供应链中 RFID 信息的复合访问控制模型*)

闫新庆　尹周平　熊有伦

(华中科技大学数字制造装备与技术国家重点实验室　湖北 430074)

摘　要　供应链中实体间关系的动态性、交叉性、多变性和复杂性为供应链中 RFID 数据及关联信息的安全访问带来了巨大的挑战。在分析实体和实体、用户和实体之间关系的基础上,综合多种信息访问控制模型,提出了一种适合于数字供应链的 RFID 数据及关联信息的复合访问控制模型,设计了一种信息访问控制的授权规范,建立了一种关系以实现从用户到信息访问权限的映射,给出了用户对信息访问权限的判断流程。结合关系型数据库和工作流引擎,给出了该复合访问控制模型的实现方法。

关键词　数字化供应链,RFID,访问授权,映射,工作流

Composite Access Control Model for RFID Information in Supply Chain

YAN Xin-qing　YIN Zhou-ping　XIONG You-lun

(State Key Laboratory of Digital Equipment and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract　The dynamic, crossover, versatility and complex relation among entities in a supply chain brings great challenges for the access control of RFID data and related information. Based on the analysis of relation between entities, user and entities, a composite access control model for the RFID data and related information in digital supply chain was presented, which combines some of the existed access models. An authorization specification for information access was designed, the map between user and information access authorization is established, and the workflow to decide whether a use can access some information is given. An implementation for such composite access control model is given based on relational database and workflow engine.

Keywords　Digital supply chain, RFID, Authentication, Mapping, Workflow

由于市场的全球化和分工的专业化,企业在经营过程中往往要和上游及下游企业动态组成供应链,根据各自不同的分工,在共享信息的基础上进行协同工作以快速响应,满足市场的需求。在供应链中,企业间的交互往往涉及通过互联网完成大量的产品及相关信息的及时传递和共享,形成协同网络和数字化供应链。在这个过程中,如果能给每个产品一个唯一的标识,通过标识访问产品的相关信息,则可以大大改进供应链内的物流过程,实现高效、实时的产品知识共享。

RFID(Radio Frequency Identification)标签由于无接触的批量物体识别,能赋予物理实体一个唯一的身份标识,从而建立连接物理实体世界和数字化虚拟空间的桥梁[1],构建实现物理实体间协作的"物联网"。RFID 技术已经被广泛用于企业应用的多种领域,成为企业提高效率、降低成本、实现管理信息化、增强企业核心竞争力不可缺少的技术工具和手段。将 RFID 技术引入供应链,可以为供应链的发展提供一种基础保障,作为一种催化剂使企业供应链的发展提高到一个新的阶段[2]。如沃尔玛集团就要求其供应链上游企业在送向其物流中心的货柜上贴装 RFID 标签,以实现高效的供应链和物流管理体系,加快作业进度,实现商品的高效配送和管理等。

但是,RFID 标签自身的数据存储容量有限,目前常用标签的存储容量从数百到数万字节不等,无法存储所关联实体的所有信息,通常只能为关联实体赋予唯一的身份标识,而将实体的信息存放在网络化的信息管理系统中,并依赖信息管理系统,实现从 RFID 标识到其关联实体信息之间的映射。为了保证数字供应链的高效,企业应该开放和共享 RFID 标识数据及实体相关信息。但是这些信息可能包含企业的经营机密,如果被竞争对手获取,将对企业的正常经营造成严重的损失。因此,需要考虑和设计在供应链中 RFID 及相关实体信息的安全访问机制。

但是供应链中企业之间的关系往往是动态、多变、交叉和复杂的,导致整个供应链系统成为一个网状结构[3],供应链中的不同企业可能在执行某个任务时结成合作伙伴关系,但在另外的任务中则可能为竞争对手。企业之间关系的多变性、不确定性和供应链系统的复杂结构,为供应链中 RFID 数据及相关实体信息的安全共享和访问控制带来了巨大的挑战。

网络环境下的信息访问控制一直是信息安全领域研究的热点问题,虽然目前已经提出了多种信息访问控制策略,但把这些策略直接应用到供应链中,实现 RFID 信息的安全访问控制时都还存在自己的缺点和不足。为此,在集成多种信息访问控制模型的基础上,我们提出了一种复合的信息访问控制模型,实现供应链中 RFID 信息的安全访问控制,提高供应链管理水平。

