基于 RBAC 策略的可信网格访问控制模型 *

黄 刚, 王汝传, 田 凯
(南京邮电大学 计算机学院, 南京 210003)

摘 要: 针对网格环境的特点,分析了网格中实体间的信任关系,给出了信任度的计算方法。对 RBAC 技术进行了相应的改进,提出了基于 RBAC 的可信网格访问控制模型,给出了 RTGM 模型中的结构和模块以及访问控制部分的过程。可信网格访问控制提高了网格环境下的访问安全性。

关键词: 访问控制; 信任; 基于角色的访问控制; 网格安全
中图分类号: TP393.08 **文献标志码**: A **文章编号**: 1001-3695(2010)04-1473-04
doi:10.3969/j.issn.1001-3695.2010.04.075

RBAC-based trusted access control model for grid

HUANG Gang, WANG Ru-chuan, TIAN Kai
(*School of Computer, Nanjing University of Posts & Telecommunications, Nanjing* 210003, *China*)

Abstract: As to the characteristics of grid environment, this paper analyzed the trust relationship among the grid entities and provided the method for computing the degree of trust, thus making some corresponding improvements in RBAC technology. It also put forward the trust grid access model based on RBAC. What's more, it offers structure, module and access control process in RTGM model. Trusted access control model enhances grid security in grid environment.
Key words: access control; trust; RBAC(role-based access control); grid security

0 引言

网格是将分布在不同地理位置上的异构资源通过高速网络互连起来以实现充分共享的资源集合, 形成一台巨大的虚拟计算机,以提供高性能计算、管理及服务。网格安全是网格计算的一个基础,网格安全主要集中在网格环境中的安全认证、访问控制、数据完整性、通信机密性等方面。近年来,人们在访问控制的研究方面取得了很大成果,主要的访问控制模型有自主访问控制模型和强制访问控制模型。在总结前人研究成果的基础上,Ferraiolo 和 Kuhn 在 1992 年提出了基于角色的访问控制模型(RBAC)。通过对这些访问控制模型的研究可以看出,因网格环境的分布式、异构性、不可控制等特点,网格的访问控制必须建立在现有的访问控制系统之上。针对基于角色访问控制的不足,引入了信任机制,把信任作为角色分配的一个主要依据,提出了基于角色的可信网格访问控制模型(role-based trusted grid access control model,RTGM)。

在该模型中根据信任域计算信任,用来建立网格环境下同一管理域内和不同管理域之间的实体行为信任关系,能够更加精确地评估实体之间的信任关系,并以此对角色进行分类和分组。信任概念的引入不仅提供了一定程度的身份信任,更重要的是为角色分配提供依据,同时解决了网格环境的动态性和不确定性带来的安全问题。

1 基于 RBAC 的网格访问控制模型

基于角色的访问控制是一个复合的策略,它既有自主访问控制的性质,又有强制访问控制的性质。它将访问许可权分配给角色,用户通过赋予不同的角色获得角色所拥有的访问许可权[1]。

网格中的用户集合 $U=\{U_1,\cdots,U_n\}$ 、客体集合 $O=\{O_1,\cdots,O_n\}$ 、操作集 A 三者组成空间 (U,O,A),(U_i,O_i,A_i) 是空间中的一点,表示 U_i 可对 O_i 进行 A_i 操作;定义 $M=O\times A$,权限 $p\in M$。角色 $R=\{(U_i,O_i,A_i)\mid U_i\in U,O_j\in O,A_i\in A\}$,表示一个角色与一组用户和一组权限相关联,具有该角色的用户有访问某些客体相应的权限。多个角色的并集可以表示空间 (U,O,A) 中的任何一个子集,也就是说,基于角色的访问控制模型能实现网格中的任意一个访问策略,该模型具有通用性。

网格的访问需通过网格和网格节点的授权,网格用户 U_i 的有效访问权限如图 1 中的阴影部分所示,community 在这里指网格,site 则指网格上的节点。网格中 U_i 对 O_j 的访问最后要被映射为节点 u_i 对 o_j 的访问,也就是将网格中的角色 R_i (U_i,O_j,A_k) 映射为节点的角色 $r_i(u_i,o_j,a_k)$。在映射的过程中应该遵守最小权限的原则,这种映射可以是一对一或多对一的关系。

