基于流量结构稳定性的服务器网络行为描述：建模与系统

邵国林，陈兴蜀，尹学渊，叶晓鸣

(四川大学计算机学院 成都 610065)

【摘要】针对现有基于异常特征库匹配的流量检测方法难以适应日趋复杂的网络环境需要的问题，对服务器网络流量进行了大量观测和研究，综合正常流量在某些属性上的固有稳定性及特定服务在流量层面表现出的稳定性，提取相应的流量特征，同时提出了流量结构稳定性的概念，并基于此对服务器的正常网络行为轮廓进行刻画，依据当前流量结构偏离正常轮廓的程度对服务器网络异常行为进行检测。针对流量结构差异性的定量刻画问题，提出了一种基于Spie Chart的可视化度量方法，并基于一台邮件服务器流量实现了系统，通过实验验证了系统对常见网络攻击及未知网络异常的检测效果。

关 键 词 正常行为模型； 服务器安全防护； 网络异常检测； 流量结构稳定性

中图分类号 TP393.08 文献标志码 A doi:10.3969/j.issn.1001-0548.2017.01.016

Profiling Structure-Stability-Based Server Traffic: Behavior Models and System

SHAO Guo-lin, CHEN Xing-shu, YIN Xue-yuan, and YE Xiao-ming

(College of Computer Science, Sichuan University Chengdu 610065)

Abstract Server as an important part of the institutions or organizations usually carries a particular network service, for the security protection, it usually adopts rule-based approaches to detecting attacks according to the specific characters. However, due to the new network attacks emerge in endlessly and network anomaly is difficult to define, anomaly-feature-based detection is more and more difficult to meet the needs of the increasingly complex network environment. To cope with it, we propose the concept of traffic structure stability based on both the inherent stability of normal traffic attributes and the stability of a specific service, and profile the normal network behavior model for the server to detect traffic abnormality. To describe the difference between current traffic structure and the normal profile, we propose a novel visualization measurement method based on Spie Chart. Finally, we implement the system on a mail server and confirm the validity of the model by experiments.

Key words normal behavior model; server security; traffic abnormality detection; traffic structure stability

服务器通常作为IT系统中的核心设备通过网络对外界提供特定服务，因此服务器的安全防护显得尤为重要。现有的服务器网络安全防护从研究手段方面，可主要分为以下3类：

1) 基于主机或网络边界的IDS、IPS研究；

2) 基于服务器日志关联分析与挖掘；

3) 基于服务器网络流量分析。

IDS、IPS研究主要根据入侵检测的思想编写特定的攻击流量特征，对非法网络请求进行告警和防护。SNORT[1]是目前最常用的轻量级网络入侵检测系统，此外也有许多研究[2-4]基于SNORT进行改进，提出了入侵检测模型。基于日志的服务器安全检测主要通过数据挖掘[5-6]、关联分析[7-8]等方法对服务器各方面的日志信息进行全方位的分析，从而检测服务器面临的攻击和潜在威胁。目前从流量分析角度检测服务器网络异常的研究较多，根据流量分析方法，主要分为基于统计分析、信号处理、数据挖掘、机器学习等研究方法。文献[9]从流量自相似统计特性的角度提出了异常流量检测模型；文献[10]提出了基于小波分析的网络流量异常检测方法；文献[11]基于数据挖掘算法抽取流量特征，利用K-Means聚类方法自适应的产生模型检测Dos攻击；文献[12]将K-Means聚类算法和ID3决策树学习算法用于网络异常流量的检测。文献[13]提出了一种基于贝叶斯网络与时间序列分析的异常流量检测方法。

现有的检测方法主要基于误用检测的思路，针

收稿日期：2015－07－21；修回日期：2016－01－15

基金项目：国家自然科学基金(61272447)；国家科技支撑计划(2012BAH18B05)

作者简介：邵国林(1991－)，男，博士生，主要从事计算机网络与信息安全方面的研究.

