基于Quorum系统的分布式访问控制框架研究

熊庭刚[1,2] 卢正鼎[1] 张家宏[2] 马 中[2]
(华中科技大学计算机科学与技术学院 武汉 430074)[1] (武汉数字工程研究所 武汉 430074)[2]

摘 要 从通用访问控制系统出发,提出以quorum系统来设计访问控制框架,给出了基于互斥协议的quorum分布式访问控制系统(MQ-DACS),以在保持高效率的情况下,提高访问控制决策的稳定性和安全性。进一步分析了在系统结点不可靠的环境中,系统能并行执行的访问控制容量同系统可用性之间的关系,并给出了最佳方案的选取依据。

关键词 分布式访问控制,访问控制框架,quorum系统,可用性,访问控制容量
中图法分类号 TP309 **文献标识码** A

Research on Quorum System-based Framework for Distributed Access Control

XIONG Ting-gang[1,2] LU Zheng-ding[1] ZHANG Jia-hong[2] MA Zhong[2]
(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)[1]
(Wuhan Digital and Engineering Institute, Wuhan 430074, China)[2]

Abstract By researching on generalized system for access control, the paper put forward an access control framework adopting quorum system, and presented a mutual quorum distributed access control system, with the high efficiency and the stability and security. Furthermore, the relation of system capability and system availability under the circumstance that the system nodes are not reliable was analyzed, and a result was given that the mode of the optimization of the entire system considers the capability and availability.

Keywords Distributed access control, Access control framework, Quorum system, Availability, Access control capability

1 引言

访问控制在信息系统中起着非常重要的作用,访问控制框架是实现访问控制模型和贯彻访问控制政策的平台。文献[1]提出的通用访问控制框架(generalized framework for access control,GFAC)将访问控制分为访问控制实施机构(access-control enforcement facility,AEF)和访问控制决策机构(access-control decision facility,ADF)两部分。主体访问客体前,AEF请求ADF,ADF根据主客体属性和访问政策做出访问控制决策,AEF根据ADF的决策结果决定是否实施访问。由于决策部分与实施部分分离,不仅使得信息系统自身的设计与访问控制政策的设计无关,而且支持了安全政策的变化和多元政策。国际标准组织根据GFAC制订了通用访问控制框架的标准[2]。

在基于网络的分布式系统中,访问控制通常被作为一种服务来提供[3],类似地,将访问控制实施与访问控制决策分离。其中,类似于ADF的决策机构与访问政策库集成在诸如授权引擎[4]、角色服务器[5]、或者授权服务器[6,7]等设备中,而类似于AEF的实施机构则嵌入在Web服务器、数据库服务器等各种应用服务器中,如图1所示。

但是这种框架存在着决策机构和政策库自身的安全及可靠性问题。尤其在分布式系统中,授权服务器由于是系统中的一个单点,往往成为主要受攻击对象,一旦出现故障或遭受破坏,系统的访问控制将发生混乱或者陷入瘫痪。另一方面,安全政策通常属于一个组织的秘密,不允许未经授权的人员知晓和修改。因此,在分布式系统中,特别是对安全性和可靠性要求较高的军用系统和分布式事务处理中,设计一种安全、可靠的分布式访问控制框架,提高授权服务的安全性和可靠性具有很大的意义。

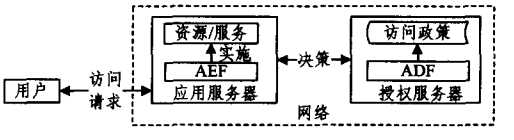


图1 常见的分布式访问控制结构

目前在工程实践中,一般的解决方案是采用防火墙技术保护授权服务等设备。然而,提高单个授权服务器的安全性和可靠性水平的能力总是有限的。显然,在分布式系统中,采用冗余技术,通过增加授权服务器的数量,并使得访问政策在多个服务器上备份,是提高授权服务器安全性和可靠性的最直接方法,但是如果简单地把访问政策在授权服务器之间多次拷贝,不仅降低了政策保密性,而且给维护政策的一致性带来困难,当政策频繁变化时,这也将是一项艰巨的任务。

