软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(3):564−574 [doi: 10.3724/SP.J.1001.2013.04242]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

面向移动终端的云计算跨域访问委托模型*

袁家斌, 魏利利, 曾青华

(南京航空航天大学 计算机科学与技术学院,江苏 南京 210016)

通讯作者: 魏利利, E-mail: liliwei05@126.com, http://www.nuaa.edu.cn/nuaanew

摘 要: 为实现移动节点跨域访问过程中的云资源保护,针对云环境和移动终端特点,借鉴已有的基于委托的RBAC 访问控制技术,提出了一种面向移动终端的跨域访问委托模型、委托机制,有效解决了移动终端所属域的动态多变问题.域管理节点维护的动态路由表,实现了移动节点的准确定位.模型给出了角色合成方法,结合量化角色技术,避免了映射过程中权限的隐蔽提升问题.委托申请频率阈值,避免了恶意节点频繁申请带来的资源耗尽风险.分析结果表明,模型具有较好的实用性和安全性,为实现现有跨域访问控制模型向移动终端扩展提供了新思路.

关键词: 跨域访问控制;移动终端;委托;角色映射;RBAC;云安全

中图法分类号: TP393 **文献标识码**: A

中文引用格式: 袁家斌,魏利利,曾青华.面向移动终端的云计算跨域访问委托模型.软件学报,2013,24(3):564−574. http://www.jos.org.cn/1000-9825/4242.htm

英文引用格式: Yuan JB, Wei LL, Zeng QH. Delegation based cross-domain access control model under cloud computing for mobile terminal. Ruanjian Xuebao/Journal of Software, 2013,24(3):564−574 (in Chinese). http://www.jos.org.cn/1000-9825/4242.htm

Delegation Based Cross-Domain Access Control Model Under Cloud Computing for Mobile Terminal

YUAN Jia-Bin, WEI Li-Li, ZENG Qing-Hua

(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Corresponding author: WEI Li-Li, E-mail: liliwei05@126.com, http://www.nuaa.edu.cn/nuaanew

Abstract: By considering the frequent migration characteristic of mobile terminal and the existing delegation based RBAC, the delegation based cross-domain access control model in cloud computing of the mobile terminal is presented. This delegation model can solve the problems of the frequent migration. It makes the management node of each domain maintain a dynamic routing table to locate the node. Also, a synthetic method to obtain synthetic mapping role is proposed. By combining the quantified-role method, the delegated node obtains the final mapping role of this cross-domain requirement. This can effectively solve the problem of permission hidden ascension in the mapping. The requirement frequency threshold will avoid the risk which is caused by the malicious node's excessive operation. Analysis shows that the model has better security.

Key words: cross-domain access control; mobile terminal; delegation; mapping role; RBAC; cloud security

云计算(cloud computing)是网格计算(grid computing)、分布式计算(distributed computing)等传统计算机技术和网络技术发展融合的产物,多个成本较低的计算实体通过整合形成了一个具有强大计算能力的系统[1].云计算无论提供何种服务,必须通过不同的终端,将云服务提供给最终用户,因此,云计算是"云"和"端"的统一体.随着智能移动终端的迅速发展,移动设备已经成为云计算最重要的终端用户类型之一.由于移动终端必须兼顾

* 基金项目: 国家自然科学基金(61139002); 国家高技术研究发展计划(863)(2009AA044601); 江苏高校优势学科建设工程资助项目; 南京航空航天大学基本科研业务费专项科研项目(NS2010230); 南京航空航天大学研究生创新基地开发基金(kfjj20110128)

收稿时间: 2011-09-07; 修改时间: 2012-02-15; 定稿时间: 2012-04-20

移动性和便携性,硬件资源相对有限,云计算强大的计算和存储能力恰巧可以弥补移动终端的不足,移动终端用户成为云计算最大的受益者之一.

云计算分布式的特点,使云环境下跨域的资源共享显得越来越重要.应用云服务过程中可能涉及多个安全域的资源,各域有自己的访问控制策略,因此,必须对共享资源制定一个公共的、双方都认同的访问控制策略.融合了移动特征的跨域资源访问,由于终端的频繁迁移,将面临新的挑战.

如图 1 所示场景,D_0 域中的节点 u 向 D_1 域发起跨域访问请求,交互过程中,节点 u 不断移动,在尚未完成本次交互的情况下,u 移动至 D_2 域甚至其他域中.这种应用场景要求跨域访问机制必须能够同步适应环境的动态变化,面向移动终端的跨域访问控制成为重要的研究内容之一[2,3].

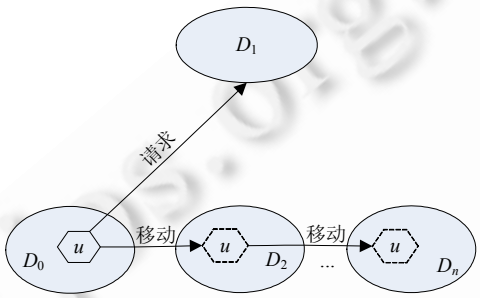


Fig.1 Diagram of cross-domain access nodes' dynamic migration

图 1 跨域访问节点动态迁移示意图

1 相关工作

目前,实现多域间 RBAC 策略合成的方法主要是角色映射,其方法包括基于权限和非基于权限两类.非基于权限的合成方法粒度较粗,不适合安全性要求高的环境.基于权限的 RBAC 策略合成方法分为基于请求和基于全局策略两类[4].

