基于统计方法的骨干网异常流量建模与预警方法研究*)

顾荣杰[1] 晏蒲柳[1] 邹 涛[2]

(武汉大学电子信息学院 武汉 430072)[1] (北京系统工程研究所 北京 100101)[2]

摘 要 近几年来,Internet上频繁发生的蠕虫爆发和大规模分布式拒绝服务事件使网络服务的安全性面临严重的威胁。本文介绍了一个基于异常流量检测的Internet骨干网流量早期预警系统ESTAB(Early-warning System of Traffic Anomaly Based)。它基于Internet骨干网异常流量发现原理,通过对端口、长度分布、TCP标志等直接变量(Direct Variable)的监测,并结合统计学中的时间序列分析方法,实时分析发现流量异常,并提出告警。文中提出了多种事件联合监测的概念,从流量监测角度有效地对付已知流量威胁(如已知蠕虫),并对未知流量威胁提供了相应的监测策略。

关键词 流量异常检测,Internet骨干网,时间序列分析,预测,预警,滑动时间窗

The Backbone Network Traffic Modeling and Anomalous Forecasting Approach Research Based on Statistic Method

GU Rong-Jie YAN Pu-Liu ZOU Tao[2]

(School of Electronic Information, Wuhan University, Wuhan 430072)[1] (Beijing Institute of System Engineering, Beijing 100101)[2]

Abstract Worm and Dos, DDos attacks take frequently place more and more nowadays. It makes the internet security facing serious threat. This paper introduced the algorithm and design of ESTABD, an internet backbone Early-Bird System of Traffic Anomaly Detection Based. ESTABD analyzes real-time traffic to discover the abrupt traffic anomalous and generate warnings. A traffic anomaly detection algorithm based on Statistic Prediction theory is put forward and the algorithm has been tested on real network data. Further more, Alerts correlation algorithm and system policy are addressed in this paper to detect the known worms& Dos attacks and potentially unknown threats.

Keywords Traffic anomaly detection, Internet backbone, Forecasting, Time serial analysis, Early-warning, Slip window

1 研究背景

随着网络计算和电子商务应用的不断发展,Internet已经渗透到现代社会的每一个角落。日益增大的网络规模给现代网络管理增加了巨大的难度和复杂性。尤其是近几年来,频繁的蠕虫爆发事件给互联网的整体安全带来了巨大的威胁,导致区域以至全球的网络陷于瘫痪。2001年7月,Code-Red蠕虫在不到9h时间里,感染了250,000台计算机,直接经济损失26亿美元;2003年1月,SQL Slammer蠕虫在爆发的前5min里就导致了9.5至12亿美元的损失,与Code-Red蠕虫每37min翻一番的扩散速度相比,它只需8.5s[1,2]。蠕虫由于其攻击目的贪婪性决定了多数蠕虫以快速扫描方式进行传播[3],伴随产生巨大的网络流量,导致大量依赖于网络的服务受到严重影响,如ATM终端无法提款、航班因网络通信受阻无法起飞[4~6]。包括蠕虫在内,网络中发生的拒绝服务攻击、分布式拒绝服务攻击以及因不适当的网络配置所引起的流量拥塞也严重影响了网络的正常运行。

由于互联网处在不间断的运行当中,异常的发生时间没有一定规律,要求监测的工作人员24h在线观察和干预是不现实的,由此自动发现并告警成为系统设计的首要要求。第二,由于近几年来,蠕虫爆发的规模越来越大,速度越来越快,在其繁殖扩散的早期发现并启动相应紧急措施以扼制其进一步扩散成为该系统的潜在需要。第三,系统要求能全天候在线实时监测,检测算法的处理过程要求迅速以符合实时性要求,完成检测过程耗时应少于1min。第四,系统能检测未知异常,并对已知流量事件进行监控。所谓流量事件,此处定义为在流量上有明显特征的异常事件,包括蠕虫或者DDOS。

在Internet骨干网上进行流量预警,有以下一些特点:

