基于虚拟组织和移动代理的网格认证机制研究*)

陈宏伟[1] 王汝传[1,2] 韩光法[1]

(南京邮电学院计算机与科学系 南京210003)[1]

(南京大学计算机软件新技术国家重点实验室 南京210093)[2]

摘 要 认证是网格安全的重要组织部分。在网格中,认证的基本场景包括:证书和证书链、身份认证、会话认证。基于虚拟组织和移动代理的网格特色是以虚拟组织为基本管理单元、以移动代理作为网格结点之间重要的交互手段。本论文的主要内容是把网格认证的基本场景内容引入到基于虚拟组织和移动代理的网格中。基于虚拟组织的网格认证场景主要包括:用户登录虚拟组织、用户获取虚拟组织内部资源、用户获取虚拟组织外部资源。基于移动代理的网格认证场景主要包括:移动代理和移动代理平台之间交互、移动代理之间交互、移动代理迁移。

关键词 认证,网格安全,虚拟组织,移动代理

Authentication Mechanism Study in Grid Based on Virtual Organization and Mobile Agent

CHEN Hong-Wei[1] WANG Ru-Chuan[1,2] HAN Guang-Fa[1]

(Department of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003)[1]

(State Key Laboratory for Novel Software Technology at Nanjing University, Nanjing 210093)[2]

Abstract Authentication is an important aspect of grid security. In grid, the basic scenes of authentication include certificate and certificate chain, dentity authentication and session authentication. We can regard the VO(virtual organization) as the basic management unit of grid, and the MA(mobile agent) as an interactive means of nodes in grid thesis. The main content of the thesis is to introduce the basic content of authentication in grid to the grid based on VO and MA. Authentication Scenes of a grid based on VO include that users logging on VO, obtaining resources in VO, and obtaining resources beyond VO. Authentication Scenes of a grid based on MA include interaction of a MA and MAP(mobile agent platform), interaction of a MA and MA, migration of a MA.

Keywords Authentication, Grid security, Virtual organization, Mobile agent

1 引言

网络计算就是指通过高速网络把分散在各处的硬件、软件、信息资源连结成一个巨大的整体,从而使得人们能够利用地理上分散于各处的资源,完成各种大规模的、复杂的计算和数据处理的任务。网格安全问题是网格计算中的一个核心问题。网格必须提供基本的安全服务包括:认证、授权、访问控制、完整性、审核、保密以及抗否认等。此外,良好的体系结构中还应包括安全的单点登录、合并的审核日志和日志分析、安全性管理、会话保护、统一的安全性粒度等特性。目前常用的网格安全技术主要有 Kerberos,X.509,SSL 等。

认证是网格中的最基本的安全服务功能之一。认证是对实体所宣称的身份确定其有效性的过程。那些请求访问某个受保护组件请求发起者,或者是某个安全会话或事务处理的发起者,必须提供能够证实其身份的凭证信息。本论文主要探讨基于虚拟组织和移动代理的网格认证安全机制。因此,在讨论网格环境中认证机制之前,先介绍虚拟组织和移动代理。

网格整合分布在局域网或广域网的资源,使这些资源成为一个巨大的虚拟计算机系统。目的是在大量个体、机构组织等之间利用安全、协同式的资源共享,创建一个动态虚拟组织(VO-Virtual Organization),基于这种虚拟动态组织的网格计算不仅跨地域,而且延伸到不同的组织、异构的软件硬件平台,为每一个连接到网格的用户提供一个无限的计算能力、沟通协作能力及信息获得能力。在网格计算环境下,采用基于虚拟组织的分布式管理模式,它使得作业实体从资源控制、任务调度和管理的复杂的工作中解脱出来。为了获得充分而必需的资源,各个 VO 可以通过使用标准的、开放的、通用的协调和接口进行交互信息,并根据这些信息来协调各自的资源使用策略,避免系统的盲目查找和不合理远程调用的现象,以此大大提高了网格计算环境的智能性,体现了具有"网格意识"的特征。在地域上分布的异构网格计算环境下能自主地将计算任务从一计结点迁移到另一结点;并可与其它 VO 组织或资源组交互以实现作业和资源的管理和自适应。

