自适应滤波实时网络流量异常检测方法

颜若愚[1,2]，郑庆华[1]，牛国林[1]
(1.西安交通大学电子与信息工程学院，710049，西安；2.广东海洋大学信息学院，524088，广东湛江)

摘要：针对网络中的各种常见攻击，提出一种基于自适应滤波的网络流量异常检测方法.首先对多种流量指标进行递推最小二乘法预测，然后以预测误差所构造的统计量容许范围进行异常检测，最后对检测结果实施归一化评估.该方法具有无需任何历史训练数据、能大量减少报警次数、突出报警严重程度的特点.在DARPA入侵检测评估数据集上的实验表明，所提方法更适合检测拒绝服务攻击引起的异常，较之相同权向量下的同类方法，其异常检测率、误报率和检测速度等性能更好.

关键词：网络流量；递归最小二乘法；拒绝服务攻击；异常检测
中图分类号：TP393 **文献标志码**：A **文章编号**：0253-987X(2009)12-0001-05

On-Line Anomaly Detection Method for Network Traffic Based on Adaptive Filtering

YAN Ruoyu[1,2], ZHENG Qinghua[1], NIU Guolin[1]
(1. School of Electronics and Information Engineering, Xi′an Jiaotong University, Xi′an 710049, China; 2. School of Information Science, Guangdong Ocean University, Zhanjiang, Guangdong 524088, China)

Abstract: A network traffic anomaly detection method based on adaptive filter is proposed to detect all kinds of network traffic attacks. Multiple network traffic indicators are predicted by recursive least square and the allowable statistical range based on the prediction errors are used to detect anomaly. Detection results are finally normalized. The method has the following traits: no training from any historical data, reducing the number of alarms, remarkably, and highlighting the severity of alarms. Testing results on DARPA intrusion detection data sets show that the proposed method is more suitable to detect denial of service attacks, and has a higher detection rate, faster speed and lower alarm rate than similar existing methods with same dimension of weight vectors.

Keywords: network traffic; recursive least square; denial of service attack; anomaly detection

网络规模的日益扩大、系统漏洞的不断被发现以及用户业务需求的逐步提高等因素，都增加了当前网络管理的难度.在尽量不妨碍用户正常应用的前提下，如何对网络流量进行实时监测和管理，及时发现网络流量异常并报警，对提高网络的可靠性和可用性具有重要意义.

网络安全中基于流量的异常检测方法主要有基于特征的异常检测[1]和基于统计的异常检测[2].这两类异常检测方法普遍存在一个共同问题，即事先需要获取一段时间的正常(异常)流量，时间少则1天，多则数月，然后对采集到的历史流量进行模式训练、正常(异常)行为的刻画或方差分析等预处理，因此实时性往往要受到前期数据收集工作的限制，而且这种收集工作是一个持续的过程，对用户的正常应用也会造成一定影响.

目前有许多经典的线性预测模型用于流量预

收稿日期：2009-03-17. 作者简介：颜若愚(1974—)，男，博士生；郑庆华(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60633020，60473136)；国家高技术研究发展计划资助项目(2006BAH02A24-2，2006BAK11B02，2007AA01Z475，2008AA01Z415).

测,而基于这些流量预测算法的统计检测方法一般需先对原始流量进行预测处理,在得到某个间接统计量后再进行异常检测,如利用 AR 模型结合滑动时间窗进行检测[2],利用 ARMA 或 ARIMA 模型进行流量的预测检测建模[3-4]等. 文献[2]主要针对网络设备故障引起的流量异常进行预测检测,文献[3]针对传感器网络中的拒绝服务(DoS)攻击进行预测检测,文献[4]对仿真的网络流量进行异常检测,但这些方法都存在预测窗口过大、预测精度低和时效性差等问题.

本文采用递归最小二乘(RLS)自适应滤波算法对网络中多个实时流量指标进行预测检测,并综合检测结果,结合报警简化方法对流量的总体态势进行归一化评估.

