维普资讯 http://www.cqvip.com

一种运用限幅自相似性的新型DDoS入侵检测机制*)

罗光春　卢显良　薛丽军
(电子科技大学信息中心　成都610054)

摘　要　本文提出了一种新型的DDoS入侵检测方法，在建立正常网络流量模型基础上，对网络流量的自相似性—Hurst参数、Hurst参数的时变函数H(t)进行分析，对网络流量进行实时限幅，由自相似性的变化来预测DDoS攻击，并用数据库对攻击定位。试验表明基于网络流量的统计分析方法能够在一定程度上检测出DDoS攻击，比传统的基于特征匹配的DDoS入侵检测方法，在实时性、准确率上有较大提高。

关键词　入侵检测，分布式拒绝服务攻击，自相似性

A Novel Mechanism of DDoS Intrude Detection Based on Setting a Limit and Self-Similarity

LUO Guang-Chun　LU Xian-Liang　XUE Li-Jun
(Information Center of UEST of China, ChengDu 610054)

Abstract　This paper presents a novel mechanism of DDoS Intrude Detection. We do researches on constructing normal model of network traffic, analysizing Self-Similarity of network traffics--Hurst Parameter, and its time variable function H(t). Through limiting the extent of network traffic in time, we measure the change of H Parameter brought by DDoS attack. Moreover we use Distributed Database to refine the DDoS attack. As it shown by the research result, this statistical analysis method can detect DDoS attack and is more reliable on the recognition of kinds of DDoS attack than any other traditional method based on character recognition.

Keywords　Intrude detection, DDoS, Self-similarity

真实的网络业务具有统计上的自相似性，通过在网络中抽样检测网络流量，并通过快速算法得出相应的自相似性参数值，可以判断网络的当前数据流是否符合网络业务在统计上的自相似性以及得到相应的自相似性特征。DDoS攻击(Distributed Denial of Service 分布式拒绝服务攻击)是近年来对Internet具有巨大影响的恶意攻击方式，给互联网业务带来了不可估量的损失，对网络流量的自相似性特征有明显的影响。传统检测方法使用基于特征匹配的检测，先前方法使用网络流量的自相似性，但传统方法与先前论述的方法存在几个问题：1. 由于自相似参数的估计方法需要一个大的网络流量的样本，检测通常是滞后的，不能满足对DDoS检测的实时性要求；2. 使用网络流量的自相似性分析符合网络流量的统计特性，但仅能粗略分析是否遭到攻击，不能准确对攻击定位(如确定攻击的源或目的)，也就无法采取相应的控制措施。我们进行了对真实业务流量的自相似性的限幅分析，得出了检测DDoS的新方法——建立正常的网络流量模型，由于DDoS攻击分为连续攻击、间断攻击，相应地，我们使用不同的方法进行检测分析：对于连续攻击，将正常、异常的自相似性(H参数)进行比较，得到连续攻击的特性；对于间断攻击，计算异常时的自相似性，再用正常的网络流量对异常时的流量进行限幅，计算限幅后的自相似性，将限幅前后的自相似性进行比较，得到间断攻击的特性。在得到了基于网络的DDoS的攻击特性之后，我们使用分布式数据库，依据变化率，运用判决树，对接收的包头信息进行处理，从而对攻击定位，详细到能断定攻击的类型、攻击的源、目的等，以便能控制攻击。总之，我们提出一种新的DDoS的检测方法：建立正常流量模型，对网络流量的自相似性分析，对网络流量进行实时限幅以及使用数据库统计分析的DDoS检测方法。该方法在对网络流量异常(如DDoS)检测时，达到准确、实时的目的。

1　网络流量的自相似性含义及其分析方法

1.1　网络流量的自相似性含义

自相似的广义定义：若依赖时间的随机过程(时间序列)满足下述条件，则是自相似的：

$$y(t)\overset{d}{=}a^{H}y(\frac{t}{a}), \tag{1}$$

其中，$\overset{d}{=}$表示同概率特性，H为自相似性程度参数，$1/2<H<1$，同网络带宽的利用率成正比。

统计描述：设$X=\{X_j, j=1,2,\cdots\}$为一协方差平稳的随机序列，即X具有恒定均值$\mu=E[X_i]$，和有限方差$\sigma^2=E[(X_i-\mu)^2]$，其自相关函数$r(k)=E[(X_i-\mu)(X_{i+k}-\mu)]/\sigma^2$ $(k=0,1,2,\cdots)$仅与k有关。假设X的自相关函数具有形式：$r(k)\sim k^{-\beta}L_1(k)$，$k\to\infty$，其中$0<\beta<1$，$L_1$满足$\forall x>0$，有$\lim_{t\to\infty}\frac{L_1(tx)}{L_1(t)}=1$。

