

文章编号:1001-9081(2010)05-1191-03

## 基于多服务提供者模型的分布式CA系统研究

王伟<sup>1,2</sup>, 马自堂<sup>1</sup>, 孙磊<sup>1</sup>, 卢明龙<sup>1</sup>

(1. 信息工程大学 电子技术学院, 郑州 450004; 2. 解放军 63883 部队, 河南 洛阳 471000)

(wangw525@sohu.com)

**摘要:** 为了提高公钥基础设施(PKI)中认证中心(CA)系统的服务能力,使其具备较高的可用性,提出一个基于多服务提供者模型的分布式CA系统,以提高CA系统的抗毁顽存和容错能力。并基于服务质量(QoS)属性采用自动修正判断矩阵的层次分析法对候选服务集中的服务进行QoS评估,以达到快速选择最优服务的目的。实验结果表明该方法有效提高了服务请求的执行效率,满足了用户的QoS需求。

**关键词:** 认证中心;分布式;服务质量;层次分析法;容错

**中图分类号:** TP393 **文献标志码:** A

## Study on distributed certificate authority system based on multi-provider model

WANG Wei<sup>1,2</sup>, MA Zi-tang<sup>1</sup>, SUN Lei<sup>1</sup>, LU Ming-long<sup>1</sup>

(1. Institute of Electronic Technology, Information Engineering University, Zhengzhou Henan 450004, China;

2. Troops 63883 of the Chinese People's Liberation Army, Luoyang Henan 471000, China)

**Abstract:** To improve the service ability and availability of Certificate Authority (CA) system in the Public Key Infrastructure (PKI), a distributed CA system based on the model of multi-provider was proposed, which can improve the CA's ability of survivability and fault-tolerant. On the basis of Quality of Service (QoS), an Analytical Hierarchy Process (AHP) approach with automatically modifying judgement matrix was proposed to estimate the quality of service, so that the best service could be selected quickly. The experimental results show that this strategy increases running efficiency of service request and meets the needs of user's QoS requirement.

**Key words:** Certificate Authority (CA); distributed; Quality of Service (QoS); Analytical Hierarchy Process (AHP); fault-tolerant

### 0 引言

认证中心(Certificate Authority, CA)是公钥基础设施(Public Key Infrastructure, PKI)的核心组件<sup>[1]</sup>,为了提高CA系统的可靠性、稳定性和连续提供服务的能力,研究CA系统的抗毁顽存,增强系统在复杂网络环境下的生存能力,是当前PKI技术发展要解决的重要课题。目前解决这种问题常常采用的是双机备份方式,但是该模式中服务节点在地理位置上比较靠近,仍旧存在很大隐患。当出现网络遭到局部破坏或干扰等情况时,CA系统容灾抗毁能力不强,扩展不便,不能保证不间断的证书签发和管理服务。

针对以上问题,本文重点研究如何提高CA系统容错性、可用性等内容,提出了一个基于多服务提供者模型的分布式CA系统,其关键是如何选择高质量的CA提供服务。并基于QoS使用自动修正判断矩阵的层次分析法,对候选服务进行质量评估、排序,以达到快速选择最优服务的目的。

### 1 多服务提供者分布式CA模型

通过对公钥基础设施PKI中CA系统的分析,为了增强CA系统的可靠性、稳定性和连续提供服务的能力,本文重点研究如何提高CA的容灾抗毁能力。为保证当出现网络遭到局部破坏或干扰等情况时CA系统能够正常工作,本文基于多服务提供者模型对CA系统进行改进,以提高其可用性。

多服务提供者模型是指由多个功能相同的提供者共同承担某服务,服务的可靠性取决于各提供者的综合故障情况,只要还有一个提供者是正常的就仍可对外提供服务,而不会受到部分提供者故障的影响。多服务提供者模型主要用于提高系统的容灾抗毁能力,并可将多个服务提供者部署在不同的物理环境中,确保提供者不会同时被毁灭,从而实现系统的高抗毁能力。

