一种管理增强的RBAC模型*)

A Management-Enhanced Model for RBAC

姚立红　李振东　谢　立

(南京大学软件新技术国家重点实验室　南京大学计算机科学与技术系　南京210093)

Abstract The manner of permission management in Role-Based Access Control is similar to the actual one in application fields, and it greatly simplifies system management. How to define and manage hundreds of permissions, roles, users and relations among them (all are called RBAC special framework in this article)in large systems is one key problem that models for RBAC must resolve. This article studies the management of RBAC special frameworks, takes the management relations among roles into frameworks, and puts forward Management-Enhanced Model for RBAC. Special frameworks created according to this model are very similar to the management structures in application fields, and can manage themselves. This model also supports dynamic maintenance of management formwork while it is working.

Keywords Information security, Role-based access control, Inherited permissions, Hierarchy relations of management

1 引言

基于角色的访问控制RBAC(Role-Based Access Control)[1,2]是近年来兴起的新型访问控制技术,它的基本思想是在用户与权限之间引入了角色的概念,利用角色来实现用户和权限的逻辑隔离,即用户与角色相关联,角色与权限相关联,用户通过成为相应角色的成员而获得相应权限。

RBAC这种以角色为中介的权限管理模式同应用领域中的权限管理方式非常类似,简化了系统的权限管理,受到广泛的重视,出现了很多描述RBAC技术的理论模型,如Ferraiolo的RBAC模型[3]、Sandhu等人的RBAC96模型[4]、Nyanchama的角色图模型[5]等。同时,RBAC技术逐渐应用于实际系统,如Novell的Netware和Windows NT等操作系统的系统管理[4]、Intranet管理[6]和Web服务器管理[7]等。

上述模型重点研究了如何以角色为中介简化安全管理,很少考虑角色的管理问题,默认由管理员集中管理所有的角色。在组织结构简单、角色数量较少的情况下,如上述提到的几种应用实例,集中式管理比较有效,但在涉及到众多角色的大系统中,如何根据特定安全策略的需求定义和管理这些成百上千的权限、角色、用户及它们之间的关系(本文把特定应用中所有权限、角色、用户及它们之间关联的总和称为RBAC实例框架,简称框架)就成为RBAC模型重点需要解决的问题。尽管Sandhu等人提出的ARBAC97模型[8]能够在一定程度上实现分布式框架管理,但存在管理层次差、安全策略的作用范围不明确、动态维护能力差等缺点,难以真正解决RBAC框架的管理问题。

本文研究了应用领域的权限管理方式,把管理关系引入到角色层次关系中,提出了一种管理增强RBAC模型(Management-Enhanced RBAC,ME_RBAC),该模型完全模拟现实生活中的权限管理方式,支持对RBAC框架自身的管理和框架运行过程中的局部动态调整,同时安全策略的层次性在该模型中也得到充分体现。

2 ME_RBAC模型

2.1 模型的原理与概述

把角色对应于工作职位是RBAC应用于实际信息系统时最常见的理解,如图1。现实生活中很多职位包含两种性质不同的工作职能:具体业务处理职能和管理职能,不同的职能对应不同性质的权限,如图2,例如部门经理的职位既拥有某些业务的处理权,也拥有对部门内部其它职位的管理权。职位对应的这两种职能(业务处理职能和管理职能)及权限(业务处理权限和管理权限)分属不同的范畴,难以组织在一起。ME_RBAC模型把工作职位的具体职能作为构造角色的原型,并通过区分不同类型的角色和权限来进一步模拟应用领域中的权限组织方式。图3给出了ME_RBAC模型的基本元素及其相互关系。

