# 一种基于区间值的模糊访问控制策略研究

薛 丹,杨 宸,周 健
(陕西师范大学 计算机科学学院,陕西 西安 710062)

**摘 要**:访问控制是网络中一种重要的安全防护技术。在传统的模糊访问控制中,所评判的用户指标都是由某个确定的值来表示,但是大多数情况下,在用户的评语指标上,属于该指标的某个评语的程度并不能用一个确定的数来表示。针对这一问题,文中通过区间值来表示用户的评语指标,提出了基于区间值模糊访问控制的策略,运用区间值模糊综合评判法分析出用户的访问权限,更好地满足了普适计算环境下访问控制的安全性和实用性。并且通过实例分析表明,基于区间值的模糊访问控制在实际应用中是有效的。

**关键词**:模糊访问控制;模糊授权;区间值模糊评判;普适计算
**中图分类号**:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)01-0246-04

# Research on Interval-Valued Based Fuzzy Access Control

XUE Dan, YANG Chen, ZHOU Jian
(College of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

**Abstract**: On the network, access control is an important security technique. In the traditional fuzzy access control, the evaluation of the users' properties is indicated by the determined value. But in most cases, in the users' comment index, deterministic is not necessarily a certain number. To address this problem, use interval-valued to represent the users' comment index. Propose, based on interval value fuzzy expression, a new access control strategy. Analyze users' access purview which is counted by the interval-valued fuzzy comprehensive evaluation method. This method can better satisfy the security and practicality in the pervasive computing. And the application instance shows that the interval-valued based fuzzy access control is effective in practice.

**Key words**: fuzzy access control; fuzzy authorization; interval-valued fuzzy evaluation; pervasive computing

## 1 问题引入

访问控制在资源授权的安全防范措施中占据着重要的地位,给定的计算环境下,访问控制通常是一个子系统,授予用户操作客体的权利,同时根据定义好的安全策略控制主体的访问权限。访问控制的主要任务是确保资源的完整与信息的安全,是保证资源安全最重要的核心策略之一。随着人们对访问控制的研究,先后出现了自主访问控制 DAC,强制访问控制 MAC,基于角色的访问控制 RBAC,基于任务的访问控制 TBAC,基于任务角色的访问控制 TRBAC 等等[1]。

传统的访问控制很适合运用在能够对用户进行确定分配的机构中。我们知道,普适计算[2]是把现实世界与计算世界融合起来,以用户、应用为中心的一种新的环境,而不是传统意义上的以计算机为中心的环境,这样在进行访问控制时,要求访问评判根据各种评语指标进行动态的授权机制[3,4]。同时,在普适计算环境下,通常系统会拥有大量的用户,如果由确定的系统管理员为用户一一进行评判并授权,必然会给管理员带来沉重的负担,对传统的访问控制指派关系的维护既耗时又易出错。如果由于管理员的疏忽而在为用户进行授权时出错,将会导致一系列严重后果。

为了满足普适计算环境的要求,使安全策略规范化、提高安全性,同时减轻管理员的负担,人们引入了模糊策略。在以前的模糊综合评判中,大多数情况下都是用某个确定的值来表示评判对象,从而计算出每个用户的访问权限。但是在大多数情况下,用户评判指标往往带有不确定性,也就是说,在用户的评判指标上属于某个评语的程度不是一个确定的数,而是由某个区间值来表示,针对这一问题,文中提出了一种基于区间值的模糊访问控制策略[1,5]。

## 2 区间值模糊访问控制

用户对客体进行访问时,最重要的就是系统对用户进行客观公平的等级评判,由于评判因素的不确定性以及评价等级的模糊性[6],用户就某些评判指标和

**收稿日期**:2011-05-31;**修回日期**:2011-09-10
**基金项目**:陕西省科技攻关项目(2008K01-58)
**作者简介**:薛 丹(1987-),女,陕西渭南人,硕士研究生,研究方向为信息安全与密码学。

等级通常都是由某个确定的值来表示。如果以区间值考虑评判指标,通过综合评估,以区间值的大小来评判最终的等级评判结果,将会更客观、更安全。

### 2.1　构成区间值模糊访问控制模型的元素

(1) $X=\{x_1,x_2,\cdots,x_n\}$ 是因素集,其中 $x_i$ 是评语指标,表示用户在进行访问时,所需要进行的评判因素。如学生评价中的"身体状况"、"心理状态"等;