根据以上分析,本文设计一个基于多服务提供者模型的分布式CA系统,该系统具有容错、抗毁、可用性强等特点。

多服务提供者分布式CA模型由部署在多个地点的CA系统构成,CA之间形成备份关系,实现CA系统的抗毁顽存功能。该模型采用高可扩展结构,可根据实际需要加入新建的CA。平时可设一个或多个CA对外提供服务,若需要提高服务性能或抗毁能力时,可在本地或异地快速建设新的CA,并将其加入到多服务提供者CA集合中,共同对外提供服务。

多服务提供者分布式CA模型如图1所示,主要由服务提供者CA集合、服务提供者控制模块、服务请求者RA和服务质量(Quality of Service, QoS)评估与选择模块等四部分组成。

1) 服务提供者CA集合中的CA相互等价,能实现完全相同的功能,多个CA之间相互形成备份关系,任何一个CA失效时,将导致当前服务请求失败,随后的请求将由其他CA处理。CA的选择受服务提供者控制模块的控制。

收稿日期:2009-12-07;修回日期:2010-01-31。 基金项目:国家863计划项目(2008AA01Z404)。

作者简介:王伟(1981-),女,河南许昌人,工程师,硕士研究生,CCF会员,主要研究方向:系统工程、信息安全; 马自堂(1962-),男,安徽合肥人,教授,主要研究方向:信息系统安全; 孙磊(1973-),男,河南洛阳人,副研究员,博士,主要研究方向:信息安全; 卢明龙(1983-),男,河南商丘人,硕士研究生,主要研究方向:网络安全、资源发现。

2) 服务提供者控制模块根据 CA 管理员制定的控制策略实现 CA 服务状态的选择,即提供服务或处于静默状态。根据服务提供者集合中各 CA 的负载状况,进行业务调度,使多服务提供者 CA 的负载达到均衡状态,不产生业务瓶颈。

3) 服务请求者 RA (Registration Authority) 是 CA 的注册申请机构,实现证书管理请求的管理<sup>[1]</sup>。

4) QoS 评估与选择模块对服务提供者的 QoS 进行评估并维护评估结果,为请求者提供 CA 的基本信息和 QoS 信息,使 RA 有选择地接受 CA 集合提供的相关服务。

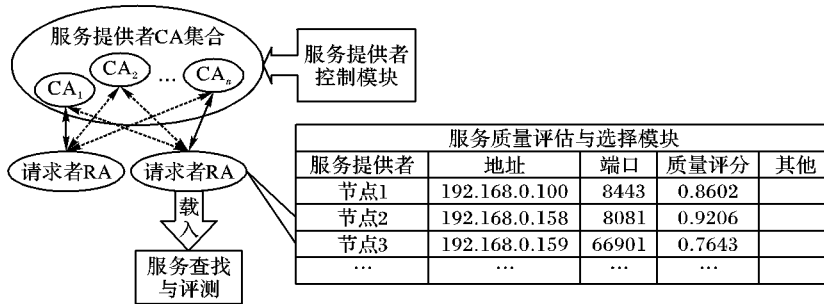


图1 多服务提供者分布式 CA 模型

## 2 基于 QoS 的多服务提供者选择算法

QoS 评估与选择模块对提供者的 QoS 进行评价,并从多服务提供者集合中选择 QoS 最优的服务提供者,在此过程中, QoS 属性是评价和选择的重要因素。

### 2.1 QoS 属性参数定义及 QoS 模型

根据分布式多服务提供者 CA 模型,结合国际标准 ISO 8402 和 ITU E. 800 对 QoS 的定义,我们可以给出分布式多服务提供者的 QoS 定义:“分布式多服务提供者的 QoS 主要体现的是一种服务使用者对服务提供者所提供服务的感知效果。”

在多服务提供者分布式 CA 系统中,影响 CA 服务质量的因素很多,但是在整个服务过程中最重要的三个因素是:响应时间、响应成功率和连续响应成功率,下面定义它们的 QoS 参数。

**响应时间** 服务  $s$  的响应时间  $q_{\text{time}}(s)$  是从调用服务的请求发出开始到该请求的结果收到之间的时间延迟。响应时间  $q_{\text{time}}(s)$  由处理时间  $T_{\text{process}}(s)$  和传送时间  $T_{\text{trans}}(s)$  组成,其计算表达式为:  $q_{\text{time}}(s) = T_{\text{process}}(s) + T_{\text{trans}}(s)$ 。

