一种基于时间序列面向预警的警报分析方法*)

梅海彬　龚　俭

（东南大学计算机科学与工程学院　南京 210096）（江苏省计算机网络技术重点实验室）

摘　要　本文通过对警报数据的观察和分析，提出了一种基于时间序列分析理论适合对大规模网络 IDS 警报数据进行实时宏观分析的新方法。该方法利用正常情况下每天 IDS 警报数的自相似性来建立 IDS 警报数的季节模型，并利用该模型和警报数在宏观上的关系对网络中出现的像 DDoS 和蠕虫等大规模入侵进行预警。理论分析和实验结果表明，此方法能及时发现网络中的大规模网络入侵并进行预警，并具有比基于网络流量异常的入侵预警方法准确和与 IDS 集成好的优点。

关键词　入侵检测系统，网络安全，警报分析，时间序列，季节模型，预警

An IDS Alarm Analysis Method for Intrusion Warning Based on Time Series Theory

MEI Hai-Bin　GONG Jian

(School of Computer Science and Engineering, Southeast University, Nanjing 210096)

Abstract　It is a wel-l-known fact that intrusion detection systems create large amounts of alarms and most of them are false alarms. How to analyze alarms automatically and find useful information from them has attracted a lot of interests. Although many approaches have been proposed, most of them focus on the relationship of different types or attributes of alarms, and they have deficiency in the large-scale network environments. This paper pays attention to the relation between alarm numbers and presents a novel alarm analysis method based on time series theory. Using the self-similar characteristic of alarms under normal conditions, a season model of alarms is constructed. With this model and the relationship of alarm number, warning information is quickly given when large-scale network intrusions, such as DDoS and worms, occur. This method has been tested on real world data, and experimental results demonstrate that the approach has a high degree of warning accuracy when large-scale network intrusions happen and can be integrated with IDS easily.

Keywords　Intrusion detection system (IDS), Network security, Alarm analysis, Time series, Season model, Intrusion early warning

1　引言

入侵检测系统(IDS)是保障网络安全的有效工具，它能够检测网络上的攻击行为，并提示系统管理员进行及时响应，以避免入侵带来的损失[1,2]。但是目前 IDS 技术还不成熟，无论是基于滥用检测的 IDS 还是基于异常检测的 IDS 都普遍存在报告的警报数目过多，且警报中包含大量误报的问题[3~6]。这些数目众多又含有大量误报的警报数据使得安全管理员手工分析警报犹如大海捞针，很难从中找到真正的警报和获得有价值的网络安全信息，也限制了 IDS 的自动响应。

鉴于此，人们提出了多种方法来试图解决该类问题。一种途径是从底层，从根本上找到一种好的检测模型来提高 IDS 的检测准确度，减少 IDS 产生的警报数。但实际上，研究有效的检测模型难度较大，文[7]用贝叶斯理论对此进行了分析说明。因此，有些学者开始从高层对 IDS 产生的警报进行分析，利用警报中的规律来减少需要管理者查看的警报数目、降低误报率，或向管理员提供有利于网络安全管理的有用信息，这成了近来 IDS 领域中一个新的研究热点。其中，一种比较具有代表性的方法是利用警报之间的前因后果关系来关联入侵警报[3~5]，通过这种警报的关联方法可以减少警报数目、降低误报率、构建入侵图，甚至还可以预测入侵者的下一步攻击并预警；第二种是基于概率的警报分析方法，它利用警报特征之间的相似关系来对入侵警报进行关联，从而减少警报数目[8]。此外，还有基于概念聚类的方法，它对相似的警报进行聚类来发现产生大量警报的根源，从而从根源上消除大量警报[12]；还有基于数据挖掘的方法，该方法对历史警报数据进行分析，发现对以后警报处理有用的信息，便于管理员对警报的处理[9~11]。

虽然上述方法在一定程度上减少了警报数目，降低了误报率，但要将这些方法较好地应用到大规模网络 IDS 的警报分析上仍显不足：一是这些方法大多存在关联分析计算量大、效率低和实时性不强等局限性[13]，这在大规模网中更为突出，采用这些技术的效果并不理想甚至难以实施；二是对于大规模网络上的 IDS，由于产生的警报快且数目过多，即使采用了这些方法，需要安全管理员手工分析的警报还是很多，仍无法对每条警报进行逐一分析和响应。另外，在实际中我们注意到，对于大规模网络的安全管理员来说，他们更需要关心的是整个网络的宏观安全状态，而非 IDS 报告的每条警报的细节内容，特别是当大规模网络中出现大规模入侵(指攻击主机数目多以及涉及范围广的网络入侵行为，像 DDoS 和 worm

