一种自适应非参量 CUSUM 控制图算法*)

于 明[1] 陈卫东[2] 周希元[2]
(大连理工大学电子与信息工程学院 大连 116023)[1]
(中国电子科技集团公司第 54 研究所 石家庄 050081)[2]

摘 要 针对 CUSUM 控制图中存在的固定检测门限和对异常终止反应迟钝的缺点,提出了一种自适应的非参量 CUSUM 控制图算法。该算法首先利用固定门限剔除野值,同时简化了对显著异常的检测过程。然后,采用简单滑动平均算法对非野值数据进行平滑,并基于切比雪夫不等式理论对平滑后的数据进行转换,使之满足非参量 CUSUM 算法的使用条件。最后,由算法根据数据转换结果自适应地设置 CUSUM 算法中的检测门限,并在发出异常告警后实施异常终止监控。在针对 SYN 洪流攻击的仿真检测试验中,利用该算法能够在检测时延不超过 7 个采样周期且攻击持续期间不发生漏警的要求下,准确地检测出最低攻击流量仅为正常业务流量 20%的攻击行为。

关键词 控制图,自适应检测,CUSUM,SYN 洪流攻击

Adaptive Nonparametric CUSUM Control Chart

YU Ming[1] CHEN Wei-dong[2] ZHOU Xi-yuan[2]
(School of Electronics and Information Engineering, Dalian University of Technology, Dalian 116023, China)[1]
(The 54th Research Institute of CETC, Shijiazhuang 050081, China)[2]

Abstract Fixed thresholds and slow response to end of the anomalies are two shortcomings of the traditional CUSUM control chart. Three measures are taken in this paper to solve both problems. Firstly, a fixed threshold was set to eliminate outliers and simplify the detection of obvious anomalies. Secondly, the filtered data were smoothed and transformed based on the simple moving average method and the Chebyshev inequality. Lastly, an adaptive threshold was set according to the transformed results, and the decision-making process would continue monitoring the anomaly for its possible end after an alarm was raised. Simulations of source end defense against SYN flooding attacks on a real traffic trace show that attack traffic which is as low as 20% of the averaged normal traffic can be accurately detected within no more than 7 sampling periods and no miss of alarms during the attacks.

Keywords Control chart, Adaptive detection, CUSUM, SYN flooding attacks

在工业异常监控中,CUSUM 控制图常用于检测生产过程中产品属性均值的变化,该算法具有计算量小、检测迅速、实施简单的优点。近年来,CUSUM 控制图在网络安全研究中备受关注。H. Wang 等人基于非参量 CUSUM 控制图构建了一个用于 SYN 洪流攻击防御的 FSD 系统[1]。P. Tao 等人则利用非参量 CUSUM 控制图构建了一种基于源 IP 地址进行 DDoS 攻击检测的 SIM 系统[2]。陈伟等人提出了一种用于源端网络 DDoS 攻击检测的轻量级方法[3],该方法首先使用 Bloom 滤波器进行网络数据提取,然后用 CUSUM 控制图对数据进行异常分析,从而达到使用少量资源进行准确检测的目的。

然而,由于 CUSUM 控制图及其非参量版本均使用固定的检测门限进行异常判决,因而对检测门限的设置具有很大的依赖性。此外,CUSUM 控制图在应用时存在过量积累的问题,导致其对目标过程恢复正常反应迟钝[4]。对此,本文提出了一种自适应的非参量 CUSUM 控制图算法,主要解决了两个问题,即自适应检测门限的设计和对异常终止的及时检测。

1 算法设计

本文算法由两个模块组成,即野值处理模块和自适应非参量 CUSUM 处理模块(以下简称自适应处理模块)。前者主要负责对显著异常进行处理,以简化检测过程,后者主要负责微弱异常的检测。

