普适计算环境下基于模糊ECA规则的访问控制方法

张立臣[1,2] 王小明[1] 窦文阳[1] 刘 丁[1]
(陕西师范大学计算机科学学院 西安 710062)[1] (陕西师范大学非线性综合集成实验室 西安 710062)[2]

摘 要 上下文信息是普适访问控制的关键因素,对主体授权和权限使用过程具有决定性影响。普适计算环境下,主体权限、资源访问控制强度和安全策略应随上下文的变化而动态自调节。已有访问控制模型均未考虑上下文对普适环境下访问控制的主动性影响,使得访问控制的主动性和自适应性较差。为了描述上下文对普适访问控制中主体权限、访问控制强度和安全策略的主动性影响,通过对传统ECA规则进行模糊扩展,设计了一种基于区间值模糊集合理论的模糊ECA规则模式,提出了基于模糊ECA规则模式的主动访问控制方法,使授权和访问控制自适应于普适计算环境。

关键词 访问控制,主动访问控制,区间值模糊推理,模糊ECA规则,普适计算
中图法分类号 TP309 **文献标识码** A

Access Control Method Based on Fuzzy ECA Rules for Pervasive Computing Environments

ZHANG Li-chen[1,2] WANG Xiao-ming[1] DOU Wen-yang[1] LIU Ding[1]
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)[1]
(SNNU LAB-NCI, Shaanxi Normal University, Xi'an 710062, China)[2]

Abstract Context information is one of the key factors in pervasive access control systems, which exerts a decisive influence on authorization and access control on subjects. Permissions of the subjects, threshold intensity of the resources and security policies of the system should be automatically adjusted as the changes of the context information in pervasive computing environment, without thorough consideration by current access control models. In order to describe the active influence of fuzzy context information on pervasive access control (permissions of the subjects, the threshold intensity and the security policies of the system), based on the traditional ECA rules and the interval fuzzy set theory, a fuzzy ECA rule scheme was designed, and an active access control method was proposed based on the proposed fuzzy ECA rule scheme. By applying the new access control method, the pervasive access control can be self-adjusted in the pervasive environments.

Keywords Access control, Active access control, Interval-valued fuzzy reasoning, Fuzzy ECA rule, Pervasive computing

1 前言

普适计算(pervasive computing/ ubiquitous computing)把现实世界(物理空间)与计算世界(虚拟空间)深度融合,在这个融合空间中,用户可以随时随地、透明地获得数字化的服务[1-3]。为了对用户提供智能化和个性化服务,同时对用户使用服务的过程进行有效控制,访问控制系统需要访问大量与用户活动相关的上下文,并依据这些上下文对用户进行授权和访问控制,以防止非授权的信息泄露。因此,普适访问控制具有主动性和自适应性,能够随着上下文的变化主动快速地调整用户权限,资源访问控制强度也随着变化的上下文而动态自调节。但是,普适计算所具有的高度开放性、分布式计算和能量受限等特征使得实现对用户的快速授权和动态访问控制成为一个挑战,快速主动访问控制成为普适访问控制研究的一个关键问题;另一方面,普适计算环境中的上下文通常是模糊的、不完备的和动态变化的[4-6],如何从模糊、不完备的上下文中推导出可靠的授权和访问控制结论成为普适访问控制研究中需要解决的另一个关键问题。目前,将传统访问控制(如强制访问控制MAC、自主访问控制DAC和基于角色的访问控制RBAC等)直接应用于普适计算环境中存在如下缺陷:首先,从模型描述层面上讲,传统访问控制是被动式访问控制,缺乏授权和访问控制的主动能力,只有在用户提出资源访问请求后,访问控制系统才进行分析推理,从而导致其授权和访问控制效率较低;其次,传统访问控制建立在被控对象的精确数学描述基础上,不能对访问控制策略的模糊不确定性进行有效刻画,这就直接导致了在普适计算系统中实施的访

到稿日期:2012-05-13 返修日期:2012-11-07 本文受国家自然科学基金项目(60970054,61173094),教育部留学回国人员科研启动基金,陕西师范大学博士科研启动基金资助。
张立臣(1979—),男,博士,讲师,主要研究方向为普适计算、访问控制,E-mail:zhanglichen@snnu.edu.cn;**王小明**(1964—),男,教授,博士生导师,主要研究方向为系统安全、无线传感器网络、访问控制;**窦文阳**(1979—),男,博士生,主要研究方向为系统安全、访问控制;**刘 丁**(1980—),男,博士生,主要研究方向为无线传感器网络、访问控制。

