访问控制主体相似性与约束

阿不都艾尼·阿不都西库尔[1] 开依沙尔·热合曼[1] 努尔买买提·黑力力[1,2]
(新疆大学数学与系统科学学院 乌鲁木齐 830046)[1]
(新疆多语种信息技术自治区级重点实验室 乌鲁木齐 830046)[2]

摘 要 约束是访问控制中的重要因素,它通过限制客体的敏感组合集中于相似主体来达到防止商业欺骗或错误的目的。但是传统访问控制约束缺乏灵活性。为了提高约束的灵活性,首先分析访问控制中的主体与客体各自内部之间潜在的关系以及它们相互之间的关系,并提出相似主体组的概念,在此基础上提出修正的访问控制约束。其次进行主体访问客体的实验,结果表明提出的约束是可行和灵活的。修正的约束除了具有传统访问控制约束的功能外,还能有效防止相似主体共谋攻击系统。

关键词 访问控制约束,职责分离,中国墙策略,主体相似性
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.4.024

Access Control Subject Similarity and Constraints

Abdugheni ABDUXUKUR[1] Kaysar RAHMAN[1] Nurmamat HELIL[1,2]
(College of Mathematics and System Science, Xinjiang University, Urumqi 830046, China)[1]
(Xinjiang Key Laboratory of Multilingual Information Technology, Urumqi 830046, China)[2]

Abstract Constraint is an important factor in access control. It restricts sensitive combination of objects to be accumulated into similar subjects. However, conventional access control constraints lack flexibility. In order to improve the flexibility of constraints, we firstly respectively analysed potential inner-relationships among subjects and objects, and the relationships between them in access control. Then we proposed the concept of similar subject groups, and on this basis proposed revised access control constraint. Secondly, we implemented an experiment of subjects accessing objects. Experimental result shows the presented constraint is feasible and flexible. This revised constraint not only has the capability of conventional access control constraints, but also effectively prevents similar subjects' collusive attack to the system.

Keywords Access control constraints, Separation of duty, Chinese wall policy, Subject similarity

1 引言

约束[1-4]是访问控制的主要动机。基于角色访问控制(Role-Based Access Control, RBAC)[5,6]中的职责分离约束[1,4]和中国墙策略(Chinese Wall Policy)[2]是访问控制中的主要约束。这两种约束有关的主要研究工作见文献[1,3,4,7-12]。文献[1,3,4,7,9]与RBAC约束有关。文献[1]对RBAC约束进行分类,提出RBAC约束的基于集合论的表示和实施。文献[4]提出基于角色的约束语言(Role-Based Constraints Language 2000, RCL 2000)用于形式化地表示RBAC的职责分离约束。文献[3]挖掘不同类型的RBAC约束。文献[7]提出的基于信任和风险的访问控制机制可以灵活地表示文献[1]中列举的基于角色的、基于权限的以及基于对象的职责分离约束。文献[9]首次定义基于属性的访问控制(Attribute Based Access Control, ABAC)[13]的约束语言——基于属性的约束描述语言(Attribute Based Constraints Specication Language, ABCL),它可表示RBAC的职责分离约束。文献[7,8,10-12]等与中国墙策略有关。文献[7]提出的访问控制机制允许高信任度的用户越过中国墙安全策略,比较灵活。文献[8]提出一种最小限制地实施中国墙安全策略的方法。文献[11,12]利用RBAC实施中国墙策略。文献[7,8,12]等的目的是降低中国墙安全策略的严格性,提高灵活性。文献[10]提出中国墙集中式管理系统(Chinese Wall Central Management System, CWCMS),它在云计算中能有效地实施中国墙安全策略。

约束可以在很大程度上降低访问权限的风险[14]。前期工作[7]分析若干用户合谋访问高风险权限集合中的权限带来的风险,其中给出潜在用户组的概念。文献[15]提出在

到稿日期:2014-05-23 返修日期:2014-09-15 本文受国家自然科学基金项目(11261057,11461069),新疆维吾尔自治区教育厅高校科研计划重点项目(XJEDU2012I01),新疆维吾尔自治区人力资源和社会保障厅留学人员科技活动项目资助。
阿不都艾尼·阿不都西库尔(1991-),男,硕士生,主要研究方向为访问控制,E-mail:abudu777@163.com;**开依沙尔·热合曼**(1978-),男,博士,讲师,主要研究方向为数值计算、最优化;**努尔买买提·黑力力**(1976-),男,博士,副教授,主要研究方向为网络信息安全、访问控制,E-mail:nurmamat@gmail.com(通信作者)。

