一种主动防御的网络传输系统

胡汉平, 梁 兴, 张宝良
(图像信息处理与智能控制教育部重点实验室, 华中科技大学图像识别与人工智能研究所, 湖北武汉 430074)

摘 要: 本文在注重提高服务安全性的同时, 也兼顾了满足区分服务的一般要求, 提出一种基于主动防御的自适应端系统模型, 在此基础上通过基于自相似序列理论的网络预测、模糊 C-均值算法实时地对传输服务器状态进行聚类, 根据聚类结果和对用户请求的分级, 给出了一种随机混排的自适应负载调度方法. 该方法优化系统资源分配, 保证了数据传输的安全性和可靠性. 此外, 该模型不依赖原操作系统的实现, 具有可移植和可扩展的特点.

关键词: 数据安全; 负载动态分配; 主动防御; 网络测量和预测
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2005) 04-0701-05

A Proactive-Defense Network Transmission System

HU Han-ping, LIANG Xing, ZHANG Bao-Liang
(*Institute of Image Recognition and Artificial Intelligence, Huazhong University of Science and Technology, Wuhan, Hubei 430074, China*)

Abstract: In order to enhance the security of web service as well as to support the differentiated service, the paper puts forward an adaptive model which is based on active defense strategy. It uses a predictive network model on base of self-similar sequence theory to estimate current states of transfer servers in end-system, then classifies them with Fuzzy-C-means clustering method. Finally we bring forward a load balancing algorithm that is founded on the classification results and grading users' requests. In that way, it optimizes the allocation of system resources and ensures data security and reliability. Moreover, this model, not dependent on the original operating system, is transplantable and extensible.

Key words: data security; dynamical load distribution; active defense; measurement and prediction

1 引言

随着网络应用的普及以及日益复杂化, 互联网的效率和安全问题渐渐成为关注的焦点. 于是研究者提出了多种方案加以改进, 比如, 有的系统在一个接入路由器上提供另外一个拨号连接的低速接入链路来提高负载能力, 但由于其接入点仍然是通过一个路由器接入到 Internet, 对于抵御网络攻击没有本质意义; 而有的系统通过多 ISP 接入到网络, 按照路由协议进行负载均衡, 这实际上是一种资源的浪费. 因为一般的路由协议只提供了可到达信息, 而没给出流量控制、区分服务等有关协议的说明和具体调度措施, 这使得系统性能不会有明显改善. 更严重的是, 它们几乎都沿用了被动防御策略. 但是, 由于网络的攻击具有无边界性、蔓延性和隐蔽性等特点, 而被动防御策略是一种非对称的攻守(往往守方需要考虑所有的攻击可能, 而攻方却只需从所有的可能方法找出一个即成功), 导致系统的可靠性和安全性较低.

为此, 本文提出了基于主动防御策略的接入系统模型及其实现技术[1]. 该接入系统模型为多点接入、多层服务、分级调度的三层结构模型(如图 1 所示). 它不仅可通过自动检测和动态分配系统资源, 保证了用户对服务质量的不同要求, 而且基于主动防御策略, 根据业务数据的不同安全级别, 在接入的过程中注入了一定数量的、与真实业务数据具有相同统计特性的诱骗报文, 通过在不同接入服务器之间随机切换传输流, 经过不同 ISP 接入因特网, 由此保证了接入系统的通信连接不会因为单点失效而中断, 有效地预防了针对特定主机和特定端口的窃听和攻击.

