基于改进 CUSUM 算法的路由器异常流量检测*

孙知信+, 唐益慰, 程 媛

(南京邮电大学 计算机学院,江苏 南京 210001)

Router Anomaly Traffic Detection Based on Modified-CUSUM Algorithms

SUN Zhi-Xin+, TANG Yi-Wei, CHENG Yuan

(College of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210001, China)

+ Corresponding author: Phn: +86-25-85198095, E-mail: sunzx@njupt.edu.cn, http://www.nupt.edu.cn

Received 2004-08-24; Accepted 2005-01-07

Sun ZX, Tang YW, Cheng Y. Router anomaly traffic detection based on modified-CUSUM algorithms. *Journal of Software*, 2005,16(12):2117−2123. DOI: 10.1360/jos162117

Abstract: The paper aims at the change of core routers ports' ingress and egress traffic, employing a modified CUSUM (cumulative sum) algorithm to trace their statistics characteristic in real time and detect network flow abnormity. According to the characteristics of multi-ports in a router, the paper puts forward a matrix-based, multi-statistics modified CUSUM algorithm (M-CUSUM). M-CUSUM presents an adjustable parameter setup system to increase detecting accuracy. M-CUSUM algorithm can monitor changes of the equal value in real time through calculating the ratio between the subtracting and plus absolute value among ingress and egress ports traffic. Simulation experiments indicate that the algorithm has the higher detecting speed and accuracy to DOS/DDOS attacks, and spends less system resources. The algorithm has been used successfully in software routers.

Key words: CUSUM (cumulative sum) algorithm; DOS (denial of service); DDOS(distributed denial of service); router; intrusion detection

摘 要: 针对核心路由器端口的输入、输出流量的变化,用改进的 CUSUM(cumulative sum)算法对其统计特性进行实时监控,检测网络流量异常.基于路由器多端口的特点,提出了矩阵式的多统计量 CUSUM 算法(M-CUSUM),并提出了可调的参数设定体系,以提高准确性.M-CUSUM 算法通过对输入、输出端口流量的绝对差与和之比进行统计,实时地监控其均值的偏移情况.通过对该算法在计算机中的模拟实现,验证了该算法对 DOS/DDOS 攻击具有较高的检测速度和精度,且系统开销小,已成功运行在软件路由器之上.

关键词: CUSUM 算法;拒绝服务攻击;分布式拒绝服务攻击;路由器;异常流量

中图法分类号: TP393 文献标识码: A

* Supported by the National Natural Science Foundation of China under Grant No.70271050 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2005AA775050 (国家高技术研究发展计划(863)); the Scientific Research Foundation for the Returned Overseas Chinese Scholars, Ministry of Education of China and Nanjing Government (国家教育部和南京市回国人员基金); the Scientific Research Foundation of Huawei and ZE Corporation of China (华为和中兴通讯基金)

作者简介: 孙知信(1964−),男,江苏南京人,博士,教授,主要研究领域为计算机网络与安全,计算机仿真,软件工程;唐益慰(1982−),男,硕士生,主要研究领域为计算机网络与安全;程媛(1981−),女,硕士生,主要研究领域为计算机网络与安全.

由于 Internet 在全球的普及,网络的安全问题日益受到人们的重视.目前的网络基本使用的是 TCP/IP 协议,但其本身具有一定的不足之处,成为黑客们攻击网络的理论基础.他们利用大量的垃圾流量堵塞网络,使正常流量不能得到有效的传输.基于攻击结构的不同,可以分为拒绝服务攻击(DOS)和分布式拒绝服务攻击(DDOS).

由于拒绝服务攻击隐蔽性好,且许多网络系统对其还没有免疫能力,从 2000 年 2 月起,这种攻击方法开始大行其道,成为黑客攻击的主流手段.Yahoo,eBUY,Amazon,CNN 等众多知名站点相继被身份不明的黑客在短短几天内连续破坏,系统瘫痪将近几个小时甚至几十个小时之久.我国的新浪网和部分的政府站点也遭到不同程度的攻击.为了保证网络稳定,信息的安全,阻止拒绝服务攻击势在必行.