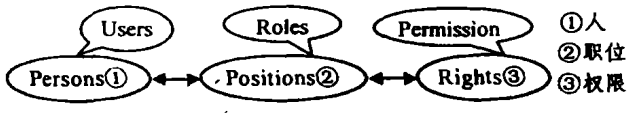


图1　一般RBAC的应用原型

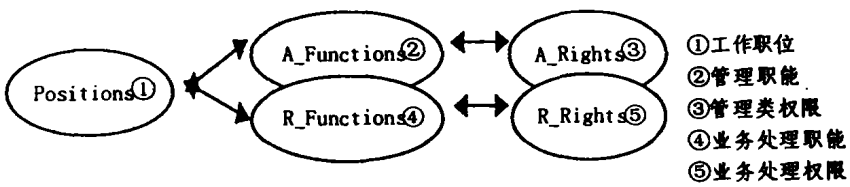


图2　职位与权限的实际关系

*)本课题得到国家"863"资助(NO:863-301-6-4)。姚立红　博士生,研究方向:信息安全。李振东　博士生,研究方向:信息系统安全、网络安全。谢　立　教授,博士生导师,研究方向:分布式操作系统、安全操作系统。

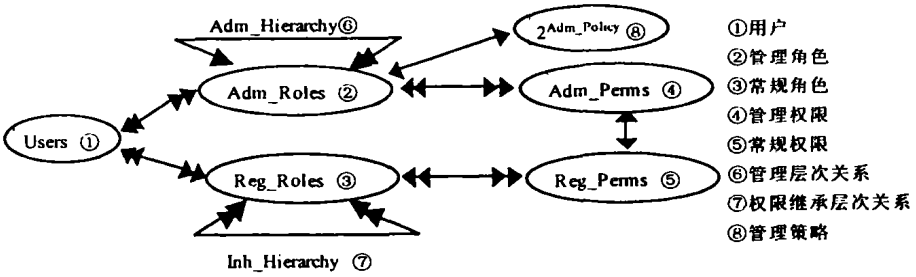


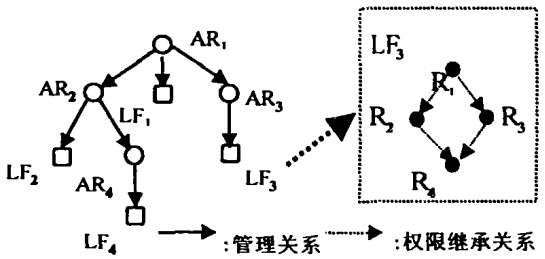
图3 ME_RBAC模型实体要素及其关系

2.1.1 *两种权限和两种角色* Reg_Perms(常规权限)对应一般的资源访问权限,Adm_Perms(管理权限)对应一般资源访问进行授权的权限。Reg_Roles(常规角色)与Reg_Perms相关联,Adm_Roles(管理角色)与Adm_Perms相关联。

2.1.2 *两种角色层次关系* Inh_Hierarchy(权限继承层次关系),即高级常规角色继承低级常规角色的权限。常规角色按照权限继承关系组织成一定层次结构,权限继承的动因和作用参见文[9~11]。

Adm_Hierarchy(管理层次关系),即高级管理角色全权管理低级管理角色。管理角色按照管理关系组织成一定层次结构。

管理关系体现了自顶向下的权限逐步细化、管理逐步具体的思想,权限继承体现自底向上的权限聚集的思想。ME_RBAC模型综合了这两种思想,在全局上通过管理层次关系来组织RBAC框架,以反映管理逐渐细化的过程;针对到某个局部,单个管理员(或管理角色)清楚所有权限管理细节,用权限继承关系表示角色层次关系,如图4。



AR:管理角色 R: 常规角色 LF:局部框架

图4 两种角色层次关系

为保证管理一致性,ME_RBAC模型约定每个管理角色或常规角色只存在一个管理角色对它直接管理(下文称该角色为直接管理角色),对应用领域中多管理者的情况,通过将该直接管理角色指派给多个用户来解决。

由于隶属于不同的直接管理角色,常规角色被划分为多个子集,每个子集内的常规角色及其相关的授权称为局部框架,对应于最基本的子部门的组织结构。(注:常规角色划分到不同局部框架中,并不表示用户也被划分到不同的局部框架中,同一用户可以同时在多个常规局部框架中承担角色。)