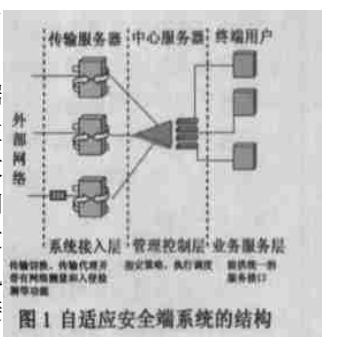

图 1 自适应安全端系统的结构

在系统接入层配置了传输切换、传输代理、网络测量和入侵检测等功能模块. 传输代理、网络测量和入侵检测等模块在应用层上实现; 传输优化、安全路由选择则在网络层上实现. 这点与普通网关几乎一致, 大量已有软件和协议不加修改, 就可应用到传输服务器上. 传输切换和传输代理支持区分服务, 提供传输中继以及与外部网络的透明连接. 在管理控制层配置了通信控制服务器. 作为接入系统的调度和控制中心, 根据

收稿日期: 2004-04-26; 修回日期: 2004-11-24
基金项目: 国家自然科学基金(No. 90104029)

来自接入层的网络状态信息和业务层的应用的信息以及业务的属性,制定优化调度的策略,提供满足质量和安全要求的调度服务.在业务服务层提供了一种统一的服务说明和接口标准,配置了邮件服务器、对业务数据包进行安全处理等多种不同的应用服务系统.

本文的其余部分是这样安排的:在本文的第二部分中,根据对接入服务器的实时测量与预测,据此按一定聚类算法将接入服务器动态地划分成 n 类,从而为系统的自适应负载均衡的调度提供了决策基础;在第三部分中,为了隐藏真实报文信息,根据网络的状态信息和业务数据的不同安全级别,在接入的过程中注入了一定数量的、与真实业务数据具有相同统计特性的诱骗报文,并提出多点接入的随机切换机制及其自适应负载均衡的调度方法,与传统的无状态静态调度算法轮叫调度(RR)算法、加权轮叫调度(WRR)算法和最小连接的动态调度算法(LCC)等[2]相比,本调度算法不仅提高了传输服务器系统的效率,而且当系统中单个传输服务器出现故障时,其效率没有受到较大影响;在第四部分中,为完成代理对象的随机切换,在维持 SOCKSv5 原有语义的兼容性基础上进行了一定扩展,根据该扩展协议,实现了多点接入的随机切换机制及其自适应负载均衡的调度方法;在第五部分中,给出了相应的实验结果,并将该结果与其他方法进行比较分析.

2 端系统性能的预测与分类方法

根据实际情况,可以对接入层的测量做这样的三点假设:测量的粒度为秒粒度;传输服务器(被测对象)的状态参数变化是渐变而非突变;正常情况下传输服务器的数据采样不明显改变自身的性能.

在对传输服务器的性能状态进行跟踪监测的同时,要求传输服务器每隔 T 秒将监测结果反馈给管理服务器.然而这些监测数据不可避免地带有干扰的因素,为此需要人为对其进行过滤处理:首先对原始序列 $x_0, x_1, x_2, \cdots, x_m$,求出均值 $E(x)$,然后检查每个样本 x_t $(t=1,2,3,\cdots,m)$,如果 $|x_t - E(x)| \leqslant \alpha E(x)$ (α 称为平滑系数),保留该样本点,否则舍去.下面将用 x 表示处理过的样本.

网络业务流在秒粒级上具有自相似结构[3],分形插值函数能较好地拟合了网络性能的波动变化.因此,本文采用基于自相似序列理论的网络预测模型(1)对网络业务流进行预测:

$$\begin{cases} y^t_{m+1} = \left(\dfrac{x_t}{x_{m+1}}\right)^{-H} y_t, \quad t = 0, 1, \cdots, m \\ y_{m+1} = \dfrac{1}{m+1}\displaystyle\sum_{t=0}^{m} y^t_{m+1} \end{cases} \tag{1}$$

上式中 x_t $(t=1,2,\cdots,m)$ 为预处理过的序列点,H 为 Hurst 系数.由于本测量中的预测方法对数值精度并不敏感,所以通过经典的 R/S 统计分析[4]方法,由式(2)可获得该系数 H:

$$E[R(m)/S(m)] \sim cm^H \tag{2}$$

式中 $S(m)$ 为样本序列的方差.详细算法和有关迭代函数系吸引子的具体描述可参见文献[4].