·能使监控工作着眼宏观,监控大范围网络整体的动态变化,为监测蠕虫等大规模威胁Internet安全的事件提供一个全景式的观测平台。

·骨干网上用户(主机)数量巨大。据统计,美国目前拥有Internet用户1.56亿人,而中国的这一数字为8,700万人。由于拥有丰富的样本,突发的个体行为(比如通过网络下载Gigabytes的电影)不会造成流量的大起大伏,骨干网络的各项整体指标分布呈现出较强的统计学意义。这一特性(feature)为本文利用统计学对网络流量进行分析提供了充分的理论基础。

·骨干网的瞬时流量巨大(Gigabytes/sec量级),要求检测系统必须满足高速实时要求,检测算法要尽可能简单,以免加重系统负担。另一方面,由于骨干网上的流量太大,在实用系统中不可能提取并存储所有信息,因此细节信息的获取需要消耗较大的资源。

*)国家自然科学基金项目(90204008)。顾荣杰 博士研究生,主要研究方向:计算机网络通信、智能网络管理、骨干网络安全等;晏蒲柳 博士,教授,博士生导师,长期从事计算机网络通信、网络管理等方面的研究。

流量异常检测预警系统作为 Internet 网络安全监测的前端部分，为后续安全模块的运行提供预警和跟踪依据，为整体网络的安全提供决策信息。

2 相关工作

在 Internet 异常流量检测和蠕虫的检测研究方面，许多人已经从理论和应用角度做出了自己的贡献。P. Barford [7] 等人将信号分析理论——小波分析方法运用于流量异常检测，并给出了基于其理论的 4 类异常结果，但该方法晦涩复杂，不适合在高速骨干网上进行实时检测。A. Lakhina 等人 [8] 研究了网络流量的特性后认为，同时对网络通信中的所有连接进行建模是不恰当的，他们利用主成分分析方法（PCA）分析了源和目标之间 OD 数据流，并将 OD 数据流的高维结构空间分解到 3 个主成分上，以 3 个新的复合变量来重构网络流的特征，并以此发展出一套检测方法。PCA 方法要求用于学习过程的数据集具有足够的代表性和覆盖度，但在真实的网络环境中却很难实现这一要求，通常需要记录足够大量的数据进行训练也不一定能达到这一要求。随着硬件技术的发展，目前千兆 IDS 甚至万兆 IDS 的使用，使得在 Internet 骨干网上监测已知蠕虫成为可能。因为一般蠕虫除非发生变种，其病毒体是可以找到特征代码的，从而可以将这一特征串定义为特征，并利用高速字符串匹配算法从巨大的骨干网数据流中匹配这一特征进行监测。但它们也存在着不足，主要表现在：a)高误报率(False Positive)；b)对出现的新攻击无能为力，其能力过分依赖于规则库，无法自主学习。有部分学者(Madhusudan 等人 [9])试图弥补这些不足，他们提出频繁字符串特征自动提取方法，以取得未知蠕虫的特征。但这必然会影响系统的效率和性能，同时无法验证这些特征的有效性。

本文描述了一个基于异常流量检测的 Internet 骨干网流量早期预警系统 ESTAB(Early-warning System of Traffic Anomaly Based)的原理和结构设计。它基于 Internet 骨干网异常流量发现原理，通过对端口、长度分布、TCP 标志等直接变量(Direct Variable)的监测，并结合统计学中的时间序列分析方法，实现分析发现流量异常，并提出告警。文中提出了多种事件联合监测的概念，从流量监测角度有效对付已知流量威胁(如已知蠕虫)，并对未知流量威胁提供了相应的监测策略。

3 系统设计与算法实现

3.1 ESTAB 系统架构设计

ESTAB 是一个多层分布式体系结构，它的主体结构如图 1。

ESTAB 构建于一个分布式的数据采集平台之上，该平台由许多分布在各监测子网的数据引擎(Data Engine)构成，这些引擎根据控制中心(Console)下发的策略有选择性地进行数据的采集。这部分工作分两部分：a)对原始数据流进行协议；b)在协议分析基础之上提取原始变量。Data Engine 采集的流量数据有几种：1)根据协议归类的流量数据(按端口分类)；2)按数据包特征信息统计的流量数据，如 SYS/FIN 以及包长度等 TCP 标志，这些量值在一定程度上反映流量变化的特征)。流量引擎对一个采样时间间隔之内流过监测网端的流量数目进行累计，得到该采样时间点的变量数值。各引擎采集到的流量，经过数据传输通道，被传送到数据汇总中心(Data Center)，并按照时间顺序形成不同的原始时间序列向量。

