多类支持向量机的DDoS攻击检测的方法

徐 图，罗 瑜，何大可

(西南交通大学信息科学与技术学院 成都 610031)

【摘要】为了利用SVM准确的检测DDoS，需要找到区分正常流和攻击流的特征向量，根据DDoS攻击的特点，提出了独立于流量的相对值特征向量。为了在指示攻击存在的同时，也指示攻击强度，多类支持向量机(MCSVM)被引入到DDoS检测中。实验表明，RLT特征与MCSVM相结合，可以有效检测到不同类型的DDoS攻击，并且能准确地指示攻击强度，优于目前已有的检测方法。使用RLT特征进行DDoS检测，比使用单一攻击特征进行识别的方法，包含更多的攻击信息，可以得到较高的检测精度。

关 键 词 分布式拒绝服务攻击； 多类支持向量机； 相对值特征向量； 支持向量机

中图分类号 TP393 **文献标识码** A

Detecting DDoS Attack Based on Multi-Class SVM

XU Tu, LUO Yu, and HE Da-ke

(School of Information Science and Technology, Southwest Jiaotong University Chengdu 610031)

Abstract In order to detect distributed denial of service (DDoS) attacks with support vector machine (SVM) measures, the feature vectors that can distinguish normal stream from attack stream are required. According to the characters of DDoS attacks, a group of relative value features are proposed. For indicating the existence and attack intensity of DDoS attack simultaneously, multi-class SVM (MCSVM) is introduced to detecting DDoS Attacks. As shown in our numeric experiments, the combination of RLT features and MCSVM can detect several kinds of DDoS attacks effectively and indicate attack intensity precisely. The detection results are better than other detection measures. Because the RLT features include more attack information than the detection measures using single attack character, a better detection result is available.

Key words distributed denial of service attack; multi-class SVM; relative value feature vector; support vector machine

近年来，分布式拒绝服务(distributed denial of service，DDoS)攻击已经成为威胁互联网正常运行的主要因素。自DDoS攻击出现开始，研究人员就已经提出了不少识别DDoS的算法。文献[1]提出用数据流的功率谱密度(PSD)分析法识别DDoS。文献[2]利用TCP流的特定属性的信息熵来识别DDoS攻击流。文献[3]则提出利用网络流的相似度变化来识别DDoS攻击流。这些检测法的共性，就是它们均根据网络流的某种特征来区分DDoS流。而目前的DDoS攻击发起者，为了逃避IDS的检测，往往先发起低速率的或周期性的DDoS攻击，以麻痹布置在目标端的IDS系统[4]，使上述的识别方法的检测率下降。为获得更好的检测效果，机器学习算法被引入到DDoS检测中。

支持向量机(support vector machine，SVM)是基于核方法的机器学习算法[5]，由于SVM具有良好的泛化性能，可以有效克服传统学习机的“维数灾难”和“过学习”问题，因此获得广泛关注。文献[6]提出流连接密度(FCD)概念，用FCD的自适应自回归(AAR)模型参数作为特征向量，使用SVM进行DDoS攻击检测。但将DDoS检测看作一个二分类问题，也有一定局限性。本文认为二分类的观点，抹杀了攻击强度的概念。文献[7]将多个支持向量机引入DDoS检测，提出以网络流参数(traffic rate analysis，TRA)作为特征向量，用多个SVM识别DoS、DDoS和DRDoS攻击，并指出用多个SVM比单个SVM有更高的检测率，但其使用的特征向量仍有待改进。

基于上述情况，本文提出了一组对DDoS攻击具

收稿日期：2007－01－15；修回日期：2007－05－08
基金项目：四川省青年科技基金(07JQ0060)
作者简介：徐 图(1972－)，男，博士生，主要从事机器学习与智能网络安全方面的研究.