对特定的网络攻击特点，编写特定的流量检测规则，从而形成一个已知攻击特征库，然后将采集的流量数据与特征库一一匹配，若匹配某项特征，则对异常报警输出[14]。基于误用(基于异常特征)的检测方法的缺点是，必须针对每种攻击编写对应的规则，系统需要维护庞大的特征库。然而随着网络及应用环境日趋复杂，原有策略难以检测出层出不穷的新型网络攻击，而且在不同应用场景下，对网络异常的界定更是存在许多分歧(除网络攻击外，网络配置错误和用户操作异常等原因都会导致网络异常)，因此基于异常特征的检测方法适应性及扩展性日益难以满足防护需求。

针对上述问题，本文采用基于时间序列的流量统计方法，对某邮件服务器流量进行了长时间的流量观测，对能够表现流量结构稳定性的属性及方法进行了研究。本文研究发现，正常网络流量在某些属性上表现出一定的稳定性，同时特定服务在流量层面也表现出一定的稳定性。本文根据以上研究成果提取出相应的网络流量特征，提出了流量结构稳定性的概念，然后基于流量结构稳定性对服务器的正常网络行为进行刻画。本文基于上述模型实现了服务器网络行为描述系统，并通过实验验证了正常情况下流量结构稳定性的存在，以及根据流量结构偏离正常轮廓的程度进行异常检测的有效性。

1　流量结构稳定性研究及特征分析

1.1　基于统计的流量结构描述

为了刻画和表示服务器网络正常模型，本文对某邮件服务器进行了长时间的流量观测，对流量在各个方面的属性进行了研究，提取出能够表征流量稳定的属性。为了刻画流量的状态和稳定性，本文基于流量稳定属性提出了流量结构及流量结构稳定性的概念。

定义 1(流量结构)　一定期间网络流量各属性值的大小、规模、分布、及变化的综合状态，说明网络流量在特定时间内的统计特性和综合表现情况。

流量结构主要包括两层含义：各流量属性及属性间的构成关系。本文主要基于熵、相关性等数学方法，对特定时间窗口内的流量统计属性进行描述，综合各属性值以及各属性在系统中的构成(所占比重)表示流量结构的概念。

定义 2(流量结构稳定性)　对一定期间网络流量结构的变动程度的刻画，表现了网络在流量层面的稳定情况。

本文研究发现服务器网络流量在某些属性上表现出一定的稳定性，具体表现在SYN包比例、IP信息熵和相关性、TTL分布、端口分布、协议分布、包长分布、端口访问数等方面。因此，本文从正常网络流量的固有稳定性和特定服务的流量稳定性表现两方面入手，以流量结构的稳定性作为网络流量稳定的描述手段，对服务器网络流量正常模型进行研究。正常网络流量的固有稳定性表现出正常流量在任何应用和场景下，流量在某些属性上都表现出的稳定性，当这类属性严重偏离正常值时，通常当前网络异常。特定服务的流量稳定性表现表示的是由服务器承载的特定服务和应用带来的在流量层面的稳定性表现，当这类稳定性减弱时，通常表示服务器由于某种因素干扰而无法提供正常服务。

信息熵可以获取流量特征在分布变化上的有效信息[15]，相关性能有效检测流量突发情形(如DDos攻击[16])，本文根据各属性的属性值特点及稳定性情况采取信息熵、相关性等表示方法，选取了若干流量特征，对流量结构进行描述。

1.2　正常网络流量的固有稳定性及特征提取

正常网络流量在某些属性上表现出固有的稳定性，不因服务和应用的不同而有所差异，且其稳定性易显著地被攻击流量扰动，因此正常流量固有的稳定性能够刻画正常网络流量的轮廓，同时将异常网络流量区分开来。如流量中的SYN包比例通常较小，当流量达到一定规模时，即使在短时间内也能表现出一定的稳定性；如果网络中SYN包比例突然显著增大，则说明服务器的网络流量在某些方面出现了异常。

本文对正常情况下网络流量在各属性上的稳定性表现进行了研究，选取若干稳定性效果较好的属性进行了深入分析，图1为SYN包比例、IP信息熵、IP相关性、TTL分布4类流量属性在连续1 000个时间窗口内的统计结果，由图可看出各属性在属性值上具有较稳定的分布。其中SYN包比例稳定于10^{-2}数量级；IP信息熵属性值稳定维持于4左右；IP相关性基本在0.99以上；TTL属性值分布稳定，在64及52处出现概率最大。