**传送时间**  $T_{\text{trans}}(s)$  根据服务方法过去的实际执行情况进行估算,更新函数可以表示成:

$$[T_{\text{trans}}(s)]_{n+1} = \frac{n-1}{n}[T_{\text{trans}}(s)]_n + \frac{1}{n}T_n(s)$$

其中:  $T_n(s)$  是第  $n$  次服务传送时间;  $[T_{\text{trans}}(s)]_{n+1}$  是第  $n$  次后服务传送的期望时间;  $n$  是过去响应次数的数量。

**响应成功率** 即响应成功的次数/总次数,其计算表达式为:  $q_{\text{rat}}(s) = N_c(s)/K$ 。其中:  $N_c(s)$  是服务  $s$  在最大期望时间内成功响应的次数;  $K$  是响应的总次数。

**连续响应成功率** 即连续响应成功的次数/成功次数,其计算表达式为:  $q_{\text{sc}}(s) = N_s(s)/N_c(s)$ 。其中:  $N_c(s)$  是服务  $s$  在最大期望时间内成功响应的次数;  $N_s(s)$  是其中能够连续响应成功的次数。

综合上面给出的定义,多服务提供者模型中服务  $s$  的综合质量向量定义为:  $Q(s) = (q_{\text{time}}(s), q_{\text{rat}}(s), q_{\text{sc}}(s))$ , 该 QoS 向量可以根据用户的需求任意扩展<sup>[2]</sup>。

上面是单个服务  $s$  的质量模型,在多服务提供者模型中,

有  $n$  个能够满足功能条件的服务提供者 CA, 该集合  $S$  表示为  $\{s_1, s_2, \dots, s_n\}$ , 将所有的候选服务的 QoS 质量向量合并, 得质量矩阵  $Q_S$  表示如下:

$$Q_S = \begin{bmatrix} q_{\text{time}}(s_1) & q_{\text{rat}}(s_1) & q_{\text{sc}}(s_1) \\ q_{\text{time}}(s_2) & q_{\text{rat}}(s_2) & q_{\text{sc}}(s_2) \\ \vdots & \vdots & \vdots \\ q_{\text{time}}(s_n) & q_{\text{rat}}(s_n) & q_{\text{sc}}(s_n) \end{bmatrix} = \begin{bmatrix} Q_{11} & Q_{12} & Q_{13} \\ Q_{21} & Q_{22} & Q_{23} \\ \vdots & \vdots & \vdots \\ Q_{n1} & Q_{n2} & Q_{n3} \end{bmatrix} \quad (1)$$

式(1)把能够完成任务的所有可选服务的 QoS 属性表示成一个矩阵,该矩阵的列表示某种质量属性的 QoS 值,比如第一列表示各个可选服务的响应时间。矩阵的行表示某个服务针对其具体 QoS 属性的属性值。式(1)将多服务的 QoS 属性和完成任务的所有可选服务统一表述,并支持多服务 QoS 属性的可扩展性,当增加一个新的质量属性时,矩阵新增加一列。

### 2.2 QoS 属性参数规范化

为了找到质量最优的服务提供者,需要综合计算每个可选服务的多个 QoS 属性值。而 QoS 具体属性的特性是复杂多样的,通过对质量属性进行分析,本文归纳出所有的质量属性分两种特性:增量型质量属性是指 QoS 值越高质量也就越高,比如响应成功率;与增量型质量属性相对应的是减量型质量属性,即 QoS 值越高质量却越低,比如响应时间。

由于各属性值的表述方式差异较大,量化单位各不相同,有的用整数表示,有的用百分数表示,在多个 QoS 属性间并没有一个统一的度量标准,这使得相互的比较缺乏一个公认的基础。因此,需要将各服务的 QoS 属性进行无量纲化和归一化处理,即规范化<sup>[3-4]</sup>。归一化是指把各属性的值都映射到  $[0, 1]$  区间。无量纲化是指通过数量变换,消除量纲和数量级对质量属性的影响,使属性实际值转化为评价属性值的方法。