2.1.3 *管理权限描述和安全管理策略* ME_RBAC模型简化了Adm_Perms(管理权限)的表示,每种常规权限rp对应一种管理权限ap,ap表示扩散权限rp的许可,隐含了与rp授权相关的所有管理权限。

与ARBAC97模型[8]相比,ME_RBAC模型管理权限的简化表示更能体现管理角色开展管理工作的自主性和独立性。此外,为了高级管理角色从宏观上对低级管理角色的管理行为进行指导和约束,ME_RBAC模型给管理角色配置一定的安全管理策略(Adm_Policy),管理角色在行使管理权限时必须遵守相应的安全管理策略。

2.2 ME_RBAC模型的形式化描述

2.2.1 基本实体元素

定义1(用户) 用户是指能够独立访问信息系统中各种资源的主体,用USERS表示所有用户的集合。

定义2(常规权限、常规权限集) 常规权限是对特定应用环境下的资源进行特定操作的许可,用REG_PERMS表示常规权限的集合。

对包含授权信息的资源进行操作可能涉及到系统授权管理,常规权限不包括对这些资源进行操作的许可。

定义3(管理权限,管理权限集合) 管理权限是对常规权限进行直接或间接授权的许可。REG_PERMS中的每一常规权限rp都存在相应管理权限ap,记作 $ap \pm rp$。用ADM_PERMS表示所有管理权限的集合 。

定义4(常规角色、管理角色) 角色是联系用户和权限的一种语义结构,根据所联系的权限不同分为常规角色和管理角色,它们的全集分别记作REG_ROLES和ADM_ROLES。

定义5(权限管理策略) 权限管理策略是实施权限管理时的一些约定,体现应用领域的安全策略,用ADM_POLICY表示权限管理策略的集合。

访问控制的主要内容就是权限管理,在访问控制技术中,安全策略主要体现为权限的管理策略。

2.2.2 局部框架

定义6(常规权限配置RR_RP) $RR\_RP \subseteq REG\_ROLES \times REG\_PERMS$,$(rr, pp) \in$ RR_RP表示常规角色rr拥有常规权限rp。

定义7(常规角色用户指派RR_U) $RR\_U \subseteq REG\_ROLES \times USERS$,$(rr, u) \in$ RR_U表示常规角色rr指派给用户u。

定义8(常规权限继承关系RR_RR) $RR\_RR \subseteq REG\_ROLES \times REG\_ROLES$,$(rr_1, rr_2) \in RR_RR$表示常规角色$rr_2$继承$rr_1$的所有权限,$rr_2$称为$rr_1$的高级角色。

常规角色之间的权限继承关系具有传递性,常规角色除了拥有直接配置的权限外,还将拥有直接或间接继承来的权限。

定义9(局部框架集合LF) $LF \subseteq 2^{REG\_ROLES} \times 2^{RR\_RP} \times 2^{RR\_U} \times 2^{RR\_RR}$,LF中的每一个元素称为一个局部框架。对局部框架$lf(RR_{lf}, RR_RP_{lf}, RR_U_{lf}, RR_RR_{lf})$,若常规角色$rr \in RR_{lf}$,称为$rr$隶属于$lf$,记作$rr \triangleright lf$。

每个局部框架对应于应用领域中从管理上不能再细分的子部门的组织结构，这些子部门通常很小，可以由单个管理者（角色）直接实施所有的管理。

规则1（框架间角色隔离规则） $\forall rr \forall lf_1 \forall lf_2(((rr \triangleright lf_1) \wedge (rr \triangleright lf_2)) \rightarrow (lf_1 = lf_2))$

规则2（局部框架的一致性规则） 对 $lf(RR_{lf}, RR\_RP_{lf}, RR\_U_{lf}, RR\_RR_{lf}) \in LF$，$\forall rr((((rr, rp) \in RR\_RP_{lf}) \vee ((rr, u) \in RR\_U_{lf}))) \rightarrow (rr \in RR_{lf})) \wedge \forall rr_1 \forall rr_2(((rr_1, rr_2) \in RR\_RR_{lf}) \rightarrow ((rr_1 \in RR_{lf}) \wedge (rr_2 \in RR_{lf})))$。