*)国家 973 计划课题(2003CB314804)；江苏网络与信息安全重点实验室资助项目(BM2003201)。梅海彬　博士生，主要研究方向为网络安全；龚　俭　教授，博士生导师，主要研究方向为网络安全、网络行为学。

等)时,需要尽早发现和采取相应的响应措施,以便将攻击带来的损失降到最低。

因此,很有必要提出实时分析大规模网络 IDS 警报数据的新方法,来辅助安全管理者实时掌握整个网络的宏观安全状态,及时发现网络中出现的大规模入侵和进行预警。本文通过连续观察和分析实际大规模网络入侵检测系统 Monster3.0(这是 CERNET 华东北地区网络中心开发的面向大规模网络的分布式入侵检测系统)的警报数据,发现在正常情况下 IDS 每天所产生的警报数目具有自相似性(具体数据结果见 3.1 节图 1)。而当网络中出现大规模的入侵时,警报数目会急剧上升,远大于正常情况下的警报数,即 IDS 警报数出现异常,并且这种异常往往预示着大规模网络入侵的一步或多步的开始。

据此,本文提出一种基于时间序列分析理论适合对大规模网络 IDS 警报数据进行实时宏观分析的新方法。该方法依据大规模网络 IDS 警报分析的实际需要,区别于以上的警报分析方法,分析的重点不是单个的警报而是整个警报流,它的主要目的不是减少警报数目和降低误报率,而是通过分析 IDS 警报数据来对大规模网络安全的宏观状态进行实时监控,及时发现入侵警报数据因大规模网络入侵引起的异常并进行预警,从而让安全管理员尽早地对大规模入侵做出响应,减少入侵带来的损失。通过 CERNET 江苏省网主干 IDS 的警报数据进行测试获得的实验结果和相关分析表明,本文提出的方法能及时发现网络中的大规模网络入侵并进行预警,并且在效率上要好于基于意图识别的预警方法[14,15],以及具有比基于网络流量异常的预警方法[16~18]更准确和与 IDS 集成好的优点。

2 警报数据的预处理

为了对警报数据进行时间序列分析和建模,需要将采集到的警报数据转换为用于分析的警报数时间序列,首先给出相关定义,然后是具体的转换步骤。

定义 1(警报序列 A_S) 警报序列 A_S 为 IDS 警报按其被报告的时间顺序构成的一个序列,即

$$A\_S=\langle A_{t1},A_{t2},\cdots,A_{tn}\rangle$$

其中,A_{ti} 表示一个 IDS 警报,t_i 表示该警报 A_n 被报告的时间且满足 $t_1\leqslant t_2\leqslant\cdots\leqslant t_n$。

定义 2(时间窗口序列 W_S) 将总的警报数据采集时间 T 划分为 m 个等长的时间窗口 w_i,由这些时间窗口按序构成的序列定义为时间窗口序列 W_S,即

$$W\_S=\langle w_1,w_2,\cdots,w_m\rangle$$

其中 $w_1.et<w_2.st<,\cdots,w_{m-1}.et<w_m.st$ 和 $T=w_m.et-w_1.st$,而 $w_i.st$ 为 w_i 的起始时间,$w_i.et$ 为 w_i 的结束时间,并记 $w_i.length$ 为窗口 w_i 的时间长度,$w_i.length=w_i.et-w_i.st$;

定义 3(警报数时间序列 X_T) 依次统计 A_S 在 W_S 的每个时间窗口 w_i 中的警报个数,并把得到的一数目序列定义为警报数时间序列 X_T,即

$$X_T=\langle x_1,x_2,\cdots,x_m\rangle$$

其中 $x_i=|\{A_{ti}|w_i.st\leqslant t_i<w_i.et\}|,i=1,2,\cdots,m$。

警报数据转换的具体步骤为:

步骤 1:我们将采集到的警报数据按警报的报告时间顺序构建一警报序列 $A\_S=\langle A_{t1},A_{t2},\cdots,A_{tn}\rangle$,其中 $n=531516$;

步骤 2:将本文中总的采集时间 T($T=7$ 天$\times$24 小时$\times$60 分钟$=10080$ 分钟)按 $w_i.length$ 为 15 分钟来建立时间窗口序列 $W\_S=\langle w_1,\cdots,w_m\rangle$,则其中 $m=10080\div15=672$;