类似上述过程,还能对网络系统的利用率、吞吐率和可用带宽等性能参数进行测量及预测,从而获得了端系统中传输服务器的性能状态参数 $x_p: [x_{p1}, x_{p2}, \cdots x_{pr}, \cdots, x_{pR}]^T$.下面本文利用模糊 C-均值聚类分析算法——FCM[5],根据对传输服务器的性能状态参数的预测结果,将传输服务器分为 Q 类.

设每一聚类的权值为 $e \in [1, \infty]$,接入层共有 P 个传输服务器,并定义传输服务器性能状态的目标函数 $J(U, V)$ [5,6]

$$J(U, V) = \sum_{p=1}^{P}\sum_{q=1}^{Q} (u_{pq})^e (d_{pq})^2 \tag{3}$$

其中 $\boldsymbol{U} = [u_{pq}]$ 为置信系数矩阵,

$$u_{pq} \in [0, 1], \quad \sum_{q=1}^{Q} u_{pq} = 1$$

d_{pq} 为服务器 p 隶属于类 q 的度量指标[7],且

$$d_{pq}^2 = \| \boldsymbol{X}_p - \boldsymbol{V}_q \|^2 = (\boldsymbol{X}_{pr} - \boldsymbol{V}_{qr})^T \boldsymbol{A} (\boldsymbol{X}_{pr} - \boldsymbol{V}_{qr}) \tag{4}$$

在式(4)中,$\boldsymbol{V}_q = [v_{q1}, v_{q2}, \cdots, v_{qR}]$ $(q = 1, 2, 3, \cdots, Q)$ 为各类的聚类中心.在本文中,可不失一般性地假设 $Q = 3$,并设其各自的中心 $\boldsymbol{V}_1$、$\boldsymbol{V}_2$ 和 $\boldsymbol{V}_3$ 与原点[0, 0, …, 0]的加权距离分别为 ω_1、ω_2 和 ω_3.又如 $\omega_1 \geqslant \omega_2 \geqslant \omega_3$,则将 T_1、T_2 和 T_3 分别定义为最优状态、次优状态和最差状态.

3 端系统的自适应随机调度方法

在上节中对传输服务器的状态实时地进行了预测和分类.在此基础上,本节将进一步讨论根据不同用户所提出的不同要求的业务请求,提出具有自适应特点的随机性调度方法.

本文的重点在于研究端系统的安全性,并兼顾满足区分服务的一般要求,将用户请求分为三个级别:A(安全传输)级、B(高速传输)级和 C(普通传输)级.根据需求还可将 A 级业务进一步细化为 τ(在本文中,不妨设 $\tau = 3$)个安全等级.对于 A 级的请求,基于主动防御策略,在数据传输过程中,需要根据其安全等级,按比例随机性地加入一定数量的虚假诱骗报文.在本文中,在概率统计的意义上,将真、假报文的比例范围随着业务安全强度和网络综合状态的变化设定为:1:1~1:5.同时,还需要随机性地选择 T_2 类或 T_1 类传输服务器发送这些报文(虚假诱骗报文或发真实报文),使得攻击者无法跟踪到发送真实报文的传输服务器,以提高报文传输的安全性和可靠性;B 级请求主要是针对视频流传输等实时数据量较大的请求,对此业务则主要是满足低延时和最少抖动的要求,因此,采用 T_1 类传输服务器发送 B 级数据报文并根据负载状况切换服务器;C 级请求为普通业务请求,为保证与原有网络的兼容,可采用"尽力而为"的传输方式.因此,采用 T_1 类、T_2 类和 T_1 类传输服务器发送 C 级数据报文并根据负载状况切换服务器.需要指出的是:上述分级并不是唯一的,若有需要的话,还可以分成更多的级别来满足不同用户的需求.对于 B 级和 C 级业务,在其他相关文献中已有比较详细的介绍,所以在下面将只对 A 级业务做进一步地讨论.