规则1和规则2表明每个常规角色只能隶属于一个局部框架，每个局部框架中权限配置、用户指派只涉及隶属于它的常规角色。这两个规则保证局部框架作为基本管理单元的独立性。

2.2.3 管理层次关系

定义10（管理权限配置 AR_AP） $AR\_AP \subseteq ADM\_ROLES \times ADM\_PERMS$，$(ar, \cdot ap) \in AR\_AP$ 表示管理角色 ar 拥有管理权限 ap。令 AP_{ar} 表示针对 ar 所配置的管理权限集合。

定义11（管理策略配置 AR_MP） $AR\_MP \subseteq ADM\_ROLES \times 2^{ADM\_POLICY}$，$(ar, mp)$ 表示 ar 实行配置给它的管理权限必须符合 mp 中所有管理策略的约束。令 MP_{ar} 表示针对 ar 所配置的管理策略集合。

定义12（管理角色用户指派 AR_U） $AR\_U \subseteq ADM\_ROLES \times USERS$，$(ar, u) \in$ AR_U 表示管理角色 ar 指派给用户 u。令 U_{ar} 表示 ar 指派用户集合。

管理角色指派给某个用户，该用户就拥有为管理角色配置的管理权限，但是该用户在行使这些管理权限时必须满足该管理角色相应的管理策略，RBAC 技术中常见的安全策略如互斥角色、前提角色、前提权限[12]等都可以用 ME_RBAC 模型的管理策略来表示。

定义13（管理层次关系 AH） $AH \subseteq ADM\_ROLES \times (ADM\_ROLES \cup FL)$，$(ar, X) \in AH$ 表示角色 ar 管理 X（X 为低级管理角色或局部框架），ar 称为 X 的直接（高级）管理角色，记作 $ar \succ X$。若存在 $ar_1, \cdots, X$ 满足 $ar_1 \succ \cdots \succ X$，则称 ar_1 为 X 的（高级）管理角色，记作 $ar_1 \succ * X$。

管理层次关系是 ME_RBAC 模型的特色，管理层次关系除表示上下层的管理关系外，还隐含管理策略的继承和权限撤销的传递。

管理角色在实施管理权限时，不但要遵照直接配置给它的管理策略，还要满足它的高级管理角色相关联的管理策略。

若高级管理角色失去了某种管理权限，那么下层管理角色将自动失去这种管理权限，同时该高级管理角色所直接或间接管理的常规局部框架中的常规角色也将自动失去这种管理权限所管理的常规权限。

规则3（独立管理规则） 对任意管理角色 ar_1、ar_2、ar_3 和任意框架 fl 满足：

$(((ar_1 \succ ar_3) \wedge (ar_2 \succ ar_3)) \vee ((ar_1 \succ fl) \wedge (ar_2 \succ fl))) \rightarrow (ar_1 = ar_2)$

该规则表明每个管理角色只能由一个直接高级管理角色、每个局部框架只能由一个直接管理角色。独立管理规则保证了管理的一致性。

2.2.4 授权的有效性和一致性保证

定义14（无效管理角色） 如果管理角色 ar 相关的管理违背了系统的管理策略，则称 ar 为无效管理角色，记作 $Invalid(ar)$。

推论1 正在进行创建或维护的管理角色是无效管理角色。

为了保证授权的一致性，ME_RBAC 模型把正在被维护的管理角色也视为违背了安全策略，也认为是无效管理角色。

推论2 $\exists ar_1 \exists ap((ar_1 \succ * ar) \wedge (ap \in AP_{ar}) \wedge (ap \notin AP_{ar_1})) \rightarrow Invalid(ar)$。

推论3 $\exists ar_1((ar_1 \succ * ar) \wedge \neg MP_{ar_1}(AP_{ar}, U_{ar})) \rightarrow Invalid(ar)$。

