文章编号:1001 - 9081(2009)09 - 2332 - 04

P2P 环境下基于信任度的可控委托信任管理模型

高 迎[1],战 疆[2]
(1. 首都经济贸易大学 信息学院,北京 100070; 2. 中国人民大学 信息学院,北京 100872)
(yinggao517@126.com)

摘 要:结合基于角色的访问控制和信任管理各自的优势,提出一个适用于开放式环境的基于信任度的可控委托授权模型,实现对角色中包含的本地和继承权限的委托控制。提出了为本地策略中的角色分配信任度阈值的方法,为角色授权增加信任度的考虑,给出在这种扩展后的信任管理系统中计算实体信任度的算法,并结合具体实例对模型的使用进行了说明。

关键词:授权;信任度;委托深度;访问控制;角色
中图分类号: TP301 **文献标志码**:A

Controllable delegation trust management model based on trustworthiness in P2P

GAO Ying[1], ZHAN Jiang[2]
(1. *School of Information, Capital University of Economics and Business, Beijing* 100070, *China*;
2. *School of Information, Renmin University of China, Beijing* 100872, *China*)

Abstract: A controllable delegation authorization model that is suitable for open environments was presented. It integrated the merits of both Role Based Access Control (RBAC) and role-based trust management and can effectively control the propagation of permissions of different inheritance hierarchy in roles. An approach for assigning trustworthiness thresholds to permissions in local access control policy was discussed. The algorithm of calculating the values of trustworthiness of entities in the extended framework was proposed. The usage of the model was illustrated through a typical example.

Key words: authorization; trustworthiness; delegation depth; access control; role

0 引言

P2P 技术又称对等计算,它引导网络计算由集中向分布式转变。分布式的、分散的、动态的环境在安全管理方面具有许多与传统的封闭式系统不同的新特点:1)在开放的网络中,信任关系不是静止的而是动态变化的;2)很难用绝对的、精确的标准对系统安全进行度量;3)在分布式的网络环境中,没有集中的信任管理机制,因此安全信息只能分布存放;这为随后的一致性验证造成困难。因此,我们认为开放的分布式环境下信任管理模型应该具有评估实体合理信任度的能力。依据实体的信任度,根据资源访问控制策略,可以建立实体之间合理的信任关系。这是实现开放的分布式环境下信任管理的前提和基础。

为了适应开放式环境的特点,我们提出的基于角色信任度的可控委托信任管理模型中将角色与信任度阈值绑定,实体之间的信任度通过主观信任度模型的计算获得。这样实体可以根据需求设定本地角色的信任度阈值,进而授予信任度满足要求的实体。

不仅如此,在我们提出的模型中,关于角色的委托授权进行了严格的基于信任值的控制。实体对于继承的角色没有权利进行直接转授,必须通过已经存在的信任链,判断角色拥有者与本次授权实体之间的信任度。这种方式能够有效地限制委托授权的深度,提高信任管理系统的安全性和可靠性。

1 相关工作

最近几年发展起来的公钥基础设施(Public Key Infrastructure, PKI)为网络环境下的安全服务提供了统一的基础支撑体系[1]。1996 年,KeyNote、policyMaker、REFEREE[2-3]等信任管理系统的出现,将传统的访问控制推广到了开放的分布系统环境中。它们通过定义一个统一的信任与安全策略描述语言来描述请求、授权以及访问控制策略;提供一个信任管理模型用于判断实际的访问请求是否被接受。然而现有的 PKI 机制依赖于集中管理属性,缺少信任产生评估机制。而信任管理系统基于严格的逻辑推导和证明的形式化验证方法处理实体间信任关系存在着策略制定复杂、无法刻画信任关系的不确定性和模糊性等诸多问题。主观信任度评估模型提供了一种能够很好地刻画和描述信任关系的方法,并且能够解决在完全分布对等的网络中实现实体之间信任关系建立的问题。基于角色的访问控制(Role Based Access Control, RBAC)[4-5]通过引入角色的概念,实现了用户和权限逻辑分离,权限被授予角色,降低了授权管理的代价。但是在开放式环境下,存在大量彼此陌生的自治实体,资源的拥有者难以依据陌生实体的身份进行授权。因此,传统的 RBAC 不适合这种开放式的应用环境。

