一种基于移动 P2P 系统的访问控制框架①

方　芳[1]，陈世平[1,2]，裘慧奇[2]，王佳炳[1]

[1](上海理工大学 光电信息与计算机工程学院，上海 200093)
[2](上海理工大学 信息化办公室，上海 200093)

摘　要：针对移动 P2P 网络中的对等端容易耗尽系统资源、受到拒绝服务攻击等问题，提出了一种访问控制框架。在 RBAC 模型的基础上提出 MT-RBAC 访问控制框架，模型使用了空间上下文、信任约束和资源控制来实现移动 P2P 系统的访问控制机制。有效地避免了恶意节点的资源请求对系统资源的消耗，提高了系统可用性。

关键词：移动 p2p；访问控制；信任模型

Access Control Framework Based on Mobile P2P System

FANG Fang[1], CHEN Shi-Ping[1,2], QIU Hui-Qi[2], WANG Jia-Bing[1]

[1](School of Optical-Electrical Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China)
[2](Office of Information, University of Shanghai for Science and Technology, Shanghai 200093, China)

Abstract: In order to solve the problem which has existed in the mobile p2p network, for example, the excessive consumption of system resources and the attacks of denial service, a new access control is proposed in this paper. Based on RBAC access control framework, MT-RBAC access control framework adopts the techniques of spatial context, trust constraint and resource control to achieve the access control mechanism of the Mobile P2P System. The new access control framework can effectively and efficiently increase the usability of the system, and prevent the system from the irrational resource request from spite nodes.

Key words: mobile peer to peer; access control; trust model

1　引言

随着 P2P 技术的广泛应用与移动网络的飞速发展，使得移动 P2P 网络的研究受到学术界越来越多的关注，已成为当前研究的又一新热点。安全技术是移动 P2P 网络的潜能是否得到充分施展的一个核心因素[1-2]。

移动 P2P 网络安全技术研究的主要内容有信任管理、访问控制、攻击检测，如何建立节点间的信任关系是移动 P2P 网络安全的核心内容，访问控制机制则是保障系统机密性和完整性的主要手段。然而目前绝大多数对 P2P 系统访问控制的研究主要集中在提供服务方面，而较少关注对资源的控制[3]。移动 P2P 系统中的对等端同个人计算机相比更容易耗尽系统资源，受到拒绝服务攻击，因此基于移动网络的 P2P 系统对访问控制技术提出了新的要求：可用性、易用性和高性能。可用性是指移动对等端必须对关键应用给予及时响应；易用性是指访问控制规则应尽可能简单，过于复杂的规则会导致移动用户失去耐心而关闭访问控制机制；高性能是指移动终端的硬件水平决定了其本身无法进行大规模的计算，过多的数据操作会导致性能严重下降。

本文首先针对文献[4]所提出的 RBAC 模型[4]进行扩展，引入空间上下文和信任约束的概念到访问控制理论之中，提出了一种适应移动 P2P 网络环境的动态访问控制模型——MT-RBAC(Mobile Trust-Role BAC)模型，在此基础上给出了应用于移动终端的访问控制框架，在该框架中将用户权限的获取与用户的可信度关联起来，同时允许为关键应用预留动态资源，系统对预留的资源进行统一的管理，防止关键应用与其它

① 基金项目:国家自然科学基金(60573142);上海市重点学科建设项目(S30504)
收稿时间:2010-11-15;收到修改稿时间:2011-01-01

程序竞争系统资源时产生冲突，避免了恶意节点的资源请求对系统资源的消耗，提高了系统可用性。

1 MT-RBAC模型概述

MT-RBAC 模型是在以 NIST 标准中核心 RBAC 模型基础上引入空间上下文、信任约束条件和资源控制建立起来的。核心 RBAC 模型只包含了用户、角色、权限和会话四类实体，模型中权限只能被赋予给角色，而不是用户，当一定角色分配给用户时，该用户就拥有了该角色包含的访问权限，而会话是用户和激活角色集合之间的映射。本文提出的 MT-RBAC 模型对主体-角色、角色-权限的分配关系及其约束控制进行了改进，以实现对移动网中的数据访问进行实时、灵活、有效的控制。模型框架用空间上下文来定义角色的使用环境，用信任度来激活角色的分配，用资源控制保障移动终端的可用性，为访问控制技术的应用提供了一种新的解决方案。