1 基于 RLS 的流量异常检测模型及方法

基于 RLS 的流量预测检测模型如图 1 所示. 流量采集程序采集某个网段中的实时流量,并根据需要按一定时间间隔进行统计分析,得到 4 种协议流量指标. 对这 4 种流量指标的预测检测及结果归一化评估是该模型的重点.

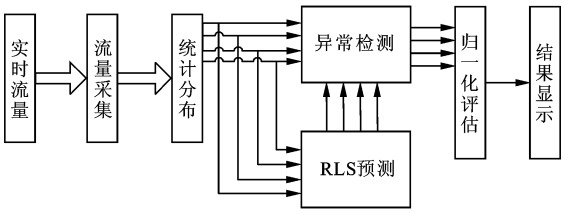


图 1 基于 RLS 预测的流量异常检测模型

1.1 RLS 流量预测算法

RLS 算法目前主要用于信号过滤除噪,但也可应用于信号的预测. 在网络流量预测中,随着预测步数的增加,预测性能下降很快,因此本文只对流量进行一步预测.

设 RLS 滤波器在 $n(n=1,2,\cdots,k)$ 时刻的权向量表示为 $\boldsymbol{W}(n)=[w_0(n),w_1(n),\cdots,w_{N-1}(n)]^{\mathrm{T}}$,将 n 时刻之前(包括 n 时刻)的 N 个数据即流量指标原始值构成的信号向量表示为

$$\boldsymbol{X}_N(n)=[x(n),x(n-1),\cdots,x(n-N+1)]^{\mathrm{T}}$$

则 $\boldsymbol{X}_N^{\mathrm{T}}(n)\boldsymbol{W}(n)$ 表示 RLS 滤波器在 n 时刻对 $n+1$ 时刻原始值 $x(n+1)$ 的预测. N 值越大说明滤波器利用的历史信息越多,处理的结果在拟合意义上越逼近纯净信号,但增大 N 值无疑会加大运算量,本文实验中将滤波器权向量的维数固定为 $N=2$. 权向量初始值可取为较小的数值,比如 0,滤波器在随后的迭代计算过程中会对它不断进行修正更新.

RLS 算法用于预测的计算步骤归纳如下.

(1)初始化

$$\boldsymbol{W}(0)=\boldsymbol{X}_N(0)=0$$

$$\boldsymbol{T}(0)=\delta\boldsymbol{I}$$

式中:δ 为自相关逆阵的初值系数,$\delta\gg1$.

(2)循环迭代. ①读取输入值 $x(n)$,$\boldsymbol{X}_N(n)$;②计算原始值和预测值之间的估计误差 $\xi(n|n-1)=x(n)-\boldsymbol{X}_N^{\mathrm{T}}(n-1)\boldsymbol{W}(n-1)$;③计算增益向量 $\boldsymbol{g}(n)=\dfrac{\boldsymbol{T}(n-1)X_N(n)}{\lambda+\boldsymbol{X}_N^{\mathrm{T}}(n)\boldsymbol{T}(n-1)\boldsymbol{X}_N(n)}$;④计算权向量 $\boldsymbol{W}(n)=\boldsymbol{W}(n-1)+\boldsymbol{g}(n)\xi(n|n-1)$;⑤计算 n 时刻样值的自相关逆阵 $\boldsymbol{T}(n)=\dfrac{1}{\lambda}[\boldsymbol{T}(n-1)-\boldsymbol{g}(n)\boldsymbol{X}_N^{\mathrm{T}}(n)\boldsymbol{T}(n-1)]$,其中 λ 为遗忘因子.

自相关逆阵的初始值对计算结果影响很小,可以取单位矩阵. 遗忘因子 λ 对参数估计的收敛速度影响较大,遗忘因子小则收敛振荡较小,但识别延迟会比较大,遗忘因子较大则可以加快收敛,但会引起剧烈的振荡. 在实际应用中 λ 的值一般取为 0.99.