令$X_k^{(m)}=\frac{(X_{km-m+1}+\cdots+X_{km})}{m}$$(k=1,2,3,\cdots)$为X的$m$阶聚集过程，并记时间序列$X^{(m)}=(X_1^{(m)},X_2^{(m)},\cdots)$的自相关函数为$r^{(m)}$，$m=1,2,3,\cdots$。

定义1　过程被称为严格二阶自相似的且具有自相似系数$H=1-\frac{\beta}{2}$，如果其m阶聚集过程$X^{(m)}$具有与原过程X同样的相关函数，即$r^{(m)}(k)=r(k)$对所有$(m=1,2,\cdots,k=1,2,$

*)本文由国家九七三(项目号973-1-4-2)和电子科技大学青年基金支持。罗光春　博士研究生；卢显良　教授，博士生导师；薛丽军　硕士研究生。

维普资讯 http://www.cqvip.com

…)成立。

定义2 过程 X 被称为是渐近二阶自相似的，且具有自相似系数 $H=1-\frac{\beta}{2}$，如果 $r^{(m)}(1)\to 2^{1-\beta}-1, m\to\infty$ 及 $r^{(m)}(k)\to\frac{1}{2}\delta^2(k^{2-\beta}), m\to\infty(k=2,3,\cdots)$，式中 $\delta^2(f)$ 表示作用在 f 上的二次差分算子，即 $\delta^2(f(k))=f(k+1)-2f(k)+f(k-1)$。

1.2 自相似性的分析方法

假设过程 X 为自相似(或渐进自相似)过程，则分析方法有：

1)使用聚集方差法 过程 X 的聚集过程 $X^{(m)}$ 的方差($m=1,2,3\cdots$) $\mathrm{Var}X^{(m)}\sim\sigma_0^2 m^{\beta}$，当 $m\to\infty$，$\beta=2H-2<0$。$\mathrm{Var}X^{(m)}$ 在 log-log 图中对于 m 线性减小(对于大 m)。通过画 log(var($X^{(m)}$))对应于 log(m)，并对平面中的所得的点作最小二乘线，忽略小 m，得到所谓的方差－时间曲线。在－1与0之间的渐进斜率估计 β 的值为自相似性，并对自相似性的程度的估计值为 $H=1-\beta/2$。

2)R/S 分析法 $X=\{X_k,k=1,2,\cdots\}$，令其均值为 $\overline{X}$，部分和 $Y(X)=\sum_{i=1}^{n}X_i$，样本方差 $S^2(n)=(1/n)\sum_{i=1}^{n}X_i^2-(1/n)^2Y(n)^2$，则有 R/S 统计为：

$$\frac{R}{S}(n)=\frac{1}{S(n)}\left[\max_{0\le t\le n}\left(Y(t)-\frac{t}{n}Y(n)\right)-\min_{0\le t\le n}\left(Y(t)-\frac{t}{n}Y(n)\right)\right]$$

将整个样本 X 分成 k 个不重叠的块，每个块的大小为 n，并对于每个新的开始点 $t_1=1, t_2=N/K+1, t_3=2N/K+1,\cdots$(满足$(t_i-1)+n\le N$)计算变比例调整范围 $R(t_i,n)/S(t_i,n)$。因此，对于一个 n 的给定值(滞后)，得到 R/S 的许多样本，对于小 n，样本数为大(K)，并当 n 接近于总样本大小 N 时，为小。接下来，使用 log 空间的 n 的值，起点为 $n\approx 10$。对 log(n)画 log($R(t_i,n)/S(t_i,n)$)得到变比例调整范围图。如果以 log$\{E[R/S(n)]\}$为纵坐标，以 log$n$ 为横坐标作图，并用最小二乘法进行直线拟合，所得的直线的斜率即为 H。

3)周期图法 特别对于分形高斯过程 $X_j: j=1,2,3,\cdots,N$，周期图曲线估计值为 $I(\lambda)=\frac{1}{2\pi N}\left|\sum_{j=1}^{N}X_j e^{ij\lambda}\right|^2$，$\lambda$ 为频率，N 为过程 X 时间序列长度。有周期图曲线估计值 $I(\lambda)\sim|\lambda|^{\gamma}$，以 $I(\lambda)$ 为纵坐标，以 log$|\lambda|$ 为横坐标作图，并用最小二乘法进行直线拟合，得到 γ，$H=(\gamma+1)/2$。

4)Whittle 法 该方法基于周期图法。谱密度 $f(\lambda;\eta)$ 已知，由 Whittle 表达式

$$Q(\eta)=\int_{-\pi}^{\pi}\frac{I(\lambda)}{f(\lambda;\eta)}d\lambda+\int_{-\pi}^{\pi}\log f(\lambda;\eta)d\lambda$$