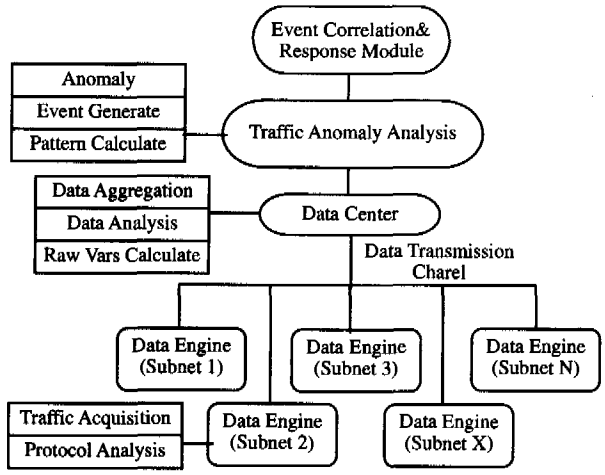

图 1 ESTAB 的系统设计图

3.2 原始变量提取

数据引擎对流经的数据流进行协议分析后提取相关的变量，并在引擎的统计时间间隔内对到来的数据包进行关于符合该变量的数据包的数量统计，本文定义该数值为原始变量。这些变量的变化灵敏地或者相对灵敏地表征网络状态的变化。

目前定义的变量有：

- 端口协议统计流量。在一定时间范围内对所监控的每种协议对应端口的流量按包数或字节数进行统计；
- 包长度统计变量。本文对包长度按区间进行划分并监控，因为蠕虫的内容长度一般是一定的，比如 SQL Slammer 使用等长的单包进行扩散，该变量可以用于监视突增的某种长度的蠕虫数据包；
- SYN 统计变量。TCP 握手发起事件；
- ACK 统计变量。TCP 握手响应事件；
- ICMP 不可到达事件数变量。Ping 命令的目标如果不存在就会产生该事件。

需要指出的是，这部分的定义是可扩充的。

3.3 异常流量检测算法描述——周期性业务流量与非周期性业务流量

根据 3.1 节，原始数据从数据引擎采集上来之后，按原始变量形成各种（time，count-value）一维时间数据序列。流量异常检测模块对这些时间序列进行异常分析。

根据前文的分析，骨干网上的流量监测具有样本容量大的特点，因此个体的突发活动不会影响整体流量的变化趋势，在骨干网进行监测得到变量序列，在时间上是先后相关的。历史流量数据反映着未来的趋势。正常情况下，序列不会发生跳变。根据我们在某骨干网上连续 15 个月的监测经验，发现所有流量在正常状态下都是平稳变化的，并且可以划分为两大类：非周期性业务流量和周期性业务流量(如图 2)。

非周期性流量在所有监测对象中是最常见的，多数流量属于这种情况。在正常情况下(无异常发生时)，一段时间内的非周期性流量呈现平稳的变化(如图 2(a))。

某些流量呈现周期性的原因是一些经常使用的服务，比如 web，smtp，ftp，它们与人们日常生活紧密相关，其应用的频度受人们的生活作息规律影响而呈现(present)规律性变化，周期一般是 24h。在正常情况下(无异常发生)，一段时间之内的流量呈现平稳(无显著趋势)且有周期性的变化(如图 2(b))。根据图 2(b)中近期的几个完整周期的数据，可以提

取一个周期内的流量变化曲线如图 2(c)，并把它定义为最近一段时间的周期模板。由于它是随着流量变化自动提取不断变化的，可以称之为动态模板。在应用中，可以将实际到来的流量数据与模板曲线中相应的数值进行比较。如果偏差超过一定阈值，则认为异常。这个阈值的产生和异常的判断由下面的算法完成。异常检测算法对周期性和非周期性流量采用不同的检测方式。