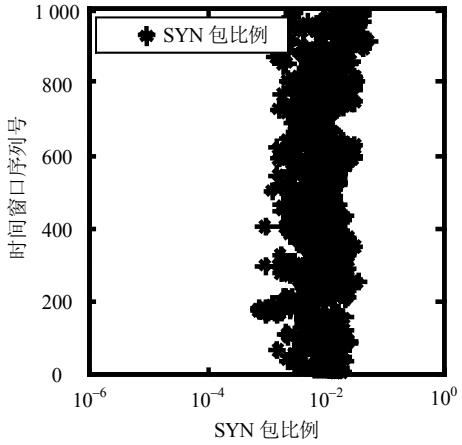
本文根据这些属性特点分别提取出对应的流量特征：

1) SYN包比例：SYN包占总包数的比例；

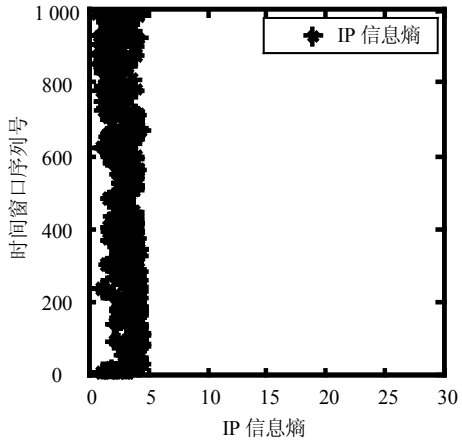
2) IP信息熵：根据信息熵定义，针对IP序列中各IP对应流量占比求取的熵值；

3) IP相关性：当前时间窗口内IP序列及各IP对应流量与上一时间窗口的相关性；

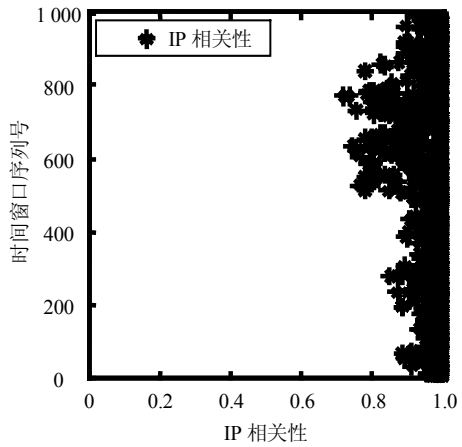
4) TTL分布熵：根据信息熵定义，针对各TTL对应流量占比求取的熵值。需要注明的是，本文主要采取基于时间序列的统计方法，因此各网络特征都是特定时间窗口内的统计结果；此外，为了便于计算和比较，特征2)和特征3)对IP进行了映射处理，IP代指映射后的逻辑IP。