RBAC中权限越集中于少数用户，则风险就越大。通过获取若干权限完成一个敏感任务，要求一定数量的用户参与。总之，访问控制中只考虑主体（或用户）和客体（或对象）之间的关联关系是不够的，还需考虑主体之间的关联关系。例如，考虑同一个指导导师的两个博士生 A 与 B，他们毕业后 B 撰写一篇学术论文向某个学术期刊投稿。由于他们同行，A 可能被选为 B 的论文的审稿人，这时 A 可能会滥用自己的权限而给予 B 的低质量的论文很高的评价，最终可能导致学术欺骗。从访问控制的角度看，同一篇论文的投稿和审稿不能由同一个主体甚至不能由若干相似主体完成。该例子中 A 与 B 有很多相似性，如他们的指导导师、毕业院校、研究方向等都相似；此外他们在博士期间可能合作发表过学术论文，我们可以认为他们是相似用户。该期刊的在线投稿审稿系统指定审稿专家时，如果条件允许有必要考虑 A 与 B 在属性上的相似性，以限制 A 做 B 的论文的审稿人。所以访问主体的属性信息或他们之间的关联关系在一定程度上可以回答哪些主体会恶意合作。

RBAC中的职责分离约束只考虑角色意义上的主体相似性，没有显式地定义相似主体，而中国墙策略没有考虑主体相似性。访问控制约束中引进访问主体的相似性能够提高约束定义的灵活性和有效性。为此本文主要考虑访问控制中主体之间的相似性，挖掘相似主体，在此基础上提出基于相似主体的访问控制约束。

2 访问控制约束及主体和客体之间的关系

约束是访问控制中的一个重要概念。常见的约束有RBAC的职责分离约束和中国墙策略。约束可以防止若干主体合谋分工访问应用系统中可能会给系统带来巨大损失的客体。所以需要更清晰地认识约束的初衷，分析访问控制中主体之间的关系客体之间的关系以及主体与客体之间的关系。

2.1 访问控制约束

下面举两个典型的约束的例子。

(1)$(R,\{ob_{i_1},ob_{i_2},\cdots,ob_{i_k}\}),ob_{i_1},ob_{i_2},\cdots,ob_{i_k}\in\{ob_1,ob_2,\cdots,ob_n\},2\leqslant k\leqslant n$（基于客体的职责分离约束）：该约束要求任何角色不能同时访问特定客体集$\{ob_1,ob_2,\cdots,ob_n\}$中的 k 个客体 $ob_{i_1},ob_{i_2},\cdots,ob_{i_k}$。该约束意味着客体集$\{ob_1,ob_2,\cdots,ob_n\}$中的任何 k 个客体 $ob_{i_1},ob_{i_2},\cdots,ob_{i_k}$ 的组合是有额外风险的。这种约束防止若干主体一起通过相同角色同时对这些风险客体集中的客体进行特定的操作以完成某个特定的任务。

(2)$(U,\{ob_1,ob_2\},op)$（中国墙策略）：该约束要求任何一个用户都不能同时对客体 ob_1 和 ob_2 进行操作 op。它意味着客体 ob_1 和 ob_2 的组合是有额外风险的，即这种约束防止任何用户通过对这些客体同时进行特定的操作以完成某个特定的任务。

总之，(1)不仅考虑客体的风险集合，还考虑了相似主体，这个风险组合针对拥有相同角色的主体。该约束防止拥有相同角色的主体通过分工访问风险客体集合中的部分或全部元素。(2)可以看成(1)的特殊情况，可以假定用户与自己相似。此外，由于权限是由客体和客体上的操作组成的，因此基于权限的职责分离约束$(R,\{p_{i_1},p_{i_2},\cdots,p_{i_k}\}),p_{i_1},p_{i_2},\cdots,p_{i_k}\in\{p_1,p_2,\cdots,p_n\},2\leqslant k\leqslant n$，也可以归一到基于客体的职责分离约束(1)。为了简洁，本文在后面仅讨论客体的风险集合。