对 $f(\lambda;\eta)$ 归一化可以使加号的右项为0，使得上式成立的 η 最小(也就是 H)。将 Whittle 的近似 MLE 方法与聚集方法相结合，来获得自相似参数 H 的置信间隔：对于给定的时间序列，考虑相应的聚集过程 $X^{(m)}$ 有 $m\to 100,200,300,\cdots$，选择最大的 m 值以至于相应序列 $X^{(m)}$ 的样本大小不小于100。对于每个聚集序列，通过离散估计自相似参数 H，$f(x;(1,H^{(m)}))$ 表示分形高斯噪声的功率谱密度。这个过程得到 H 的估计值 $\hat{H}^{m}$，并相应地得到形式为 $\hat{H}^{m}\pm 1.96\hat{\sigma}_H$ 的95%的置信间隔，$\hat{\sigma}_H^2$ 由中心极限理论得出。最终，我们用它们的95%置信间隔，相对 m 画 H 的近似值 $\hat{H}^{m}$。

2. 真实业务流量的自相似性的限幅分析

2.1 基于限幅的自相似性方法选取

为研究 LAN 上的业务流量，选取电子科技大学网络中心的206室子网网段监测的两周数据。数据为从2002年12月24日0:00am 开始到2003年1月4日0:00am 为止的所有该子网上传送的数据包的大小(以 byte 记)(采样间隔1s)，监测时间共约11天，其峰值位率约为244Mbps(采样间隔1s)，平均位率约为414k bps，标准差为3.8189e+006bps，这些数据基本可以代表 LAN 中，及 LAN-WAN 互联时传输的突发业务。图1左图为未经限幅的网络流量，对之限幅，阈值为 $y=2\times10^7$，得到图1右图。

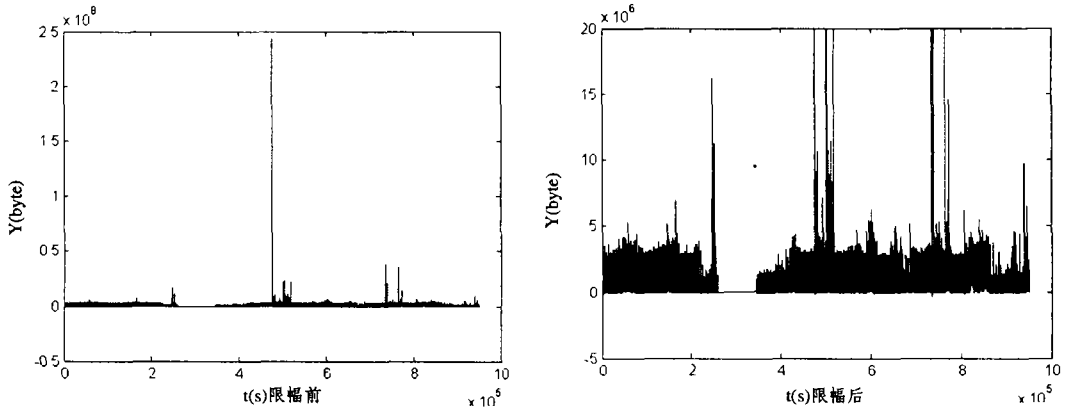

图1

我们将对数据进行期望值规正后，用上述的方法进行处理估计采样序列的 Hurst 系数。将总数据样本分为94个子样本，每个子样本大小为10000(实际时间长度上为2.78小时)，然后对每个子样本运用上述的方法，得到图2左图 H(其中聚集方差法为带○的直线、R/S 法为带 x 的点划线、周期图法为＋的虚线，下面各部分都是如此)，再运用 Whittle 法，得到图2右图。

1)限幅前：

以下是上述方法的 H 的均值、方差：

H	聚集方差	周期图	R/S	Whittle
均值	0.7866	0.8765	0.7481	0.8464
方差	0.0629	0.0813	0.0119	0.0360