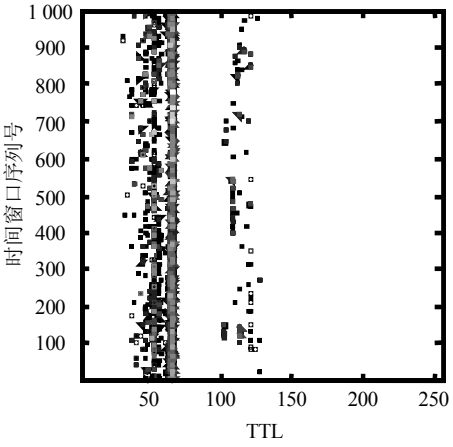
a. SYN包比例分布



b. IP信息熵分布



c. IP相关性分布

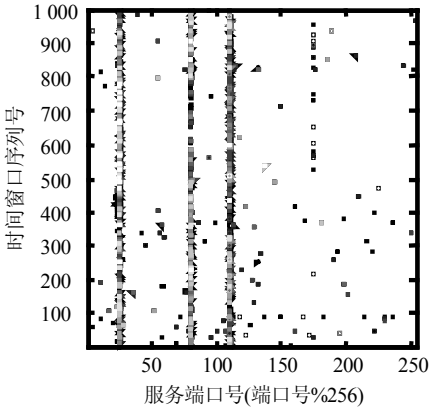


d. TTL属性值分布

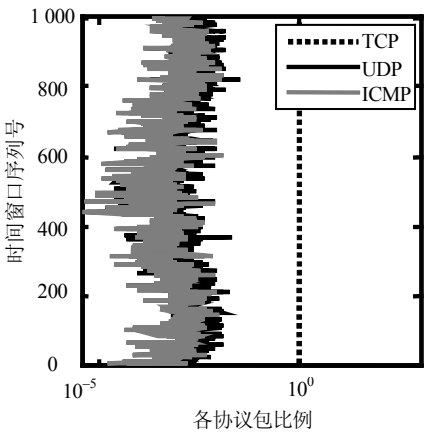
图1 正常网络流量固有属性的稳定性表现

1.3 特定服务表现的流量稳定性及特征提取

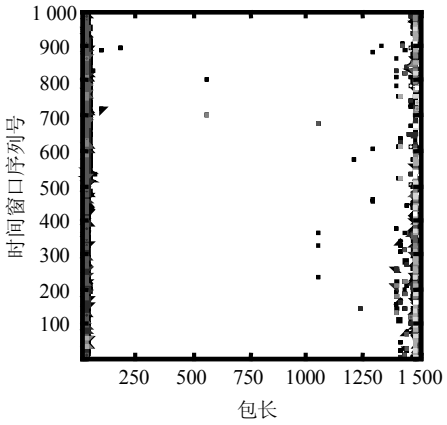
通常由于特定服务和应用的特点、以及相关用户的生活、工作习惯等特点，也能够导致流量在某些属性表现出稳定性，这种由业务特性以及用户特性带来的宏观稳定性通常不具有一般性，而由服务器的功能决定。如对于一台邮件服务器而言，其SMTP及POP3的流量必然占大多数，假如网络中P2P流量激增，则表明网络出现异常。



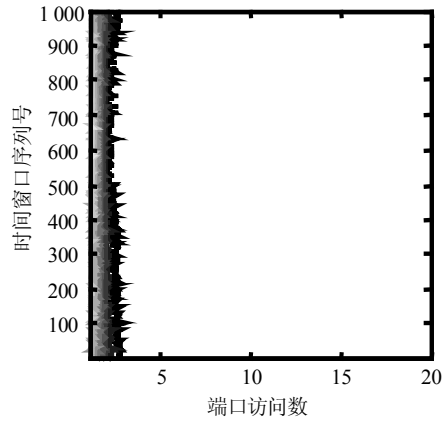
a. 服务端口号分布



b. 各类协议数据包比例分布



c. 包长分布



d. 端口访问数分布

图2　特定网络服务的流量稳定性表现

图2是对一台邮件服务器流量属性研究的统计结果，由图可看出流量在服务端口号分布、协议分布、数据包长分布、端口数访问情况等属性上具有较稳定分布，其中服务端口号分布集中于25(SMTP)、80(HTTP)及110(POP3)，与邮件服务器职责相匹配；各类协议的数据包比例分布较稳定；由IP包负载长度可知网络中主要是短包和长包；绝大多数IP访问服务器端口数小于3。

本文根据以上研究成果分别提取出对应的流量特征：

1) 端口号分布熵：根据信息熵定义，针对各端口号对应流量占比求取的熵值；

2) 协议分布熵：根据各协议对应流量占比求取的熵值；

3) 包长分布熵：根据各包长对应流量占比求取的熵值；

4) 端口访问指数：以每个IP访问服务器端口数目为研究对象，综合端口数目和该数目出现概率对其进行刻画，数目越大且出现概率越低，对应的端口访问指数越大。

2　基于流量统计的服务器行为建模

2.1　服务器动态网络行为轮廓描述

通过观测发现，流量各属性在较短时间内具有相对的稳定性，在较长时间内则存在缓慢的周期变化过程。大量研究表明，网络流量存在明显的周期性[17-19]，因此，难以使用一个静态的、恒定不变的网络行为轮廓对服务器在任一时刻的网络行为进行描述。本文基于此提出了动态网络行为轮廓对服务器流量正常轮廓进行描述。

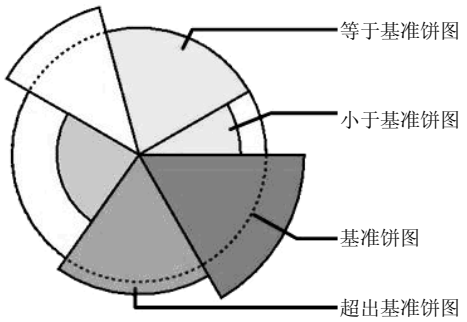
定义 3(动态网络行为轮廓)　不定义一个静态的、固定的正常流量轮廓，而是充分考虑当前流量规模及特点，从而定义一个适合描述当前流量结构的正常轮廓。

由于邻近时间窗口间的业务水平及流量结构相当，因此，本文基于当前时间窗口前N个无明显异常的历史流量数据构建当前时刻的动态网络行为轮廓。为了消除历史数据中的异常值，本文主要基于格拉布斯准则[20]对异常数据(离群值)进行分析剔除，从而获得正常的历史数据用于构建适合描述当前流量结构的正常轮廓。