本文采用非比例变换法来作规范化,此法将属性之差按一定比例进行归一化和无量纲化。

增量型质量属性的规范化计算公式如下:

$$V_{i,j} = \begin{cases} \left( \frac{Q_{i,j} - Q_j^{\min}}{Q_j^{\max} - Q_j^{\min}} \right), & Q_j^{\max} - Q_j^{\min} \neq 0 \\ 1, & Q_j^{\max} - Q_j^{\min} = 0 \end{cases} \quad (2)$$

减量型质量属性的规范化计算公式如下:

$$V_{i,j} = \begin{cases} \left( \frac{Q_j^{\max} - Q_{i,j}}{Q_j^{\max} - Q_j^{\min}} \right), & Q_j^{\max} - Q_j^{\min} \neq 0 \\ 1, & Q_j^{\max} - Q_j^{\min} = 0 \end{cases} \quad (3)$$

在式(2)、(3)中,  $Q_j^{\max}$  是质量矩阵  $Q$  中某 QoS 属性(列)的最大值,  $Q_j^{\max} = \max(Q_{i,j}) (1 \leq i \leq n)$ ; 而  $Q_j^{\min}$  是质量矩阵  $Q$  中某 QoS 属性(列)的最小值,  $Q_j^{\min} = \min(Q_{i,j}) (1 \leq i \leq n)$ 。

用式(2)、(3)的变换把各属性的值都映射到  $[0, 1]$  区间,得到标准化质量矩阵  $V$ :

$$V = \begin{bmatrix} V_{11} & V_{12} & V_{13} \\ V_{21} & V_{22} & V_{23} \\ \vdots & \vdots & \vdots \\ V_{i1} & V_{i2} & V_{i3} \\ \vdots & \vdots & \vdots \\ V_{n1} & V_{n2} & V_{n3} \end{bmatrix}; 1 \leq i \leq n \quad (4)$$

### 2.3 基于自动修正判断矩阵的 QoS 最优选择策略

对候选服务 CA 进行 QoS 排序,就要计算每个候选服务 CA 的 QoS 评分,需确定每个服务提供者 CA 的 QoS 属性的权重。

层次分析法 (Analytical Hierarchy Process, AHP)<sup>[5]</sup> 是一种非常合适权重计算的方法,它将主观与客观、定性与定量相结合,通过计算判断矩阵的最大特征值及其相应的特征向量,得到各层次要素对上层次某要素的重要性次序,从而建立权重向量。层次分析法要求判断矩阵具有满意的一致性,否则要对判断矩阵进行调整,直至满足一致性为止。

传统的层次分析法在检验判断矩阵出现不一致时,需要反馈给用户重新调整判断矩阵,且一般不能给出最快的调整方式,不能排除需要经过多次调整才能通过一致性检验的可能性,不利于优化算法的自动执行,影响了效率,且可操作性不强,限制了层次分析法的应用。

本文基于文献[6],根据用户需求给出的各 QoS 属性的相对重要性,采用自动修正判断矩阵的层次分析法对多个 QoS 属性进行加权处理,计算 QoS 属性的权重,将多目标的问题转化为单目标多约束问题,免去了人机交互的繁琐操作,提高了计算效率。

最优 QoS 的选择算法如下。

步骤 1 构造判断矩阵。

由用户提供各 QoS 属性的相对重要性,构造满足互反性的判断矩阵  $A$ 。QoS 两两属性间的重要性的比值是一个数值  $a_{ij} = w_i/w_j$ ,得判断矩阵  $A = (a_{ij})_{n \times n}$ ,下标  $i, j$  分别对应两两不同的属性,那么,判断矩阵的形式为:

$$A = \begin{matrix} & A_1 & A_2 & \cdots & A_i & \cdots & A_n \\ \begin{matrix} A_1 \\ A_2 \\ \vdots \\ A_j \\ \vdots \\ A_n \end{matrix} & \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1i} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{j1} & a_{j2} & \cdots & a_{ji} & \cdots & a_{jn} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{ni} & \cdots & a_{nn} \end{bmatrix} \end{matrix}$$

