ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.10, October 2009, pp.2899−2906
doi: 10.3724/SP.J.1001.2009.03685

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于概要数据结构可溯源的异常检测方法*

罗 娜+, 李爱平, 吴泉源, 陆华彪

(国防科学技术大学 计算机学院,湖南 长沙 410073)

Sketch-Based Anomalies Detection with IP Address Traceability

LUO Na+, LI Ai-Ping, WU Quan-Yuan, LU Hua-Biao

(School of Computer, National University of Defense Technology, Changsha 410073, China)

+ Corresponding author: E-mail: ccmaxluna@gmail.com

Luo N, Li AP, Wu QY, Lu HB. Sketch-Based anomalies detection with IP address traceability. *Journal of Software*, 2009,20(10):2899−2906. http://www.jos.org.cn/1000-9825/3685.htm

Abstract: In this paper, an anomaly detection method is proposed based on the summary data structure—sketch. It records the network traffic information in sketch online and detects anomalies at every circle. After using EWMA forecasting model to get each circle's forecast sketch, this paper computes the errors between the recoded sketch and forecast sketch. Then, the network traffic change reference is constructed by establishing the Mean-Standard deviation model on the error sketch. The method is effective in detecting DDOS attack, scan attack and so on. Particularly, it can track the IP address of anomaly. Evaluated by the experiment, this method can detect anomaly in the backbone network with small computing and memory resource.

Key words: anomaly detection; sketch; traceability; EWMA; mean-standard deviation model

摘 要: 提出一种基于sketch概要数据结构的异常检测方法.该方法实时记录网络数据流信息到sketch数据结构,然后每隔一定周期进行异常检测.采用EWMA(exponentially weighted moving average)预测模型预测每一周期的预测值,计算观测值与预测值之间的差异sketch,然后基于差异sketch采用均值均方差模型建立网络流量变化参考.该方法能够检测DDoS、扫描等攻击行为,并能追溯异常的IP地址.通过模拟实验验证,该方法占用很少的计算和存储资源,能够检测骨干网络流量中的异常IP地址.

关键词: 异常检测;概要数据结构;溯源性;EWMA;均值均方差模型

中图法分类号: TP393 **文献标识码**: A

随着计算机网络的飞速发展,网络规模越来越大,网络设备日益复杂,应用也日新月异,网络上不断出现的网络攻击和安全威胁事件,都会造成网络流量异常.同时,互联网流量每年成倍增长,如何对高速骨干网络流量进行实时监测和管理,及时地发现网络流量异常并追踪定位异常源,使得网络管理员能够采取有效措施阻断、减缓异常行为,对提高网络的可靠性和可用性具有重要意义.

* Supported by the National High-Tech Research and Development Plan of China under Grant Nos.2007AA01Z474, 2006AA01Z451, 2007AA010502 (国家高技术研究发展计划(863))

Received 2008-11-28; Accepted 2008-12-30

1 相关研究

异常检测主要可以分为两类,基于特征的检测和基于统计的检测.基于特征的检测主要是通过寻找能与已知异常特征相匹配的模式来检测异常,需要预先设定特征库或规则库.这种方法的优点是能够精确地检测已知的异常,缺点是不能检测未知的异常,同时,随着异常种类的增多,特征库很庞大,监测性能下降.因此基于特征的检测只适用于局域网,不能满足骨干链路的速率.基于统计的检测不需要预先了解异常的特征和属性,能够有效地检测已知的以及新出现的异常.在基于统计的检测方法中很重要的一部分就是变化检测,主要方法是通过历史流量得到一个正常的流量模型,然后通过检测在短期内不符合此模型的行为来发现异常.