移动代理是一个能在异构网络中自主地从一台主机迁移到另一台主机,并可与其他 Agent 或资源交互的程序,实际上它是 Agent 技术与分布式计算技术的结合体。在网格计算中引用移动 Agent 技术将会有以下优点:(1)地域上分布的异构网格计算环境下能自主地将计算任务从一个计算结点迁移到另一结点;并可与其它 Agent 或资源交互以实现对作业和资源的管理和自适应。(2)移动 Agent 可以迁移到网格计算环

*)本课题得到国家自然科学基金(60173037和70271050)、江苏省自然科学基金(BK2003105)、江苏省计算机信息处理技术重点实验室基金(jks03061)资助。陈宏伟 博士生,主要研究方向为网络技术、移动代理和信息安全等。王汝传 教授,博士生导师,主要研究方向是计算机软件、计算机网络、信息安全、移动代理和虚拟现实技术等。韩光法 硕士研究生,主要研究方向为基于网络的计算机软件技术。

境的各个任务运行结点上，与之进行本地高速通信，它不再占用网络资源，从而大大降低了网格的通讯量，并提高了网络资源的利用效率。(3)在网格计算中，移动 Agent 不需要统一的调度。由用户创建的 Agent 可以异步在不同计算结点运行，等任务完成再将结果传送给用户。同一用户或同一计算结点可创建多种 Agent，同时在一个或多个结点运行，形成并行求解的能力。

2 网格环境中的基本认证机制

2.1 网格环境中的基本认证场景

基于场景的安全分析方法是考察网格计算安全性要求的最直接的方法。网格环境中的基本认证场景包括身份认证和会话认证。身份认证主要采用非对称加密的方法进行数字签名，从而确定双方的身份。在身份认证之后，双方可以通过公钥加密体制进行保密通信，然而由于公钥加密的速度较慢，以此进行保密通信不太合适，因此会话认证是通过单钥加密体制进行加密的。此外会话认证还采用杂凑函数对消息进行完整性认证。

证书是由某个可信任的认证中心 CA 建立，并由 CA 或用户存放，以方便其他用户访问。在身份认证中，双方要相互交换自己的公钥。可以通过公钥证书的方式使得双方安全地交换公钥。在双方进行会话时，需要共用一个会话密钥才能会话，会话密钥的生成可以通过在身份认证中完成。

可对符号作出如下定义：E-加密；D-加密；SK-秘密钥；PK-公开钥；K-会话密钥；M-消息；H-杂凑函数；ID-标识；T-时戳；R-随机数；CA-认证中心；CERT-证书；A、B-认证主机。

2.2 证书和证书链

证书的格式为：$CERT_A=ESK_{CA}(T_A,ID_A,PK_A)$。该公钥证书由 CA 为用户 A 建立；该证书由 CA 通过私钥加密作为数字署名可用来证明 A 身份，并提供 A 的公钥，其中时戳可以看成是证书的截止日期。

证书验证为：$DPK_{CA}[CERT_A]=DPK_{CA}[ESK_{CA}(T_A,ID_A,PK_A)]=T_A,ID_A,PK_A$。也就是只要接收方有 CA 的公钥就能验证 CA 为 A 发放的证书。接收方通过解读证书，就能获取发送方的公钥。

在证书验证的时候，有时会遇到证书链的问题。假设 X《Y》表示 X 为 Y 发放证书，则认证链 X《Y》Y《A》表示 X 为 Y 发放证书，Y 为 A 发放证书。若接收方 B 知道认证中心 X 的公钥，则 B 通过此链可得到 A 的公钥。此链可无限延长。

