混合二次网络流量异常状态模型研究

孙知信,焦 琳,姜举良
(南京邮电大学 计算机系,江苏 南京 210003)

摘 要:提出了一种网络流量异常状态统计模型——混合二次网络状态模型 MQNSM-G(D_{KS},D_{KKS},D_{AKS})。该模型从动态性原则以及降低误检率和漏检率思想出发,改进原有统计模型,建立了可以动态设定描述网络流量状态参数的加权统计模型。基于混合二次网络状态模型 MQNSM-G(D_{KS},D_{KKS},D_{AKS})的入侵检测系统进一步证明了该模型可以更大程度上提高异常检测性能,降低其误检率和漏检率。

关键词:分布式拒绝服务攻击;入侵检测;误检率;漏检率
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2007)03-0153-03

Research on Mixed Quadratic Network Traffic Abnormal States Model

SUN Zhi-xin, JIAO Lin, JIANG Ju-liang
(Dept. of Computer Sci. and Techn., Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: A statistical model for detecting abnormal network traffic - mixed quadratic network states model MQNSM-G(D_{KS}, D_{KKS}, D_{AKS}) is presented. Based on principles of developments and reducing FNP and FPP, this paper builds up a statistical model with weights that can dynamically set parameters of network traffic states, which improves on former statistical models. It has proved that performances of anomaly detection can be improved to a great degree and the FPP and FNP can be cut down prominently in an IDS based on the mixed quadratic network states model MQNSM-G(D_{KS}, D_{KKS}, D_{AKS}).

Key words: distributed denial of service; intrusion detection; false positive probability; false negative probability

0 引 言

目前网络入侵的频率越来越高,入侵的危害性也越来越大,尤其是消耗网络资源的入侵行为愈演愈烈,例如目前变幻莫测的 DOS 攻击[1]。而网络带宽作为一种宝贵的资源,直接影响到人们访问网络的质量。因此,人们纷纷提出各种基于网络的入侵检测方法[2~4]。基于网络的入侵检测技术传统上分为两大类型:异常入侵检测(anomaly detection)和误用入侵检测[5],异常入侵检测方法与误用入侵检测方法相比其优点在于检测不依赖于攻击特征,它是根据检测目标发现网络异常,预测未知攻击。异常入侵检测方法有很多种,例如基于模式预测的异常检测、基于聚类的异常检测和基于网络流量统计的异常检测等等[5]。但是异常检测的缺点是有误检率(False Positive Probability)和漏检率(False Negative Probability)[6]。其中基于网络流量统计的入侵检测不失为一种降低误检率和漏检率的较好的异常检测方法[7,8]。CIDS[9](Correlation Intrusion Detection System)利用特征间交叉相关的变化来确定当前流量是否存在攻击,文献[7]提出的状态统计模型,比较全面地总结了对网络流量状态描述的方法,但是在这些统计模型中网络流量状态只是对固定的特征参量有不变的依赖程度,因此这些模型缺乏动态性,仍然有误检率和漏检率。

文中旨在找到一种区别于以往的异常流量统计模型,以期实时地、动态地识别网络异常流量,并有效控制误检率和漏检率。

1 网络状态模型 (MQNSM-G)

分析以往建立的网络状态模型[7,9],明显感觉到其缺乏变动性,无法根据实际网络状态增加必要的统计参数,或减少不必要的统计参数。文中力求建立一种可以根据网络实际状态,动态增减统计参数的网络状态统计模型(MQNSM-G)。

收稿日期:2006-05-25
基金项目:国家自然科学基金(60573141);华为基金资助
作者简介:孙知信(1964-),男,安徽宣城人,教授,研究方向为计算机网络及安全。

设节点当前网络状态 $\boldsymbol{X}(x_1,x_2,\cdots,x_n)\in[0.0,1.0]^n$ 和历史网络状态 $\boldsymbol{Y}(y_1,y_2,\cdots,y_n)\in[0.0,1.0]^n$，$x_i(1\leqslant i\leqslant n)$ 是网络状态的各个数值表现，为了有相同的测试标准，对 x_i 进行了归一化，$\boldsymbol{Y}$ 是 $\boldsymbol{X}$ 的最近的一个历史向量。不同数值表现的权值 $\boldsymbol{W}(w_1,w_2,\cdots,w_n)$，$0\leqslant W_i\leqslant 1$。$\boldsymbol{W}$ 表示该数值表现对网络流量和测试的影响。

定义 改进的 KS、改进的 KKS 和改进的 AKS：

$$D_{KS}=\sum_{j=1}^{k}\{\max_{(i,j)}\}\{W_i\mid X_i-Y_i\mid\}$$

$$D_{KKS}=\sum_{j=1}^{k}\{\max_{(i,j)}\}\{W_i(X_i-Y_i)\}+\sum_{j=1}^{k}\{\max_{(i,j)}\}\{W_i(Y_i-X_i)\}$$

$$D_{AKS}=\{\sum_{j=1}^{k}\{\max_{(i,j)}\}\{W_i\mid X_i-Y_i\mid\}\}+\{\sum_{i=1}^{n}W_i\mid X_i-Y_i\mid\}$$