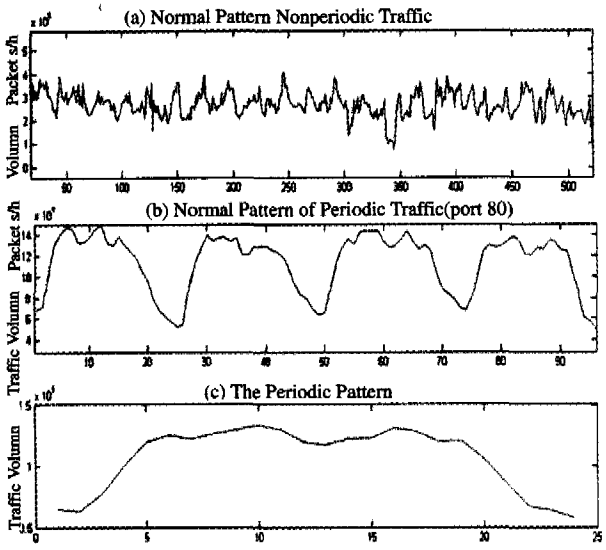

图 2　周期性与非周期性流量

1)非周期性业务流量采用指数平滑预测方法，它从移动加权平均方法[10]发展而来，是经济学上常用的一种用于时间序列的预测方法。其特点是简单并且动态赋予历史上所有的观测点不同权值：离当前越近的点权值越大，反之越小。

设流量序列为 $x_1, x_2, \cdots, x_n$，指数平滑方法的一般公式为：

$$S_{n+1}=\alpha x_n+(1-\alpha)S_n \tag{3.1}$$

S_n 是 n 时刻的指数平滑值，α 是平滑常数。基于指数平滑方法的预测是将第 $n+1$ 时刻的平滑值作为当期的预测值，即

$$\hat{x}_{n+1}=S_{n+1}=\alpha x_n+(1-\alpha)S_n=\alpha x_n+(1-\alpha)\hat{x}_n \tag{3.2}$$

其中 $\hat{x}_n$ 是 n 时刻的预测值。

误差计算：均方误差

$$\text{MSE}=\frac{\sum_{t=1}^{n}e_t^2}{n}=\frac{\sum_{t=1}^{n}[x_t-\hat{x}_t]^2}{n}$$

或

$$\text{绝对误差 MAE}=\frac{\sum_{t=1}^{n}|x_t-s_{t-1}|}{n} \tag{3.3}$$

在这个模型的应用中，α 的选择对平滑和预测的结果有较大影响：α 取值越大，则各观测值的加权衰减越快，越近的数据对预测的贡献越大。当 $\alpha=1$ 时，$\hat{x}_{n+1}=x_n$，在平滑中起作用的观察数据越少。理论上，α 的选择应该满足：

$$\alpha=\{\alpha|\min(\text{MSE})\}=\{\alpha|\min(\frac{\sum_{t=1}^{n}[x_t-\hat{x}_t]^2}{n})\} \tag{3.4}$$

但有实验表明，$\alpha=0.2$ 时，无论 MSE 和 MAE 都能取到最小值，故可以将 0.2 作为首选值。接下来，本文将根据预测值和 MSE 计算下一个观测值的正常可能范围(range)。为此，引入滑动时间窗(sliding window)的概念，滑动时间窗用来计算最近长度为 T 的序列中预测的偏差程度，为下一个预测点提供精确度描述。假设当前预测点为 $\hat{x}_{n+1}$，滑动时间窗的长度为 L，则时间窗覆盖的序列为：

$$\{x_{n-L-1}, x_{n-L-2}, \cdots, x_n\}$$

令 $\sigma_{n+1}=\sqrt{\text{MSE}}$，则

$$\sigma_{n+1}=\sqrt{\frac{\sum_{t=0}^{L-1}e_{n-t}^2}{L}}=\sqrt{\frac{\sum_{t=0}^{L-1}[x_{n-t}-\hat{x}_{n-t}]^2}{L}} \tag{3.5}$$