异常检测中主要的变化检测技术有以下几种:阈值、预测模型、马尔可夫链、人工神经网络等.但是这些方法都不能满足在大规模网络条件下实时处理的要求,大规模网络条件下数据报文到达速度快,数据量大.以10G 的骨干链路来说,报文以每秒百万的数量级的速率到达,在最坏情况下(每个报文 40 字节),报文到达间隔仅为 32ns,因而直接处理这些数据来发现异常是不现实的,可以采用降维的方法.目前对流量数据通过降维进行异常检测的研究方法主要有:主成分分析法 PCA(principal component analysis)和概要数据结构 sketch.PCA 是一种坐标变化方法,将给定数据点映射到一些新的坐标轴,这些新的坐标轴就成为主成分;Lakhina 等人[1]提出子空间方法利用 PCA 将流量分为两部分,正常部分和异常部分,正常部分是可以预测的,异常部分是有噪声的,包含网络中的毛刺.而 sketch 是一种高效的概要数据结构,它占用的内存资源少,计算和更新的复杂性小,能够满足在大规模网络条件下实时处理的要求.Krishnamurthy 等人[2]首次将 sketch 用于异常检测并提出一种启发式方法自动设置 sketch 的参数;Schweller 等人[3]采用 IP 地址分块 hash 和 IP 扰乱两种方法来解决 sketch 可溯源性的性能问题;Dewaele 等人[4]在 sketch 的基础上应用非高斯边缘分布(non Gaussian marginal distribution)的多时间尺度特性,可以多种攻击,包括检测低强度持续时间长的攻击和持续时间短的端口扫描攻击.

本文所提检测方法采用 sketch 方法存储骨干网络数据流概要信息,采用 EWMA 预测模型预测下一周期的预测值,计算观测值与预测值之间的差异 sketch,基于差异 sketch 建立网络流量变化参考模型,不符合参考模型的流量即为异常流量.该方法能够追溯异常的 IP 地址,使得网络管理员能够采取有效措施阻断异常行为,减缓攻击影响.

2 异常检测方法

本文以检测 DDoS 为例,将汇聚到相同目的 IP 地址的报文序列看作一个流,如果这个流的报文数在一段时间内异常显著增加,则该目的地址可能受到 DDoS 攻击.

我们采用数据流模型表示网络流量数据,用 sketch 概要数据结构来统计一定周期内不同目的 IP 地址到达的报文数,采用预测模型预测这一周期的报文数,计算观测值与预测值之间的差异 sketch,基于差异 sketch 建立网络流量变化参考模型,如果目的 IP 地址不符合此模型,即为异常的目的 IP 地址,同时,这些目的 IP 地址即为可能受 DDoS 攻击的主机.下面几节首先介绍基本概念:数据流模型、sketch 数据结构以及 EWMA 预测模型.然后具体讲述检测方法和过程.

2.1 数据流模型

人们对数据流提出了很多模型来描述,包括时间序列、缓冲寄存器模型和十字转门[5]模型,我们使用最通用的十字转门模型.$L=\{a_i|i\in L\}$,L 表示逐个元素顺序到达的数据流,其中 $a_i=(key_i,u_i)$,key_i 表示此元素的标识,u_i 为此元素的特征值,$[n]=\{0,1,\ldots,n-1\}$表示流数据模型的 key 空间.$U[a_i]$表示对所有标识为 a_i 的元素的统计量,当一个元素到达时,更新对应的统计量,$U[a_i]+=u_i$.通过检测那些统计量有巨大变化的元素来发现异常.

本文中,数据流为骨干链路上的网络流,元素为 IP 报文,key 定义为目的 IP 地址,特征值定义为报文数目,在这里每个元素的 u_i 恒为 1.本文通过检测到达同一个目的 IP 地址的报文数目,来发现 DDoS 等报文数目有急剧变化的攻击行为.

2.2 sketch数据结构

sketch 记录输入数据流的概要信息,包括两部分:hash 计算和概要数据结构.下面首先描述如何选择合适的 hash 函数,然后介绍概要数据结构.

哈希函数的碰撞问题是需要解决的关键问题,完全消除碰撞是不可能的事情,但是我们却可以通过某种方法将碰撞的概率控制在某个上限之内.使用通用散列函数(universal hash)可以达到这个目的.

通用散列函数簇(universal hash classes)[6]:G 是从 A 映射到 B 的一系列函数,如果 G 满足:$\forall x,y\in A$,且 $x\neq y$,则 x,y 在 G 的所有函数下碰撞的次数 $\leq |G|/|B|$,则称 G 为通用散列函数簇.从通用散列函数簇随机取一个函数 f,具有性质:$\forall x,y\in A$,且 $x\neq y$,则 $P(f(x)=f(y))\leq 1/|B|$.