虽然目前有些系统提出了在传统的 RBAC 基础上引入信任度如 TBAD[6-7],但是这些系统中在委托的形式化定义时并未涉及角色与信任度的关系,信任度仅仅与用户实体直接

收稿日期:2009 - 03 - 19;**修回日期**:2009 - 05 - 17。 **基金项目**:国家自然科学基金资助项目(60703007)。
作者简介:高迎(1973 -),女,辽宁鞍山人,副教授,博士,主要研究方向:高性能数据库、信息安全、信息检索; 战疆(1972 -),男,山东济南人,副教授,博士,主要研究方向:高性能数据库、信息安全。

关联,当用户具有多个角色或权限时,单一的用户信任度将不能满足系统要求。

此外,关于委托授权深度的安全控制问题,现有的工作大都集中在信任管理引擎的构建上,对于委托过程中的权限的传播问题没有从安全的角度给予足够的重视。唯一考虑了授权深度问题的 SPKI 只是采用布尔值来控制委托过程,可以指定本次委托是否允许任何后继委托。而这种布尔控制是完全不考虑后继委托实体信任值的具体情况,其表达能力非常有限。Cassandra,DL 和 RT[5] 都是用整数值进行委托深度的控制,而整数值的设定没有考虑随后的被授权实体的具体可信度情况,具有很大的不准确性和盲目性。文献[9]虽然提出了使用主观信任度进行委托深度控制的思想,但是其提出的信任计算方法假设凭证链是线性结构,而基于角色的信任管理中,信任链是图的结构,因此难以满足需求。文献[7]虽然也提出了一种基于信任度的可控委托授权模型,但在委托形式化定义时并未涉及角色与信任度的关系,信任度仍然与用户直接关联。

为此,在综合了传统的信任管理和主观信任度评估模型各自优势的基础上,结合分布式开放网络的具体特点,为了适应开放式环境,我们提出的基于角色信任度的可控委托信任管理模型中将角色与信任度阈值绑定,实体之间的信任度通过主观信任度模型的计算获得。不仅如此,实体对于继承的角色没有权利进行直接转授,必须比较角色拥有者与本次授权实体之间的信任度方可判断授权是否可以进行。

2　对 RBAC 进行基于信任度的可控委托扩展

传统的基于角色的信任管理 RBAC 只涉及到确定实体间信任关系后如何进行基于角色的权限的分配以及转授,忽略了实体(尤其是不同管理域的陌生实体)如何获得角色和其获取角色时的信任度,以及权限转授过程中的控制问题。由于 RBAC 目前的转授机制没有很好的定量的控制,很容易造成访问控制策略的漏洞。

目前的 RBAC 模型中,可以对权限实现基于角色的直接授权和委托授权。在这两种授权的过程中,均假设授权的主体已经充分信任授予和委托对象,这是无条件可信。在一个稳定的封闭环境中这种假设是存在的,但是在目前大量存在的开放多个自治的管理域环境中这将会带来两个缺陷。1)针对直接授权,不同管理域间实体的直接授权是有条件可信的,属于不同管理域的实体只有确定了一定信任关系的才能够进行安全可靠的授权。在 RBRC 模型中完全没有考虑条件的设定,会造成访问控制资源的不安全。2)针对间接授权,RBAC 模型中关于委托授权没有任何控制。实际上,不同管理域的实体之间如果存在权限的转授,那么在考虑实体间获得信任关系而进行直接授权的基础上还要保证对于继承权限能够实现可控委托。

为了克服在开放的环境中 RBAC 模型存在的上述问题,本文提出扩展角色的概念:角色应该不仅仅是权限或拥有某一权限的实体的集合,除此之外,角色应该包含对拥有者的最低的信任的约束。这种解决方法很好地保持了角色作为权限的集合的整体特征,从而能够在大量复杂授权中实现操作的简化。现有的一些方案中[6],提出为角色中的每一个权限制定一个最小的信任度阈值,实现细粒度的基于角色的授权。从根本上说,这种方法没有充分利用角色概念在授权方面存在的简化操作的优点,而且使它成为授权的一种负担,所有的授权操作最终的判断都要分析角色所包含的基本权限逐一进行。

