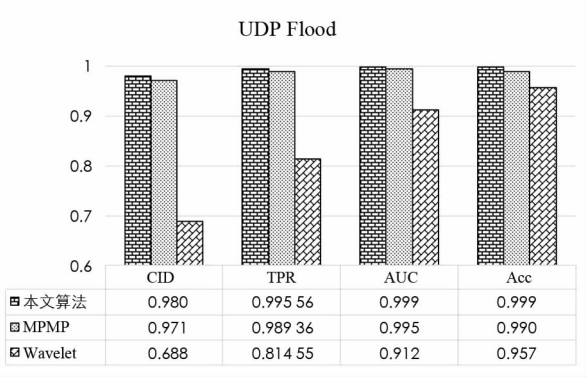
2.2 实验结果与分析

使用2个和3个流量类对本文算法进行性能评估，数据集包括30%训练集和70%的测试集. 2个流量类包括攻击和无攻击流量，而3个流量类包括2个攻击. 在两类评估中，分别讨论了TCP SYN flood和BOUN UDP攻击的检测，测试结果如图2和图3所示. 由图2、图3可以看出，与其他方法相比，本文方法以更高的CID,TPR,AUC和Acc提供了更好的结果.



	CID	TPR	AUC	Acc
本文算法	0.983	0.996 58	1	0.999
MPMP	0.946	0.978 26	0.990	0.990
Wavelet	0.680	0.809 26	0.907	0.953

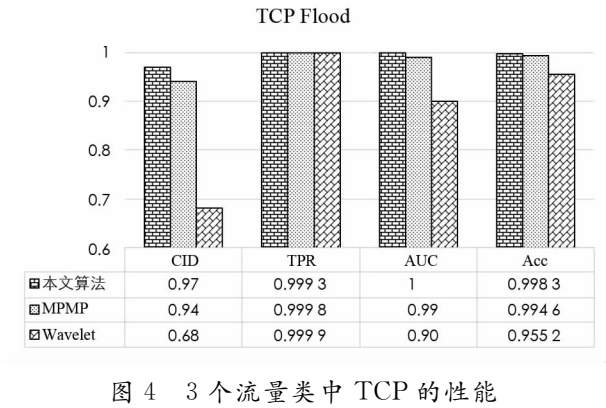
图2 2个流量类中TCP的性能



	CID	TPR	AUC	Acc
本文算法	0.980	0.995 56	0.999	0.999
MPMP	0.971	0.989 36	0.995	0.990
Wavelet	0.688	0.814 55	0.912	0.957

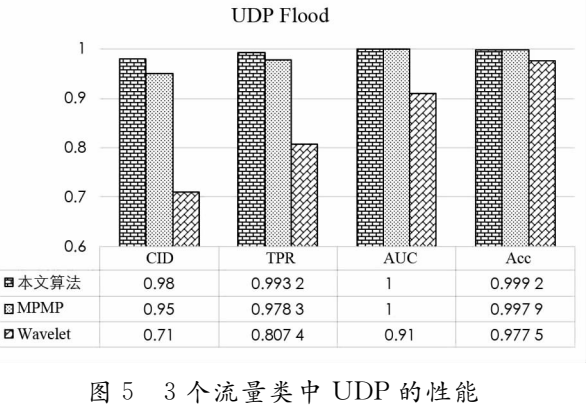
图3 2个流量类中UDP的性能

3个流量类包括2个攻击，由于没有公开可用的DDoS数据集包含一种以上的洪水攻击，因此使用BOUN数据集来处理3种流量级别的情况. 将TCP和UDP flood数据集合并以获取包含更多攻击类别的流量，其结果如图4、图5、图6所示.



	CID	TPR	AUC	Acc
本文算法	0.97	0.999 3	1	0.998 3
MPMP	0.94	0.999 8	0.99	0.994 6
Wavelet	0.68	0.999 9	0.90	0.955 2

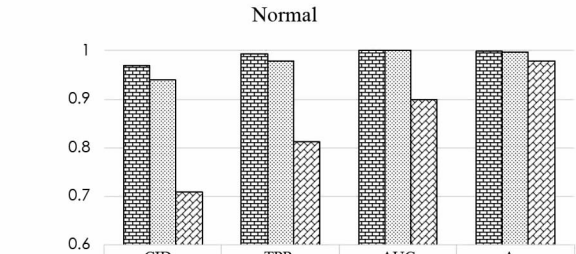
图4 3个流量类中TCP的性能



	CID	TPR	AUC	Acc
本文算法	0.98	0.993 2	1	0.999 2
MPMP	0.95	0.978 3	1	0.997 9
Wavelet	0.71	0.807 4	0.91	0.977 5

图5 3个流量类中UDP的性能

由图 4、图 5、图 6 可以看出，当流量数据有 2 个以上的攻击类型时，本文算法比基于 MPMP 和小波的算法表现得更好. 虽然 MPMP 具有较高的性能指标，但对于 UDP flood 和无攻击类，MPMP 方法的 CID 和 TPR 较低. 本文算法在不知道流量类型并且只对正常流量进行建模的情况下也能非常好地工作，这是因为本文算法同时利用多种网络流量特征，基于 AMP 生成异常指示值，并将异常指示值与使用人工神经网络的智能决策机制相结合进行 DDoS 攻击检测.