1.1 野值处理模块

该模块沿袭了固定门限的检测思路,利用一个简单门限(T_o)剔出了野值数据,并简化了对显著异常的检测。高于门限 T_o 的数据被视为野值数据,低于门限 T_o 的数据由自适应 CUSUM 处理模块做进一步处理。野值处理模块中设置了一个野值累计变量 A_O,用于累计野值出现的次数,告警信号(d_n)由一个告警控制参数 K_O 控制产生。当 A_O 增至 K_O 时,产生显著异常告警信号,同时利用变量 *AlarmDur* 对告警时间(单位:采样周期)进行累计,用于自适应处理模块中的参数复位操作。野值处理流程如图 1 所示,图中变量 A_N,A_D 是与自适应处理模块相关的两个累计变量。

1.2 自适应处理模块

1.2.1 数据平滑与转换

令独立随机变量序列 $X=\{x_n\}_{n=1}^{\infty}$ 表示输入数据,并设置一个大小为 N 的滑动窗口。利用简单滑动平均算法对 X 进行平滑处理后得到一个新的序列,记为 $U=\{u_n\}_{n=N}^{\infty}$。其中,$u_n=\frac{1}{N}\sum_{i=n-N+1}^{n}x_i$。不过,序列 U 并不能直接作为 CUSUM 算法的输入序列进行处理,因为非参量 CUSUM 算法要求样本序列的数学期望值为负值[5]。由于这一条件常常无法得到满足,因而需要选择一个合适的偏移常数 β,使序列 U 满足数学

*)国家"863"计划资助课题(资助号:2005AA123910)。于 明 博士研究生;周希元 博士生导师,研究员。

期望为负值的要求。与传统的 CUSUM 控制图算法凭经验设置偏移常数的做法不同，本文算法基于切比雪夫不等式理论构建了一种自适应的偏移常数，其构建过程包括以下两个步骤。

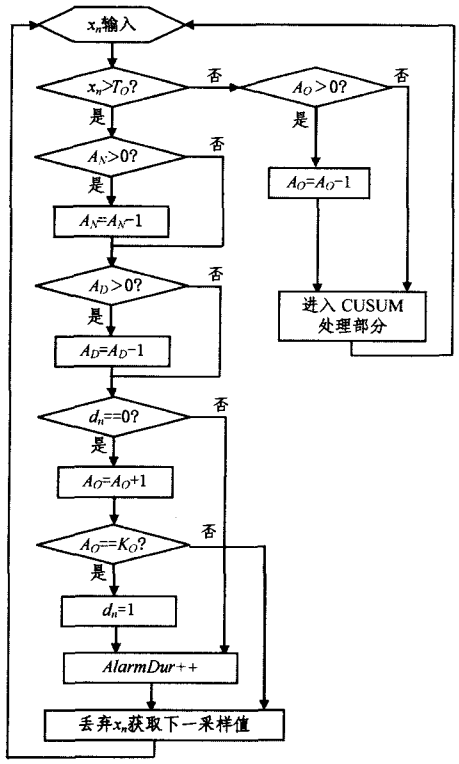

图 1　野值处理流程图

步骤 1　对序列 U 的均值 $\hat{\mu}_n(n\geqslant N)$ 和方差 $\hat{\sigma}_n(n\geqslant N)$ 进行在线估计和更新。具体方法为

$$\begin{cases}\hat{\mu}_n=(1-p)*\hat{\mu}_{n-1}+p*u_n\\ \hat{\mu}_N=u_N\end{cases}\tag{1}$$

$$\begin{cases}\hat{\sigma}_n=\sqrt{(\sum_{i=N+1}^{n}(u_i-\hat{\mu}_{i-1})^2)/(n-1)}\\ \hat{\sigma}_N=\sqrt{(\sum_{i=1}^{N}(u_i-\hat{\mu}_N)^2)/(N-1)}\end{cases}\tag{2}$$

其中，p 为平滑因子。当判定数据异常或处于告警状态时，$\hat{\mu}_n=\hat{\mu}_{n-1}$，$\hat{\sigma}_n=\hat{\sigma}_{n-1}$。