有良好区分度的相对值特征向量，并用多类支持向量机(multi-classification SVM，MCSVM)进行DDoS攻击识别。在识别DDoS的同时，指示DDoS攻击的强度。

1　支持向量机和多类支持向量机

SVM是在结构风险最小化的思想下建立的分类机。当样本点线性可分时，根据分类间隔最大化原则构造分类超平面；当样本点非线性可分时，利用非线性映射$\boldsymbol{\Phi}$，将样本点映射到高维特征空间中，使其在特征空间中线性可分，再通过核函数计算特征空间的内积，获得原空间的分类超平面表达式。若考虑到样本错分的情况，可以引入惩罚参数C和松弛变量ξ，采用$\sum\xi_i$作为一种度量，描述错分的样本。仍采用间隔最大化方法，求出最优超平面[5]。

标准的支持向量机是二分类器，在多个类标间分类，需使用多类支持向量机(MCSVM)。文献[5]总结了目前应用较广泛的一类对余类(1-v-r)、一类对一类(1-v-1)、多类目标函数三种MCSVM。

本文使用1-v-1多类分类器，这种多分类算法是基于二分类器的，在所有的类别中，每两个类别之间都建立一个二分类器，故称一类对一类。若有n个类别，共需要$n(n-1)/2$个分类器。对于输入x，将其输入到所有的分类器，并对每个分类器输出进行计票。最后，当所有的分类器都给出结果后，得票最多的类别就是x的最终类别。

2　特征向量的选取

选择合适的特征向量，是利用MCSVM识别DDoS攻击的关键。在确定特征向量时，本文遵循两个原则：(1) 考虑到Internet中不同的网络节点处流量并不相同，尽量采用相对值作为特征，即特征值不直接依赖于流量大小。(2) 选择能反映正常流和攻击流差异的参数作为特征值。根据这两个原则，本文确定下列特征，且特征值均是在采样间隔T=1 s时计算的。

(1) 单边连接密度。在本文的前期工作中，提出了单边连接密度(one-way connection density，OWCD)的概念[8]：在IP流中，某个IP包发送后，若能收到目标端的回复包，称这两个包构成一个双边连接(two-way connection，TWC)；反之，若某个IP包没有收到目标端的回复包，则这个包构成一个单边连接(one-way connection，OWC)。在采样间隔T中，属于OWC的包占总包数的比例，就称为采用间隔T下的单边连接密度OWCD=$\left(\sum\text{OWC Packtes}\right)\Big/\left(\sum\text{IP Packtes}\right)\times100\%$。实验表明，在DDoS攻击中，如果使用虚假的源IP地址，会使OWCD显著增加。正常流中，OWCD的取值在30以下；而DDoS攻击中，OWCD会趋于100。

(2) IP流的平均长度。本文引入广泛使用的IP流的概念。具有相同的五元组(源IP地址、源端口、目的IP地址、目的端、协议类型)的报文集合，称为IP流。一个五元组唯一确定一个IP流。本文仅考虑TCP、UDP、ICMP三种协议的双向IP流。IP流长度是指一个IP流包含的IP包的个数。IP流平均长度定义为采样间隔T中，IP流的平均长度为：Lave_flow=$\left(\sum\text{IP Packets}\right)\Big/\left(\sum\text{Number of IP Flows}\right)$。正常流的IP流平均长度通常在5～10之间；而在DDoS攻击中，由于长度为1的流大量增加，Lave_flow 将趋于1。

(3) IP包的流入流出比。正常流中，流入与流出的IP包的比例处于平衡状态。而对一般自治网而言，由于是Internet网的消费者，流入包数量会大于流出包数量，但比例一般在15以内。DDoS攻击时，由于攻击包均为流入包，因此该比例会急剧增加为R_{io}=$\left(\sum\text{Incoming IP Packets}\right)\Big/\left(\sum\text{Outgoing IP Packets}\right)$，一般均都在1 000以上。