其中，$1\leqslant i\leqslant n$，$0<k<n$，$\{\max_{(i,j)}\}\{P_i$ 表示取数组 P_i 的第 j 个最大数，$\sum_{j=1}^{k}\{\max_{(i,j)}\}\{P_i$ 的意义就是取数组 $P(P_i)(1\leqslant i\leqslant n,0<k<n)$ 的最大的 k 个数。

设当前网络状态 $M(t)=(D_{KS},D_{KKS},D_{AKS})$，$M(t_0)$ 为历史网络状态，得

$$MQNSM-G(D_{KS},D_{KKS},D_{AKS})=\mid M(t)\cdot(M(t))^{T}-M(t_0)\cdot(M(t_0))^{T}\mid$$

网络处于正常状态时 MQNSM－G 应该处于一个稳定的状态(即值在一个范围内变动)。一旦 MQNSM－G 出现异常，有理由相信网络流量有异常，此时需要提供一定的流量处理方法，使 MQNSM－G 达到正常状态。文中不对流量处理策略做分析。当 D_{KS},D_{KKS},D_{AKS} 处于稳定状态时，MQNSM－G 处于稳定状态，当 D_{KS},D_{KKS},D_{AKS} 中有一个处于不稳定状态，MQNSM－G 将不再处于稳定状态。这里所要做的是设定一个稳定状态的合理的范围，因为在一种特别情况下，当 D_{KS},D_{KKS},D_{AKS} 都处于稳定范围时，而 G 却超越了稳定范围，因为 MQNSM－G 有可能叠加 D_{KS},D_{KKS},D_{AKS} 三种模型的正常变化值。但是这是一种非常极端的情况，因为网络在正常状态时 D_{KS},D_{KKS},D_{AK} 应该都保持很小的变化值，三种很小的变化的叠加，相对于网络异常时发生的状态突变仍然是很小的。

为了准确描述网络状况，需要为选取的参数设定权值，以实现动态原则。权值(范围 0～1)表示模型对该参数的依赖程度，权值为 0 则与该参数无关，权值为 1 则最大相关。每个参数的初始权值依据经验而定。MQNSM－G 首先对网络状态进行分析，区分当前网络状态是正常的还是异常的，并根据分析结果进行参数权值调整，具体调整方法如下：

首先设定参数波动上限 U_i 和波动下限 D_i。

在正常状态时：

1) 变动较大的参数(波动范围 $>U_i$) 对网络状态标识不稳定，应该降低模型对其的依赖程度，减小其权值；

2) 变动较小的参数(波动范围 $<D_i$) 对网络状态标识稳定，应该增强模型对其的依赖程度，增加其权值。

在异常状态时：

1) 变动较大的参数对网络异常状态具有很大的特殊标识意义，应该增强模型对其的依赖程度，增加其权值；

2) 变动较小的参数对网络异常状态具有很小的特殊标识意义，应该降低模型对其的依赖程度，减小其权值。

在正常状态和异常状态中，都可能会有些参数波动范围介于 U_i 和 D_i 之间，说明这些参数能反映当前网络状态，但是并不是很明显，故应保持这些参数的权值不变。

2 基于 MQNSM－G 的入侵检测系统

MQNSM－G 已应用于一个入侵异常检测系统中，该入侵检测系统部署在路由器端局域网侧一个高性能服务器上，其软件实现如图 1 所示。

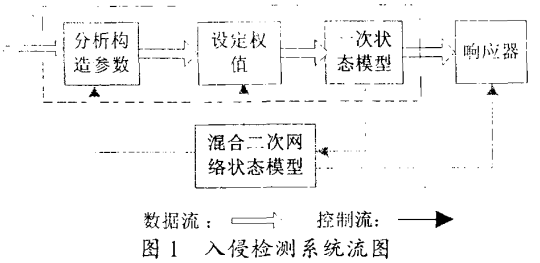

图 1 入侵检测系统流图

在该入侵检测系统中共提取网络流量的 20 个属性，部分属性及其初始权值如表 1 所示。为了检测在不同网络流量状况下该模型的性能，在实验中设定了 3 种不同情况的流量分别进行检测。在这 3 种流量中

表 1 网络流量属性

Index	Name	Weight
1	Ip－in－packet－length	0.353
2	Ip－in－packet－rate	0.462
…	…	…
20	Ip－in－byte－rate	0.481