(2) $Y=\{y_1,y_2,\cdots,y_n\}$ 是评语集,其中 $y_i$ 是模糊语言,表示专家为用户打分时所依据的等级判断。如对学生评价指标中的"优秀"、"良好"等,这实际上是些模糊集合;

(3) $U=\{u_1,u_2,\cdots,u_n\}$ 是用户集,表示被评判的对象,即访问控制的主体。如学生;

(4) $O=\{o_1,o_2,\cdots,o_n\}$ 是客体集,表示用户需要访问的资源等;

(5) 权限集:表示用户对客体进行特定模式的访问操作,其本质取决于系统的实现细节,如操作系统中需要保护的文件、目录、设施等,其相应的操作为读、写等;

(6) $N=\{N_1,N_2,\cdots,N_n\}$ 表示模糊授权集合,即根据用户的评判标准分配给用户所具有的权限集合;

(7) 区间值[7]:用 $[R]$ 表示实数集 $R$ 上全体闭区间所形成的集合,即 $[R]=\{[a^-,a^+]:a^-\leqslant a^+;a^-,a^+\in R\}$。表示对用户所进行评价的一个区间范围。注:文中所提到的区间值均为正区间值。

### 2.2　区间值模糊评判

由于用户的评语指标本身所具有的模糊性、不确定性、不完整性等特性,使得系统在评判时会出现一个变动的评判数,当然,这个数的波动通常是在一个固定的区间里。传统的访问控制方法和模型是基于精确的数学理论形成的,随着信息技术的发展,引入了普适计算的概念,其所具有的透明性、灵活性、模糊性、不确定性等特性,使得传统的访问控制已经不能满足普适计算环境下人们对它的要求。在日常生活中,通常会有一些模糊的概念,如:在使用智能教室时,需要确保教室的最高温度为 40℃,最低温度为 0℃,那么,教室的温度就有可能是在 0℃ ~40℃之间,可以将这种"可能性"定义为[0,40],而它并不是一个确定的值。

由此可见,区间值模糊评判[8]是通过使用一个数值区间来描述某因素对给定模糊概念的隶属程度。这样,将比传统的模糊评判更切合实际、更精确。由上面的例子可以看出,在某些情况下习惯用区间值代替确定的值来表示隶属关系。

区间值模糊评价是模糊评价的推广,相对于模糊评价而言,它更能够满足人们日常的需求,增强了实用性。在实际的应用系统中,运用区间值模糊综合评判法进行访问控制时,应遵循以下步骤[8,9]:

(1) 首先专家通过投票或打分的方法对用户的各个评语指标进行评价,实行公正的评价方法,根据实际情况,给出一个评价的结果区间值;

(2) 根据在实际应用中所需的等级来确定隶属函数,对每个指标的权重进行分配;

(3) 通过区间值模糊综合评估矩阵进行加权平均,分别对用户的各个指标进行模糊评判,得到每个用户的模糊授权区间;

(4) 利用模糊数学中区间数的序关系确定主体的"最大"区间值,即确定了用户的评价指标,从而对用户进行授权决策。

注:实际应用中,专家的人数、用户的指标以及每个指标的权重由系统根据实际情况来确定其大小。

这样,加强了访问控制的安全性和实用性,利用这种方法,可以评定出评判对象的基本情况,得到的等级就是通过原指标区间简化的结果。

### 2.3　模糊授权规则

区间值模糊访问控制在授权的过程中,也会具有模糊性,系统会根据模糊评判分析结果对用户授予权限,这样就满足了普适计算环境下对访问控制的要求[10]。

定义不同的模糊授权集合,同时,根据具体情况把授权分成不同程度的集合。如果用户需要访问的客体即为文件,表 1 是给出的学生对多媒体教室中文件的访问权限的模糊授权集合:

表 1　模糊评估集合

| 模糊授权集合 | 授权 | 权限 |
|---|---|---|
| $N_1$ | 不授权 | |
| $N_2$ | 弱授权 | 读 |
| $N_3$ | 部分授权 | 读,写 |
| $N_4$ | 强授权 | 读,写,拷贝 |
| $N_5$ | 完全授权 | 读,写,拷贝,修改 |

假设这里有 5 种模糊授权方式:不授权、弱授权、部分授权、强授权、完全授权等,它们分别对应的权限如表 1 所示。本次研究中,假设评语分为五个等级:很差、一般、中等、良好、优秀。如果综合模糊评判为"很差",对申请访问的用户进行"不授权";如果综合模糊授权评判为"一般",对申请访问的用户进行"弱授权"等,以此类推,一般情况下,定义评语等级与授权方式一一对应。并没有明确地给出各个评判语的取值范围,而是根据区间模糊综合评判法来分析结果,找出评判结果的最大区间,继而找到该用户的最大概率的授权。这样,分析综合考评,能够更确切地得到每个用户的授权机制。以此避免了授权过程中的不公平现象。

在下一节中，根据一个具体的实例来说明基于区间值的模糊访问控制的策略。该实例更好地体现了这种方法的可用性和实用性。

## 3 区间值模糊访问控制的授权原理

通过模糊访问控制授权机制，可以实现区间值模糊访问控制的授权[7,11]。我们知道，区间值模糊综合评估的目的就是要从评语集中选择出最佳的评语作为最后的评估结果[9]，判断出用户的授权集合，确定用户能够进行的访问权限，最终完成用户的访问服务，满足用户的需求。

下面以学生为例，分析区间值模糊访问控制的授权原理，通过下面的验证，更清晰地理解这种授权方法的过程和优势。

根据日常评判，学生素质的指标及权重可以被定为：

$x_1$：遵纪守法，$w_1 = 0.3$；

$x_2$：热爱生活，$w_2 = 0.1$；

$x_3$：爱护公物，$w_3 = 0.2$；

$x_4$：身体状况，$w_4 = 0.15$；

$x_5$：心理状态，$w_5 = 0.25$；

于是，得到指标集 $x$ 和权重集 $w$：$x = \{x_1, x_2, x_3, x_4, x_5\}$，$w = \{w_1, w_2, w_3, w_4, w_5\}$。通常，各个指标对最终的评判授权的影响结果是不同的，因此，根据实际情况对评价指标分配不同的权重。注，权重 $w_i$ 通常满足 $w_1 + w_2 + w_3 + w_4 + w_5 = 1$。

在这里，假设评语分为五个等级：$y_1$：很差；$y_2$：一般；$y_3$：中等；$y_4$：良好；$y_5$：优秀，从而得到评语集 $y = \{y_1, y_2, y_3, y_4, y_5\}$。建立评估矩阵：因素与用户之间可以通过建立隶属关系，最终用模糊关系矩阵 $\boldsymbol{R}$ 来表示。在这里，$y_i$ 表示区间[0,100] 上的模糊集，评语集本身就具有模糊性，通过建立的隶属函数能够更清晰地体现出这种模糊性，$t$ 表示区间值，即用户指标通过专家的评判所得到的评价得分，在这里，定义 $t \in [0, 100]$。

则建立的隶属函数依次为：

$$y_1(t) = \begin{cases} 1, 0 \leqslant t \leqslant 40 \\ \dfrac{60 - t}{20}, 40 \leqslant t \leqslant 60 \\ 0, 60 \leqslant t \leqslant 100 \end{cases}$$

$$y_2(t) = \begin{cases} 0, 0 \leqslant t \leqslant 40, 80 \leqslant t \leqslant 100 \\ \dfrac{t - 40}{20}, 40 \leqslant t \leqslant 60 \\ 1, 60 \leqslant t \leqslant 70 \\ \dfrac{80 - t}{10}, 70 \leqslant t \leqslant 80 \end{cases}$$

$$y_3(t) = \begin{cases} 0, 0 \leqslant t \leqslant 60 \\ \dfrac{t - 60}{10}, 60 \leqslant t \leqslant 70 \\ 1, 70 \leqslant t \leqslant 80 \\ \dfrac{100 - t}{20}, 80 \leqslant t \leqslant 100 \end{cases}$$