	CID	TPR	AUC	Acc
本文算法	0.97	0.992 2	1	0.998 7
MPMP	0.94	0.978 7	1	0.996 8
Wavelet	0.71	0.812 7	0.9	0.977 7

图 6　3 个流量类中 Normal 的性能

3　结　　语

本文提出一种基于网络流量特征和自适应匹配追踪(AMP)的混合 DDoS 攻击检测算法，用来检测低密度的资源耗尽型 DDoS 攻击. 该算法从包含原始网络数据包的数据集中提取网络数据包的属性生成特征向量，使用 K-SVD 方法从网络流量的参数中生成在 Frobenius 范数意义下具有最小残值的字典，基于 MP 算法根据每个时间窗口的残差向量生成异常指示值，将从字典中获得的异常指示值与智能决策机制结合进行 DDoS 攻击检测. 实验结果表明，在具有多个攻击的混合入侵检测系统中，本文算法可以有效检测低密度的资源耗尽型 DDoS 攻击. 未来的工作是考虑在多个入侵检测数据集上进行实验，从而更全面地验证本文算法的效果.

参考文献：

[1] XIA H, FANG B, ROUGHAN M, et al. A BasisEvolution Framework for Network Traffic Anomaly Detection [J]. Computer Networks, 2018, 135: 15-31.

[2] 汪　洋，伍忠东，朱　婧. 基于深度序列加权核极限学习的入侵检测算法 [J]. 计算机应用研究，2020，37(3)：829-832.

[3] ATEŞ Ç, ÖZDEL S, YıLDıRıM M, et al. Network Anomaly Detection Using Header Information with Greedy Algorithm [C]//2019 27th Signal Processing and Communications Applications Conference (SIU). Sivas: IEEE, 2019.

[4] BEHAL S, KUMAR K, SACHDEVA M. D-FACE: an Anomaly Based Distributed Approach for Early Detection of DDoS Attacks and Flash Events [J]. Journal of Network and Computer Applications, 2018, 111: 49-63.

[5] DAVID J, THOMAS C. Efficient DDoS Flood Attack Detection Using Dynamic Thresholding on Flow-Based Network Traffic [J]. Computers & Security, 2019, 82: 284-295.

[6] YIN D, ZHANG L M, YANG K. A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework [J]. IEEE Access, 2018, 6: 24694-24705.

[7] IDHAMMAD M, AFDEL K, BELOUCH M. Semi-Supervised Machine Learning Approach for DDoS Detection [J]. Applied Intelligence, 2018, 48(10): 3193-3208.

[8] ARIVUDAINAMBI D, VARUN KUMAR K A, SIBI CHAKKARAVARTHY S. LION IDS: a Meta-Heuristics Approach to Detect DDoS Attacks Against Software-Defined Networks [J]. Neural Computing and Applications, 2019, 31(5): 1491-1501.

[9] 刘　敏，滕　华，何先波. 基于核函数的软件定义网络 DDoS 实时安全系统 [J]. 计算机应用研究，2020，37(3)：843-846，850.

[10] PANDEY V C, PEDDOJU S K, DESHPANDE P S. A Statistical and Distributed Packet Filter Against DDoS Attacks in Cloud Environment [J]. Sādhanā, 2018, 43(3): 1-9.

[11] ELEJLA O E, ANBAR M, BELATON B, et al. Flow-Based IDS for ICMPv6-Based DDoS Attacks Detection [J]. Arabian Journal for Science and Engineering, 2018, 43(12): 7757-7775.

[12] KRASNOV A E, STATE INSTITUTE OF INFORMATION TECHNOLOGIES AND TELECOMMUNICATIONS, NADEZHDIN E N, et al. Detecting DDoS Attacks by Analyzing the Dynamics and Interrelation of Network Traffic Characteristics [J]. Vestnik Udmurtskogo Universiteta Matematika Mekhanika Komp'Yuternye Nauki, 2018, 28(3): 407-418.

[13] YAN B H, HAN G D. Effective Feature Extraction via Stacked Sparse Autoencoder to Improve Intrusion Detection System [J]. IEEE Access, 2018, 6: 41238-41248.

[14] WANG M, LU Y Q, QIN J C. A Dynamic MLP-Based DDoS Attack Detection Method Using Feature Selection and Feedback [J]. Computers & Security, 2020, 88: 101645.

[15] KESAVAMOORTHY R, RUBA SOUNDAR K. Swarm Intelligence Based Autonomous DDoS Attack Detection and Defense Using Multi Agent System [J]. Cluster Computing, 2019, 22(4): 9469-9476.

[16] SU Y Z, MENG X R, MENG Q W, et al. DDoS Attack Detection Algorithm Based on Hybrid Traffic Prediction Model [C]// 2018 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC). Qingdao: IEEE, 2018.

DDoS Detection Based on Network Traffic Characteristics and Adaptive Matching Pursuit

MENG Wei-dong[1], BI Fang-ming[2]

1. *College of Big Data Industry, Yancheng Kindergarten Teachers College, Yancheng Jiangsu 224005, China;*

2. *School of Computer Science and Technology, China University of Mining and Technology, Xuzhou Jiangsu 221116, China*

Abstract: Research on low-density resource exhausted distributed denial of service (DDoS) attack detection. In this paper a hybrid DDoS attack detection algorithm has been proposed based on network traffic characteristics and Adaptive Matching Pursuit (AMP). The algorithm extracts the attributes of the network packet from the data set containing the original network packet to generate a feature vector, and then uses the K-Singular Value Decomposition (K-SVD) method to generate a dictionary with the smallest residual value in the sense of the Frobenius norm, and then based on the MP algorithm according to each time The residual vector of the window generates an abnormal indication value, and finally the decision-making module uses a trained artificial neural network (ANN) to generate alerts. The experimental results show that for all traffic categories (including non-attack traffic categories), the performance of the proposed algorithm is better than the compared algorithm.

Key words: distributed denial of service attack; adaptive matching pursuit; network traffic characteristics; intrusion detection system

责任编辑 夏 娟