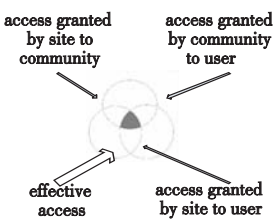

图1 网格用户的有效权限

收稿日期: 2009-08-13; **修回日期**: 2009-09-22 **基金项目**: 国家"863"计划资助项目(2007AA01Z404)
作者简介:黄刚(1961-),男,南京人,副教授,主要研究方向为计算机软件理论、计算机网络(huanggang@njupt.edu.cn);王汝传(1946-),男,教授,主要研究方向为计算机软件理论、计算机网络;田凯(1982-),男,讲师,主要研究方向为计算机网络.

2　信任计算

网格的动态性和不确定性的特点使网格应用环境很复杂，为了保证网格应用的安全，实体间的信任问题显得格外重要，网格中的信任关系可粗略分为身份信任和行为信任。身份信任主要负责身份验证以及用户权限等问题，可通过传统的安全机制如加密技术、访问控制等来解决；行为信任反映网格实体在交互过程中的可靠程度，实体间可根据过去相互间直接的或间接的行为接触经验及时动态地调整更新彼此间的信任关系，从而最大程度地保证网格实体行为的安全可靠。

2.1　网格信任的划分

2.1.1　域间信任与域内信任

网格中不同的安全域可能采用不同的安全策略对域内进行安全管理，各个域之间很难建立一种全局的管理策略。针对网格环境特点，根据实体所处管理域的不同，将网格实体间的信任关系分为域间信任关系和域内信任关系。域内信任关系包括域管理者对管理域内实体在相互协作过程中的行为进行监控、评估，从而确定每一个实体在管理域内的信任度，这个值也是该管理域为网格中其他管理域的实体提供的信任度；域间信任关系指不同管理域之间的推荐信任关系的建立和修改。在这个信任模型的管理下，网格中的资源提供者可以根据域间推荐关系和域内实体的信任度来确定两个实体之间的信任关系，从而接受或拒绝用户的申请。网格信任关系结构如图 2 所示[2]。

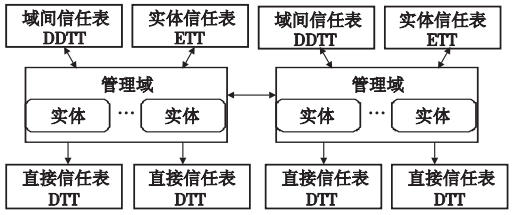

图2　网格信任关系的划分

每个管理域为域内的实体维护一张实体信任表(entity trust table，ETT)，记录域内每个实体的信任度。实体信任表主要是为实体协作提供信任度，它还负责维护域间信任关系表(domain-domain trust table，DDTT)，表中包含了所有与之有过直接交易的域。网格管理域每隔一定的时间就自动更新它的信任表。

域间信任关系基于域间实体之间的交互行为，两个域之间的信任度是根据它们的直接信任关系和其他域的评估综合得出。这里域间信任关系指的是域作为一个整体与其他域之间的直接信任关系，域间实体之间的交易会影响域间信任关系。

2.1.2　直接信任与间接信任

实体之间的信任关系可以分为两类，即直接信任和推荐信任[3]，如图 3 所示。

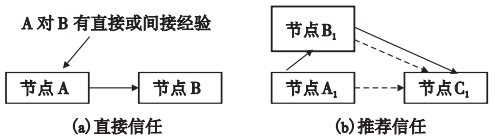

图3　直接信任与推荐信任

直接信任是指两个实体之间曾经有过直接的交易。实体 A 具有对实体 B 的某类经验信息(包括所有直接或间接的经验)。它们之间建立了一种直接信任关系，信任值来源于根据双方的交易情况得出的直接经验。

在一个大规模的分布式系统中，一个实体要想获得系统中其他所有实体的信息是非常困难的，而系统中其他任何一个实体都可能成为该实体的潜在通信对象。当需要与一个陌生的实体交互时，必须先了解它的信誉，以此来决定是否进行交互。而关于这个陌生实体的信息可以通过其他实体的推荐间接得到。推荐信任是指两个实体之间没有进行过直接的交易，而是根据其他实体的推荐建立的一种信任关系。它们之间的信任值是根据其他实体的评估得出的结果。如图 3 所示，A_1 点与 C_1 点的信任关系是在 B_1 点的推荐下形成的。