$$y_4(t) = \begin{cases} 0, 0 \leqslant t \leqslant 70 \\ \dfrac{t - 70}{10}, 70 \leqslant t \leqslant 80 \\ 1, 80 \leqslant t \leqslant 90 \\ \dfrac{100 - t}{10}, 90 \leqslant t \leqslant 100 \end{cases}$$

$$y_5(t) = \begin{cases} 0, 0 \leqslant t \leqslant 80 \\ \dfrac{t - 80}{10}, 80 \leqslant t \leqslant 90 \\ 1, 90 \leqslant t \leqslant 100 \end{cases}$$

这里定义的隶属函数是在实际应用中根据评语等级来确立的，如果评语等级发生了变化，这些隶属函数可以由系统设计人员进行调整[12,13]。

假设对四名同学进行授权，评委用打分或投票的方法对四个用户的五项指标分别进行评价，得分情况见表 2：

表 2 四名同学的综合得分表

| 指标 | Alice | Bob | Cairo | Dalton |
|---|---|---|---|---|
| $x_1$ | [82,84] | [85,88] | [89,95] | [87,92] |
| $x_2$ | [88,92] | [75,78] | [83,87] | [90,93] |
| $x_3$ | [89,90] | [78,80] | [90,91] | [93,94] |
| $x_4$ | [90,93] | [82,83] | [82,85] | [85,86] |
| $x_5$ | [85,87] | [74,76] | [78,84] | [94,96] |

以 Alice 为例：为了得到模糊关系矩阵，将 Alice 关于 $x_1$ 的得分[82,84]分别代入到隶属函数中，得到 Alice 在指标 $x_1$：遵纪守法上属于很差，一般，中等，良好，优秀的程度分别为：(0,0,[0.8,0.9],1,[0.2,0.4])。

依次将 Alice 的其余四项指标代入隶属函数中，就可以得到关于 Alice 的区间模糊综合评判矩阵：

$$\boldsymbol{R}_A = \begin{pmatrix} 0,0,[0.8,0.9],1,[0.2,0.4] \\ 0,0,[0.4,0.6],[0.8.1],[0.8,1] \\ 0,0,[0.5,0.55],1,[0.9,1] \\ 0,0,[0.35,0.5],[0.7,1],1 \\ 0,0,[0.65,0.75],1,[0.5,0.7] \end{pmatrix}$$

因为每个指标对最终的评判结果影响不同，进一步用加权平均模型做矩阵乘法：

$\boldsymbol{W} \cdot \boldsymbol{R}_A$ = (0,0, [0.595,0.7025], [0.935,1], [0.595,0.745])

记 $\triangle_A = \sum_{i=1}^{n}[a_i^-, a_i^+] = [2.125, 2.4475]$,即把矩阵 $\boldsymbol{W} \bullet \boldsymbol{R}_A$ 的每项所对应的左右区间值分别相加。

再做区间除法,即平均加权法:$[a_i^-, a_i^+]/[\triangle_A^-, \triangle_A^+]$。使得 $\boldsymbol{W} \bullet \boldsymbol{R}_A$ 变为 $H_A = (0, 0, [0.243, 0.331], [0.382, 0.471], [0.243, 0.351])$,这是为了求出每个评语在整个评估策略中所占的比重。依据比较区间值的大小:对于任意给定的区间值$[a,b]$,$[c,d]$,如果 $a < c$、$b < d$,那么$[a,b] < [c,d]$;如果 $a > c$、$b < d$,且 $a + (b-a)/2 < c + (d-c)/2$,那么$[a,b] < [c,d]$。显然,$H_A$ 中最大的区间数是$[0.382, 0.471]$,也就是说,基于其他的评语,Alice 的区间值模糊综合评判更趋近于“良好”。所以,Alice 的综合评判属于“良好”。

相似的,很容易求出 Bob 和 Cairo、Dalton 其他三位同学的区间值:

$H_B = (0, [0.050, 0.118], [0.409, 0.483], [0.318, 0.432], [0.075, 0.140])$;

$H_C = (0, [0, 0.027], [0.214, 0.401], [0.308, 0.546], [0.202, 0.407])$;