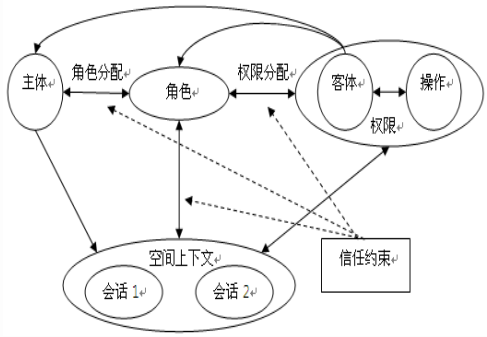

图 1 MT-RBAC 模型

MT-RBAC 模型如图 1 所示，模型的主要特点体现在以下几个方面：

(1) 空间上下文

这里的空间上下文是指移动网中与移动用户的位置、状态及业务相关的事件。MT-RBAC 模型强调了空间范围对资源访问的约束条件，即在角色分配时要根据用户的空间信息来确定，不同的空间范围内有不同的角色。因此为了适应移动网络环境中访问控制的特点，MT-RBAC 模型中引入了空间上下文概念来定义角色赋予逻辑位置域以指定角色可以活动的空间范围。角色的可用性依赖于用户从移动终端获得的当前物理位置。

(2) 信任约束

虽然 RBAC 策略有很多优势，但是对可信要求程度较高的移动 P2P 系统仅通过基于角色的访问控制并不能实现网络的可信，必须通过分布式的信任机制来保证网络中的用户行为是可信的。在 MT-RBAC 模型中，每个用户能够根据他在系统中的交互历史、其他用户提供的推荐信息以及自身相关知识为对方计算出一个信任度，将该信任度与系统的每项访问权限的最低可信度阈值进行比较，只有信任度不低于这个阈值的用户才能在具体会话中通过授予的角色获得相应访问权限。

(3) 资源控制

MT-RBAC 模型框架为了更好达到可用性要求，考虑了移动终端资源有限性的特点，将移动终端资源分为了动态和静态资源两种类型。利用资源预留监控机制实现对动态资源的控制。系统通过对资源的控制保证了移动用户对关键应用的响应，提高了系统的可用性和可扩展性。

2 MT-RBAC访问控制框架

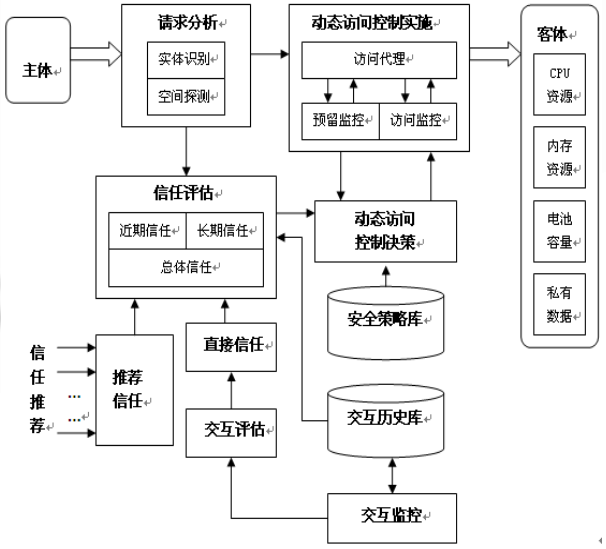

图 2 MT-RBAC 访问控制框架

MT-RBAC 信任模型为实体间的信任建立提供了一种保障机制，对资源控制为移动终端的高可用性提供了可能。在此 MT-RBAC 信任模型和移动终端资源控制基础上的访问控制框架，有效地将用户的权限获取与用户的可信度关联起来，启动了为关键应用预留动态资源机制，避免了恶意节点的资源请求对系统资