从总体上来看,无论是 DOS 攻击还是 DDOS 攻击,都是用同一种方法,即用大量的垃圾数据包来堵塞网络,使得网络终端过于繁忙,超出了其正常运行的范围,使其不能完成正常的服务.可以看出,DOS/DDOS 攻击都会使网络的流量发生大的变化,从而使路由器端口的输入与输出比在统计特性上发生异常.我们可以用 CUSUM(cumulative sum)算法来发现这种特征,从而准确地检测网络的异常流量,尽早地发现 DOS/DDOS 攻击,并采取相应的手段,制止攻击所产生的破坏,挽回损失.

本文第 1 节介绍目前在检测网络异常流量上的方法.第 2 节给出 CUSUM 算法,并提出适合路由器端口检测的改进 M-CUSUM 算法.第 3 节把改进的 M-CUSUM 算法运用在网络环境中,针对路由器,检测网络中的异常流量.最后给出本文的总结,并且提出将来所需要做的工作.

1 相关性研究

在文献[1,2]中,提出了针对 SYN FLOOD 进行检测的 CUSUM 算法,即基于在正常传输情况下,TCP 包中 SYN 包与 FIN 包是有一定的对应关系,运用非参数的 CUSUM 算法对其进行统计.由于发生 SYN FLOOD 攻击的时候,SYN 包和 FIN 包的比例关系被打破,就检测出了攻击.从文献[3]中可以知道,在正常的网络流量中,有 90%以上的数据包都是 TCP 包,其他的数据包所占的比重较少,SYN 数据包和 FIN 数据包的流向正好是相反的,所以对于路由器端口流量输入输出比进行 CUSUM 也有一样的效果,但文献[1]中的算法只能用于检测 SYN FLOOD 攻击,而对于其他的 DOS/DDOS 攻击则无法检测.

因为 DOS/DDOS 使流量的统计特性发生变化,所以许多方法都是基于统计特性检测,如文献[4]运用了网络流量的自相似性特性进行分析.文献[3]中作者在 MIT 实验室分别对改进的门限算法(adapted threshold algorithm)和 CUSUM 算法做了长时间、多方面的实验,进行了比较分析,证明了 CUSUM 算法的优点.

文献[5]中提出了一种利用协方差分析的异常流量检测算法,对于不同协议,在单位时间内,对不同的数据包分别累积,然后对不同时段的数据包累积向量,算出相应的协方差矩阵,并对此矩阵进行量化,从中得知网络中各种数据包量的变化情况.如对于 TCP 协议,分别对 URG,ACK,PSH,RST,SYN,FIN 这 6 种数据包进行检测分析.通过分析,不仅可以检测出 SYN FLOOD 攻击,而且可以检测出基于 UDP,ICMP 等协议的攻击,但是文献[5]中的方法要对大量数据进行操作,且计算协方差、矩阵量化都需要大量的运算工作,而且实现起来也有一定的困难.对于网络中的核心路由器,其每秒通过的数据量巨大,用过于复杂的算法来分析是不可取的.

文献[6]运用熵的方法对网络流量进行检测,根据在网络截获的数据包的源 IP 地址的数量变化特征,用统计方法来计算其总体能量的变化特征,检测网络的异常.此方法比较适合分布式的拒绝服务攻击,但对源 IP 地址变化比较固定的攻击效果不好.

根据上面的分析,结合在路由器环境下的网络实际情况,我们设计了一种利用改进的 M-CUSUM 来监控网络端口输入输出流量变化的方法,能够快速、准确地检测出异常,且不影响网络正常运行,综合性能好.

2 基于路由器异常流量检测的改进 CUSUM 算法(M-CUSUM)

2.1 CUSUM算法描述

CUSUM 算法[8−10]是工业异常监控常用的算法,它可以检测到一个统计过程均值的变化.CUSUM 算法基于这一事实:如果有变化发生,随机序列的概率分布也会改变.