Hash 函数的选择主要有两项指标:均匀分配流和保证异常行为的可溯源性.通用散列函数簇中的函数可以符合这两个要求.通用散列函数有冲突概率的保证,可保证流均匀分配;同时选择通用散列函数簇中独立的 H 个函数,只要 H 足够大就可以保证异常 key 的可溯源性.本文中的 hash 函数选自文献[7]中的通用散列函数簇,如公式(1)所示,其中 p 是大于 key 空间[n]元素个数的素数,δ_i 为素数空间[p]中的任意元素,k 表示通用散列级别.

$$h(key)=\left(\sum_{i=0}^{k-1}\delta_i key^i \bmod p\right)\bmod M \tag{1}$$

概要数据结构用一个 H 行 M 列的二维数组来存储统计量,对应 $H\times M$ 个计数器.数组的每一行对应一个 hash 函数,一行中的 M 个计数器表示 hash 函数的 M 个桶,每个计数器记录 hash 到此桶的数据流元素的特征值统计量,如图 1 所示.

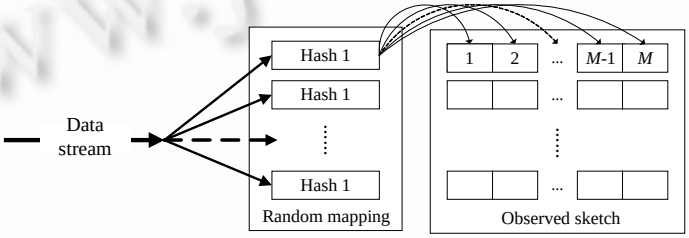


Fig.1 Conceptual architecture of data recording

图 1 数据记录示意框图

2.3 EWMA预测模型

指数权重移动平均(exponentially weighted moving average)又称为指数平滑模型,它是一种由前一时刻观测值和前一时刻的预测值来得到时间序列当前时刻预测值的简单算法.若 $\tilde{y}_{t-1}$ 表示 $t-1$ 时刻的预测值,y_{t-1} 表示 $t-1$ 时刻的观测值,则第 t 时刻的预测值 $\tilde{y}_t$ 如公式(2)所示:

$$\tilde{y}_t=\begin{cases}\alpha y_{t-1}+(1-\alpha)\tilde{y}_{t-1}, & t>2\\ y_1, & t=2\end{cases} \tag{2}$$

这种预测实际上是时间序列中过去时刻的所有观测值的加权求和,且假设下一时刻的预测值与距离它最近的观测值关系最大,随着距离的增大,过去时刻观测值的权值呈指数递减.其中,$\alpha(0<\alpha<1)$称为平滑系数,它确定了在预测过程中历史数据权重的衰减率$(1-\alpha)$.

2.4 异常检测框图

系统分为数据记录和异常检测两部分.

数据记录部分实时地将到达的报文信息存储到 sketch 数据结构中,如图 1 所示.当到达一个新的报文(key_i,u_i)时,经过 hash 计算得到 H 个计数器,进而更新 sketch 数据结构中相应计数器的统计量,如公式(3)所示:

$$S[h][hash_h(key_i)]+=u_i,\ h\in\{0,1,2,...,H-1\} \tag{3}$$

异常检测部分如图 2 所示,通过对 sketch 的计数器统计量进行运算来判定异常目的 IP 地址,分为预测和检测两部分.预测部分使用 EWMA 预测模型得到当前周期的预测 sketch $f[H][M]$,检测部分通过计算当前周期的预测 sketch $f[H][M]$与数据记录部分得到的观测 sketch $S[H][M]$之间的差异得到当前周期的误差 sketch $e[H][M]$,进而根据此误差 sketch,采用统计学方法来判断异常.

其中,数据记录实时地进行,而异常检测部分在后台每周期启动 1 次.