源的消耗，提高了系统可用性。如图 2 所示，该框架包含以下几个主要部分：

(1) 请求分析：截获用户请求，分析用户的标识与空间上下文信息；

(2) 交互监控：监控用户的行为特征，对用户行为进行风险评估；

(3) 信任评估：计算用户信任度，建立网络中用户之间的信任关系；

(4) 动态访问控制决策：根据系统的安全策略决定访问控制约束条件；

(5) 动态访问控制实施：根据安全策略为主体赋予相应的访问权限。

3 MT-RBAC模型的实现

3.1 空间上下文探测的实现

为了能让模型支持空间上下文，需要通过空间检测技术来获取物理位置以及怎样描述空间位置，本文研究并改进了文献[5]中空间位置描述的方法，以及逻辑位置域和位置映射函数的实现[5]。如今已有 GPS、RFID 等移动终端位置检测技术的支持，可很容易地获取用户的当前物理位置，用函数 $GetLocation(Q_i)$ 来表示获取用户节点 Q_i 的当前物理位置。

上下文感知的应用程序需要描述位置，用位置来为物理环境建模，当前使用最广泛的位置模型有两类：层次型的和笛卡尔的。由于层次型的位置模型能较好地表达空间关系，且具有良好的用户可读性，本文采用它来描述空间位置。层次型的空间位置模型可把物理环境分解成不同级别的空间。

物理位置域：它定义了用户所在的物理区域，我们假设物理位置域覆盖了 MT-RBAC 的整个职责区域。物理位置域用 $RDom$ 来表示。获取用户节点 Q_i 的当前物理位置的函数 $GetLocation(Q_i)$ 返回值就是 $RDom$ 。

逻辑位置域：它定义了用户所承担的角色的逻辑空间边界。逻辑位置域用 $LDom$ 表示。通常，物理位置域和逻辑位置域之间存在紧密关联，逻辑位置域可由物理位置域构成。例如，可用位置表达式 $DepDom=[\pi 1,\pi 2]$ 来表示，它指的是物理位置域 $\pi 1$ 和 $\pi 2$ 覆盖的区域。

位置映射函数：$LDom\ MapLocation(GetLocation(Q_i))$，函数名 $MapLocation$，函数参数是节点物理位置 $GetLocation(Q_i)$，返回值是节点的逻辑位置域。位置映射函数实现了将节点实际位置映射到逻辑位置域的功能。

3.2 信任约束的实现

根据 MT-RBAC 机制，当主体 Q_j 向客体 Q_i 提出资源访问请求时，系统访问控制模块在空间上下文 SC 中为其创建会话 s，为了建立用户之间的信任关系，Q_i 计算 Q_j 的可信度 $T_n(Q_i,Q_j)$，可信度 T 的计算方法采用文献[2]中所提出的方法进行计算。用户 Q_j 选择在会话 s 中需要激活的角色，访问控制模块根据信任约束条件将 $T_n(Q_i,Q_j)$ 作用于的各项访问权限。下面给出激活会话中角色的信任条件约束列表 1，该表给出了信任值达到何种程度才允许激活角色的具体规则。

表 1　信任条件列表

空间上下文 *SC*	角色 *Role*	信任度 *TrustRange*	限定数量 *Amount*
sc_1	r_1	$x_1 \le T \le x_2$	m_1
sc_1, sc_2	r_2	$x_2 \le T \le x_3$	m_2
……	……	……	
sc_k	r_t	$x_{n-1} \le T \le x_n$	m_t

若表中 $r_1 \le r_2 \le ... \le r_n$，$x_1 \le x_2 \le ... \le x_n$，则在 sc_1 中 $r_1 \le r_2$ 表示角色 r_2 可以获得比 r_1 更高的权限，但是也需要更高的信任度阈值，因为 $x_1 \le x_2$ 。

3.3 移动终端资源控制的实现

1.访问代理模块伪代码：

```
AccessAgent() {
request=GetAccessRequest(); //截获访问请求
SecurityStrategy=ReadAccessStrategy(request);//读取安全策略
remainer=RemainController(SecurityStrategy);//预留资源策略
monitor=AccessMonitor(SecurityStrategy); //访问监控策略
OutputPermission(remainer,monitor); //输出权限裁决
}
```

2.资源预留监控模块伪代码：

```
RemainController(SecurityStrategy) {
ResRemainSet=NULL;
ResRemainSet+=RemainCPU(SecurityStrategy); //预留 CPU
ResRemainSet+=RemainMemory(SecurityStrategy); //预留内存
ResRemainSet+=RemainBattery(SecurityStrategy);
//预留电池容量
ResRemainSet+=RemainOther(SecurityStrategy); //预留其他资源
return ResRemainSet;                          //返回预留资源集合
}
```

