使用交叉熵检测和分类网络异常流量

颜若愚[1,2]，郑庆华[1]
(1. 西安交通大学电子与信息工程学院，710049，西安；2. 广东海洋大学信息学院，524088，广东湛江)

摘要：针对准确识别网络攻击行为的问题，提出了一种基于交叉熵的流量异常检测和分类方法. 首先使用流头部特征属性和行为特征属性对DoS攻击、端口扫描和网络扫描等3种常见攻击进行描述，并使用交叉熵来度量各属性上流量的分布变化，建立各攻击的行为特征向量，然后使用指数加权滑动平均控制图方法对多种交叉熵指标进行异常检测得到检测异常向量，最后以检测异常向量和各行为特征向量的相似度来判别攻击类型. 针对路由器中Netflow流量的实验结果表明，对于强度较小的攻击，相比香农熵度量法，交叉熵度量法的攻击分类正判率和精确率平均提高了13%和15%，正确率提高了13%.

关键词：交叉熵；异常检测；指数加权滑动平均；攻击分类
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2010)06-0010-06

Using Cross Entropy to Detect and Classify Network Anomalous Traffic

YAN Ruoyu[1,2], ZHENG Qinghua[1]
(1. School of Electronics and Information Engineering, Xi′an Jiaotong University, Xi′an 710049, China; 2. School of Information Science, Guangdong Ocean University, Zhanjiang, Guangdong 524088, China)

Abstract: A traffic anomaly detection and classification method based on cross entropy is proposed to identify network attack behaviors accurately. Both features of traffic flow header and traffic behavior are used to characterize three types of common attacks, such as DoS attacks, port scans and network scans. The cross entropy is used to measure traffic distribution changes for each traffic feature, and a behavior vector for each attack type is built. Then exponentially weighted moving average control chart method is applied to multiple cross entropy indicators for anomaly detection, and an anomaly vector is generated. The similarity between the anomaly vector and each behavior vector is computed to classify attacks. Experimental results and comparisons with the Shannon entropy measurement on Netflow traffic in a router show that under relatively weaker attacks, the true positive rate, average precision and accuracy of the cross entropy measurement in attack classification rise by 13%, 15%, and 13%, respectively.

Keywords: cross entropy; anomaly detection; exponentially weighted moving average; attack classification

网络攻击检测所面临的主要问题是如何判断网络正常活动和攻击活动. 基于特征选择的异常检测方法[1-4]是众多检测方法中应用较广泛的一种. 该方法首先从一组特征中挑选出能够准确检测异常的特征子集，然后利用这些特征对攻击行为进行准确分类，但是这种方法难以选择符合实际的特征对各种攻击类型进行恰当描述. 使用流量特征分布(如IP地址、端口号分布等)来捕捉各种网络行为是目前常

收稿日期：2009-10-18. 作者简介：颜若愚(1974—)，男，博士生；郑庆华(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60825202，60803079，60633020)；国家高技术研究发展计划资助项目(2008AA01Z131)；国家科技支撑计划资助项目(2006BAK11B02，2008BAH26B02，2009BAH51B00)；中国科学院复杂系统与智能科学重点实验室开放基金资助项目(20080101).

见的一种特征度量方法[2-4]，而且这种基于信息理论的度量方法已经成功用于检测各种类型的攻击流量，具有很好的检测效果. 文献[4]对信息熵检测能力的经验评估表明，同时使用流的头部特征属性分布和行为特征属性分布能够提高检测异常的能力，这为构造合适的流量特征子集提供了依据. 文献[5]基于 IP 地址前缀聚集提出一种区域流概念，用 3 种流量特征来描述区域之间的流量模式，并使用交叉熵度量这 3 种特征，但是该文献也仅指出交叉熵可以用来度量流量的动态变化. 文献[6]指出交叉熵可以用来检测异常流量，并采用交叉熵对 IF flow 流量进行 DDoS 攻击检测，实验结果表明交叉熵具有较好的异常检测能力，但未进一步研究其对流量的分类能力.

