基于属性关联的客体聚合信息级别推演方法

曹利峰,陈性元,杜学绘,邵 婧
(解放军信息工程大学,河南郑州 450004)

摘 要: 为解决客体关联性引起的泄密问题,本文对客体关联性进行了深入分析,提出了基于属性关联的客体聚合信息级别推演方法.该方法根据客体属性依赖关系,挖掘出高关联度的客体,通过客体关联属性级别模糊集可能性测度,推演出关联客体推导出更高级别信息的可能性,以此指导多级安全网络访问控制策略的制定,控制主体对关联客体的访问,降低系统失泄密的风险.

关键词: 多级安全; 等级保护; 客体聚合; 推理通道; 级别推演
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2013)07-1442-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.07.031

A Level Inference Method for Aggregated Information of Objects Based on Associated Attributes

CAO Li-feng, CHEN Xing-yuan, DU Xue-hui, SHAO Jing
(*The PLA Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: A level inference method for aggregated information of objects based on associated attributes is put forward in order to give a solution to information leakage caused by the association among objects. According to dependency relationships, highly associated objects are found, and then the probability of higher level information inferred by aggregation of associated objects is computed by probability estimates of fuzzy sets on secure level of attribute. The method may contribute to establish access control policy in multi-level secure network, and control restricted access of associated objects in order to reduce the risk on information system.

Key words: MLS; classified security protection; object aggregation; inference channel; level inference

1 引言

信息系统进行分级保护后,系统间无疑会构建起严格的保护和隔离壁垒,形成新的数据孤岛,如何在不破坏原有信息系统正常运行和等级化安全特性的前提下,继续保持信息系统间的互联互通是等级保护必须要解决的关键问题.

经典的多级安全模型 BLP(Bell LaPadula),通过为主客体分配安全标记实施强制访问控制,尽管达到了信息系统间访问控制的目的,但是在等级化网络中,客体间关系异常复杂,存在着关联客体聚合而引起的泄密问题,即客体聚合推导问题[1],主体对客体的访问不再仅仅是遵从 BLP 的简单安全特性和 * -特性[1,2],也应该考虑客体间的关系[3].

聚合推导已被证明是个 NP 完全问题[4].目前对它的研究,主要的研究对象为数据库,研究内容为检测并消除推理通道[5],其方法主要为两类,一类是在数据库设计阶段发现推理通道,通过提升数据安全级别消除推理通道,另一类是在数据库查询阶段,依据既定的推理控制规则,检测潜在的推理通道并拒绝查询.但是此类方法并不完全适用于关系更为复杂的网络信息客体,主要体现在:(1)网络信息客体由不同主体创建,相比单一的数据库管理更为复杂,难以在设计阶段避免推理通道的发生;(2)数据库中属性推导关系主要体现在①$A\rightarrow B$或②$A\rightarrow B, B\rightarrow C \Rightarrow A\rightarrow C$,而网络客体更为复杂,还包括③$A_1\rightarrow_{p_1} B, A_2\rightarrow_{p_2} B\Rightarrow A_1, A_2\rightarrow_{p(\geqslant \max(p_1,p_2))} B, A_1\rightarrow_{p_1} B, A_2\rightarrow_{p_2} C\Rightarrow (A_1,A_2)\rightarrow_p (B,C)$与④$A = A_1 \parallel A_2\Rightarrow O(A_1), O(A_2)\rightarrow_p O(A)$等关联关系,其中 $O(A_i)$为拥有属性 A_i 的客体,这也是数据库中所忽略的.尽管文献[6]研究了客体聚合信息级别推演方法,但研究对象为相似客体,并非关联客体.

收稿日期:2012-04-19;修回日期:2013-02-22;责任编辑:李勇锋
基金项目:国家 973 计划前期研究专项(No.2011CB311801);河南省杰出科技创新人才计划(No.114200510001h)

因此,本文针对③④两种关联关系进行了深入分析,提出了一种客体关联度计算方法,以有效地挖掘高关联度的客体,依据客体间关联属性,给出了关联客体推导出更高级别信息可能性的推演算法,以指导网络边界访问控制策略的实施,降低系统泄密的风险.

2　客体关联性发现方法

为了更好地发现出客体之间的关联性,本文首先基于决策表知识约简[7],对已有的实例化数据进行了属性约简获取推导规则,构建领域先验推导知识库 K,形如$\{(R,\mu)\}$,R 为规则,μ 为强度,用于指导后续客体的关联性发现.

2.1　基于属性推导路径的客体关联发现

针对第三种关联情况,本文提出了基于属性推导路径的客体关联发现方法.

定义 1　A 为属性集,$p,q,l_1,l_2,\cdots,l_k\in A$,若 $p\rightarrow_{\gamma_1} l_1, l_1\rightarrow_{\gamma_2} l_2,\cdots, l_k\rightarrow_{\gamma_{k+1}} q$,则 $\exists\,\gamma'$,使得 $p\rightarrow_{\gamma'} q$,称 $l_1,l_2,\cdots,l_k$ 为属性 p 和 q 的属性推导路径,记作 AIP_{pq}. 其中,γ_i 为属性依赖度[7],$\gamma'=\gamma_1\gamma_2\cdots\gamma_k\gamma_{k+1}$.

定义 2　令 $p,q,s,t\in A$,则定义:

(1)若 $p\rightarrow_{\gamma_1} s$,$q\rightarrow_{\gamma_2} s$,则 $\exists\,\gamma$,$\gamma\geqslant\max(\gamma_1,\gamma_2)$,$p\rightarrow_{\gamma} q$,$\gamma=\gamma_1+\gamma_2-\gamma_1\gamma_2$.