$H_D = (0, 0, [0.162, 0.267], [0.298, 0.446], [0.366, 0.499])$。

分别找出他们的各个评语在整个评估中所占的最大比重,也即是用户评语最大的区间值,分析可得:这三位同学的综合评判分别为“中等”,“良好”,“优秀”。根据模糊授权规则得到四个用户的授权集合分别为:强授权、部分授权、强授权、完全授权。如表 1,对应每个授权的权限,可以看出每个用户对于资源的访问权限。发现对 Alice 和 Cairo 来说,他们都赋予“强授权”,但是,根据上面对区间值大小进行判断的分析结果,不难看出$[0.382, 0.471] < [0.308, 0.546]$。这时,根据区间值之间比较的大小,可以对他们两人进行优先级分配,对于同一个授权区域来说,区间值大的享有优先的访问权限,也就是说,当 Alice 和 Cairo 同时对资源进行访问时,优先处理 Cairo 的申请。

上面的例子,将模糊数学中的区间值模糊运用到访问控制中,详细介绍了基于区间值的模糊访问控制的授权原理,可以看出,这种策略更适合运用到实际应用中。当然,可以将其扩展到各个领域内,通过模糊评判、模糊授权对用户的访问进行动态的授权,更好地体现了访问控制的公平性,同时,通过比较区间值的大小来判断用户的优先级,保证了资源优先为优先级高的用户来提供授权。

## 4　结束语

引入区间值模糊综合评判法是文中对访问控制研究的核心。授权是访问控制的依据,文中是通过评价矩阵来实现的。

从上节的实例中可以看出,将区间值模糊综合评判运用到访问控制中,能够更好地满足现实的要求,确保更公平地分配给每个用户访问权限,同时确保了评价的正确性,即使修改了某个评价值,也不会影响到整个的授权机制。但是,随着信息技术飞速发展,需要进一步思考在普适计算环境下对访问控制的安全性要求,确保访问资源的完整性和保密性,需要检测器来对用户进行访问资源后进行审计,重新确定用户的访问权限。同时,建立多级评估模型,以提供更全面、更准确、更安全的评估策略,以确保安全授权。

**参考文献:**


[1] 张海娟. 普适计算环境下基于信任的模糊访问控制模型[J]. 计算机工程与应用,2009,45(27):107-112.

[2] 3GPP TS 23.228, V.8.2.0. IP Multimedia Subsystem (IMS)[S]. 2007.

[3] Want R, Borriello G, Pering T, et al. Disappearing hardware[J]. IEEE Pervasive Computing, 2002, 1(1): 36-47.

[4] Satyanaryanan M. Pervasive Computing: Vision and Challenges[J]. IEEE Personal Communications, 2001, 8(4): 10-17.

[5] 窦文阳,王小明,张立臣. 普适环境下的动态模糊访问控制模型研究[J]. 计算机科学,2010,37(9):63-67.

[6] Larsen K L, Matthiesen E V, Schwefel H P, et al. Optimized Macro Mobility within the 3GPP IP Multimedia Subsystem[C]. [s.l.]: [s.n.], 2006.

[7] 孟广武,张兴芬,郑亚林. 基于区间值模糊集的聚类方法[J]. 工程数学学报,2001,1(2):69-73.

[8] 李国成. 学生管理中的区间值模糊综合评判模型[J]. 中国西部科学,2011,10(7):4-5.

[9] 戴　刚. 基于使用控制和上下文的模糊访问控制模型研究[D]. 重庆:重庆大学,2009.

[10] 路　川,胡欣杰,纪　锋. 基于角色访问控制的协同办公系统设计与实现[J]. 计算机技术与发展,2010,20(3):230-233.

[11] 李鸿吉. 模糊数学基础及实用算法[M]. 北京:科学出版社,2005.

[12] 刘逸敏,王智慧,周皓峰,等. 基于 Purpose 的隐私数据访问控制模型[J]. 计算机科学与探索,2010,4(3):222-230.

[13] 张宇卓,苑　飞. 一种基于模糊加权均衡匹配度的区间值模糊推理方法[J]. 辽宁工业大学学报(自然科学版),2009,29(5):343-346.