1.2 基于预测的流量异常检测

在本预测检测系统中,使用 σ^2 表示 n 时刻以前 M 个原始值和预测值之间的估计误差的平方和均值,即 $\sigma^2=\sum\xi^2(n\mid n-1)/M$,使用检测统计量 τ 表示 n 时刻估计误差与 σ 的比值,即当 $\sigma>0$ 时,$\tau=\xi(n+1|n)/\sigma$,否则 $\tau=0$. 对于某种流量指标,其观测值序列设为 $S_1,S_2,\cdots,S_m$,用 $\{\tau_i\}$ 表示由该序列计算得到的统计量 τ 的序列,$\{\tau_i^+\}$ 表示 $\{\tau_i\}$ 中正值组成的序列,$\{\tau_i^-\}$ 表示 $\{\tau_i\}$ 中负值组成的序列. 根据序列 $\{\tau_i^+\}$ 和 $\{\tau_i^-\}$ 可分别计算 τ 的正负值统计量的平均值 $\overline{\tau^+}$、$\overline{\tau^-}$ 及相应的标准差 σ^+、σ^-. 由此得到该流量指标的统计量 τ 的容许范围 $(\overline{\tau^-}-p\sigma^-,\overline{\tau^+}+p\sigma^+)$,这里 p 取较小的正常数. 进行异常检测时,若当前 τ 值超出容许范围,则表示异常(为 1),否则表示正常(为 0).

1.3 归一化异常评估方法

虽然当前局域网络遭受攻击的形式多样、手段各异,但这些攻击都是针对传输层的 UDP、TCP 协议,或链路层的 ARP 协议等,因此将这 3 个协议的

基本流量作为评估的观测点，总的流量也作为一个评估的观测点，所选定的指标集合为{总数据包数，TCP 数据包数，UDP 数据包数，ARP 数据包数}. 采用加权求和的方法得到多个流量指标的综合异常度

$$F_{\text{traffic}}=\sum_{i=1}^{4}w(i)F_{\text{obs}}(i)\quad\sum_{i=1}^{4}w(i)=1\quad(5)$$

式中：$w(i)$为指标集合的相对权重，参考网络流量在不同协议中的分布情况，将权重的初始向量设为 $\boldsymbol{w}=[0.3,0.3,0.2,0.2]$；$F_{\text{obs}}(i)$为对指标集合进行检测得到的异常度值(用 0，1 表示). 综合异常度 F_{traffic}是判断流量是否正常的最终指标，往往以超出阈值的方式给予报警.

实验显示，使用归一化方法比仅使用总流量进行检测得到的报警数要少，检测性能有所提高. 考虑到某种流量发生异常时可能不足以引起总流量发生异常，反映到流量综合异常度上往往会出现漏报. 本文针对连续发生异常的流量指标的权值进行修正来减少漏报，即每次权值增加 0.1，直到后面该指标又出现正常时将权值恢复到初始值. 对报警状况的进一步分析表明，归一化后得到的报警有相当一部分是连续 2 个以上的报警，因此可以对报警做进一步的简化，即只对连续时间警报的第一个进行报警，后续的警报只对第一个异常度初始值进行修正，每次修正增加一个常数值 0.1，当异常度增加到 1 时便截止. 经过这样处理后不但再次减少了报警数，而且也能够突出报警的重要程度.

2　实验和结果分析

本文主要针对 DoS/DDoS 攻击进行下面的实验，由于绝大部分 DoS/DDoS 攻击持续时间为 1～30 min[5]，因此实验中只将持续时间 30 s 以上的攻击纳入检测范围.

2.1　DARPA 评估实验数据集上的检测和分析

实验以 1999 年 DARPA 入侵检测评估实验数据集[6]为测试数据，所选用的 4 月份中 5 天的测试样本见表 1. 由于几乎所有的攻击都发生在早上 8：00 到晚上 21：00 这段时间，所以只需要从这段时间的流量中提取所需的统计量，流量统计的时间间隔为 5 s.

选取模型参数值 $p=6$，对表 1 中的数据集进行异常检测的结果见表 2 和表 3. 结果显示，本文模型针对大于 30 s 的 DoS 攻击和所有异常攻击的检测率分别达到 78.3%和 68.9%，而误检率和报警频率都非常低. 显然本文方法对 DoS 攻击的检测效果更理想，这主要是因为 DoS 攻击往往比其他攻击更容易引起流量的变化. 对于那些没能检测到的攻击，其漏检的主要原因一个是攻击的强度比较弱，另一个是攻击的持续时间较短.