IRBAC 2000(interoperable role based access control)[5]是典型的多域环境下基于角色的访问控制模型,通过关联实现外域角色到本域角色的转换,在两个角色层次间建立映射后,两个角色层次图连接成一个组合的角色层次图,利用该图可以确定 A 域角色到 B 域角色的映射关系.但是,当 IRBAC2000 模型推广到多个(两个以上)域时,将会出现域穿梭和隐蔽提升问题.因此,该模型不能用于多域穿梭的角色映射,尤其是不能适应多域环境下的信息共享需求.

为解决角色映射中权限的隐蔽提升问题,文献[6]在角色映射方案中建立了两种域间链接,分别是外域角色到本域角色的"角色-角色"链接和外域角色到本域权限的"角色-权限"链接.这种混合映射方案很好地解决了权限隐蔽提升和角色映射冲突问题,但是却提高了管理难度.文献[7]提出的量化角色方案,采用屏蔽值方法,将允许授权的权限标识位置为 1,不允许授权的权限标识位置为 0.文献[8]在文献[7]的基础上,进一步提出度量角色的概念,引入角色委托机制,将允许映射的权限标识位置为其委托深度值,不允许映射的权限标识位置为 0.通过度量角色矩阵,实现了对委托深度的限制.

委托(delegation)授权的基本思想是,用户将自己所具有的部分或全部权限转授给其他用户,让接受授权的用户代表发出授权用户执行某些任务.基于角色的转授权技术为在分布式系统中实现角色访问控制提供了一种有效的手段.现有的基于角色的委托授权模型主要有 RBDM0[9],RDM2000[10]和 PBDM[11].

文献[12]提出的 3 项措施——第三方委托代理(third-party delegation)、量化属性值(valued attribute)、持续的监测(continuous monitoring),有效地提高了跨域访问的安全性.文献[13]中基于角色的细粒度委托限制框架,将角色分为对象角色和委托角色,实现了角色的细粒度控制,并给出了一种时间复杂度为 $O(n^2)$的基于图论的一致性检测算法,条件委托和受控使用有效地防止了非法扩散和权限滥用.文献[14]对角色委托限制的需求进行了详细地分析,包括临时性限制、常规角色关联性限制、部分性限制和传播限制,提出了一种支持临时性限制

和常规角色关联性限制的基于角色的委托模型,并给出模型的形式化描述.

针对移动实体的资源访问控制需求,文献[15]通过多个实体间的相互协商,将节点所处的位置进行归类,定义位置类型变量,为不同的变量配置不同的权限集,赋予资源本身通过专用通道传递资源的能力.

2 面向移动终端的基于角色的委托授权模型

2.1 模型概述

本文在基于 RBAC 访问控制模型的基础上引入委托机制,提出一种支持细粒度授权的面向移动终端的角色映射跨域访问委托模型.模型原理如图 2 所示.

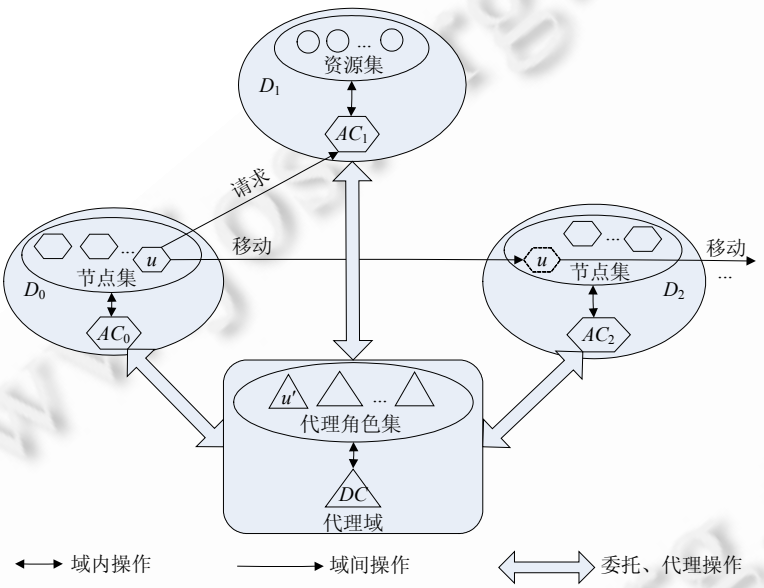


Fig.2 Diagram of cross-domain access nodes' dynamic migration

图 2 跨域访问节点动态迁移示意图

不失一般性地假设:D_0 域的中节点 u 向 D_1 域发起跨域的资源请求 req,在请求尚未结束时,节点 u 移动至 D_2 域.

当 D_0 域管理节点 AC_0 监测到 u 即将移出本域时,向云服务器中委托域 DD 的管理节点 DC 发出委托申请,注册委托节点 u',此后,u'全权代替节点 u 与被访问域 D_1 继续互操作.访问结束时,查询动态路由表定位节点 u,将结果集反馈给节点 u.

2.2 基础元素及相关定义

定义 1. 多自治域构成的域的集合 $D=\{D_0,D_1,D_2,\ldots\}$,对应的管理节点集合 $AC=\{AC_0,AC_1,AC_2,\ldots\}$.

定义 2. 委托谓词 $delegate(u,r,u',t)$,表示用户 u 在 t 时刻将角色 r 委托给用户 u'的状态.

定义 3. RBAC96 模型[12]:(U,R,P,S,URA,PRA,RH,CON).其中,U 代表用户集;R 为角色集;$P\subseteq OBJ\times ACC$ 为权限集,表示客体(OBJ)上操作(ACC);S 为会话集;$URA\subseteq U\times R$ 为用户到角色的映射关系;$PRA\subseteq R\times P$ 为角色到权限的映射关系;$RH\subseteq R\times R$ 是角色集上的偏序关系,用≥表示,记 RH^*为 RH 的自反与传递闭包;CON 为约束的集合.