本文以路由器中 Netflow 流量为检测对象，提出使用交叉熵来度量流量特征的分布变化，使用流头部特征属性和行为特征属性交叉熵来定义 3 种常见攻击模式，即带宽 DoS 攻击(B/W DoS)、端口扫描(Port Scan)和网络扫描(Net Scan)，在此基础上运用指数加权滑动平均(EWMA)方法检测异常流量，采用欧氏距离判别攻击类型，结果表明交叉熵度量在异常检测和分类上具有较高的准确性.

1　使用交叉熵描述流量分布变化

1.1　信息熵理论

阶为 α 的交叉熵计算公式为

$$L_\alpha(P,Q)=\frac{1}{1-\alpha}\mathrm{lb}\sum_{i=1}^{N}\frac{p_i^\alpha}{q_i^{\alpha-1}} \tag{1}$$

式中：P、Q 是离散分布；p_i、q_i 是 P、Q 的分布函数. 交叉熵度量了分布 P 在统计区分意义上不同于分布 Q 的程度，又称相对信息. 交叉熵的一个重要特性是 $L_\alpha(P,Q)\leqslant 0$，如果 $\alpha\geqslant 0$，要使 $L_\alpha(P,Q)=0$，当且仅当 $P=Q$ 或 $\alpha=0$. 交叉熵的另外一个特性是 $L_\alpha(P,Q)$ 越小，则从一个观测点需要获得更多的信息来区分 P 和 Q，因此通过计算系统的当前观测点和前一观测点的相对信息，就可以知道当前状态偏离以前状态的程度，并判断当前状态是否异常. 为计算方便，本文选择 $\alpha=0.5$，式(1)可重写为对称形式的式(2)，使得交叉熵总是非负

$$L_{0.5}(P,Q)=-2\mathrm{lb}\sum_{i=1}^{N}(p_iq_i)^{1/2} \tag{2}$$

通常网络流量在一定时间内是稳定的，随时间发生改变的可能性很小，其交叉熵趋近为 0，但一些异常行为，如 DoS 攻击、网络扫描等会导致网络流量特征突然变化，使得 2 个连续观测点之间的交叉熵突然增大，因此可以设置阈值如 3σ 准则来检测发生的异常，如果交叉熵超过阈值则认为当前网络流量中有异常行为存在.

1.2　交叉熵和香农熵实例比较分析

为了比较交叉熵和香农熵表现流量分布变化的能力，分别使用它们度量从路由器中实际采集的流量在目的端口上的分布变化状况，图 1 为目的端口属性上的交叉熵和香农熵的时间序列. 通过比较可以发现香农熵对流量在目的端口上的分布变化反应不够灵敏，熵值变化不大，而交叉熵对分布变化的反应非常明显，即更容易凸显流量异常情况. 这主要是因为香农熵的计算只考虑到流量在某个观测点上的静态分布状况，而交叉熵不仅考虑到流量的空间分布，同时也考虑了 2 个不同观测点上流量的动态变化.