在改进模型中,如果陌生的实体之间能够进行本地角色的授予,一定是角色的发布方认为接受方的信任值不小于角色本身绑定的最低信任值。比如,实体 A 能够允许实体 B 共享本地的文件资源,那么实体 A 一定已经通过以前与 B 的交往或其他实体的推荐获得了对实体的信任的一个认知,并且这个信任值大于具有允许共享文件资源的角色的最低阈值。如果实体之间授予的角色不是本地角色,而是实体从其他实体处获得的,在这个委托授权的过程中同样要保证实体间的信任度不低于角色的最低阈值。此外,角色的最低信任度是角色的所有者定义的,在角色的委托授权中,委托实体的判断是否符合角色所有人的判断必须经过严格的量化衡量。如,实体 B 企图获得共享实体 A 本地资源的一个角色,但是实体 A 对它的信任值的评估低于角色绑定的最低值,此时实体 B 不可能从实体 A 处直接获得希望的角色,但是它可以通过与它熟悉的实体 C 间接获得实体 A 发布的角色。上述情况表明,在角色的委托过程中,可能会存在一些安全方面的漏洞。我们应该考虑到委托过程中的信任的衰减[8] 问题,实现委托的可控操作。

定义 1　模型基本要素。ROS,OPS,OBS 分别代表角色的集合、操作的集合、实体的集合。

定义 2　直接信任度、推荐信任度和角色信任度阈值。

直接信任度　在开放式环境下,如果实体 HY 利用实体 AX 提供的服务完成了一次合作,那么 AX 与 HY 之间存在直接信任关系。实体 AX 对实体 HY 行为的评价称为实体 AX 与 HY 之间的直接信任值。直接信任值的取值为[0,1],记为 dtv_{HY}^{AX}。

推荐信任度　在开放式环境下,从未进行直接合作的陌生实体之间存在信任关系,信任值由实体间的推荐获得。记为 tv_{HY}^{AX}。

角色信任度阈值　角色的拥有者要求被授予该角色的实体具备的最低信任度值。记为 th。

只有当角色拥有者与角色被授予实体之间的信任度值高于角色信任度阈值时授权才能成立。

定义 3　角色、角色继承。

角色　被命名的一组权限,是权限的集合。由于角色可以进行授权,因此角色必须包含角色信任度阈值。记为 $ROS(OB,OPS,th)$,其中,OB 代表角色的所有者实体,OPS 代表角色所包含的权限的集合,th 代表角色的信任度阈值。

角色继承　$DRH \subseteq ROS \times ROS$,是角色间的继承关系,由于角色的转授形成的角色间的层次关系。

我们模拟了一个 P2P 环境下资源协作的场景[7]:在系统中,用户实体可以有选择地共享其他实体的软件和硬件资源,如文件下载、使用其他用户的 CPU 等。为了保证在资源共享过程中的资源安全,用户实体需要对其资源通过发布安全凭证的方式进行访问控制。同时,在用户不断协作、共享的过程中将获得他们的全局信任值,这个信任值将成为用户实体间确立信任关系的基础。文献[9]假设存在 A,B,C,D,E,F 七个用户实体,他们各自拥有具有某些权限的角色,并设定了角色的信任度阈值,如表 1。

在我们提出的基于信任度的委托控制策略中,针对所有者直接将角色进行授予的情况,我们要求被授予的用户的信任值必须大于角色的最低信任度阈值。如上例中,H 希望将他所拥有的 *member* 权限授予实体 G。如果此时 *member* 角色没有

继承任何角色的权限,那么只需要 *member* 的拥有者 H 与实体 G 之间的信任度值大于角色的信任度阈值就可以完成此次的授予。针对角色转授的情况,实体 D 将拥有的角色 *prepered* 授予拥有 *member* 角色的实体 H,因此 *member* 角色继承了 *prefered* 角色的权限。而实体 H 又将这个角色授予了实体 G。在这种情况中,实体 G 不仅拥有角色 *member* 固有的权限,而且包含 *member* 角色继承的 *prefered* 角色的权限。在上述的角色授予过程中,出现了 *perferec* 角色的转授。针对转授部分,我们必须重新利用信任值做出是否允许的授权的判断。此处我们需要判断的是角色所有者 D 实体对于 G 实体的信任度值是否操作了角色 *member* 的信任度阈值,以这种方式可以有效地控制委托授权的深度。