综上可见 R/S 方法较为稳定，Whittle 次之，周期图法对

维普资讯 http://www.cqvip.com

向高端突变较为灵敏，聚集方差法对向低端突变较为灵敏。

2)限幅后：阈值为 $y=2\times10^7$，令 H=|H(限幅前)−H(限幅后)|，得到图3。

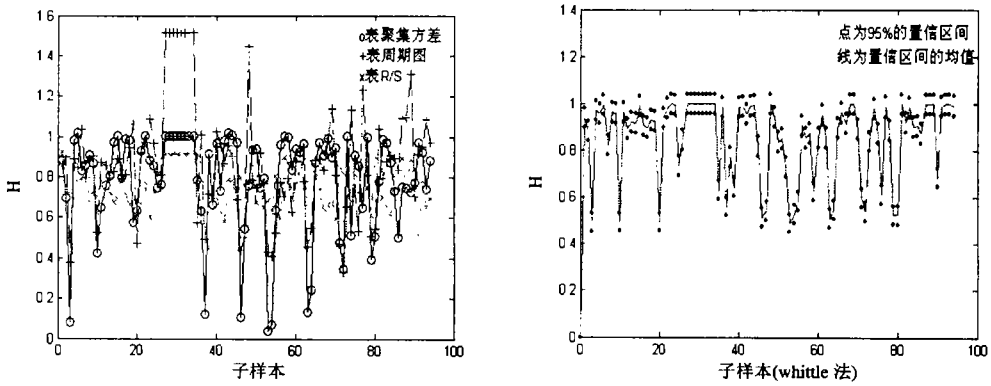

图2

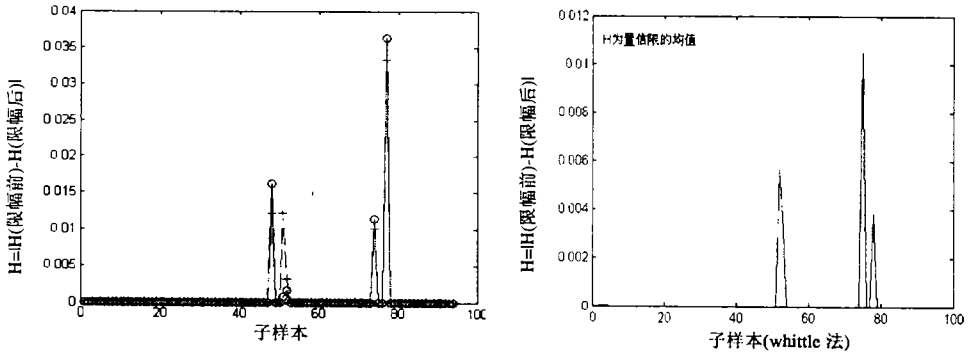

图3

H	聚集方差	周期图	R/S	Whittle
均值	0.7871	0.8768	0.7481	0.8466
方差	0.0629	0.0813	0.0119	0.0360

综上可见，在总体样本上，对于限幅前后，H 的方差无变化，对于聚集方差、周期图、Whittle，H 的均值有少许的改变，但对于 R/S，H 的均值无变化。在子样本上，对于限幅前后，对于聚集方差、周期图，H 有较大改变；对于 Whittle，H 有明显改变；对于 R/S，H 无明显变化。

2.2 阈值变化的限幅特征

使用聚集方差、周期图方法、R/S，对网络流量数据运用不同的阈值进行限幅，得到图4。

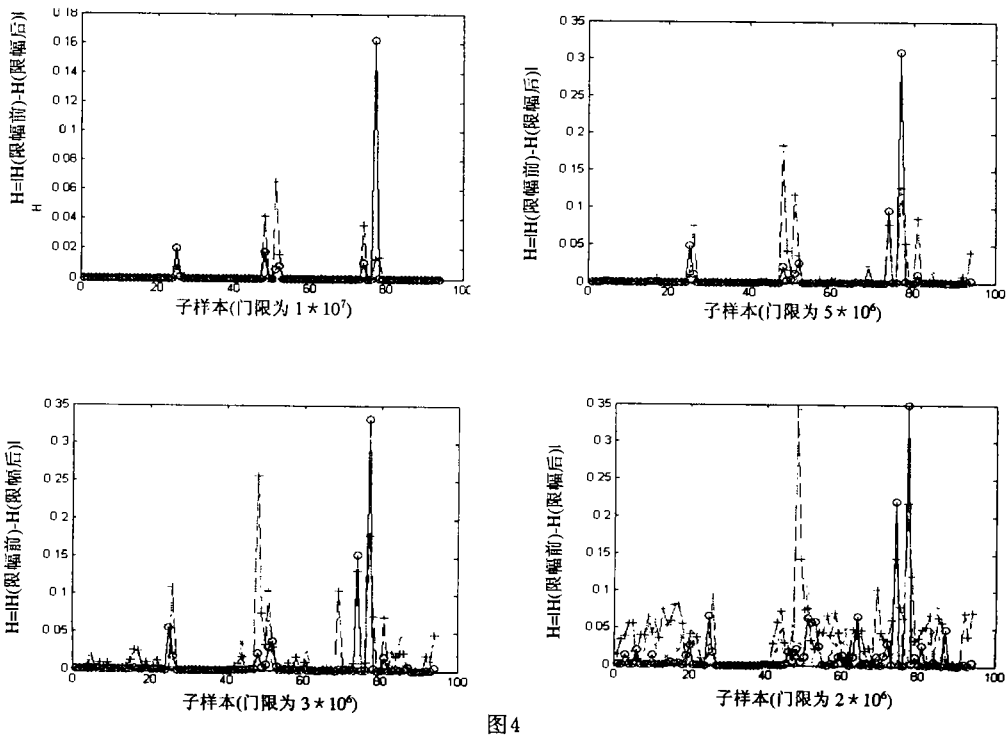

图4

维普资讯 http://www.cqvip.com

从上面可见对于阈值越低，H 在限幅前后的变化越明显，对于网络流量的异常(DDoS)，可以通过限幅比较前后(正常、异常)的 H 的变化，准确地检测攻击。由于聚集方差、周期图对限幅变化较为灵敏，又由于 R/S 的相对稳定的特点，我们得出了将三种方法混合的异常判断方法(见第4节)。