其中:  $a_{ii} = 1 (i = 1, 2, \dots, n)$ ;  $a_{ij} = 1/a_{ji} (i, j = 1, 2, \dots, n)$ ;  $a_{ij} = a_{ik}/a_{jk} (i, j, k = 1, 2, \dots, n)$ , 本文中只取  $i, j = 1, 2, 3$ 。 $A_1$  代表响应时间,  $A_2$  代表响应成功率,  $A_3$  代表连续响应成功率。 $a_{ij}$  表示属性  $A_i$  对属性  $A_j$  的相对重要性,通常  $a_{ij}$  取 1, 2, ..., 9 及它们的倒数,其含义为: 1 表示属性  $A_i$  与属性  $A_j$  相比,两者同样重要; 3 表示属性  $A_i$  比属性  $A_j$  稍微重要; 5 表示属性  $A_i$  比属性  $A_j$  明显重要; 7 表示属性  $A_i$  比属性  $A_j$  强烈重要; 9 表示属性  $A_i$  比属性  $A_j$  极端重要。2, 4, 6, 8 表示上述两相邻判断的中间值。根据判断矩阵计算 QoS 属性的权重时,要对判断矩阵进行一致性检验。当找到错误时,采用自动修正判断矩阵的方式,修改 QoS 属性的相对重要性。

步骤 2 采用几何平均法<sup>[3]</sup> 计算判断矩阵  $A$  的特征根  $\lambda_{\max}$  和特征向量  $W$ :

由判断矩阵  $A$  满足等式  $AW = \lambda_{\max} W$ ,  $\lambda_{\max}$  是最大特征根,  $W$  是对应的特征向量,即各属性的权重,则有:

$$W_i = \frac{\sqrt[n]{\prod_{j=1}^n a_{ij}}}{\sum_{i=1}^n \sqrt[n]{\prod_{j=1}^n a_{ij}}}, \lambda_{\max} = \sum_{i=1}^n \frac{(AW)_i}{nW_i} \quad (5)$$

其中  $(AW)_i$  表示向量  $AW$  的第  $i$  个分量。

步骤 3 判断矩阵的一致性检验。

一致性指标  $CI = \frac{(\lambda_{\max} - n)}{(n - 1)}$ ; 平均随机一致性指标  $CR =$

$CI/RI$ , 其中  $RI$  表示同阶平均随机一致性指标,其值在表 1 中给出。

如果  $CR < 0.10$ , 转步骤 5; 否则转步骤 4。

步骤 4 自动修正判断矩阵。

a) 对判断矩阵  $A$  作归一化处理,得到矩阵  $A'$ :

$$A' = (a'_{ij})_{n \times n}$$

其中  $a'_{ij} = a_{ij} / (\sum_{i=1}^n a_{ij}) (j = 1, 2, \dots, n)$ 。

b) 由  $a''_{ij} = a'_{ij} / a'_{i1} (i, j = 1, 2, \dots, n)$ , 得矩阵  $A'' = (a''_{ij})_{n \times n}$ 。

c) 取  $A''$  中最小的  $a''_{ij} (i = 1, 2, \dots, n; j = 2, 3, \dots, n; i \neq j)$ , 通常最小的  $a''_{ij} < 1$ 。当对应  $A$  中的  $a_{ij} > 1$  时,调整后新的  $a_{ij} = a_{ij} + 1$ , 其对应的  $a_{ji} = 1/(a_{ij} + 1)$ ; 当对应  $A$  中的  $a_{ij} < 1$  时,调整后新的  $a_{ij} = 1 / (\frac{1}{a_{ij}} - 1)$ , 其对应的  $a_{ji} = \frac{1}{a_{ij}} - 1$ , 转步骤 2。

步骤 5 调整结束,得到的判断矩阵满足一致性要求,输出权值。

步骤 6 服务选择。得到各 QoS 质量属性的权重  $W_j (W_j \in [0, 1], \sum_{j=1}^3 W_j = 1, j = 1, 2, 3)$  后,可根据  $E_i = \sum_{j=1}^3 (W_j \times V_{ij}) (i = 1, 2, \dots, n, j = 1, 2, 3)$ , 计算出每个服务的综合质量  $E_i$ , 按照  $E_{\text{best}} = \max_{i \geq 1} (E_i)$ , 可从  $n$  个满足条件的可选 CA 服务中选择 QoS 最优的 CA。将排序第一位的 CA 作为最优服务,当其响应时间超出阈值时,使用轮叫调度算法用次优服务来响应用户的请求,同时更新排序列表。