2.2　信任计算

在角色分配和角色激活过程中，遵循最小特权原则和职责分离原则，以用户的信任度为衡量标准，分配和激活合适的角色。在给角色授权过程中，为了实现细粒度和动态授权，引入了信任度参数。因此，一个重要目标是考虑用户的历史行为信息和上下文信息，准确衡量用户的信任度。用户的主观信任度依赖两方面信息：a)用户与资源的直接交互经验，属于直接信任；b)其他实体对用户的评价，属于推荐信任[4]。

信任度评估模型借鉴 A. Josang 的主观逻辑理论的思想，采用概率论的二项事件后验概率理论[5]，根据社会学个人信任行为，在同一自治域范围内，用户的行为近似于概率 p 的二项事件，因此可利用二项事件后验概率分布服从 beta 分布的特性推导信任关系。设 r 和 s 分别表示观测到的用户所产生的肯定事件数和否定事件数，概率变量为 θ，则用户的概率确定性密度函数为

$$\varphi(\theta|r,s)=\frac{\Gamma(r+s+2)}{\Gamma(r+1)\Gamma(s+1)}\theta^{r}(1-\theta)^{s};0\leqslant\theta\leqslant1,r\geqslant0,s\geqslant0$$

则主观信任度三元组 $\omega_B^A=\{b_B^A,d_B^A,u_B^A\}$ 使用下式将 ω 定义为事实空间中肯定事件数 r 和否定事件数 s 的函数：

$$b_B^A=\frac{r+1}{r+s+2},\ d_B^A=\frac{s}{r+s+2},\ u_B^A=\frac{1}{r+s+2}$$

2.2.1　域内信任度的计算

域内信任关系基于域内实体之间的交易以及综合其他实体的评估来计算信任度[6]，用下式计算：

$$TT_Y^X=\beta DTT_Y^X+(1-\beta)RDTT_Y^X,0\leqslant\beta\leqslant1$$

用 TT_Y^X 来表示同一管理域中实体 X 对 Y 的信任度，DTT_Y^X 表示 X 对 Y 的直接信任度，$RDTT_Y^X$ 表示同一管理域中其他实体对 X 推荐 Y 的信任度，β 由实体 X 自己选择设定，表明 X 在重新评价和其他实体之间的信任度时，自己原来持有的对该实体的直接信任记录的影响权重。如果 $\beta=0$ 表明 X 只参考来自推荐路径的联合评价，$\beta=1$ 表明 X 只信任自己的历史评价，$\beta=0.5$ 表明 X 对等看待来自推荐信任路径的联合评价和自己持有的历史评价。

在模型中，每个网格实体维护一张直接信任关系表，表中包含了所有与之发生过直接联系的域内节点。直接信任关系表中的每个表项包括节点名称 name、交互记录$\langle r,s\rangle$、信任度 T，即三元组(name，$\langle r,s\rangle$，$\langle b_Y^X,d_Y^X,u_Y^X\rangle$)。

计算域内两个实体 X、Y 的信任度的计算步骤如下：

a)计算直接信任度。通过查找实体 X 的直接信任表，获得直接信任度 DTT_Y^X，如果没有查找到实体 Y，则 X、Y 之间没有直接交互记录，$DTT_Y^X=\{0,0,1\}$。

b)计算推荐信任度。在查找实体 X 的直接信任表的同时，通过与实体 X 有直接交互的节点递归查找节点 Y，构造推荐网络，通过信任度的传递与合成计算 $RDTT_Y^X$。为了避免查找路径太深，可以限定递归深度，忽略路径对推荐信任度的计

算结果影响很小。

c)计算实体间信任度。通过直接信任度和推荐信任度,选取适当的权重系数 β,通过 $TT_Y^X = \beta DTT_Y^X + (1-\beta)RDTT_Y^X$ $(0 \leqslant \beta \leqslant 1)$计算域内实体间信任度。