步骤 3:按定义 3 生成警报数时间序列 $X_T=\langle x_1,\cdots,x_m\rangle$,其中 $m=672$。

3 基于时间序列的警报分析模型

3.1 警报数据的模型识别

模型的识别的主要目的是辨别时间序列满足什么样的模型以及模型的阶数是多少,较为直观的模型的识别方法是根据序列的自相关系数和偏相关系数来判断,具体方法可参见文[19]。从警报数据序列 X_T 的分布图 1 和序列的自相关图 2 可以看出警报数序列呈现周期性,且周期为 24h。根据时间序列理论,当时间序列的变化包含很明显的周期性规律时,可以对时间序列建立季节性模型。通常一个序列 Z_t,如果它符合以下模型:

$$\Phi(B^s)\nabla_s^D z_t=\Theta(B^s)A_t \tag{1}$$

则称 z_t 为周期为 s 的季节性模型序列。(1)式称为季节性模型,其中:$\nabla_s^D=(1-B^s)^D$,$\Phi(B^s)=1-\Phi_1B^s-\Phi_2B^{2s}-\cdots-\Phi_nB^{ns}$,$\Theta(B^s)=1-\Theta_1B^s-\Theta_2B^{2s}-\cdots-\Theta_nB^{ns}$,$s$ 为正整数,B 称为后移算子,满足:$x_{t-k}=B^k\cdot x_t$ 和 $a_{t-k}=B^k\cdot a_t$。(1)式中如果 A_t 不为白噪声,则可用 $ARIMA(n,d,m)$ 模型对 A_t 建模为

$$\varphi(B)\nabla^d A_t=\theta(B)a_t,a_t\sim NID(0,\delta_a^2) \tag{2}$$

其中,$\varphi(B)=1-\varphi_1B-\varphi_2B-\cdots-\varphi_nB^n$,$\theta(B)=1-\theta_1B-\theta_2B-\cdots-\theta_mB^m$,则由(1)和(2)式得到乘积型的季节模型:

$$\varphi(B)\Phi(B^s)\omega_t=\theta(B)\Theta(B^s)a_t,\omega_t=\nabla^d\nabla_s^D z_t \tag{3}$$

其阶次常用$(n,d,m)\times(p,D,q)s$ 表示。

对于满足周期变化的季节性数据显然是非平稳的,如将某时刻的数据与前一周期的同一时刻的数据相减,就可能将数据中的周期性变化消除,使新得到的序列接近平稳序列,为此,可对序列做周期为 24h 的季节性差分来消除序列的周期性变化。图 3 为季节差分消除后的序列的时序图。图 4 和图 5 为其相应的自相关函数和偏相关函数图。从图 4 和图 5 上可知,序列的自相关系数存在"拖尾"现象,且下降速度较快。由时间序列分析理论可知,经过消除后的序列已是平稳序列[21](从图 3 也可看出)。从经过周期消除后的警报数据序列的偏相关图上来看,偏相关图存在"截尾"现象,且从第 2 个点以后值都非常小。根据判断理论可知,该周期消除后的序列应是满足 $AR(2)$ 模型的序列。又根据文[22]可知,当 $\omega_t=\nabla^d\nabla_s^D z_t$ 能够用低阶的 ARMA 模型拟合时,季节模型并不表现出疏系数的形式(即$(m,d,n)\times(p,D,q)s$ 中的 $p=q=0$),只是在对 z_t 做差分运算时,含有以周期为步长的差分形式而已。此时,ω_t 的参数估计与非季节模型完全相同,这时乘积型的季节模型 $\varphi(B)\Phi(B^s)\omega_t=\theta(B)\Theta(B^s)a_t,\omega_t=\nabla^d\nabla_s^D z_t$。可写为 $\varphi(B)\omega_t=a_t,\omega_t=\nabla_s z_t$,或更进一步写为$(1-\varphi_1B-\varphi_2B^2)\omega_t=a_t,\omega_t=\nabla_s z_t$,即

$$\omega_t=\varphi_1\omega_{t-1}+\varphi_2\omega_{t-2}+a_t,\omega_t=\nabla_s z_t \tag{4}$$

