doi:10.3969/j.issn.1000-436x.2013.09.001

以社区域为中心基于信任的访问控制

姚志强[1,2]，熊金波[1,2]，马建峰[1]，李琦[1]，刘西蒙[3]
(1. 西安电子科技大学 计算机学院，陕西 西安 710071；2. 福建师范大学 软件学院，福建 福州 350108；
3. 西安电子科技大学 通信工程学院，陕西 西安 710071)

摘 要：智能服务 agent 基于上下文感知的交互与协作为数字社区提供动态服务的同时，也带来了安全访问问题。在综合分析数字社区中 agent 的信任、社区域内外协作等特征的基础上，提出以社区域为中心基于信任的访问控制模型，即依据 agent 自身上下文及信任证书建立社区域，其后信任等级随会话动态调整，通过信任等级与信任阈值的匹配关系有效地控制权限的激活和使用。与最新研究成果相比，该模型突出的特点是实现动态权限控制，同时满足社区域内及社区域间角色的安全交互与协作。

关键词：数字社区；智能体；信任；协作；访问控制
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)09-0001-09

Community field-centric trust-based access control model

YAO Zhi-qiang[1,2], XIONG Jin-bo[1,2], MA Jian-feng[1], LI Qi[1], LIU Xi-meng[3]
(1. School of Computer Science and Technology, Xidian University, Xi'an 710071, China;
2. Faculty of Software, Fujian Normal University, Fuzhou 350108, China;
3. School of Telecommunication Engineering, Xidian University, Xi'a na)

Abstract: Context-aware interaction and cooperation among agents provids digital community services. However, it also brings new problems of secure access. A novel community field-centric trust-based access control model (referred to as the CTBAC) was developed by thoroughly considering both the trust level of agent and the cooperation among agents inside and outside of community fields in digital commun ty. There are two novel ingredients. Firstly, a community field was established in terms of agent's own contexts and trust certificate. Thus, the trust level could be dynamically adjusted based on the sessions. Secondly, the activation and use of access control permissions according to the match relationship between the trust level of agents and trust threshold. The proposed CTBAC model was compared to several access control models and its effectiveness in both dynamic permission control and security protection was demonstrated.
Key words: digital community; agent; trust; cooperation; access control

1 引言

无线网络技术和普适计算技术的快速发展促进数字社区中大量智能服务的蓬勃增长，包括数字家庭、健康医疗、数字消防、智能交通和数字城市等。智能体(agent)被认为是实现这种智能服务的基本单元，具有自治性、主动性、社会性和移动性等特点，而数字社区可以抽象成一个多智能体系统(MAS, multi-agent systems)。在 MAS 中，agent 之间丰富的交互能够实现无缝协作，潜在地为大规模复杂问题提供有效的解决途径而成为学术界研究热点[1]。先后提出了多种 MAS：如普适信息社区组

收稿日期：2012-07-02；**修回日期**：2012-11-20
基金项目：长江学者和创新团队发展计划基金资助项目(IRT1078)；国家自然基金委员会—广东联合重点基金资助项目(U1135002)；国家自然科学基金资助项目(61370078)；国家科技部重大专项基金资助项目(2011ZX03005-002)；中央高校基本科研基金资助项目(JY10000903001)；福建省自然科学基金资助项目(2011J01339)
Foundation Items: The Fund for Changjiang Scholars and Innovative Research Team in Un versity (IRT1078); The Key Program of NSFC- Guangdong Union Foundation (U1135002); The National Natural Science Foundation of China (61370078); Major National S&T Program(2011ZX03005-002); The Fundamental Research Funds for the Central Univers ies(JY10000903001); The Natural Science Foundation of Fujian Province (2011J01339)

织[2]和社区计算[3]等。已有的MAS中agent之间的动态协作在一定程度上支持上下文感知需求，然而，MAS的安全性问题，如认证、隐私保护和访问控制等，对各种MAS的实用性构成显著的挑战。本文中主要研究访问控制问题。

访问控制是保障MAS安全的一项关键技术，主要用于防止非授权访问和确保合法agent对信息资源的受限访问和使用。基于角色的访问控制(RBAC, role-based access control)模型[4]及其演化模型以其灵活性和系统无关性等潜在优势而成为MAS访问控制的首选。然而，绝大部分访问控制模型都没有考虑agent之间的交互与协作[1]。而在数字社区或MAS中，agent为了执行某一任务，往往需要与伙伴agent进行多次交互与动态协作，对伙伴进行操作甚至让其执行它的任务以最终实现目标。这种情况下，交互与协作的安全性对目标的实现非常关键，如果agent之间的交互与协作没有合适的授权控制，则非授权的交互或访问可能导致严重的安全威胁[5]。

为此，Jung等提出基于角色交互的访问控制模型(RiBAC, role interaction based access control model)[6]，通过引入交互权限的概念，将agent之间的交互作为访问控制保护的实体实现社区内agent之间的交互安全，但该模型不支持agent之间的安全协作。在RiBAC模型的基础上，文献[1]提出以社区为中心的CRiBAC模型(community-centric RiBAC)，该模型对RiBAC进行扩展以支持协作问题。在CRiBAC模型中，管理员依据agent自身的上下文及任务将其划入相应社区，给agent分配角色，并慎重分配相应的权限给社区内的角色，以保证MAS中社区内部agent之间交互与协作的安全性。

而将社会学中基于信任的理论与方法结合到访问控制机制中，以提高大规模复杂系统对陌生主体的权限控制能力成为当前研究热点[7]。文献[8]将信任和上下文引入基于角色的访问控制中以增强Web服务安全，文献[9]在分布式环境中建立动态可信评估模型，文献[10]在普适计算环境中建立基于信任与推荐的访问控制模型。以上成果为将信任引入数字社区访问控制中以有效控制权限的激活与使用提供新思路。