问控制策略与实际的安全需求之间始终存在语义上的间隙；再次，在传统访问控制过程中，资源访问控制强度一旦确定，将在整个访问控制过程中都不会发生任何变化，无法满足普适计算对访问控制强度的动态自适应性要求；最后，传统访问控制一般是基于用户的身份而不是用户所处的上下文状态进行授权和访问控制，而用户的身份在普适计算环境中有时是不知道的，这使得往往无法对用户授权，用户的权限也不能随着上下文状态的变化而动态自调节。因此，普适访问控制必须能主动监控上下文的状态，在上下文发生变化时能从模糊的、不完备的上下文中推导出可靠的授权和访问控制结论，并依据此结论对用户进行授权、对用户使用权限的过程进行有效控制、动态自适应地调节资源访问控制强度和用户权限。总之，普适访问控制应该从模型层面描述并实现访问控制的主动性、模糊性和动态自适应性。

ECA(Event-Condition-Action，事件-条件-动作)规则是主动数据库理论的核心概念[7,8]。基于事件触发机制，ECA 规则可以在策略描述层面上体现用户权限和资源访问控制强度随环境上下文动态自调节的思想，而且可以描述对用户的权限使用过程进行主动控制的思想，这有利于描述普适访问控制的主动性和自适应性需求。另一方面，传统 ECA 规则建立在对知识的精确描述基础上，其事件、条件和动作都是确切定义的，而普适访问控制具有高度的模糊不确定性。这导致了传统 ECA 规则不能直接用于描述普适计算环境中模糊的、不完备的上下文，也不能直接描述模糊访问控制。因此，对 ECA 规则进行模糊化使其适应普适计算环境下主动模糊的访问控制成为研究的一个新思路。

面向普适计算的访问控制研究得到了学者和安全专家的广泛关注，已取得了一定的研究成果[9]。支持隐私保护的访问控制[10]、属性访问控制[11-13]、上下文感知访问控制[14,15]、模糊访问控制[16,17]、基于信任的访问控制[18,19]和动态访问控制[20-23]等模型被相继提出。ECA 规则的研究目前仍主要集中在主动数据库理论和工作流应用方面[24,25]，尚未开展面向普适计算的访问控制模型和应用的研究。

为了克服传统访问控制理论和技术在普适计算环境下支持主动和模糊访问控制的缺陷和不足，本文设计了一种基于区间值模糊集合理论的 ECA 规则(以下简称 FECA 规则)形式；采用 FECA 规则形式，提出了一种面向普适计算的主动访问控制方法。该方法充分考虑了普适访问控制的模糊不确定性、对用户授权的主动性和透明性以及访问控制强度的动态自调节性。FECA 规则由应用环境中的模糊事件所触发，当应用环境中的上下文状态满足 FECA 规则所定义的条件时，主动执行 FECA 规则所定义的模糊动作，对用户进行授权或改变资源访问控制强度，使得对用户的授权和用户使用权限的过程可以自适应于普适计算环境，从而实现自适应和主动访问控制。

2 FECA 规则

ECA 规则也称主动规则(active rules)。基于事件触发机制，ECA 规则可以表示具有主动性的知识，是知识表示和推理领域的研究热点之一。ECA 规则的执行语义是：当预先定义的精确事件发生时，自动触发相应 ECA 规则并评估所触发规则的条件是否满足，如果规则的条件完全满足，则执行规则所预定义的动作。ECA 规则与产生式规则的主要区别在于：ECA 规则中的事件作为一个相对独立的成分，具有专门的监视机制，使得 ECA 规则具有更强的知识描述能力，能够描述环境中各种状态变化，有效表达主动性的知识。另一方面，模糊理论可以有效描述普适环境中的模糊上下文，基于模糊上下文进行模糊推理，可以得出可靠的推理结论；又因为对象的隶属度函数一般难以确定，而其区间值模糊数往往容易确定，所以本文基于区间值模糊集合理论对传统 ECA 规则进行模糊扩展，设计了适用于普适访问控制的 FECA 规则。

定义 1 FECA 规则由模糊事件(fuzzy event)、模糊条件(fuzzy condition)和模糊动作(fuzzy action)组成，记为 FECA。

模糊事件是触发 FECA 规则的事件，其发生的确切性程度是模糊的。模糊事件既包括普适计算环境中的事件，如“用户进入智能教室”、“智能教室的灯光变暗”等，又包括系统对环境的反馈事件，如“授予用户使用打印机的权限”、“FECA 规则发生改变”、“用户的授权数据库发生改变”等。模糊条件就是对当前系统状态的一个查询，可以与普适环境上下文有关，如“智能教室的灯光较暗”、“智能教室有学生”等，也可以与普适计算环境上下文无关，如“用户 A 具有使用打印机的权限”等。模糊动作表示为系统的主动行为，如对用户授权、改变上下文状态、改变访问控制强度等。