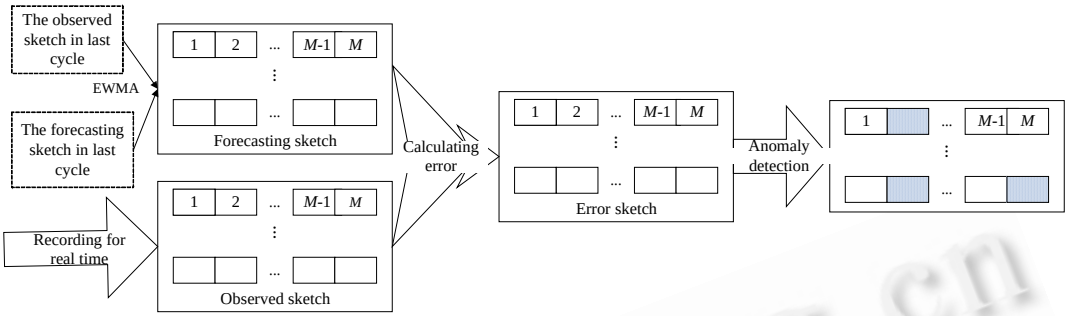


Fig.2 Conceptual architecture of anomaly detection

图 2 异常检测示意框图

3 异常检测流程

本文中的异常检测方法主要基于 sketch 概要数据结构,它占用很小的内存资源,即使在高速骨干网络上也能满足报文实时记录的要求,下面详细介绍这一检测流程.

3.1 数据记录

数据记录具体流程如图 3 所示.

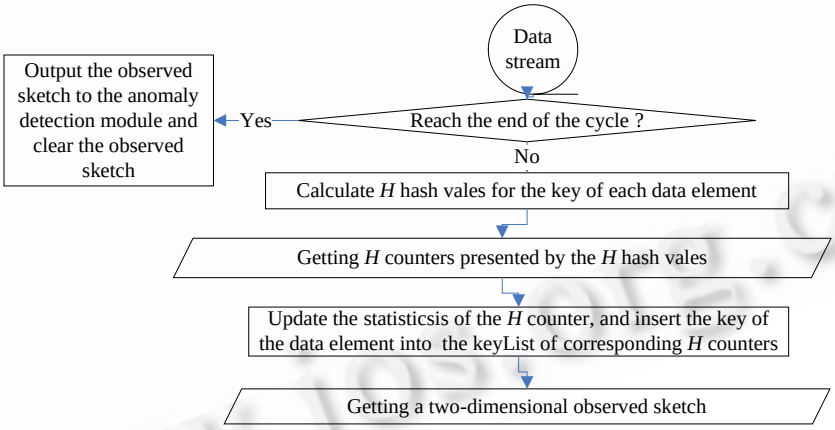


Fig.3 Process of data recording

图 3 数据记录过程

1) 当一个元素$(keyi,ui)$到达时,计算 H 个哈希函数值得到 H 个计数器, $hash_h(key_i)\in\{0,1,...,M-1\}$ $h\in\{0,1,...,H-1\}$.

2) 将这 H 个由 $hash_h(key_i)$标识的计数器统计值更新,如公式(3)所示,同时将 key_i 加入到对应计数器的 key 链表 $List_{h,hash(key_i)}$ 中.

3) 当一个周期结束,得到此周期的观测 sketch $S[H][M]$,将其输出到异常检测部分,并且清空此观测

sketch,进入下一周期的记录阶段.

观测 sketch 数据结构 $S[H][M]$用一个 H 行 M 列的二维数组来存储统计量,每一个元素为一个特征量计数器,观测 sketch 对应的 $H\times M$ 个计数器.hash 到每个计数器的 key 用一个链表结构 List 来存储,即每个计数器对应一个 key 链表结构,存储观测 sketch 所有计数器的 key 集合需要 $H\times M$ 个链表,key 链表用于异常检测过程中追溯异常的 IP 地址.

3.2 异常检测

在每一个周期的末尾进行异常检测,异常检测流程如图 4 所示.

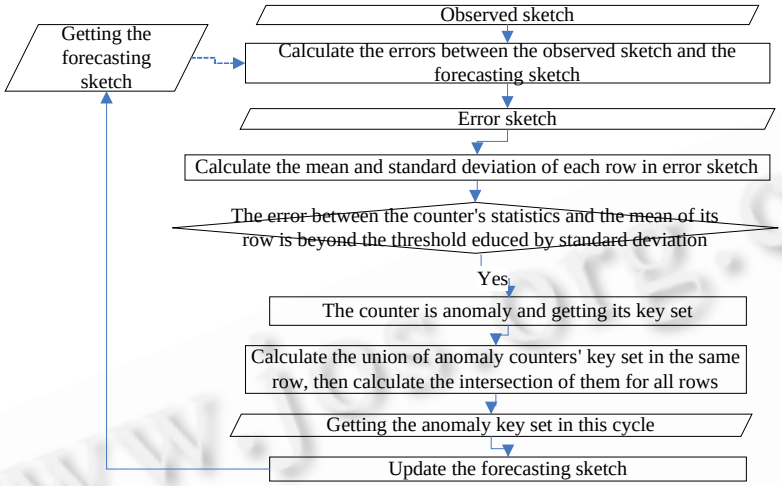


Fig.4 Process of anomaly detection

图 4 异常检测过程

步骤大致如下:

1) 将数据记录阶段得到的当前时间窗口的观测 sketch $S_t[i][j]$与上一时间窗口末尾得到的当前时间窗口的预测 sketch $f_t[i][j]$作差运算,得到当前时间窗口的误差 sketch $e_t[i][j]$.