2.2 主体和客体之间的关系

访问控制中主体之间的关系、客体之间的关系以及主体与客体之间的关系可以通过一个例子来说明。如图1所示，具有相似性的主体 s_1,s_2,s_3,s_4,s_5 中，s_1,s_3,s_5 试图先后分别访问风险客体集合中的部分客体 ob_1,ob_3,ob_4。s_1,s_2,s_3,s_4,s_5 可能是在某机构同一份部门工作的几个人，所以具有一定的相似性。$RC_OB_3=\{ob_3,ob_4,ob_1\}$是由风险客体集合 $Risky\text{-}Combination\_OB=\{ob_1,ob_2,ob_3,ob_4\}$ 中的3个客体 ob_1,ob_3,ob_4 组成的。ob_1,ob_3,ob_4 可能是该机构中的3份部分资料，它们的组合可能重构一份重要资料。该机构原则上不允许同一个办公室的人查看资料 ob_1,ob_2,ob_3,ob_4 中的任何3个，否则会有一定的风险。这是一种访问控制约束，如果假设主体的相似性由其角色决定，且同一个办公室的人具有相同的角色，则以上提到的基于客体的职责分离约束(1)反映并防止这种情形。如果主体的相似性不能由角色决定，那么(1)不能刻画该机构的访问控制约束策略，缺乏灵活性。

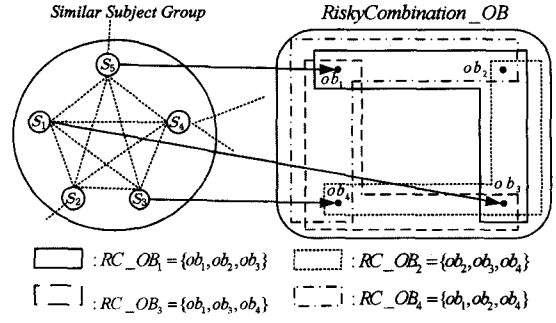

图1 主体和客体之间的关系示例

3 相似主体挖掘与修正的访问控制约束

3.1 相似主体挖掘

如上节讨论，不同主体访问同一个风险客体集合中的客体时，应考虑主体之间的相似性，访问控制中有必要挖掘相似主体组。

从RBAC约束的含义来看，RBAC中的主体相似性是由一个角色决定的，实际上角色可以称为主体的一个属性，而访问控制决策根据主体的角色属性进行。不失一般性，本文讨论基于属性的访问控制 ABAC(Attribute Based Access Control)[13] 中的相似主体和风险客体。

假设在一个 ABAC 系统中的属性集合为 $ATTR=\{Attr_1,Attr_2,\cdots,Attr_t\}$，这些属性的权重分别为 $w_1,w_2,\cdots,w_t$，$\sum_{k=1}^{t}w_k=1,w_k>0$，主体 s 的属性值分别为 $AttrV_1(s),AttrV_2(s),\cdots,AttrV_t(s)$，本文只讨论属性值均为离散的情况，下面给出主体属性相似度的定义。

定义1 定义两个主体 s_i 与 s_j 的属性相似度为：

$$ATTR\_SIM(s_i,s_j)=\sum_{k=1}^{t}w_kAttrSim_k(s_i,s_j) \tag{1}$$

其中

$$AttrSim_k(s_i,s_j)=\begin{cases}1, & AttrV_k(s_i)=AttrV_k(s_j)\\ 0, & AttrV_k(s_i)\neq AttrV_k(s_j)\end{cases}$$

在一个 ABAC 系统中，可以根据系统需要定义属性相似

度阈值，两个主体之间的相似度如果大于等于这个阈值，就可以说两个主体相似。对于两个以上的主体有下面的定义。

定义 2（相似主体组） 设 ABAC 系统属性集合为 $ATTR=\{Attr_1,Attr_2,\cdots,Attr_t\}$，这些属性的权重分别为 $w_1,w_2,\cdots,w_t$，$\sum_{k=1}^{t} w_k=1$，$w_k>0$，对于给定的相似度阈值 $wATTR\_SIM_\tau$，定义集合 $SC=\{s_1,s_2,\cdots,s_r\}$ 为相似主体组，如果 $\forall s_i,s_j\in SC$，就有 $ATTR\_SIM(s_i,s_j)\geqslant wATTR\_SIM_\tau$，$s_i$ 与 s_j 称为相似主体，记 $s_i \overset{w}{\cong} s_j$。