为了使真、假报文的比例值得到控制,管理服务器为每一业务分别建立对应的长度为 γ 的待发数据包队列(因为数值 1~6 的最小公倍数等于 60,所以取 $\gamma = 60$).当需要发送某一安全级的业务数据时,系统采用一个周期不超过 2^Γ(由是降低模运算的计算复杂度)的线性同余随机数发生器[8](其数学表达式如以下式(5)所示),当其产生的伪随机数 Y_n 大于预定

阈值β时, 就将该业务数据中的某一真实数据包加入相应的队列 L, 否则将一虚假诱骗数据包加入队列 L; 当随机数发生器所产生的下一伪随机数 Y_{s+1} 大于 β 时, 将该业务数据中的下一真实数据包加入队列 L, 否则将另一虚假诱骗数据包加入队列 L. 上述过程重复 ¥ 次后, 即完成对应于某一业务中的某一待发数据包队列的建立过程. 对于非安全级业务数据, 在为其建立队列长度过程中, 只要将业务数据中(真实)数据包依次加入相应的队列即可. 式(5)中, a 为乘子(乘数), c 为增量, 均为非负整数; Γ 为正整数, 并且 $2^{\Gamma} > ¥$; β 为小于 2^{Γ} 的正整数. 在本文中, 通过调整 β 值, 使得在概率统计的意义上保证将真、假报文的比例范围为: 1∶1~ 1∶5.

$$Y_s = (aY_{s-1} + c)(\mathrm{mod}\ 2^{\Gamma}), \quad S = 1, 2, 3, \cdots, ¥ \qquad (5)$$

在上述分析和讨论的基础之上, 本文将给出调度算法. 该算法在将某一业务数据分成多个数据包后, 为该业务建立长度为 ¥ 的待发数据包队列; 根据对传输服务器进行分类的结果, 为不同的传输服务器分别赋予不同的权值 W 及发包行向量 $\boldsymbol{H}$, 由此构造一个能反映网络性能状态的调度矩阵, 该矩阵与业务级别无关. 调度算法将依据调度矩阵选择传输服务器来发送数据包队列中的数据包.

假设对传输服务器进行分类的结果为: T_1 类传输服务器有 N_1 个; T_2 类传输服务器有 N_2 个和 T_3 类传输服务器有 N_3 个. 并且 T_1、T_2、T_3 类聚类中心到坐标原点的距离(即性能状态综合比)分别为 ω_1、ω_2、ω_3. 为了简化计算, 对 ω_1、ω_2 和 ω_3 分别向下取整后得 W_1、W_2 和 W_3, 即 $W_1 = [\omega_1]_f > W_2 = [\omega_2]_f > W_3 = [\omega_3]_f$(算子$[\cdot]_f$ 表示向下取整运算). 本文所提出的 RS-WRR 算法为 T_1、T_2、T_3 类传输服务器分别建立与之对应的发包行向量 $\boldsymbol{H}_{1,i} = [\delta_{i,0}, \delta_{i,1}, \cdots, \delta_{i,k}, \cdots, \delta_{i,¥}]\ (i = 1, 2, \cdots, N_1)$、$\boldsymbol{H}_{2,j} = [\delta_{j,0}, \delta_{j,1}, \cdots, \delta_{jk}, \cdots, \delta_{i,¥}]\ (j = 1, 2, \cdots, N_2)$ 和 $\boldsymbol{H}_{3,l} = [\delta_{l,0}, \delta_{l,1}, \cdots, \delta_{lk}, \cdots, \delta_{l,¥}]\ (l = 1, 2, \cdots, N_3)$, 其中 $\delta_{i,k}$、δ_{jk}、$\delta_{lk} \in \{0, 1\}$(“1”表示此次由对应的传输服务器发送从队列中取出的数据包,“0”表示对应的传输服务器此次轮空不发送数据包). 在发包行向量 $\boldsymbol{H}_{1,i}\ (i = R_1 + 1, R_2 + 2, \cdots, N_1)$ 中, δ_{ik} 为“1”的个数可以由式(6)和式(7)计算得到. 即, 在 R_1 个行向量 $\boldsymbol{H}_{1,i}\ (i = 1, 2, \cdots, R_1)$ 中, δ_{ik} 为“1”的个数为 $I_1 + 1$; 在 N_1-R_1 个行向量 $\boldsymbol{H}_{1,i}\ (i = R_1 + 1, R_1 + 2, \cdots, N_1)$ 中, δ_{ik} 为“1”的个数为 I_1; 在发包行向量 $\boldsymbol{H}_{2,j}$ 中, δ_{jk} 为“1”的个数可以由式(8)和式(9)计算得到. 即, 在 R_2 个行向量 $\boldsymbol{H}_{2,j}\ (j = 1, 2, \cdots, R_2)$ 中, δ_{jk} 为“1”的个数为 $I_2 + 1$; 在 N_2-R_2 个行向量 $\boldsymbol{H}_{2,j}\ (j = R_2 + 1, R_2 + 2, \cdots, N_2)$ 中, δ_{jk} 为“1”的个数为 I_2; 在发包行向量 $\boldsymbol{H}_{3,l}$ 中, δ_{lk} 为“1”的个数可以由式(10)和式(11)计算得到. 即, 在 R_3 个行向量 $\boldsymbol{H}_{3,l}\ (l = 1, 2, \cdots, R_3)$ 中, δ_{lk} 为“1”的个数为 $I_3 + 1$; 在 N_3-R_3 个行向量 $\boldsymbol{H}_{3,l}\ (l = R_2 + 1, R_2 + 2, \cdots, N_2)$ 中, δ_{lk} 为“1”的个数为 I_3. 在式(6)~(11)中, 对于 A 级业务请求, $\xi_2 = 0$, $\xi_1 = 1$; 对于 B 级业务请求, $\xi_1 = \xi_2 = 0$; 对于 C 级业务请求 $\xi_2 = \xi_1 = 1$.