其中 φ_1,φ_2 为待估参数,s 的值为 96(因为周期为 24h,而时间窗口长度为 15min,所以有 $24\times60/15=96$)。

3.2 模型参数的估计

模型选定后,下一步工作就是估计模型(4)参数 φ_1,φ_2。由于本文的待估参数的模型是 $AR(2)$ 模型,因此这里只介绍 AR 模型的参数估计。对于 AR 模型参数估计方法较多,像最

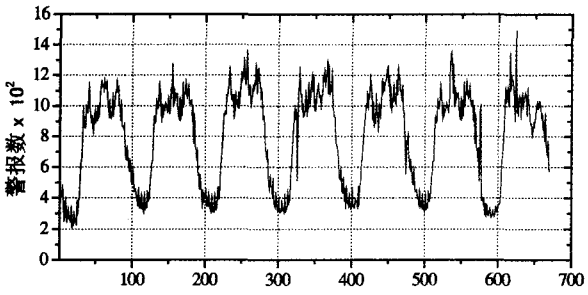

图 1　原始时间序列

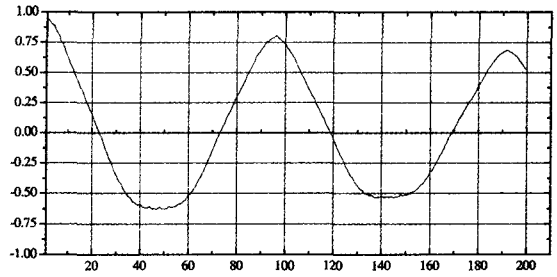

图 2　原始时间序列的自相关图

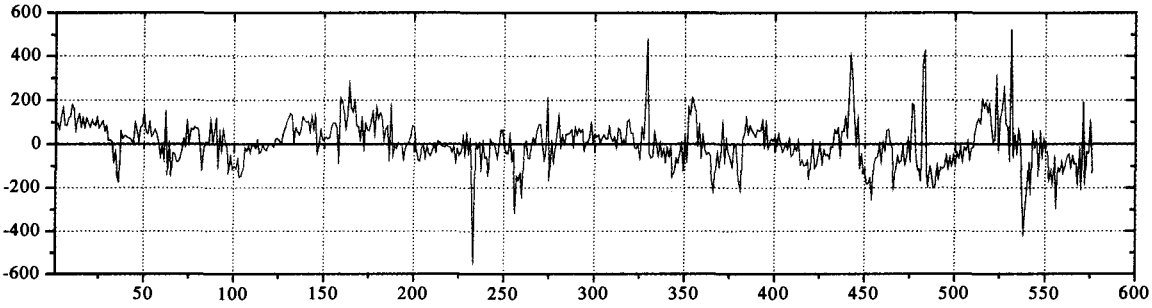

图 3　周期消除后的时间序列

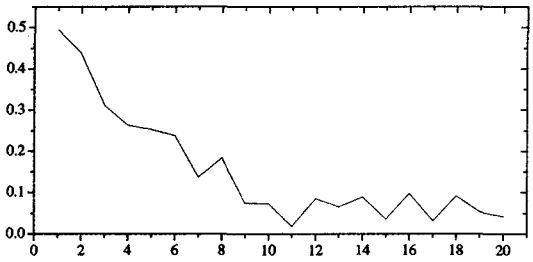

图 4　周期消除后时间序列的自相关图

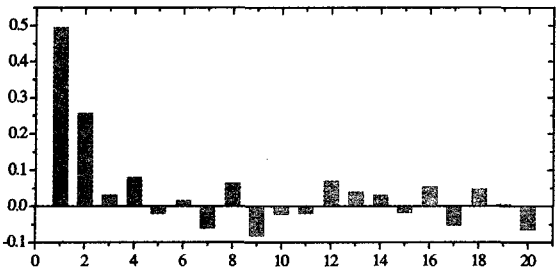

图 5　周期消除后时间序列的偏相关图

小二乘法、矩阵递推估计法、参数递推估计法等，本文采用最小二乘法来估计参数[21]。其具体求法为

$$\hat{\varphi}=(X^TX)^{-1}X^TY$$

其中：

$$Y=[x_{n+1}\quad x_{n+1}\quad \cdots\quad x_N]^T$$

$$\hat{\varphi}=[\hat{\varphi}_1\quad \hat{\varphi}_2\quad \cdots\quad \hat{\varphi}_n]$$

$$X=\begin{bmatrix} x_n & x_{n-1} & \cdots & x_1 \\ x_{n+1} & x_n & \cdots & x_2 \\ \cdots & \cdots & \cdots & \cdots \\ x_{N-1} & x_{N-2} & \cdots & x_{N-n} \end{bmatrix}$$