在数字社区中，agent具有很强的移动性和社会性特征，需要一种比CRiBAC模型[1]更科学和更灵活的社区建立与访问授权方法，如基于信任关系实现agent到社区的注册与动态权限控制；另一方面，多医院联合会诊，紧急交通事故救助、保险赔付等数字社区服务都需要多社区域间的agent之间实施安全且动态的、上下文感知的交互与协作。而代表该领域最新成果的CRiBAC模型中仅考虑社区内部agent之间的交互与协作显然不能充分满足数字社区的协作需求。

针对以上不足，本文提出以社区域为中心基于信任的访问控制模型(CTBAC, community field-centric trust-based access control model)。其核心思想为：首先，为agent引入信任机制，依据agent的信任证书及自身上下文信息注册到社区域，并获取相应角色；然后，在交互与协作过程中，根据直接信任与间接信任的计算获得agent的信任值，从而得到相应的信任等级，实现信任等级的动态调整，并依据信任等级与信任阈值的匹配关系实现对角色所获取权限的激活和使用；最后，CTBAC模型扩展了CRiBAC模型的功能，能同时满足社区域内和社区域间多agent间安全的动态交互与协作。本文方法是基于信任访问控制机制在数字社区的应用扩展，为解决数字社区中访问权限的有效控制与角色之间的安全交互与协作提供一种有益探索。

2 数字社区

本文将数字社区抽象为一个MAS，通过agent之间的交互与协作提供用户所需数字社区服务。当一个服务目标确定时，由系统管理员规划需要的角色，并通过招募合适的agent以形成社区域。社区域建立好后，其角色与协作过程等社区结构可以重用到其他目标的社区域中。当目标实现，则解散社区域并释放成员agent。图1表示数字社区的抽象结构，其元素及描述如下。

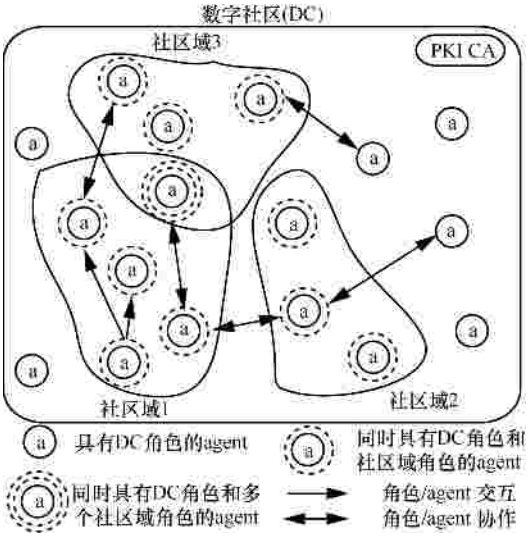

图1 数字社区的组织结构

agent：是数字社区的基本实体单元，agent 可以根据需要加入一个或多个社区域中。

社区域(C, community field)：是一个面向目标的多 agent 协作组，可以根据目标的需要动态创建和解散，所有社区域都属于数字社区。

数字社区(DC, digital community)：包含多个社区域和游离 agent，所有属于数字社区的 agent 具有一个或多个 DC 角色，它同时还可能属于某个社区域而具有 C 角色。

3　CTBAC 模型

3.1　CTBAC 模型的形式化描述

CTBAC 模型建立在 CRiBAC 模型[1]的基础上：1) 增加 agent 的信任等级，实现 agent 到目标社区的注册，在随后的交互和协作过程中，agent 的信任等级能够自适应动态调整；2) 根据信任等级判定是否激活赋予的权限；3) 使用 agent 的信任等级不仅支持社区内角色之间的交互与协作，而且支持社区间角色之间的交互与协作。图 2 表示 CTBAC 模型的整体结构。

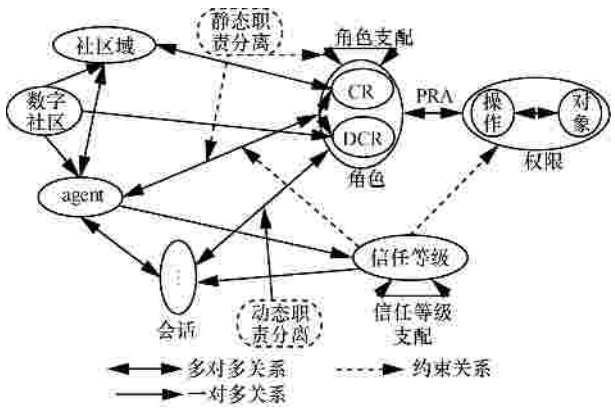

图 2　CTBAC 模型结构

CTBAC 模型定义依据元素的集合及各元素间的相互关系。下面给出 CTBAC 模型的相关元素及其形式化描述。

定义 1　CTBAC 模型具有如下元素与关系。

1) A：数字社区中所有 agent 的集合，其元素为 $a \in A$。每个 agent 自身都具有资源、上下文和任务，$a=\{RSC_a, CONT_a, TSK_a\}$，其中，$RSC_a \subset RSC$，$CONT_a \subset CONT$，$TSK_a \subset TSK$ 表示 a 的资源、上下文和任务的集合。

2) R：数字社区中所有可用角色的集合，分为数字社区角色 DCR 和社区域角色 CR，$R = DCR \cup CR$。

3) $SESS$：CTBAC 模型中所有会话的集合。agent 通过激活会话注册到社区域和发起访问请求。

4) $TrustLev$：agent 信任等级的有限序列集合。每个 agent 在激活一次会话时，根据其资源、上下文和任务等可以获得一个信任等级，根据信任等级获得社会中某个角色。agent 的信任等级随其访问日志、协作者推荐和上下文信息等的变化而动态调整。