根据定义 2，ABAC 系统中相似主体组的挖掘事实上变成了主体的重叠分组问题，可以用 CFinder[1)][16,17] 得到系统中所有主体的相似聚类。对于给定的相似度阈值 $wATTR\_SIM_\tau$ 和属性权重 $w_1,w_2,\cdots,w_t$，可以得到系统中的所有主体 $SUBJECT$ 的相似主体组 $SC_1,SC_2,\cdots,SC_m$，且 $SUBJECT=\bigcup_{i=1}^{m} SC_i$。

3.2 修正的访问控制约束

通过定义相似主体组，下面提出如何约束相似主体访问风险客体集合中的全部客体或部分客体。首先给出相似主体访问控制约束的定义。

定义 3（相似主体访问控制约束） 定义三元组 $\langle RiskyCombination\_OB,\kappa,T_\Delta\rangle$ 为相似主体访问控制约束，如果其中 $RiskyCombination\_OB=\{ob_1,ob_2,\cdots,ob_n\}$ 是一个风险客体的集合，对任意时刻 T，风险客体集合中的 κ 个客体在时间间隔 $[T,T+T_\Delta]$ 内连续被同一个相似主体组成员访问是禁止的。

假设：

- $RiskyCombination\_OB_i$，$i=1,2,\cdots,l$，为系统中所有风险客体集合；
- κ_i 为风险客体集合 $RiskyCombination\_OB_i$ 中风险客体的个数，$i=1,2,\cdots,l$；
- $T_{SC,i}$ 为相似主体组 SC 成员首次访问风险客体集 $RiskyCombination\_OB_i$ 中的一个客体的时间；
- $[T_{SC,i},T_{SC,i}+T_{i\Delta}]$ 为针对主体组 SC 和风险客体集 $RiskyCombination\_OB_i$ 执行相似主体方控制约束的时间间隔，如果 SC 成员最后一次访问 $RiskyCombination\_OB_i$ 中的某个客体的时间超出 $[T_{SC,i},T_{SC,i}+T_{i\Delta}]$，且成功访问，则将 $T_{SC,i}$ 改为这次访问的时间。

$H\_OB_{SC,i}$ 为在给定时间间隔 $[T_{SC,i},T_{SC,i}+T_{i\Delta}]$ 内 $RiskyCombination\_OB_i$ 中已被给定相似主体组 SC 中的主体访问过的不同客体组成的集合，$i=1,2,\cdots,l$。

图 2 所示的算法给出了相似主体组成员访问风险客体集合中给定客体的访问控制决策算法，该算法能执行定义 3 中的约束。

下面分析图 2 所示的算法如何执行定义 3 中的约束。对于主体 s 访问 ob 的请求，如果 ob 不属于任何风险客体集，则不执行定义 3 中的约束，按正常访问控制决策算法进行决策，此处不再赘述。如果客体是风险客体集合元素，则先找出该客体所属的风险客体集合 $RiskyCombination\_OB_i$，假设 $ob\in RiskyCombination\_OB_i$，要执行定义 3 中的约束，也就是要保证任何一个相似主体组成员在给定时间间隔内访问 $RiskyCombination\_OB_i$ 中的客体个数不能超过 κ_i-1，所以对 s 所属的所有的相似主体组逐一检查。假设 $SCliques(s)$ 为 s 所属的所有的相似主体组组成的集合，对所有 $SC\in SCliques(s)=\{SC_i\mid s\in SC_i,i=1,2,\cdots,m\}$，检查在 $t\in[T_{sc,i},T_{sc,i}+T_{i\Delta}]$ 内该主体组成员从 $RiskyCombination\_OB_i$ 中成功访问过的客体个数是否小于 κ_i-1，亦即 $|H\_OB_{SC,i}|<\kappa_i-1$。如果是，则主体的访问请求允许，进行后续工作，将此次访问的客体加入到 $H\_OB_{SC,i}$ 中。对于超时的相似主体组，将开始访问 $RiskyCombination\_OB_i$ 的时间调成当前时间。如果 $|H\_OB_{SC,i}|=\kappa_i-1$，则拒绝访问。