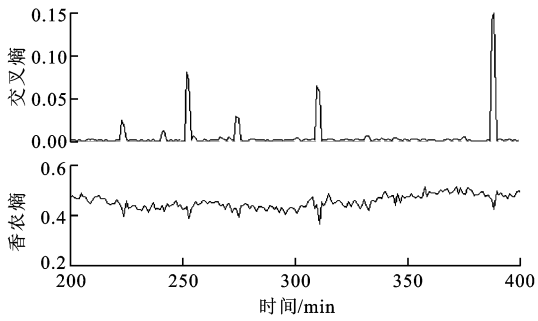

图 1　目的端口属性上的交叉熵和香农熵时间序列

2　3 种攻击模式行为特征分析和定义

2.1　2 种向量的定义

为了准确定义网络异常行为在流量中的表现模式，本文使用 7 种流量属性的交叉熵作为度量指标，其中包括流的头部特征属性(目的 IP 地址(DestIP)、源 IP 地址(SrcIP)、目的端口(DestPort)、源端口(SrcPort)、流大小(FSD))和流的行为特征属性(入度(InDegree)、出度(OutDegree)). 流大小是一个流中传输的数据包数目，入度是主动连接一个主机的所有主机数目，出度是一个主机主动连接其他主机的数目. 使用以上 7 个指标检测和分类攻击行为需要定义如下 2 种向量.

(1)检测异常向量 $\boldsymbol{A}$：使用检测方法对 7 个指标进行异常检测得到的结果向量 $\boldsymbol{A}=\{A_{\mathrm{DestIP}},A_{\mathrm{SrcIP}},A_{\mathrm{DestPort}},A_{\mathrm{SrcPort}},A_{\mathrm{FSD}},A_{\mathrm{InDegree}},A_{\mathrm{OutDegree}}\}$，其中每个元素均为二元变量{0,1}，0 代表正常，1 代表异常.

(2)行为特征向量 $\boldsymbol{S}$：攻击行为或正常行为在每

个指标上都有自己特有的行为表现，故定义行为特征向量 $\boldsymbol{S}=\{S_{\mathrm{DestIP}}, S_{\mathrm{SrcIP}}, S_{\mathrm{DestPort}}, S_{\mathrm{SrcPort}}, S_{\mathrm{FSD}}, S_{\mathrm{InDegree}}, S_{\mathrm{OutDegree}}\}$，$S_i \in \{0, 0.5, 1\}$. 其中：1 代表异常，即 top$N$ 流量发生较大变化，交叉熵增大；0 代表正常，即 top$N$ 流量基本无变化，交叉熵不变；0.5 代表 top$N$ 流量分布不确定，交叉熵随机. 下面通过这种定性的分析即可确定各攻击行为特征向量中元素的值.

由于路由器中的流量非常大，计算流量在多个属性上的分布状况需要耗费大量时间，因此影响检测的实时性. 为了加快计算速度并保证熵值的相对准确性，可以只选取属性分布最广的 N 个取值（表示为 top$N$）所汇聚的流量代替总流量来计算交叉熵，如本文使用分布最广的 20 个取值（表示为 top20）所汇聚的流量代替总流量来进行计算. 图 2 为出度属性的 3 种熵值时间序列，注意香农熵值进行了上移，以方便对照结果，可见使用香农熵对整个数据和对 top20 数据进行处理得到的熵值变化趋势几乎一样，而使用 top20 数据计算得到的交叉熵和香农熵的变化趋势非常相近.

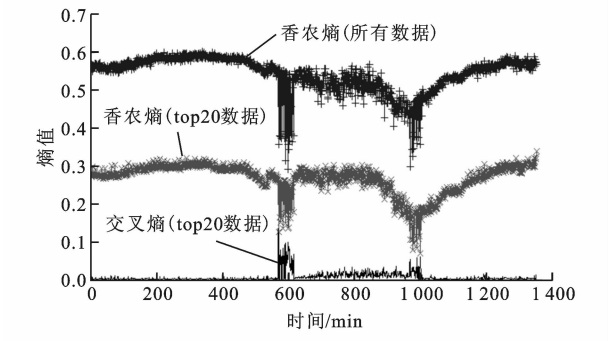

图 2 出度属性上的 3 种熵值趋势对比

2.2 3 种典型攻击的行为特征向量

（1）带宽 DoS 攻击：大量主机对一台受害主机发起攻击，每个攻击主机和受害主机建立一个固定端口的流连接，因此流量在目的地址和目的端口属性上高度集中. 出度属性值为 1 的主机数也非常多，目的地址、目的端口和出度这 3 个属性特征表现为交叉熵增大. 对于源端口，源 IP 地址和入度属性分布的影响非常小，在 top$N$ 上很难表现出来，源端口、源地址和入度这 3 个属性特征表现为交叉熵不变. 另外，流大小特征表现不确定，B/W DoS 攻击的行为特征向量为 $\boldsymbol{S}=\{1,0,1,0,0.5,0,1\}$.