定义 4. 跨域访问 REQ^{D_0} 表示为 $REQ^{D_0}\subseteq R^{D_0}\times session\times P_x^{D_1}\times history\times time\times count$,其中, R^{D_0} 为 D_0 域的角色集,$session$ 为会话集, $P_x^{D_1}$ 为节点 x 对域 D_1 的请求权限集,$history$ 为访问请求的相关历史记录集,$time$ 为本次访问申请持续的时间,$count$ 表示当前为第几次访问.

2.3 被委托节点的角色合成

本模型给出一种新的角色合成算法,将映射角色集分为两类:一类是本地映射角色集 R_1,另一类是基于请求的映射角色集 R_2.节点 u'在被访问域 D_1 的最终合成角色集记作 R'.假设 u 的跨域访问请求为

$$req=(D_0\_u.r,s,P_u^{D_1},h,t,c).$$

(1) 本地映射角色集 R_1

参照 Kamath 等人[16]提出的基于可信用户的策略合成方法,将风险值转化为信任值,进而确定可信用户集.运用 Kamath 的方法,在 D_1 域中查询同 $D_0\_u.r$ 具有相同可信用户集的角色集或者能够全部包含 $D_0\_u.r$ 可信用户集的最小角色集,即为 R_1.

(2) 基于请求的映射角色集 R_2

求解 D_1 域中满足 $P_u^{D_1}$ 的最小角色集即为 R_2.将 D_1 域中与 $D_0\_u.r$ 具有相同角色层次的角色集作为 tang[17]贪心算法的初始搜索集,缩小了 tang 算法的初始搜索空间.如果求得满足要求的结果则返回;如未求得满足条件的解,将搜索集根据角色层次分别向上、向下扩大一级,如此循环,直至求得解 R_2;否则,拒绝本次访问申请.

(3) 被委托节点的合成角色集 R'

角色合成过程如图 3 所示.首先,比较 R_1,R_2 对应的权限集是否相同:如果相同,则任选其中之一(例如 R_2)进行量化处理,得到量化角色 R_2',合成角色集 $R'=R_2'$;如果 $R_1\supseteq R_2$,则量化处理 R_2,得到 R_2',合成角色集 $R'=R_2'$;如果 $R_1\subset R_2$ 不成立,表明节点 u 在 D_0 中的角色映射至 D_1 域后不足以支持请求权限集,拒绝本次访问.

量化角色的采用文献[7]的方法,通过设置屏蔽值,将与请求权限集对应的权限标识位置 1,其余置 0,从而避免权限扩放.

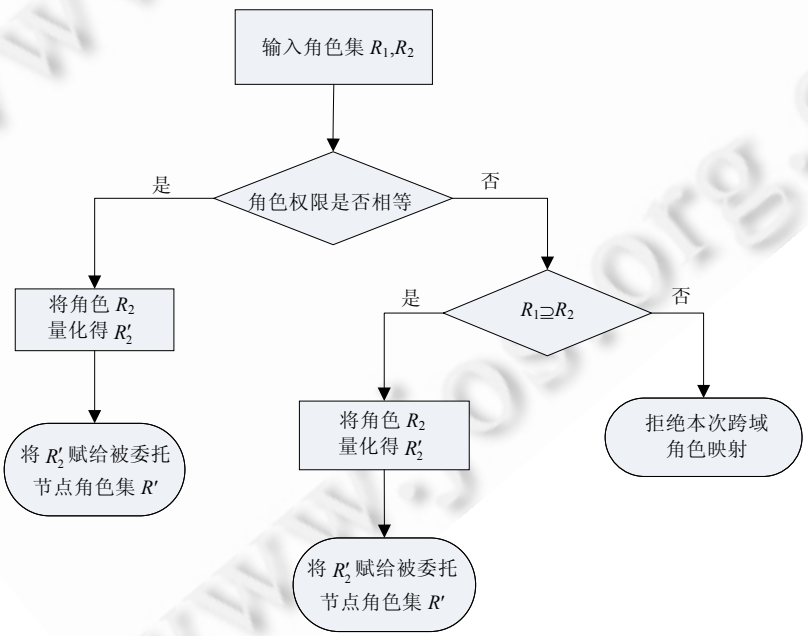


Fig.3 The flow chart of the entrusted nodes' role synthetizing

图 3 被委托节点角色合成流程图

2.4 移动终端的动态迁移

为实现移动节点定位,发起域管理节点维护见表 1 所示的动态路由表,下一跳域管理节点维护见表 2 所示的动态路由表.当管理节点 AC_0 监测到节点 u 即将离开本域时,向表 1 中添加新记录.

对于下一跳域管理节点(例如 AC_2)监测到未完成访问的节点 u 时,将 u 中否涉及未完成的跨域访问的标识位置为 1,在 u 再次即将再次离开时,向表 2 增加路由记录.

Table 1 Structure of routing table

表 1 路由表结构

序号	发起访问节点	跨域访问初始域	被访问资源域	下一跳域
1	u	D_0	D_1	D_2
2	…	…	…	…

Table 2 Structure of routing table

表 2 路由表结构

序号	发起访问节点	下一跳域
1	u	D_3
2	…	…

路由表的删除更新,分为强制删除和自主删除两种.根据 $req=(D_0\_u.r,s,P_u^{D_1},h,t)$ 中申请的访问时间 t,如果在 t 时间内正常结束,则各域管理节点自主删除相关的路由记录;如果超过时间 t,仍未完成访问,则由系统强制删除相关路由记录.