$$I_1 = [¥/(N_1 \cdot W_1 + \xi_1 \cdot N_2 \cdot W_2 + \xi_2 \cdot N_3 \cdot W_3)]_f \cdot W_1 \qquad (6)$$

$$R_1 = (¥ - I_1 \cdot N_1) \cdot (1 - \xi_1) \cdot (1 - \xi_2) \qquad (7)$$

$$I_2 = [(¥ - I_1 \cdot N_1)/(N_2 \cdot W_2 + \xi_2 N_3 \cdot W_3)_2]_f \cdot W_2 \cdot \xi_1 \qquad (8)$$

$$R_2 = (¥ - I_1 \cdot N_1 - I_2 \cdot N_2) \cdot (1 - \xi_2) \cdot \xi_1 \qquad (9)$$

$$I_3 = [(¥ - I_1 \cdot N_1 - I_2 \cdot N_2)/(N_3 \cdot W_3)]_f \cdot W_3 \cdot \xi_2 \qquad (10)$$

$$R_3 = (¥ - I_1 \cdot N_1 - I_2 \cdot N_2 - I_3 \cdot N_3) \cdot \xi_2 \qquad (11)$$

需要说明的是: 根据策略——保证三类服务的传输等级; 保证所有服务器发送等长(必须为整数)的数据包链; 保证负载的综合均衡, 可确定上述(6)~(11)公式.

在满足上述条件的前提下, 原则上可随机地设置 δ_{ik}、δ_{jk} 的值为“1”或者“0”, 但考虑到负载的平衡性, 应尽可能地使在行向量中“0”、“1”是均匀排列的. 只要将 $(N_1 + N_2 + N_3)$ 个传输服务器的发包向量分别按与相应类别的传输服务器一一对应关系进行组合, 就可以得到当前调度矩阵 $\boldsymbol{M}$. 在该矩阵 $\boldsymbol{M}$ 中, 元素“1”表示此次由对应的传输服务器发送从队列中取出的数据包, 元素“0”表示对应的传输服务器此次轮空不发送报文. 显然, 该矩阵中“1”的个数之和为 ¥, 并且其行、列数分别为 $N_1 + N_2 + N_3$、$I_1 + I_2 + I_3$. 随着网络性能状态的变化, 矩阵 $\boldsymbol{M}$ 也将随之变化, 但其中“1”的个数恒等于 ¥(队列长度).