到稿日期:2009-08-04 返修日期:2009-10-01

熊庭刚(1963-),男,研究员,CCF高级会员,主要研究方向为容错计算和信息安全等,E-mail:xtg_hb@yahoo.com.cn;卢正鼎(1944-),男,教授,博士生导师,主要研究方向为分布式计算和信息安全等;张家宏(1980-),男,博士,主要研究方向为信息安全和密码算法理论;马 中(1962-),男,研究员,博士生导师,主要研究方向为容错计算和计算机系统设计等。

Quorum 系统是一种以“冗余”设计为基础的集合系统[8]，已经被成功应用于诸如互斥、名字服务和选择信息分发等分布控制和管理问题的研究中[9]。每个 quorum 由多个结点组成，它们通过相互通信和数据复制来保持数据的一致性，同时，quorum 之间又通过相交结点把各自内部的数据复制给其它 quorum。因此，不仅实现了 quorum 内部结点间的数据备份，而且也把备份信息发布到其它 quorum，保证了 quorum 间的数据一致性。如果其中某些结点发生故障或者遭到攻击破坏，通过执行特殊的访问协议，总能够从余下的有效结点获取正确的信息。

本文提出一种基于 Quorum 系统的分布式访问控制框架。该框架不仅能够提高访问控制决策的安全性和可靠性，而且能够提高并发访问控制请求的决策速率，并有效实现政策的动态维护和管理。

2 相关概念

2.1 Quorum 系统定义

定义 1(Quorum 系统) 设结点集 $U=\{s_1,s_2,\cdots,s_n\}$，Quorum 系统 QS 是 U 的非空子集的集合，其每一对子集都相交。即，$QS\subseteq 2^U$，$\forall Q_i,Q_j\in QS, Q_i\cap Q_j\neq\emptyset$，$Q_i$ 称之为一个 quorum。

为简单起见，以下将 Quorum 系统简称为 QS，quorum 简称为 Q。

根据使用方式的不同，人们把数据的读、写操作与不同的 Q 结合在一起，又提出了读-写 QS 的概念[10,11]。

定义 2(R-W QS) 设结点集 U 及其上的一对集合(R,W)，如果 W 是 U 上的一个 QS，并且满足 $\forall W_i\in W$，$\forall R_i\in R, W_i\cap R_i\neq\emptyset$，则称集合对$(R,W)$是 U 上的一个 R-W QS。其中每一个 $W_i\in W$ 称为一个写 Q，每一个 $R_i\in R$ 称为一个读 Q。

R-W QS 的提出，方便了 QS 在数据复制操作方面的分析和运用。

2.2 Quorum 访问协议

QS 的访问协议主要有选举协议和互斥协议两大类[12]。

选举协议允许写 Q 中含有数据不同步和读 Q 中含有数据丢失或者不一致的错误。只要当前 Q 中有效结点足够多(通常大于|Q|的一半)，客户端仍然可以完成对 Q 的写操作或者从读 Q 获得正确的数据。否则，在 QS 中寻找下一个 Q，若找不到这样的 Q，则整个系统失败。

互斥协议只允许写不包含遭攻击失效结点的写 Q 和从不包含遭攻击失效结点的读 Q 中获取有效数据。当两个写 Q 对相交的结点执行写操作时，需要执行写操作互斥策略。

自从 QS 的概念提出以来，人们已经研究了大量的 QS，基本上可以分为两大类：按互斥协议尽可能从不含故障结点的 Q 中获取有效数据的 *R-W* QS，如 *Crumbling Walls* QS，*Grid* QS，*Tree* QS 和 *Paths* QS 等[9,11,12]；按照选举协议尽可能地从含有故障结点的 Q 中获取有效数据的 QS，如 *Byzantine* QS[13]，除采用的访问协议不同外，*Byzantine* QS 实质上是一种特殊的读 Q 与写 Q 相同的 *R-W* QS。文献[14]提出门限 *Byzantine quorum* 系统的概念，并应用于分布式存储。