算法初始化时，令前两个预测值等于观测序列的前两个实际值，进入一个周期为 L 的预测初始化，之后开始异常检测。异常判断算法的伪代码如图 3 所示。

```
BEGIN: (1) x̂_1 ← x_1, m ← 1
       (2) WHILE (m<=L)
           DO {
                x̂_{m+1} ← αx_m + (1-α)x̂_m
                e_m ← (x̂_{m+1} - x_{m+1})
                m ← m+1}
       (3) n ← L+1
       (4) WHILE (TRUE)
           DO { S ← 0
                FOR m ← 1 TO L DO{
                S ← S + e_m^2 }
                σ_{n+1} = SQRT (S/L)
                x̂_{n+1} ← αx_n + (1-α)x̂_n
                delta ← Abs(x_{n+1} - x̂_{n+1})
                RISKLEVEL ← 0 (Normal)
IF delta > 8*σ_{n+1}
   THEN
        RISKLEVEL ← 1 (High)
ELSE IF (delta > 5*σ_{n+1})
   THEN
        RISKLEVEL ← 0.5(Middle)
ELSE IF (delta >3*σ_{n+1})
   THEN
        RISKLEVEL ← 0.2(Low)
IF(RISKLEVEL ≠ 0)
   THEN
        Call Alert-Generator (RISKLEVEL)
        x_{n+1} ← x̂_{n+1}
   n ← n+1}
END.
```

图 3　非周期模型计算伪代码

2)周期性业务流量。季节性水平乘法模型针对周期性业务流量的特点，可以认为在考察的若干个周期在正常流量条件下其单周期均值无明显变动趋势，主要受季节变动和不规则的变动影响而产生波动。根据此特点，本文采用时间序列分析中的季节性水平乘法模型。此方法的原理请参考相关资料，在此仅给出预测方程和使用方法。该模型将时间序列分解成 2 个指标：长期趋势 T 和季节因素 S。预测方程如下：

$$y_{t+\tau}=T_t * S_{t+\tau-L},(\tau=1,2,3,\cdots,L) \tag{3.6}$$

$$T_t=\alpha\frac{x_t}{S_{t-L}}+(1-\alpha)T_{t-1} \tag{3.7}$$

$$S_t=\gamma\frac{x_t}{T_t}+(1-\gamma)S_{t-L} \tag{3.8}$$

其中，τ：预测步长，T_t：由过去 $t-L$ 期预测的趋势值，S：季节指数，L：周期长度，α：趋势平滑指数（经验取 $0.05\leqslant\alpha\leqslant0.3$），$\gamma$：季节平滑常数(0.5～0.6)。

算法初始化时，根据第 1 周期的数据初始化 T 和 S：

$$T_L=\frac{1}{L}\sum_{i=1}^{L}x_i,(i=1,2,\cdots,L) \tag{3.9}$$

$$S_i=\frac{x_i}{T_L},(i=1,2,\cdots,L) \tag{3.10}$$

本文选择前5个周期数据进行学习，为进一步预测准备足够信息。预测误差评价方法同前面。初始化完成之后，每到来一个新周期的观测值，根据以下步骤计算：

1)根据过去的5个周期，计算预测的平均均方误差：

$$\sigma_i=\frac{\sum_{n-k-4}^{k-1}e_{nL+i}^2}{4}=\frac{\sum_{n-k-4}^{k-1}[x_{nL+i}-\hat{x}_{nL+i}]^2}{4},i=1,2,\cdots,L \tag{3.11}$$

2)计算当前观测值偏离预测值的程度：

$\delta_{nL+i}=|X_{nL+i}-\hat{x}_{nL+i}|$

如果 $\delta_{nL+i}<3\sigma_i$，直接转至下一步，否则进行判断：

- 若 $\delta_{nL+i}>8\sigma$，高风险，转入异常处理；
- 若 $\delta_{nL+i}>5\sigma$，中风险，转入异常处理；
- 若 $\delta_{nL+i}>3\sigma$，低风险，转入异常处理。

异常处理：将当前观测值用预测值取代：$x_{nL+i}\leftarrow\hat{x}_{nL+i}$，并上报控制中心。

3)如果新的一周期结束，根据方程(3.7)、(3.8)计算当前周期的趋势指数和季节指数。

3.4 异常事件联合监测与重点监测策略

一种蠕虫的传播，由于其传染扩散机理的不同，可能会影响到一个或多个关联的端口。CERT/CC近年来公布的蠕虫资料，见文[10]。

根据前述的方法，可以通过监测某个端口的流量变化来发现某种蠕虫的爆发。根据先验知识，如果在某预先设定的时间窗口内监测到某种端口组合的蠕合爆发，则可以直接定位一种已知的蠕虫。此外，快速随机蠕虫扫描会伴随大量的ICMP目标不可到达消息产生，通过监控这一事件也有助于骨干网上蠕虫的检测。与此类似，由于不少目标主机或者服务不存在，导致大量的SYN扫描事件与ACK响应消息数量之比急剧增大，该值(SYN/ACK比)对于实际检测亦有指导价值。