2) 对此误差 sketch 绝对值的每一行计算一个均值 $E_t(i)$和均方差 $F_t(i)$,如公式(4)所示:

$$E_t(i)=\sum_{j=1}^{M}\left|e_t[i][j]\right|\Big/M,\quad V_t(i)=\sqrt{\sum_{j=1}^{M}\left(\left|e_t[i][j]\right|-E_t(i)\right)^2\Big/M} \tag{4}$$

3) 判断误差 sketch 第 i 行的所有计数器值与 $E_t(i)$的差值是否超过$\beta V(i)$,如果大于这个阈值,则说这个计数器是异常的,否则是正常的.这里,β称为均方差系数,一般取[2,10]之间比较合适.

4) 得到异常计数器 C_{ij} 对应的链表结构 $List_{ij}$ 中存储的 key(目的 IP 地址)集合 U_{ij}.

5) 将误差 sketch 同一行的 U_{ij} 求并集,再将所有行得到的并集取交集,得到异常 key 集合,即

$$\bigcap_{i=0}^{H-1}\left(\bigcup_{C_{ij}\text{异常}}U_{ij}\right).$$

6) 根据 EWMA 预测模型更新预测值,如公式(5)所示:

$$f_{t+1}[i][j]=\begin{cases}\alpha S_t[i][j]+(1-\alpha)f_t[i][j], & t\geq 2\\ S_t[i][j], & t=1\end{cases} \tag{5}$$

最后得到的异常目的 IP 地址集合为可能受攻击的目的主机集合.可以通过进一步观测这些目的 IP 地址的报文来确认具体的攻击,并采取措施阻断攻击,减缓攻击产生的影响.

4 算法实验

4.1 实验数据

采用 NLANR PMA 组在 Internet2 实验网上获取的真实 trace 数据.这里,选取 IPLS-KSCY 数据[8],该数据为美国 Indianapolis 到 Kansas City 的 OC192 链路数据,时间为 2004 年 8 月 19 日,每个数据文件持续时间长度为 10 分钟,我们选择下午 2 点的 6 个 trace 文件顺序连接成一个小时文件.6 个 Trace 文件的主要特性见表 1.

Table 1 Characteristic of Trace data

表 1 Trace 流量特性

Trace	Rate (Mbps)	Num of IP packet	Num of TCP packet
IPLS-KSCY-20040819-140000-0	625.339	51 984 093	43 631 137
IPLS-KSCY-20040819-141000-0	750.993	53 690 155	45 028 538
IPLS-KSCY-20040819-142000-0	829.982	54 378 499	45 767 584
IPLS-KSCY-20040819-143000-0	780.441	53 453 631	44 963 990
IPLS-KSCY-20040819-144000-0	834.752	52 827 335	45 247 975
IPLS-KSCY-20040819-145000-0	714.669	51 155 444	43 740 481

4.2 实验结果

我们的异常检测方法涉及到的主要参数有:sketch 数据结构参数 H,M,预测模型平滑系数σ,均方差系数β,检测周期 T.在实验中,我们设定参数如下:

1) H 为 8,M 为 1 024;

2) α为 0.4;

3) β为 4;

4) T 为 5 分钟.

我们与文献[3]提出的流量参考模型作比较.文献[3]的网络流量参考模型简单介绍如下,如果某个计数器的变化量(观测值相对于预测值)大于流量整体变化量的一定比例,则称此计数器变化异常,为异常计数器.即,设 D_i 表示误差 sketch 第 i 行之和,即 $D_i=\sum_{j=1}^{M}E[i][j]$,如果公式(6)成立,则计数器 C_{ij} 是异常的,否则计数器 C_{ij} 正常.公式(6)中,ϕ即为整体变化量比例阈值.