N 为样本长度，$x_k(k=1,\cdots,N)$ 为样本中的第 k 个元素，$\hat{\varphi}_i(i=1,\cdots,n)$ 为待估参数。对于本文，$N=576$，$n=2$，通过计算，得到的参数的值为：$\hat{\varphi}_1=0.3742$；$\hat{\varphi}_2=0.2998$。这样，经过季节消除后的时间序列 ω_t 的模型为

$$\omega_t=0.3742\omega_{t-1}+0.2998\omega_{t-2}+a_t,a_t\sim NID(0,\hat{\sigma}_a^2) \quad (5)$$

其中，$\hat{\sigma}_a^2=\frac{1}{576-2}\sum_{t=2+1}^{576}(x_t-\sum_{i=1}^{2}\hat{\sigma}_i x_{t-i})^2=4235.48$。

3.3　警报数据预测

对于 $AR(p)$ 模型 $x_t=\varphi_1x_{t-1}+\varphi_2x_{t-2}+\cdots+\varphi_px_{t-p}+a_t$ 的时间序列，利用平稳线性最小方差预测，可以得到比较准确的预测值[21]。由于本文模型属于 $AR(p)$ 模型，因此采用平稳线性最小方差预测方法来进行预测。设 $\{x_t\}$ 是平稳的、零均值的序列，用符号 $\hat{x}_t(l)$ 表示由 t 时刻以及以前的历史数据对 x_{t+l} 所作的 l 步平稳线形最小方差预测，则 l 步平稳线形最小方差预测公式为

$$\hat{x}_t(l)=\varphi_1\hat{x}_t(l-1)+\varphi_2\hat{x}_t(l-2)+\cdots+\varphi_p\hat{x}_t(l-p),l>0 \quad (6)$$

且有 $\hat{x}_t(-l)=x_{t-l},l\geqslant 0$，则有 $AR(p)$ 模型预测的递推公式：

$$\hat{x}_t(1)=\varphi_1x_t+\varphi_2x_{t-1}+\cdots+\varphi_px_{t-p+1}$$

$$\hat{x}_t(2)=\varphi_1\hat{x}_t(1)+\varphi_2x_t+\cdots+\varphi_px_{t-p+2}$$

$$\cdots$$

$$\hat{x}_t(p)=\varphi_1\hat{x}_t(p-1)+\varphi_2x_t(p-2)+\cdots+\varphi_{p-1}\hat{x}_t(1)+\varphi_px_t$$

$$\cdots$$

$$\hat{x}_t(l)=\varphi_1\hat{x}_t(l-1)+\varphi_2x_t(l-2)+\cdots+\varphi_{p-1}\hat{x}_t(l-p+1)+\varphi_p\hat{x}_t(l-p),l>p$$

由上可知，只要知道 $x_t,x_{t-1},\cdots,x_{t-p+1}$ 这 p 个时刻的观测值，无须更多的历史数据，就可以根据这些递推公式来计算 $AR(p)$ 模型的任意步最小方差预测值。

根据时间序列理论，假设 $e_t(l)=\omega_{t+l}-\hat{\omega}_t(l)$ 为序列在 t 时刻向后 l 步预测的误差，则 l 步预测最小均方误差为

$$e_t^2(l)=\sigma_a^2(G_0^2+G_1^2+G_2^2+\cdots+G_{l-1}^2)$$

其中 G_j，$j=0,\cdots,l-1$ 为序列格林函数[20]。它与预测时间无关，只与预测步数 l 有关：预测步数越多，误差会越大。考虑预测的准确性，本文中仅做一步预测。由(5)和(6)式可知，

当 $l=1$，做一步预测时，只需要知道前 2 个时刻的观测值，预测公式为

$$\hat{\omega}_t(1)=0.3742\omega_t+0.2998\omega_{t-1} \quad (7)$$

4 实验和结果分析

本文采用的实验数据是利用 Monster3.0 系统对 CERNET 江苏省网主干连续采集到的警报数据，采集时间为一周，总共收到 531516 条警报。该数据集是经过 Monster3.0 系统冗余消除模块进行冗余消除后的结果集，冗余消除的目的是消除警报报告中冗余现象，减少警报数目，便于警报分析[19]。由于数据来自省网主干的真实数据，因此具有较好的代表性。