为提高系统资源的利用率, 本文对上述发包过程进行了并行处理, 在管理服务器上为每一传输服务器建立一个队列, 用实节点存放数据报文, 而用虚节点表示一次轮空. 同时, 利用线程的并行特点, 为每一队列启动一个线程, 由线程自行根据队列进行管理, 如判断发包或者轮空. 该调度方法对同一队列中数据包的处理是并行的, 而对队列之间数据包的处理是串行的.

4　接入系统的实现技术

为了实现上述随机性调度方法, 在维持其原有语义的兼容性基础上, 本文对 SOCKSv5 协议进行了一定扩展, 引入了连接场景(connection Context)的概念. 连接场景是由连接记录元构成的列表, 用于多个代理之间的通信切换管理, 软件模型如图 2 所示. 连接记录元 *CONN_ITEM* 的定义为: 〈*ID*, *sourceIP*, *sourcePort*, *destIP*, *destPort*, *STATUS_DATA*〉, 其中 *ID* 为连接标识号, *STATUS_DATA* 是该连接的状态参数, 这些参数根据不同需求进行调整. 系统各个传输实体以连接记录元的形式保留各个连接的状态, 集群系统根据连接记录元进行切换, 这些连接记录元构成了统一的通信场景.

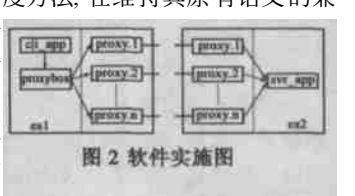

图 2 软件实施图

将切换过程分为两个步骤: 切换请求和建立连接请求, 对应指令为 *E_SWITCH* 和 *E_RCONNECT*, 它们是通过扩展 SOCKSv5 请求类指令得到的. 类似地, 扩展定义了 *E_SWITCHBIND*、*E_REBIND* 命令; 相应地, 定义了它们应答指令 *E_REPLY*. 扩展的指令格式为:

VER	CMD	RSV	ATYP	DST. ADDR	DST. PORT	C_ITEM1	C_ITEM2
1	1	X'00	X'00	X'0000	X'0000	Variable	Variable

表中各字段含义如下:

- *VER*　protocol version: X'05'
- *CMD*

- *E_SWITCH* *X*'05
- *E_RECONNECT* *X*'06
- *E_SWITCHBIND* *X*'07
- *E_REBIND* *X*'08
- *RSV* explanation of *SLA*
- *ATYP* compatible with SOCKSv5
- *DST.ADDR* *X*'0000, keep compatibility
- *DST.PORT* *X*'0000, keep compatibility
- *CONN_ITEM*1, *CONN_ITEM*2 connection element

接入系统在会话层拦截传输连接. 通过表示会话有关状态的连接元实现会话管理, 一个连接元中的状态数据有: 已写的字节数、读的字节数等. 而用户也可以对连接元域进行扩展, 以适应不同服务定义, 提高系统的灵活性. 用户的传输需求通过保留字 *RSV* 来说明, 本系统将 *RSV* 定义为 *SLA* 字段, 即服务级协商字段. 因此, 本系统实现的是一种隐式 *SLA*. 传输代理可以根据该 *SLA* 的说明, 确定应用数据流所需要的传输服务级别. 接入系统使用上述指令进行会话切换过程如图 3 所示.