本文的结构如下:第 1 节对常用的信息访问控制模型和

*)国家 863 计划项目(项目批准号:2006AA04A110),国家重点基础研究发展计划(973)(项目批准号:2003CB716207),国家杰出青年基金项目(批准号:50625516)。**闫新庆**　博士后,主要研究领域为 RFID 应用、网格计算、中间件技术等;**尹周平**　博士,教授,博士生导师,主要研究领域为电子制造、数字化制造、网络制造等;**熊有伦**　教授,博士生导师,中国科学院院士,主要研究领域为电子制造和数字化制造等。

目前企业间的 RFID 信息共享方法进行了分析；第 2 节提出了一种针对 RFID 信息在供应链系统中企业间共享的访问方法，在分析供应链中企业之间复杂关系的基础上，提出了信息访问控制方法，定义了一种规范的 RFID 信息访问控制语言，并给出了信息访问控制的授权算法；第 3 节给出了结合关系型数据库和工作流的复合访问控制模型的实现方法例；最后总结了本文的工作。

1 相关的研究工作

信息的访问控制研究起源于 20 世纪 70 年代。尤其是近年来，互联网的发展给信息的安全和访问控制带来了巨大的挑战，世界各国的研究人员也先后提出了多种信息访问控制模型。目前最常用的信息访问控制模型有基于角色的访问控制模型(Role Based Access Control，RBAC)、基于任务的访问控制模型(Task Based Access Control，TBAC)、基于联盟的访问控制模型(Coalition Based Access Control，CBAC)和关系驱动的访问控制模型(Relation Driven Access Control，RDAC)等。

Ferraiolo 等[4,5]提出的 RBAC 模型，其突出优点是简化了各种环境下的信息访问授权管理。通过引入角色这一中介，实现了用户与资源访问权限的逻辑分离。角色指定了对资源访问控制的权限，一个用户可以隶属于多个角色。RBAC 是目前最常用的信息访问控制模型的基础，已经被用于多种领域。虽然 RBAC 已经达到了成熟的应用水平，但是仍然无法解决需要所有分布式应用系统中信息访问控制的需求，研究人员在 RBAC 的基础上，提出了许多新的扩展模型，如 TBAC 和 CBAC 等。

TBAC[6]把任务作为资源的访问控制和授权的一项重要参数。作为一种主动的安全模型，它适用于为了执行某项任务，为用户设定对数据、信息和应用系统的访问权限。TBAC 基于主体-客体模式，使用访问决策函数来决定主体是否拥有对信息访问的权限，从应用的角度提供了信息安全访问管理机制。

CBAC[7]则面向联盟体多个企业间资源共享的多变性和企业间的信任关系，提供了在联盟体中跨多个组织环境下的资源访问控制方案，强调针对组织内和跨组织的信息安全的不同需求，设置不同的信息访问控制权限。

RDAC[8]则针对动态和复杂的多企业组成的组织中的信息访问控制，提出了共享资源的访问控制策略应该基于访问请求者和资源提供者之间的关系决定。在 RDAC 中，资源请求者和提供者之间的关系是动态和双向的。

由于供应链中企业间关系的动态性、复杂性、不确定性甚至矛盾性，这几种信息访问控制模型都无法直接用于解决对供应链中 RFID 信息进行访问时的安全控制问题。

目前，在 RFID 系统中，还很少使用这些信息访问控制模型。如在目前常用的 EPCglobal 组织提出的 EPC 网络中，RFID 信息在多个组织之间的共享是通过本地 ONS(Object Naming System)、全局 ONS 和 Web 服务使能的 EPCIS(EPC Information System)等协同完成的[9]。一个企业的产品在供应链中移交给另外一个组织时，同时会将该产品的 RFID 信息从自己的 ONS 里复制到另外组织的 ONS 中，新的产品拥有者拥有对该 RFID 信息的完全控制权，这种方案的安全访问控制机制显然还是非常初级的。

为此，我们在集成前面讨论的信息访问控制模型的基础上，提出了一种在数字供应链中 RFID 信息访问控制的复合模型，有效解决了供应链中 RFID 信息的安全共享问题。