2.3 身份认证

在 A、B 进行相互身份认证时，可以通过认证中心 CA 来参与认证。有第三方参与的身份认证过程如下：

(1)$A\rightarrow CA:EPK_A(ID_A,ID_B)$

(2)$CA\rightarrow A:EPK_A(ESK_{CA}(T_A,ID_A,PK_A),ESK_{CA}(T_B,ID_B,PK_B))$

(3)$A\rightarrow B:EPK_B(ESK_{CA}(T_A,ID_A,PK_A),ESK_{CA}(T_B,ID_B,PK_B),ESK_A(T,K,R))$

(4)$B\rightarrow A:EPK_A(ESK_B(T,K,R))$

其中，在第(3)步中，R 表示 A 发向 B 的一个随机产生的数，它可以防止网络上的重新攻击。K 表示 A 和 B 为进行会话而产生的会话密钥。

2.4 会话认证

会话认证主要对双方来回传递的消息进行认证。会话认证的过程如下：

(1)$A\rightarrow B:E_K(M_A,ESK_A(H(M_A)))$

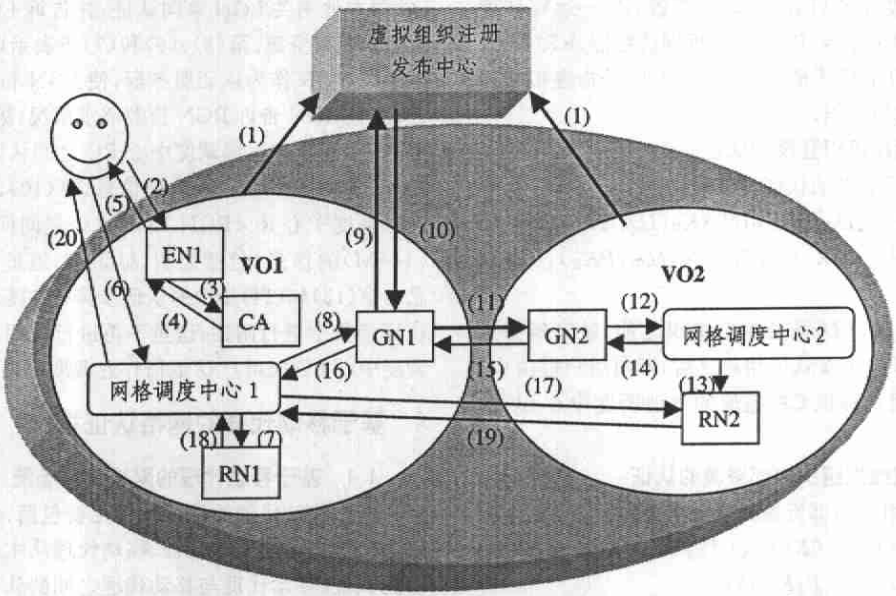
(2)$B\rightarrow A:E_K(M_B,ESK_B(H(M_B)))$

消息的杂凑使用公钥加密算法和发方的秘密钥加密后，与消息连接，再对连接后的结果用单钥加密算法加密，这种方法提供了保密性和数字签名。

3 基于虚拟组织的网格认证机制

3.1 基于虚拟组织的网格认证场景

图1是基于虚拟组织的网格认证场景的示意图。



注：VO-虚拟组织；EN-入口结点；GN 网关结点；RN-资源结点；CA-认证中心

图1 基于虚拟组织的网格认证场景示意图

其中入口结点(entrance node)是指为用户注册和登录到虚拟组织，并获得网格服务的结点。网关结点(gateway node)

是指虚拟组织之间能够进行直接交互的结点。资源结点(resource node)是指能够为用户提供服务资源的结点;资源包括计算资源、存储资源、打印机、传感器等等。虚拟组织注册发布中心用于注册和发布虚拟组织所提供的服务,它类似于 Web Services 中的 UDDI。网格调度中心的功能是对用户提交的作业进行调度,并对虚拟组织内的资源进行管理。