（2）网络扫描：一台或多台主机对大量受害主机发起扫描，扫描主机会和受害主机建立一个固定端口的流连接，并且每个连接往往只发出一个数据包探测固定端口是否开放. 因此，流量在源地址、目的端口属性上高度集中，数据包数为 1 的流数量非常大，即流大小属性值高度集中，入度属性值固定的目的主机逐渐增多，源地址、目的端口、流大小和入度这 4 个属性特征表现为交叉熵增加，而网络扫描对目的地址和出度属性分布的影响非常小，在 top$N$ 上表现不出来，目的地址和出度这 2 个属性特征表现为交叉熵不变. 另外，源端口特征表现不确定，Net Scan 攻击的行为特征向量为 $\boldsymbol{S}=\{0,1,1,0.5,1,1,0\}$.

（3）端口扫描：一台主机对多台受害主机发起扫描，扫描主机会和受害主机建立很多具有顺序目的端口的流连接，并且每个连接只发出一个数据包探测某个端口是否开放. 因此，流量在源地址、目的地址属性上高度集中，数据包数为 1 的流数量非常大，即流大小属性值高度集中，这 3 个属性特征表现为交叉熵增加，而端口扫描对源端口、目的端口、出度和入度属性分布的影响非常小，在 top$N$ 上表现不出来，源端口、目的端口、出度和入度这 4 个属性特征表现为交叉熵不变. Port Scan 攻击的行为特征向量为 $\boldsymbol{S}=\{1,1,0,0,1,0,0\}$.

B/W DDoS、Net Scan、Port Scan 攻击的行为特征向量和正常行为（Normal）特征向量的总结如表 1 所示，正常行为在所有维度上都为正常，因此全部取值为 0.

表 1 行为特征向量表

攻击类型	S_{DestIP}	S_{SrcIP}	S_{DestPort}	S_{SrcPort}	S_{FSD}	S_{InDegree}	$S_{\mathrm{OutDegree}}$
B/W DoS	1	0	1	0	0.5	0	1
Net Scan	0	1	1	0.5	1	1	0
Port Scan	1	1	0	0	1	0	0
Normal	0	0	0	0	0	0	0

3 基于 EWMA 的流量异常检测和分类

对于一个时间序列 $X(n)$，EWMA 控制图表达式为

$$Z(i)=\lambda_1 X(i)+(1-\lambda_1)Z(i-1),\quad 0<\lambda_1<1 \tag{3}$$

式中：$X(i)$ 是 i 时刻的观测值；$Z(i)$ 是 i 时刻对下一时刻观测值的预测值；λ_1 是遗忘因子，其大小决定着预测模型对变化的响应速度，λ_1 越大模型估计值则更多地依赖最新的数据，模型对变化的响应速度

就越快.

EWMA 的上下控制界为 $X(i-1)\pm L\sigma_e(i-1)$，其中 L 为控制置信区间参数，通常 $L=2.33$，置信度为 99%，$\sigma_e(i-1)$为 $i-1$ 时刻对下一时刻误差的预测值，其计算公式为

$$\sigma_e^2(i)=\lambda_2 e^2(i-1)+(1-\lambda_2)\sigma_e^2(i-1)$$
$$0<\lambda_2<1 \qquad (4)$$

式中：λ_2 为预测误差的遗忘因子；$e(i)$为预测误差，由 $e(i)=X(i)-Z(i-1)$计算得到. 进行检测时，根据历史数据对当前时刻值进行预测，然后计算 2 条控制线，如果当前值超出上控制线或低于下控制线，则认为该时刻出现了异常. 与香农熵不同的是，流量分布发生变化(集中或分散)时，交叉熵值都会增加，因此只需使用 EWMA 的上控制线进行异常检测，减少了检测步骤.