当委托节点 u'的访问在 t 内正常结束,u'向管理节点 AC_0 发起路由查询请求 *route_req*(u).如果节点 u 恰好位于此域,u'将结果集 *result* 反馈给节点 u;如果不在,则由 AC_0 查找本域的动态路由表,得到下一跳域(例如 D_2),进一步向其管理节点(例如 AC_2)发起路由查询.如此循环,直至找到节点 u 所在域(D_x),将结果集反馈给节点 u,同时更新相应路由表.

2.5 节点风险函数研究

本文基于前期基于风险的跨域访问控制模型,提出新的更适合跨域移动终端节点的风险函数形式.

设 $x_1,x_2,x_3,\ldots,x_N$ 表示系统中的 N 个节点,$X=\{x_1,x_2,x_3,\ldots,x_N\}$称为实体域.$\forall x_i$,评估某节点的风险程度有 4 项测量指标,分别表示为 $Y_1(x_{ij}),Y_2(x_{ij}),Y_3(x_{ij}),Y_4(x_{ij})$,指标集合表示为 $Y=\{Y_1,Y_2,Y_3,Y_4\}$,其中,每个元素 $0\leqslant Y_m\leqslant 1(m=1,2,3,4)$.

Y_1 表示直接风险值,定义如下:

$$Y_1(x_{ij})=\begin{cases}1-\dfrac{S_{ij}}{\sum\limits_j(S_{ij}+F_{ij})}, & \sum\limits_j(S_{ij}+F_{ij})!=0\\ 1, & \sum\limits_j(S_{ij}+F_{ij})=0\end{cases} \tag{1}$$

式(1)中的 S_{ij} 和 F_{ij} 分别表示节点 i 与节点 j 直接交易的过程中,节点 i 认为成功和失败的交易次数.交易成功的次数越多,风险越小;交易失败的次数越多,风险则越大.

Y_2 表示间接风险值,定义如下:

$$Y_2(x_{ij})=\begin{cases}\dfrac{\sum\limits_{k\in P_{ij}}Y_1(x_{ik})Y_1(x_{kj})}{\sum\limits_{k\in P_{ij}}Y_1(x_{ik})}, & P_{ij}!=\varnothing\\ 1, & P_{ij}=\varnothing\end{cases} \tag{2}$$

$P_{\{ij\}}=\{k|S_{ik}+F_{ik}>0,Y_1(x_{ik})>0\}$表示被询问节点 k 必须与询问节点 i 有历史交易,并且在节点 i 看来,节点 k 可信.

实体 i 对 j 的访问频率 $P_{ij}=\dfrac{c}{T^x}$,域内的平均访问频率为 $P^x=\dfrac{\sum\limits_{i=1}^{m}P^{ij}}{m}$,则定义实体 i 的活跃程度 $f_{ij}=\dfrac{P^{ij}}{P^x}$.实体越活跃,访问越频繁,其对应的风险值越大.

Y_3 表示实体活跃程度对应的风险,定义如下:

$$Y_3(x_{ij})=1-e^{-f_{ij}} \tag{3}$$

Y_4表示访问时间对应的风险,定义如下:

$$Y_4(x_{ij})=\frac{t}{T_i^j} \tag{4}$$

其中,t 为 req 中的参数,表示本次请求的时间;T_i^j 为资源域 j 对 i 申请的跨域访问时间的上限.本次申请的访问时间越长,表明实体 i 对资源的占用时间越长,风险就越大.

设ϖ_m表示第 m 个 $DF(Y_m(x_{ij}))$相对于其他 DF 的重要性程度,并且ϖ_m满足$0\leqslant\varpi_m\leqslant 1,\sum_{m=1}^{4}\varpi_m=1$,则称$\varpi_m$为$Y_m(x_{ij})(m=1,2,3,4)$的分类权重.

设$\Gamma(x_i,x_j,req)$表示节点x_i在某次向节点x_j发出跨域访问申请req时,该节点对应的风险值,称为节点风险值.由上述分析和定义可知:

$$\Gamma(x_i,x_j,req)=\sum_{m=1}^{4}\omega_m Y_m(x_{ij}) \tag{5}$$

3 模型分析

3.1 委托撤销

委托撤销的类型有:

① 时限撤销:委托角色和权限被限定在 t 时间内,如果超时系统自动撤销被委托实体的角色和权限;

② 一旦权限委托成功,委托实体不能撤销委托,必须由管理员进行撤销;

③ 自主撤销:被委托实体所获得的权限必须由委托实体撤销[18].

本模型的委托基于时限撤销和自主撤销两种.根据 req 中 t 的限制,一旦达到委托时间 t,终止全部操作,并由系统自动强制撤销委托关系;如果在 t 时间内,访问正常结束,遵循谁申请、谁撤销的原则,由委托发起节点 AC_0 和委托实体 u 向被委托域管理节点 DC 发出自主委托撤销请求,完成 u'的撤销.

3.2 资源锁定

为保证域中资源共享操作的完整性,为每个资源引入互斥锁,保证资源在任意时刻只能被一个节点访问.