(4) IP流长度的熵。熵是描述变量随机性的量纲。对于离散随机变量x，设取第i个分量的概率为p_i，则x的熵定义为$E_x=-p_i\sum\log_2 p_i$。E_x越大，说明x的随机性越强，包含的信息量越大。在正常流中，由于流平均长度Lave_flow比较大，因此源IP地址的随机性相对较小，在DDoS攻击中，使用大量虚假源IP地址，且这些地址各不相同，使得包的IP地址随机性增大，而这可以通过Lave_flow来体现，Lave_flow越小说明IP地址的随机性越大。因此，用Lave_flow的熵来描述源IP地址的随机性。设在T中，流的集合为$F(f_1, f_2, \cdots, f_n)$，每个流的长度分别为$l_{f_1},l_{f_2},\cdots,l_{f_n}$，令$p_i=l_{fi}$/(总包数$N$)，则IP流长度的熵$E_{\text{flow_length}}=-p_i\sum\log_2 p_i$。在正常流中，$E_{\text{flow_length}}$为2～4；在攻击流中为8～10。

(5) 协议熵。在正常流中，TCP包、UDP包和ICMP包所占的比例是比较固定的，协议的随机性也是比较固定的，即协议的熵也是比较固定的，约为0.43。而在Flood攻击中，相同的协议几乎占据了整个带宽，协议熵将趋于0。用p_{t}，p_{u}和p_{i}分别表示T中TCP包、UDP包和ICMP包所占的比例，则协议熵可

定义为$E_p=-p_t\log_2 p_t-p_u\log_2 p_u-p_i\log_2 p_i$。

(6) 协议比例。TCP、UDP和ICMP是常用于产生攻击的三种协议，这三种协议包在间隔T中所占的比例，也能很好地反映DDoS攻击的存在。分别用R_t、R_u和R_i表示三种协议的比例。

由于协议比例包含3个特征，加上前面5个特征，共构成一个8维特征向量：OWCD、Lave_flow、R_{io}、E_{flow_length}、E_p、R_t、R_u、R_i。因均使用相对值作为特征，故称为相对特征(relative features)，下文简称RLT特征。

3 实验结果与分析

在本文的实验中，将攻击强度分为正常、轻度、中度和重度4个等级，类别分别是0、1、2、3。使用1-v-1多分类器作为分类算法。正常数据流采自于西南交通大学信息科学与技术学院网络出口处，其网络拓扑图如图1所示，实验数据均由检测主机采集。

为了产生不同强度的攻击数据，采集TFN2K产生的DDoS攻击数据流，用tcpreplay进行重放，分别使用tcpreplay的重放速度参数multiplier 0.5/0.75/1产生轻度、中度和重度攻击数据。重放参数的选择主要考虑了文献[8]中对轻度、中度和重度攻击的区分标准。采包工具使用Ethereal Ver 0.10.14，分别采集了SYN Flood、UDP Flood、ICMP Flood数据用于训练和检测。采样间隔为1 s。

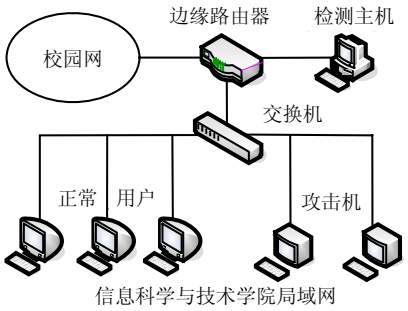


图1 实验网络拓扑图

为了检验相对值特征向量的区分能力，实验中，将与Jungtaek提出的TRA特征向量进行比较，TRA特征定义可参见文献[7]。

3.1 多类SVM的训练

训练数据包括4个样本集T_0，T_1，T_2和T_3，分别代表正常、轻度、中度和重度攻击数据。T_0含400个样本，T_1、T_2和T_3各含300个样本，分别是与其分类标号对应的100个SYN Flood、UDP Flood、ICMP Flood样本之和，即总的训练样本数为1 300个。

对这1 300个样本，分别提取RLT特征和TRA特征，并进行训练。由于使用了1-v-1多分类器，共需训练2×6个SVM，训练算法使用收敛较快的SMO算法。采用高斯核函数，经过多次实验，最后取C=50、ε=0.1、λ=0.001和σ=10。机器配置为Inter Xeon 3G、1 G RAM，编译环境为C++ Builder 6.0。