实验过程分为警报数据的实时采集、警报数据到时间序列数据的转换、时间序列的预测和入侵预警。试验框架如图 6 所示。

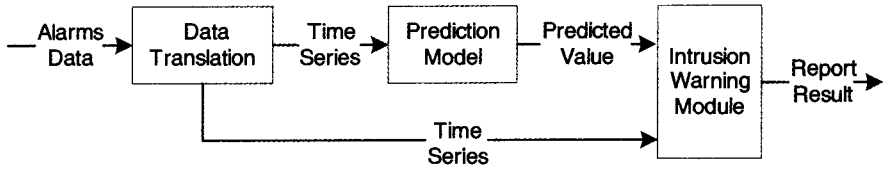

图 6 试验框架

为了验证本文提出的方法的可行性，需要验证两点：一是在网络没出大规模入侵情况下，预测值是否可信，因为本文预警的基本原理是检测实测值与预测值的差值是否大于设定的阈值，所以如果预测值不准确，那预警也会有问题；二是当被入侵监测系统监控的网络中出现大规模入侵时，本文的方法是否能正确地进行异常检测和预警。

4.1 对警报数据预测的验证

本文在网络没出现大规模入侵的情况下，任意选取了两天 Monster3.0 系统在 CERNET 江苏省网主干上报告的警报数据做一步实时预测实验。实验结果如图 7 和图 8，图中 Y 轴为警报数目，X 轴为时间窗口序号，时间窗口长度为 15min。

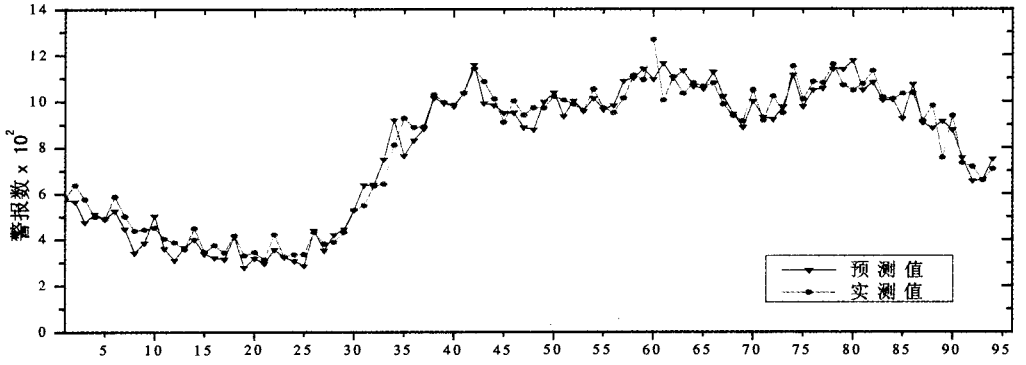

图 7 预测结果 1

根据 3.2 节中得到的预测模型(5)式知，当 t 固定时，ω_t 和 a_t 具有相同的概率分布，则可根据 a_t 的概率分布对 ω_t 的真值范围作出概率上的判断。因 a_t 是白噪声且是服从正态分布的，其方差为 $\hat{\sigma}_a^2$。当取 95% 的置信度时，ω_t 的真值以 95% 的概率落在以下区间内：$(\hat{\omega}_t-1.96\hat{\sigma}_a,\hat{\omega}_t+1.96\hat{\sigma}_a)$，其中 $\hat{\omega}_t$ 表示 ω_t 的预测值。如果设定实际值落到该预测区间，就认为预测是准确的。可以统计出图 6 中预测正确的数目为 89 次，而又已知总的预测点数为 96－ 2＝94 个，故可求出预测的准确率为 89/94 * 100%＝94.7%。

同样对图(7)的预测结果进行统计。预测正确的点的个数为 84 个，预测的准确率为 84/94 * 100%＝89.4%。显然，从实际警报数据所做的两次实验来看，在网络正常环境下，本模型的预测效果是可信的。