$MP_{ar_1}(AP_{ar}, U_{ar})$ 表示关于 ar 的权限配置和用户指派满足 ar_1 关联的管理策略，推论3表明，有效管理角色的权限配置和用户指派必须满足它所有的高级管理角色相应的管理策略，体现安全管理策略的继承特性。

推论4 $\exists ar_1((ar_1 \succ * ar) \wedge Invalid(ar_1)) \rightarrow Invalid(ar)$。

定义15（无效局部框架、无效常规角色） 如果局部框架 lf 自身或对它的管理违背了安全管理策略，则称 lf 为无效局部框架，记作 $Invalid(lf)$。对其中任意常规角色 rr，则称为无效常规角色，记作 $Invalid(rr)$。

同无效管理角色一样，正在进行维护的局部框架也被视为无效框架。

根据定义15，对局部框架 $lf(RR_{lf}, RR\_RP_{lf}, RR\_U_{lf}, RR\_RR_{lf})$ 存在推论5-7：

推论5 $\exists ar((ar \succ * lf) \wedge \exists rp \exists rr(((rr, rp) \in RR\_RP_{lf}) \wedge \neg(\exists ap((ap \in AP_{ar}) \wedge (ap \pm p))))) \rightarrow Invalid(lf)$

该推论表明局部框架中指派的权限不能超出它的（直接或间接）管理角色所管理的范围。

推论6 $\exists ar((ar \succ * lf) \wedge \neg MP_{ar_1}(lf)) \rightarrow Invalid(lf)$

$MP_{ar}(lf)$ 表示框架 lf 满足管理角色 ar 关联的管理策略，局部框架规模较小且管理策略可能会同时涉及到多个角色（如互斥角色），ME_RBAC 模型把整个常规局部框架作为整体判断是否满足相应的管理策略。

推论7 $\exists ar((ar \succ * lf) \wedge Invalid(ar)) \rightarrow Invalid(lf)$

推论4和推论7体现了无效管理的传递性，若一个高级管理角色是无效的，那么它直接或间接实施的各种权限指派也是无效的，这和应用领域中的情况是一致的。

规则4（局部无效规则） 在定义和维护框架的过程中，除无效角色的用户指派无效外，RBAC 框架的其它部分都能正常运行。

RBAC 的各种权限指派要发挥作用最终体现在用户利用其中定义的角色而获得相应的权限，ME_RBAC 模型并不禁止无效局部框架和无效管理角色的存在，只是禁止无效角色的用户指派发生作用。规则4体现了 ME_RBAC 模型的动态维护能力，在维护过程中，除了维护涉及到的部分外不影响框架其它部分正常运行。

3 应用实例

江苏省政府政务公文流转系统是一个大型的分布式协作办公系统（下称公文系统），它涉及到政府办公所需的各种公文、函件、通报等资源的管理。与一般信息系统的权限管理相比，该系统据具有显著的特点：

（1）资源访问（在本系统中指公文办理等）授权无法一步到位，且过程非常复杂。如省政府收到一个公文，根据公文的

性质和管理规定交给某厅级部门，厅级部门再按规定转给相应的处级部门，直到最基层部门的管理者指派某公务员办理，办理之后还要逐层上缴、复批等，这一系列的公文流转过程在计算机信息系统中对应复杂的资源(即公文)访问授权和撤权过程。

(2)复杂的授权过程贯穿系统运行的始终。公文不断产生、作废，复杂的授权和撤销权限随时都在进行，而且公文的流转过程还会随政府管理策略的改变而变化。这对应到RBAC技术就是：客体不断产生、消亡，权限集合不断变动，权限与角色的联系不稳定，即使系统初始运行时构造出合理的角色层次关系，系统运行中还要进行复杂的角色权限配置。

公文系统的上述特点使得采用集中式管理的RBAC模型难以在此发挥作用，由于公文系统的权限集合不固定，权限配置到具体角色需要逐级授权，即使RBAC96模型与它的管理模型(ARBAC97/99模型)配合工作也不能收到满意的效果。相反，ME_RBAC模型的逐级管理、逐级授权的特点在这里得到充分的体现。