2 RFID 信息复合访问控制模型

2.1 供应链中的实体关系

供应链中用户和企业之间、企业与企业之间的关系是实现整个系统中 RFID 信息安全访问控制的基础，因为企业根据用户和关联企业彼此之间的关系决定 RFID 信息共享访问控制的策略。我们可以把供应链中用户、企业和企业间的关系分为如下的 4 类：

1)角色和企业之间的关系。角色是用于授权用户访问某些信息的基本方法，它反映了企业中具有不同作用的工作岗位的语义抽象描述。角色之间通常具有层次关系，通常可以通过多种规则指定这种层次关系。在供应链中，用户常常需要访问其它企业受保护的 RFID 数据及对应实体的信息，需要实现在某个企业中定义的角色能被正确映射到另一个关联企业中的角色集合中。

2)企业和企业之间的关系。在供应链中，多个企业可能会形成复杂的关系，如隶属关系、合作关系、竞争关系等，而且企业间的关系在供应链中是动态的。如两个企业可能在实施和完成不同的任务时，互为供应链的上下游企业；多个企业也可能在完成不同任务时，形成不同的竞争或合作关系。供应链中企业关系的多样化和动态不确定，是实现供应链中信息安全访问控制的最大挑战。

3)基于任务联盟的关系。多个企业在完成一项任务时，可以结为动态的联盟。企业中和任务相关的部分信息需要在联盟企业之间共享。随着联盟的动态建立和撤销，这些信息访问机制也需要相应进行改变。在企业同时参与多个任务联盟时，针对不同的联盟需要设置不同的信息访问控制权限。

4)企业和供应链系统的成员资格关系。通常，供应链中的信息是只对加入供应链系统的成员开放，只有在企业加入该供应链后，才能访问和使用这些信息。

基于用户和企业之间、企业和企业之间的这 4 种关系，可以把供应链中共享的 RFID 及实体信息分为三类：供应链内的共享信息、面向任务的联盟内共享信息和企业间的共享信息。供应链内的共享信息可以被加入供应链中的所有企业共享和访问；面向任务的联盟内的共享信息可以被联盟内的企业根据访问控制规则授权访问，信息的发布者可以为联盟中不同的成员设定不同的访问权限。企业的信息可以被企业内部和关联企业的人员依据授权规则，使用不同的权限进行访问。

2.2 访问控制规范

基于信息访问控制的 RBAC，TBAC，CBAC 和 RDCA 模型，我们设计了一种供应链中 RFID 及实体信息访问控制的复合授权规范，如图 1 所示。

在 Ahn 和 Sandhu 提出的 RBAC 限制语言[10]的基础上，我们提出了一种正规化和严格的信息访问控制授权语言。该语言的基本元素和功能如表 1 所示。供应链中信息的发布者根据自己的需要，使用该访问控制语言指定对发布的 RFID 数据及相关信息的访问授权，限制供应链中的用户和企业对信息的访问。

表 1 访问控制语言的基本元素和函数

$U=\{u_1,u_2,\cdots,u_n\}$，用户集合

$R=\{r_1,r_2,\cdots,r_n\}$，角色集合

$T=\{t_1,t_2,\cdots,t_n\}$，任务集合

$C=\{c_1,c_2,\cdots,c_n\}$，公司集合

$CO=\{co_1,co_2,\cdots,co_n\}$，联盟集合

$OP=\{op_1,op_2,\cdots,op_n\}$，操作集合

$OBJ=\{obj_1,obj_2,\cdots,obj_n\}$ 对象集合

$P=OP\times OBJ$，访问许可$\{p_1,p_2,\cdots,p_n\}$

$S=\{s_1,s_2,\cdots,s_n\}$，会话集合

$CT=$分类类型，{"role","task","company","relationship","coalition"}

$RH\subseteq R\times R$，角色的层次关系

$CR\subseteq C\times C$，公司之间的关系

$WF\subseteq T\times T$，多个任务组成的工作流

$CLS=R\cup T\cup U\cup CR\cup CO$，对象的分类

$UA\subseteq U\times R$，多对多的用户－角色对应关系

$TA\subseteq R\times T$，多对多的角色－任务对应关系

$RA\subseteq R\times C$，多对一的角色－公司对应关系

$CA\subseteq C\times CO$，多对多的公司－联盟对应关系

$PA\subseteq P\times R\cup P\times T\cup P\times C\cup P\times CO$，多对多的访问授权关系，可以对角色、任务、公司和联盟进行访问授权