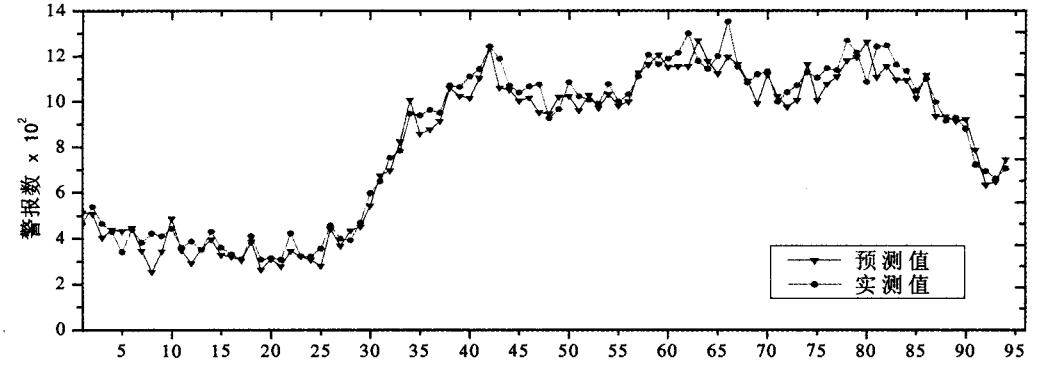

图 8 预测结果 2

4.2 大规模入侵的预警

为了验证本文方法在网络中出现大规模入侵时能否检测到警报流的变化并给出相应的预警，本文首先设定预测值和实际测值的差值超过给定阈值(本次实验中设定的阈值为300)的点为异常点，然后当警报流中出现异常点时就产生预警信息。实验中，本文利用一款基于高级扫描技术、适合大规模扫描的扫描器 L-ScanPort1.0 在 Monster3.0 系统监测的 CERNET 江苏省网主干上注入了两次大的网络扫描攻击流：一次注入时间是中午 12 点，另外一次是下午 1：30。图 9 为实验结果，图中 Y 轴为警报数目，X 轴为时间窗口序号，时间窗口长度为 15min；图中阴影标示的点为检测到的异常点，它对应于一次大的扫描活动；图中的警戒值是预测值加上阈值，超过警戒值的点即为异常点。从图可以看出本文的方法对于两次大规模的扫描攻击均能准确地检测到，这说明本文方法在预警上是可行的。

目前，入侵预警主要有两种形式：一种是根据复合攻击的多步性，通过检测到的攻击来预测攻击者下面会采取的攻击，并向管理员发出预警，像文[14,15]中提到用意图识别的方法；另一种就是根据网络流量的一些异常来进行入侵预警，像文[16～18]等。前一种方法的优点是预测相对准确，但需要保存一些前面攻击的状态，这在大规模网上进行实时预警存在性能问题，而且这种预警只能针对已知的复合攻击。后一种方法不需要知道复合攻击的具体步骤，能对未知的大规模复合攻击进行预警，也不需要保留中间状态，在性能上优于前一种方法。但由于网络流量异常原因多样化，有些异常可能不是入侵引起，可能造成错误的预警。本文方法与基于网络流量异常的预警方法类似，但本文提出的方法是直接利用 IDS 产生的警报，这样本方法具有实现简单且与 IDS 集成性好的特点。此外，由于是对 IDS 所报告的警报进行二次分析，本方法不会像基于流量异常方法对非入侵引起的网络流量异常产生预警，因此准确性要高于基于流量异常方法。