表 1　5 天测试样本数据

编号	星期	数据描述	开始时间	结束时间
1	Thursday	Testing Data	1 日 08：00：01	2 日 05：59：49
2	Friday	Testing Data	2 日 08：00：00	3 日 05：59：53
3	Monday	Testing Data	5 日 08：00：02	6 日 05：59：56
4	Tuesday	Testing Data	6 日 08：00：00	7 日 05：59：58
5	Wednesday	Testing Data	7 日 08：00：00	8 日 05：59：52

表 2　DoS 攻击检测结果统计

编号	DoS 攻击数	报警总数	检测到的攻击数	检测率	误检率	报警频率/次·h^{-1}
1	3	90	2	0.667	0.009 4	6.92
2	2	96	2	1.000	0.010 0	7.38
3	9	92	7	0.778	0.009 1	7.08
4	5	94	4	0.800	0.009 6	7.23
5	4	110	3	0.750	0.011 4	8.46
总计	23	482	18	0.783	0.009 9	7.42

表 3　所有攻击检测结果统计

编号	DoS 攻击数	报警总数	检测到的攻击数	检测率	误检率	报警频率/次·h^{-1}
1	12	90	9	0.667	0.008 7	6.92
2	15	96	11	0.733	0.009 1	7.38
3	17	92	9	0.471	0.008 9	7.08
4	16	94	12	0.688	0.008 8	7.23
5	14	110	10	0.643	0.010 7	8.46
总计	74	482	51	0.689	0.009 2	7.42

为了验证模型中报警简化方法的有效性，表 4 列出了本实验中得到的总流量指标报警数、4 种流量归一化后报警数以及最终简化后报警数的比较结果. 经过 2 次报警简化后，报警频率平均降低了近 40%，表明这种简化方法非常有效.

表 4　报警简化前后结果的比较

编号	报警总数	归一化后		最终简化报警后	
		报警数	简化率	报警数	简化率
1	147	126	0.143	90	0.388
2	149	130	0.128	96	0.356
3	150	127	0.153	92	0.387
4	153	129	0.157	94	0.386
5	161	147	0.087	110	0.317
总计	760	659	0.133	482	0.366

2.2 与文献[2]方法的比较分析

文献[2]使用了方差分析法消除流量的周期性，但这样做的缺点是前期需要采集数周的流量做方差分析，在检测的时候又要对待检测流量做预处理，而且长期(如1个月甚至数月)不间断地采集历史数据往往会因受到多种因素影响而无法实现，使得该方法难以推广到实际应用中.

对比实验使用文献[2]中提到的AR模型加单窗法进行流量预测，前期使用1999年DARPA数据集中的3周训练数据进行方差分析，该方法仅对总流量进行异常检测，其他的实验步骤都按照本文中的模型进行，2种方法的预测模型中权向量维数 N 都为2，求 σ^2 的时间窗长度 M 都为20. 为了直观比较2种方法的实验结果，这里以不同的 p 值进行检测，并将结果绘成图2中的接受者操作特性(ROC)曲线，作为方法评估标准. 从图2中可以看出：本文方法在相同误检率下的检测率要明显高于对比方法；在0～5%的误检率范围内，本文方法的检测率为比较方法的1.14倍左右；在0～2.5%的误检率范围内，本文方法对DoS攻击的检测率为对本实验中所有攻击的检测率的1.14倍左右. 当误检率高于5%以后，2种方法在检测率上越来越接近，最后都在误检率7%左右达到完全检测异常，这主要是随着容许范围越来越小，2种方法检测到异常的能力越来越接近.