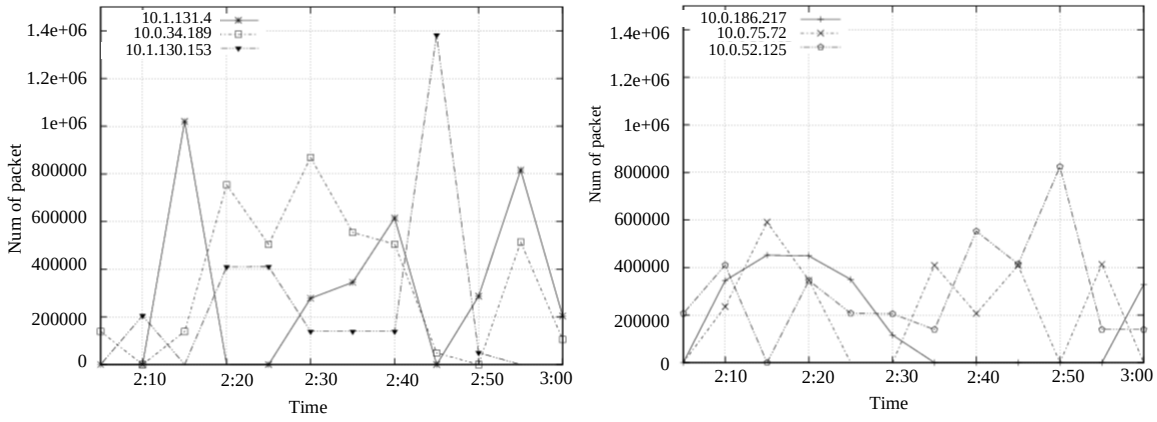
$$\frac{E[i][j]-D_i/M}{1-1/M}\geq\phi D_i,\quad \text{即}E[i][j]\geq\left(\phi D_i\left(1-1/M\right)+D_i/M\right) \tag{6}$$

在本实验中,文献[3]提出的流量参考模型 sketch 数据结构参数 H,M,预测模型平滑系数α,检测周期 T 与我们的参考模型设置相同,整体变化量比例阈值ϕ设为 0.02.

为了得到一个好的预测初始值,我们以计数器前 3 周期的统计量的平均值作为初始预测值,从第 4 周期开始检测异常.

文献[3]提出的参考模型能够监测出的异常 IP 地址,我们的参考模型也都能监测,如图 5 所示.图 5(a)检测出的 3 个 IP 地址变化很突出,比如,在 2 点 35 分到、在 2 点 40 分到达 10.1.130.153 的报文只有 20 万左右,而在 2 点 40 分到、在 2 点 45 分到达 10.1.130.153 的报文突增到 140 万,这种突增代表了明显的流量异常,造成这种异常的原因可能是 DDoS 攻击或者突发访问.图 5(b)中,IP 地址 10.0.75.72 与 10.0.52.125 的变化也较明显,但 IP 地址 10.0.186.217 的变化比较缓慢,有可能是算法不精确造成的.

我们的检测方法还能够检测出另外一些报文数目变化较大的 IP 地址,如图 6 所示.虽然文献[3]的方法通过降低整体变化量比例阈值ϕ也能检测出这些 IP 地址,但会带来很大的误检率.从图 6 可以看出,IP 地址 10.0.0.54 在 2 点 30 分~2 点 35 分之间有着显著变化,表现出一定的异常,在 2 点 50 分~2 点 55 分之间也类似有着异常表现.其他 2 个 IP 地址在一些时间段变化也很大.



(a) (b)

Fig.5 Common result of both approaches

图 5 两种方法的共同检测结果

基于 sketch 的检测方法的最大优点是,当流量整体看不出异常时,sketch 中的某个计数器可能表现异常,如图 7 中以 IP 地址 10.1.130.153 为例.从图 7 可以看出,网络流量整体上变化平稳,但 IP 地址 10.1.130.153 却有显著的异常变化.基于 sketch 的异常检测无论是在空间上还是在计算开销上都远远优于基于 per flow 的检测,在当今骨干链路基于 per flow 的检测的情况下是不现实的;但同时,基于 sketch 的异常检测能够检测隐藏于大量背景流量下的异常,优于基于整体流量特征的检测(若把整个网络流量看成一个时间序列).基于 sketch 的异常检测较之这两者具有明显的优势.