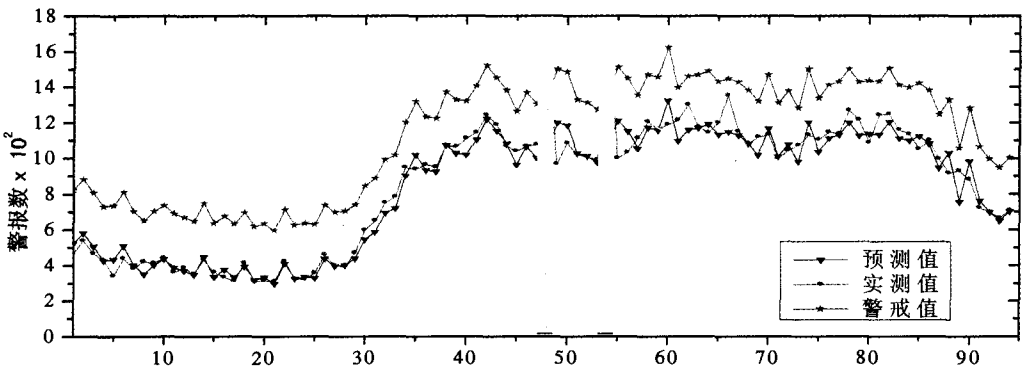

图 9 对大规模攻击的预警

结论 近年来，对 IDS 报告的大量警报数据的自动分析和处理已变得非常需要。本文经过对大量实际警报数据的观察和分析，提出了基于时间序列分析理论适合对大规模 IDS 警报进行宏观分析来预警的新方法。该方法能对正常情况下 IDS 所报告的警报数建立时间序列模型，然后利用该模型进行 IDS 警报的预报和异常检测，达到大规模网络入侵的预警目的。本文采用 CERNET 江苏省网主干下的实测警报数据进行测试，实验结果验证了该方法对大规模网络入侵预警的可行性。本文方法是对 IDS 所报告的警报进行二次分析，所以具有比基于网络流量异常的入侵预警准确，实施简单以及与 IDS 容易集成等好处。此外，由于不需要保存一些前面攻击的状态，在效率上要好于基于意图识别的预警方法。

参 考 文 献

1 龚俭，陆晟，王倩. 计算机网络安全导论. 南京：东南大学出版社，2000

2 Denning D E. An intrusion detection model. IEEE Trans on Software Engineering, 1987, 13(2): 222～232

3 Ning Peng, Cui Yun, Reeves D, et al. Tools and techniques for analyzing intrusion alerts. ACM Trans on Info and System Security, 2004, 7(2): 273～318

4 Ning Peng, Xu Dingbang, Christopher G, et al. Building attack scenarios through integration of complementary alert correlation methods. In: Proceedings of the 11th Annual Network and Distributed System Security Symposium. San Diego, 2004. 97～111

5 Ning Peng, Xu Dingbang. Learning attack strategies from intrusion alerts. In: Proceedings of the 10th ACM Conference on Computer and Communications Security, Washington D C, 2003. 200～209

6 Debar H, Wespi A. Aggregation and correlation of intrusion detection alerts. In: Proceedings of 4th International Symposium on Recent Advances in Intrusion Detection (RAID). Davis, 2001. 85～103

7 Axelsson S. The base-rate fallacy and the difficulty of intrusion detection. ACM Transactions on Information and System Security, 2000, 3(3): 186～205

8 Valdes A, Skinner K. Probabilistic alert correlation. In: Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID). Davis, 2001. 54～68

9 Julisch K, Dacier M. Mining intrusion detection alarms for actionable knowledge. In: Proceedings of the 8th International Conference on Knowledge Discovery and Data Mining. New York, 2002. 366～375

10 Julisch K. Mining alarm clusters to improve alarm handling efficiency. In: Proceedings of 17th Annual Computer Security Applications Conference. New Orleans, 2001. 12～21

11 Clifton C, Gengo G. Developing custom intrusion detection filters using data mining. In: Proceedings of Military Communications Int'l Symposium. California, 2000. 440～443

12 Julisch K. Clustering intrusion detection alarms to support root cause analysis. ACM Trans on Information and System Security, 2003, 4(6): 443～471

13 穆成坡，黄厚宽，田盛丰. 入侵检测系统报警信息聚合与关联技术研究综述. 计算机研究与发展，2006，43(1)：1～8

14 Qin Xinzhou, Lee Wenke. Attack plan recognition and prediction using causal networks. In: Proceedings of Annual Computer Security Applications Conference. Tucson, 2004. 370～379

15 张剑. 可回卷的动态反馈自动入侵响应系统：[博士论文]. 南京：东南大学，2004

16 Cliff C, Gong Weibo, Towsley Don, et al. The monitoring and early detection of internet worms. IEEE Trans on Networking, 2005, 13(5): 961～974

17 Barford P, Kline J, Plonka D, et al. A signal analysis of network traffic anomalies. In: Proceedings of ACM SIGCOMM Internet Measurement Workshop. Marseilles, 2002. 71～82

18 Kim S S, Reddy A L N, Vannucci M. Detecting traffic anomalies at the source through aggregate analysis of packet header data. In: Proceedings of Networking. Athens, 2004. 1047～1059

19 龚俭，梅海彬，丁勇，等. 多特征关联的入侵事件冗余消除. 东南大学学报，2005，35(3)：366～371

20 杨位钦，顾岚. 时间序列分析与动态数据建模. 修订本. 北京：北京理工大学出版社，1988

21 杨叔子，吴雅，等. 时间序列分析的工程应用. 武汉：华中理工大学出版社，1991

22 安鸿志，陈兆国，等. 时间序列的分析与应用. 北京：科学出版社，1983