5) OBJ：数字社区中关于操作 OPS 的所有对象的集合，包括数字社区中系统资源、角色及角色的任务等。

6) OPS：数字社区中对 OBJ 所有操作的集合，典型的操作如读、写、创建、执行和删除等。

7) $PRMS$：数字社区中授予角色执行任务的所有权限集合，$PRMS = 2^{OBJ \times OPS}$。

8) $C=\{< g_c, A_c, CR_c, CONT_c >\}$，社区域 C 包含 agent 的集合 $A_c \subset A$，及其目标 $g_c \in G$ (G 为目标集)、角色集合 $CR_c \subset CR$ 和社区域上下文 $CONT_c \subset CONT$。

CTBAC 模型存在以下元素之间的数学关系，形式化描述如下。

1) $ARA \subseteq A \times R$，agent-角色之间多对多的分配关系。$ARA = DCRA \cup CRA$，其中，$DCRA \subseteq A \times DCR$，表示 agent- DC 角色之间的分配关系；$CRA \subseteq A \times CR$。$ARA$ 必须满足 agent 的信任等级阈值要求。

2) $PRA \subseteq PRMS \times R$，权限- 角色之间多对多的分配关系。$PRA$ 为预分配的待用权限集合。

3) $AgentSession(a:A) \rightarrow 2^{SESS}$，agent a 到一个会话集合的映射。

4) $SessionRoles(s:SESS) \rightarrow 2^R$，会话 s 到角色集合的映射。

5) $STA \subseteq SESS \times TrustLev$：会话到信任等级的多对一映射。

6) $PT \subseteq PRMS \times TrustLev$，权限与信任等级之间的激活关系，表示当 agent 的信任等级达到信任阈值要求时，才能激活授予相应角色的待用权限，从而实现安全的交互或协作。

7) $RD \subseteq R \times R$，集合 R 上的偏序关系，表示角色之间的支配(dominate)关系，用 $\propto$ 表示支配。在 CTBAC 模型中，存在 2 种可能的支配关系：角色激活支配(A)与权限继承支配(I)。比如 $r_1 \propto_A r_2$ 表示分配给角色 r_1 的 agent 能够激活角色 r_2，但是 r_1

并不继承 r_2 的权限；$r_1 \propto_I r_2$ 则表示 r_1 继承 r_2 的所有权限。利用以上支配关系可以很好地解决基数约束问题，并实现更灵活的策略控制。

数字社区中，为了实现更灵活有效的访问控制，除了定义上面的关系外，还需要定义 CTBAC 模型的相关约束。

定义 2 CTBAC 模型的职责分离和基数约束。

1) $SSoD \subseteq 2^R \times N$，表示 CTBAC 模型的静态职责分离，包括 2 个方面：根据 agent $a \in A$ 的职责要求，当满足信任等级阈值要求时被分配角色 $r_1 \in R_1$, $R_1 \subseteq R$，但不能同时分配给互斥角色 $r_2 \in R_2$, $R_2 \subseteq R$；另外，表示数字社区中，任何一个满足信任等级阈值要求的 agent 不能从激活的角色集合 Rs 中授予超过数量 n 的角色，其中，$Rs \subseteq R$, $n \in N$。形式化为 $\nexists a \in A, TrustLev_a \geq threshold(r) \wedge |authorized\_roles(a) \cap Rs| \geq n$，其中，函数 $authorized\_roles(a)$ 表示 agent $a \in A$ 能分配的角色数量，$TrustLev_a \geq threshold(r)$ 表示 a 满足信任等级阈值要求。

2) $DSoD \subseteq 2^R \times N$，表示 CTBAC 模型的动态职责分离，包括 2 个方面：根据 agent $a \in A$ 的职责要求，在一次会话过程中，满足信任等级阈值要求的 a 激活角色 $r_1 \in R_1, R_1 \subseteq R$ 时，不能同时激活互斥角色 $r_2 \in R_2, R_2 \subseteq R$；另外，表示在一次会话过程中，任何一个满足信任等级阈值要求的 agent 不能从角色集合 Rs 中激活超过数量 n 的角色，其中，$Rs \subseteq R$, $n \in N$。形式化为 $\nexists s \in SESS, TrustLev_a \geq threshold(r) \wedge |\{r \in SessionRoles(s) | r \in R\}| \geq n$，其中，函数 $SessionRoles(s)$ 表示一次会话能够激活的角色数量。

SSoD 和 *DSoD* 实现的是职责分离约束，体现出任何一个满足信任等级阈值要求的 agent 能够承担的角色类型及数量的约束。而每个角色最多能包含多少个 agent？这是基数约束问题。

3) $S\text{-}Cardinality \subseteq A \times N$，表示 CTBAC 模型的静态基数约束。对于给定角色 r，能分配给它的且满足信任等级阈值要求的 a 的数量为 $n = [n_1, n_2]$。形式化为 $n_1 \leq |\{r \in R, a \in A, TrustLev_a \geq threshold(r) \wedge |agent\_assigned(r)\}| \leq n_2$，其中，函数 $agent\_assigned(r)$ 表示分配给角色 r 的 agent 数量。

4) $D\text{-}Cardinality \subseteq A \times N$，表示 CTBAC 模型的动态基数约束。在一次会话过程或特定的时间段中，对于给定角色 r 或它的权限继承支配角色 r'，能分配给它的且满足信任等级阈值要求的 a 的数量为 $n = [n_1, n_2]$。形式化为 $n_1 \leq |\{s \in SESS, a \in A, r \in R, TrustLev_a \geq threshold(r) \wedge |r' \propto_I r, agent\_assigned(r)\}| \leq n_2$。

