网络安全的综合风险评估*)

赵冬梅[1,2] 张玉清[3] 马建峰[1]

(西安电子科技大学计算机学院 西安 710071)[1] (河北师范大学计算中心 石家庄 050016)[2]

(中科院研究生院国家计算机网络入侵防范中心 北京 100039)[3]

摘 要 本文对网络安全风险评估提出了一种新的综合风险评估方法。采用AHP方法与模糊逻辑法相结合的方法进行风险评估,并根据网络安全风险评估的实际情况对AHP方法与模糊逻辑法进行了改造。应用模糊逻辑法对各因素的评判不是直接评价其重要度,而是将各风险因素从概率方面、从影响方面、从不可控制性方面分别进行评判。先用AHP方法将风险评估分为三层,在确定第三层各风险因素的排序权向量时采用模糊逻辑法。最后利用AHP方法求出各风险因素的综合风险权重。通过实例分析可知,该方法可以方便地用于网络安全风险评估,实验结果符合实际。

关键词 风险评估,AHP法,模糊逻辑法

Comprehensive Risk Assessment of the Network Security

ZHAO Dong-Mei[1,2] ZHANG Yu-Qing[3] MA Jian-Feng[1]

(School of Computer Science and Engineering, Xidian University, Xi'an 710071)[1]

(Computer Center of Hebei Normal University, Shijiazhuang 050016)[2]

(National Computer Network Intrusion Protection Center, GSCAS, Beijing 100039)[3]

Abstract A new comprehensive risk assessment method is introduced to the estimation of the network security risk. The method, which combines AHP method and fuzzy logical method, is applied to the risk assessment. AHP method and Fuzzy logical method are altered according to the actual condition of the network security risk assessment. Applying fuzzy logical method, the important degree of each actor is judged in the aspects of the probability, the influence and uncontrollability, not judged immediately. The risk assessment is carved up 3 layers applying AHP method, the sort weight of the third layer is calculated by fuzzy logical method. Finally, the comprehensive risk weight is calculated by AHP method. The study of the case shows that the method can be easily used to the risk assessment of the network security. The results are in accord with the reality.

Keywords Risk assessment, AHP method, Fuzzy logical method

1 引言

随着计算机网络的飞速发展,网络安全逐渐成为人们关注的焦点,而网络安全实践的起点是对网络系统的风险评估。风险是客观存在的潜在威胁对系统的脆弱点进行攻击,从而造成了对系统的破坏和损失。风险评估是分析和说明风险的过程,它由三个基本活动组成:第一,决定评估的范围和方法;第二,收集和分析数据;第三,说明风险分析结果。

目前国内外关于风险评估的方法有许多种。可分为基于概率论的方法、层次分析法、模糊逻辑方法。基于概率论的方法,是以故障树和事件树为分析与计算工具,运用主逻辑图、事件树分析及故障树分析综合对风险进行评估。这种方法不足之处在于:第一,由于风险因素的不确定性和多样性,使得在对风险因素进行描述时,要做到严格的定量化或准确性是不现实的;第二,要求有大量的历史资料可供参考;第三,方法过于繁琐。关于层次分析法,以前的讨论大多是对每一层元素构造评判矩阵,评判矩阵是由元素之间的比较得到的。而对网络安全风险诸因素很难直接对比其重要度。关于模糊逻辑法,在以前发表的文章的讨论中大多是构造风险因素集和评价因素集,由专家直接打分评判出某风险因素的风险水平,这种打分带有很大的主观性。另外,也有的文章是将AHP方法和模糊逻辑法结合的方法,先用模糊逻辑法,由专家直接评定各因素的风险高低,这显然是较难进行的(而把风险因素分别从概率、影响和不可控制性上分别评估较容易进行),然后对各因素的权重再采用层次分析法考虑,将权重向量与隶属度矩阵相乘作为评估结果,这种方法存在着很大的主观性和重复计算问题。本文采用层次分析法与模糊逻辑法相结合的方法,对层次分析法与模糊逻辑法进行了改造。在模糊逻辑法中对各因素的评判不是直接评价其重要度,而是将各风险因素从概率方面、从影响方面、从不可控制性方面分别进行评判。这样,我们首先用层次分析法将风险评估分为三层,其中第二层的准则分别为概率、影响和不可控制性。另外,在确定第三层各风险因素的排序权向量时采用模糊逻辑法,通过给出各风险因素对准则的隶属度矩阵,并利用模糊逻辑运算公式求出各风险因素的排序权向量。最后利用层次分析法求出各风险因素的综合风险权重,确定出哪些因素是系统的高风险因素。