3. 网络流量的正常模型

将11天的网络流量数据 $X=\{X_k, k=1,2,\cdots\}$(以包的个数记)对天进行平均，滤去毛刺，然后通过聚集 $X_k^{(m)}=\frac{(X_{km-m+1}+\cdots+X_{km})}{m}(k=1,2,3,\cdots)$，得到含较少的白噪声信号的网络流量，再对这样的网络流量样本进行放大($Y((k-1)*m-1:k*m)=X_k^{(m)}$)，再用 $Y'(k)=Y(k)-X_k$ 表示流量中夹杂的白噪声信号，用 $Y'+Y$ 表示正常的网络流量模型，如图5所示。

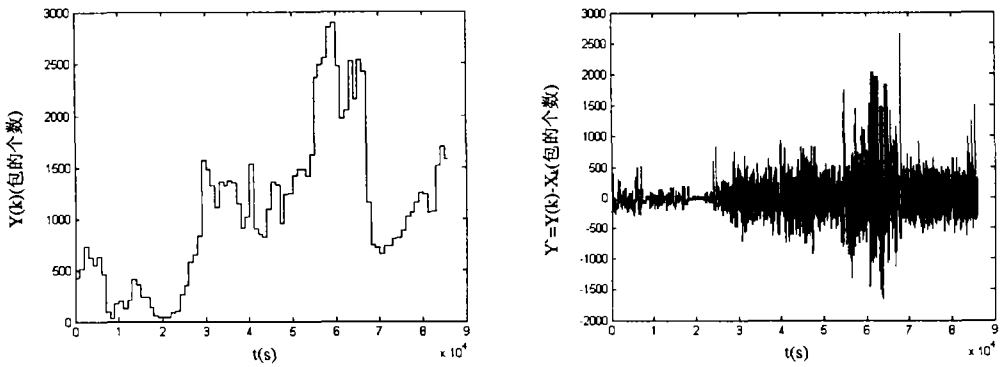

图5

4. DDoS 攻击、结合网络流量自相似性、正常模型的实时限幅检测方法

4.1 DDoS 攻击

我们在电子科技大学网络中心的206室子网网段进行攻击实验：从2003年4月11日00:00am 到2003年4月11日10:00am，采用了如图6左图所示的连续的攻击方式；从2003年4月14日20:30到2003年4月14日22:30采用了如图6右图所示的间断的攻击方式，攻击类型为 FakeUDP、FakeTCP(SYN)、FakeICMP 等。异常的网络流量见图7。

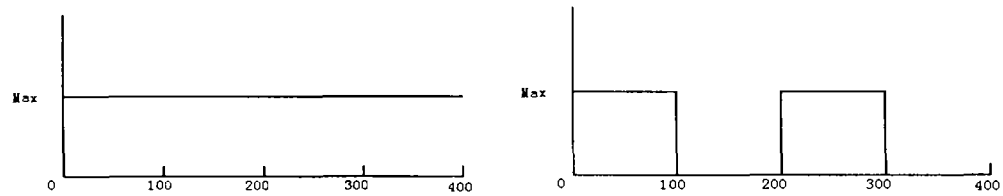

图6

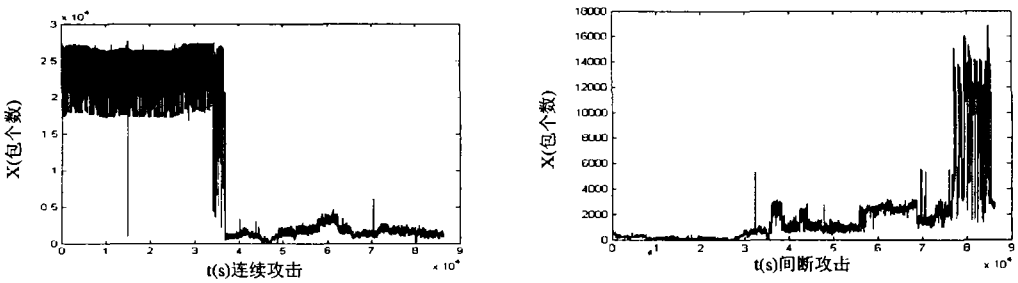

图7

4.2 结合网络流量自相似性、正常模型的实时限幅检测方法

1)对连续攻击图7左图：使用 $H_{差}=H_{异常}-H_{正常}$，再对 $H_{差}$ 在不重复的区间(大小为10)上做聚集，再取绝对值，得到 $H_{均差}$ 来描述攻击的可能性的大小。