本文利用实验的方法求得最佳预测遗忘因子 λ_1. 对 7 个指标分别用 EWMA 算法进行预测，并计算误差、误差的均值和方差，其中 λ_1 从 0.01～0.99 以 0.01 为步长取值. 实验结果显示，7 个指标的误差均值随 λ_1 增大都趋向于 0，说明预测总体较准确. 然而，不同指标的误差方差变化趋势却不相同，本文希望误差的抖动要小，即取误差方差最小时的 λ_1 值，分别得到 7 个误差指标$\{E_{\mathrm{DestIP}},E_{\mathrm{SrcIP}},E_{\mathrm{DestPort}},E_{\mathrm{SrcPort}},E_{\mathrm{FSD}},E_{\mathrm{InDegree}},E_{\mathrm{OutDegree}}\}$的最佳遗忘因子 λ_1 为$\{0.16,0.03,0.05,0.07,0.21,0.16,0.21\}$. 为了简化模型，对所有检测指标固定 $L=2.33$，即保证置信度为 99%. 另外根据文献[7]中所述，λ_2 的取值越小越好，实验中所有检测指标选取 λ_2 为 0.01.

鉴于网络攻击往往在多个流量指标上都有异常表现，因此当有 2 个及其以上指标发生异常时认为是攻击的可能性非常大，如果没有或只有 1 个观测指标出现异常，则认为是正常情况的可能性非常大. 基于以上思想，可以先计算检测异常向量 $\boldsymbol{A}$ 与正常行为特征向量 $\boldsymbol{S}$ 的欧氏距离来对异常行为进行初步判定. 如果距离 $d(\boldsymbol{A},\boldsymbol{S})>1$，则认为可能存在攻击异常，需要进行攻击分类. 在攻击分类时，以相似度最大作为选择类别的标准，即计算检测异常向量 $\boldsymbol{A}$ 与所有行为特征向量 $\boldsymbol{S}$ 的欧氏距离，选择距离值最小的那类作为该异常的类型.

4　实验结果及分析

4.1　对真实网络流量进行攻击分类

首先从西安交通大学校园网的某个路由器中采集一周的 Netflow 流量，按上述 7 种流量属性分别提取统计量，统计时间间隔为 1 min，然后计算它们的交叉熵得到 7 个检测指标；接着使用 EWMA 方法对这一周背景数据的流量指标进行异常检测，初步筛选出 404 个符合异常要求的点，仅占原数据量的 4%；最后将异常点的检测异常向量 $\boldsymbol{A}$ 分别与 B/W DoS、Port Scan、Net Scan 及 Normal 行为特征向量 $\boldsymbol{S}$ 进行相似度分析，得到如表 2 所示的检测结果.

表 2　真实流量中检测到的攻击情况

攻击类型	B/W DoS	Port Scan	Net Scan	Normal
检测个数	35	43	175	151

进一步分析 Netflow 流量发现：①分类为 B/W DoS 攻击的 35 个点中有 31 个疑似为 DoS 行为，说明分类 DoS 攻击质量比较高；②分类为 Port Scan 攻击的 43 个点中有 34 个疑似为 Port Scan 行为，分类为 Net Scan 攻击的 175 个点中有 135 个疑似为 Net Scan 行为，其他主要是网络性能变化造成的；③归类为正常行为的 151 个点都是由于网络异常变化或其他攻击造成的，导致在多个维度上出现熵值较大波动. 可见，该检测方法具有较好的检测分类性能，但对 Port Scan 和 Net Scan 攻击的分类有待提高. 误报较多的主要原因是网络性能的变化往往容易和 Port Scan 及 Net Scan 攻击相混淆，此外攻击的特征向量选取及行为特征分析对分类结果也有一定影响.