3.2 攻击数据的测试

为了检测使用上述训练集获得的学习机器的分类能力，分别采用两种数据源作测试集：(1) 采自图1所示的实验网络，数据可以给出类标；(2) 采自MIT林肯实验室的DDoS攻击数据集，数据没有类标。

实验一中，采集正常、轻微、中度和重度四类样本，每类样本各包含1 200个数据，三种协议各有400个数据，共4 800个测试数据。

经过检测，分别计算每类数据的检测率(true positive，TP)，误警率(false positive，FP)，漏警率(false negative，FN)。检测结果在表1中示出。

表1表明，在测试带类标的数据时，两种特征的检测率都较高，RLT特征的总体检测结果高于TRA特征。

表1 实验一的检测结果

类别	RLT特征(%)			TRA特征(%)		
	TP	FP	FN	TP	FP	FN
正常	100.0	0.0	0.0	99.5	0.5	0.0
轻微	99.7	0.3	0.0	93.4	4.7	1.9
中度	98.2	0.8	1.0	92.8	1.5	5.7
重度	98.6	0.5	0.9	96.5	1.3	2.2

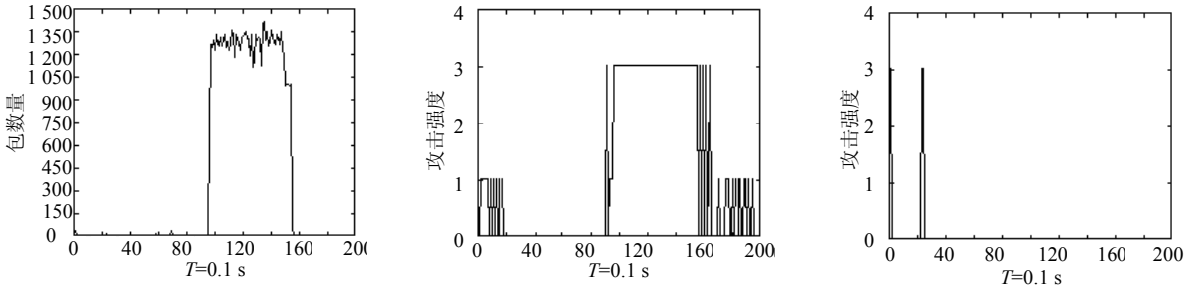
在第二个实验中，使用MIT林肯实验室的DDoS攻击数据集LLDOS1.0和LLDOS2.0.2[9]，表2列出了这两个数据集的基本信息。两个数据集的攻击时间都比较短，分别为6 s和8 s，因此从中各截取20 s的数据，将攻击过程包含其中。设置采样时间T=0.1 s，将获得的20 s数据进行特征提取，送入训练好的MCSVM中进行检测，并得到结果曲线。包曲线是指每个采样间隔内IP包的数量构成的曲线。

表2 林肯实验室数据集信息

数据集	包数量	跨越时间/s	攻击时间/s
LLS_DDOS1.0	649 787	11 652	6
LLS_DDOS2.0.2	347 987	6 166	8

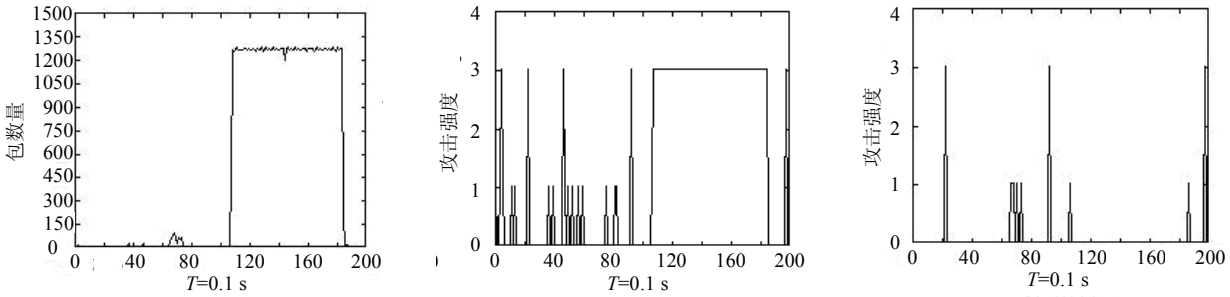
图2和图3分别显示了LLS_DDOS1.0和LLS_DDOS2.0.2中攻击的包曲线图和用RLT特征、TRA特征对攻击进行识别的结果曲线。图2和图3表明，用RLT特征准确检测出了LLDOS1.0和LLDOS2.0.2中