2.2.2　域间信任度的计算

信任代理维护域间信任表 DDTT,表中包含了所有与之发生过直接联系的管理域。域间信任表中的每个表项包括域名称 name、交互记录$\langle r,s\rangle$、信任度 T,即三元组(name,$\langle r,s\rangle$,$\langle b_Y^X, d_Y^X, u_Y^X\rangle$)。不同管理域之间两个实体 *MX* 对 *NY* 的信任度的计算步骤如下:

首先计算管理域间的信任度 TT_N^M,TT_N^M表示管理域 *M* 对管理域 *N* 的信任度,即管理域间的直接信任度和推荐信任度。

1)域间直接信任度　*M* 的信任代理查找其域间信任表 DDTT,看是否与 *N* 有直接信任关系,如果有,则将相应的信任度赋予 DTT_N^M,否则 $DTT_N^M = \{0,0,1\}$ 表示 *MN* 之间无直接信任关系。

2)域间推荐信任度　在查找管理域 *M* 的直接信任表的同时,通过与管理域 *M* 有直接交互的其他管理域递归查找管理域 *N*,构造推荐网络,通过信任度的传递与合成计算 $RDTT_N^M$。同样为了避免查找路径太深,可以限定递归深度。

3)域间信任度　根据域间直接信任度和域间推荐信任度来计算域间信任度:

$$TT_N^M = \beta DTT_N^M + (1-\beta)RDTT_N^M, 0 \leqslant \beta \leqslant 1$$

其中:β 表示域间直接信任关系和间接信任关系所占的比重,称为信任权重因子,由管理域 *M* 自己选择设定,表明管理域 *M* 在重新评价与其他管理域之间的信任度时,自己原来持有的对该域的直接信任记录的影响权重。如果 β=0 表明 *M* 只参考来自推荐路径的联合评价,β=1 表明 *M* 只信任自己的历史评价,β=0.5 表明 *M* 对等看待来自推荐信任路径的联合评价和自己持有的历史评价。

再计算实体 *MX* 对 *NY* 的信任度:查找管理域 *N* 的实体信任表,找到域 *N* 赋予域内实体 *Y* 的信任度 T_{NY}^N,则

$$TT_{NY}^{MX} = (\beta DTT_N^M + (1-\beta)RDTT_N^M) \otimes T_{NY}^N, 0 \leqslant \beta \leqslant 1$$

即 *MX* 与 *NY* 所属的两个管理域之间的信任度对管理域 *N* 中实体 *NY* 信任度的推荐。

3　网格中基于信任的访问控制

目前网格为用户分配角色的过程是由安全管理员完成的,安全管理员为用户分配角色后,不能根据用户的行为对用户的角色进行修改,这样不利于控制用户的恶意行为。在实际系统中,如有用户盗取或恶意修改信息网格中的信息或数据,那么他的访问应被受到限制,甚至会被从系统中注销。

基于信任的访问控制把信任值当做为用户分配角色的重要依据,通过建立角色与信任值之间的动态映射,从而有效地控制用户对资源的访问。首先对用户的行为进行信任评估,然后基于信任的量化值对用户进行动态授权[7]。图 4 对有无信任评估的访问控制流程进行了对比分析。

4　可信网格访问控制模型

4.1　网格 RBAC 机制分析

基于 RBAC 的可信网格访问控制模型 RTGM 是在 RBAC 模型基础上增加信任度而来的,RTGM 由用户、角色、信任度、对象、操作、权限、会话等部分构成,如图 5 所示。用户与角色不再预先绑定到一起,用户与信任级别自动协商,根据信任度分配角色集给用户。当用户访问网格时,网格计算用户的信任值,然后根据信任值分配角色,用户获得相应的访问权限。

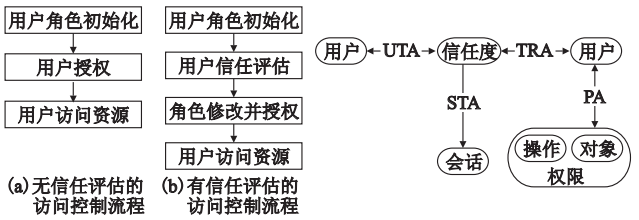

图4　有无信任评估的访问控制流程对比分析

图5　可信RBAC的组成元素

在网格环境中,虚拟组织(VO)作为独立单元对访问控制和资源进行管理。针对虚拟组织中资源数量种类繁多、管理控制复杂的问题,在模型内采用分组的方式对资源进行管理,分组规则由管理员依据资源提供的对象和操作的特点来制定,并且应确保资源具有明确的归类。