3.2 CTBAC 授权决策框架

CTBAC 模型的访问控制授权决策过程如图 3 所示，简要解释如下。

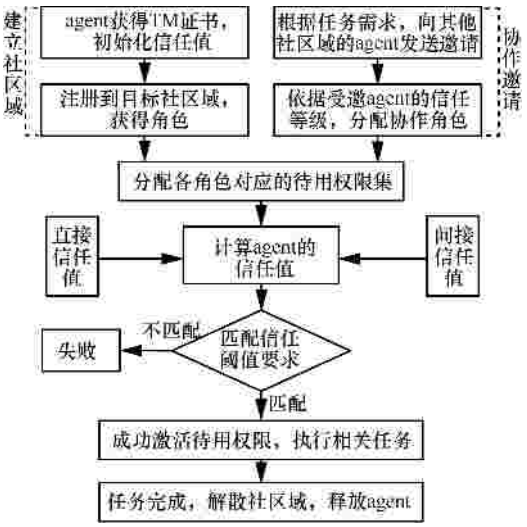

图 3 CTBAC 授权决策过程

1) **建立社区域**：数字社区管理员根据某一个目标任务需求规划社区域，域内 agent 根据其上下文、能力与任务特征等获得数字社区 CA 颁发的 TM (trust management)证书，初始化其 *Trust* 值，达到 *Trust* 阈值要求的 agent 自动注册到目标社区域并通过 *ARA* 关系建立角色，其数量达到职责分离(SSoD 和 DSoD)和基数约束(S-cardinality 和 D-cardinality)条件后，社区域正式成立。

2) **协作邀请**：根据任务需要，如果某社区域的角色不足以实现既定目标时，则需要向其他社区域的角色或 agent 发送协作邀请。与该任务相近的 agent 依据其上下文及任务等决定是否同意加入，社区管理员根据受邀 agent 的 *Trust* 值及对应的 *TrustLev*，达到阈值要求的 agent 根据 *ARA* 分配协作角色。这个过程是可选的。

3) **分配待用权限**：根据完成目标任务的需要，通过 *PRA* 关系给各角色分配相应的权限，包括交互权限和协作权限。该权限为角色获得的待用权限集，表明该权限集暂时不能使用，需要满足一定的信任阈值条件方可使用。

4) *Trust* 值计算：在激活角色的待用权限之前，

还需要计算 agent 的 *Trust* 值以确定 *TrustLev*。每个 agent 根据上下文信息(含数字社区、社区域和自身相关的上下文)、访问日志记录及其他 agent 推荐 *Trust* 值综合计算自身的 *Trust* 值，即可确定 *TrustLev*，从而实现 *TrustLev* 的动态调整。

5) 待用权限激活：*TrustLev* 确定好后，根据匹配信任阈值要求，分选激活待用权限和拒绝待用权限激活两者之一。

6) 社区域解散：目标任务一旦实现，则数字社区管理员解散社区域，并释放社区域角色及所含的 agent。

3.3 CTBAC 模型的交互与协作

在数字社区中，根据任务的复杂性，往往需要多个社区域内的角色相互协作才能很好地完成某一目标任务。CTBAC 模型旨在解决社区域内和社区域间角色的交互与协作问题，下面给出交互与协作及其权限的定义。

定义 3　数字社区中角色对合作伙伴角色及其任务的访问称为 CTBAC 交互，所有交互的集合称为 CTBAC 协作。

角色交互包含 agent 之间的交互，CTBAC 交互/协作包括社区域内和社区域间的交互/协作。

从定义知道，交互分为面向角色(RO, role-oriented)的交互和面向任务(TO, task-oriented)的交互两类[1]。RO 交互表明一个主体角色 R_s 发起一个交互对客体角色 R_o 执行操作。TO 交互表明 R_s 要求 R_o 执行 R_o 的任务以实现某个目标。要实现一次成功的 RO 交互，主体角色必须有相应的交互权限；而对于 TO 交互，客体角色也应该具有能完成请求任务的必要权限。交互权限的集合为协作权限。

在 CTBAC 模型中，社区域内的交互权限关系类似文献[1]，社区域间的角色交互权限如图 4 所示，图中 a_1 和 a_2 分别表示 agent1 和 agent2，c_1 和 c_2 分别表示社区域 1 和社区域 2。CTBAC 模型通过社区域间的交互权限实现社区域间 agent 的交互与协作，通过信任阈值匹配关系保障交互与协作的安全性。

3.4 信任计算

本文将基于信任的访问控制[10,11]引入到 CTBAC 模型中，信任是建立在 agent 与系统对象 OBJ 之间的关系。本文关注 agent 的基于某些属性信息的信任等级，用于初始化 agent 注册及随后信任等级的动态调整，最终实施于访问控制决策中。

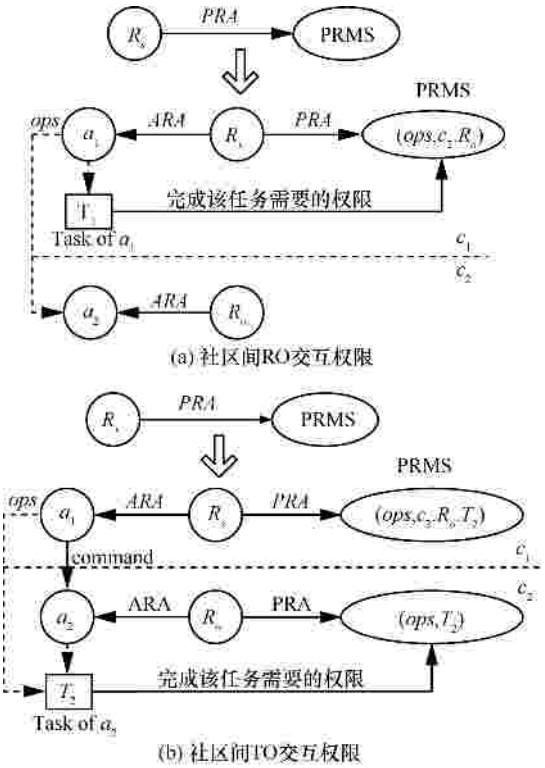

图 4　CTBAC 模型中社区域间的角色交互权限

1) 信任证书注册

在 CRiBAC 模型[1]中，社区域采取招募 agent 的方式，agent 依据自身能力和任务决定是否加入到发出邀请的社区域中，从而给潜在的恶意 agent 进入社区域提供便利。而在数字社区中，选择合适且安全的 agent 对于社区域的组建、社区域间的安全交互与协作等十分重要。因此，在 CTBAC 模型中，除了考虑 agent 的能力及任务之外，还采用可信第三方(如 PKI CA)的 TM 方法，由 CA 提供的 agent 的 TM 证书初始化 agent 的信任值，超过注册信任阈值的 agent 则可注册到目标社区域中。