互斥锁(locked)采用标记位形式,$locked$=1 表示资源被锁定,$locked$=0 表示资源未被锁定.当节点 u_i 申请访问资源 $resource_i$ 时,$resource_i$ 的域管理节点首先查看该资源是否已被锁定,如果 $locked$=0,则允许 u_i 的访问申请,同时调用 $init$:{$locked$=1},初始化互斥锁;如果 $locked$=1,则拒绝 u_i 的申请.互斥锁的撤销采用强制撤销和自主撤销相结合的方式:当本次访问正常结束时,由资源所在域的管理节点自主调用互斥锁撤销操作 $destroy$:{$locked$=0};若访问非正常结束,由系统自动强制完成互斥锁撤销操作 $destroy$:{$locked$=0}.

3.3 安全性分析

本模型限制实体委托深度,不允许二次委托,整个委托仅涉及委托实体和被委托实体两方,不存在多次委托过程产生的角色和权限冲突.被委托实体来自于第三方云服务器,不涉及委托节点的相关服务,因此无需进行角色是否互斥等验证.

为防止恶意节点频繁发起委托请求,导致资源耗尽,本模型为每个申请域主观设定申请频率阈值σ^i,该阈值可以由管理节点维护.在委托域中设置计数器实时记录固定时间ΔT内,域 X 的委托申请次数 $count^X$,并计算其申请频率 $f^X=\frac{count^X}{\Delta T}$.如果 $f^X\leqslant\sigma^X$,表明访问频率正常,将计数器归零后,继续监控下一ΔT 时间内域 X 的访问频率;如果$f^X>\sigma$,表明访问频率超出正常范围,可能存在风险,则拒绝此后 $T'=T(T>\Delta T)$时间内来自域 X 的委托申请.到达 T'时间后,重新接受域 X 的申请.如果再次连续出现申请频率超出正常范围,则调整 $T'=2T$,此后,域 X 每连

续出现一次申请频率异常,T'增加 T;如果下一个 T 时间内申请频率恢复正常,则 T'减少 T,直至 $T'=T$.通过对委托申请频率的监控,有效避免了恶意节点的攻击.

3.4 机密性分析

3.4.1 系统状态表示

为便于描述,将访问发起域节点称作主体,被访问域资源称作客体.模型中节点状态集合记 $V=\{V_0,V_1,V_2,\ldots,V_n\}$,其中,$V_0$ 为初始状态.状态 $v\in V$ 由四元组(b,M,f,sM)表示,其中,

- $b\subset(S\times O\times A)$:表示在特定状态下,哪些主体以何种访问属性访问哪些客体,其中,S 是主体集合,O 是客体集合,满足$(S\subseteq D)\cap(O\subseteq D)$,$A=\{r,a,w,x\}$是访问属性集;
- M:表示访问矩阵,其中,元素 $M_{ij}\subseteq A$,表示主体 S_i 对客体 o_j 具有的访问权限;
- 安全函数集合 $f\subseteq F$:表示访问类函数,$F=\{f_{SH},f_{SL},f_{IH},f_{IL},f_{SO},f_{IO}\}$,这些函数满足$\forall s\in S\Rightarrow f_{SH},f_{SL}\wedge f_{IH},f_{IL}sM:=\{o|o\in B(s:r,w)\}$.其中$f_{SH},f_{SL}$为主体保密级函数,$f_{IH},f_{IL}$为主体完整级函数;
- 主体的访问记忆集 $sM:=\{o|o\in B(s:r,w)\}v\in V$,其中,$B(s:r,w)$表示主体以 r,w 方式访问过客体的集合[22].

3.4.2 模型安全规则

系统是安全状态,iff 系统的每一个状态 $v\in V$ 均为安全状态.一个系统是安全的,当且仅当它满足相应的机密性规则.本模型的机密性规则:

公理 1. 简单安全性.状态 $v=(b,M,f,sM)$满足简单安全特性,当且仅当所有的 $s\in S\Rightarrow[(o\in b(s:r)\Rightarrow f_{SH}(s)\geqslant f_{SO}(o)\geqslant f_{SL}(s))]$,其中,符号≥表示前者支配后者[22].

3.4.3 模型机密性分析

规则 1(跨域访问请求规则). 用于域 X 中节点 u 请求得到域 Y 中某资源的访问权.为便于证明,表示为主体 s_i 请求得到对客体 o_j 的访问权.定义

$$req'(req,v)=\begin{cases}v, & \text{拒绝申请}\\ (b\cup(s_i,o_j,r),M,f,sM), & \text{允许申请}\\ v, & \text{其他}\end{cases} \tag{6}$$

证明:证明规则 1 满足公理 1.

设 $o'\in(b',r)$,若 $o'\in(b,r)$,则 $f_{SH}(s_i)\geqslant f_{SO}(o')\geqslant f_{SL}(s_i)$;若 $o'\neq o_j$,则 $o'\in(b,r)$,由此可得 $f_{SH}(s_i)\geqslant f_{SO}(o')\geqslant f_{SL}(s_i)$.

总之,若 $o'\in(b',r)$,则 $f_{SH}(s_i)\geqslant f_{SO}(o')\geqslant f_{SL}(s_i)$,规则 1 满足公理 1,满足简单机密性. □

规则 2(委托规则). 用于域 X 将节点 u 的本次跨域访问委托给第三方域中的节点 u'.为便于证明,表示为主体表示为将主体 s_i 委托给客体 o_j,同样可以证明本规则满足机密性要求.其他规则类似给出,这里省略.

4 仿真实验及结果分析

本次仿真实验分别从有效性和动态适应性两个方面进行评估,通过构造多组具有典型代表的参数,评测本文的模型.