3 基于 QS 的分布式访问控制框架

基于 QS 构造的分布式访问控制框架如图 2 所示。遵循通用访问控制框架的原则，将 AEF 与 ADF 分离，其中，AEFs 驻留在不同的应用服务器中，而 ADFs 分布在每个授权服务器/代理中，组成访问控制决策系统。用户对受控资源提出的任何访问请求或者要求获得某种受控服务的请求，都必须通过应用服务器(的 AEF)得到授权服务子系统(的 ADF)认可。

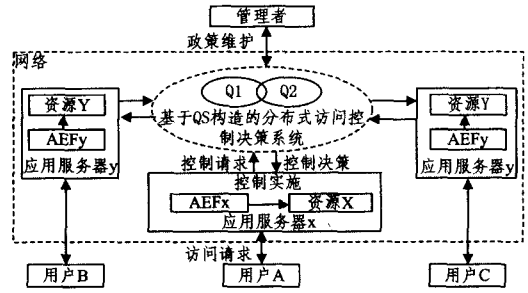


图 2 安全和可靠的分布式访问控制框架

显然，如果能够得到每一个授权服务器的认可即是最可信的，但是每一个授权服务器都可能出现故障或者受到攻击、破坏，不能做出决策或者不能做出正确的决策，这时就需要 quorum 结构的系统能使其在某个结点服务器受攻击的情况下，整个系统的安全性还能得以保障。另外，访问每个服务器的时间开销也是很大的，需要一种途径能使所有授权服务器的某个子集能够代表整个系统的行为，从而避免访问所有服务器结点。

3.1 访问控制框架的构造

分布式访问控制决策系统基于 QS 结构来构造，以充分利用 QS 系统所具有的安全性、容错性特点。每一个有效的读 Q 都可以代表整个授权子系统，响应授权决策请求，做出决定；每一个有效的写 Q 都可以代表整个授权子系统，响应政策管理者提出的政策维护请求，对系统实施有效的政策更新；多个访问控制决策过程可以并行执行，提高访问控制系统的执行响应能力。

譬如，用户 A 通过网络对应用服务器 x 发出访问资源 x 的请求，应用服务器中的 AEFx 以用户 A 和资源 x 的属性，申请分布式访问控制决策系统做出决策。与此同时，用户 B，C 也可以分别对应用服务器 y,z 发出访问资源 y,z 或者 x 的请求，分布式访问控制决策系统能够并行做出决策，决定是否允许用户 B,C 的访问。若允许，则提请 AEFx 使访问继续，否则中断用户请求。

根据定义 1 和定义 2，基于 QS 的分布式访问控制决策系统构造方式如下：

定义 as 为一个访问控制决策结点(或授权服务器，以下简称决策点)，令 $U=\{as_1,as_2,\cdots,as_n\}$。基于 QS 构造的分布式访问控制决策系统是一个 R-W QS 系统，记为 QS_{as}。其中 $W_{as}\subset 2^U$，是一个 QS，满足 $\forall W_i,W_j\in W_{as}, W_i\cap W_j\neq\emptyset$，称为写 Q 集合，实施政策维护；而 $R_{as}\subset 2^U$ 是所有满足 $\forall R_i\in R_{as}$，$\forall W_i\in W_{as}, W_i\cap R_i\neq\emptyset$ 的 Q 的集合，称为读 Q 集合，实施访问控制决策。

3.2 访问控制决策的控制协议

设时间 $t\in T_C$，T_C 是一个所有决策点均可以获得的全局时钟。$P=\{\langle g_i,t_j\rangle|\langle g_i,t_j\rangle=\langle$控制规则，当前时间$\rangle\}$是在某时刻 t_j，以某种形式(复制/分段共享)预先布署在分布式访问控制决策系统上的访问控制政策。实施访问控制决策的过程就是获取一个读 Q 中全部或者大多数决策点关于某一/某些

控制规则 g_i 决策结果的过程；实施政策维护的过程就是在某一时刻 t_j 更新某一个写 Q 中某一/某些控制规则 g_i 的过程。因此，在政策维护/更新时，规则 g_i 与当前时间 t_j 一并写入；在决策时，规则 g_i 的决策结果与储存的 t 一同返回。