令 $x_1, x_2, ..., x_t$ 为独立的 $N(0,1)$ 同分布, $x_{t+1}, x_{t+2}, x_{t+3}, ...$ 为独立的 $N(\delta,1)$ 同分布,其中 t 为未知变点,对于给定的观察序列 $x_1, x_2, x_3, ..., x_n$,假设 $t = v(v < n)$ 对于原假设 $t = \infty$ 的似然比统计量为(以 $\phi(\bullet)$ 表示标准正态分布 $N(0,1)$ 的分布密度函数):

$$L_{n,v} = \frac{\prod_{i=1}^{v}\phi(x_i)\prod_{i=v+1}^{n}\phi(x_i-\delta)}{\prod_{i=1}^{n}\phi(x_i)} = \frac{\prod_{i=v+1}^{n}\phi(x_i-\delta)}{\prod_{i=v+1}^{n}\phi(x_i)} = \exp\left\{\delta\sum_{i=v+1}^{n}\left(x_i-\frac{\delta}{2}\right)\right\} \tag{1}$$

由于 $\prod_{i=n+1}^{n}\phi(x_i)=1$, $\sum_{i=n+1}^{n}x_i=0$,对数化为 $A_{n,v}=\ln L_{n,v}=\delta\sum_{i=v+1}^{n}\left(x_i-\frac{\delta}{2}\right)$.

假设变量 $x_1, x_2, ..., x_t$ 与 $x_{t+1}, x_{t+2}, .x_{t+3}, ...$ 有偏移,那么其对数似然统计量为

$$\Lambda_n = \max_{1\le v<n}\Lambda_{n,v} = \max\left\{\delta\sum_{i=v+1}^{n}\left(x_i-\frac{\delta}{2}\right)\right\} \tag{2}$$

假设我们检测的为向上偏移,即 $\delta > 0$,则上述的对数似然统计量等价于下面的统计量

$$Z_n = \max_{1\le v<n}\sum_{i=v+1}^{n}\left(x_i-\frac{\delta}{2}\right) \tag{3}$$

定义 **1**. 设 $n-1$ 个观测值没有均值偏移,即 $Z_i \le h, i=1,2,...,n-1$,h 为门限.如果在时刻 n,满足 $x_n - \delta/2 > h$,或 $x_n + x_{n-1} - \delta > h$,或 $x_n + x_{n-1} + x_{n-2} - 3\delta/2 > h$,…,或 $x_n + x_{n-1} + ... + x_1 - n\delta/2 > h$,则这个过程发生了均值偏移.

记 $\tilde{x}_i = x_i - \frac{\delta}{2}$; 且 $\tilde{x}_0 = 0, \tilde{S}_k = \sum_{i=0}^{k}\tilde{x}, \tilde{S}_0 = 0$, 于是可得:

$$Z_n - Z_{n-1} = \tilde{x}_n - \min\left\{0, \tilde{S}_n - \min_{0\le v\le n-1}\tilde{S}_v\right\} = \max\left\{\tilde{x}_n, \tilde{x}_n - \tilde{S}_n + \min_{0\le v\le n-1}\tilde{S}_v\right\} = \max\{\tilde{x}_n, \min_{1\le v\le n-1}\tilde{S}_v - \tilde{S}_{n-1}\} = \max\{\tilde{x}_n, -Z_{n-1}\} \tag{4}$$

用不定参数 k 代替 $\delta/2$, 就得到了 Z_n 的递推公式:

$$Z_n = \max\{0, Z_{n-1} + x_n - k\}, n = 1,2,... \tag{5}$$

这就是 CUSUM 算法.若设定报警门限为 $h > 0$,如果在第 n 个观察点满足 $Z_n > h(Z_i \le h, i = 1,2,...,n-1)$, 则报警,确定在过程 n 以前的统计量发生了均值偏移.

2.2 基于路由器的改进**CUSUM**算法(**M-CUSUM**)

通常,CUSUM 需要随机序列的参数模型,以便可以用概率密度函数来监控序列.但因特网是一个非常动态而复杂的实体,因特网业务模型的理论结构是一个复杂的问题,因而,一个主要的难题是如何模拟随机序列(X_n),而非参数方法不是具体的模型,更适合于分析因特网.非参数 CUSUM 算法的主要思想是,累积明显比正常运行情况下的平均水平高的 X_n 值.算法的优点之一是,它能以连续方式监控输入的随机变量,从而达到实时检测.

基于路由器特殊的网络环境,我们要对 CUSUM 算法采取一些改进措施.由于路由器一般情况下的端口总数不只一个,要对多个端口同时进行检测,必须运用矩阵的方法对每个路由端口设定统计数值.