通过签发安全凭证,实体的角色可以进行授权。角色的不断转授可以形成比较复杂的安全凭证链的关系(如表2),也形成了角色之间的继承关系,如图1。

表1 角色及信任度阈值

角色所有者	角色名称	角色信任度阈值
A	*Use*	0.70
B	*Use*	0.80
C	*Member*	0.78
D	*Preferred*	0.75
E	*Read*	0.68
F	*Use*	0.70
H	*Member*	0.70

表2 为实现角色授予而签发的安全凭证

用户	安全凭证	信任值
A	*A. use* ← (*D. prefered*(:0.7)	0.70
B	*B. use* ← (*C. member*(:0.76)	0.80
C	*C. member* ← *G*(:0.7)	0.78
D	*D. prefered* ← *H. member*(:0.68)	0.75
E	*E. read*(?*y*) ← *F. use*(?*y*)(:0.65)	0.68
F	*F. use* ← *A. use* ∪ *B. use*(:0.8) *F. use*(*file*1) ← *G*(:0.68)	0.70
G	—	0.84
H	*H. member* ← *G*(:0.68)	0.70

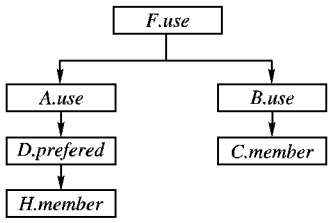

图1 角色继承关系

总之,在我们的策略中如果角色只包含本地权限,那么只需要判断角色拥有实体与被授予实体之间的信任值是否超过信任度阈值;如果角色之间存在继承关系,那么我们要考虑被继承的角色所有者实体与授予实体之间的信任值与角色信任阈值的大小关系。

3 实体间信任值的计算

实体间信任关系可以通过实体之间的直接交往和推荐来获得。开放环境下,由于实体之间存在相互的合作,所以形成信任关系图。存在合作关系的实体之间的信任值可以根据合作的结果由实体相互设定。没有存在合作关系的实体之间可以根据信任关系图通过实体之间的推荐间接获得实体间信任值。

定义4 信任关系图 $G=(V,E)$ 是包括节点集合 V 和边集合 E 的有向图。边的权重代表相邻实体之间的直接信任值,记为 $dtv_{v_i}^{v_j}$。信任关系图描述了一个开放式环境中实体之间由于具有直接信任值而形成的一种关系图,如图2所示。

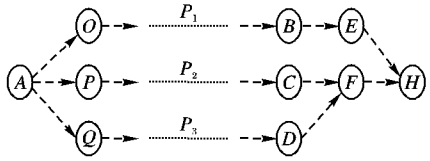

图2 信任关系网络

图2中,由有向边连接而成的两个实体之间存在直接信任关系,因此容易获得他们之间的信任值,即 dtv_{HY}^{AX},如实体 A 与实体 P。而不直接相连的两个实体之间的信任关系较难获得,如实体 A 与实体 H。

定义5 在有向图 $G=(V,E)$ 中,从节点 A 到节点 H 的一条路径,称作 A 到 H 的推荐信任路径,记作 p_i。推荐信任路径起始于实体 A,终止于实体 H,中间可包含一个或多个实体。这个推荐信任路径具有推荐信任值,记为 $rdtv_H^A(p_i)$。

通常,实体间的推荐信任路径存在多条。设 $P_1,P_2,\cdots,P_k$ 是实体 A 与实体 H 之间的多条推荐信任路径。$N(P_i)$ 代表第 i 条推荐信任路径所包含的实体的集合。

如果 $\forall P_i,P_j,N(P_i)\cap N(P_j)=\{A,H\},1\leqslant i,j\leqslant m$,那么称 $P_1,P_2,\cdots,P_m$ 为独立的推荐信任路径。否则,P_i,P_j 称为相关的推荐信任路径。如图2,其中路径 P_1,P_2 为独立的推荐信任路径,P_2,P_3 为相关的推荐信任路径。