定义 2 模糊事件是普适访问控制系统运行中某一特定时刻的一个对系统有意义的发生，其发生的确定性程度是模糊的。

模糊事件与传统的精确事件的主要区别在于，模糊事件发生的确定性程度是模糊的、不能精确判断的，而传统的精确事件的发生是确切的，要么发生，要么不发生，没有第三种状态。由于模糊事件的特殊性，它的发生有一个发生的程度趋向，称之为发生度。模糊事件体现了知识的不确定性，比如有状态：“智能教室的温度为 30℃”，这意味着忽略了 29℃、29.5℃和 30.2℃等情况，而这些数值在实际应用中也是有用的。如果将上述状态用“当智能教室的温度 30℃附近时”这一个模糊事件来表达，那么模糊事件变成了一个模糊集，可以用一定的隶属函数描述。因此对于上述模糊事件，如果给定一个温度，则按照隶属函数将其模糊化，就可以确定其隶属度，从而表示该模糊事件发生的程度。

定义 3 模糊条件是普适访问控制系统运行中某一特定时刻的一个系统状态的有限描述，其满足的确定性程度是模糊的。

模糊条件可以描述普适系统中模糊的上下文，一般用一阶模糊谓词表示。模糊谓词的区间值隶属度表示模糊条件的满足程度，比如有模糊条件：“智能教室的温度在 30℃附近”的隶属度为[0.6,0.8]。隶属度[0.6,0.8]表示该模糊条件被满足的程度。

普适计算环境下，根据 FECA 规则所描述的安全策略的不同侧重点，模糊事件和模糊条件有时可以互相转化。比如一阶模糊谓词“智能教室有人时”，在一个 FECA 规则中，它被定义为模糊事件(即“有人进入之智能教室”)，当该模糊事件发生时，触发该规则；而在另一个 FECA 规则中，它被定义为模糊条件(即“有人在智能教室内”)，若该规则被触发，那么

系统需要判断规则的模糊条件“有人在智能教室内”的满足程度，并根据其满足程度决定是否执行该规则的模糊动作。

定义 4 模糊动作是在普适访问控制系统运行中的一个系统的主动行为，其执行过程所涉及的操作对象具有模糊性。

FECA 规则的模糊动作与传统 ECA 规则的动作既有共同点，也有不同点。其共同点是：两者的执行过程均具有确定性和原子性，模糊动作要么执行，要么不执行；模糊动作所涉及的数据操作要么全部执行，要么全部不执行。其不同之处在于：模糊动作具有模糊性，其模糊性一般体现为模糊动作所涉及的数据对象的模糊性。比如模糊动作：“对接近智能教室的用户发出该智能教室正在进行考试的消息”，其中限定模糊动作所涉及的用户范围的谓词“接近智能教室”具有模糊性，用区间值隶属度表示。当模糊条件成立的确定性程度大于规则的执行阈值时，规则将对所有“接近”程度在所规定的隶属度范围内的用户发出“智能教室正在进行考试”的消息。再比如模糊动作：“授权用户使用打印机”，其中用户享有使用打印机的权限的程度可以是模糊的，用区间值隶属度表示。当模糊条件成立的确定性程度大于规则的执行阈值时，授权用户使用打印机，用户享有使用打印机的程度用区间值隶属度表示。模糊动作的执行过程可能产生新的模糊事件或者改变某些模糊条件成立的确定性程度。

在普适访问控制中，模糊动作通常有 3 种类型：对用户进行模糊授权、对访问控制强度进行模糊调整和对环境上下文状态进行改变。

定义 5 FECA 规则的结构模式如式(1)所示。

$$\begin{aligned} r,\lambda:&\text{WHEN } (E,[x^-,x^+]),\theta \\ &\text{IF } (P_1,[y_1^-,y_1^+],w_1)\wedge(P_2,[y_2^-,y_2^+],w_2)\wedge \\ &\quad\cdots\wedge(P_n,[y_n^-,y_n^+],w_n),\mu \\ &\text{THEN } (A,[z^-,z^+]) \end{aligned} \tag{1}$$

式中，r 是 FECA 规则标识；λ 是规则 r 的可信度，其中 $0\leqslant\lambda\leqslant 1$，表明规则 r 的推理结果的可靠性程度；符号“WHEN”含义是“一旦、当”；E 表示规则 r 的模糊事件，其隶属度用区间值 $[x^-,x^+]$ 表示，含义是模糊事件 E 发生的确定性程度，其中用户发出的资源访问请求是模糊事件集合中的一种确定性事件，其隶属度用区间值 $[1,1]$ 表示；θ 表示规则 r 的触发阈值 $(0.5\leqslant\theta\leqslant 1)$，当实际发生的模糊事件 E' 与规则 r 定义的模糊事件 E 之间的匹配度 θ' 大于预先定义的触发阈值 θ 时，触发规则 r，否则不触发规则 r；符号“IF”含义是“如果”；$P=(P_1,[y_1^-,y_1^+],w_1)\wedge(P_2,[y_2^-,y_2^+],w_2)\wedge\cdots\wedge(P_n,[y_n^-,y_n^+],w_n)$ 表示规则条件，其中的每一个子条件用模糊谓词表示；第 $i(1\leqslant i\leqslant n)$ 个模糊谓词 P_i 表示规则 r 的第 i 个子条件，其区间值隶属度 $[y_i^-,y_i^+]$ 表示 P_i 所代表子条件的满足程度；$w_i(0\leqslant w_i\leqslant 1)$ 表示 P_i 在规则条件 P 中的权重，表明该模糊谓词在模糊推理过程中对推理结果的影响程度，权重越大，对推理结果的影响越大，并且 $w_1+\cdots+w_n=1$；符号“$\wedge$”的含义是逻辑“与”，表示规则条件 P 中的所有子条件必须得到满足；μ 表示规则 r 的激活阈值 $(0.5\leqslant\mu\leqslant 1)$，用来刻画规则条件能激活规则 r 的最小满足程度，如果上下文与规则条件的匹配度大于激活阈值，那么该规则被激活，否则不被激活；符号“THEN”的含义是“那么”；模糊动作 A 是规则条件 P 得到模糊满足时所要执行的动作，其区间值隶属度 $[z^-,z^+]$ 表示该推理结果为真的程度。