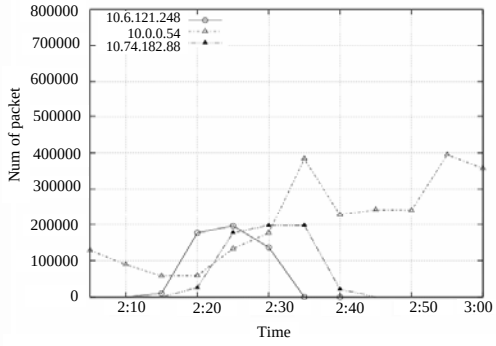


Fig.6 Result detected only by our approaches

图 6 仅被本文方法检测出 IP 地址

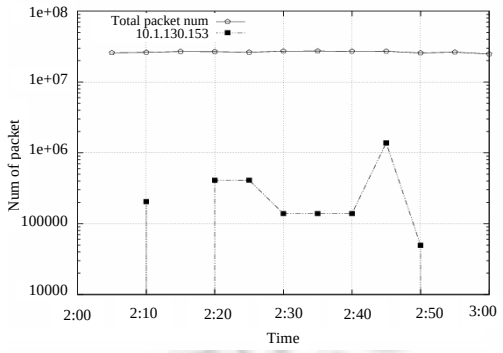


Fig.7 Anomaly of a single flow when the whole normal

图 7 网络流量整体正常情况下,单一流的异常变化

5 总 结

本文提出一种基于 sketch 概要数据结构的异常检测方法,该方法能够检测 DDOS、扫描等攻击行为,并能追溯异常的 IP 地址,使得网络管理员能够采取有效措施阻断异常行为,减缓攻击影响.基于观测 sketch 与预测 sketch 之间的差异 sketch,提出了采用均值均方差建立网络流量变化参考模型.通过实验验证了该模型具有很好的精度,与文献[3]提出的模型相比,能够检测出更多的异常.

基于 sketch 异常变化检测的应用前景很广阔,虽然这种检测方法已实际用于检测某些特定的异常,但现在面临的问题是如何完善其理论以及如何找出一个完备最优的 key 集和对应的特征集,而这也是一个艰难且极富挑战性的难题.

References:

[1] Lakhina A, Crovella M, Diot C. Diagnosing network-wide traffic anomalies. In: Proc. of the 2004 Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communication. New York: ACM Press, 2004. 219−230. http://portal.acm.org/citation.cfm?id=1015492

[2] Krishnamurthy B, Sen S, Zhang Y, Chen Y. Sketch-Based change detection: Methods, evaluation, and applications. In: Proc. of the ACM SIGCOMM Internet Measurement Conf. New York: ACM Press, 2003. 234−247. http://portal.acm.org/citation.cfm?id=948236

[3] Schweller R, Li ZC, Chen Y, Gao Y, Gupta A. Reverse hashing for high-speed network monitoring: Algorithms, evaluation, and applications. In: Proc. of the 25th IEEE Int'l Conf. on Computer Communications. New York: IEEE, 2006. 1397−1408.

[4] Dewaele G, Fukuda K, Borgnat P. Extracting hidden anomalies using sketch and non gaussian multiresolution statistical detection procedures. In: Proc. of the Int'l Multimedia Conf. of the 2007 Workshop: Large Scale Attack Defense. New York: ACM Press, 2007. 145−152. http://portal.acm.org/citation.cfm?id=1352664.1352675

[5] Muthukrishnan S. Data streams: Algorithms and applications. 2007. http://www.cs.rutgers.edu/~muthu/stream-1-1.ps

[6] Lawrence CJ, Wegman MN. Universal classes of hash functions. Journal of Computer and System Sciences, 1979,18(2):143−154.

[7] Wegman M, Carter J. New hash functions and their use in authentication and set equality. Journal of Computer and System Sciences, 1981,22(3):265−279.

[8] NLANR. Retrieved May 10, 2008. ftp://pma.nlanr.net/traces/long/ipls/5/

罗娜(1983－),女,河北邢台人,硕士,主要研究领域为网络安全.

吴泉源(1942－),男,教授,博士生导师,主要研究领域为分布计算软件,人工智能与专家系统.

李爱平(1974－),男,博士,副研究员,CCF高级会员,主要研究领域为海量数据分析,人工智能,网络安全.

陆华彪(1983－),男,硕士,主要研究领域为高性能计算机网络,网络安全.