访问控制决策的控制协议分为控制决策协议和策略维护协议，分别对应于读 Q 操作协议和写 Q 操作协议。读 Q 操作协议保证读操作并发执行，并且读操作的结果是最近写操作更新后的结果；写 Q 操作协议和读 Q 操作协议相排斥，避免读操作的结果是脏数据，写 Q 操作协议应能保证系统数据的一致性。

Quorum 采用不同的访问方式对应着不同的分布式访问控制模式，对 quorum 访问大致上可分为互斥协议和选举协议两种，据此可得到基于互斥的分布式访问控制和基于选举的分布式访问控制。本文接下来就提高控制决策的安全性和可靠性，提高并发访问控制请求的决策速率以及有效实现策略的动态维护和管理这些方面的性能为目的，根据网格 quorum 系统模型[10]提出一个基于互斥协议 quorum 系统的分布式访问控制决策系统，并对相关的性能进行分析。

4 基于互斥协议 quorum 系统的分布式访问控制决策系统(MQ-DACDS)

如 3.1 节所述，所有的决策点构成一个集合 U，$|U|=k$，$U=\{as_1, as_2, \cdots, as_k\}$。对每条访问策略 x 而言，决策点都冗余备份其信息，其中包括 x 的响应策略内容及此策略存储/更新的时间戳；每个结点都有可能受到攻击而失效，失效的点不能正确发出返回消息。每个决策点有一个互斥标志，互斥标志由最先访问该决策点的 AEFx 置位，直至其访问结束，在此期间该结点对其它任何 AEFx 发来的访问请求予以屏蔽。结点如果处于正常工作状态，且互斥标志未被置位，则能在有效时间内响应 AEF 发起的各种访问请求；如果处于失效状态，则不能在有效时间内正确响应 AEF 发起的任何访问请求。

设 $k=m\times n$，满足上述要求的集合 U 可看作是一个拓扑结构为纵横排列的网格，再按照 3.1 节的方式定义其上的读写 quorum，可得到基于互斥协议的分布式访问控制决策系统(MQ-DACDS)。

4.1 访问控制协议

将所有的访问控制决策结点视为 m 行×n 列的拓扑结构排列，则每个决策结点都有其固定的行列号。

访问控制决策协议(读操作)按图 3 所示的步骤进行。AEF_k 为当前对基于 QS 构造的分布式访问控制决策系统(ADFs)发起决策请求的某个访问控制实施点。在读操作中，做出正确响应的各决策点(即被设置了互斥标志的服务器结点)构成了一个列覆盖集(C-cover)[10]，称之为读 quorum。

S1. 用读操作的方法选定某列覆盖集；

S2. 管理者 M 为在 S1 中选定的列覆盖集所在列随机选择一个序列，下面操作按照此序列的顺序访问各决策结点列(列覆盖集所在列)；

S3. 管理者 M 据 S2 产生的序列依次访问各列；

S4. 管理者 M 对当前访问结点列中的所有结点发送访问控制策略维护请求 $\beta=\langle g_{inew}, t_{new}\rangle$，其中 g_{inew} 是将要更新的策略，$t_{new}\in TC$；

S5. 在有效时间内管理者 M 接收各结点返回的响应信息，若每个访问结点都发回了响应信号，是对该列各结点设置互斥标志，策略维护请求成功，跳第 6 步，否则跳到第 3 步，重复此过程直到所有列都访问完毕，跳第 6 步；

S6. 若策略维护请求成功，则管理者 M 用 g_{inew} 替换第 5 步中选定列的所有结点和第 1 步中选出的列覆盖集中的所有结点的相应策略内容，并用这些结点中时间戳最大的 t' 替换所有结点的时间戳值。

图 3 读操作

访问控制策略维护协议(写操作)按图 4 所示的步骤进行。在写操作中，选出的某一列的所有结点和列覆盖集中的结点构成的集合，称之为写 quorum。

S1. AEF_k 随机选择一个序列，以下按照此序列的顺序访问各决策结点行；

S2. AEF_k 据 S1 产生的序列依次访问各行；

S3. AEF_k 对当前访问结点行中不属于已响应列的结点发出访问决策请求 $\alpha=$(用户名，操作名，对象名)；

S4. 在有效时间内 AEF_k 接收各结点返回的响应信息，记录成功返回信息的各结点的所在列号，并将划分为已响应列，设置互斥标志；

S5. 若已响应列个数等于 n 则跳到第 6 步，否则跳到第 2 步，直到所有行都访问完毕，跳第 6 步；

S6. 若已响应列个数不等于 n，则读决策操作失败，否则 AEF_k 根据所有得到的 as_i 返回的决定值集合 $A=\{\langle v_i, t_i\rangle \mid as_i\in R_k\}$，选择其中具有最大时间戳 t_m 的服务器传来的有效读数据 v_m 作为决策数据。