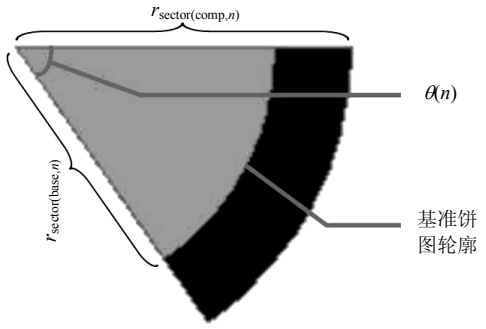
正常网络行为轮廓流量结构包括两部分内容：各属性的参照值及各属性在流量结构中的构成(比重)。属性参照值主要根据正常历史数据平均求得，比重通过各属性的稳定性求得。基于动态网络行为轮廓的稳定性描述方法充分考虑了正常网络行为轮廓随时段周期性变化的过程，对异常检测更具有参考意义。

2.2　服务器异常行为检测

本文提出了一种基于Spie Chart[21]的可视化度量方法，Spie Chart如图3a所示，基准饼图固定了扇形角度，比较饼图叠加在基准饼图之上，每个扇形半径偏离基准饼图的程度反映了每个构成的相对变化，这样Spie Chart强调了构成，又反映了构成的变化，从而有效衡量两个相同构成饼图的差异性。



a. Spie Chart示意图



b. Spie Chart差异性度量示意图

图3 Spie Chart及差异性度量示意图

本文将正常网络行为轮廓的流量结构作为基准饼图，将当前网络流量结构作为比较饼图，每个扇形表示流量结构的一个特征，将两个饼图对应扇形的面积差作为偏离度的衡量值。为了方便描述，令每个饼图的扇形数为N，$r_{\text{sector(base,}n)}$、$r_{\text{sector(comp,}n)}$分别为基准饼图及比较饼图的第$n$个扇形半径。在Spie Chart中，将$r_{\text{sector(base,}n)}$设为1，表示正常网络行为轮廓，$r_{\text{sector(comp,}n)}$则为实际网络流量结构特征值与正常轮廓中对应特征值(正常参考值)的比值。本文以基准饼图与比较饼图的差异作为差异性的度量依据，即图3b中黑色部分面积。

由于每个特征的稳定性存在差别，因此各特征对应的扇形角度不同，这里使用稳定系数描述，第n个扇形的稳定系数表示为$\alpha(n)$，$\alpha(n)$越大表明越稳定。特征的稳定系数决定了对应扇形的角度$\theta(n)$，扇形的角度越大，对最终计算差异性$\text{diff}(n)$影响越大。

1) 扇形角度$\theta(n)$

$\alpha(n)$反映了每个特征对差异值影响力的大小，在饼图中则通过对应扇形角度$\theta(n)$体现。$\theta(n)$根据$\alpha(n)$通过式(1)计算：

$$\theta(n)=\frac{2\pi\alpha(n)}{\sum_{i=1}^{N}\alpha(i)} \tag{1}$$

2) 稳定系数$\alpha(n)$

稳定系数$\alpha(n)$反映了特征n正常情形的稳定程度，本文基于变异系数c_v描述$\alpha(n)$，变异系数是反映数据变动度的绝对指标，对多组数据的大小、量纲等性质无要求，适于确定多指标综合评价中的权系数[22]，c_v通过式(2)计算：

$$c_v=\frac{\sigma}{\mu} \tag{2}$$

式中，c_v为变异系数；σ为标准差；μ为平均值。c_v越小，说明数据越不易变动，对应的稳定性系数也越大，因此c_v与$\alpha(n)$存在反相关关系，本文通过对数形式表示反相关性，基于式(3)计算$\alpha(n)$：

$$\alpha(n)=-\ln\left(\frac{c_v(n)}{\sum_{i=1}^{N}c_v(i)}\right) \tag{3}$$

3) 差异性度量

本文基于Spie Chart扇形面积差度量当前流量结构与正常网络轮廓的偏离度，差异性$\text{diff}(n)$可通过式(4)计算求得，当$\text{diff}(n)$超过特定阈值时，说明当前流量结构偏离正常轮廓的程度较大，从而判定为异常：

$$\text{diff}(n)=\frac{1}{2}\sum_{n=1}^{N}\theta(n)\left|r_{\text{sector(comp,}n)}^{\ 2}-r_{\text{sector(base,}n)}^{\ 2}\right| \tag{4}$$