$H_{均差}$	子区间			
	1	2	3	4
聚集方差	0.4622	0.3890	0.0059	0.0806
周期图	0.4523	0.1888	0.0848	0.0039
R/S	0.0286	0.0379	0.1046	0.0348

从上述可见，对于连续攻击，聚集方差、周期图有较好的区分度，而 R/S 区分度较差。

2)对连续攻击图7右图：使用 $H_{差}=|H_{限幅前}-H_{限幅后}|$，再对 $H_{差}$ 在不重复的区间(大小为10)上做积分，得到 $H_{均差}$ 来描述攻击的可能性的大小。

$H_{均差}$	子区间			
	1	2	3	4
聚集方差	0	0.0059	0	0.6943
周期图	0.0000	0.0103	0.0000	0.5749
R/S	0	0	0	Not-a-Number

维普资讯 http://www.cqvip.com

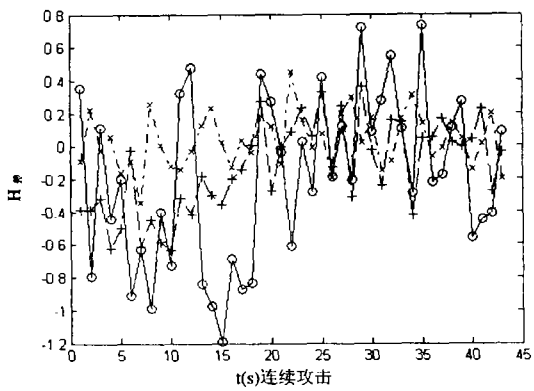

图8

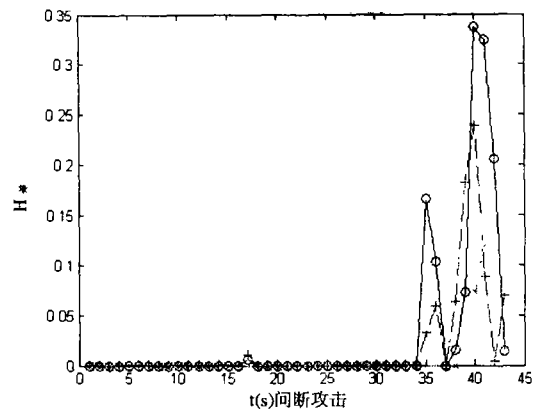

图9

由此可见，对于间断攻击，聚集方差、周期图有较好的区分度，而R/S区分度较差。

综合1)、2)，适当调整子区间的大小，使用自相似性分析中的聚集方差/周期图，可以识别网络流量异常现象，可以达到实时检测网络流量异常(DDoS)的目的。

5. 运用分布数据库统计分析

在前面的自相似性分析的基础上，分别对应于过去时段内、现在时段，对子网中的每个主机建立包头信息表，并依据不同的协议建立多个表(如IP，TCP，UDP)等，对各个表依据图10判决树的顺序进行统计分析。

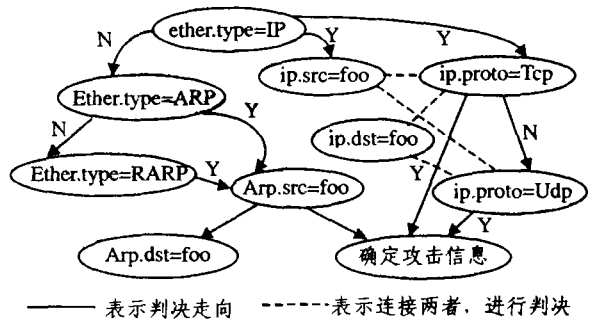

图10

6. 该新型方法与旧方法的对比

为了验证新方法，我们进行了一系列的实验，实验环境为：100兆以太网(两个子网)，两台100兆交换机，4台攻击计算机(Win2K)，1台检测计算机(RedHat Linux)。