图 4 写操作

由读写操作的步骤可知，每次读操作要读取一列结点中的至少一个，那么肯定读到了被最近一次写操作更新过的结点，而通过比较时间戳，最近被更新的结点将作为最终数据被读出，因此每次读操作都能读到最新的策略内容，这保证了访问所获得信息的一致性。由于写操作要锁定一列，读操作要锁定一个列覆盖集，这样必有某一个结点会引起读写操作冲突，因此写操作和读操作不能并发进行，写写操作也由于类似原因不能并发进行。而读操作则可能同时进行，这一特性提高了 MQ-DACDS 系统并行决策的能力。

4.2 性能分析

Quorum 规模的定义为其所包含结点的个数，MQ-DACS 中 quorum 分两类——读 quorum 和写 quorum，那么读 quorum 的规模为：

$$size(R_{as})=|\text{列覆盖集}|=n=(\sim\sqrt{|U|}),$$

写 quorum 的规模为：

$$size(W_{as})=size(R_{as})+n=2n=(\sim 2\sqrt{|U|})$$

负载(load)是 quorum 系统的重要性能特征，定义为系统中最忙结点的最小访问概率[9,13]。对分布式访问控制决策系统而言，访问策略 w 对每个 Q 有访问概率 $w(Q)$，对 quorum 的访问概率引入了对结点 as 的访问概率 $l_w(as):=\sum_{as\in Q_i} w(Q_i)$，最忙访问结点就是指系统中能使 $l_w(as)$ 取值最大的 as，由此引入系统对访问策略 w 的负载 $L_w(\mathcal{Q})=\max_{as\in U}\{l_w(as)\}$，而系统负载即最小的 $L_w(\mathcal{Q})$ 值，$L(\mathcal{Q})=\min_w\{L_w(\mathcal{Q})\}$[9]。

定理 1 如果 $\mathcal{Q}$ 是 n 个元素的全集上的 quorum 系统，则 $L(\mathcal{Q})\geqslant\max\{\frac{1}{c(\mathcal{Q})}, \frac{c(\mathcal{Q})}{n}\}$，$c(\mathcal{Q})$ 表示 $\mathcal{Q}$ 中的最小 quorum 规模，还有 $L(\mathcal{Q})\geqslant\frac{1}{\sqrt{n}}$。

证明：$\exists Q'\in\mathcal{Q}, s.t.\ |Q'|=c(\mathcal{Q})$，设 w 为任一 $\mathcal{Q}$ 上的访问策略，考察 Q' 中所有结点的负载，可得：

$$\sum_{as\in Q'} l_w(as)=\sum_{as\in Q'}\sum_{as\in Q_i} w(Q_i)=\sum_{Q_i}(|Q'\cap Q_i|\cdot w(Q_i))\geqslant$$

$$\sum_{Q_i} w(Q_i)=1$$

因此，Q'中必存在一点，其负载至少为$\frac{1}{|Q'|}=\frac{1}{C(②)}$。

考察 w 策略下的所有结点的负载之和：

$$\sum_{as\in U} l_w(as)=\sum_{as\in U}\sum_{as\in Q_i} w(Q_i)\sum_{as\in U}(|Q_i|\cdot w(Q_i))\geqslant\sum_{Q_i}(c(②)\cdot w(Q_i))=c(②)$$