我们通过上述ME_RBAC模型实现了公文系统的访问控制和安全管理。根据实际的省政府各部门的组织结构和公文流转的管理要求，利用自顶向下的方式生成了包含管理层次关系的RBAC总体框架，如图5。

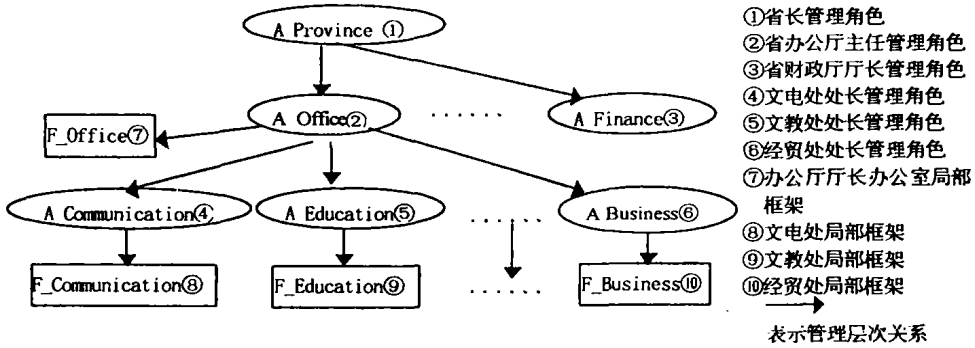


图5 公文系统的管理层次关系

图5给出了公文系统中管理角色和局部框架的管理层次关系。在管理角色和管理层次关系逐步确定的同时，我们通过管理角色利用自底向上的方法分别创建了各自所直接管理的局部框架，在每个局部框架内部，权限继承关系作为角色间的层次关系。图6给出了文电处处长管理角色创建的文电处局部框架。

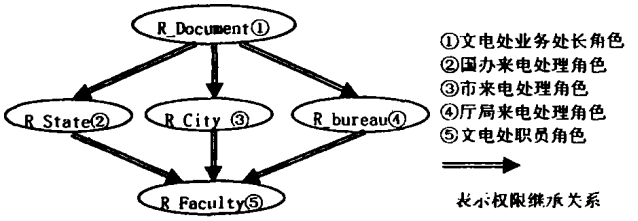


图6 文电处局部框架

在总框架形成(或部分形成)后，每收到一外部公文，经过各级管理角色从上到下的逐级授权，最后该公文的审批权配置给某局部框架中的某些具体业务处理角色，在处理完毕后，从下到上逐级撤销相应的管理权限及审批权限，完全模拟实际生活中公文处理的流程。

在框架运行过程中，如果动态调整某个具体的局部框架或管理角色，基本上不会影响到其它不相关部分的框架的运行。

4 相关工作比较

RBAC框架的管理问题在很多RBAC模型中很少涉及，大都默认为由系统管理员集中式管理，这些RBAC模型难以在组织结构复杂的领域得到应用。RBAC96模型[4,13]与其管理模型(ARBAC97模型[8]或ARBAC99模型[14,15])的组合是目前最流行的带有框架管理能力的解决方案。同这种组合相比，ME_RBAC模型具有明显的优点，具体表现在：

(1)ARBAC97/99模型采用权限继承来组织管理角色间的层次关系[15,16]，权限继承关系是越层管理的体现。ME_RBAC模型的管理层次关系明显比ARBAC97/99模型的权限继承关系更加贴近应用领域中的组织管理结构。

(2)ME_RBAC模型为管理角色指定局部管理策略，不同的局部管理策略按层次关系进行组织，下级继承上级的管理策略，每部分需要满足怎样的管理策略一目了然，便于验证。