2) 信任等级动态调整

在 CTBAC 模型中，每个社区域维护一个关于角色、agents、agent 的信任等级、最后一次信任等级修改的时间列表。agents 的信任等级主要考虑访问控制策略中的主体、上下文和时间 3 个维度[10]，用 $\{A, OBJ, CONT, t\}$ 表示信任关系。

agent 的信任等级由其信任值通过映射函数 $Trust_a \in [0.2\times x-0.2, 0.2\times x) \rightarrow TrustLev_a = x$ 确定。其中，$x=\{1,2,3,4,5\}$ 表示信任共分 5 个等级，则 $Trust_a \in [0.0, 1.0)$。agent 的信任等级动态调整通过信任值的变化实现，而信任值主要考虑两方面因素：直接信任值($Trust_{\text{dir}}$)和间接信任值($Trust_{\text{recom}}$)，则 agent

的信任值 $Trust_a = a \times Trust_{\mathrm{dir}} + (1-a) \times Trust_{\mathrm{recom}}$，即

$$Trust_a(a, OBJ_i, CONT_i, t_i) = a \times Trust_{\mathrm{dir}}(a, OBJ_i, CONT_i, t_i) + (1-a) \times Trust_{\mathrm{recom}}(a, OBJ_i, CONT_i, t_i)$$

其中，权值参数 $a \in [0,1]$ 为正常数，通过 a 可以精细调整信任值的大小。

当 agent 之间没有发生交互与协作时，其信任值随时间而衰减，设衰减函数 $f(\Delta t) = k_1 + k_2 \mathrm{e}^{-s \times \Delta t} = k_1 + k_2 \mathrm{e}^{-s \times (t_c - t_0)}$，其中，$\Delta t = t_c - t_0$ 表示 agent 之间没有发生交互与协作的时间间隔，t_c 为当前时间，t_0 为没有发生交互与协作的起点时间，s 为衰减因子，k_1 和 k_2 分别为经验系数和矫正系数[12]。在数字社区中，取 $k_1 = 0.2$，$k_2 = 0.8$，Δt 以小时为单位，s 分别取值为 0.15、0.25 和 0.5 时的衰减函数如图 5 所示。则信任值衰减函数为

$$Trust_a(a, OBJ_i, CONT_i, t_i) - Trust_a(a, OBJ_i, CONT_i, t_i + Dt) = Trust_a(a, OBJ_i, CONT_i, t_i) \times f(Dt)$$

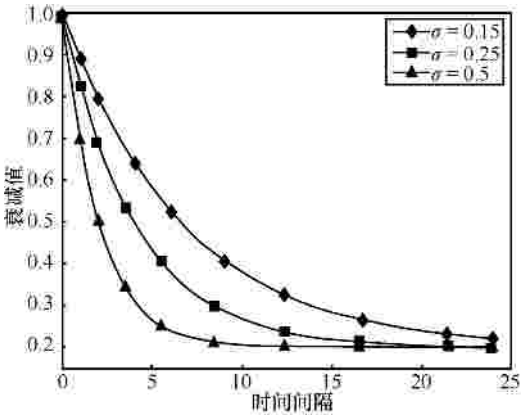

图 5 基于时间的衰减函数

3.4.1 直接信任值计算

agent $a \in A$ 的直接信任值的计算主要依据以下 2 个来源：a 自己激活访问请求和与同伴交互或协作时的上下文信息 $CONT_a$（包括协作相关的数字社区/社区域上下文信息和 agent 自身的上下文信息），与 a 相关的访问日志记录 LOG_a。

上下文信息 $CONT_a$ 定义为 $CONT_a = \{PN \mid PT, W\}$，其中，$PN$ 表示上下文参数名称的集合，$PN = \{pn_1, pn_2, \cdots, pn_n\}$；$PT$ 表示与 PN 对应的上下文参数类型的集合，如 $PT = \{pt_1, pt_2, \cdots, pt_n\}$；$W$ 表示各上下文参数的权重值。比如考虑 agent 位置、网络类型和系统负载等 3 个因素的上下文为 $\{< location \mid string, w_1 >, < networktype \mid long, w_2 >, < systemload \mid integer, w_3 >\}$。定义一个上下文取值函数 $getvalue(pn_i)$，则 $CONT_a = \sum_{i=1}^{N} (getvalue(pn_i) \times w_i) / N$。

从访问日志记录 LOG_a 中抽取与 a 相关的访问历史信息，分为良性访问记录和恶意访问记录。如在过去某一段时间内，a 与对象 OBJ_i 发生交互或合作，产生良性访问记录时的信任值为 $Trust_i$；产生恶意访问记录时的信任值为 $Trust_k$。本文定义 l 和 m 分别为良性访问记录的奖励因子和恶意访问记录的惩罚因子，则

$$LOG_a = \frac{l \times b \times \sum_{i=1}^{N} Trust_i + m \times (1-b) \sum_{k=1}^{M} Trust_k}{N + M}$$

其中，权值参数 $b \in [0,1]$ 为正常数。

综上，直接信任值 $Trust_{\mathrm{dir}} = g \times CONT_a + (1-g) \times LOG_a$，其中，权值参数 $g \in [0,1]$ 为正常数。