2 网络安全风险因素识别

2.1 识别系统威胁

识别应用系统的薄弱点所产生的威胁,人为和非人为的、恶意的和非恶意的、内部攻击和外部攻击等。对网络安全的威胁主要表现在:非授权访问、冒充合法用户、破坏数据完整性、

*)承担项目:国家信息关防与网络安全保障持续发展计划、国家863高技术研究发展计划(2002AA142151)、中国科学院知识创新工程方向性项目(KGCX2-106)、北京市科技计划项目(H020120090530)。赵冬梅 副教授,博士生,研究方向:网络安全;张玉清 副研究员,博士后;马建峰 教授,博士生导师。

干扰系统正常运行、利用网络传播病毒、线路窃听等方面。安全威胁主要利用以下途径：系统安全的漏洞；系统安全体系的缺陷；使用人员的安全意识薄弱；管理制度的薄弱。

2.2 识别系统的薄弱点

识别与每一个威胁有关的薄弱点，产生一个威胁/薄弱点对。薄弱点可以结合构成一个或多个威胁。可以通过风险评估文件、审计、系统缺陷报告、安全报告和公告、自动工具和技术安全评估等来识别威胁和薄弱点。这些薄弱点包括漏洞和后门、电磁辐射、串音干扰、硬件故障、软件故障、人为因素、网络规模、网络物理环境和通信系统等。

2.3 描述风险

描述薄弱点在系统的网络信息保密性、完整性和网络系统的可用性方面产生的风险，系统遭受的损失和掌握的数据。

2.4 识别现有的安全控制

识别现有的安全控制，它们可以减少：①利用系统的薄弱点产生威胁的可能性；②系统可利用的薄弱点的造成的损失值。这些安全控制是依据识别的威胁/薄弱点对和系统风险所采取的管理、操纵和技术控制措施。

3 构造递阶层次结构

层次分析法(analytic hierarchy process，简称 AHP)是一种有效地处理不易定量化变量下的多准则决策手段。它可以将复杂的问题分解成递阶层次结构，然后在比原问题简单得多的层次上逐步分析；可以将人的主观判断用数量形式表达和处理，可以同时处理可定量和不易定量因素，也可以提示人们对问题的主观判断是否一致。运用 AHP 解决问题，可分为四个步骤：第一，建立问题的递阶层次结构；第二，构造两两比较判断矩阵；第三，由判断矩阵计算被比较元素的相对权重；第四，计算各层元素的组合权重。

首先构造递阶层次结构。递阶层次的最上层为目标的焦点，我们在网络安全风险评估中定义为“风险因素重要度”。按照我们前面的讨论，在网络安全风险评估中各风险因素的比较应从概率、影响和不可控制性三方面分别进行。所以我们将第二层的准则定义为“风险概率”、“风险影响”和“不可控制性”。第三层为要考虑的各风险因素，根据系统的不同而不同。例如，图 1 是某系统风险评估的递阶层次结构。

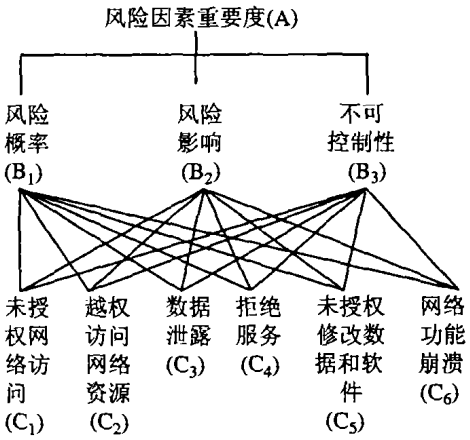

图 1 风险评估的递阶层次结构

4 计算第二层次的相对权重

将 AHP 方法应用于网络安全风险评估时，对该方法进行了改进。第二层次准则的相对权重仍采用传统的 AHP 方法计算。第三层次风险因素的相对权重采用改进的模糊评估法。

4.1 构造判断矩阵

先对第二层次的要素以第一层的要素为准则进行两两比较，并根据评定尺度确定其相对重要度，建立判断矩阵。

$$\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ & \cdots\cdots & & \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix}$$

b_{ij} 表示从判断准则 A 角度考虑要素 B_i 对要素 B_j 的相对重要度。其中判断尺度的取值按相对重要程度取 1～9 之间的自然数。

4.2 计算第二层次的相对权重

根据第二层次的判断矩阵，利用方根法计算各元素的相对权重。先求出特征向量 M。

$M=(m_1,m_2,\cdots,m_n)$，

其中 $m_i=\sqrt[n]{b_{i1}b_{i2}\cdots b_{in}}$ (1)