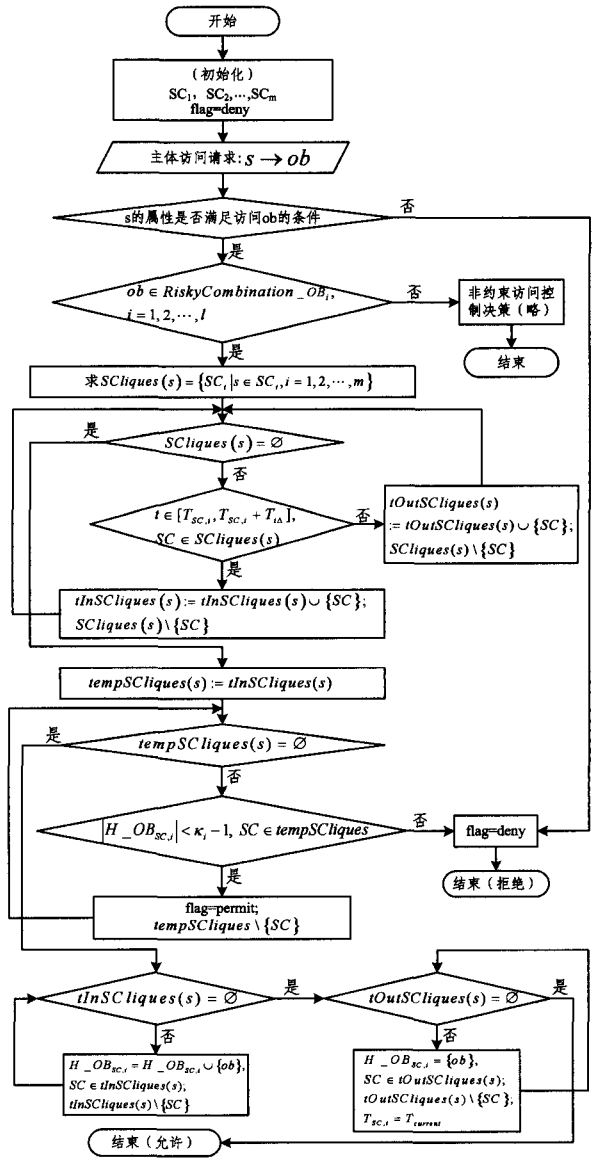

图 2 相似主体组的访问控制决策算法

需要补充的是，本文提出的修正的访问控制约束算法能够处理 RBAC 的基于客体的职责分离约束(1)，从而支持(2)。对主体进行聚类时，将角色看成主体的一个属性即可。

4 实验与分析

为了评价本文方法，实现了一个基于 J2EE 的简单的原型系统，以进行主体访问客体的小规模模拟测试。系统的运行环境为 Intel(R) Core(TM)2 Quad CPU Q9500 @ 2.83Hz

1) CFinder (http://www.cfinder.org/)

的 PC 机，内存为 4GB，操作系统为 Windows 7 旗舰版，数据库管理软件使用 MySQL5.6，Web 服务器软件使用 Apache Tomcat7.0。测试在局域网内举行。测试过程如下：在数据库中创建 2000 个主体、100 个属性和 2000 个客体；为了简洁，定义属性值为布尔类型(0,1)，为每个主体随机选择 5 个属性，赋值为 1，其余的赋值为 0；为每个客体随机指定 10 个属性，如果主体的值为 1 的属性是这 10 个属性中的一个，主体就能访问该客体。再根据定义 1、2，对 2000 个主体通过 CFinder2.0.6 进行重叠分组，实验中计算主体相似度时，对相似度的计算公式做以下改动。

$$AttrSim_k(s_i,s_j)=\begin{cases}1, & AttrV_k(s_i)=AttrV_k(s_j)=1\\ 0, & \text{其它}\end{cases}$$

且属性的权重 $w_i=0.01, i=1,2,\cdots,100$，相似度阈值 $wATTR\_SIM_\tau=0.02$。于是得到不同规模的相似主体组，相似主体组规模和个数如表 1 所列。

表 1　相似主体组

相似主体组规模	2	3	4	5	6	7	8	9
相似个体组个数	53255	4768	2106	850	234	69	11	1

然后从局域网内另一台 PC 机随机形成并向服务器发送 10000 个主体访问客体的请求，请求实际上简单地查询主体 s_i 是否有访问客体 ob_j 的权限，主体请求按照基于属性的访问控制进行访问控制决策，不考虑相似主体组，也不设置并考虑风险客体的集合。结果有 3948 个请求被允许，剩余 6052 个请求被拒绝。之后随机设置风险客体的集合，如表 2 所列，上面形成的 10000 个访问请求针对已得到的相似主体组以及设置的风险客体集合重新测试，也即启用本文中的相似主体访问控制约束，最终得到原有 3948 个被允许的请求中有 53 个请求被拒绝。易见，原因是同一个相似主体组成员试图访问风险客体集合中的 κ 个客体。