记{$x_{n,m}$}为在第 n 个时间段,第 m 个端口的统计量,我们有

$$\delta_{n,m} = (1-\beta)\times\delta_{n-1,m} + \beta\times x_{n,m}, \delta_{0,m} = x_{0,m} \tag{6}$$

$$Z_{n,m} = x_{n,m} - \delta_{n,m} - d \tag{7}$$

$$S_{n,m} = \sum_{i=0}^{n} Z_{i,m}, S_{0,m} = 0 \tag{8}$$

$$Y_{n,m} = S_{n,m} - \min_{1\le k\le n} S_{k,m} \tag{9}$$

其中$\delta_{n,m}$为第 m 个端口统计序列{$x_{n,m}$,n=1,2,3,…}的均值,β为 EWMA(exponentially weighted moving average)系数.通常情况下取β=0.01~0.03,d 为使统计量 $E(Z_{n,m})$在正常情况下小于 0 的偏移.

定义 **2**. 在 $n\times m$ 的随机矩阵中,对于第 m 列序列的统计量,如果在 $t-1$时间段内没有检测出异常,那么在 t 时刻检测出异常当且仅当(其中 h 为门限)

$$Y_{n,m} \le h, n = 1,2,3,\ldots,t-1,$$

$$Y_{t,m}>h.$$

此为改进的 CUSUM 算法(M-CUSUM).

由上述定义可得:

$$Y_{n,m}-Y_{n-1,m}=Z_{n,m}-\min\left\{0,S_{n,m}-\min_{1\le k\le n-1}S_{k,m}\right\}=\max\left\{Z_{n,m},Z_{n,m}-S_{n,m}+\min_{1\le k\le n-1}S_{k,m}\right\}$$
$$=\max\left\{Z_{n,m},\min_{1\le k\le n-1}S_{k,m}-S_{n-1,m}\right\}=\max\{0,-Y_{n-1,m}\}.$$

有下面的递推式:

$$Y_{n,m}=(Y_{n-1,m}+Z_{n,m})^{+},\ Y_{0,m}=0 \tag{10}$$

其中 X^{+} 定义为

$$X^{+}=\begin{cases}x, x>0\\ 0, x\le 0\end{cases} \tag{11}$$

$Y_{n,m}$ 增长得越快,该端口遭到的攻击就越强.

3 改进的 CUSUM 算法检测路由端网络异常流量

3.1 统计量分析

通过对网络中的流量进行实时监测,根据检测得到的数据,总结各种典型网络访问的规律,得知典型的路由器端口信息流量具有以下观测事实,核心路由器某个端口输入、输出的流量存在一定的统计特征:

- 正常使用模式端口下入出流量基本持平

$$C_{out}(n)\sim C_{in}(n)\quad 0\le E\left(\frac{|C_{in}(n)-C_{out}(n)|}{C_{out}(n)+C_{in}(n)}\right)<t<1 \tag{12}$$

- 异常流量情况下网络端口流量的变化

$$C_{out}(n)<<C_{in}(n)\text{或}C_{in}(n)<<C_{out}(n),\ 1>E\left(\frac{|C_{in}(n)-C_{out}(n)|}{C_{out}(n)+C_{in}(n)}\right)>>t \tag{13}$$

式中 C_{in} 表示输入路由器某端口的流量, C_{out} 表示输出路由器某端口的流量,t 表示正常模式下统计量观测值上限,对于具体网络 t 的值也不同.可以在正常情况下做一定时期的观察获得,具体方法为

$$t=\max\left\{E\left(\frac{|C_{in}(n)-C_{out}(n)|}{C_{out}(n)+C_{in}(n)}\right),n=1,2,3,\ldots\text{when attack is not happened}\right\} \tag{14}$$

3.2 算法分析

文献[8]中已经证明,在一个时间序列中的值是独立的并且是同一参数模型的同一分布,那么 CUSUM 对于多变点检测问题是近似最佳的.将 CUSUM 应用于上述的随机序列(X_n)有两个必要条件:一是随机变量之间的依赖性随着时间增长而下降,二是随机变量的值是有限的.

对于核心路由器的某个端口 m,定义在第 n 时间段的统计量为

$$x_{n,m}=\frac{|C_{in}(n,m)-C_{out}(n,m)|}{C_{out}(n,m)+C_{in}(n,m)},n=1,2,3,\ldots \tag{15}$$

由于 $Z_{n,m}$ 是由因特网业务衍生的,而因特网上长程依赖过程非常普遍, $Z_{n,m}$ 的抽样之间的依赖性会随着间隔的增长而衰减.又因为在正常情况下 $x_{n,m}\in(0,t),t<1$,由于 $Z_{n,m}=x_{n,m}-\delta_{n,m}-d$,其中 $\delta_{n,m}$ 和 d 是有限的常数,所以 $Z_{n,m}$ 的值也是有限的,因此检测变量 $Z_{n,m}$ 可以很容易地满足以上两个必要条件.