3 网络行为描述系统及有效性验证

3.1 邮件服务器网络行为描述系统

为了验证该模型的有效性，本文基于某邮件服务器流量构建并部署了服务器网络行为描述系统，对服务器网络流量进行监测，同时通过实施攻击实验观察流量结构的变化情况。

系统工作流程为：1) 针对流量结构各特征基于时间序列对流量进行统计。2) 基于前120个时间窗口的历史数据构建正常网络行为轮廓(首先基于格拉布斯准则剔除历史数据中的异常值，基于正常值的均值确定正常参考值；其次基于各特征值在历史数据中表现出的稳定性求稳定系数及扇形角度，即确定各特征的权重)。3) 基于当前时间窗口的实际流量结构和正常网络行为轮廓，根据本文提出的Spie Chart差异性度量方法计算偏离度。4) 若偏离度超过特定阈值，则对异常进行告警。

由于不同服务器及不同的网络环境表现出的稳定性不同，因此偏离度阈值也应不同。本文阈值设定方法是：基于格拉布斯准则将偏离度历史数据中的正常值和异常值分开，计算各自均值，然后以二者中间值作为阈值。

为了验证该系统对异常流量的检测效果，本文从已知异常(网络攻击)检测和未知异常检测两个方面进行分析。

3.2 针对已知异常的检测验证

本文主要通过对服务器实施常见的网络攻击实现对已知异常检测的效果评估。表1是系统对端口扫描、SYN Dos及UDP Flood 3种常见网络攻击的检测效果。针对不同的攻击类型，实验分别选取了3种不同的攻击规模(表示每个时间窗口内的探测次数)，共

实施了9组实验，每组实验实施30次攻击。

表1　针对网络攻击的检测结果

攻击类型	攻击规模	攻击次数	检测次数	平均差异值	检测率/%
Port Scan	120	30	5	3.49	16.7
Port Scan	240	30	30	8.92	100
Port Scan	600	30	30	40.32	100
SYN Dos	600	30	11	4.021	36.7
SYN Dos	1 800	30	28	18.84	93.3
SYN Dos	3 000	30	30	38.94	100
UDP Flood	600	30	24	9.29	80
UDP Flood	1 200	30	28	20.41	93.3
UDP Flood	1 800	30	30	30.84	100

结果显示系统对端口扫描具有较灵敏的检测效果，当攻击规模达到240时，检测率就已达到100%，随着攻击规模加大，异常值也在增大。当攻击规模分别达到1 800和1 200时，SYN Dos和UDP Flood的检测率都能达到93.3%，随着攻击规模的增大，检测率和差异值也在不断增大。由实验结果可知，系统对能够影响网络流量结构的常见网络攻击具有较好的检测效果。

3.3　针对未知异常的检测验证

针对未知异常的检测结果如表2所示，包括3列数据，分别表示正常情形、某周期性网络异常及某次邮件密码暴力破解3类情形下的流量结构变化情况。理论正常情形是各流量特征与正常轮廓对应特征相等(即表中各特征值为1)，差异值为0，但是网络不可能是一成不变的。表中第1列数据是对43 200个时间窗口(30 d)流量结构数据经格拉布斯准则剔除异常值后的均值统计结果，由表中数据可看出正常情形下各特征较稳定，流量结构与正常轮廓差异较小，同时这也验证了流量结构稳定性的存在。

表2中第2列数据表示的是系统从邮件服务器流量中检测出的某类未知网络异常的流量结构。流量监测数据显示，异常发生期间TCP连接数、网络数据包数、SYN包数显著增大，分别达到邻近时刻数据水平的6倍、10倍和8倍左右，使流量结构在各方面偏离正常轮廓，差异值达到19.448。鉴于该异常长期且持续发生于每天早上6:22左右，时间和模式较固定，因此猜测可能是邮件服务器自身某项定时功能或配置导致的网络异常。

表2中第3列数据表示的是某次异常事件的流量结构，数据显示异常发生期间SYN包比例、端口分布熵、协议分布熵等变化较剧烈，总差异值达到14.824。分析原始数据发现为一次邮件密码暴力破解活动，持续时间近3 min，共进行了13 298次密码猜解。