4.1 有效性分析

a) 优良节点(good node).此类节点无论是作为访问发起方,还是被访问方,或者是提供对其他节点的评价,都是客观公正的,记为 G 类节点;

b) 恶意节点(malicious node).此类节点作为访问发起方,还是被访问方,或者在对其他节点进行评价,有大于等于 50%的概率可能提供不客观的结果,记为 M 类节点.

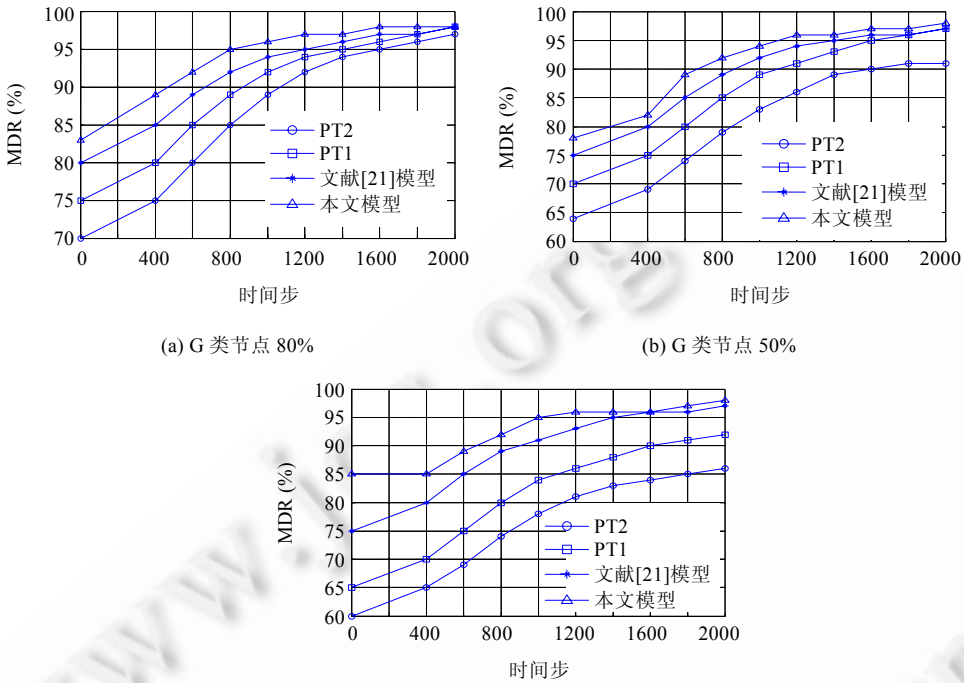
实验用恶意节点的检测率(MDR)作为评价模型有效性的指标.分别取下列 3 组数据,对 PT1 模型[19]、PT2 模型[20]、文献[21]模型和本文模型进行结果比较.

(a) G 类节点:80%,M 类节点:20%;

(b) G 类节点:50%,M 类节点:50%;

(c) G 类节点:20%,M 类节点:80%.

仿真结果如图 4 所示.



(a) G 类节点 80%　　(b) G 类节点 50%

(c) G 类节点 20%

Fig.4 MDR of alicious nodes

图 4 恶意节点检测率

图 4 中显示,本文中模型的恶意节点检测率明显高于其他 3 类模型,而且随着时间步的增加,3 种网络节点环境中都达到 95%以上.在初始时刻,本文模型就显示了较好的有效性,达到 80%以上,明显优于其他 3 类模型.

综上所述,本文的模型较其他 3 种模型,具有最优的有效性.

4.2 动态适应性分析

用交互操作的成功概率(SSP)作为指标来说明模型的动态适应能力: $SSP=\frac{sucessNum}{totalNum}$ 是成功交互操作数与总交互操作数的比值[21].

用以下两个参数来描述系统的动态性:

a) 服务请求频度 SRF,反映了系统的繁忙程度.SRF 越大,说明服务请求越频繁;

b) 节点动态移动频率 SCF,反映了系统中服务提供者或资源的不稳定性.SCF 越大,表明网络越不稳定.

设置如下 6 组数据,对 PT1 模型、PT2 模型、文献[21]模型和本文模型的动态适应性进比较:

(a) 稳定不繁忙网络:*SRF*=20%,*SCF*=20%;

(b) 稳定繁忙网络:*SRF*=80%,*SCF*=20%;