4.2　网格访问控制机制的描述

通过前面的分析,可信访问控制模型 RTGM 形式化描述为

$$RTGM = \{USERS, ROLES, PERMS, TT_{NY}^{MX}S\}$$

其中:USERS、ROLES、PERMS、TT_{NY}^{MX}S 分别代表用户集、角色集、权限集和信任度集。

图 5 中,UTA、TRA、STA 分别表示用户—信任、信任—角色和会话—信任之间的关系。其中:

UTA⊆USERS × TRUSTS,表示用户和自己信任度之间的关系;

TRA⊆TRUSTS × SESSIONS,表示信任度和角色之间的关系;

STA⊆SESSIONS × TRUSTS,表示信任度和会话之间的关系;

1)角色指派

$RA_{in} \subseteq R_{in} \times U_{in}$,对内角色指派

$RA_{out} \subseteq R_{out} \times U_{out}$,对外角色指派

$RA = RA_{out} \cup RA_{in}$,表示了角色和主体间的多对多关系

$R(u) = \{r \mid$指派给主体 u 的角色,$u \in U\}$

2)许可集合

$P_{group1} = 2^{(O \times m)_{group1}}$,group1 中资源的对象操作的许可集

$P = P_{group1} \cup P_{group2} \cup \cdots \cup P_{groupN}$整个 VO 中所有资源的对象操作的许可集

3)许可指派

$PA_{out} = R_{out} \times P$ 对外许可指派,$PA_{in} = R_{in} \times P$ 对内许可指派

$PA = PA_{OUT} \cup PA_{in}$表示了许可与角色之间的多对多关系

4)组关系

$O_{group1} \cap O_{group2} \cap \cdots \cap O_{groupN} = \varnothing$限定了一个资源实体只能隶属于一个组,避免由于资源的多重归属问题而增加访问决策的难度

5)角色关系

$R_{in} \cap R_{out} = \varnothing$对外角色和对内角色之间互相独立

$R_{in}H \subseteq R_{in} \times R_{in}$,$R_{out}H \subseteq R_{out} \times R_{out}$表示了对内对外角色各自内部的层次继承关系

6)激活角色集

主体在一次会话开始时所启用的角色集,用 $AR(s)$ 表示会话 s 的激活角色集:

$\exists \forall s \quad (s \in S) \quad (AR(s) \subseteq R)$

如果在会话 s 中激活了角色 r_i,r_i所包含的下层角色 r_j 也同样被会话 s 所激活。

7)约束规则

约束规则主要作用在角色层和会话层,分别在角色指派和启用会话的过程中定义约束规则,并利用访问控制部分加以实施。

约束策略的制定以静态互斥角色集和动态互斥角色集为依据。其中静态互斥角色集是指在访问授权时不能同时指派给主体的两个或多个角色的集合。

$$\text{sta\_mutex}(r_i) = \{r_j \mid r_j \text{和} r_i \text{满足静态互斥}, i \neq j\}$$

动态互斥角色集则是指主体在启用会话时不能同时激活的两个或两个以上角色的集合。

$$\text{dyn\_mutex}(r_i) = \{r_j \mid r_j \text{和} r_i \text{满足动态互斥}, i \neq j\}$$

约束规则:静态互斥角色集的两个角色不能同时指派给同一主体。动态互斥角色集的两个角色不能在任意一次会话中被同时启用。

$$\forall u, r_i, r_j (r_i \in R(u) \wedge r_j \in R(u)) \Rightarrow r_j \notin \text{sta\_mutex}(r_i)$$

$$\forall s, r_i, r_j (r_i \in AR(s) \wedge r_j \in AR(s)) \Rightarrow r_j \notin \text{dyn\_mutex}(r_i)$$