的攻击，并指示攻击强度为重度攻击，而用TRA特征却完全检测不到两个数据集的攻击。



a. 包曲线图　　b. RLT特征的识别结果　　c. TAR特征的识别结果

图2　LLS_DDOS1.0的识别结果



a. 包曲线图　　b. RLT特征的识别结果　　c. TAR特征的识别结果

图3　LLS_DDOS2.0.2的识别结果

仔细分析TRA特征，10个特征中的前8个特征都只与TCP协议有关，即使是在TCP Flood攻击下，前8个特征中的大部份值也是0，而在UDP Flood和ICMP Flood中，由于TCP包很少，前8个特征的值都将趋于0，使得TRA特征所包含的攻击信息大大降低，造成了它的检测精度也大受影响。

4　结　论

用SVM检测DDoS攻击的关键是要提取能区分正常流和攻击流的特征向量，特征的区分度越好，则其检测率越高。在Internet中，不同的结点处流量是不同的，但由于网络流具有自相似性，它们的一些特性是与流量无关的，尽量提取这些相对值作为特征，可以避开因流量不同而造成的干扰，准确反映网络流的异常情况。于是，独立于流量的RLT特征被提出。为了反映攻击强度，MCSVM也被引入到DDoS检测中，将攻击分为正常、轻微、中度和重度四个等级。这样，在检测DDoS时，不但能指示攻击的存在，还能指示攻击的强度，在遭受攻击时，可为网络管理员采取相应措施提供依据。

参　考　文　献

[1] CHENG C M, KUNG H, TAN K S. Use of spectral analysis in defense against Dos attack[C]//In: Proceedings of IEEE GLOBECOM. Taipei, china: IEEE, 2002.

[2] FEINSTEIN L, SCHNACHENBERG D, BALUPARI R, et al. Statistical approaches to DDoS attack detection and response[C]//In: Proceedings of the DARPA Information Survivability Conference and Exposition. Washington D C: IEEE, 2003.

[3] 何　慧, 张宏莉, 张伟哲, 等. 一种基于相似度的DDoS攻击检测方法[J]. 通信学报, 2004, 25(7): 176-184.

[4] SHEVTEKAR A, ANANTHARAM K, ANSARI N. Low rate TCP denial-of-service attack detection at edge routers[J]. IEEE Communication Letters, 2005, 9(4): 363-365.

[5] 邓乃杨, 田英杰. 数据挖掘中的新方法—支持向量机[M]. 北京: 科学出版社, 2004.

[6] 孙钦东, 张德运, 高　鹏. 基于时间序列分析的分布式拒绝服务攻击检测[J]. 计算机学报, 2005, 28(5): 767-773.

[7] SEO J, LEE C, SHON T. A new DDoS detection model using multiple SVM and TRA[C]//In: Proceedings of The First International Workshop on Security in Ubiquitous Computing Systems(SecUbiq`05). Nagasaki: LNCS, 2005.

[8] XU Tu, HE Da-ke, ZHENG Yu. Detecting DDoS attack based on one-way connection density[C]//In: Proceedings of The Tenth IEEE International Conference on Communications Systems. Singapore, IEEE CDROM，2006.

[9] MIT Lincoln Laboratory. 2000 DARPA intrusion detection scenario specific data sets. [DB/OL]. [2006-01-18]. http://www.ll.mit.edu/IST/ideval/ data/2000/2000_data_index.html.

编　辑　熊思亮