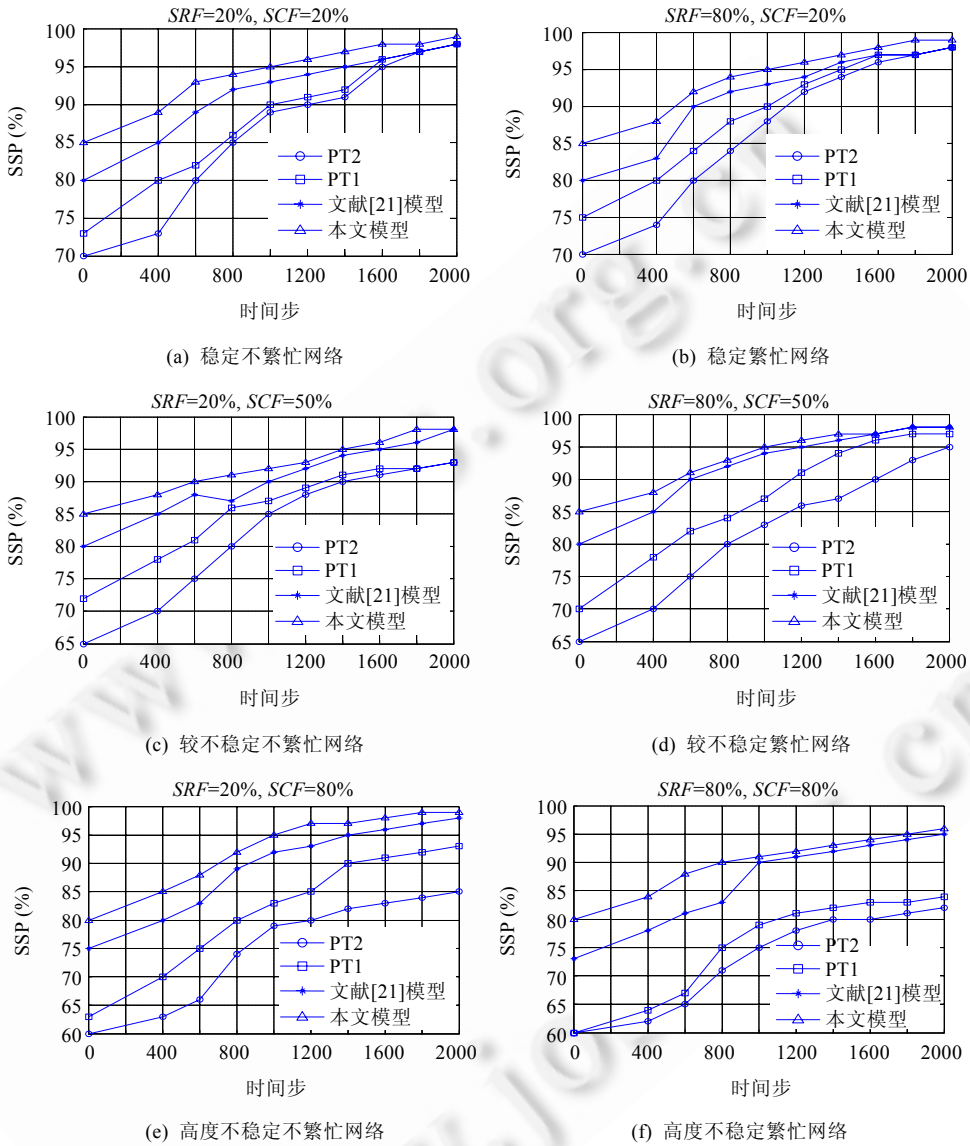
(c) 较不稳定不繁忙网络:*SRF*=20%,*SCF*=50%;

(d) 较不稳定繁忙网路:*SRF*=80%,*SCF*=50%;

(e) 高度不稳定不繁忙网络:*SRF*=20%,*SCF*=80%;

(f) 高度不稳定繁忙网络:*SRF*=80%,*SCF*=80%.

仿真结果如图 5 所示.



(a) 稳定不繁忙网络 (b) 稳定繁忙网络

(c) 较不稳定不繁忙网络 (d) 较不稳定繁忙网络

(e) 高度不稳定不繁忙网络 (f) 高度不稳定繁忙网络

Fig.5 SSP of interoperation

图 5 互操作成功概率

在相对较稳定的网络环境中,如图 5(a)和图 5(b)所示,4 类模型都有较好的表现,相互间差别不大.但随着网络环境越来越复杂,本文提出的模型在初始时刻即可达到较好效果,且 SSP 指标一直优于其他 3 类模型,比表现最差的 PT2 模型高出 20%以上.

综上所述,本文的模型较其他 3 种模型具有最优的动态适应性.

5 结束语

本文对云环境下基于移动终端的跨域访问需求和特点进行了深入探讨,分析了基于委托的 RBAC 模型研

究现状,提出了一种基于委托的面向移动终端的跨域访问控制模型,为解决移动节点跨域资源防护提供了新思路.本模型通过引入委托机制,向云服务器中的委托域申请移动节点的代理节点,解决了跨域访问过程中,移动节点在多域间动态迁移带来的交互困难问题;域管理节点维护的移动节点的动态路由表,解决了跨域访问结束后,结果反馈过程中的节点定位问题.本模型定义了本地映射角色和基于请求的映射角色两种角色集,并在这种角色分类的基础上提出了新的角色合成方法,结合已有的量化角色技术,将映射角色集进行量化处理,避免了映射过程中权限的隐蔽提升问题,实现细粒度的角色映射.本模型中,为委托域设置委托申请频率阈值,有效地避免了恶意节点过度频繁申请带来的资源耗尽等风险,提高了模型的安全性.理论和实验分析表明,本模型具有较好的实用性和安全性.

致谢 感谢云计算组各位同学为本文研究所做出的贡献.

References:

[1] Cloud computing (in Chinese with English abstract) 2011. http://baike.baidu.com/view/1316082.htm.2011

[2] Feng DG, Zhang M, Zhang Y, Xu Z. Study on Cloud computing security. Ruanjian Xuebao/Journal of Software, 2011,22(1):71−83 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3985.htm [doi: 10.3724/SP.J.1001.2011.03958]

[3] Wang YZ, Feng DG. A survey of research on inter-domain authorization interoperation. Journal of Computer Research and Development, 2010,47(10):1673−1689 (in Chinese with English abstract).

[4] Zhang QY. Research and Implement on Multi-Domain Policy Integration based on RBAC [MS Thesis]. Shanghai: Shanghai Jiaotong University, 2010 (in Chinese with English abstract).

[5] Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R. Proposed NIST standard for role-based access control. ACM Trans. on Information and System Security, 2001,4(3):224−274. [doi: 10.1145/501978.501980]

[6] Hu JW, Li RX, Lu ZD. Establishing RBAC-based secure interoperability in decentralized multi-domain environments. Berlin, Heidelberg: Springer-Verlag, 2007,4817:49−63. [doi: 10.1007/978-3-540-76788-6_5]

[7] Zhai ZD. Quantified-Role based controllable delegation model. Chinese Journal of Computers, 2006,29(8):1401−1407 (in Chinese with English abstract).