对 M 进行归一化处理，得到排序权向量 W。

$W=(w_1,w_2,\cdots,w_n)$

其中 $w_i=m_i/\sum_{i=1}^{n}m_i$ (2)

计算矩阵的最大特征根。

$$\lambda_{max}=\sum_{i=1}^{n}\frac{(AW)_i}{nw_i} \quad (3)$$

再进行一致性检验，一致性指标为 $C.I.$。

$$C.I.=\frac{\lambda_{max}-n}{n-1} \quad (4)$$

其中 n 为判断矩阵的阶数。当 $C.I.<0.1$ 时，表明矩阵一致性成立，各项权重无逻辑错误。

5 计算第三层次风险因素相对于第二层次准则的相对权重

按传统 AHP 法，首先要计算第三层次风险因素相对于第二层次准则的判断矩阵。即对风险因素 C_1、C_2、…、C_n 相对上一层次的准则 B_1、B_2、B_3 分别构造判断矩阵。要求对各因素进行两两比较，直接得到判断矩阵。为了克服各因素之间比较的主观性，我们采用模糊判断，对各因素进行定量评定。

5.1 建立模糊集合

首先构造风险因素集，设为 $U=\{u_1,u_2,\cdots,u_n\}$。然后构造评判集，相对于上一层的不同的准则，专家对各风险因素逐个给出风险程度评语，将各个指标的评语分为 m 个等级，以衡量在该指标上的表现及由此而来的相关风险的大小。对不同的准则，可以设立不同的评判集。设评价所确立的等级集合的评判集为 $V=\{v_1,v_2,\cdots,v_m\}$。

5.2 建立隶属度矩阵 R

根据上一层不同的准则，专家给出各因素的评语，构造模糊映射 $f:U\to F(V)$，$F(V)$ 是 V 上的模糊集全体，$u_i\to f(u_i)=(r_{i1},r_{i2},\cdots,r_{im})\in F(V)$，映射 f 表示风险因素 u_i 对评判集中各评语的支持程度。令风险因素 u_i 对评判集 V 的隶属向量 $R_i=\{r_{i1},r_{i2},\cdots,r_{im}\}$，$i=1,2,\cdots,n$。于是得到隶属度矩阵 R 如下：

$$R=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ & \cdots\cdots & & \\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{bmatrix}$$

风险因素相对于不同的准则得到不同的隶属度矩阵。

5.3 确定第三层次相对于第二层次准则的排序权向量

首先将隶属度矩阵 R 变换为其转置矩阵 R' 如下：

$$\boldsymbol{R}'=\begin{bmatrix} r_{11} & r_{21} & \cdots & r_{n1} \\ r_{12} & r_{22} & \cdots & r_{n2} \\ & \cdots\cdots & & \\ r_{1m} & r_{2m} & \cdots & r_{nm} \end{bmatrix}$$ 因为评判集中各个指标中程度的高低直接影响风险大小，所以，对评判集中每个评价指标赋予不同的权重。如"风险影响"评判集中的"V_1 可忽略的、V_2 微小、V_3 一般、V_4 严重、V_5 关键"的权重分别赋予 1/25、3/25、5/25、7/25、9/25，满足归一化条件。设权重分配集为 $A=(a_1, a_2, \cdots, a_m)$。由模糊变换的运算

$$\boldsymbol{B}=\boldsymbol{A}\cdot\boldsymbol{R}=(a_1,a_2,\cdots,a_m)\begin{bmatrix} r_{11} & r_{21} & \cdots & r_{n1} \\ r_{12} & r_{22} & \cdots & r_{n2} \\ & \cdots\cdots & & \\ r_{1m} & r_{2m} & \cdots & r_{nm} \end{bmatrix}$$

$$=(b_1,b_2,\cdots,b_n)$$

B 为各风险因素在某准则下的相对权重，归一化后得到排序权向量。

5.4 计算风险因素的综合重要度

计算出各层相对于上一层的相对排序权向量后，风险因素的综合重要度即为风险因素相对于各准则的权重乘以准则相对于顶层的权重，再取它们的和。

6 实例分析

对图 1 所示网络系统的递阶层次结构模型，首先构造第二层次相对于第一层次的判断矩阵。第二层准则"风险概率"、"风险影响"、"不可控制性"以第一层"风险因素重要度"为依据的判断矩阵 A_B 为

$$\boldsymbol{A\_B}=\begin{bmatrix} 1, & 1/2, & 5 \\ 2, & 1, & 7 \\ 1/5, & 1/7, & 1 \end{bmatrix}$$