因此，U 中必存在一点 as，其负载至少为$\frac{C(②)}{|U|}=\frac{C(②)}{n}$。

负载是在系统有最优访问策略的情况下，且没有任何结点失效时才能达到的，负载越小，单个结点被访问到的次数就小，就能够为其它访问提供服务，这样系统的稳定性就越强。若 $m\approx n$，按照读 quorum 的选取方法可知，其规模为 $k(k=m\times n)$，此时读 quorum 负载 $L^R\geqslant\max\{\frac{1}{C(②)},\frac{C(②)}{k}\}=\frac{1}{\sqrt{k}}$；同样，写 quorum 规模为 $2k$，此时写 quorum 负载 $L^W\geqslant\max\{\frac{1}{2\sqrt{k}},\frac{2\sqrt{k}}{k}\}=\frac{2}{\sqrt{k}}$。显然，增大 quorum 系统的服务器结点容量能减少 quorum 的读写负载，但也不能为了减少 quorum 的负载而一再增加 quorum 系统的结点数，因为这会增加系统的成本和加大读写延时的开销。

上节给出的分布式访问控制决策系统 MQ-DACDS 中，作为授权服务决策点的服务器有可能遭受入侵攻击行为而失效，若将每个结点失效看作为等概率且独立的事件，则可设每个结点在某一时刻有效工作的概率为 p，而读 quorum 的成功率表示为 $Ava^R_{m,n}$，写 quorum 的成功率表示为 $Ava^W_{m,n}$。

根据之前读操作的描述可知，读 quorum 的可用性(availability)即为在决策结点集 $U=\{as_1,as_2,\cdots,as_k\},k=m\times n$ 中能成功挑选出某个列覆盖集的概率，而对某一列来说，其中至少有一个结点存活，此概率为 $1-(1-p)^m$，则 $Ava^R_{m,n}=$[存在列覆盖集]$=(1-(1-p)^m)^n$

写 quorum 的可用性(availability)是在读 quorum 成功的基础上再成功挑选出一列决策结点的概率，也可看作是读 quorum 成功的概率去掉读 quorum 成功却无法成功挑出一列存活结点的概率，考察其中一列，至少有一个结点存活又不能所有点都存活事件的概率为 $1-(1-p)^m-p^m$，那么对所有列，存在一个列覆盖集同时不存在完整存活的一列的概率为 $(1-p^m-(1-p)^m)^n$，因此写 quorum 概率可表达为：

$$Ava^W_{m,n}=(1-(1-p)^m)^n-(1-p^m-(1-p)^m)^n$$

系统访问能力也是衡量 quorum 系统性能的重要参数，MQ-DACDS 系统的主要功能是为 AEF 提供访问控制的决策结果，其系统的访问性能主要体现在读操作的效率上。MQ-DACDS 系统的读操作不能和写操作并发执行，但由于写操作是在访问控制策略需要更新/维护时才进行的，这与系统内随时在进行的请求访问控制决策结果(即读操作)的次数是数量级上的差别。不妨忽略写操作带来的负面影响，考虑系统在有结点失效情况下的读并发执行能力，称此能力为系统访问容量(Cap)。

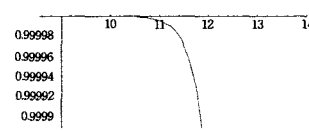
设 MQ-DACDS 为 $m\times n$ 网格 quorum 系统，其各结点有效工作的概率为 p，整个系统存活率在不低于 S 的条件下，$Cap(②)$为系统最多能同时提供的读访问的个数。若系统能同时提供 r 个读访问，则有 r 个读 quorum 同时存在，即有至少 r 个列覆盖集能被同时挑出。首先，能成功挑出第一个列覆盖集的事件为在每一列中必须有至少 1 个结点存活，此事件发生的概率为 $1-(1-p)^m$(即式(1))，n 列就是 $P^R_1=(1-(1-p)^m)^n$；在这之后能成功挑出第二个列覆盖集可看作在 $(m-1)\times n$ 规模的系统内挑出一个列覆盖集，那么此事件成功的概率就为 $P^R_2=(1-(1-p)^{m-1})^n$；……；依此类推，成功挑出第 r 个列覆盖集的概率为 $P^R_r=(1-(1-p)^{m-(r-1)})^n$，再依照概率的链式法，能同时发生以上 r 个事件即能成功提供 r 个读访问的概率为发生这 r 个事件的概率之积。