4.3　RTGM 模型

针对网格自身的特点提供了统一的认证和授权机制,在保证了网格实体进行安全认证的基础上,简化了实体认证,满足了网格安全访问控制中信任管理的要求,同时解决了由于资源动态性和策略自主性而造成的管理困难问题,适应了网格环境固有的特点。该模型主要由身份认证、可信访问控制模块和策略资源管理模块(图 6)三个部分组成。具体步骤如下:

a)主体(资源或用户)或者是主体的代理请求与资源进行认证。

b)虚拟组织的身份认证中心或者是资源管理中心根据临时安全域策略决定主体与资源的验证过程。临时安全域中的资源主体不用进行身份验证;否则,安全任务用户与资源逐一进行身份验证,普通任务可以信任对方身份。

c)主体通过 VO 的身份验证后向策略执行模块提出访问请求。其中包含有主体的身份信息和请求的操作内容。

d)策略执行模块将请求交给上下文处理器进行格式转换。

e)上下文处理器根据需要向信任评估模块发送 UTA 请求信息。

f)上下文处理器对请求转换格式后根据主体的身份信息选择发送目的地。

g)内部策略决策模块或外部策略决策模块对请求进行处理并将 TRA 结果返回,上下文处理器再将返回的结果转换成策略执行模块接受的形式。

h)策略执行模块根据返回的信息执行访问控制。

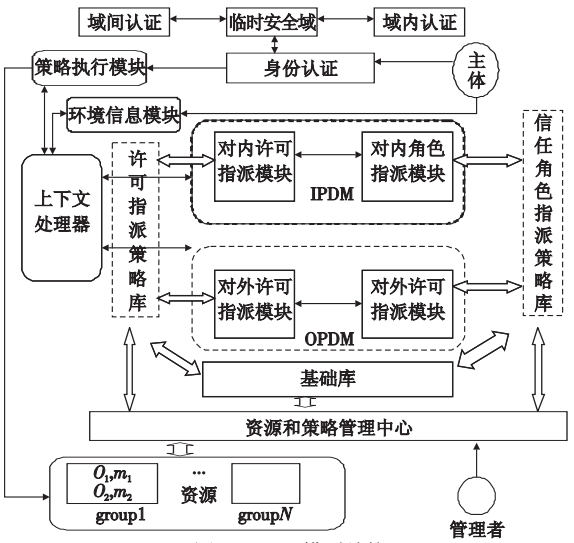

图6　RTGM模型结构

资源管理者通过资源和策略管理中心对策略库、基础库和资源分组规则进行管理。

该模型将身份认证与访问控制结合到一起的同时,也对资源访问控制策略的管理提供了安全便捷的接口。

4.4　可信访问控制模块

可信访问控制模块结构如图 7 所示。其中,策略执行模块负责对主体的请求进行处理,执行访问控制操作。内部策略决策模块和外部策略决策模块分别根据相应策略进行对内和对外的角色及权限指派工作。上下文处理器则负责将请求转换成标准的 XACML 格式供内部策略决策模块和外部策略决策模块使用,以适应模型中策略描述 XACML 规范化的要求,同时也对决策结果进行翻译[8]。

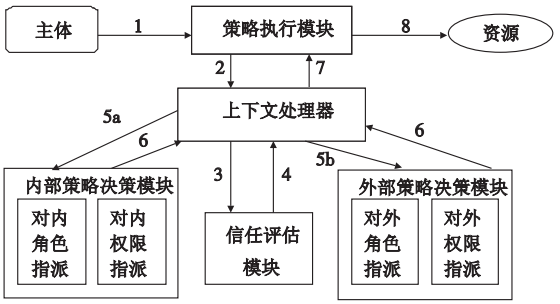

图7　可信访问控制模块结构

信任评估模块提供所需的主体环境信息,以一个实例来说明 RTGM 模型的访问控制过程如下:

a)主体通过 VO 的身份验证后向策略执行模块提出访问请求。其中包含有主体的身份信息和请求的操作内容。

b)策略执行模块将请求交给上下文处理器进行格式转换。

c)上下文处理器根据需要向信任评估模块发送主体 UTA(用户—信任度之间关系)请求。

d)信任评估模块执行命令将主体的信任度信息发送给上下文处理器。

e)上下文处理器对请求转换格式后根据主体的身份信息选择发送目的地:(a)主体属于本地 VO,将请求和信任度信息发送给内部策略决策模块;(b)主体属于外部 VO,则发送给外部策略决策模块。