关于监测的端口问题，理论上存在65536种可能(分TCP与UDP则更多)，同时监测如此众多的端口对监测系统是一个很大的负担。考虑到蠕虫要大规模传播，必须依赖广泛存在的常用服务端口，因此只对常用服务进行监控，即可完成绝大多数情况的检测。

4 结果分析与验证

本文提出的算法和理论已经在实际的骨干网络上进行了测试并得到验证。所有的流量数据采自某国家级骨干网。以下是对取自某骨干网络出入口18天的21号端口的数据进行的异常分析(如图4A)。图4B是本文的预测分析过程，其中，虚线是预测结果的上边界，破折线(——)是预测值的下边界。经过分析检测，结果如图4C。事件被上报到控制中心，每个事件按其异常程度赋予一定风险级别(告警可以根据异常偏离程度、前后时序关系等多种因素进行相应的风险量化，此处不再进行方法介绍)。

图5是本文算法在某骨干网出入口上对Witty蠕虫爆发时的检测结果，时间为2004年3月13日至3月25日。可见，当蠕虫爆发时，流量的统计模式发生了重大的变化，算法及时检测到了变化并在第一时间提出了告警。

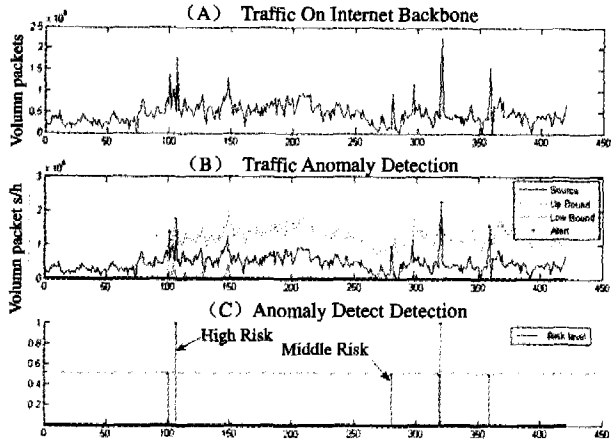

图4 某骨干网上非周期性异常流量检测实例

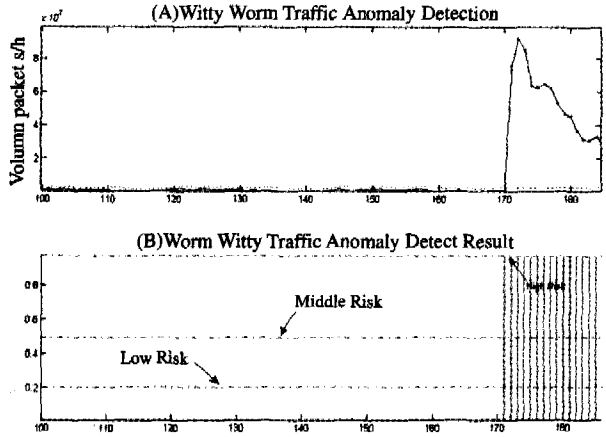

图5 Witty蠕虫爆发异常流量检测

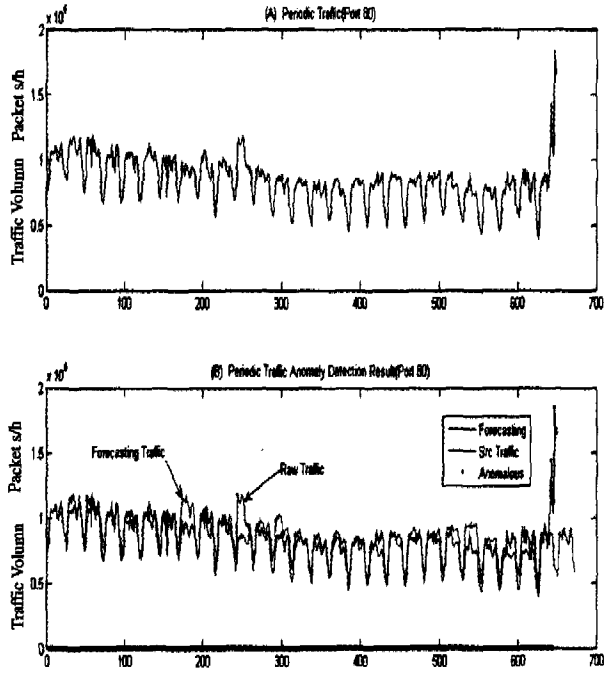

图6 某骨干网28天HTTP流量的异常检测

我们在骨干网上对某几个ISP的HTTP流量连续进行了几个月的跟踪，获取了发生异常前28天的流量(见图6)。可以看到，数据轮廓表现出显著的周期性特点，并且连续28天无明显的升降趋势发生。图6(B)显示了异常检测过程，其

中蓝色曲线代表原始流量，红色曲线代表预测值。蓝线上的红色粗圆点表示检测到的异常。其中异常程度即风险级别的定义如上文，图中没有标出异常点的风险级别。利用本文的算法，正如所期待的，检测到了流量异常。

总结与展望 本文介绍了一种基于异常流量检测方法的骨干网早期预警系统 ESTAB 算法和框架设计，详细论述了基于周期性和非周期性业务流量的异常检测方法，并用来自骨干网的真实数据进行了测试验证。结果进一步说明，该方法是可行的。今后的工作将继续对模型的适应性进行改进，以实现更精准的检测，并进一步完善系统的性能。

参 考 文 献

1 Moore D, Shannon, et al. Code-Red: a case study on the spread and victims of an Internet worm. IMW, 2002

2 Moore D, Paxson V, et al. The Spread of the Sapphire/Slammer Worm. CAIDA, ICSI, Silicon Defense, UC Berkeley EECS and UC San Diego CSE, 2003