因此 $Cap(②)$满足如下关系：

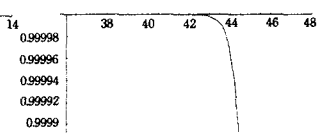
$LP:Cap(②)=\max\{r\}$，

$$s.t.\begin{cases}Ava=\prod_{l=0}^{r-1}P^R_l\\ P^R_l=(1-(1-p)^{m-l})^n\\ Ava\geqslant S\end{cases}$$

对不同的(m,n)取值，系统中每个结点正常工作的概率 $p=0.99$，则系统同时提供的读访问个数 r 与系统可用性的关系如图 5－图 7。由图可知，对每种(m,n)的组合都存在一个阈值 r_m，当系统提供的读访问个数小于 r_m 时，系统可用性为接近于 1 的概率值，说明此时系统相当健壮，还有余力提供更多的读服务，而一旦提供的读个数大于 r_m，系统可用性下降得非常迅速，因此 r_m 应作为系统的最佳选择，是系统容量的合理取值，既保证了系统能以相当高的可用性稳定运行，又能挖掘出系统的最大潜能，同时为访问控制实施机构提供多个并行的访问控制决策。

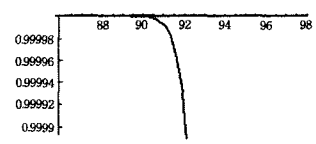


$m=n=15,p=0.99,r_m=11$



$m=n=50,p=0.99,r_m=43$

图 5　读容量和系统可用性的关系　图 6　读容量和系统可用性的关系



$m=n=100,p=0.99,r_m=91$

图 7　读容量和系统可用性的关系

结束语　本文提出了一种以 quorum 访问方式设计的通用访问控制系统，新型的系统具有如下特点：

(1)访问控制决策过程不再依赖于单个 as，提高了访问控制的可用性；

(2)通过写 Q 的交叉性质，保证了全体 as 数据(访问政策)的一致性和有效性；

(3)通过读 Q 的构造方式，实现了多访问控制决策的并行执行；

(4)读 Q 和写 Q 分离，将访问控制决策过程与政策管理分隔开，即：应用服务器的 $AEFx$，只有通过请求读 Q 才能完成并行的访问控制决策；而政策管理者，只能通过请求写 Q 才能实施访问控制政策的维护与更新，增强了访问控制的安全性；

(5)读 Q 和写 Q 交叉性质，确保了访问控制决策过程得

(下转第 111 页)

OL]. http://java.sun.com/products/jini/2.1/doc/specs/html/js-spec.html,2002

[4] Murphy A L, Picco G P, Roman G-C. LIME: A Coordination Model and Middleware Supporting Mobility of Hosts and Agents[J]. ACM Transaction on Software Engineering and Methodology, 2006, 15(3): 279-328

[5] Grimm R, Davis J, Lemar E, et al. System Support for Pervasive Applications [J]. ACM Transactions on Computer Systems, 2004, 22(4): 421-486

[6] Welsh M, Culler D, Brewer E. SEDA: An Architecture for Well-conditioned Scalable Internet Services [C]// Proceedings of the Symposium on Operating Systems Principles (SOSP). Chateau Lake Louise, Canada, 2001: 230-240

[7] Eugster P T, Felber P A, Guerraoui R, et al. The many faces of publish/subscribe [J]. ACM Computing Surveys, 2003, 35(2): 114-131

[8] Segall B, Arnold D, Boot J, et al. Content based routing with elvin4 [C]// Proceedings AUUG2K. Canberra, Australia, June 2000

[9] Opyrchal L, Prakash A. Secure distribution of events in content-based publish subscribe systems [C]// 10th USENIX Security Symposium. Aug. 2001

[10] Carzaniga A, Rosenblum D S, Wolf A L. Design and evaluation of a wide-area event notification service [J]. ACM Transactions on Computer Systems, 2001, 19(3): 332-383

[11] Cugola G, Di Nitto E, Fuggetta A. The JEDI event-based infrastructure and its application to the development of the OPSS WFMS [J]. IEEE Transactions on Software Engineering, 2001, 27(9): 827-850