然后计算第二层次的相对权重。首先求出特征向量 $\boldsymbol{M}=(1.357, 2.410, 0.306)$。对 $\boldsymbol{M}$ 进行归一化，得到排序权向量 $\boldsymbol{W}=(0.333, 0.592, 0.075)$。矩阵的最大特征根 $\lambda_{max}=\sum_{i=1}^{n}\frac{(AW)_i}{n_{w_i}}=3.014$，一致性指标 $C.I.=\frac{\lambda_{max}-n}{n-1}=0.007<0.1$，表明判断矩阵一致性成立。

下面计算第三层次的相对权重。首先构造模糊集合 $U=\{C_1, C_2, \cdots, C_6\}$，其中 $C_1, C_2, \cdots, C_6$ 分别为风险因素"未授权的网络访问"、"越权访问网络资源"、"数据泄露"、"拒绝服务"、"未授权修改数据和软件"、"网络功能崩溃"。再构造评判集，对于不同的准则构造不同的评判集。对于准则 B_1-"风险概率"来说，风险因素集 U 的评判集 $V=\{V_1, V_2, \cdots, V_7\}$，其含义见表 1。

表 1 风险概率等级定义

概率等级	描述
V_1 可忽略的	基本不可能发生
V_2 很低	每 5 年可能发生二到三次
V_3 低	每一年或不到一年可能发生一次
V_4 中等	每六个月或不到六个月可能发生一次
V_5 高	每个月或不到一个月可能发生一次
V_6 很高	每个月可能发生多次
V_7 极高	每天可能发生多次

由专家参照上表对风险因素 U 进行概率评价，每个专家对各个风险因素确定其风险概率为 V_1、V_2、…、V_7 中的一种。结合各个专家的评定意见，计算各风险因素隶属于各指标的概率则可得到 B_1-C 隶属度矩阵 $\boldsymbol{R}$。

$$\boldsymbol{R}=\begin{bmatrix} 0.0,0.0,0.1,0.1,0.2,0.4,0.2 \\ 0.1,0.2,0.3,0.2,0.1,0.1,0.0 \\ 0.1,0.1,0.2,0.2,0.2,0.1,0.1 \\ 0.0,0.1,0.1,0.1,0.3,0.3,0.1 \\ 0.0,0.0,0.1,0.1,0.3,0.3,0.2 \\ 0,1,0.3,0.3,0.2,0.1,0.1,0.0 \end{bmatrix}$$

下面由隶属度矩阵计算排序权向量。对 B_1-C 隶属度矩阵，确定标准 V_1、V_2、…、V_7 的权重依次为 1/28、2/28、3/28、4/28、5/28、6/28、7/28，按照公式 $\boldsymbol{B}=\boldsymbol{A}\cdot\boldsymbol{R}'$ 求得各风险因素在准则 B_1-"风险概率"下的相对权重为(0.196, 0.018, 0.143, 0.175, 0.193, 0.104)，归一化后得到排序权向量为(0.212, 0.127, 0.154, 0.188, 0.208, 0.112)。

对于准则 B_2-"风险影响"来说，风险因素集 U 的评判集 $V=\{V_1, V_2, \cdots, V_5\}$，其含义见表 2。

表 2 风险影响等级定义

影响等级	描述
V_1 可忽略的	风险事件的发生对系统几乎没有影响
V_2 微小	对系统有一些很小的影响，只须很小的努力就可恢复系统
V_3 一般	能引起系统声望的损害，或是对系统资源或服务的信任程度的降低，需要支付重要资源维修费
V_4 严重	可引起重要系统的中断，或连接客户损失或商业信任损失
V_5 关键	可引起系统持续中断或永久关闭，可引起代理信息或服务的重大损失

专家参照上表对风险因素 U 进行影响评定，得到 B_2-C 隶属度矩阵 $\boldsymbol{R}$。

$$\boldsymbol{R}=\begin{bmatrix} 0.0,0.1,0.2,0.4,0.3 \\ 0.1,0.1,0.3,0.4,0.1 \\ 0.1,0.2,0.3,0.3,0.1 \\ 0.2,0.3,0.3,0.2,0.0 \\ 0.0,0.1,0.1,0.4,0.4 \\ 0.1,0.2,0.3,0.2,0.2 \end{bmatrix}$$