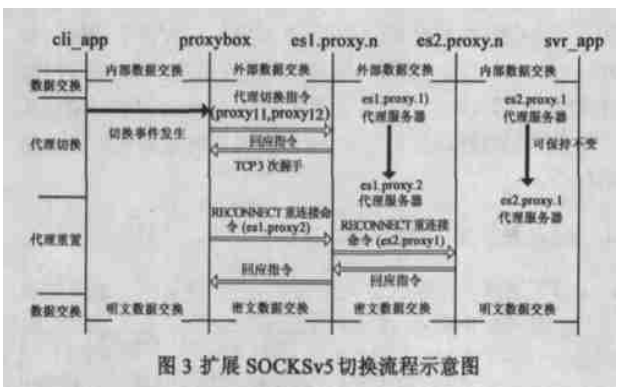

图 3 扩展 SOCKSv5 切换流程示意图

有安全需求业务的传输过程主要为: 发端通信控制器接到传输请求后, 根据用户要求, 按照预定规则确定服务级别, 由服务级别保留字段表示; 然后对任务进行编号、数据分块. 通信控制器按规则"随机"地选出若干传输代理, 向目端发送连接请求; 收到成功响应后, 选择其中一个称为"主"机的代理传送真实报文, 其他传输服务器作为"僚"机发送诱骗报文. 上述过程采用 SOCKSv5 中的连接指令, 并在连接场景中记录连接状态. 在某一时刻如需切换, 发端通信控制服务器"随机"选择某一僚机作为主机, 将下一个真实报文通过该主机的连接进行传输. 其他传输服务器作为僚机, 发送诱骗报文. 同时, 系统可以动态地改变传输数据端口. 重复上述过程, 直至全部任务发送完毕.

5 实验结果与分析

本实验中的接入系统采用了 6 台传输服务器 $S_i(i=1,2,\cdots,6)$ 和 1 台管理服务器, 其传输服务器的硬件系统配置基本上是相同的: P4 1.6G 处理器、3COM 10MB 网卡. 在实验中分别采用了普通的 WRR 算法和本文所提出的方法对接入系统中的传输服务器进行了调度, 分别传输具有安全要求的(真、假报文的比例设定为: 1:1)、一定长度(100KB、1MB、10MB 和 40MB)的文件, 然后对其所需要的时间开销进行了比较.

对接入系统中的传输服务器的性能状态参数分别进行了四组测量, 并根据其状态参数: 利用率、吞吐率和可用带宽, 采用上述模糊聚类算法对传输服务器进行了分类, 其结果如表 1 所示.

表 **1** 在四组测量中接入系统性能状态的分布情况

组数 / 类别	1	2	3	4
T_1	S_1, S_3	S_1	S_1, S_3	S_1
T_2	S_2, S_4, S_6	S_2, S_3, S_6	S_2, S_6	S_3, S_6
T_3	S_5	S_4, S_5	S_4, S_5	S_2, S_4, S_5

通过计算可以发现: 在 4 组测量中第 3 组测量数据的类中心偏移量最小, 所以将该组的分类结果作为进一步调度依据. 在第 3 组测试结果中, 描述 T_1 类和 T_2 类传输服务器($N_1=2$; $N_2=2$)综合性能的参数分别为: $W_1=3$; $W_2=1$. 根据式(6)~(11)可分别计算出: $I_1=21$; $I_2=9$; $I_3=0$; $R_1=R_2=R_3=0$. 根据上述方法可构造出调度矩阵 $\boldsymbol{M}$ 如下:

$$\begin{bmatrix} 1\,1\,1\,0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,1\,0\,1\,0\,1\,1\,0\,1\,1\,1\,0\,1\,0\,1\,0\,1\,1\,1 \\ 1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1 \\ 0\,1\,1\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,1 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 1\,0\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,1\,0\,0\,1 \end{bmatrix}_{630} \begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \\ S_5 \\ S_6 \end{bmatrix}$$

表 **2** 采用两种算法所用时间的比较

文件 / 算法	100kB	1MB	10MB	40MB
RS-WRR	0.109	1.258	12.020	113.01
WRR	0.085	1.246	14.567	127.01
故障时	0.129	1.304	15.020	129.01