DOS/DDOS 攻击检测系统有两个关键的指标:第 1 个是错误告警率,第 2 个是检测时间.然而,这两个参数是相互矛盾的,很难在缩短检测时间的同时降低错误告警率,因此,必须在这两个指标之间进行折中.

根据前面的分析,检测时间 T_a 和算法攻击反应时间 ρ_n 可以定义如下:

$$T_a=\inf\{n:Y_n>h\} \tag{16}$$

$$\rho_n=T_n-T_a \tag{17}$$

其中 inf 为下确界, T_a 为攻击的开始时间.

由以上论述可知,参数的设置和检测效率的关系如下:

算法是通过选择最佳参数 d 和 h 来降低告警速率和缩短检测时间.设定的 d 越大,在(Z_n)中出现正值的可能性就越小,因此测试统计量 Y_n 累积到一个较大的值来显示攻击的可能性就越小. h 是 Y_n 的攻击门限, h 越大,错误告警的速率就越低,但检测时间会越长.

参数设定方法如下:

根据一般情况下攻击对 $x_{n,m}$ 产生的抖动情况,可以设定:

$$d = \mu \times \delta_n,\ \mu \in (0.05, 0.25) \tag{18}$$

$$h = \lambda \times \delta_n,\ \lambda \in (10, 20) \tag{19}$$

其中 μ 为偏移比率, λ 为门限倍数,端口均值 $\delta_n = \sum_{i=1}^{m} \delta_{n,i}$.

由式(6)、式(7)和式(17)得:

$$\rho = \inf\left\{k : \sum_{i=0}^{k} (x_{n,m} - \delta_m - d) > h\right\} \tag{20}$$

偏移比率 μ 和门限倍数 λ 都为实验值.我们做了大量的攻击实验,一般的攻击都会使均值产生大于 50%的变化,在严重情况下甚至大于 250%,而变化率过于小的攻击,产生的攻击效果也不好,所以对网络产生的危害不大.这样设定 μ 和 λ 使系统能在不多于 10 个时隙内检测出高强度的攻击(对端口 m 的统计数据 $x_{n,m}$ 的震动幅度大于其均值 250%左右的攻击),平均 30 个时隙内检测出低强度攻击(对端口 m 的统计数据 $x_{n,m}$ 的震动幅度为其均值 50%左右的攻击).利用公式(20)可以算出设定具体参数的 CUSUM 算法对攻击的反应时间,便于参数的调整.由于网络中流量随着时间的变化而变化,所以需要系统能够根据参数 μ 和 λ 实时地得到适合当前网络流量的 h 和 d .

3.3 系统的实现

系统主要由以下模块所组成:端口数据采集模块、输入输出流量统计模块、控制模块、CUSUM 检测模块、日志模块和异常相应模块,如图 1 所示.

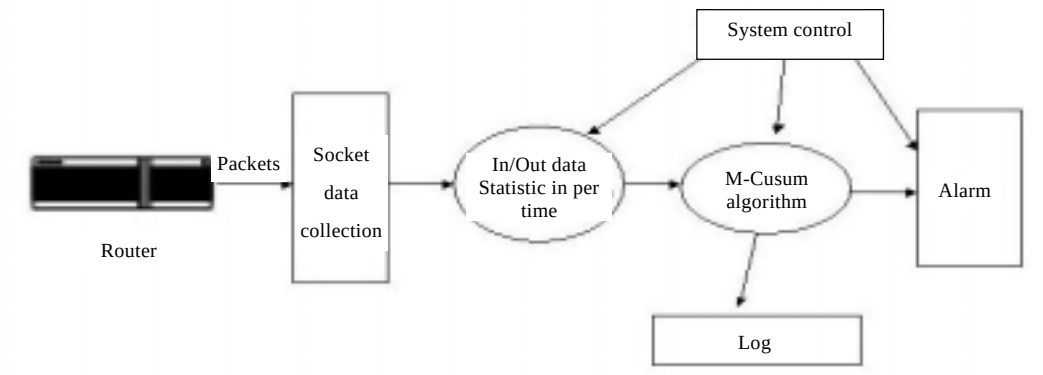

Fig.1 System structure

图 1 系统结构

图 1 中系统控制模块主要是用来对这个模块的参数进行设置和修改,系统日志模块主要用来记录攻击信息,并且记录算法的历史参数.由于网络中流量随着时间的变化而变化,所以控制模块会定时地根据参数 μ 和 λ 得到适合当前网络流量的 h 和 d .