(3)ME_RBAC模型的实例框架的动态维护能力强，在框架调整过程中，除维护涉及的部分外，其它部分能够正常运行。

结束语 基于角色的访问控制是解决大型应用系统安全管理的有效技术，RBAC技术应用于实际系统时，资源访问权限的管理也就演化为角色相关的管理，角色、权限配置和用户指派等方面的有效管理是RBAC技术应用于大型系统的关键。本文重点研究了RBAC中的角色管理问题，提出了能够实现自身管理的RBAC模型，该模型中的管理层次关系更加形象地模拟了应用领域的组织管理结构。本文提出的模型已经应用于上文提到的系统中，既实现了系统的安全管理，又类似实际的公文管理流程，为用户提供了友好的权限管理人机界面。

参考文献

1 Ferraiolo D F, Cuginiand J, Kuhn D R. Role Based Access Control: Features and Motivations. In: Proc. Of the 11th Annual Conf. on Computer Security Applications. 1995

2 Sandhu R S, et al. Role-based Access Control: A Multi-Dimension View. In: Proc. Of the 10th Annual Conf. on Computer Security Applications. 1994

3 Ferraiolo D F, Kuhn D R. Role_Based Access Control. In: Proc. of the 15th National Computer Security Conf. 1992

(下转第52页)

态变化的情况下，它往往不能满足求解态势评估问题的要求。因此，为了反映态势与事件间随观察变化的连接关系，下面我们考虑使用一种动态的贝叶斯网络来求解态势评估问题。

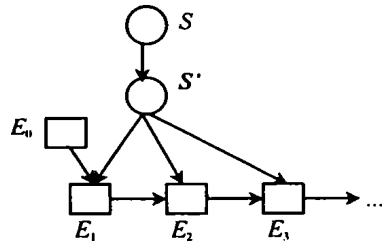


图2　态势评估的动态贝叶斯网络模型

假设目标的当前态势 S，$S=\{S_1,S_2,\cdots\}$是一个有限集，其中 $S_1,S_2,\cdots$互斥且组成完备的 S，态势 S 表示了目标的当前意图。假设目标当前发生了事件 E_0，我们使用当前态势 S 和当前事件 E_0来对目标的下一态势和下一事件进行预测，并在观察到新的事件发生时，在建立的贝叶斯网络上动态添加新的事件结点，然后在网络结点间传播和融合这些新的信息，获得更新的态势结点的置信度。建立的贝叶斯网络模型如图2所示。

在图2所示的模型中，根据假设独立性原则，有：

$$P(E_1|S',S,E_0)=P(E_1|S',E_0) \tag{16}$$

当 $n\geqslant 0$时，有

$$P(E_{n+1}|S',S,E_0,\cdots,E_n)=P(E_{n+1}|S',E_n) \tag{17}$$

因此，我们可以获得以下的更新式子：

$$\begin{aligned}&P(E_1|S,E_0)\\&=\sum_i P(E_1|S'_i,S,E_0)P(S'_i|S,E_0)\\&=\sum_i P(E_1|S'_i,E_0)P(S'_i|S,E_0)\end{aligned} \tag{18}$$

$$P(S'|S,E_0)=P(S'|S) \tag{19}$$

当 $n\geqslant 0$时，有

$$\begin{aligned}&P(E_{n+1}|S,E_0,\cdots,E_n)\\&=\sum_i P(E_{n+1}|S'_i,S,E_0,\cdots,E_n)P(S'_i|S,E_0,\cdots,E_n)\\&=\sum_i P(E_{n+1}|S'_i,E_n)P(S'_i|S,E_0,\cdots,E_n)\end{aligned} \tag{20}$$

$$\begin{aligned}&P(S'|S,E_0,\cdots,E_{n+1})\\&=\frac{P(E_{n+1}|S',S,E_0,\cdots,E_n)P(S'|S,E_0,\cdots,E_n)}{P(E_{n+1}|S,E_0,\cdots,E_n)}\\&=\alpha P(E_{n+1}|S',E_n)P(S'|S,E_0,\cdots,E_n)\end{aligned} \tag{21}$$