3.访问监控模块伪代码：

```
AccessMonitor(SecurityStrategy) {
```

sub=MonitorSubject(*SecurityStrategy*) ;//主体访问安全需求

obj=MonitorObject(SecurityStrategy) ;//客体访问安全需求

return monitor=Merge(*sub,obj*) ; //返回监控结果

}

4 小结

本文提出了一种基于 MT-RBAC 模型访问控制框架，该框架结合了空间上下文和信任约束等条件对 RBAC 模型进行扩展。通过对 MT-RBAC 信任模型设置约束条件，系统的访问控制模块来计算资源请求用户的信任度，并应用信任约束条件确定该用户在当前会话中的有效权限，用户的系统访问行为就限定为与这些有效访问权限对应的系统资源访问操作。该模型强化了对移动终端资源的控制，保证了访问控制的高可用性。

基于信任和信誉的访问控制模型研究已成为移动 P2P 网络研究热点之一。如今移动网络的安全问题已经远远不止保密性和完整性的问题，单一的安全技术很难保证系统的真正安全，访问控制技术与其他安全技术进一步的结合将成下一步研究的内容，如访问控制与密钥、证书、数字签名、认证等技术的结合将是解决系统安全访问控制的有效途径。

参考文献

1 牛新征,佘堃,等.移动 P2P 计算研究进展.计算机应用研究,2007,24(5):269−272.

2 Sandhu R, Zhang X. Peer-to-peer access control architecture using trusted computing technology. Proc the 10th ACM Symposium on Access Control Models and Technologies (SACMAT’05). Stockholm，2005.147−158.

3 Edjlali G, Acharya A, Chaudhary V. History-based access control for mobile code. Proc the 5th ACM Conference on Computer and Communication Security (CCS’98). San Francisco, 1998.38−48.

4 陈世平,王佳炳,等.一种移动环境中的 P2P 网络信任模型.计算机应用,2009,29(10):2603−2605.

5 张宏,贺也平,石志国.一个支持空间上下文的访问控制形式模型.中国科学,2007,37(2):254−271.

(上接第 176 页)

CBR 封包 512Btyes。设置 A、B 的移动速度为 1~2m/s。仿真结果如图 4。可见在同样网络负荷情况下，加入了端混音机制后会议的语音丢包率更低。

5 结语

针对 WMN 的结构特点，本文提出了分布式的会议方案，并加入了终端处理机制，减轻了系统流量压力，降低了网络拥堵和丢包率。由于无线 mesh 带宽限制，所提方案只能传输语音，而不适合视频。同时该方案的延时依赖于 mesh 多跳本身的延时特性，仍是以后研究的重点和方向。

参考文献

1 Rosenberg J, Schulzrinne H, Camarillo G. RFC3261 SIP: Session Initiation Protocol. IETF, 2002.

2 Venkatesha PR, Hurni R, Jamadagni HS. A Scalable Distributed VoIP Conferencing Using SIP. Proc. of the Eighth IEEE International Symposium on Computers and Communication (ISCC 2003). Los Alamitos: IEEE Computer Society Press, June 2003.608−613.

3 孟颖达,徐恪.基于 SIP 协议的分布式会议系统管理框架.计算机工程,2007,33(24):231−233.

4 Zhang Y, Luo JJ, Hu HL.无线网状网:构架、协议与标准.郭达,张勇,彭晓川,译.北京:电子工业出版社,2008.

5 Joung YJ, Chien PH. P2Pconf:A Medium-Size P2P Internet Conference with Effective Floor Control. Proceedings of the International Conference on Information Networking 2008 (ICOIN 2008). Busan: International Conference on, January 2008.1−5.

6 Lennox J, Schulzrinne H. A Protocol for Reliable Decentralized Conferencing. Proc. of the 13th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV 2003). California: ACM Press, 2002.72−81.

7 薛卫,都思丹,叶迎宪.小波变分辨率频谱特征静音检测和短时自适应混音算法.计算机科学,2009,36(7):211−214.