可对图1的基于虚拟组织的网格认证场景作如下说明:(1)虚拟组织 VO1和 VO2向虚拟组织注册发布中心注册其服务。(2)用户向虚拟组织 VO1的入口结点 EN1传递认证信息。(3)EN1把用户的认证信息转发给认证中心 CA。(4)CA 认证通过,并进行电子签名;把信息转交给 EN1。(5)EN1把用户认证通过和 CA 签名的信息转交给用户。(6)用户向虚拟组织 VO1的调度中心1提出作业要求。(7)调度中心1获取本地网格资源 RN1,并向 RN1分配任务。(8)调度中心1发现虚拟组织 VO1的资源无法完成用户任务,则向网关结点 GN1汇报。(9)GN1向虚拟组织注册发布中心提出服务查询要求。(10)虚拟组织注册发布中心告诉 GN1有关虚拟组织 VO2的信息,包括 GN2地址和有关认证信息。(11)GN1向 GN2提出认证要求和请求有关资源的信息。(12)GN2认证通过,则向 VO2的调度中心2提出资源请求。(13)调度中心2选取合适资源 RN2,并告诉网格调度中心1的认证信息。(14)网格调度中心2通知 GN2有关资源结点 RN2的信息。(15)GN2转告 GN1有关资源结点 RN2的信息。(16)GN1转告任务调度中心1有关资源结点 RN2的信息。(17)任务调度中心1向远程网格资源 RN2认证,并向 RN2分配任务。(18)RN1完成任务,向任务调度中心1返回运行结果。(19)RN2完成任务,向任务调度中心1返回运行结果。(20)任务调度中心1汇集运行结果,并向用户返回运行结果。

从用户角度看,基于虚拟组织的认证场景包括:用户向虚拟组织登录的认证、用户获取虚拟组织内部资源的认证、用户获取虚拟组织外部资源的认证。可对符号作出如下定义:U—用户,EN—入口结点,CA—本地认证中心,RCA—远程认证中心。LC—本地调度中心,LRN—本地资源,RC—远程调度中心,LGN—本地网关结点,RGN—远程网关结点,RRN—远程资源,VOR—虚拟组织注册发布中心。本地是指虚拟组织内,而远程是指跨虚拟组织。

3.2 用户向虚拟组织登录的认证

用户向虚拟组织登录的认证步骤为:

(1)$U \rightarrow EN \rightarrow CA: ID_U, EPK_{CA}(ESK_U(ID_U, ID_{LC}))$

(2)$CA \rightarrow EN \rightarrow U: EPK_U(ESK_{CA}(T_U, ID_U, PK_U), ESK_{CA}(T_{LC}, ID_{LC}, PK_{LC}))$

第(1)步中,在用户 U 登录虚拟组织之前,就已经知道 CA 的公钥。第(2)步中,CA 认证用户之后,不向用户提供 CA 签署的证书,还向用户提供 CA 签署的本地调度中心 LC 的公钥证书。

3.3 用户获取虚拟组织内部资源的认证

用户获取虚拟组织内部资源的认证步骤为:

(1)$U \rightarrow LC: EPK_{LC}(ESK_{CA}(T_U, ID_U, PK_U), ESK_{CA}(T_{LC}, ID_{LC}, PK_{LC}), ESK_U(T, K, R))$

(2)$LC \rightarrow U: EPK_U(ESK_{LC}(T, K, R))$

(3)$U \rightarrow LC: E_K(M_U, ESK_U(H(M_U)))$

(4)$LC \rightarrow LRN(1 \cdots M)$:

(5)$LRN(1 \cdots M) \rightarrow LC$:

(6)$LC \rightarrow U: E_K(M_{LC}, ESK_{LC}(H(M_{LC})))$

在第(1)和(2)步中,用户 U 和本地调度中心 LC 完成相互身份认证,并提供会话密钥 K。第(3)步中,用户 U 和本地调度中心 LC 进行会话,用户 U 向本地调度中心提出作业调度要求。第(4)和(5)步中的认证步骤将在基于移动代理的网格认证场景中进行阐述,这里不再进行说明。第(6)步中,本地调度中心 LC 向用户 U 返回作业调度结果。

3.4 用户获取虚拟组织外部资源的认证

用户获取虚拟组织外部资源的认证步骤为:

(1)$U \rightarrow LC: EPK_{LC}(ESK_{CA}(T_U, ID_U, PK_U), ESK_{CA}(T_{LC}, ID_{LC}, PK_{LC}), ESK_U(T, K, R))$

(2)$LC \rightarrow U: EPK_U(ESK_{LC}(T, K, R))$

(3)$U \rightarrow LC: E_K(M_U, ESK_U(H(M_U)))$

(4)$LC \rightarrow LGN: EPK_{LGN}(ESK_{CA}(T_{LC}, ID_{LC}, PK_{LC}), ESK_{LC}(M_{LC}))$

(5)$LGN \rightarrow VOR: EPK_{VOR}(ESK_{VOR}(T_{LGN}, ID_{LGN}, PK_{LGN}), ESK_{LGN}(M_{LGN}))$

(6)$VOR \rightarrow LGN: EPK_{LGN}(ESK_{VOR}(T_{LGN}, ID_{LGN}, PK_{LGN}), ESK_{VOR}(T_{RGN}, ID_{RGN}, PK_{RGN}))$

(7)$LGN \rightarrow RGN: EPK_{RGN}(ESK_{VOR}(T_{LGN}, ID_{LGN}, ID_{LGN}), ESK_{VOR}(T_{RGN}, ID_{RGN}, PK_{RGN}), ESK_{LGN}(M_{LGN}))$

(8)$RGN \rightarrow RC: EPK_{RC}(ESK_{RCA}(T_{RGN}, ID_{RGN}, PK_{LGN}), ESK_{LGN}(M_{LGN}))$

(9)$RC \rightarrow RRN(1 \cdots M): EPK_{RRN(1 \cdots M)}(ESK_{RCA}(T_{RC}, ID_{RC}, PK_{RC}), ESK_{RC}(M_{RC(1 \cdots M)}))$

(10)$RC \rightarrow RGN: EPK_{RGN}(ID_{RC}, ESK_{RC}(M_{RC}))$

(11)$RGN \rightarrow LGN: EPK_{LGN}(ID_{LGN}, ESK_{RGN}(M_{RC}))$

(12)$LGN \rightarrow LC: EPK_{LC}(ID_{LGN}, ESK_{LGN}(M_{RC}))$

(13)$LC \rightarrow RRN(1 \cdots M)$:

(14)$RRN(1 \cdots M) \rightarrow LC$:

(15)$LC \rightarrow U: E_K(M_{LC}, ESK_{LC}(H(M_{LC})))$

第(1)、(2)和(3)步同上面一样,用户 U 和本地调度中心 LC 相互认证,并生成会话密钥。第(4)步表示本地调度中心 LC 向本地网关 LGN 单向认证,并告诉 LGN 用户需要跨虚拟组织调用资源。第(5)、(6)和(7)步表示以虚拟组织注册发布中心 VOR 作为认证服务器,使 LGN 和 RGN 完成相互认证;并且 LGN 告诉 RGN 资源需求情况。第(8)、(9)步表示远程网关 RGN 与远程调度中心 RC 之间认证、RC 与远程资源结点 RRN(1…M)之间认证信息。第(10)、(11)、(12)步表示远程调度中心 RC、RGN、LGN、LC 之间回传远程资源 RRN(1…M)的信息(包括公钥、标识符、地址、资源属性等等信息)。第(13)和(14)步中的认证步骤将在基于移动代理的网格认证场景中进行阐述,这里不再进行说明。第(15)步中,本地调度中心 LC 向用户 U 返回作业调度结果。