会话用户：$U\rightarrow T$，把会话映射到用户的函数；

用户：$R\rightarrow U$，把一个角色映射到一个用户集合的函数；

角色：$U\cup P\cup S\rightarrow R$，把集合 U，P 和 S 映射到一个角色集合的函数；

公司：$U\rightarrow C$，把每个用户映射到一个公司集合的函数

会话：$U\rightarrow S$，把每个用户映射到一个会话集合的函数；

访问许可：$R\cup T\cup C\cup CO\rightarrow P$，把集合 R，T，C 和 CO 映射到一个访问许可集合的函数；

操作：$R\times OBJ\rightarrow OP$，对每个角色和对象映射一个操作集合的函数；

关系：$C\times C\rightarrow CO$，把两个公司映射成为联盟的函数；

拥有：$OBJ\rightarrow C\cup CO$，返回 Obj 对象的拥有者的函数；

分类：$OBJ\times CT\rightarrow CLS$，映射一个对象和分类类型到一个分类集合的函数。

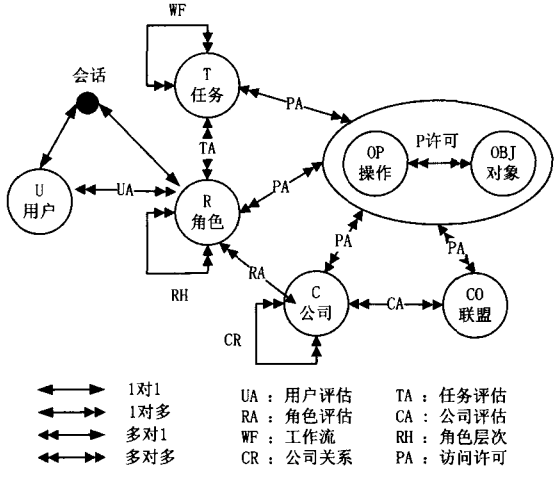

图 1　供应链中 RFID 信息的复合访问控制模型

2.3　RFID 信息的授权访问控制

根据供应链中的用户和企业之间、企业和企业之间的复杂关系和 RFID 信息共享的不同授权，我们设计的复合信息访问控制模型以 RBAC，TBAC，CBAC 和 RDAC 为基础，在这些模型中定义的信息访问授权机制在模型中得到了保留。从资源共享授权方面出发，我们定义了 4 种基本的授权控制方法。

• 角色授权控制：一个角色授权控制指定了一个用户要访问特定资源和相关信息时必须具备的角色。例如，公司 X 可以只允许自己的产品买主访问共享的 RFID 及相关信息。基于角色的 RFID 信息共享可以用信息访问控制语言表示为：$|\text{role}(U)\cap \text{classification}(OBJ,\text{"role"})|\geqslant 1$；

• 任务授权控制：任务授权控制指定了一个企业和用户只有参与某种任务才能访问某种信息。例如，RFID 及关联信息中的敏感部分只能在进行某些任务时才能访问，当任务完成后，这些敏感部分的访问权限将被取消或重新定义。可以用信息访问控制语言定义为：$|\text{task}(U)\cap \text{classification}(OBJ,\text{"task"})|=1$；

• 企业授权控制：表示了一个依赖于企业之间关系的授权。对于企业拥有的信息可以基于用户和企业之间的关系使用这种方法进行授权，由于企业之间可能具有层次关系，一个用户也可能属于多个企业，完整的企业控制授权可能涉及嵌套和递归计算。为了减少计算的复杂度，我们针对 RFID 及关联信息的分类定义了较大粒度的数据授权访问机制，定义为：$\{|C(U)\cap \text{Classification}(OBJ,\text{"company"})|=1\}\cap\{|\text{relationship}(\text{company}(U),\text{owner}(OBJ))\cap \text{classification}(OBJ,\text{"relationship"})|=1\}$；

• 联盟授权控制：指定了联盟中成员的权限，如指定 RFID 信息中的某些部分只能被联盟中的某些成员访问。定义为：$|\text{affiliation}(\text{company}(U)\cap \text{classification}(OBJ,\text{"coalition"})|\geqslant 1$。