步骤 2　对序列 U 进行转换，得到序列 $Z=\{z_n\}_{n=N}^{\infty}$。其中，$z_n=u_n-\hat{\mu}_{n-1}-3\hat{\sigma}_{n-1}$。由切比雪夫不等式可知，$P(|u_n-\hat{\mu}_n|<3\hat{\sigma}_n)\geqslant 0.89$，而 $P(u_n-\hat{\mu}_n-3\hat{\sigma}_n<0\cap u_n-\hat{\mu}_n+3\hat{\sigma}_n>0)\geqslant 0.89$。所以，在保守估计下，$P(u_n-\hat{\mu}_n-3\hat{\sigma}_n<0)>0.89$。在目前国内外有关 CUSUM 控制图的研究中，这种转换方法尚属首次提出，也是本文算法的第一个自适应性特征。

1.2.2　自适应 CUSUM 检测

为了降低处理开销，本文算法采用了非参量 CUSUM 算法的递归形式[5]，其处理过程如下：

$$\begin{cases}S_n=(S_{n-1}+z_n)^+\\ S_N=0\end{cases}\tag{3}$$

其中，S_n 为检测统计量数据，$x^+=\mathrm{MAX}(x,0)$。令变量 T_A 表示检测门限，并将 T_A 的初始值设为零，则对于异常发生的检测流程如图 2 所示。从图中可以看出，检测门限 T_A 的设置取决于 z_n 大于 0 时的取值以及告警控制参数 K_A。这是本文算法的第二个自适应性特征，也是目前国内外首次提出的一种自适应 CUSUM 门限设置方法。

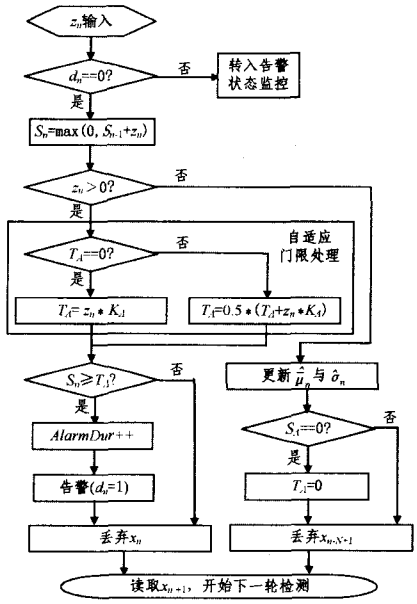

图 2　非参量自适应 CUSUM 算法的检测流程

1.2.3　异常告警状态监控

这一处理方式主要是为了及时地对异常终止作出反应。在算法执行过程中，以下两种情况中任何一种的发生都将被视为异常终止：(i)连续出现 $z_n\leqslant 0$ 的情况；(ii)$z_n>0$ 但原始数据 x_n 本身取值出现陡然下降的情况。对于情况(i)，主要利用变量 A_N 进行状态累积，利用预置常量 K_N 进行取消告警控制。对于情况(ii)，本文算法在数据陡降的判决中引入了自适应门限的思想，分别设置了一个数据陡降参考门限 T_D（初始值为 0），一个陡降累计变量 A_D（初始值为 0）和一个陡降告警取消控制参数 K_D。其中，T_D 利用指数加权滑动平均(EWMA)算法进行更新，K_D 由用户指定。具体的陡降判断规则为

(i)当 $x_n<T_D$ & $(T_D-x_n)\geqslant(T_D-\hat{\mu}_n)/2$ 时，判断原始数据发生陡降。

(ii)每检测到一次陡降，A_D 累计一次，当 $A_D=K_D$ 时便取消告警。

另外，若异常持续时间超过了一定的时限，在取消异常告警的同时将进行参数复位操作。该时限值由用户指定，用变量 T_L 表示。图 3 给出了异常告警后的状态监控过程。

需要指出的是，算法设计中引入了 6 个控制参数，分别为 T_o，T_L，K_O，K_N，K_A 及 K_D。对这些参数的设置要求比较宽松：对 T_o 的设置要求其高于检测变量的经验均值；T_L 的设置以 5～6 个采样周期为宜；K_O 与 K_A 保持一致，体现用户对检测时延的要求；K_N 与 K_D 保持一致，体现用户对取消告警时延的要求。