[8] Cai WH. Wei G. Xiao S. Fine-Grained role delegation model based on mapping mechanism. ACTA Electronica Sinica, 2010,38(8): 1753−1758 (in Chinese with English abstract).

[9] Barka E, Sandhu R. Framework for role-based delegation models. In: Proc. of the 16th Annual Computer Security Applications Conf. New Orleans, 2000. [doi: 10.1109/ACSAC.2000.898870]

[10] Zhang LH, Ahn GJ, Chu BT. A rule-based framework for role-based delegation. In: Sandhu RS, Jaeger T, eds. Proc. of the 6th ACM Symp. on Access Control Models and Technologies. New York: ACM Press, 2001. 153−162. [doi: 10.1145/373256.373289]

[11] Sun B, Zhao QS, Sun YF. TRDM—Temporal role-based delegation model. Journal of Computer Research and Development, 2004, 41(7):1104−1109 (in Chinese with English abstract).

[12] Freudenthal E, Pesin T, Port L, Keenan E, Karamcheti V. dRBAC: Distributed role-based access control for dynamic coalition environments. Berlin, Heidelberg: Springer-Verlag, 2002. 411−420. [doi: 10.1109/ICDCS.2002.1022279]

[13] Liu W, Cai JY, He YP. Role-Based fine-grained delegation constraint framework in collaborative environments. Journal on Communication, 2008,29(1):83−91 (in Chinese with English abstract).

[14] Xu Z, Li L, Feng DG. A constrained role-based delegation model. Ruanjian Xuebao/Journal of Software, 2005,16(5):970−978 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/970.htm [doi: 10.1360/jos160970]

[15] Hennessy M, Riely J. Resource access control in systems of mobile agents. Electronic Notes in Theoretical Computer Science, 1998, 16(3):174−188. [doi: 10.1016/S1571-0661(04)00141-0]

[16] Kamath A, Liscano R, El Saddik A. User-Credential based role mapping in multi-domain environment. In: Proc. of the Privacy, Security, Trust (PST). 2006. [doi: 10.1145/1501434.1501507]

[17] Tang Z, Li RX, Lu ZD. A request-driven role mapping for secure interoperation in multi-domain environment. In: Proc. of the Int'l Conf. on Network and Parallel Computing-Workshops (IFIP 2007). 2007. 83−90. [doi: 10.1109/NPC.2007.33]

[18] Deng Y, Chen JG, Wang RC, Zhang L. Authorization delegation mechanism based trust level in grid computing. Journal of Communications, 2008,29(9):10−17 (in Chinese with English abstract).

[19] Li X, Liu L. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. on Knowledge and Data Engineering, 2004,16(7):843−857. [doi: 10.1109/TKDE.2004.1318566]

[20] Liang ZQ, Shi WS. Enforcing cooperative resource sharing in untrusted P2P computing environments. Journal of Mobile Networks and Applications-Springer, 2005,10(6):971−983.

[21] Li XY, Gui XL. Trust quantitative model with multiple decision factors in trusted network. Chinese Journal of Computers, 2009, 32(3):405−416 (in Chinese with English abstract).

[22] Sun ZH. The Security Enhancement Study of Embedded Linux Operating System [MS. Thesis]. Nanjing: Nanjing University Aeronautics and Astronautics, 2008 (in Chinese with English abstract).

附中文参考文献:

[1] 云计算 2011. http://baike.baidu.com/view/1316082.htm.2011

[2] 冯登国,张敏,张妍,徐震.云计算安全研究.软件学报,2011,22(1):71−83. http://www.jos.org.cn/1000-9825/3958.htm

[3] 王雅哲,冯登国.域间授权互操作研究综述.计算机研究与发展,2010,47(10):1673−1689.

[4] 张清源.基于 RBAC 的多域间策略合成机制研究与实现[硕士学位论文].上海:上海交通大学,2010.

[7] 翟征德.基于量化角色的可控委托模型.计算机学报,2006,29(8):1401−1407.

[8] 蔡伟鸿,韦岗,肖水.基于映射机制的细粒度 RBAC 委托授权模型.电子学报,2010,38(8):1753−1758.

[11] 孙波,赵庆松,孙玉芳.TRDM-具有时限的基于角色的转授权模型.计算机研究与发展,2004,41(7):1104−1109.

[13] 刘伟,蔡嘉勇,贺也平.协同环境下基于角色的细粒度委托限制框架.通信学报,2008,29(1):83−91.

[14] 徐震,李斓,冯登国.基于角色的受限委托模型.软件学报,2005,16(5):970−978. http://www.jos.org.cn/1000-9825/16/970.htm

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

[21] 李小勇,桂小林.可信网络中基于多维决策属性的信任量化模型.计算机学报,2009,32(3):405−416.

[22] 孙卓海.嵌入式 Linux 操作系统的安全性增强研究[硕士学位论文].南京:南京航空航天大学,2008.

袁家斌(1968－),男,江苏兴化人,博士,教授,博士生导师,CCF 高级会员,主要研究领域为信息安全,高性能计算,量子密码.
E-mail: jbyuan@nuaa.edu.cn

魏利利(1987－),女,硕士,主要研究领域为云安全.
E-mail: liliwei05@126.com

曾青华(1987－),女,硕士,主要研究领域为云计算.
E-mail: zeng_qh@126.com