组合这 4 种基本的 RFID 信息访问授权控制，这种复合访问控制模型可以支持多种高级的信息访问控制。在供应链系统中，当用户要访问某 RFID 数据及关联信息时，首先使用图 2 中的访问控制评估过程来判断该访问能否得到授权。先根据用户的角色判定是否能得到授权，如果不能则直接返回"Deny Access"；如果可以，则使用基于任务的访问控制继续进行判断，如果不能则同样直接返回"Deny Access"；如果可以，则根据用户所在企业和信息提供企业之间的关系进行判断，如果企业之间的关系是无效的，同样返回"Deny Access"；最后根据企业之间的联盟关系进行判定，如果用户所在企业和信息发布企业隶属于同一个任务联盟，则返回"Permit Access"，否则返回"Deny Access"。

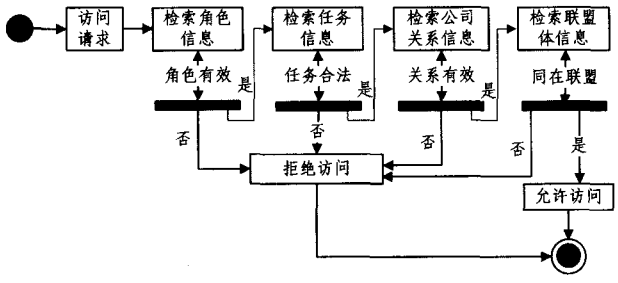

图 2　信息访问授权过程

3　实现及应用

为了实现对 RFID 数据及关联信息访问的复合控制模型，我们在供应链的 RFID 数据管理种中使用了关系型数据库，将表 1 中定义的各种基本元素分别映射为关系型数据库的表，使用表之间的关联关系来表示表 1 中定义的映射函数。基本的关系数据库中表的概要可以用表 2 表示。在表 2 中，下划线字段代表了表的主键，斜体字段表示了表的外键。

表 2　基本的关系型数据库结构表概要

User(U_ID, U_Name, Position, Login, Password, *C_ID*)

Role(R_ID, R_Name, R_Desc)

Task(T_ID, T_Name, T_Desc, Start, Expiration, End, *W_ID*)

Workflow(W_ID, W_Name, W_Desc, Start, End)

Company(C_ID,C_Name,Location,Phone,*Coal_ID*)
Coalition(Coal_ID,Coal_Name,Coal_Desc)
Object(O_ID,O_Name,O_Desc,*Con_ID*)
ObjectConstraints (O_ID,Con_ID,Desc)
Constraints(Con_ID,*R_ID*,*T_ID*,*C_ID*,C_Type,*Coal_ID*,Permission,Start,End)
UserRole(U_ID,R_ID,Desc,Status)
UserTask(U_ID,T_ID,Start,End)

对于给定的 RFID 数据和关联信息，我们可以根据信息的性质、所属的企业、进行访问的用户角色、用于完成的任务和为完成该任务所动态组成的任务联盟等定义访问控制信息。企业在发布信息时，将相关的访问控制信息保存在供应链系统的关系数据库中，同时在系统中提供一个访问 RFID 及相关信息的 Web 服务，在用户请求访问该 RFID 数据及关联信息时，判定用户的访问请求是否得到系统的许可。从第 2 节的讨论可以看出，用户对信息的访问许可判断是通过一个由多个步骤组成的流程来完成的，可以在访问请求许可判断的 Web 服务实现中，引入工作流引擎，进行实现。

基于 Microsoft 公司的 SQL Server 关系型数据库管理系统、Visual Studio. NET 软件开发环境，和提供的工作流开发工具 Windows Workflow Foundations，我们实现了 Internet 环境下数字供应链中 RFID 数据及关联信息的复合访问控制的 Web 服务，用户在对 RFID 数据及相关联信息进行访问时，首先要调用该 Web 服务，根据复合访问控制模型进行权限判断，以决定用户是否有访问该信息的权限。

目前，本文提出的 RFID 信息的复合访问控制模型已经在我们开发的 RFID 应用系统中间件中实现和应用。在 RFID 应用系统中间件中，有机集成了 RFID 标签信息和相关的企业产品多种实体信息，并基于本文提出的访问控制模型，可以将这些信息安全地授权给多个组织中的用户进行访问和使用。