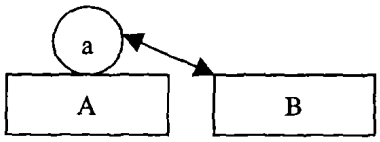
4 基于移动代理的网格认证机制

4.1 基于移动代理的网格认证场景

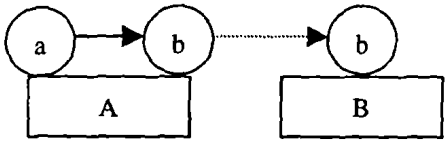
基于移动代理的认证场景主要包括:移动代理和非本地移动代理平台之间的认证、移动代理从本地移动代理平台迁移的认证、移动代理与移动代理之间的认证。图2是基于移动代理的网格认证场景的示意图。

我们可以通过基于移动代理的网格计算中任务调度的场景的例子对图2网格认证场景作如下说明:(a)a 是任务调度 agent;a 在移动代理平台 A 上。B 是资源结点上的移动代理平台。任务调度 agent a 与资源结点上的移动代理平台 B 进

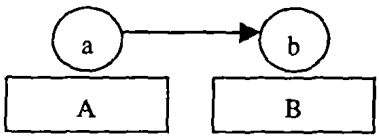
行相互认证。(b)任务调度 agent a 创建子任务 agent b,并把 b 迁移到移动代理平台 B 上执行。(c)任务调度 agent a 和子任务 agent b 相互传递消息:如 agent a 监视 agent b 的执行情况;agent a 和 agent b 执行相互协作;以及 agent b 向 agent a 返回结果等等。



(a) 移动代理和非本地移动代理平台之间的认证



(b) 移动代理从本地移动代理平台迁移的认证



(c) 移动代理从本地移动代理平台迁移的认证

注: a、b—移动代理; A、B—移动代理平台

图2 基于移动代理的网格认证场景示意图

基于移动代理的认证场景可以用如下符号进行描述:

$a(A,B,act)\rightarrow b(C,D)|C$ 表示移动代理 a 在移动代理平台 A 中被创建,当前的位置正在移动代理平台 B 上,a 正在执行动作 act。act 包括创建(create),迁移(migrate),复制(clone),销毁(destroy),认证(authenticate),传输消息(transfer)等等。$\rightarrow$ 表示 a 所交互的对象为移动代理 b(表示移动代理 b 在移动代理平台 C 中被创建,当前的位置正在移动代理平台 D 上),或移动代理平台 C。

$A(act)\rightarrow b(C,D)|C$ 表示移动代理平台 A 正在执行动作 act。act 行为以上可参考。$\rightarrow$ 表示 A 所交互的对象为移动代理 b(C、D 解释同上)或移动代理平台 C。

假设移动代理平台 A、B 互相知道对方的公钥,并信任对方。

4.2 移动代理和非本地移动代理平台之间的认证

移动代理和非本地移动代理平台之间的认证步骤为:

(1)$A(create)\rightarrow a(A,A):ESK_A(ID_a,T_a,PK_a),(ID_B,T_B,PK_B)$

(2)$a(A,A,authenticate)\rightarrow B:EPK_B(ID_a,ESK_A(ID_a,T_a,PK_a),ESK_a(ID_a,K_{aB}))$

(3)$B(authenticate)\rightarrow a(A,A):EPK_a(ID_B,ESK_B(ID_B,K_{aB}))$

第(1)步表示移动代理平台 A 创建移动代理 a;并向 a 签署表明 a 身份的证书;以及向 a 提供移动代理平台 B 的公钥信息。第(2)和(3)步表示 a 与 B 相互认证,并生成会话密钥。