3.4.2 间接信任值计算

agent $a \in A$ 的间接信任值主要依据与 a 发生过交互或协作的其他 agent 关于对 a 的推荐信任值，包括社区域内其他 agent 的推荐信任值（$Trust_{\mathrm{in}}$）和其他社区域的 agent 的推荐信任值（$Trust_{\mathrm{out}}$）。$Trust_{\mathrm{recom}} = d \times Trust_{\mathrm{in}} + (1-d) \times Trust_{\mathrm{out}}$，其中，权值参数 $d \in [0,1]$ 为正常数。以上所有权值参数均为经验值，需要多次实验以获得最优值。

社区域内推荐信任值 $Trust_{\mathrm{in}}$ 可以由所有推荐者推荐信任值与推荐者的信任等级 $Trust$ 乘积的平均值求得：

$$Trust_{\mathrm{in}}(a, OBJ_i, CONT_i, t) = \sum_{j=1}^{N_{\mathrm{in}}} (Trust_j(a, OBJ_j, CONT_j, t) \times Trust_j) / N_{\mathrm{in}}$$

其中，N_{in} 表示社区域内所有推荐者的总数。用 N_{out} 表示其他社区域所有推荐者的总数，则其他社区域推荐信任值 $Trust_{\mathrm{out}}$ 为

$$Trust_{\mathrm{out}}(a, OBJ_i, CONT_i, t) = \sum_{j=1}^{N_{\mathrm{out}}} (Trust_j(a, OBJ_j, CONT_j, t) \times Trust_j) / N_{\mathrm{out}}$$

综上所述，根据 $Trust_a = a \times Trust_{\mathrm{dir}} + (1-a) \times Trust_{\mathrm{recom}}$，即可计算出每次交互或协作时的信任值 $Trust_a$。然后根据映射函数即可对应到信任等级 $TrustLev$ 上，最终实现对信任等级的动态调整。

3.5 CTBAC 原型系统体系结构

本节提供数字社区中 CTBAC 原型系统的体系

结构，如图 6 所示。该体系结构解释了本文提出的 CTBAC 模型各模块之间的关系，也为真实数字社区环境中实现 CTBAC 模型提供设计指南。

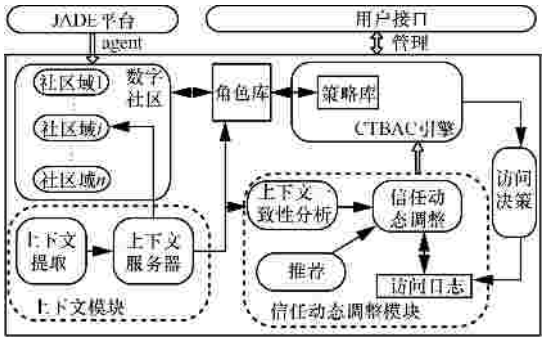

图 6　数字社区中 CTBAC 原型系统体系结构

该体系结构基于 JADE (Java agent development framework)开发平台，主要包含以下几个模块。

1) JADE 平台。该平台是一个著名的 agent 开发平台，广泛应用于 MAS 的开发、仿真和测试[1]。在 CTBAC 原型系统中，数字社区由 JADE 平台的 Jade agent 容器模拟，社区域和 agent 由 Jade agent 模拟，并利用该平台模拟 agent 行为以测试 CTBAC 访问控制策略。

2) 上下文模块。包括上下文提取和上下文服务器：前者提取数字社区/社区域相关上下文以及 agent 自身上下文信息，并将其送给上下文服务器；后者通过上下文本体规范前者提取的上下文信息，如上下文类型和取值，然后将相关信息反馈给社区域、角色库和信任动态调整模块。

3) 角色库。角色库依据上下文服务器提供的上下文信息给相应的 agent 分配角色，角色库与数字社区关联主要实现角色之间的交互与协作功能，与策略库关联主要实现访问控制相关功能。

4) 信任动态调整模块。该模块包含 4 个部分：上下文一致性分析主要接收上下文服务器提供的上下文信息，并与访问请求中的上下文要求进行比较，如果上下文匹配，则进一步处理请求。另外，该一致性分析将匹配的上下文信息送给信任动态调整；信任动态调整功能还接收推荐信任信息，并从访问日志记录中提取信任相关的信息并依据 3.4 节进行信任值计算，以实现信任等级的动态调整。该模块的输出发送给 CTBAC 引擎。

5) CTBAC 引擎。CTBAC 引擎接收来自信任动态调整模块的信息并调整系统数据结构，并依据访问控制策略对访问请求实施访问决策，并将结果保存在访问日志记录中以便随后的动态信任分析。

6) 用户接口。系统管理员通过用户接口实现系统所需的各种管理功能，包括社区域的创建和注销、上下文类型的确定、权限的管理、分配关系的管理和访问策略的制定等。

与 CTBAC 相近的访问控制模型的效能对比分析如表 1 所示，主要从以下 3 个方面进行阐明。

1) 上下文相关信息用于访问控制决策

文献[13]考虑的是普适计算应用环境，利用空间实体对客体、用户位置和地理边界角色建立 GEO-RBAC 模型。文献[14]的上下文感知访问控制(context-aware RBAC)模型中，将上下文信息用于角色成员与权限分配，为上下文感知应用建立一个编程框架。以上仅考虑上下文信息用于授权与决策，文献[15,16]基于行为的访问控制(action-based access control)模型及其管理模型综合角色、环境与时态信息，适用于移动计算和协作计算环境下较灵活的访问控制。文献[17]中的访问控制策略需要负责管理上下文安全需求和上下文改变时策略的动态部署。

然而，以上文献仅考虑外界上下文如时间、位置和其他环境等信息，而没有考虑主体自身的上下文信息如年龄、性别、职务和社会经历等用于授权决策中。而在协作环境中，个人的职务、特长、职称和能力等上下文信息对于协作组织为某一任务