表 1 同阶平均随机一致性指标  $RI$

矩阵阶数 $n$	$RI$
1	0
2	0
3	0.58
4	0.90
5	1.12
6	1.24
7	1.32

### 3 实验与结果分析

实验的目的是验证本文所采用的基于 QoS 的层次分析法对服务提供者 CA 选择的可行性和自动修正判断矩阵算法的有效性。用平均响应时间和平均响应成功率来衡量实验效果。将本文的算法和随机选择服务算法(一种不考虑 QoS 的最普遍的算法)进行比较。

在实验中用 3 台计算机模拟 CA 组成服务提供者集合,用 6 台计算机模拟 RA。这 6 个 RA 随机向 3 个 CA 发出服务请求。在实验过程中,规定每个 RA 的响应时间的阈值是 3 s,若超过 3 s 未得到回应则认为此次请求失败,那么该次响应时间按阈值 3 s 计算。每个 RA 分别按照本文的基于 QoS 的自动修正判断矩阵的层次分析法和随机选择服务算法对服务提供者集合中的 CA 进行选择。统计一段时间内这 6 个 RA 的响应时间和响应成功率的算术平均值如图 2, 3 所示(每隔 10 s 检测一次)。

(下转第 1220 页)



信号替换前1 s,水印图像表明被修改位置为前面的段,由图7(b)可知具体是第1~22段遭恶意篡改,第22段只是前半段遭篡改,而且替换的水印篡改评估值较剪切要小。

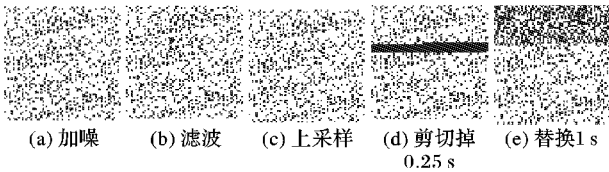


图6 常规攻击和篡改下得到的反置乱前的半脆弱水印对比

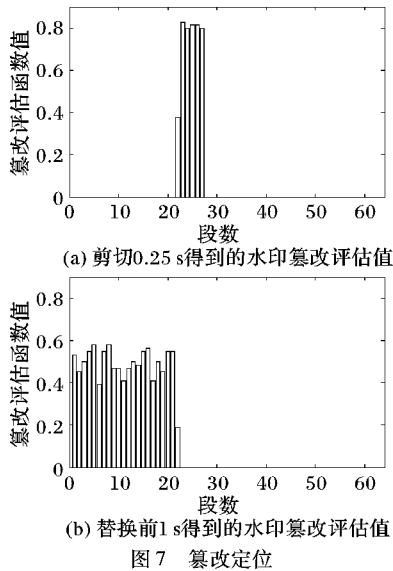


图7 篡改定位

## 5 结语

本文应用小波包分解,将改进的零水印和半脆弱水印结合,完成载体信号的版权保护和内容认证。改进的零水印算法由于引入了小波包分解,抵抗各种常见攻击的能力很强,表现出较高的鲁棒性,因此,在版权保护上更有优势。在版权保

护通过之后,进行内容认证。用来进行内容认证的半脆弱水印能区分出常规操作和恶意篡改,并在嵌入的二值水印图像和载体音频上同时对篡改进行定位,解决了以往只定位水印图像,而不对载体音频定位的问题。而且,本文算法修正了以往双水印算法内容认证上鲁棒性差,对正常媒体处理过于敏感的不足,实用性更强。