4.2　对仿真网络流量进行攻击分类

4.2.1　*仿真攻击流量的生成方法*　由于背景流量中的攻击情况已知，故可以剔除背景中攻击行为的影响，然后向背景流量中加入不同攻击类型流量. 人为加入攻击流量时遵循这样一个假设，即某一个时刻只发生一种攻击异常，不存在多个攻击同时存在，以方便验证攻击分类的效果. 网络攻击对各特征属性上的流量分布的影响主要包括 3 个方面：流量分布发生较大变化、流量分布无变化、流量分布发生随机变化，生成仿真攻击流量也即对这 3 种情况进行模拟.

(1)仿真分布发生较大变化的流量：在某个特征属性流量聚集中加入一个攻击引起的流量变量，该变量取值为攻击前一时刻该属性上 top20 流量聚集和的 10%，这个值可看作为攻击强度. 该流量变量生成后加入到当前的 top20 流量中进行由大到小排序，得到新的 top20 流量，该 top20 流量即仿真了一个攻击在该属性上的流量分布影响. 基于这种方式

仿真流量分布发生较大变化的理由是：top20 流量对流量分布的贡献在正常情况下是相对稳定的，即分布变化很小，但是一旦有攻击发生，流量分布中某个统计量会发生显著改变，导致 top20 流量不再稳定，从而使得分布发生显著变化.

(2)仿真分布基本无变化的流量：仿真 top20 流量基本无变化时，使用攻击前一时刻和当前时刻该属性上 top20 流量的均值作为当前新的 top20 流量.

(3)仿真分布变化不确定的流量：为了准确仿真变化不确定的流量，本文定义相对变化度来表示 2 个相邻时刻上流量发生变化的程度. 2 个相邻时刻点 $i-1$、i 上 top$N$ 流量中第 j 个数值即 top$(i-1,j)$和 top(i,j)的相对变化度的计算公式为 $r(i,j)=|\text{top}(i,j)-\text{top}(i-1,j)|/\max(\text{top}(i,j),\text{top}(i-1,j))$，该式表明变化度越高，2 个时刻的流量变化越大. 根据对真实数据的观察，2 个相邻时刻点上 top20 流量的变化都较小，以 destIP 属性为例，其相对变化度在 0～0.5 以内的概率为 95%. 仿真时以前一时刻点流量分布为依据按统计的概率情况和相对变化度以增加或减少流量的方式随机生成 20 个流量变量，然后和当前时刻的 top20 流量一起由大到小排序确定新的 top20 流量.

(4)攻击流量仿真步骤：首先将背景流量中确定为异常的点除去，然后从背景流量中随机抽取一段长度为 100 的序列，随机选择异常发生的时刻，确定攻击强度和持续时间，使用以上仿真方法根据不同攻击类型的行为特征向量生成攻击流量. 考虑到真实环境中异常与正常的比例情况，每次攻击时间选取为 1 min. 基于上述仿真步骤对每一种攻击类型分别产生攻击强度为 10%的 100 个攻击样本用于实验.

4.2.2 分类结果及分析 本文方法分类结果如表 3 所示，可见分类的总体效果很好，但是 Port Scan 和Net Scan类型的攻击被误判为正常的情况较多，主要原因是仿真流量的攻击强度太小.

表 3 模拟攻击强度为 10%的 3 种攻击类型的分类结果

真实类型	分类结果样本数				总计
	B/W DoS	PortScan	NetScan	Normal	
B/W DoS	94	0	0	6	100
Port Scan	4	82	4	10	100
Net Scan	4	2	78	16	100
所有攻击	102	84	82	32	300

为了比较分别以交叉熵和香农熵为度量对流量进行分类的能力，定义如下指标. ①总正确率：分类正确的样本总数占测试样本总数的比例. ②正判率：判断正确的样本数占该类样本总数的比例. ③精确率：判断正确的样本数占分为该类的样本数的比例.

