P.O.Box 8718, Beijing 100080, China	Journal of Software, Dec. 2005,16(12):
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2005 by The Editorial Department of *Journal of Software*

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

孙知信, 唐益慰, 程 媛
(南京邮电大学 计算机学院,江苏 南京 210001)
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.
联系人: 孙知信 Phn: +86-25-85198095, E-mail: sunzx@njupt.edu.cn, http://www.nupt.edu.cn

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

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.

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
http://www.jos.org.cn/1000-9825/16/2117.htm

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.

基金项目：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)

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.