例如，一条 FECA 规则如式(2)所示：

$$\begin{aligned} &rule_1,0.6;\text{WHEN Enter}(u,\text{conference.location}),0.8 \\ &\text{IF IsIdle}(\text{projector}),[0.8,1.0],0.7 \\ &\text{THEN (Grant}(u,\text{projector,use}),[0.8,0.9]) \end{aligned} \tag{2}$$

式中，$rule_1$ 是规则标识；$\lambda=0.6$ 是规则 $rule_1$ 的可信度；二元谓词 Enter(u, conference. location)是模糊事件，表示用户 u 进入智能教室(conference. location)；该规则的触发阈值 $\theta=0.8$；一元谓词 IsIdle(projector)是模糊条件，表示投影仪(projector)是空闲的，其隶属度规定为$[0.8,1.0]$；该规则的激活阈值 $\mu=0.7$；三元谓词 Grant(u, projector, use)是模糊动作，表示授权用户 u 使用(use)投影仪(projector)，该模糊动作的隶属度规定为$[0.8,0.9]$。FECA 规则 $rule_1$ 的语义是，如果一名用户 u 进入了智能教室(conference. location)，并且系统所判断的用户进入的程度大于规则的触发阈值，则该规则被触发，立即评估模糊条件 IsIdle(projector)，如果其满足程度大于激活阈值，规则被激活，即执行规则所定义的模糊动作 Grant(u, projector, use)，授予用户 u 使用投影仪的权限。

一般地，FECA 规则的执行过程描述如下：当规则定义的模糊事件发生，且该模糊事件的发生度大于规则的触发阈值时，触发 FECA 规则；然后评估规则的模糊条件，如果规则的模糊条件被满足的程度(当前上下文与规则条件中的模糊谓词的匹配度)大于规则所预定义的激活阈值，那么规则被激活；最后执行规则的模糊动作。基于主动触发机制，通过引入 FECA 规则模式，普适访问控制可以实现对用户的主动授权，调整访问控制强度和改变上下文状态。

3 基于 FECA 规则的访问控制方法

FECA 规则既可以有效描述主动性的知识，又可以有效描述模糊不确定的知识。普适环境下，访问控制系统实时监控访问控制相关的模糊事件，当模糊事件发生时，触发相应规则，并查找规则相关的上下文并依据所查找的上下文评估所触发规则的条件是否满足，从模糊的、不完备的上下文中推导出可靠的授权结论和访问控制结论；然后主动实施规则所预定义的模糊动作，从而实现对用户的主动授权和对用户使用权限的过程进行主动自适应控制。

根据规则执行过程的不同，FECA 规则可划分为可挂起规则和不可挂起规则。可挂起规则是指当模糊事件触发该规则时，如果当前上下文不能满足规则条件，该规则将进入挂起状态；当上下文发生改变并满足规则条件时，该规则将被重新执行。不可挂起规则是指被触发规则的模糊条件如果不满足，那么立即结束该规则的后续操作，将不再执行该规则的模糊动作，并删除该规则实例。

图 1 是 FECA 规则执行过程的状态转换图。一条 FECA 规则最初处于休眠状态。当模糊事件发生时，如果模糊事件的发生度大于规则的触发阈值，则规则进入触发状态，否则继续处于休眠状态。处于触发状态的规则，如果当前上下文满足规则条件(即当前上下文与模糊条件的匹配度大于规则激活阈值)，则规则进入激活状态，否则根据规则的类型进行不同的处理。挂起规则进入挂起状态，不可挂起规则实例被删除。进入挂起状态的规则，当规则条件得到满足时，将重新进