表 1　本文模型与其他访问控制模型的效能对比分析

访问控制模型融合的元素	文献[1]	文献[3]	文献[13]	文献[14]	文献[15]	文献[16]	文献[17]	文献[18]	文献[20]	文献[21]	文献[8]	文献[9]	文献[10]	文献[22]	文献[23]	文献[24]	本文
发挥上下文信息	v	v	v	v	v	v	v	v	×	×	v	×	v	×	×	v	v
支持交互	v	v	×	×	×	×	×	v	v	×	v	v	×	v	v	×	v
支持协作	v	v	×	×	×	×	×	v	v	v	v	v	×	v	v	×	v
参考上下文的信任等级	×	×	×	×	×	×	×	×	×	×	v	×	v	×	×	v	v
参考日志记录的信任等级	×	×	×	×	×	×	×	×	×	×	×	v	v	×	v	×	v
参考推荐元素的信任等级	×	×	×	×	×	×	×	×	×	×	×	×	v	v	v	×	v

挑选协作伙伴时非常关键。为此，文献[18]从 people-tagging 中推导用户属性用于实施协作环境的访问控制策略中，文献[1, 3]在对 agent 授予交互权限时考虑 agent 自身的上下文信息。与此不同的是，在数字社区协作环境中，CTBAC 模型综合考虑与 agent 相关的外部上下文信息和自身上下文信息 2 个方面，用于计算 agent 的直接 Trust 值，以便根据信任阈值判断是否能够激活已分配的交互或协作权限，而已有工作均不能实现这一功能。

2) 支持交互与协作的访问控制

文献[19]是关于协作系统访问控制方面的经典综述，综述了用于协作系统中的各种访问控制模型，但是已有的模型均不支持不同组的安全策略组合，且针对动态协作缺乏有效的管理模型。为此，文献[20]基于组的 RBAC 模型考虑协作系统访问控制策略的组协作问题，但不支持上下文信息。文献[21]假设为某一共同目标的用户或信息都能集合到一组，实现以组为中心的安全信息共享，但是不支持上下文信息和交互授权控制。而文献[1]和 CTBAC 模型都支持这一功能，比文献[1]更完善的是，CTBAC 模型不仅支持社区域内的交互与协作，而且支持社区域间的角色交互与协作，更适合数字社区复杂、动态的协作需求。

3) 融合信任度量的访问控制机制

将信任关系引入协作系统的访问控制决策中也得到研究。文献[8]结合上下文和信任融入 Web 协作应用的访问控制策略中，并根据人类行为和相关的访问上下文信息提出一个可能利用统计模型实现信任等级动态调整的构想，但没有具体的措施。文献[22]在协作云环境中根据不同协作活动、基于属性的推荐和用户之间连接强度的交互推荐解决文件共享时的数据泄露问题，启发本文依据社区域内、外交互 agent 的推荐信息进行间接信任值的计算。文献[23]在云计算环境中提出面向不可信服务消费者的服务可信协商及访问控制策略。文献[9]在分布式计算环境中建立动态可信度评估模型，通过历史交互信息获得直接可信度，并根据每个节点的信用记录和其直接可信度函数的信息量对其直接可信度进行修正，但该文并未考虑间接可信度如何计算和评估。文献[24]进行信任值计算时仅依据上下文信息，而文献[10]的访问控制方案既考虑上下文，还考虑访问控制日志记录和推荐信息等动态计算信任值。

与之不同的是，CTBAC 模型不仅考虑从访问控制日志记录、与 agent 相关的外部和自身上下文信息计算直接 *Trust* 值，还依据与之交互过的社区域内、外其他角色或 agent 的推荐信息计算间接 *Trust* 值，并通过每次会话实现信任等级的动态调整。只有达到信任阈值要求的 agent 才能激活相应分配给角色的权限，从而实现角色之间的安全交互与协作。

4 结束语

提升数字社区中各 agent 之间交互与协作的安全性直接影响数字社区的服务质量，本文提出的 CTBAC 模型与已有访问控制模型相比，具有以下突出特征。

1) 信任等级动态调整机制。CTBAC 模型综合考虑 agent 直接信任计算源和间接信任计算源，得出每次会话的信任值并获得相应的信任等级，实现信任等级的动态调整。

2) 只有当信任等级达到信任阈值要求时，agent 才能激活相应分配给角色的交互或协作权限，并执行任务。如果信任等级低于阈值要求，则权限激活失败，从而有效保护待用权限，实现安全交互与协作。

3) CTBAC 模型不仅支持社区域内角色之间的交互与协作，而且支持社区域间的角色交互与协作。

笔者将进一步的研究工作有：CTBAC 模型的有效管理问题，设计各种管理函数，以实现社区域创建/解散、agent 加入/退出、角色之间的交互与协作等的有效管理；对 X-GTRBAC[25]和 CRiBAC[1]相关的规范语言进行适当扩展，研究一种支持 CTBAC 模型的策略规范语言；根据数字社区的实际协作应用场景，开发并实现所提 CTBAC 原型系统，并对 CTBAC 协作访问控制策略进行性能评估。

参考文献：

[1] JUNG Y, JOSHI J B D. CRiBAC: community-centric role interaction based access control model[J]. Computers & Security, 2012, 31(4): 497-523.

[2] KUMAR M, SHIRAZI B A, DAS S K, *et al*. PICO: a middleware framework for pervasive computing[J]. IEEE Pervasive Computing, 2003, 2(3):72-79.

[3] JUNG Y, KIM M. Situation-aware community computing model for developing dynamic ubiquitous computing systems[J]. Journal of Universal Computer Science, 2010, 16(15):2139-2174.

[4] SANDHU R S, COYNE E J, FEINSTEIN H L. Role-based access

control models[J]. IEEE Computer, 1996, 29(2):38-47.

[5] JUNG Y, KIM M, MASOUMZADEH A, *et al.* A survey of security issue in multi-agent systems[J]. Artificial Intelligence Review, 2012, 37(3):239-260.