## 参考文献:

- [1] VOYATZIS G, PITAS I. The use of watermarking in the protection of digital multimedia products [J]. *Proceedings of IEEE*, 1999, 87(7): 1197-1207.
- [2] BENDER W, GRUHL D, MORIMOTO N, *et al.* Techniques for data hiding [J]. *IBM System Journal*, 1996, 35(3/4): 313-336.
- [3] WU SHAO-QUAN, HUANG JIWU, HUANG DAREN, *et al.* Efficiently self-synchronized audio watermarking for assured audio data transmission [J]. *IEEE Transactions on Broadcasting*, 2005, 51(1): 69-76.
- [4] 杨义先, 钮心忻. 多媒体信息伪装综述[J]. *通信学报*, 2002, 23(5): 32-38.
- [5] 温泉, 王树勋. 零水印的概念和应用[J]. *电子学报*, 2003, 31(2): 214-216.
- [6] 高星明, 蔡翔云. 基于奇异值分解的盲数字音频脆弱水印算法[J]. *电声技术*, 2008, 32(4): 66-68.
- [7] 赵红, 沈东升. 基于支持向量机的半脆弱数字音频水印算法[J]. *计算机工程与设计*, 2009, 30(7): 1745-1748.
- [8] PAQUEIA A H, WARD R K, PITASC I. Wavelet packets-based digital watermarking for image verification and authentication [J]. *Signal Processing*, 2003, 83(10): 2117-2132.
- [9] 高志, 余啸海. *Matlab 小波分析与应用* [M]. 2版. 北京: 国防工业出版社, 2007.
- [10] 张德丰. *Matlab 小波分析* [M]. 北京: 机械工业出版社, 2009.
- [11] 张兵路, 姜建国, 冯复科. 基于 DWT 的音频“零数字”水印技术研究[J]. *计算机工程*, 2009, 31(18): 148-149.
- [12] 赵红, 沈东升, 朱元辉. 一种抗裁剪的半脆弱音频水印算法[J]. *自动化学报*, 2008, 34(6): 647-651.

(上接第1193页)

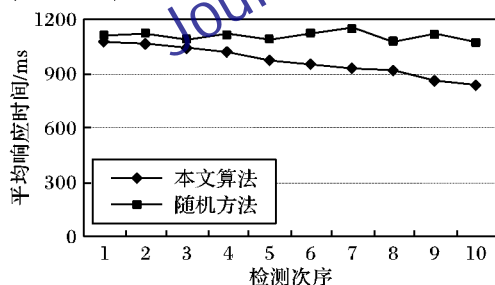


图2 平均响应时间实验结果比较

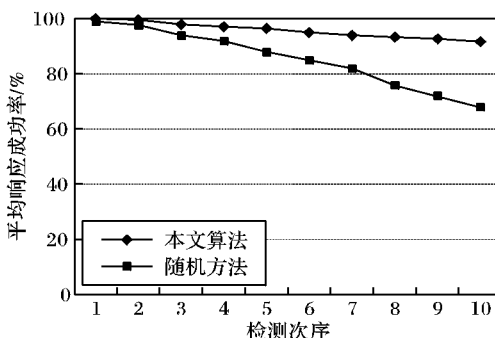


图3 平均响应成功率实验结果比较

从图2、3中可以看出,刚开始两者比较接近,但是随着时间的延长、实验次数的增多,采用本文算法的平均响应时间要

小于随机算法,而本文算法的平均响应成功率要远高于随机算法。综上,说明本文算法能够成功选择响应时间较快、QoS好的CA提供服务,能有效提高服务请求的执行效率。

## 4 结语

为了增强CA系统的可靠性、稳定性和连续提供服务的能力,本文提出了一个基于多服务提供者模型的分布式CA系统,以提高CA系统抗毁顽存和容错能力。实验分析结果表明,基于QoS的自动修正判断矩阵的层次分析法来实现最优选择策略,既真实、详细地反应了用户QoS属性之间的相对重要性需求,又体现了QoS属性值的客观性,并且该方法使服务请求具有较高的执行效率。

## 参考文献:

- [1] 关振胜. 公钥基础设施PKI及其应用[M]. 北京: 电子工业出版社, 2008.
- [2] 代钰, 杨雷, 张斌, 等. 支持组合服务选取的QoS模型及优化求解[J]. *计算机学报*, 2006, 29(7): 1167-1178.
- [3] 宣家骥. 多目标决策[M]. 长沙: 湖南科学技术出版社, 1989: 80-120.
- [4] 程理民, 吴江, 张玉林. 运筹学模型与方法教程[M]. 北京: 清华大学出版社, 2002: 50-200.
- [5] 吕永波. 系统工程: 修订版[M]. 北京: 清华大学出版社, 2006.
- [6] 骆正清. AHP中不一致性判断矩阵调整的新方法[J]. *系统工程理论与实践*, 2004, 24(6): 84-92.