入激活状态。进入激活状态的规则，随后被调度执行，并进入执行状态。模糊动作执行完毕，规则又将重新进入休眠状态。

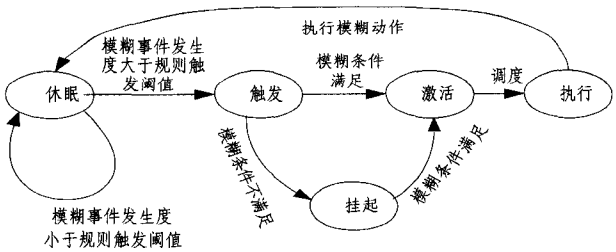

图 1　FECA 规则的状态转换图

图 2 是 FECA 规则的执行过程，其主要步骤如下。

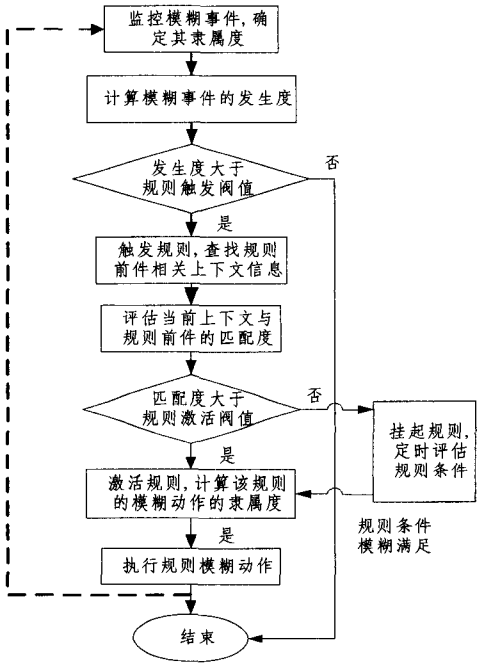

图 2　FECA 规则执行过程

Step 1　系统监控着所有与 FECA 规则相关的模糊事件，当模糊事件发生时，确定其隶属度，其中用户主动发出的资源访问请求是模糊事件中的确定性事件，其隶属度为[1,1]；

Step 2　系统计算已发生的模糊事件的发生度；

Step 3　系统判断发生度是否大于 FECA 规则的触发阈值；

Step 4　如果是，则触发该 FECA 规则，并并查找与之相关的上下文，否则结束；

Step 5　系统评估已查找到的上下文与已触发规则条件的匹配度；

Step 6　系统判断匹配度是否大于已触发规则的激活阈值；

Step 7　如果是，则激活该规则，计算其推理结果；如果不是，则挂起可挂起规则实例，删除不可挂起规则实例；

Step 8　执行已激活规则所定义的模糊动作；

Step 9　结束。

在上述过程中，如果规则模糊动作产生新的模糊事件，并被系统所监测，则重新进入步骤 1。当模糊条件满足，处于挂起状态的规则将被重新激活，再次计算该规则的推理结果，进入步骤 8。

普适访问控制系统根据用户的模糊权限是否大于资源访问控制强度，得出用户可以访问的所有资源列表，并在用户发出资源访问请求之前对用户进行授权。因此，依据 FECA 规则的主动触发机制，普适访问控制系统根据上下文动态调整用户的权限，实现了对用户的透明授权。另一方面，模糊事件的发生可能导致用户的模糊权限或者资源访问控制强度发生变化，因此，系统不断监控用户使用权限的过程，并在用户的模糊权限或访问控制强度发生变化时重新评估用户的模糊权限。在用户的模糊权限小于资源访问控制强度时，禁止用户继续使用该资源，从而实现对用户和资源的主动控制。

FECA 规则的执行过程中，当前上下文与 FECA 规则的模糊条件的匹配度计算属于区间值模糊推理[26,27]的范畴。为了提高区间值模糊推理效率，以适应能量受限的普适计算网络，在传统区间值模糊推理的基础上，本文提出了一种简单高效的计算方法。

(1) 模糊事件 E' 的发生度计算方法。

已知：E' 的隶属度是 $([x^-,x^+])$。

求：E' 的发生度，其计算公式为：

$$N(E')=(x^-+x^+)/2 \tag{3}$$

(2) 当前模糊上下文 P' 与 FECA 规则模糊条件 P 的匹配度计算方法。

已知：P 中各个原子模糊谓词的隶属度和权重分别依次是：$([x_1^-,x_1^+],w_1),([x_2^-,x_2^+],w_2),\cdots,([x_n^-,x_n^+],w_n)$。

给定：P' 中各个原子模糊谓词的隶属度分别是：$[y_1^-,y_1^+],[y_2^-,y_2^+],\cdots,[y_n^-,y_n^+]$。

求：P' 与 P 的匹配度。

首先，对于任意两个区间值隶属度 x、y，其中 $x=[x^-,x^+]$，$y=[y^-,y^+]$，y 相对于 x 的相似度 $S(y,x)$ 定义为：

$$S(y,x)=\begin{cases}(x^+-y^-)/(y^+-x^-), & x^-\leqslant y^-<x^+<y^+\\ (y^+-x^-)/(x^+-y^-), & y^-<x^-<y^+\leqslant x^+\\ 1, & x^-\leqslant y^-\leqslant y^+\leqslant x^+\\ 0, & \text{otherwise}\end{cases} \tag{4}$$