表2　针对未知异常的检测结果

统计项目	类型		
	正常流量均值	周期性网络异常	密码暴力破解
SYN包比例	1.061	4.621	7.996
IP信息熵	0.996	1.730	0.714
IP相关性	0.999	0.998	1.001
TTL分布熵	0.991	1.361	0.617
端口号分布熵	1.013	4.473	0.322
协议分布熵	1.108	0.445	0.082
包长分布熵	0.990	1.616	0.765
端口访问指数	1.031	6.154	0.548
差异值	1.027	19.448	14.824

研究过程发现，针对不同的网络异常，其所影响的流量结构属性及程度也各不相同。如SYN Dos攻击对SYN比例影响巨大，端口扫描对端口访问指数影响巨大，UDP Flood对协议分布熵影响较大，某周期性网络异常对端口访问指数等影响较大，密码暴力破解对SYN比例及协议分布熵影响较大。而研究过程中也发现，IP相关性在许多网络异常期间一直较稳定，主要原因是已考察的网络异常都未能明显改变访问服务器的IP列表，IP相关性如果出现明显扰动，则可能预示着分布式网络攻击的发生。因此对于流量结构而言，所包含的稳定性属性越全面，其所代表的流量状态也越准确。

4　结 束 语

本文基于流量结构的稳定性对服务器正常网络行为进行建模，根据当前网络流量结构与正常轮廓的偏离度进行流量异常检测。本文从正常流量固有稳定性及业务特性、用户特性等表现的流量稳定性两方面，对流量属性进行了深入研究，基于信息熵、相关性等方法提取了若干流量特征描述流量结构。针对正常流量轮廓随业务强度在不同时段周期性变化的问题，提出了根据临近时间窗口的流量结构构建动态网络行为轮廓的概念，从而使正常轮廓更具参考意义。为了对流量结构的偏离程度定量描述，提出了一种基于Spie Chart扇形面积差的度量方法。本文基于流量结构稳定性的服务器网络行为模型在一台邮件服务器上构建了系统进行验证，证明了流量结构稳定性的存在，同时该系统对常见网络攻击及未知网络流量异常都具有较好检测效果。然而当前提取的流量属性还较单一，依据流量结构稳定性的评判依据，提取和选择出更多来源和粒度的属性表示流量结构，是下一步的研究方向。

参 考 文 献

[1] ROESCH M. Snort: Lightweight intrusion detection for networks[C]//LISA. Washington, USA: ACM, 1999: 99: 229-238.

[2] 郑礼良, 吴国凤, 胡晓明, 等. 基于Snort的入侵检测系统的研究与改进[J]. 合肥工业大学学报: 自然科学版, 2011, 34(4): 529-532.
ZHENG Li-liang, WU Guo-feng, HU Xiao-ming, et al. Research on intrusion detection system based on Snort and its improvement[J]. Journal of Hefei University of Technology (Natural Science), 2011, 34(4): 529-532.

[3] SAGANOWSKI Ł, GONCERZEWICZ M, ANDRYSIAK T. Anomaly detection preprocessor for Snort IDS system[M]//Image Processing and Communications Challenges 4. Berlin Heidelberg: Springer, 2013: 225-232.

[4] WANG H X, CHENG G Y, HAN Y F. Research on increasing speed of rule-matching in Snort[J]. Computer & Information Technology, 2013, 21(1): 30-33.

[5] 郁继锋. 基于数据挖掘的Web应用入侵异常检测研究[D]. 武汉: 华中科技大学, 2011.
YU Ji-feng. Research on anomaly intrusion detection od Web application based on data mining[D]. Wuhan: Huazhong University of Science and Technology, 2011.

[6] 雷惊鹏, 颜世波. 基于Windows日志的主机入侵检测[J]. 吉林工程技术师范学院学报, 2013, 29(1): 71-72.
LEI Jing-peng, YAN Shi-bo. Host intrusion detection based on windows log[J]. Journal of Jilin Teachers Institute of Engineering and Technology, 2013, 29(1): 71-72.

[7] 何鹏程, 方勇. 一种基于Web日志和网站参数的入侵检测和风险评估模型的研究[J]. 信息网络安全, 2015(1): 61-65.
HE Peng-cheng, FANG Yong. A risk assessment model of intrusion detection for Web applications based on Web server logs and website parameters[J]. Netinfo Security, 2015(1): 61-65.