2　算法性能分析

对于算法的野值处理部分来说，其产生虚警的概率与野值剔除门限 T_o 和控制参数 K_O 有关。令 $f_0(x)$ 表示正常情况下检测变量的概率分布密度，则野值处理部分产生的虚警

概率可以表示为：

$$P_{F_0}=[\int_{T_0}^{\infty}f_0(x)\mathrm{d}x]^{K_0} \tag{4}$$

在本文算法中，P_{F_0} 可以忽略不计，其原因在于：(i) T_0 可靠地高于检测变量在正常情况下的经验均值，从而使得正常数据高于 T_0 成为稀有事件；(ii)控制参数 K_O 的设置不仅进一步降低了正常数据高于 T_0 的概率，而且大大降低了瞬时突发随机异常对 P_{F_0} 的影响。此外，野值处理部分的漏警概率也可以忽略不计，因为对低于 T_0 的非野值数据，CUSUM 处理部分会做进一步处理。因此，本文只针对 CUSUM 处理部分的检测性能进行分析。

迄今为止，对非参量控制图算法进行精确的性能分析仍然是一件非常困难的事情，这方面最重要的理论成果集中体现在由 B. E. Brodsky 和 B. S. Darkhovsky 合著的“Nonparametric Methods in Change-point Problems”[5]一书中。该书中对非参量 CUSUM 算法的性能进行了较为详尽的讨论，其分析结果对于非参量 CUSUM 算法的设计来说具有指导意义。基于该书中的相关结论，结合本文算法的设计思想，我们对影响非参量自适应 CUSUM 算法的虚警概率和归一化检测时延(及检测时延)的因素进行了分析。

令 h 表示检测门限，μ_0 (μ_1) 和 σ_0 (σ_1) 分别表示正常(异常)状态下平滑序列 U 的均值和方差，$\mu_0^{(Z)}$ 和 $\mu_1^{(Z)}$ 分别表示正常状态下和存在异常时序列 Z 的均值，m 和 t_a 分别表示异常的起始时刻及其首次告警时刻。根据文献[5]，可以得到以下关于非参量 CUSUM 算法的虚警概率(P_F)和归一化检测时延(ρ_τ)的表达式。

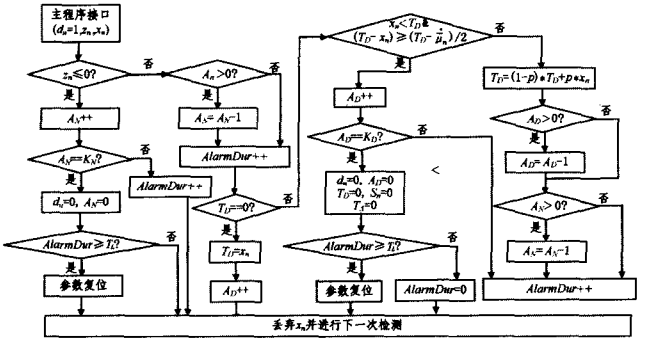

图 3　异常告警后的状态监控过程

1)虚警概率：

$$P_F\leqslant c_1\exp(-c_2h) \tag{5}$$

其中，c_1 和 c_2 为两个正常数，其取值只与被检测序列的边际分布和混合系数(mixing coefficients)有关，而与检测算法无关。

2)归一化检测时延：

定义检测时延 $\tau_s=(t_a-m)^+$，当 $h\to\infty$ 时，归一化检测时延可以表示为

$$\rho_\tau=\frac{\tau_s}{h}\to\frac{1}{\delta-|\mu_0^{(Z)}|} \tag{6}$$

其中，δ 表示异常发生前后被检测序列的均值之差。

基于(5)式和(6)式，可以对本文所提出的非参量自适应 CUSUM 算法的虚警概率和归一化检测时延进行分析。

首先分析本文算法的虚警性能。在执行异常检测功能时，本文算法与非参量 CUSUM 算法的差异仅在于检测门限的不同，而对于算法的性能分析而言，只要获得 T_A 的表达式即可对本文算法的虚警性能做出定性分析。设：自 $S_n=0$ 时的某一时刻起至发出告警期间，共有 $z_1, z_2, \cdots, z_M$ 等 M 个大于零的 Z 序列值，根据本文算法的设计思想(参见图 2)，可将发出异常告警时的检测门限值表述为：