使用香农熵进行检测分类的方法步骤和使用交叉熵的一样，不同的是流量分布的集中或分散会使香农熵变小或增大，因此在使用 EWMA 检测异常时要使用上下控制线，增加了计算开销. 2 种度量方法对 3 种仿真攻击的分类评价结果如表 4 所示，对于所有 3 种攻击，交叉熵和香农熵分类结果的总正确率分别为 84.7%和 71.7%. 表 4 的结果显示：①相比香农熵度量法，交叉熵度量法无论在总正确率、精确率和正判率上都要占优，总正确率提高了 13%，精确率平均提高了近 15%，正判率平均提高了 13%，尤其是针对 Net Scan 攻击的正判率比香农熵提高了 24%；②2 种度量方法对 B/W DoS 攻击的分类效果非常好，说明 B/W DoS 的行为特征向量准确描述了该攻击的特性，但对 Port Scan 和 Net Scan 攻击的分类效果要差一些，尤其是香农熵度量对 Net Scan 攻击的分类很差，只有 54%的正判率，究其原因可能有 2 个，一是行为特征向量的定义可能不是很适当，二是攻击强度太弱，导致一些攻击难以被检测到.

表 4 2 种度量的分类评价结果

攻击类型	交叉熵分类结果		香农熵分类结果	
	正判率/%	精确率/%	正判率/%	精确率/%
B/W DoS	94	92.0	86	84.3
Port Scan	82	97.6	75	80.6
Net Scan	78	95.1	54	77.1

5 结论与展望

本文方法能够对路由器中大规模流量进行异常检测及分类，并具有较强的实际检测分类能力. 基于仿真流量的实验结果表明，即使是强度较小的攻击，基于交叉熵度量的方法比基于香农熵度量的方法具有更高的检测和识别能力. 为了进一步提高检测和分类的总体正确率，将来可以对流量属性和攻击行为特征做进一步的研究，选择更合适的流量属性来描述各种网络行为特征. 此外，在检测过程中如何使 EWMA 算法中的参数能够自适应调整也是一项重

要的工作.

参考文献：

[1] 陈光英，张千里，李星. 基于 SVM 分类机的入侵检测系统[J]. 通信学报，2002，23 (5)：51-56.
CHEN Guangying，ZHANG Qianli，LI Xing. SVM classification-based intrusion detection system [J]. Journal of China Institute of Communications，2002，23 (5)：51-56.

[2] KRISHAN K，JOSHIL R C，KULDIP S. A distributed approach using entropy to detect DDoS attacks in ISP domain [C]// Proceedings of International Conference on Signal Processing，Communications and Networking. Piscataway，NJ，USA：IEEE，2007：331-337.

[3] ANUKOOL L，MARK C，CHRISTOPHE D. Mining Anomalies using traffic feature distributions [C]// Proceedings of Special Interest Group on Data Communication Conference. New York，USA：ACM，2005：217-228.

[4] GEORGE N，VYAS S，DAVID G，et al. An empirical evaluation of entropy-based traffic anomaly detection [C]// Proceedings of Internet Measurement Conference. New York，USA：ACM，2008：151-156.

[5] QIN Tao，GUAN Xiaohong，LI Wei，et al. Dynamic features measurement and analysis for large-scale networks [C]// Proceedings of International Conference on Communications. Piscataway，NJ，USA：IEEE，2008：212-216.

[6] YAN Ruoyu，ZHENG Qinhua. Using renyi cross entropy to analyze traffic matrix and detect DDoS attacks [J]. Information Technology Journal，2009，8(8)：1180-1188.

[7] MONTGOMERY D C，MASTRANGELO C M. Some statistical process control methods for autocorrelated data [J]. Journal of Quality Technology，1991，23 (3)：179-193.

（编辑　刘杨　苗凌）