对于路由器的某个端口 m,算法启动后,首先由端口数据采集模块对流经该端口的数据进行采集,并把采集的数据输入端口统计模块,以此来统计端口的输入数据包量和输出数据包数量,当一个统计时间段结束时,取出

两个统计量并清空端口统计模块的数据,然后用式(15)计算 $x_{n,m}$,然后将 $x_{n,m}$ 送入改进的 M-CUSUM 算法模块进行运算.运算步骤如下:

(1) 式(6)计算出当前 $x_{n,m}$ 的均值$\delta_{n,m}$;

(2) 式(7)计算出 $Z_{n,m}$;

(3) 式(10)计算出累积值 $Y_{n,m}$;

(4) 比较 $Y_{n,m}>h$,如果成立,立即向报警模块发送消息,并存储日志.

在系统正式运行时,首先设定数据采集模块的采集频率,然后要在正常的网络环境运行一段时间,使系统能够根据公式(6),计算出较稳定的 δ_n ,然后利用控制模块设定的 $\mu \in (0.05,0.25)$ 和 $\lambda \in (3.5,7.5)$;系统用式(18)、式(19)计算出所需要的门限 h 和零值偏移 d ,然后才能进入检测工作.当然,为了使检测的准确性和速度尽可能高,要多次调整 h 和 d ,使系统与网络环境相协调.

3.4 系统测试

在网络环境中对此系统进行了实验.设 $\mu = 0.15$, $\lambda = 5.0$,β=0.01,时隙 100ms(采样频率 10 次/s),在正常网络下运行一段时间,得到了比较稳定的δ_n=0.089055,从而求得 $d = 0.01336$, $h = 1.7811$ 在前 50 个时间段内在正常状态下运行,在后 50 个时间段对端口 m 进行分布式 SYN FLOOD 攻击.系统所采集的统计数据如图 2~图 4 所示.