$$T_A=K_A(\frac{z_1}{2^{M-1}}+\sum_{j=2}^{M}\frac{z_j}{2^{M-j+1}}) \tag{7}$$

其数学期望值为：

$$E(T_A)=K_AE(\frac{z_1}{2^{M-1}}+\sum_{j=2}^{M}\frac{z_j}{2^{M-j+1}})=K_AE(z_j\,|\,z_j>0) \tag{8}$$

由于 $z_j=u_j-\hat{\mu}_{j-1}-3\hat{\sigma}_{j-1}$，因而在正常状态下：

$$\mu_0^{(Z)}=E(z_j)=E(u_j-\hat{\mu}_{j-1}-3\hat{\sigma}_{j-1})=E(u_j)-\mu_0-3\sigma_0=-3\sigma_0 \tag{9}$$

自 $S_n=0$ 时的某一时刻起至发生虚警时，

$$E(z_j\,|\,z_j>0)\geqslant E(u_j)-\mu_0-3\sigma_0 \tag{10}$$

且 $\mu_0+3\sigma_0\leqslant E(\mu_j)\leqslant T_0$。

当发生异常时，不妨假设 $E(\mu_j)=\lambda\mu_0$，其中 λ 表示异常现象的显著状况，由(9)式可以得到 $E(z_j\,|\,z_j>0)\geqslant(\lambda-1)\mu_0-3\sigma_0$。因此

$$E(T_A)\geqslant K_A[(\lambda-1)\mu_0-3\sigma_0] \tag{11}$$

将式(11)代入式(5)中，可以得到：

$$P_F\leqslant c_1\exp\{-c_2K_A[(\lambda-1)\mu_0-3\sigma_0]\} \tag{12}$$

当异常发生后，$\mu_1^{(Z)}=E(z_j)=E(u_j)-\mu_0-3\sigma_0$，故而

$$\mu_1^{(Z)}=(\lambda-1)\mu_0-3\sigma_0 \tag{13}$$

$$\delta=\mu_1^{(Z)}-\mu_0^{(Z)}=(\lambda-1)\mu_0 \tag{14}$$

将式(9)、(11)、(13)和(14)代入(6)式，即可得到：当 $K_A\to\infty$ 时，

$$\rho_\tau\to\frac{1}{(\lambda-1)\mu_0-3\sigma_0} \tag{15}$$

$$\tau_s\to K_A \tag{16}$$

由式(12)、(15)、(16)可以看出：

(i)提高用户可控参数 K_A 的取值可以将虚警概率限制在更小的范围内，但同时也导致(归一化)检测时延的增加。

(ii)虚警概率上界的取值还与正常状态下采样数据的波动状况(由 σ_0 表示)有关。当 σ_0 增大时，虚警概率的上界值将增大。

(iii)归一化检测时延的取值与采样数据的均值(μ_0)、方差(σ_0)以及异常的显著状况有关。当 μ_0 增加或 σ_0 减小时，归一化检测时延减小；当异常显著状况增大时，归一化检测时延会降低。

(iv)K_A 的取值越高，检测时延便越接近于 K_A。

3　应用及仿真

本节研究了自适应非参量 CUSUM 控制图算法在 SYN 洪流攻击的源端网络防御中的应用，并基于实际网络流量记录对本文算法的有效性进行了验证。所采用的流量数据由 NLANR 研究组织采集于 Leipzig 大学的一条 OC3 PoS 互联网接入链路，采集日期为 2003 年 2 月 21 日，采集时间为当地时间 12 点 14 分，流量时长为 2 小时 46 分。