网络拓扑图如图11所示。

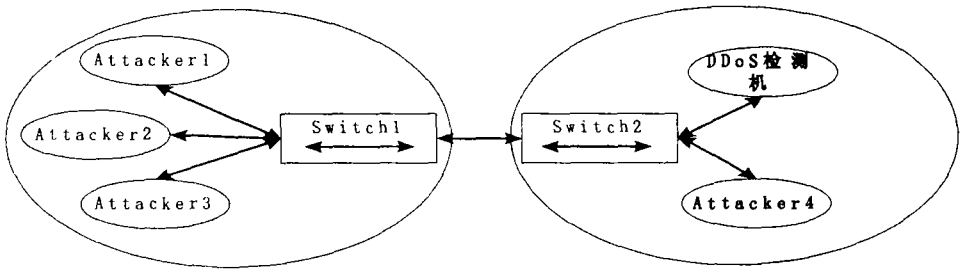

图11

分别使用攻击软件中的ICMP flood，SYN flood，UDP flood，TCP flood四种攻击手段进行各自5000次攻击测试。得出以下判断DDoS入侵的经验条件：1)连续攻击，令 $H_{均差}=0.43$；2)间断攻击，令 $H_{均差}=0.55$。在一定的时间区间内，若 $H(t)>H_{均差}$，可以判断有DDoS攻击的存在。得到表1。

表1

新的检测方法	ICMP flood	SYN flood	UDP flood	TCP flood
攻击检测率	86.3%	85.4%	86.9%	89.2%

自相似分析方法是基于网络流量自相似本质的检测方法，它和基于特征匹配的传统入侵检测方法在检测的基本原理上不同，也使用于不同的检测场合。自相似分析方法用于在受害计算机的子网上检测DDoS攻击，而传统方法是用于在黑客使用的计算机和控制计算机以及傀儡攻击计算机之间的通讯数据检测、驻留的控制程序检测和攻击程序检测。对受害计算机子网上的检测效率和过滤成功率都不高。表2显示了几种主流DDoS检测产品的检测成功率。

表2

攻击检测率 方法 / 攻击方式	NetST2103	FW3010PF	黑客愁	NetEye3.0
ICMP Flood	80%	---	77%	80%
SYN Flood	70%	80%	77%	---
UDP Flood	85%	---	77%	---
TCP Flood	75%	85%	77%	80%

由此可见，自相似性方法有较高的攻击检测率(即较小的漏判率)，比起传统方法有明显提高。

结论 本文提出了一种新型的基于网络流量自相似性的

维普资讯 http://www.cqvip.com

DDoS 入侵检测方法，该方法应用建立正常的网络流量模型、限幅，通过计算网络流量的自相似性(Hurst 参数)的变化，揭示了 DDoS 入侵对网络流量自相似性的影响，提出判断 DDoS 入侵的参数标准，并使用数据库对攻击进行定位。试验表明此方法适合作为检测 DDoS 入侵的依据并且比传统的 DDoS 入侵检测系统在检测的准确度上有较大提高。未来工作是：1、分析多种攻击的各自特点，确定各种不同网络流量异常与正常的临界点；2、我们分析的两种攻击都是流量稳定的，如何确定流量逐渐增大的攻击的特点；3、改进数据库的统计方法以提高检测速度，以便更好地适应实时检测的需要。

参 考 文 献

1 Leland W, Taqqu M, Willinger W, Wilson D. On the Self-Similar Nature of Ethernet Traffic. IEEE/ACM Transactions on Networking, 1994, 2(1): 1～5

2 Popescu A. Traffic Self-Similarity. In: Proc. of the IEEE Intl. Conf. on Telecommunications, Jun. 2001

3 Taqqu M S, Teverovsky V. On Estimating the Intensity of Long-Range Dependence in Finite and Infinite Variance Time Series. preprint Boston University, USA, 1996

4 Taqqu M S, Willinger W, Sherman R. Proof of a Fundamental Result in Self-Similar Traffic Modeling. Computer Communication Review, 1997, 27(2)

5 Meadows C. A formal framework and evaluation method for network denial of service. In: Proc. of the 12th IEEE Computer Security Foundations Workshop, June 1999

6 Willinger W, Taqqu M S, Sherman R, Wilson D V. Self-similarity through High Variability: Statistical Analysis of Ethernet LAN Traffic at the Source Level. IEEE/ACM Transactions on Networking, 1997, 5(1)

7 蔡弘，陈惠民，李衍达. 一种新型的通信网络突发业务建模方法—自相似业务. 通信学报，1997，18(11)：51～59

8 陈惠民，蔡弘，李衍达. 自相似业务：基于多分辨率采样和小波分析的 Hurst 系数估计方法. 电子学报，1998，7

9 Reiher P, Prier G, Michel S, Li J. Project D-WARD: DDoS Network Attack Recognition and Defense', UCLA. http://lever.cs.ucla.edu/ddos/, Aug. 2001

10 Erramilli A, Willinger W, Wang J L. Modeling and Management of Self-Similar Traffic Flows in High-Speed Networks. Network Systems Design, Gordon and Breach Science Publishers, 1999

11 Beran J, Sherman R, Taqqu M, Willinger W. Variable-bit rate video traffic and long-range dependence'. IEEE Trans Commun, 1995, 43: 1566～1579