下面由隶属度矩阵计算排序权向量。对 B_2-C 隶属度矩阵，确定标准 V_1、V_2、…、V_5 的权重依次为 1/25、3/25、5/25、7/25、9/25，按照公式 $\boldsymbol{B}=\boldsymbol{A}\cdot\boldsymbol{R}'$ 求得各风险因素在准则 B_2-"风险影响"下的相对权重为(0.272, 0.224, 0.208, 0.160, 0.288, 0.216)，归一化后得到排序权向量为(0.199, 0.164, 0.152, 0.117, 0.211, 0.158)。

对于准则 B_3-"不可控制性"来说，风险因素集 U 的评判集 $V=\{V_1, V_2, V_3\}$，其含义见表 3。

表 3 不可控制性等级定义

不可控制性等级	描述
V_1 可以控制	投入一定资金，经过措施防护，可以得到控制
V_2 基本可以控制	投入大量资金和精力，可以控制
V_3 不可控制	属于不可抗拒因素，经过防护措施，也不能控制

专家参照上表对风险因素 U 进行不可控制性评定，得到 B_3-C 隶属度矩阵 $\boldsymbol{R}$。

$$\boldsymbol{R}=\begin{bmatrix} 0.2,0.3,0.5 \\ 0.2,0.2,0.6 \\ 0.3,0.5,0.2 \\ 0.3,0.4,0.3 \\ 0.2,0.4,0.4 \\ 0.4,0.3,0.3 \end{bmatrix}$$

下面由隶属度矩阵计算排序权向量。对 B_3-C 隶属度矩阵，确定标准 V_1、V_2、V_3 的权重依次为 1/9、3/9、5/9，按照公式 $\boldsymbol{B}=\boldsymbol{A}\cdot\boldsymbol{R}'$ 求得各风险因素在准则 B_3-"不可控制性"下的相对权重为(0.4,0.422,0.311,0.333,0.378,0.311)，归一化后得到排序权向量为(0.186,0.196,0.144,0.155,0.175,0.144)。

计算各层权重乘积之和即得到各风险因素综合重要度，见表 4。

表 4 综合重要度

C_i	B_1	B_2	B_3	$W_i=\sum_{j=1}^{3} w_j \cdot w_{bj}$
	0.333	0.592	0.075	
C_1	0.212	0.199	0.186	0.203
C_2	0.127	0.164	0.196	0.154
C_3	0.154	0.152	0.144	0.152
C_4	0.188	0.117	0.155	0.143
C_5	0.209	0.212	0.175	0.210
C_6	0.112	0.158	0.144	0.142

根据以上分析，最后得到风险因素 C_1、C_2、…、C_6 的综合重要度分别为 0.203、0.154、0.152、0.143、0.210、0.142，风险较大的为 $B5$ 和 $B1$。要采取的风险保护措施首先必须控制未经授权而修改数据和软件并控制未授权的网络访问。

结束语 本文对网络安全风险评估的方法，考虑到了网络安全风险因素的不确定性和多变性，采用 AHP 法和模糊逻辑法相结合的方法，将风险因素分别从风险概率、风险影响和不可控制性方面进行专家评定，并用模糊逻辑法确定其权重，是一种将主客观相结合的方法，将主观评估做定量描述，可以对风险因素做比较客观的评估。

参 考 文 献

1 Baltimore. CMS Information Security Risk Assessment Methodology. Sep. 2002

2 Mustafa M A, FAI-Bahar J. Project risk assessment using the analytic hierarchy process[J]. IEEE Transactions on Engineering Management, 1991, 38(1): 46～52

3 That JHM, Carr V. A proposal for construction project risk assessment using fuzzy logic[J]. Construction Management and Economics, 2000, 18: 491～500

4 钟登华，张建设，曹广晶．基于 AHP 的工程项目风险分析方法．天津大学学报，2002，35(2)：162～165

5 李洪兴，汪培庄．模糊数学[M]．北京：国防工业出版社，1993

6 许树柏．层次分析法原理．天津：天津大学出版社，1988

(上接第 59 页)

5.3 与其它算法对比结果

采用 WCSS 得到如下对比结果。从对比结果来看，在系统未超过过载点时，二者的性能基本相近，但过超载点后，资源优化调度算法的错误连接率要好。与我们上面的真实结果较为符合。证实了 WCSS 对真实 Web 集群模拟的逼近性。