3 Weaver N, Paxson V, Staniford S, et al. A Taxonomy of Computer Worms. In: Proc. ACM CCS Workshop on Rapid Malcode, 2003

4 http://www.cnn.com/2001/TECH/internet/10/31/new.nimda.idg/

5 http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/

6 Security firm: MyDoom worm fastest yet. http://edition.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed/index.html

7 Barford P, Kline J, Plonka D, et al. A signal analysis of network traffic anomalies. In: Internet Measurement Workshop, 2002

8 Madhusudan B, Lockwood J, et al. Design of a System for Real-Time Worm Detection. In: 12th Annual IEEE Symposium on High Performance Interconnects (Hot-I), Stanford, CA, 2004. 77～83

9 Lakhina A, Papagiannaki K, Crovella M, et al. Structural analysis of network traffic flows. Proc ACM SIGMETRICS, 2004

10 http://www.itl.nist.gov/div898/handbook/pmc/section4/pmc42.html

11 http://www.cert.org

（上接第 82 页）

以减少计算量，适合这里的需要。根据具体安全需求，选定门限值 k_1。如果有 k_1 个簇头节点对 CH_2 进行控告，则 CH_2 不再被信任，其簇内的节点也不再被信任。簇头 CH_2 内的普通节点需要重新离线注册或经其它簇头节点用辅助方法认证（旁路安全信道：红外线、视频、音频等），才能重新加入网络。

簇头节点安全性较高，为本簇内所有节点信任。簇成员节点因设备简单、保护措施差，易被俘获。对普通节点的信任关系由簇头节点控制。如果一个节点发现了其邻居节点有恶意行为，或是与其通信节点的恶意行为，则向簇头节点发出一个控告消息，并对该消息签密。