(上接第74页)

此保证网络上传输的总是最新的数据。对于后一种情况，节点只发送应答帧对该情况进行说明，而不传送数据。另外，系统还对网络节点的响应设置了严格的时间限制，如果节点功能健全却不能在规定时间内发出数据，则该数据不再发出，但必须在该限定时间内发送应答帧并将相应位置1以向主控站说明。

另一方面，应用 ARTC 硬实时通信机制，正常情况下网络不会出现冲突，冲突属于网络通信故障。但是一旦网络发生冲突，按照以太网的冲突回退算法，可能引致网络通信混乱甚至瘫痪。由于现有的以太网芯片普遍支持全双工通信模式，因此通过驱动程序将网卡寄存器的相应位设置为全双工模式，则可屏蔽以太网 CSMA/CD 协议[5,6]。由此，在不改动硬件的前提下，一方面解决了由意外冲突而引发的网络故障问题，另一方面由于屏蔽了载波侦听功能也缩短了硬件发送的响应时间，并为用户使用基于 ARTC 硬实时通信建立支持软实时和非实时的综合网络提供了可能。

5. 流控

在 ARTC 的应用过程中，当数据从发送节点的发送缓冲区通过总线发往接收节点的接收缓冲区时，如果接收节点的接收缓冲区内的旧数据尚未被取走，则可能发生数据覆盖。这是由于发送节点向接收节点发送数据的速率快于接收节点从接收缓冲区中取走数据的速率。

解决数据覆盖一般是引入流量控制，使得发送方发出的数据块流量不超过接收方的接收处理速率。有两类常用的流控方法：反馈流控法和无反馈流控法。反馈流控法指接收方通过某种反馈机制，使发送方通过了解接收方的接收处理能力调节其发送速率，常用的等-停协议、滑动窗口协议都属于这一类。这类方法在解决非实时网络流控问题方面被证明是非常有效的，却较难保证网络数据实时传输，因而不太适用于实时网络。无反馈流控法指接收方按一固定的速率接收数据，发送方通过控制发送速率，使其始终不超过接收速率。这类方法在解决了流控问题的同时也较好地保证了数据的实时传输，不足之处是实现较为麻烦，需要全局考虑，要在满足整个系统的实时性前提下，对收发速率精确计算和设置。

ARTC 采用无反馈流控法避免出现接受方数据覆盖。每个节点都有一个接收任务按一定的时间间隔周期性地查询并移走接收缓冲区的数据，如果这一时间间隔设置过大，则可能导致接收缓冲区覆盖，而如果设置过小则会浪费 CPU 资源，并可能引起其它系统任务的阻塞，因此其关键就在于合理地设置节点的接收任务运行周期。实时系统中消息被分为周期消息和非周期消息，节点的发送速率受总线调度表控制。对于周期消息来说，其在总线调度表中获得调度的时间间隔是确定的，即等于其周期，只要接收任务的运行周期小于消息的周期就不会出现接收方数据覆盖[3]。由于在 ARTC 消息调度过程中所有的非周期消息都被转化成了周期消息，因此我们只需按照周期消息的方式进行处理。现场级应用中，同类终端的工作任务通常是相同的，因此在 ARTC 初始化时，将对每类节点的每一条相关消息分别进行分析，并取其相关消息的最小周期作为接收任务的运行周期，便可解决接收方数据覆盖问题，实现网络的合理流控。

总结 本文从系统结构、多级自检、监控管理、流控以及故障处理等方面，提出了基于以太网的硬实时通信系统 ARTC 系统化的可靠性解决措施，为把 ARTC 应用于现场总线控制领域奠定了坚实的基础。由于现场总线的历史成因以及应用环境存在较大差异，用户对系统的实用性、可靠性、价格以及终端设备属性等的要求不尽相同。因此我们在对 ARTC 系统研究、设计的同时，尽可能地兼顾用户应用中的不同需求，在网络构建、模块设计和终端接入等方面为用户提供足够的灵活性和选择余地。

实时网络的可靠性研究是一个长期而漫长的过程，在实际应用中我们将致力于对上述策略的不断修正和完善。

参 考 文 献

1 陈慧，熊光泽，杨仕平. 基于以太网的硬实时通信技术 ARTC. 计算机科学，2003(7)

2 An Interpretation of MIL-STD-1553B. http://www.1553.com/1553interp.htm

3 王志平，熊光泽，刘锦德. 1553B 实时网络流控问题研究. 计算机科学，1999，26(7)：80～82

4 Tanenbaum A S. Computer Networks. Prentice Hall, 1996

5 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications. http://standards.ieee.org/

6 Realtek Full-Duplex Ethernet Controller with Plug and Play Function (RealPNP). http://www.realtek.com.tw/