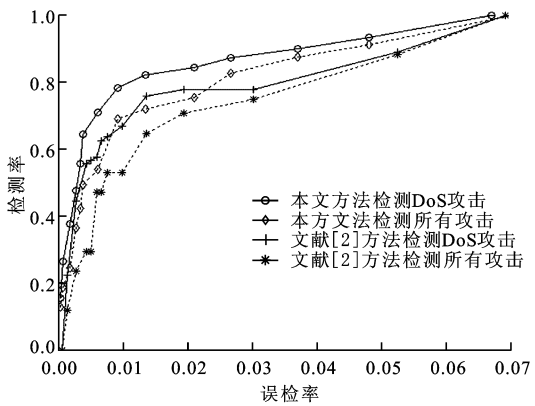


图2 2种方法的ROC曲线比较

以相加(减)和相乘(除)次数作为判断计算速度的依据，在权向量维数都为2、时间窗大小 M 都为20时，使用AR模型进行预测约需要加减运算74次，乘除运算88次，而使用RLS进行预测约需要加减运算18次，乘除运算28次，可见RLS模型的预测速度是AR模型的3倍多. 另外，从算法的空间效率来看，虽然RLS预测计算的中间变量比AR模型多一些，但这些变量都是长度为2的向量或大小为2×2的矩阵，而AR模型每次都需要利用 $M=20$ 个历史数据来拟合权向量，至少需要保存一个长度为20的向量和一个大小为20×2的矩阵，而且随着滑动窗口长度 M 的增大存储开销越大，因此RLS所需内存空间要远少于AR模型所需内存空间.

2.3 与文献[3]方法的比较分析

为了验证该检测方案检测现实网络流量的性能，利用Ethereal软件采集了实验网络中1周(2008年4月21日～27日)的实际流量，并提取了所需的4种统计流量. 本实验只针对对流量有较大影响的DoS/DDoS攻击进行标定和检测，标定方法为：首先使用EWMA(exponential weighted moving average)控制图理论寻找超出规定阈值的流量所在时间段，然后分析这些时间段的原始网络流量，以确认是否存在这样的攻击，最后确定每次攻击的真实时间范围. 采用这种标定方式对所采集的1周流量进行检查共找到13个有效的DoS/DDoS攻击，这些攻击的持续时间都在0～40 min以内，属于TCP流量类型的攻击约占60%.

使用仿真流量作为检测数据是深入比较检测方法的重要部分. 仿真异常流量的步骤在文献[7]中有很详细的描述，这里以1周真实流量为基础流量，模拟DoS/DDoS攻击生成异常流量的描述参数及其取值范围如表5所示(表5中相关参数的具体说明可参考文献[7]). 在仿真过程中，针对不同的 δ 值分别生成具有随机起始时间和持续时间的100次DoS/DDoS攻击，这些攻击都随机分布在3种流量(TCP、UDP、ARP数据包流量)中，而总的数据包流量最后由3种人工流量叠加合成.

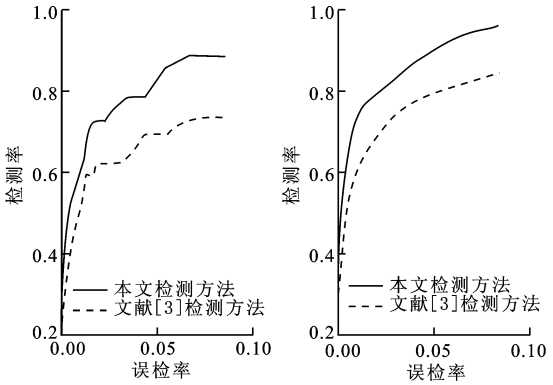
文献[3]采用ARMA(2,1)模型对传感器网络中的流量进行一步预测，预测误差 d_i 为时刻 t 的真实流量 X_i 与预测流量 $\hat{X}_i$ 的绝对差值 $d_i=|X_i-\hat{X}_i|$，当 $d_i-\varepsilon>T$ 时，即认为流量发生流量发生异常，其中 ε 为均方预测误差，T 为设定的检测阈值.