[12] Hayton R, Bacon J, Bates J, et al. Using events to build large scale distributed applications [C]// Proceedings of the ACM SIGOPS European Workshop. 1996

[13] Pietzuch P R. Event-based middleware: A new paradigm for wide-area distributed systems? [C]// 6th CaberNet Radicals Workshop. February 2002

[14] Muhl G, Fiege L. Supporting covering and merging in content-based publish/subscribe systems: Beyond name/value pairs [J]. IEEE Distributed Systems Online, 2001, 2(7)

[15] Ousterhout J K. Why Threads Are A Bad Idea (for most purposes) [C]// Presentation given at the 1996 Usenix Annual Technical Conference. January 1996

[16] Curbera F, Duftler M J, Khalaf R, et al. Colombo: Lightweight middleware for service-oriented computing [J]. IBM Systems Jouranl, 2005, 44(4): 799-820

[17] 陆钟万. 面向计算机科学的数理逻辑 [M]. 北京: 科学出版社, 1998

(上接第 94 页)

到的是最新政策。

结合互斥 quorum 协议，本文提出了一种基于互斥协议分布式访问控制决策系统 MQ-DACDS，描述了其构造读写 quorum 的方式，并对其性能作了分析。重点讨论了在系统中有服务器结点遭受入侵攻击的情况下，系统能提供的最大访问控制容量同系统可用性之间的关系。结果表明，合理的系统容量选取能使系统性在发挥充分的同时不影响系统的可用性。

这种基于 quorum 系统的访问控制系统有着高安全性和高可靠性的特点，能高速应对并发访问控制请求，使系统整体性能和安全性都有显著提升。基于 Quorum 系统的分布式访问控制这一模型还能有效运用于现有的对等网络、安全操作系统、分布式计算、军事任务管理系统等，对这些系统提出具体的访问控制模型也是进一步的研究目标。

参 考 文 献

[1] Abrams M, LaPadula L, Eggers K, et al. A generalized framework for access control: An informal description[C]// The 13th National Computer Security Conference. 1990

[2] ITU-T, Rec. X.812, ISO/IEC 10181-3, The Security Frameworks for Open Systems: Access Control Framework, 1996

[3] Beznosov K, Deng Y. Engineering access control in distribution applications. 2000

[4] Thompson M, Johnston W, Mudumbai S, et al. Certificate-based access control for distributed resources [C]// Proceeding of Eighth USENIX Security Symposium (Security '99). 1998: 215-228

[5] Park J S, Sandhu R, Ahn G. Role-based access control on the Web[J]. ACM Transaction on Information and System Security. 2001, 4(1): 37-71

[6] Woo T Y C, Lam S S. A framework for distributed authorization [C]// Proceedings of the 1st ACM Conference on Computer and Communications Security. ACM Press, 1993: 112-118

[7] Woo T, Lam S. Designing a Distributed Authorization Service [C]// Proceedings of 17th Annual Joint conference of the IEEE Computer and Communications Societies, INFOCOM, IEEE. 1998: 419-429

[8] Malkhi D. Quorum Systems [J]. Encyclopedia of Distributed Computing, 1999, 3(1): 25-30

[9] Naor M, Wool A. The load, capacity and availability of quorum systems[C]// Proceedings of 35th IEEE Sump. Found. of Comp. Science. 1994: 214-225

[10] Cheung S Y, Ahamad M. The grid protocol: A high performance scheme for maintaining replicated data[J]. Knowledge and Data Engineering, 1990, 4(6): 438-445

[11] Peris R J, Alonso G, Kemme B, et al. Are Quorums an Alternative for Data Replication[J]. ACM Transactions on Database System, 2003, 28(3): 257-294

[12] 宋平，孙建伶，何志均. 基于 Quorum 系统容错技术综述[J]. 计算机研究与发展，2004，41(4)：513-523

[13] Malkhi D, Reiter M. Byzantine quorum systems [J]. Distributed Computing, 1998, 11(4): 203-213

[14] 张薇，马建峰，王良民. 门限 Byzantine quorum 系统及其在分布式存储中的应用[J]. 电子学报，2008，36(2)：314-319