[8] 周丽, 王小玲. 基于网络审计日志关联规则挖掘的改进[J]. 计算机技术与发展, 2011, 21(6): 150-153.
ZHOU Li, WANG Xiao-lin. Improved algorithm for association rules mining based on network audit record[J]. Computer Technology and Development, 2011, 21(6): 150-153.

[9] 贾慧, 高仲合. 基于自相似的异常流量检测模型[J]. 通信技术, 2010, 43(12): 115-117.
JIA Hui, GAO Zhong-he. Anomalous-traffic detection model based on self-similarity[J]. Communications Technology, 2010, 43(12): 115-117.

[10] DAINOTTI A, PESCAPÉ A, VENTRE G. NIS04-1: Wavelet-based detection of DoS attacks[C]//Global Telecommunications Conference, 2006, GLOBECOM'06. [S.l.]: IEEE, 2006: 1-6.

[11] 高能, 冯登国, 向继. 一种基于数据挖掘的拒绝服务攻击检测技术[J]. 计算机学报, 2006, 29(6): 944-951.
GAO Neng, FENG Deng-guo, XIANG Ji. A data-mining based DoS detection technique[J]. Chinese Journal of Computers, 2006, 29(6): 944-951.

[12] YASAMI Y, MOZAFFARI S P. A novel unsupervised classification approach for network anomaly detection by k-Means clustering and ID3 decision tree learning methods[J]. The Journal of Supercomputing, 2010, 53(1): 231-245.

[13] KLINE J, NAM S, BARFORD P, et al. Traffic anomaly detection at fine time scales with bayes nets[C]//Internet Monitoring and Protection, 2008, ICIMP'08. [S.l.]: IEEE, 2008: 37-46.

[14] 程柏良, 周洪波, 钟林辉. 基于异常与误用的入侵检测系统[J]. 计算机工程与设计, 2007, 28(14):3341-3343.
CHENG Bai-liang, ZHOU Hong-bo, ZHONG Lin-hui. Intrusion detection system based on anomaly and misuse[J]. Computer Engineering and Design, 2007, 28(14): 3341-3343.

[15] 杜鑫, 杨英杰, 常德显. 基于特征分布分析的网络流量监测系统[J]. 计算机工程, 2009, 35(6): 116-118.
DU Xin, YANG Ying-jie, CHANG De-xian. Network traffic supervision system based on feature distribution analysis[J]. Computer Engineering, 2009, 35(6): 116-118.

[16] 王忠民. 基于统计分析的DDoS攻击检测的研究[D]. 河北, 秦皇岛: 燕山大学, 2012.
WANG Zhong-ming. Dos attack detection based on the stastical analysis[D]. Qinhuangdao, Hebei: Yanshan University, 2012.

[17] 张凤荔, 赵永亮, 王丹, 等. 基于流量特征的网络流量预测研究[J]. 计算机科学, 2014, 41(4): 86-89.
ZHANG Feng-li, ZHAO Yong-liang, WANG Dan, et al. Prediction of network traffic based on traffic characteristic[J]. Computer Scienc, 2014, 41(4): 86-89.

[18] 朱倩雨. 网络流量预测模型的研究[D]. 乌鲁木齐: 新疆大学, 2014.
ZHU Qian-yu, Research on prediction model of network traffic[D]. Wulumuqi: Xinjiang University, 2014.

[19] 邵雪梅. 校园网流量测量与性能优化研究[D]. 合肥: 合肥工业大学, 2013.
SHAO Xue-mei. Research on campus network traffic measurement and performance optimization[D]. Hefei: Hefei University of Technology, 2014.

[20] 孙培强. 正确选择统计判别法剔除异常值[J]. 计量技术, 2013(11): 71-73.
SUN Pei-qiang. Correct selection of statistical criterion to eliminate outliers[J]. Measurement Technique, 2013(11): 71-73.

[21] FEITELSON D G. Comparing partitions with Spie Charts[EB/OL]. [2015-04-20]. http://www.cs.huji.ac.il/~feit/papers/Spie03TR.pdf.

[22] 王明涛. 多指标综合评价中权数确定的离差, 均方差决策方法[J]. 中国软科学, 1999(8): 100-101.
WANG Ming-tao. The dispersion and mean square deviation decision method: Determination of the weight in multiple-parameters comprehensive evaluation[J]. China Soft Science, 1999(8): 100-101.

编 辑 漆 蓉