令(i) S_n 和 A_n 分别表示在第 n 个采样周期内经源端网络检测点发出的 SYN 请求和接收到的 SYN/ACK 应答的数目；(ii)$\bar{S}$ 和 $\bar{A}$ 分别表示正常情况下每采样周期内源端网络中发出的 SYN 请求和收到的 SYN/ACK 应答的平均数量；(iii) S_A 表示攻击机在一个采样周期内发出的攻击性 SYN 请求的数量，并假设 $S_A=\varepsilon\bar{S}$，其中 $\varepsilon(\varepsilon>0)$ 表示攻击流相对于正常流量的攻击强度。

构建序列 $X=\{x_n\}_{n=1}^{\infty}$，其中 $x_n=[(S_n-A_n)/S_n]^+$。正

常情况下，x_n 的取值趋近于0；攻击发生时，x_n 的取值趋近于1。令 μ_0，μ_1 分别表示攻击前后序列 X 的均值，且分别有

$$\mu_0 = E[\frac{\bar{S}-\bar{A}}{\bar{S}}] \tag{17}$$

$$\mu_1 = E[\frac{S_A+\bar{S}-\bar{A}}{S_A+\bar{S}}] = \frac{1+\varepsilon/\mu_0}{1+\varepsilon}\mu_0 \tag{18}$$

可以看出，攻击强度 ε 对 X 均值的影响与算法性能分析中定义的异常显著状况参数 λ 相似，因而可以通过 ε 来衡量算法应用于SYN洪流检测时的性能。

仿真试验分两步进行。第一步，利用本文算法对原始流量进行检测，考察算法的虚警状况。第二步，每次试验均向流量记录中注入持续时间为10分钟的攻击数据，且每次试验中攻击的开始时间相差1分钟。对本文所采用的Leipzig流量数据而言，总共进行了144次试验。仿真试验考察了本文算法的基本性能，即虚警概率 P_F、攻击检测时延 τ_s、取消告警时延 τ_c、平均最低可检测的攻击强度 $\varepsilon_{\min}$。

判断攻击是否被准确检测的标准为：(i)攻击持续期间没有出现漏警；(ii)检测时延/取消告警时延不超过7个采样周期。检测程序中需要预先设置的参数为：采样周期为20秒，滑动窗口 $N=3$，EWMA平滑因子 $p=0.98$，野值剔除门限 $T_O=0.65$，参数复位控制时限 $T_L=6$。表1给出了试验检测结果数据，图4给出了当 $K_A=K_D=4$ 时的4次攻击试验的检测结果。在表1和图4中，符号 t_s 表示单位采样周期。

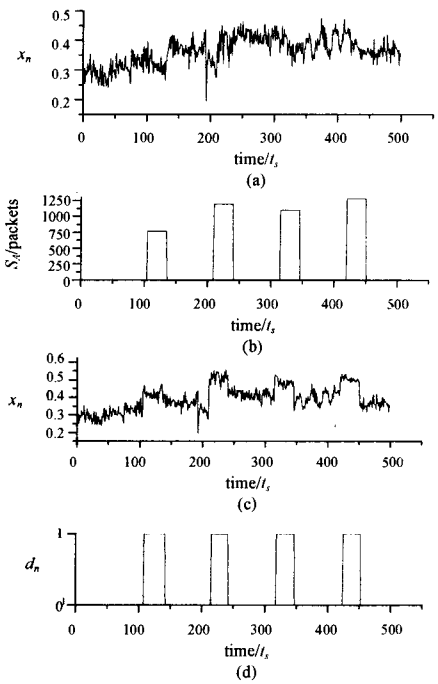

图4 攻击检测仿真验证结果。
(a) 正常采样序列；(b)攻击流量；
(c)加入攻击流量后的采样序列；(d)检测结果。

表1 对SYN洪流攻击仿真的检测结果

(K_A,K_D)	$P_F(\times10^{-3})$	$\bar{\tau}_s/t_s$	$\bar{\tau}_c/t_s$	$\varepsilon_{\min}(\%)$
(2,2)	6.0	3.1	2.2	16.3
(3,2)	6.0	4.5	2.3	18.3
(3,3)	12.0	4.5	3.2	18.3
(3,4)	14.0	4.5	3.8	18.7
(4,4)	0.0	5.6	3.9	18.7
(5,5)	0.0	6.0	4.7	18.7