攻击流量在背景流量中的比重 R 由 4% 依次减小到 1%。

在对流量进行统计检测的过程中发现当攻击流量在背景流量中的比重 R 较大时,各种测试方法单独的性能都很好,检测的误报率和漏报率都很低,基本上可以达到 0;但随着 R 的减小,以上各测试的性能在不同流量状况下就有所不同,尤其是并没有哪一种测试方法一直占有优势。文中使用 MQNSM - G(D_{KS},D_{KKS},D_{AKS}) 模型进行测试,在不同网络流量状况下都可以得到最佳的检测效果。在此定义 Misclassification Rate(MR) 为误报率和漏报率之和,可以得到在后 2 种网络流量下单独使用各种测试方法与文中采用 MQNSM - G(D_{KS},D_{KKS},D_{AKS}) 模型进行测试的检测结果比较图如图 2、图 3 所示。从各图的测试情况及比较情况可以看出使用 MQNSM - G(D_{KS},D_{KKS},D_{AKS}) 模型进行测试在任何一种网络流量下性能都是最佳的,因此性能也更为稳定。

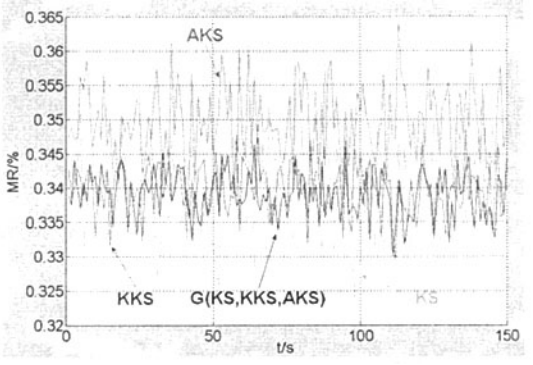

图 2　R = 2% 时各种测试结果

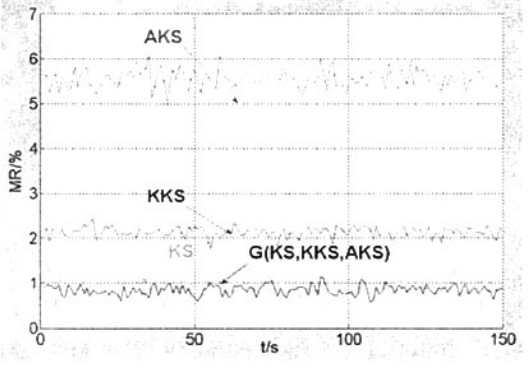

图 3　R = 1% 时各种测试结果

3　总　结

对网络流量状态进行统计是网络异常检测的一个重要环节,直接影响到异常检测的性能。文中提出的混合二次网络流量异常状态模型从动态性原则及降低误检率和漏检率思想出发,对以往统计方法和模型进行较大改进,能更加准确地描述网络流量异常。仿真试验证明,采用该统计模型的网络异常检测系统有更好的性能,误检率和漏检率更低。

参考文献:

[1] Keromytis A D, Misra V, Rubenstein D. SOS: secure overlay services[C]// Proceedings of the 2002 conference on Applications, technologies, architectures, and protocols for computer communications, ACM SIGCOMM Computer Communication Review. [s.l.]: [s.n.], 2002: 61 - 72.

[2] Yin Qingbo, Shen Liran, Zhang Rubo, et al. A New Intrusion Detection Method Based on Behavioral Model[C]// Intelligent Control and Automation, 2004 IEEE, WCICA 2004. Fifth World Congress. [s.l.]: [s.n.], 2004: 4370 - 4374.

[3] 张凤斌,杨永田,江子扬. 遗传算法在基于网络异常的入侵检测中的应用[J]. 电子学报,2004,32(5):875 - 877.

[4] 李德全,徐一丁,苏璞睿,等. IP 追踪中的自适应包标记[J]. 电子学报,2004,32(8):1334 - 1337.

[5] 卿斯汉,蒋建春,马恒太,等. 入侵检测技术研究综述[J]. 通信学报,2004,25(7)19 - 29.

[6] Bai Y, Kobayashi H. Intrusion Detection Systems: technology and development[C]// Advanced Information Networking and Applications, 2003 IEEE. AINA 2003. 17th International Conference on, Xi'an, CHINA: [s.n.], 2003: 710 - 715.

[7] Li Jun, Manikopoulos C. Early statistical anomaly intrusion detection of DOS attacks using MIB traffic parameters[C]// Information Assurance Workshop, 2003. [s.l.]: IEEE Systems, Man and Cybernetics Society, 2003: 53 - 59.

[8] 邹柏贤. 一种网络异常实时检测方法[J]. 计算机学报,2003,26(8):940 - 947.

[9] Zhang Zheng, Manikopoulos C N. Detecting denial - of - service attacks through feature cross - correlation[C]// Advances in Wired and Wireless Communication, 2004 IEEE/Sarnoff Symposium on. [s.l.]: [s.n.], 2004: 67 - 70.

(上接第 152 页)

社,1994.

[4] Howard, Blanc L. Writing Secure Code[M]. 程永敬译. 北京:机械工业出版社,2002.

[5] 焦占亚. 一次一密的密码算法研究[J]. 西安科技大学学报,2005(4):477 - 480.

[6] 卢开澄. 计算机密码学[M]. 北京:清华大学出版社,1998:73 - 75.