[6] JUNG Y, MASOUMZADEH A, JOSHI J B D, *et al.* RiBAC: role interaction based access control model for community computing[A]. Proceedings of the 4th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom'08)[C]. Orlando, FL, USA, 2009, 10(3):304-321.

[7] **郎波**. **面向分布式系统访问控制的信任度量化模型**[J]. **通信学报**, 2010, 31(12):45-54.
LANG B. Access control oriented quantified trust degree representation model for distributed systems[J]. Journal on Comm nications, 2010, 31(12):45-54.

[8] BHATTI R, BERTINO E, GHAFOOR A. A trust-based context-aware access control model for web-services[J]. Distributed and Parallel Databases, 2005,18(1):83-105.

[9] **朱友文**, **黄刘生**, **陈国良等**. **分布式计算环境下的动态可信度评估模型**[J]. **计算机学报**, 2011, 34(1):55-64.
ZHU Y W, HUANG L S, CHEN G L, *et al.* Dynamic trust evaluation model under distributed computing environment[J]. Chinese Journal of Computers, 2011, 34(1):55-64.

[10] ILTAF N, GHAFOOR A, HUSSAIN M. Modeling interaction us ng trust and recommendation in ubiquitous computing environment[J]. EURASIP Journal on Wireless Communications and Networking, 2012,(1):1-13.

[11] CHAKRABORTY S, RAY I. TrustBAC: integrating trust relationships into the RBAC model for access control in open systems[A]. Proceeding of the 11th ACM Symposium on Access Control Models and Technologies (SACMAT'06)[C]. Lake Tahoe, CA, USA, 2006. 49-58.

[12] **石志国**,**贺也平**,**张宏**. **一种对等计算安全性的时间自衰减信任管理算法**[J]. **计算机研究与发展**, 2007, 44(1):1-10.
SHI Z G, HE Y P, ZHANG H. A time self-decay trust management algorithm for P2P computing security[J]. Journal of Computer Research and Development, 2007, 44(1):1-10.

[13] DAMIANI M L, BERTINO E, CATANIA B, *et al.* GEO-RBAC: A spatially aware RBAC[J]. ACM Transactions on Information and System Security (TISSEC), 2007, 10(1):21-42.

[14] KULKARNI D, TRIPATHI A. Context-aware role-based access control in pervasive computing systems[A]. Proceedings of the 13th ACM Symposium on Access Control Models and Technologies (SACMAT'08)[C]. Estes Park, CO, USA, 2008.113-122.

[15] **李风华**, **王巍**, **马建峰等**. **协作信息系统的访问控制模型及其应用**[J]. **通信学报**, 2008, 29(9):116-123.
LI F H, WANG W, MA J F. Access control model and its application for collaborative information systems[J]. Journal on Communications, 2008, 29(9):116-123.

[16] **李风华**, **王巍**, **马建峰等**. **基于行为的访问控制模型及其行为管理**[J]. **电子学报**, 2008, 36(10):1881-1890.
LI F H, WANG W, MA J F, *et al.* Action-based access control model and administration of actions[J]. Acta Electronica Sinica,2008, 36(10): 1881-1890.

[17] PREDA S, CUPPENS F, CUPPENS-BOULAHIA N, *et al.* Dynamic deployment of context- aware access control policies for constrained security devices[J]. Journal of Systems and Software, 2011, 84(7): 1144-1159.

[18] WANG Q, JIN H, LI N. Usable access control in collaborative environments: authorization based on people-tagging[A]. Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS'09)[C]. Saint Malo, France, 2009. 268-284.

[19] TOLONE W, AHN G J, PAI T, *et al.* Access control in collaborative systems[J]. ACM Computing Surveys (CSUR), 2005, 37(1):29-41.

[20] LI Q, ZHANG X, XU M, *et al.* Towards secure dynamic collaborations with group-based RBAC model[J]. Computers & Security, 2009, 28(5):260-275.

[21] KRISHNAN R, NIU J, SANDHU R, *et al.* Group-centric secure information-sharing models for isolated groups[J]. ACM Transactions on Information and System Security (TISSEC), 2011, 14(3):1-29.

[22] WANG Q, JIN H. Data leakage mitigation for discretionary access control in collaboration clouds[A]. Proceeding of the 16th ACM Symposium on Access Control Models and Technologies (SACMAT'11)[C]. Innsbruck, Austria, 2011. 103-112.

[23] **胡春华**, **陈晓红**, **吴敏等**. **云计算中基于** SLA **的服务可信协商与访问控制策略**[J]. **中国科学:信息科学**. 2012, 42(3):314-332.
HU C H, CHEN X H, WU M, *et al.* A service trust negotiation and access control strategy based on SLA in cloud computin China Science: Information Science, 2012, 42(3):314-332.

[24] **刘武**, **段海新**, **张洪等**. TRBAC:**基于信任的访问控制模型**[J]. **计算机研究与发展**, 2011, 48(8):1414-1420.
LIU W, DUAN H X, ZHANG H, *et al.* TRBAC: trust based access control model[J]. Journal of Computer Research and Development, 2011, 48(8):1414-1420.

[25] BHATTI R, GHAFOOR A, BERTINO E, *et al.* X-GTRBAC: an XML-based policy specification framework and architecture enterprise-wide access control[J]. ACM Transactions on Informatio nd System Security (TISSEC), 2005, 8(2):187-227.

作者简介：

姚志强（1967-），男，福建莆田人，西安电子科技大学博士生，福建师范大学教授，主要研究方向为信息安全。

熊金波（1981-），男，湖南益阳人，西安电子科技大学博士生，主要研究方向为访问控制技术与结构化文档安全。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、计算机网络与信息安全。

李琦（1989-），男，江苏淮安人，西安电子科技大学博士生，主要研究方向为基于属性的密码学与访问控制技术。

刘西蒙（1988-），男，陕西西安人，西安电子科技大学博士生，主要研究方向为公钥密码学与信息安全、安全网络编码及其应用。