簇头节点维护一张恶意节点列表，表中每项包括的内容有：节点 ID、控告节点列表、行为状态。根据具体安全需求，选定另一门限值 k_2。如果恶意节点列表中节点 A 的控告列表少于 k_2 个合法的控告者，那么节点 A 被标记为可疑节点，行为状态标记为 0；否则，认为这个节点为恶意节点，不再信任此节点，行为状态标记为 1。如果有节点 A 受到 k_2 个合法节点的控告，簇头节点就在簇内广播一条签名的撤消节点 A 簇成员身份的消息，也需要向其它的簇头节点广播这一消息。消息格式如下：{节点 ID，恶意节点标记，签名}。节点 A 在整个网络中都不再被信任。这 k_2 个节点可以是其一跳邻居节点或是和它有过联系、发现它有恶意行为的节点。每个节点都存有一张被簇头节点确认的恶意用户列表，拒绝与这些节点的连接。需要选择合适的门限 $k2$，以确保合法节点不会被敌手节点的虚假信息损害。如果簇头节点发现一个节点有恶意行为，则直接把这个节点标记为恶意节点，广播签名的公告消息。

簇成员节点完全信任簇头节点，通过簇头节点维护恶意用户列表维持本簇内的信任关系。如果节点 A 被标记为恶意节点，那么它发出的控告信息都被视为无效，并且 A 将被从控告节点列表中清除。被标记为恶意节点的节点在对其控告列表中节点减少至 k_2 个以下时，可以变为可疑节点。簇头节点广播相应的签名消息，通告其行为状态。

结束语 Ad Hoc 网络是一种新型无线移动网络，它面临的特殊威胁导致了传统网络中的安全机制不再适用。现有 Ad Hoc 网络密钥管理方案多数是针对某种应用环境提出的，而且所提出的方案中有不少漏洞，目前尚缺乏有效的密钥管理方案。基于文[7,8]中的密钥管理方案，利用文[10]中的基于身份的签密体制，我们针对双频分级的 Ad Hoc 网络给出了一种分簇的密钥管理方案。方案不需要公钥证书，节省了用户的计算量、存储容量和系统的通信开销，并对恶意节点给出了有效的处理机制，而且可以对用户私钥进行有效的更新。方案具有良好的扩充性，适用于大规模的网络。我们在另一篇文章里研究了单频分级 Ad Hoc 网络的密钥管理问题。在以后的工作中，我们将进一步分析和改进分簇 Ad Hoc 网络的密钥管理方案，尤其是通信协议的仿真和优化以及方案的软件实现和效率分析。

参 考 文 献

1 Zhou L, Haas Z J. Securing Ad hoc Networks. IEEE Networks, 1999, 13(6): 24～30

2 Desmedt Y. Threshold cryptography. European Transactions on Telecommunications, 1994, 5(4): 449～457

3 Luo H, Zerfos P, Kong J, et al. Self-securing Ad Hoc Wireless Networks. In: 7th IEEE Symp on Computers and Communications, 2002. 567～574

4 Luo H, Lu S. Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks: [UCLA-CSD-TR-200030]. 2000 http://www.cs.ucla.edu/wing/publication/papers/Luo.TR200030.pdf

5 Hubaux J P, Buttyan L, Capkun S. Self-organized Public-Key Management for Mobile Ad hoc Networks. In: IEEE Transactions on Mobile Computing, 2003. 52～64

6 Hubaux J P, Buttyan L, Capkun S. The Quest for Security in Mobile Ad hoc Networks. http://www.gta.ufrj.br/～eric/tese/artigos/QuestForSecurityInMobileAdhocNetworks.pdf

7 Khalili A, Katz J, Arbaugh W A. Towards Secure Key Distribution in Truly Ad Hoc Networks. In: Proc. of IEEE Workshop on Security and Assurance in Ad hoc Networks, 2003. http://www.gta.ufrj.br/～eric/tese/artigos/id threshold.ps.gz

8 Li Guangsong, Han Wenbao. A New Scheme for Key Management in Ad Hoc Networks. In: Proceeding of 4th International Conference on Networking, LNCS 3421, 2005. 242～249

9 Zhang Y, Lee W, Huang Y. Intrusion Detection Techniques for Mobile Wireless Networks. ACM/Kluwer Wireless Networks Journal, 2003. 545～556

10 Boyen X. Multipurpose Identity-Based Signcryption: A Swiss Army Knife for Identity- Based Cryptography. In: Proceedings of Crypto '03, LNCS 2729, 2003. 383～399