结束语 供应链系统中多个企业之间关系的动态性、交叉性和多变性导致了供应链中 RFID 数据及关联的产品信息访问的安全控制机制的复杂性。本文在分析供应链中实体和实体之间、用户和实体之间的不同关系的基础上，给出了一种 RFID 数据及关联产品信息在供应链中的安全访问复合控制模型，综合使用基于角色的访问控制机制、基于任务的访问控制机制、基于联盟的访问控制机制和关系驱动的访问控制机制等，建立了一种 RFID 及关联信息在供应链中的安全访问控制模型，给出了一种对发布信息指定访问权限的规范化语言，给出了用户和信息访问权限之间的映射关系，讨论了访问许可的判断流程，以实现供应链中 RFID 及关联信息的安全访问。

同时，我们提出了一种该模型的实现机制。并基于微软公司开发的软件开发工具、关系型数据库管理系统和工作流引擎，把该复合访问控制模型通过一个 Web 服务进行实现，可以通过 Internet 进行调用。供应链中的用户在访问 RFID 及相关信息时，必须首先调用该服务以判断用户是否有对该信息的访问许可。这种供应链中 RFID 信息的安全访问控制复合模型已经用于我们开发的 RFID 应用系统中间件系统中。

参 考 文 献

[1] Finkenzeller K. RFID Handbook : Fundamentals and Applications in Contactless Smart Cards and Identification[M]. 2nd Edition, John Wiley & Sons, 2003

[2] Niederman F, Mathieu R G, Morley R, et al. Examining RFID Applications in Supply Chain Management[J]. Communications of ACM, 2007, 50(7): 92-101

[3] 陈安，刘鲁. 供应链管理问题的研究现状及挑战[J]. 系统工程学报，2002，15(2)：179-186

[4] Ferralolo D F, Sandhu R, Gavrila, et al. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security, 2001, 14(3): 224-274

[5] 许峰，赖海光，黄皓，等. 面向服务的角色访问控制技术研究[J]. 计算机学报，2005，28(4)：686-693

[6] Thomas R K, Sandhu R S. Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management[C]// Proceedings of the IFIP WG11. 3 Workshop on Database Security. California, USA. Aug. 1997: 13-19

[7] Cohen E, Thomas R K, Winsborough, et al. Models for coalition-based access control (CBAC)[C]// Proceedings of the 7th ACM Symposium on Access Control Models and Technologies. Monterey, CA, 2002: 97-106

[8] Kang H M, Park J S, Froscher J N. Access control mechanisms for inter-organizational workflow[C]// Proceedings of the 6th ACM Symposium on Access Control Models and Technologies. 2001: 66-74

[9] 谭民，刘禹，曾隽芳，等. RFID 技术系统工程及应用指南[M]. 机械工业出版社，2007

[10] Ahn G, Sandhu R. Role-based Authorization Constraints Specification[C]. ACM Transactions on Information and System Security, 2000, 3(4): 207-226

(上接第 14 页)

[21] Plaxton C G, Rajaraman R, Richa A W. Accessing Nearby Copies of Replicated Objects in a Distributed Environment [J]. Theory of Computing Systems, 1999, 32: 241-280

[22] Padmanabhan V N, Wang H J, Chou P A. Supporting Heterogeneity and Congestion Control in Peer-to-Peer Multicast Streaming [A]// Proc. 3rd Int'l Workshop Peer-to-Peer Systems 2004 (IPTPS). LNCS 3279. Springer, 2005: 54-63

[23] Zhou M, Liu J. Tree-assisted Gossiping for Overlay Video Distribution [J]. Kluwer Multimedia Tools and Applications, 2005

[24] Meddour D-E, Mushtaq M, Ahmed T. Open Issues in P2P Multimedia Streaming [A]// MULTICOMM. 2006

[25] Ratnasamy S, Francis P, Handley M, et al. A Scalable Content-addressable Network [A]// SIGCOMM '01. San Diego, CA, August 2001

[26] Jenkins K, Hopkinson K, Birman K. A Gossip Protocol for Subgroup Multicast [A]// International Workshop on Applied Reliable Group Communication (WARGC 2001). Apr. 2001

[27] Peng Gang. CDN: Content Distribution Network [R]. Research Proficiency Exam Report. Computer Science Department, SUNY at Stony Brook, NY, USA 2003, 2