由式(4)可知，如果区间值 x 与区间值 y 相等，那么 $S(y,x)=1$；如果区间值 x 与区间值 y 不相交，那么 $S(y,x)=0$；x 与 y 相交的部分越多，那么它们之间的相似度越大。模糊上下文 P' 与模糊条件 P 的匹配度的计算公式如下：

$$M(P',P)=S([y_1^-,y_1^+],[x_1^-,x_1^+])*w_1+S([y_2^-,y_2^+],[x_2^-,x_2^+])*w_2+\cdots+S([y_n^-,y_n^+],[x_n^-,x_n^+])*w_n \tag{5}$$

如果已发生的模糊事件的发生度大于规则的触发阈值，且上下文与 FECA 规则的条件的匹配度大于规则的激活阈值，则主动执行 FECA 规则的模糊动作。FECA 规则的模糊动作有以下两种不同的区间值隶属度类型。

(1) 固定值

执行模糊动作时，所涉及的模糊动作的隶属度就是规则所定义的隶属度，比如模糊动作：

SendMessage(u,near(*patient*),"patient is in danger."),[0.8,1.0]

其含义是，向接近病人(*patient*)的程度在[0.8,1.0]范围内所有用户 u 发送消息"patient is in danger"。

(2) 动态值

模糊动作被执行时，其模糊动作的隶属度会根据模糊条件的评价结果和模糊动作所预定义的隶属度计算得出，其计算公式如下所述：

$$m=[M(P',P)\cdot z^{-},M(P',P)\cdot z^{+}] \quad (6)$$

式中，m 是最终所要执行的模糊动作的隶属度，$M(P',P)$ 是上下文 P' 与规则条件 P 的匹配度，$[z^{-},z^{+}]$ 表示该规则预定义的模糊动作的隶属度。

本文提出的模糊条件匹配度算法具有如下特点：(1) 算法效率较高，时间复杂度为线性复杂度 $O(n)$，其中 n 为 FECA 规则所含模糊条件谓词的个数，适合能量受限的普适网络；(2) 与其隶属度函数相比，上下文信息的区间值隶属度更易确定；(3) 算法具有还原性，即当匹配事实的区间值隶属度与模糊规则的前件的区间值隶属度分别对应相等时，规则前件与匹配的事实的匹配度为 1，推理结果还原为 z；(4) 通过为规则的每个前件设置影响因子，来区别不同上下文信息对系统安全强度的影响。

4 普适场景实例

本文通过一个典型的普适环境实例对基于 FECA 规则的主动访问控制方法的应用予以说明。

智能教室(classroom)内安置了一台空调、一台打印机(prt_1)、一台温度检测仪(用于监控温度变化)和若干摄像头(用于监控智能教室的人员进出情况)。访问控制需求如下所述：

当一名教师在智能教室内且智能教室的温度适宜时，该教师可以在较高程度上使用打印机 prt_1。当智能教室内的温度下降且智能教室内的温度较高时，降低 prt_1 的资源访问控制强度。当用户离开智能教室，智能教室的温度较高，并且温度继续升高时，则用户在很低程度上使用 prt_1。用户能否使用打印机 prt_1 取决于用户所拥有的使用打印机 prt_1 的程度与打印机 prt_1 的资源访问控制强度的大小关系，如果用户所拥有的使用打印机 prt_1 的程度大于打印机 prt_1 的资源访问控制强度，则用户可以使用打印机 prt_1；否则，用户不能使用打印机 prt_1。

依据上述访问控制需求和专家经验，安全管理员建立了如下 3 条 FECA 规则：

$rule_1$,0.8:WHEN (Enter(user,classroom),0.6
IF ((IsMember(user,teacher),[0.9,1],0.6) ∧ (IsSuitable (classroom),[0.7,0.9],0.4)),0.9
THEN (CanUse(user,prt_1),[0.5,0.8])

$rule_2$,0.9:WHEN (DownTemp(classroom)),0.8
IF (IsHigh(classroom),[0.7,0.9],1.0),0.8
THEN (DownTheshold(prt_1),[0.3,0.4])

$rule_3$,0.7:WHEN (Leave(user,classroom) ∧ UpTemp(classroom)),0.5
IF (IsHigh(classroom),[0.2,0.3],1.0),0.8
THEN (CanUse(user,prt_1),[0.2,0.3])