f)内部策略决策模块或外部策略决策模块对请求进行处理,并将 TRA(信任度—角色关系)结果返回上下文处理器。

g)上下文处理器返回的结果转换成策略执行模块接受的形式。

h)策略执行模块根据返回的信息执行访问控制。

5　结束语

网格安全是网格中的一个重要组成部分,直接影响着网格的发展和网格系统软件的实际应用情况。访问控制是网格安全的一个关键问题,针对网格环境自身的特点对 RBAC 技术进行了相应的改进,引入信任的概念将角色分配和用户的行为联系起来,提出 RTGM 模型。基于角色的可信访问控制,给出了模型中访问控制部分的流程步骤和结构以及模块的基本划分,有效地克服了单一 RBAC 的缺点,提高了安全性也方便了管理,为管理员提供较好的实现安全策略的环境。

(下转第 1495 页)

$[\langle k\rangle(1-s_2)]$时,病毒才能在网络中持续稳定的传播。当 $d=2$,初始感染 0.03% 的个体时,由图 2 可知 $s_2=0.274$,$\langle k\rangle=4(1-0.274)=3.726$,代入 $\lambda_c=1/[\langle k\rangle(1-s_2)]$,解得 $\lambda_c=0.47$。图 3 是计算机仿真得到的稳态感染比例 I 随传播效率 λ 变化趋势图($d=2$,$p=0.05$,$\beta=1$,$\gamma=0.8$,初始感染 0.03% 的个体)。图中的 λ_c 在 0.45 ~ 0.5。仿真结果与理论计算符合得较好。

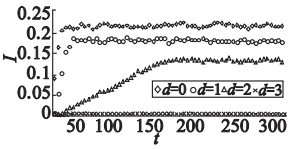

图1　不同局域控制范围对稳态感染比例的影响

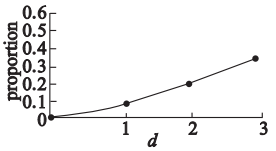

图2　被控制节点比例图

同时从式(5)可知,处于免役状态的个体失去免役能力的概率 γ 增大则稳态感染比例 I 将增大。图 4 显示了这一点($d=2$,$p=0.05$,$\alpha=0.8$,$\beta=1$,初始感染 0.03% 的个体)。

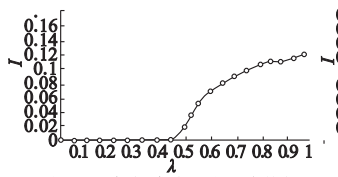

图3　稳态感染比例I随传播效率λ变化图

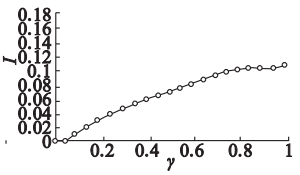

图4　稳态感染比例I随失去免役概率γ变化图

前面的理论分析得到传播临界值 λ_c 与失去免役概率 γ 无关的结论。图 5 是失去免役概率 γ 对传播临界值 λ_c 的影响($d=2$,$p=0.05$,$\beta=1$,初始感染 0.03% 的个体)。从图中可以看出,γ 较小时对传播临界值 λ_c 还是有一定的影响;但当 $\gamma>0.2$ 后传播临界值 λ_c 几乎不再随 γ 变化。

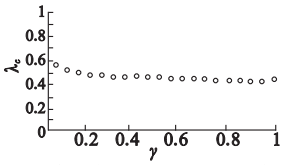

图5　失去免役概率γ对传播临界值λ_c的影响

4　结束语

本文提出了一个带有局域控制的二维规则网络 SIRS 模型。理论分析和计算机仿真都表明系统状态随时间的演化最终会达到一个稳定状态。稳态感染比例 I 与传播效率 λ 、被控制节点比例 s_2 和免役个体失去免役能力的概率 γ 有关。只有当 $\lambda>\lambda_c=1/[\langle k\rangle(1-s_2)]$时,病毒才能在网络中持续传播。在其他条件相同时,局域控制范围 d 越大,稳态感染比例 I 越小。免役个体失去免役能力的概率 γ 越小,则稳态感染比例 I 也越小。当被控制节点比例 s_2 和控制节点被传染概率 p 较小时,稳态感染比例 I 与控制节点被传染概率 p 无关。