对多条推荐信任路径综合处理后得到的推荐信任值称为路径联合推荐信任值,记为 $comrdtv_H^A$。

3.1 信任模型

在推荐信任关系图 $G=(V,E)$ 中,$A,H\in V,P$ 是连接两个点的一条推荐信任路径。$N(1),N(2),\cdots,N(k)$ 是路径上的有序节点。那么

$$rdtv_H^A(p)=\prod_{i=1}^{k-1}rtdv_{N(i+1)}^{N(i)} \tag{1}$$

由于实体对其推荐者的信任程度不同,因此它对信息采纳程度也不同。推荐系数用于推荐信息的衰减,以减低推荐信任值较低的实体对信任评估结果的影响。

在推荐信任关系图 $G=(V,E)$ 中,$A,H\in V$。A,H 之间存在 k 条推荐信任路径,$p_1,p_2,\cdots,p_k,V_1,V_2,\cdots,V_K$ 是路径上实体 H 的直接推荐实体。$rdtv_{V_i}^A(p_i)$ 代表路径 p_i 上两个实体 A,V_i 之间的推荐信任值,$rdtv_H^A(p_i)$ 代表路径 p_i 上两个实体 A 和 H 之间的信任值。

当 $p_1,p_2,\cdots,p_k$ 是独立的 k 条推荐信任路径,那么

$$comrdtv_H^A=\frac{\sum_{i=1}^{k}\left(rdtv_{V_i}^A(p_i)\times rdtv_H^{V_i}\right)}{\sum_{i=1}^{k}rdtv_{V_i}^A(p_i)}$$

当 $p_1,p_2,\cdots,p_k$ 是相关的 k 条推荐信任路径,而且在这个路径的集合中,找不到任何一个子集使得它与集合中其他路径不相交。我们称这个相关路径的集合为不可再分的。对于不可再分的一组相关推荐信任路径:

$$comrdtv_B^A=rdtv_B^A\left(Rand(p_1,p_2,\cdots p_k)\right)$$

在不可再分的相关推荐信任路径中,我们随机选取一条,利用它的推荐信任值作为关联信任路径联合推荐信任值。

如果 $p_1, p_2, \cdots, p_k$ 中既包含独立推荐信任路径又包含相关推荐信任路径。假定,$p_1, p_2, \cdots, p_j$ 是相关路径,$p_{j+1}, p_{j+2}, \cdots, p_k$ 是独立路径,V_i 代表实体 H 的某一直接推荐实体。为计算联合推荐信任值,首先将相关路径划分为不可再分的相关推荐信任的路径集合,$group_1, group_2, \cdots, group_m$。联合推荐信任值按下面公式计算:

$$comrdtv_H^A = \frac{\sum_{i=1}^{m}\left(rdtv_{V_i}^A(p_{randi}) \times rdtv_H^{V_i}\right)}{\sum_{i=1}^{m} rdtv_{V_i}^A(p_{randi}) + \sum_{i=j+1}^{k} rdtv_{V_i}^A(p_i)} + \frac{\sum_{i=j+1}^{k}\left(rdtv_{V_i}^A(p_i) \times rdtv_H^{V_i}\right)}{\sum_{i=1}^{m} rdtv_{V_i}^A(p_{randi}) + \sum_{i=j+1}^{k} rdtv_{V_i}^A(p_i)} \quad (2)$$

其中 $p_{randi} = Rand(group_1, group_2, \cdots, group_k)$。

对于既包含独立路径,又包含关联路径的情况,我们首先对相关路径进行分组,然后,从每一组关联路径中随机的选取一条路径,将这些选出的路径与其他独立的路径重新构成一组独立的路径。利用独立路径的处理方法来进行计算。

在基于推荐信任关系形成的信任关系图 $G = (V, E)$ 中,$A, H \in V$。那么:

$$tv_H^A = \alpha \times dtv_H^A + (1 - \alpha) \times rdtv_H^A \quad (3)$$

实体 A 与实体 H 的信任值由 A 与 H 直接交往获得的直接信任值和通过推荐获得的联合评价共同构成。其中 $0 \leqslant \alpha \leqslant 1$,称为信任权重因子,由实体 A 自己选择设定,表明 A 在重新评价和其他实体之间的信任度时,自己原来持有的对该实体的直接信任记录的影响权重。如果 $\alpha = 0$,表明 A 只参考来自推荐路径的联合评价;$\alpha = 1$,表明 A 只信任自己的历史评价。$\alpha = 0.5$,表明 A 对等看待来自推荐信任路径的联合评价和自己持有的历史评价。