一个具体的主动访问控制过程如下所述：

当用户 John 进入智能教室时，系统监控到模糊事件 Enter(John,classroom)发生，确定其隶属度为[1,1]。系统检索 FECA 规则库，找到模糊事件 Enter(John,classroom)可以触发的 FECA 规则 $rule_1$。采用发生度计算式(3)，可得其发生度为 1，大于规则 $rule_1$ 的触发阈值 0.6，规则 $rule_1$ 被触发。根据规则 $rule_1$ 的模糊条件 IsMember(user,teacher),[0.9,1],0.6) ∧ (IsSuitable (classroom),[0.7,0.9],0.4)，系统查询当前上下文即模糊谓词 IsMember(John,teacher)和 IsSuitable(classroom)的区间值隶属度，分别设为[1,1]和[0.6,0.8]。将已查找到的模糊谓词的区间值隶属度代入式(5)计算得到实际的模糊上下文与已触发规则的预定义的模糊条件的匹配度为：

$$N(P',P)=S([1,1],[0.9,1])*0.6+S([0.6,0.8],[0.7,0.9])*0.4=0.93$$

系统比较该匹配度 0.93 与该规则 $rule_1$ 的激活阈值 0.9 的大小关系，匹配度大于规则的激活阈值，因此，规则 $rule_1$ 被激活。假设规则 $rule_1$ 的模糊动作的隶属度是动态值，那么主动模糊规则执行器按式(6)计算已激活规则 $rule_1$ 的模糊动作的隶属度为：

$$m=[0.93*0.5,0.93*0.8]=[0.47,0.74]$$

根据计算的模糊动作的隶属度，系统主动执行规则 $rule_1$ 的访问控制模糊动作 CanUse(John,prt_1)，使得用户 John 享有使用打印机 prt_1 的权限的程度为(0.47+0.74)/2=0.6。

如果 John 此时提出使用打印机的请求，用户资源请求事件发生，系统判断 John 享有使用打印机 prt_1 的权限的程度是否大于 prt_1 的资源访问控制强度。假设打印机 prt_1 的当前资源访问控制强度为 0.55。由于 John 享有使用打印机 prt_1 的权限的程度 0.6 大于打印机当前的安全保护强度 0.55，则建立 John 与打印机的安全连接，即允许 John 使用打印机。

如果 John 离开智能教室时智能教室的温度升高，就会触发 Leave(John,classroom)和 UpTemp(classroom)模糊事件，将导致触发规则 $rule_3$，如果规则的条件被满足，系统将降低 John 享有使用打印机的资源访问控制强度。

在用户 John 使用打印机的过程中，当模糊上下文的变化使得 John 的模糊权限小于打印机的资源访问控制强度时，系统将断开 John 与打印机的安全连接，即拒绝 John 继续使用打印机。

结束语 普适访问控制具有主动性、模糊不确定性和动态自适应性。本文基于区间值模糊集合理论对传统 ECA 规则进行模糊扩展，设计了一种 FECA 规则模式，并提出了一种主动访问控制方法。FECA 规则模式可以在访问控制策略规则层面有效地刻画普适访问控制策略的模糊主动性和不确定性，实现访问控制策略对实际安全需求的无缝表达。与传统访问控制理论和技术相比，本文提出的基于 FECA 规则的主动访问控制方法可以较好地达到用户随时随地、透明地获得数字化服务的目标，使其更适合于普适计算环境。基于事件触发机制，FECA 规则的主动执行可以动态调整系统行为，改变资源安全强度，进行主动授权和主动访问控制。FECA 规则库中可以包含不同专家制定的规则，区间值模糊推理理论可以充分利用不同安全专家的知识，增加了普适访问控制的灵活性。另一方面，FECA 规则的触发阈值和激活阈值需要专家人为设定，导致普适访问控制的自适应性稍差，因此

FECA 规则的阈值自适应学习机制是进一步的研究工作。本文的后续工作主要是对普适访问控制的 FECA 规则的执行模型进行探讨，并分析和研究 FECA 规则集的静态结构特性和动态行为特性(如一致性、可终止性)以及 FECA 规则的阈值自适应学习机制。

参 考 文 献

[1] Weiser M. The computer for the twenty-first century[J]. Scientific American, 1991, 265(3): 94-104

[2] Weiser M. Hot topics-ubiquitous computing[J]. IEEE Computer, 1993, 26(10): 71-72

[3] 徐光祐，史元春，谢伟凯. 普适计算[J]. 计算机学报，2003，26(9)：1042-1050

[4] Hilary H. Security is fuzzy: applying the fuzzy logic paradigm to the multi-policy paradigm[C]// Proceedings of the ACM Workshop on New security Paradigms. New York: ACM, 1993: 175-184

[5] Chang E, Thomson P, Dillon T, et al. The fuzzy and dynamic nature of trust[J]. Lecture Notes in Computer Science, 2005, 3592: 161-174

[6] 李小勇，桂小林. 大规模分布式环境下动态信任模型研究[J]. 软件学报，2007，18(6)：1510-1521

[7] Ishikawa H, Kubota K. An active object-oriented database: a multi-paradigm approach to constraint management[C]// proceedings of 19th VLDB, 1993. 1993: 467-478

[8] Gehani N, Jagadish H, Smueli O. Event specification in an active object-oriented database[C]// Proceedings of the ACM-SIGMOD International Conference on Management of Data, 1992. CA: ACM, 1992: 81-90