根据以上结论,可以采取以下策略控制二维规则网络中的 SIRS 病毒传播:a)在条件允许的情况下,加大网络中局域控制的范围 d,则 s_2 增大,由 $S=\beta/\alpha\langle k\rangle+s_2$ 可知未感染个体比例将增大;b)提高治愈率 β 的同时,可以减小病毒的传播效率 $\lambda=\alpha/\beta$,当 $\lambda<1/[\langle k\rangle(1-s_2)]$时网络中病毒不能传播;c)由 $1/I=C\beta/\gamma+C$ 可知,降低免役个体失去免役能力的概率 γ 可以使被感染节点比例 I 降低,这里 $C=\alpha\langle k\rangle/(\alpha\langle k\rangle-\beta-s_2\alpha\langle k\rangle)$。

参考文献:

[1] BAILEY N T J. The mathematical theory of infectious diseases and its applications[M]. New York: Hafner Press, 1975.

[2] ANDERSON R M, MAY R M. Infectious diseases in humans[M]. Oxford: Oxford University Press, 1992.

[3] DIEKMANN O, HEESTERBEEK J A P. Mathematical epidemiology of infectious disease: model building, analysis and interpretation [M]. New York: Wiley, 2000.

[4] PASTOR-SATORRAS R, VESPIGNANI A. Epidemic spreading in scale-free network[J]. Physical Review Letters, 2001, 84(14): 3200-3203.

[5] PASTOR-SATORRAS R, VESPIGNANI A. Epidemic dynamics and endemic states in complex networks[J]. Physical Review E, 2001, 63(6): 066117.

[6] VOLCHENKOV D, VOLCHENKOVA L, BLANCHARD P. Epidemic spreading in a variety of scale free networks[J]. Physical Review E, 2002, 66(4): 046137.

[7] LIU Jing-zhou, WU Jin-shan, YANG Z R. The spread of infectious disease on complex networks with household-structure[J]. Physica A, 2004, 341: 273-280.

[8] PASTOR-SATORRAS R, VESPIGNANI A. Immunization of complex networks[J]. Physical Review E, 2002, 65(3): 036104.

[9] 许丹,李翔,汪小帆. 复杂网络病毒传播的局域控制研究[J]. 物理学报, 2007, 56(3):1313-1318.

[10] ERDÖS P, RÉNYI A. On random graphs[J]. Publ Math Inst Hung Acad Sci, 1959, 6: 290-297.

[11] WATTS D J, STROGATZ S H. Collective dynamics of small-world networks[J]. Nature, 1998, 393(6684): 440-442.

[12] BARABÁSI A L, ALBERT R. Emergence of scaling in random networks[J]. Science, 1999, 286(5439): 509-512.

(上接第 1476 页)

参考文献:

[1] 黄刚,王汝传. 网格计算中基于 RBAC 的访问控制模型的研究[J]. 微计算机信息,2007,23(18):130-132.

[2] 龙涛,洪帆,刘铭. 一种基于任务和角色的计算网格访问控制模型[J]. 计算机工程,2008,34(4):176-178.

[3] 王胜川,刘方爱,石晓晶. 基于网格环境的动态自适应信任机制研究[J]. 计算机技术与发展,2008,18(9):151-154.

[4] 马礼,郑纬民. 信息网格环境下的综合信任度评价模型[J]. 清华大学学报:自然科学版, 2009, 49(4): 599-603.

[5] TRAN H, WATTERS P, HITCHENS M, *et al*. Trust and authorization in the grid: a recommendation model[C]// Proc of International Conference on Pervasive Services. Piscataway, NJ: IEEE, 2005:433-436.

[6] JOSANG A, GRANDISON T. Conditional inference in subjective logic [C]//Proc of the 6th International Conference on Information Fusion. Gallup, NM: University New Mexico, 2003:635-642.

[7] 邓勇, 陈建刚, 王汝传. 网格计算环境的一种基于信任度的授权委托机制[J]. 通信学报, 2008, 29(9):10-17.

[8] ZHANG Guang-sen, PARASHAR M. Dynamic context-aware access control for grid application[C]//Proc of the 4th International Workshop on Grid Computing. Washington DC: IEEE Computer Society, 2003:101.