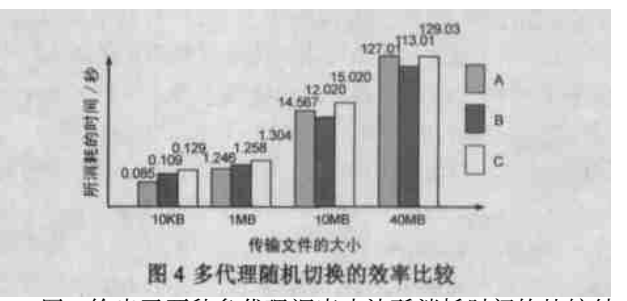

图 4 多代理随机切换的效率比较

图 4 给出了两种多代理调度方法所消耗时间的比较结果, 其中 A 和 B 分别表示在正常情况下完成随机切换调度传输和非切换调度传输所消耗的时间, C 表示在某一代理失效的情况下完成随机切换调度传输所消耗的时间. 显然, 完成两种切换调度传输所需时间几乎相同. 因此, 在不过多增加系统资源开销的情况下, 本文提出的调度方法明显地提高了数据传输的安全性和可靠性, 改善了服务质量.

综上所述, 本文所提出的接入系统模型及其实现技术具有如下特点: 采用了所扩展的支持多个"流"切换 SOCKSv5 协议, 根据反映应用要求和网络状态的自适应负载均衡调度矩阵, 使得报文随机地经由不同的 ISP 接入互联网, 由此不仅保证了通信连接不会因为单点失效而中断, 有效地防止了针对特定端口的攻击, 而且保证了用户所要求得接入服务质量; 在

接入过程中,根据应用要求和网络状态,注入了一定比例的由“僚”机发送的诱骗报文,“主”机与“僚”机动态地“随机”切换,使地攻击者难以对“主”机进行跟踪,防止攻击者对通信流量的监听,提高传输过程的隐蔽性.

参考文献:

[1] 胡汉平,张宝良,陈翔,朱海燕. 基于主动防御的传输集群模型[A]. 网络与信息安全 2002 年度学术交流论文集[C]. 北京: 2003.1: 346- 353.

[2] 章文嵩. LVS 集群的负载调度[DB]. IBM' s resource for developers, http://www900. ibm. com/developerWorks/cn/linux/cluster/lvs/part4/index. shtml, 2002, 5.

[3] 陈惠民,蔡弘,李衍达. 突发业务的多重分形建模及其参数估计[J]. 电子学报, 1999. 27(4): 19- 23.
CHEN Huimin, CAI Hong, LI Yanda. Multifractal traffic modeling and its parameter estimation[J]. Acta Electronica, 1999, 27(4): 19- 23.

[4] Fei Xue, Ben Yoo. Self-similar traffic shaping at the edge router in optical packet-switched networks[A]. IEEE International Conference on Communications[C]. Sanfransico: IEEE, 2002.4. 188- 200.

[5] 陈遵德. 基于模糊 C 均值与 RS 理论结合的模式分类方法及应用[J]. 计算机工程. 2003. 29(1): 64- 66.

[6] Egan M A. Locating clusters in noisy data: a genetic fuzzy c-means clustering algorithm[A]. Fuzzy Information Processing Society[C]. NewYork: NAFIPS, Conference of the North American. 1998. 178- 182.

[7] 徐月芳. 基于遗传模糊 C-均值聚类算法的图像分割[J]. 西北工业大学学报, 2002. 24(4): 549- 553.

[8] 刘涵哲. 随机整数序列和随机实数序列的实现方法[J]. 现代计算机, 1999, 12(8). 37- 38.

作者简介:

胡汉平　男, 1960 年生于湖北省武汉市, 教授、博士生导师, 主要从事信息安全、智能信息处理系统等方面的研究, 已发表学术论文 60 余篇, 并已获得多项国家及省部级技术发明和科技进步奖. E-mail: hphu@mail. hust. edu. cn.

梁　兴　男, 1979 年 2 月生于湖北省宜昌市, 2002 年毕业于华中科技大学, 获学士学位, 现为华中科技大学图像识别与人工智能实验室在读硕士, 主要研究兴趣网络传输安全, 动态身份认证和入侵检测.