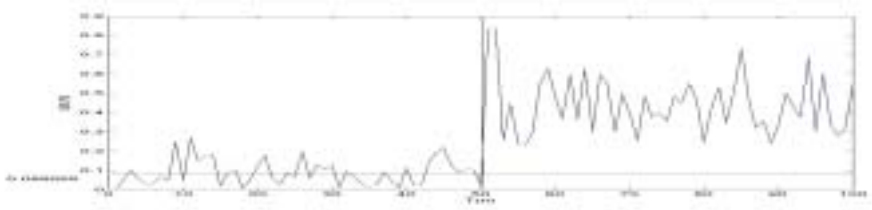

Fig.2 $x_{n,m}$ state change

图 2 $x_{n,m}$ 状态变化

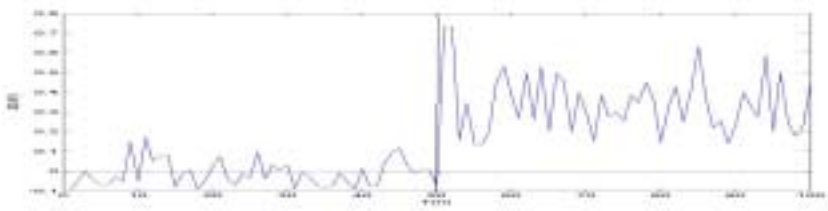

Fig.3 $Z_{n,m}$ state change

图 3 $Z_{n,m}$ 状态变化

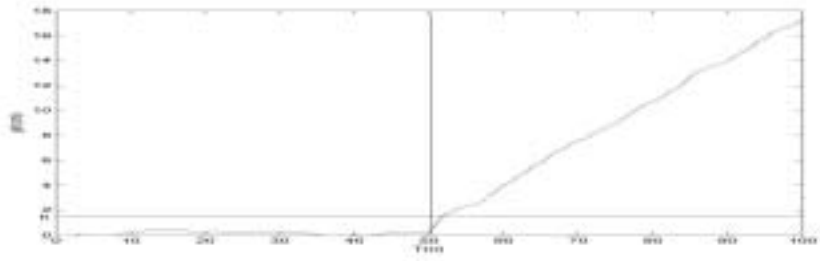

Fig.4 $Y_{n,m}$ state change

图 4 $Y_{n,m}$ 状态变化

可以明显地看出,在攻击发生时,$x_{50,m}$ 的值一下子变大,相应地,$Z_{50,m}$ 也变大,从而使 $Y_{n,m}$ 从几乎为 0 的状态慢慢增长,直到超过门限 h 发生报警.

我们针对不同的攻击做了多次实验,实验表明,在较高强度的 DOS/DDOS 攻击的情况下,M-CUSUM 算法的

异常检出率几乎达到了 100%,而误报率几乎为 0,平均反应时间为 2.25 个单位时间,在低强度攻击情况下,M-CUSUM 算法的各项指标还是比较稳定的,其异常检出率在 90%以上,报错率为 9%,平均反应时间为 15 个单位时间,由于时间间隔设定得小,所以总体效果很好.文献[3]中提到的门限算法对于高强度攻击性能很好,与 M-CUSUM 不相上下,但对于低强度攻击,检测效果就变得很差,误报率和漏报率明显上升,这说明,M-CUSUM 算法对于检测异常具有较好的稳定性.

4 总 结

本文介绍了一种新的异常流量检测方法,即使用改进的 CUSUM 算法来检测路由器输入输出流量的变化情况.该算法能提高检测的准确性及在线检测速度,降低运算开销.与以前的基于监控业务量的攻击检测机制不同的是,该算法小巧,可以作为嵌入式模块,安装在核心路由器中,提高网络的总体性能.我们接下来要做的工作是如何把攻击进行分类,使得处理模块能够针对不同的攻击,采取不同的策略.

References:

[1] Wang HN, Zhang DL, Kang GS. Detecting SYN flooding attacks. IEEE Computer and Communication Society, 2002,3(6): 1530−1539

[2] Zhu WT, Li JS, Hong PL. A router agent based distributed flooding detection system. Chinese Journal of Computers, 2003, 26(11):1585−1590 (in Chinese with English abstract).

[3] Siris, VA, Papagalou F. Application of anomaly detection algorithms for detecting SYN flooding attacks. In: Proc. of the Conf. on Global Telecommunications (GLOBECOM 2004). IEEE, 2004. 2050−2054.

[4] Xiang Y, Lin Y, Lei WL, Huang SJ. Detecting DDOS attack based on network self-similarity. IEEE Int'l Conf. on Communications, 2004,151(3):292−295.

[5] Jin SY, Yeung DS. A covariance analysis model for DDoS attack detection. In: Proc. of the Int'l Conf. on Communications. IEEE, 2004. 1882−1886.

[6] Feinstein L, Schnackenberg D, Balupari R, Kindred, D. Statistical approaches to DDoS attack detection and response. In: Proc. of the DARPA Information Survivability Conf. and Exposition. 2003. 303−314.

[7] Oskiper T, Poor HV, Matrix CUSUM: A recursive multi-hypothesis change detection algorithm .In: Proc. of the 2001 IEEE Int'l Symp. on Information Theory. 2001.

[8] Pu Xl. On the improving of cumulative sum chart. ACTA Mathematicae Applicatae SINICA, 2003,26(2):226−241 (in Chinese with English abstract).

[9] Morgenstern VM, Upadhyaya BR. Benedetti M. Signal anomaly detection using modified CUSUM method. In: Proc. of the 27th IEEE Conf. on Decision and Control. 1988. 2340−2341.

[10] Moustakides GV. Performance of CUSUM tests for detecting changes in continuous time processes. In: Moustakides GV, ed. Proc of the IEEE Int'l Symp. Information Theory. 2002.186−187.

附中文参考文献:

[2] 朱文涛,李津生,洪佩琳.基于路由器代理的分布式湮没检测系统.计算机学报,2003,26(11):1585−1590.

[8] 濮晓龙.关于累积和(CUSUM)检验的改进.应用数学学报,2003,26(2):226−241.