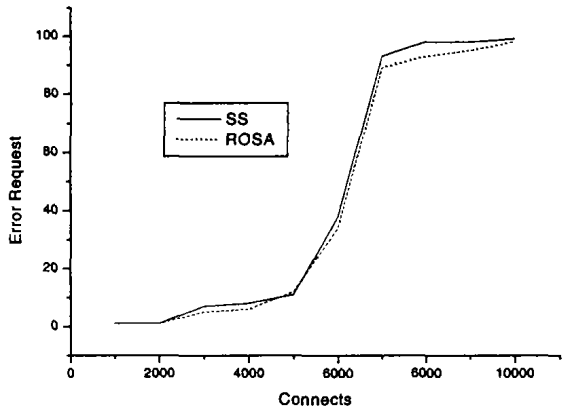

图 5 ROSA 与 SS 对比的模拟结果

结束语 本文主要探讨了 Web 集群调度算法的性能评价体系和集群模拟器 WCSS 的设计与实现，为 Web 集群调度算法的研究提供了很好的研究平台。进一步的研究工作主要包括支持各种不同 QoS 调度算法性能评价。

参 考 文 献

1 AOL. America Online Press Data Points. 2002. http://corp.aol.com/press/press_datapoints.html.

2 Crovella ME, Bestavros A. Self-Similarity in World Wide Web traffic: Evidence and possible causes. IEEE/ACM Transactions on Networking, 1997, 5(6): 835～846

3 Mogul JC. Network behavior of a busy web server and its clients. Technical Report, WRL 95/5, Palo Alto: DEC Western Research Laboratory, 1995

4 Cardellini V, Casalicchio E, Colajanni M, Yu P S. The state of the art in locally distributed Web-server systems. ACM Computing Surveys, 2002, 34(2): 1～49

5 Colajanni M, Yu P S, Cardellini V. Dynamic load balancing in geographically distributed heterogeneous web servers. In: Proc. of the 18th IEEE Intl. Conf. on Distributed Computing Systems (ICDCS'98). Amsterdam IEEE Computer Society, 1998. 295～302

6 Katz E D, Butler M, McGrath R. A scalable HTTP server: the NCSA prototype. Computer Networks and ISDN Systems, 1994, (28): 155～164

7 Cisco Systems Inc. Load balancing : amultifaceted solution for improving server avalability. Whitepaper, 2000. http: //www.cisco.com /warp/public/cc/pd/cxsr/400/tech/lobal-wp.htm.

8 Crovella M E, Carter R L. Dynamic server selection in the Internet: [TechnicalReport, TR-95-014]. Department of Com-puter Science, Bostor University, 1995. http://cs-www.bu.edu/faculty/crovdla/paper-archive/hpcs95/paper.html.

9 Lin, Chuang. Performance analysis of request dispatching and selecting in web server clusters. Chinese Journal of Computers, 2000, 23(5): 500～508

10 Estrin. Improving simulation for network research [R]: [TechRep. 99-702b]. University of Southern California Sep. 1999

11 李双庆，古平，程代杰．Web 集群系统负载均衡策略分析与研究，计算机工程与应用，2002，38(19)：40～42，64

12 Stallings W. High-Speed Networks TCIP/IP and ATM Design Principles. Englewood Cliffs, NJ: PrenticeHall, 1998

13 Cunha C, Bestavros A, Mcrovella. Characteristics of WWW client-based traces. Department of Computer Science of Boston University, [TechRep: TR-95-010]. 1995

14 Arlitt M, Williamson C. Web server workload characterization: The search for invariants (extended version). In: ACM SIGMETRICS'96. Marriott, PA, 1996

15 Abdulla G, Fox E, Abrams M. Shared user behavior on the world wide web. In: ProcWebNet97, Association for the Advancement of Computing in Education (AACE). 1997. URL. http://www.aace.org/

16 Shaikh A. Efficient dynamic routing in wide-area networks[D]: [PhD thesis]. University of Michigan, 1999

17 Banga G, Mogul J C. Resource containers: A new facility for resource management in server systems [J]. In: Proc. of the Third Symposium on Operating Systems Design and Implementation (OSDI'99), New Orleans, LA, Feb. 1999

18 雷迎春，张松，等．Web 集群服务器的分离式调度策略．计算机研究与发展，2002，39(9)：1093～1098