[9] 李凤华，苏铓，史国振，等. 访问控制模型研究进展及发展趋势[J]. 电子学报，2012，40(4)：805-813

[10] 魏志强，康密军，贾东宁，等. 普适计算隐私保护策略研究[J]. 计算机学报，2010，33(1)：128-138

[11] 林莉，怀进鹏，李先贤. 基于属性的访问控制策略合成代数[J]. 软件学报，2009，20(2)：403-414

[12] 盖新貌，沈昌祥，刘毅，等. 基于属性访问控制的 CSP 模型[J]. 小型微型计算机系统，2011，32(11)：2217-2222

[13] 王小明，付红，张立臣. 基于属性的访问控制研究进展[J]. 电子学报，2010，38(7)：1660-1667

[14] 崔永泉，洪帆，龙涛，等. 基于使用控制和上下文的动态网格访问控制模型研究[J]. 计算机科学，2008，35(2)：37-41

[15] 蒲芳，姜涛，曹奇英. 普适计算的上下文访问控制模型[J]. 计算机应用研究，2009，26(1)：317-320

[16] 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

[17] 王小明. 面向普适计算的区间值模糊访问控制[J]. 计算机科学与探索，2010，4(10)：865-880

[18] 邓勇，张琳，王汝传，等. 网格计算中基于信任度的动态角色访问控制的研究[J]. 计算机科学，2010，37(1)：51-54

[19] 徐文拴，辛运帏，卢桂章，等. 普适计算环境下信任管理模型的研究[J]. 计算机科学，2009，36(2)：103-106，133

[20] 董理君，余胜生，杜敏，等. 一种基于环境安全的角色访问控制模型研究[J]. 计算机科学，2009，36(1)：51-54，59

[21] 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

[22] 翟浩良，韩道军，李磊. 基于情景演算的动态访问控制模型[J]. 计算机科学，2012，39(6)：35-39

[23] 吴新松，贺也平，周洲仪，等. 一个环境适应的基于角色的访问控制模型[J]. 计算机研究与发展，2011，48(6)：983-990

[24] 贺春林，滕云，彭仁明. 一种基于 ECA 规则的 Web Service 工作流模型的研究[J]. 计算机科学，2009，36(8)：112-115

[25] 熊伟，吴烨，张震，等. 基于触发路径的主动规则集终止性分析[J]. 计算机学报，2012，35(1)：65-75

[26] 曾文艺，于福生，李洪兴. 区间值模糊推理[J]. 模糊系统与数学，2007，21(1)：68-74

[27] 王国俊. 三 I 方法与区间值模糊推理[J]. 中国科学(E 辑)，2000，30(4)：331-340

(上接第 64 页)

[5] Dan A, Shahabuddin P, Sitaram D. Scheduling policies for an on-demand video server with batching[C]// Proc of ACM Multimedia. New York: ACM press, 1994: 168-179

[6] Hua K, Cai Y, Sheu S. Patching: A multicast technique for true video-on-demand services [C]// Proc of ACM Multimedia. New York: ACM press, 1998: 12-16

[7] Carter S W, Long D E. Stream Tapping: a System for Improving Efficiency on a Video-on-Demand Server [R]. UCSC-CRL-97-11. Univ. of California, Santa Cruz: November 1997

[8] Viswanathan S, Imielinske T. Metropolitan area video-on-de - mand service using Pyramid Broadcasting [J]. IEEE Multimedia Systems, 1996, 51(4): 197-208

[9] Ernst-Desmulier J B, Charlet D, Chatonnay P, et al. A Peer to Peer approach for cache sibling[C]// First International Conference on Distributed Framework s for Multimedia Applications. Besancon, France, 2005: 323-330

[10] Lee G J, Cho i C K, Chi C Y, et al. P2Proxy: Peer to Peer proxy caching scheme for VOD service[C]// Sixth International Conference on Computational Intelligence and Multimedia Applications. 2005: 272-277

[11] 杨静，李润知，王宗敏. 基于时间间隔的 P2P 流媒体直播系统缓存算法[J]. 计算机工程与设计，2010，31(1)：90-93

[12] 胡懋智，徐恪，夏树涛，等. TOW：一种新的 P2P 实时流媒体缓存替换算法[J]. 小型微型计算机系统，2009，30(8)：1484-1489

[13] Cherkasova L, Gupta M. Analysis of enterprise media server workloads: access patterns, locality, dynamics, and rate of change [EB/OL]. http://www.hpl.hp.com/techreports/2002/HPL-2002-56.html, 2002-03-26

[14] 王晓东. 算法设计与分析[M]. 北京：清华大学出版社，2003：114-116

[15] Wang B, Sen S, Adler M, et al. Optimal proxy cache allocation for efficient streaming media distribution [J]. IEEE Transactions on Multimedia, 2004, 6(2): 366-374

[16] 覃少华，李子木，蔡青松，等. 基于代理缓存的流媒体动态调度算法研究[J]. 计算机学报，2005，28(2)：185-194