由于篇幅有限,本文没有介绍一致性验证中信任链查找的过程[8]。这部分也是进行可控委托授权的重要组成部分。

3.2　模型的安全性质

在一个完整的开放环境下的信任管理过程中,当实体进行角色授权时,对于本地角色进行授权,需要判断本地的角色拥有者与被授权实体之间的信任管理。对于本地角色继承的角色权限,那么需要严格的判断继承角色的初始拥有者与本次被授予实体之间的信任关系。只有当实体之间的信任值高于角色本身的信任度阈值的时候才能够允许转授发生。在信任关系的判断过程中,实体可以通过 $0 \leqslant \alpha \leqslant 1$ 信任权重因子的设定表明实体对于推荐信息的信任程度。

定理　实体 e 能够获得角色 p 当且仅当关于角色 p 的直接或委托授权存在并且角色所有者 f 与实体 e 之间的信任值超过角色的信任度阈值。

4　结语

与传统的信任模型相比,本文提出的改进模型通过严格的基于信任值的授权,并考虑推荐信任的衰减可以有效地避免信任值达不到阈值要求的实体通过间接的方法获得角色。此外,角色的拥有者也可以提高角色的绑定信任度阈值,从而提高本地资源的安全性。在这个改进的模型中,角色的安全以及角色的委托深度都得到了更大的安全保证和控制。

参考文献:

[1] SANDHU R S, COYNE E J, FEINSTEIN H L, *et al*. Role-based access control models [J]. IEEE Computer, 1996, 29(2): 38 - 47.

[2] ANSI INCITS. Role based access control [S]. ANSI INCITS 359-2004, American National Standard for Information Technology, 2004.

[3] FERRAIOLO D F, CUGINI J, KUHN D R. Role-based access control (RBAC): Features and motivations [C]// Proceedings of the 11th Annual Computer Security Application Conference. New Orleans: IEEE Computer Society, 1995: 241 - 248.

[4] JOSHI J B D, BERTINO E, LATIF U, *et al*. A generalized temporal role based access control model [J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(1): 4 - 23.

[5] LI N H, WINSBOROUGH W H, MITCHELL J C. Distributed credential chain discovery in trust management [C]// Proceedings of the 8th ACM Conference on Computer and Communications Security. New York: ACM Press, 2001: 156 - 165.

[6] 翟征德,冯登国,徐震. 细粒度的基于信任度的可控委托授权模型[J]. 软件学报, 2007, 18(8): 2002 - 2015.

[7] 廖俊国,洪帆,朱更明,等. 基于信任度的授权委托模型[J]. 计算机学报, 2006, 29(8): 1265 - 1269.

[8] 高迎,程涛远,王珊. 服务网格环境下基于行为的分层信任模型的研究[J]. 计算机应用, 2005, 25(9): 1974 - 1977.

[9] 高迎,程涛远,王珊. 基于 HILBERT 曲线的许可证存储策略及查找算法[J]. 软件学报, 2006, 17(2): 305 - 314.

(上接第 2331 页)

参考文献:

[1] EDWARD H. Attacks evolving toward exploiting network services [EB/OL]. (2003 - 12 - 02)[2008 - 05 - 15]. http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci939419,00.html.

[2] HANEMANN A, SCHMITZ D, SAILER M. A framework for failure impact analysis and recovery with respect to service level agreements [C]// Proceedings of the 2005 IEEE International Conference on Services Computing. Piscataway: IEEE Computer Society, 2005: 49 - 58.

[3] KRUGEL C, TOTH T, KIRDA E. Service specific anomaly detection for network intrusion detection [C]// Proceedings of the 2002 ACM symposium on Applied Computing. New York: ACM Press, 2002: 201 - 208.

[4] YAU S S, GONG H, HUANG D, *et al*. Automated agent synthesis for situation awareness in service-based systems [C]// COMPSAC'06: Proceedings of the 30th Annual International Computer Software and Applications Conference. Chicago: IEEE Computer Society, 2006: 503 - 512.

[5] 陈秀真,郑庆华,管晓宏. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4): 885 - 897.

[6] DoD Multidisciplinary University. Adaptable secure situation-aware service-based (AS3) systems[EB/OL]. [2009 - 02 - 24]. http://dpse.eas.asu.edu/AS3/index.shtml.

[7] 赵国生. 可生存性网络关键技术研究[D]. 哈尔滨: 哈尔滨工程大学, 2006.

[8] 王连芬,许树柏. 层次分析法引论[M]. 北京: 中国人民大学出版社, 1990.

[9] 庞永刚. 用于网络可信性评测的事件注入技术仿真研究[J]. 系统仿真学报, 2008, 20(10): 2713 - 2717.