式中，α 为归一化因子。

网络初始化时，需要事先给定态势结点 S 和事件结点 E_0 的置信度，然后利用结点间连接的条件概率矩阵更新结点 S' 和 E_1的置信度。在观察到新的事件发生时，在建立的贝叶斯网络上动态添加这些事件作为新的证据，再使用(20)和(21)式更新结点 S'和下一事件发生的置信度，直到 S'的置信度超过了预先设定的阈值，即认为该态势已经发生。

结束语　用贝叶斯网络找出态势假设和事件之间的潜在关系，正是态势评估所需完成的功能，但是利用贝叶斯网络进行态势评估，主要还存在两个方面的问题：态势元素的提取和先验知识的获取，前者直接决定了网络的结构，而当变量增多时，可能的网络结构成倍增加，也就需要更多的先验知识。对于本文建立的两种贝叶斯网络模型，先验知识的获取需要通过预先设立的知识库，尽管后一种模型可以反映战场场景的动态变化，但是动态网络在建立时由于事件发生的不确定性，使得先验知识的获取更为困难。由于我们不可能对所有的网络结构进行计算，因此在实际应用中必须依赖专家知识进行一定的网络选择。

参 考 文 献

1 Pearl J. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. San Mateo, CA, Morgan Kaufmann, 1988

2 Pearl J. On Evidence Reasoning in a Hierarchy of Hypotheses. Artificial Intelligence, 1986, 28: 9～15

3 Heckerman D. A Bayesian Approach for Learning Causal Networks. In: Proc. of the 11th Conf. of Uncertainty in Artificial Intelligence, San Francisco, 1995. 285～295

4 Kirillov V P. Constructive Stochastic Temporal Reasoning in Situation Assessment. IEEE Trans. on System, Man and Cybernetics, 1994, 21(7): 1099～1113

5 Miao A X, Zacharias G L, Kao S-P. A computational situation assessment model for nuclear power plant operations. IEEE Trans. on Systems, Man, and Cybernetics, Part A, 1997, 27(6): 728～742

6 Albrecht D, Zukerman I, Bud A. Towards a Bayesian model for keyhole plan recognition in large domains. In: Proc. of the Sixth Intl. Conf. on User Modeling, Sardinia, Italy, 1997. 365～376

（上接第104页）

4 Sandhu R S, et al. Role-Based Access Control Models. IEEE Computer, 1996, 29(2): 38～47

5 Nyanchama M, Osborn S. The role graph model and conflict of interest. ACM Transactions on Information and System Security, 1999, 2(1): 3～33

6 Ferraiolo D F, Barkley J F, Kuhn D R. A role-based access control model and reference implementation within a corporate intranet. ACM Transactions on Information and System Security, 1999, 2(1): 34～64

7 Park J S, et al. RBAC on the Web by Smart Certificates. In: Proc. of the fourth ACM workshop on role-based access control, 1999

8 Sandhu R, et al. The ARBAC97 model for role-based administration of roles. ACM Transactions on Information and System Security, 1999, 2(1): 105～135

9 Moffett J D, Lupu E C. The uses of role hierarchies in access control. In: Proc. of the fourth ACM workshop on role-based access control, 1999

10 Sandhu R S. Role Activation hierarchies. In: Proc. of 3rd ACM Workshop on Role-Based Access Control, Oct. 1998

11 钟华，等. 扩充角色层次关系模型及其应用. 软件学报, 11(6): 779～784

12 Chen Feng, et al. Constraint for Role_based Access Control. In: Proc. of the first ACM workshop on role-based access control, 1996

13 Sandhu R S. Rationale for the RBAC96 Family of Access Models. In: Proc. of first ACM Workshop on RBAC, 1996

14 Munawer Q. Administrative Models for Role-Based Access Control. Dissertation for Doctor degree, George Mason University, 2000

15 Sandhu R S, Munawer Q. The ARBAC99 Model for Administration of Roles, 1999

16 Sandhu R S, Munawer Q. The RRA97 Model for Role_based Administration of Role Hierarchies. In: Proc. of 14th Annual Computer Security Application Conf. 1998