从仿真结果中可以看出：(i)最低可检测攻击强度低于正常流量强度的20%；(ii)提高 K_A 的值或降低 K_D 的值均可以降低算法的虚警概率。表1中 $K_A=K_D=3$ 时的虚警率高于 $K_A=K_D=2$ 时的虚警率的原因在于，本文仿真试验中 $K_A=2$ 与 $K_A=3$ 时虚警率的差异并不明显，而此时 K_D 便成为影响虚警率的重要因素：K_D 越小，虚警的总时间就越短，从而虚警率就越低。这一点通过比较 $K_A=3, K_D=3$ 与 $K_A=3$，$K_D=2$时的虚警率便可得知。(iii)当 K_A 增大时，$|\bar{\tau}_s-K_A|/K_A$ 的值逐渐降低，意味着平均检测时延 $\bar{\tau}_s$ 趋近于 K_A。(iv)当 K_D 增大时，$|\bar{\tau}_c-K_D|/K_D$ 的值逐渐降低，意味着取消告警时延 $\bar{\tau}_c$ 趋近于 K_D。

与其他针对SYN洪流攻击检测的算法仿真试验相比[1-4,6]，本文算法及其仿真的优点在于：(1)在性能要求非常苛刻的情况下(攻击期间无漏警、检测时延/取消告警时延不超过7个采样周期)，可检测的最低攻击流量强度尚不足正常流量强度的20%，远低于其他算法的仿真检测结果；(2)采用时间遍历的方式充分考虑了采样数据的平稳性对算法检测效果的影响，这一点在其他检测算法的仿真试验中并没有得到实现。

结束语 在很多情况下，对动态系统实施实时监控都面临着如何对系统进行统计建模的问题，而实践中通常是利用某种简单的统计模型来模拟系统行为及其相关参量的统计分布，其监控结果大多不尽人意[7]。本文提出的自适应非参量CUSUM算法可以避免对所处理数据的分布类型和分布参数做出假设，非常适合于观察值序列的统计分布无法预知的情况。仿真试验结果表明，本文算法在对微弱异常现象的自适应检测方面具有较强的可行性。在后续的研究中，我们将对该算法的检测性能做进一步分析，并尝试将其推广应用到其他对数据缺乏先验知识的工业控制场合。

参考文献

[1] Wang Hai-ning, Zhang Dan-lu, Shin Kang G. Detecting SYN Flooding Attacks [C] // Proc. of IEEE INFOCOM 2002. New York: IEEE Press, 2002: 1530-1539

[2] Tao Peng, Leckie C, Ramamohanarao K. Proactively Detecting Distributed Denial of Service Attacks Using Source I PAddress Monitoring [C] // Proc. of NETWORKING 2004. Athens, Greece: Springer, 2004: 771-782

[3] 陈伟，何炎祥，彭文灵. 一种轻量级的拒绝服务检测方法 [J]. 计算机学报，2006，29(8)：1392-1400

[4] Yu Ming, Chen Wei-dong, Zhou Xi-yuan. Source-end defense against SYN flooding attacks: an Adaptive Detection Method [J]. Dynamics of Continuous Discrete and Impulsive Systems-Series B-Applications & Algorithms, 2006(3. Supp): 1674-1677

[5] Brodsky B E, Darkhovsky B S. Nonparametric Methods in Change-point Problems [M]. the Netherlands: Kluwer Academic Publishers, 1993

[6] Siris V A, Papagalou F. Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks [C] // Proc. GLOBECOM'2004. New York: IEEE Press, 2004: 2050-2054

[7] 刘育明. 动态过程数据的多变量统计监控方法研究[D]. 杭州：浙江大学，2006：4-9