4.3 移动代理从本地移动代理平台迁移的认证

移动代理从本地移动代理平台迁移的认证步骤为:

(1)$a(A,A,create)\rightarrow b(A,A)$:

$ESK_A(ID_a,T_a,PK_a),ESK_a(ID_b,T_b,PK_b),(ID_B,T_B,PK_B),K_{ab}$

(2)$b(A,A,migrate)\rightarrow B:K_{aB}(M_b,EPK_B(H(M_b)))$

(3)$b(A,B,Authenticate)\rightarrow B:EPK_B(ESK_A(ID_a,T_a,PK_a),ESK_a(ID_b,T_b,PK_b),E_{bB})$

(4)$B(authenticate)\rightarrow b(A,B):EPK_b(ID_B,ESK_B(ID_B,K_{bB}))$

(5)$b(A,B,transfer)\rightarrow B:K_{bB}(M_b,EPK_B(H(M_b)))$

(6)$B(transfer)\rightarrow b(A,B):K_{bB}(M_B,EPK_b(H(M_B)))$

第(1)步表示移动代理 a 创建移动代理 b;并向 b 签署表明 b 身份的证书;以及向 b 提供移动代理平台 B 的公钥信息,并生成 a 和 b 通信的会话密钥。第(2)表示移动代理平台 A 把移动代理 b 迁移到移动代理平台 B 上。第(3)和(4)表示 b 和 B 相互认证,在认证过程中存在着认证链的问题。B 和 B 生成会话密钥。第(5)和(6)步表示 b 与 B 通过会话密钥进行通信,并对消息进行认证。

4.4 移动代理与移动代理之间的认证

移动代理与移动代理之间的认证步骤为:

(1)$a(A,A,transfer)\rightarrow b(A,B):K_{ab}(M_a,ESK_a(H(M_a)))$

(2)$b(A,B,transfer)\rightarrow a(A,A):K_{ab}(M_b,ESK_b(H(M_b)))$

第(1)和(2)步表示移动代理 a 与 b 通过会话密钥进行通信,并对消息进行认证。

结束语 本论文主要是针对基于虚拟组织和移动代理的网格的认证机制的研究,它具有以下特色:(1)以虚拟组织为网格的基本管理单位;并给出了在虚拟组织内如何认证,虚拟组织之间如何认证的解决方案。(2)以移动代理技术作为网格结点之间交互的重要手段;并给出了移动代理之间,以及移动代理与移动代理平台之间不同场景如何认证的解决方案。

参 考 文 献

1 Foster I, Kesselman C, Tsudik G, Tuecke S. A Security Architecture for Computational Grids [A]. In: Proc. 5th ACM Conf. on Computer and Communications Security Conf. [C]. USA: ACM Press, 1998. 83～92

2 Foster I, Kesselman C, Tuecke S. The Anatomy of the Grid: Enabling Scalable Virtual Organizations [J]. International Journal of High Performance Computing Applications, 2001, 15(3): 200～222

3 Huang Li-can, Wu Zhao-hui, Pan Yun-he. Virtual and Dynamic Hierarchical Architecture for Chinese University e-Science Grid [A]. In: Proc. of the Intl. Workshop on Grid and Cooperative Computing[C]. 北京:电子工业出版社, 2002. 297～311

4 WANG Ru-Chuan, MU Hong, XU Xiao-Long, ZHANG Deng-Yin. Building Grid Computing Environment with Mobile Agent Technology[A]. In: Proc. of the Intl. Workshop on Grid and Cooperative Computing[C]. 北京:电子工业出版社, 2002. 1075～1084

5 杨波. 网络安全理论与应用[M]. 北京:电子工业出版社, 2002

6 都志辉, 陈渝, 刘鹏. 网格计算[M]. 北京:清华大学出版社, 2002

7 何炎祥, 陈莘萌. Agent 和多 Agent 系统的设计与应用[M]. 武汉:武汉大学出版社, 2001