采用2种方法分别以不同的 p 或 T 作为阈值对实际流量中标定的DoS/DDoS攻击以及仿真流量进行检测，得到对比结果如图3和图4所示. 图3表明，在相同的误检率下，本文方法的检测率比文献[3]方法提高了10%以上，而且随着误检率的增加，本文方法的检测比文献[3]方法提高更快. 图4表

明：当攻击强度弱到一定程度时，2 种方法都很难检测到异常，但随着攻击强度的增强，本文方法的检测率比文献[3]方法提高更快，2 种方法在相同攻击强度下的误检率都较低，但本方法的误检率比文献[3]方法更低. 因此，总的看来，本文方法在以上各检测性能指标上都要优于文献[3]方法，其主要原因是本文方法采用了更好的检测统计量和报警简化机制.

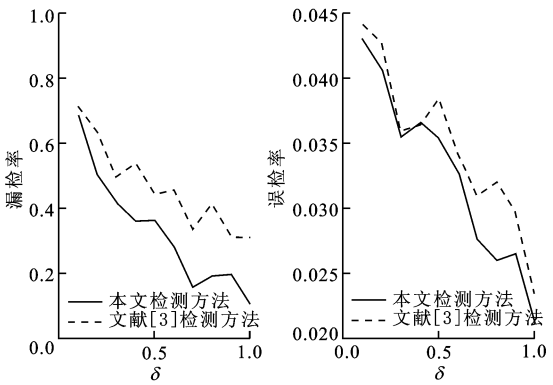
表 5　DoS/DDoS 攻击描述参数及其取值范围

持续时间/min	攻击强度	模拟函数
0.5～30	0.1≤δ≤1	Ramp Exponential



(a)真实流量　　(b)仿真流量

图 3　真实流量和仿真流量下得到的 ROC 曲线



(a)漏检率　　(b)误检率

图 4　漏检率和误检率趋势对比

3　结论和展望

本文将 RLS 流量预测方法应用到网络流量的异常检测中，实现了对 4 种流量指标的实时预测检测，并对流量总体异常态势进行了评估. 实验表明，本文方法在检测 DoS/DDoS 攻击时，在相同权向量下具有较好的总体检测效果、更快的检测速度和更小的存储开销.

本文的检测模型可以部署到多个局域网中进行分布式流量检测，从而可对不同网络中的报警进行关联分析，或配合基于特征的入侵检测系统，形成对网络流量的多方位立体监控.

参考文献：

[1] 姚婷婷，郑庆华，管晓宏，等. 一种基于主机实时流量的安全评估方法[J]. 西安交通大学学报，2006，40(4)：415-419.
YAO Tingting，ZHENG Qinghua，GUAN Xiaohong，et al. Security evaluation method based on real time traffic of hosts [J]. Journal of Xi′an Jiaotong University，2006，40(4)：415-419.

[2] 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.
ZOU Boxian. A real-time detection method for network traffic anomalies [J]. Chinese Journal of Computers，2003，26(8)：940-947.

[3] 曹晓梅，韩志杰，陈贵海. 基于流量预测的传感器网络拒绝服务攻击检测方案[J]. 计算机学报，2007，30(10)：1798-1805.
CAO Xiaomei，HAN Zhijie，CHEN Guihai. DoS attack detection scheme for sensor networks based on traffic prediction [J]. Chinese Journal of Computers，2007，30(10)：1798-1805.

[4] ZARE M H，MASNADI-SHIRAZI M A. Arima model for network traffic prediction and anomaly detection [C]// Proceedings of ITSim International Symposium on Information Technology. Piscataway，NJ，USA：IEEE，2008：1-6.

[5] VOELKER M D，SAVAGE S G M. Inferring internet denial-of-service activity [C]// Proceeding of the 10th USENIX Security Symposium. Berkeley，CA，USA：The Advanced Computing Systems Association，2001：9-22.

[6] Massachusetts Institute of Technology. Lincoln. Laboratory. DARPA intrusion detection evaluation[EB/OL]. (2008-06-01)[2009-03-02]. http：// www. ll. mit. edu/IST/ideval/data/data_index. html.

[7] AUGUSTIN S，KAVE S，NINA T. Combining filtering and statistical methods for anomaly detection [C]// Prceedings of USENIX Association Internet Measurement Conference. Berkeley，CA，USA：The Advanced Computing Systems Association，2005：331-344.

（编辑　刘杨　苗凌）