表 2　风险客体集合

风险客体集合的基数	10	5	3	2
κ	7	3	2	2
风险客体集合的个数	5	10	20	30

需要补充的是，以上设计的实验同时考虑了 RBAC 约束，定义的 100 个属性可以认为是角色，主体的某个属性的值为 1 等效于主体拥有该角色，由于 RBAC 中权限由客体和客体上的操作组成，因此给客体指定 10 个属性，如果补充客体上的操作，这样就得到这 10 个角色和由该客体与客体上补充的操作组成的权限间的权限角色指派。

结束语　本文首先分析了访问控制约束的初衷，提出相似主体组的概念，并在此基础上提出相似主体访问控制约束；其次设计了基于属性的访问控制决策实验，实验主要针对修正的访问控制约束。修正的约束不但能覆盖传统的 RBAC 约束和中国墙策略，而且能处理相似主体合谋攻击系统的情形，提高访问控制约束定义的灵活性和有效性。本文没有对风险客体集合的挖掘进行讨论，对于不同的应用系统应该具体讨论。

参 考 文 献

[1] Crampton J. Specifying and enforcing constraints in role-based access control[C]// Proceedings of the eighth ACM symposium on Access control models and technologies. ACM, 2003: 43-50

[2] Brewer D F C, Nash M J. The chinese wall security policy[C]// Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy. 1989: 215-228

[3] Ma X P, Li R X, Lu Z D, et al. Mining constraints in role-based access control[J]. Mathematical and Computer Modelling, 2012, 55(1): 87-96

[4] Ahn G J, Sandhu R. Role-based authorization constraints specification[J]. ACM Transactions on Information and System Security (TISSEC), 2000, 3(4): 207-226

[5] Sandhu R S, Coynek E J, Feinsteink H L, et al. Role-Based Access Control Models[J]. IEEE computer, 1996, 29(2): 38-47

[6] INCITS A. INCITS 359-2004, American national standard for information technology, role based access control[S]. NewYork: ANSI INCITS, 2004

[7] Helil N, Kim M, Han S. Trust and Risk based Access Control and Access Control Constraints[J]. KSII Transactions on Internet & Information Systems, 2011, 5(11): 2254-2271

[8] Sharifi A, Tripunitara M V. Least-restrictive enforcement of the Chinese wall security policy[C]// Proceedings of the 18th ACM Ssymposium on Access Control Models and Technologies. ACM, 2013: 61-72

[9] Bijon K Z, Krishman R, Sandhu R. Constraints Specication in Attribute Based Access Control[J]. Science, 2013, 2(3): 131-144

[10] Tsai T H, Chen Y C, Huang H C, et al. A practical chinese wall security model in cloud computing[C]// 2011 13th Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, 2011: 1-4

[11] 何永忠，李晓峰，冯登国. RBAC 实施中国墙策略及其变种的研究[J]. 计算机研究与发展，2007，44(4)：615-622

[12] 张毅辉，梁久祯. 侵略型中国墙安全模型的 RBAC 配置的扩展研究[J]. 计算机工程与应用，2010，46(29)：114-116

[13] Priebe T, Fernandez E B, Mehlau J I, et al. A pattern system for access control[M]// Research Directions in Data and Applications Security XVIII. Springer US, 2004: 235-249

[14] Baracaldo N, Joshi J. A trust-and-risk aware rbac framework: tackling insider threat[C]// Proceedings of the 17th ACM symposium on Access Control Models and Technologies. ACM, 2012: 167-176

[15] Chari S, Lobo J, Molloy I. Practical risk aggregation in rbac models[C]// Proceedings of the 17th ACM symposium on Access Control Models and Technologies. ACM, 2012: 117-118

[16] Palla G, Derényi I, Farkas I, et al. Uncovering the overlapping community structure of complex networks in nature and society [J]. Nature, 2005, 435(7043): 814-818

[17] Farkas I, ábel D, Palla G, et al. Weighted network modules[J]. New Journal of Physics, 2007, 9(6): 180