(2)若 $p\rightarrow_{\gamma_1} s$,$p\rightarrow_{\gamma_2} t$,则 $\exists\,\gamma$,$\gamma\leqslant\min(\gamma_1,\gamma_2)$,$p\rightarrow_{\gamma}(s\cup t)$. $p\rightarrow_{\gamma_1} s$ 和 $p\rightarrow_{\gamma_2} t$ 相互独立的,因此,γ 应为 γ_1、γ_2 的乘积,即 $\gamma=\gamma_1\gamma_2\leqslant\min(\gamma_1,\gamma_2)$.

(3)令 $AIP_{ps}=l_1^{ps},l_2^{ps},\cdots,l_k^{ps}$,$AIP_{pt}=l_1^{pt},l_2^{pt},\cdots,l_m^{pt}$,$AIP_{qs}=l_1^{qs},l_2^{qs},\cdots,l_u^{qs}$,$AIP_{qt}=l_1^{qt},l_2^{qt},\cdots,l_v^{qt}$. 由(2)和 γ' 计算式可得,$(s\cup t)$对 p 的依赖度 $\gamma^{p(s\cup t)}$ 为 $\gamma_1^{ps}\gamma_2^{ps}\cdots\gamma_{k+1}^{ps}\gamma_1^{pt}\gamma_2^{pt}\cdots\gamma_{m+1}^{pt}$. $(s\cup t)$对 q 的依赖度 $\gamma^{q(s\cup t)}$ 为 $\gamma_1^{qs}\gamma_2^{qs}\cdots\gamma_{u+1}^{qs}\gamma_1^{qt}\gamma_2^{qt}\cdots\gamma_{v+1}^{qt}$. 再由(1)可得,$(s\cup t)$对$(p\cup q)$的依赖度为 $\gamma^{(p\cup q)(s\cup t)}=\gamma^{p(s\cup t)}+\gamma^{q(s\cup t)}-\gamma^{p(s\cup t)}\gamma^{q(s\cup t)}$.

(4)依赖度不小于 $\gamma_{\min}$(依赖度最小阈值)的推导关系属性子集称之为强关联属性子集.

定义 3　k 为强关联属性子集个数,AS_i 为第 i 个强关联属性子集,客体 O_1 和 O_2 的关联度:

$Assoc_3(O_1,O_2)=\sum_{i=1}^{k} w_i\gamma(AS_i)$,其中,$\gamma(AS_i)$为 AS_i 被高级别属性或子集依赖的程度,w_i 为 AS_i 的权重.

$w_i=I(AS_i)\,C_i^{\max}/\sum_{i=1}^{k} I(AS_i)\,C_i^{\max}$. 其中,$C_i^{\max}$ 为属性子集中属性最大安全级别的量化值,$I(AS_i)$为属性子集的信息量. $assoc_{\min}$为最小关联度阈值.

据此,本文给出了基于属性推导路径的客体关联发现算法 MAOA-AIP(Mining Algorithm of Object Association based on AIP).

算法 1　基于 AIP 的客体关联发现算法 MAOA_AIP

Input: O_1, O_2, A(information objects; Attribute set)
Output: flg (flag of high association)
(1) $a[\,]=Attr[o_1]$; $b[\,]=Attr[o_2]$; $Assoc=0$;
(2) for $i=1$ to $|a|$ do
(3) begin
(4)　for $j=1$ to $|b|$ do
(5)　begin
(6)　if $(a[i],b[i])\in K$ then $G[\,]=\{a[i],b[i],\gamma^{K(a[i]\cup b[i])}\}$;
(7)　if $\exists\,s\in A, a[i]\rightarrow_{\gamma^{a[i],s}} s, b[i]\rightarrow_{\gamma^{b[i],s}} s$ then{
(8)　　compute $\gamma^{(a[i]\cup b[i]),s}$;
(9)　　if $\gamma^{(a[i]\cup b[i]),s}\geqslant\gamma_{\min}$ then
(10)　　$G[\,]=\{a[i],b[i],\gamma^{(a[i]\cup b[i]),s}\}$;
(11)　}
(12)　if $\exists\,s,t\in A, a[i]$has inference paths to s,t
(13)　and $b[i]$has inference paths to s,t then{
(14)　　compute $\gamma^{a[i],(s\cup t)}$, $\gamma^{b[i],(s\cup t)}$, $\gamma^{(a[i]\cup b[i]),(s\cup t)}$;
(15)　　if $\gamma^{(a[i]\cup b[i]),(s\cup t)}\geqslant\gamma_{\min}$ then
(16)　　$G[\,]=\{a[i],b[i],\gamma^{(a[i]\cup b[i]),(s\cup t)}\}$; }
(17)　endfor
(18) endfor
(19) for $i=1$ to $|G|$ do
(20) begin
(21)　$w_i=I(G[i,1]\cup G[i,2])\,C_i^{\max}/\sum_{j=1}^{|G|} I(G[j,1]\cup G[j,2])\,C_j^{\max}$;
(22)　$Assoc=+w_iG[i,3]$;
(23)　if $(G[i,1],G[i,2])\notin K$ then $G[i]\Rightarrow K$; //add to K
(24) endfor
(25) if $Assoc\geqslant assoc_{\min}$ then $flg=1$; else $flg=0$;
(26) return flg;

算法分为 3 部分,第 1 部分(1 行)为客体属性子集的抽取;第 2 部分(2 ~ 18 行)为在领域先验知识库的指导下,分析客体属性关联性,依据 $\gamma_{\min}$获得强关联属性子集;第 3 部分(19 ~ 26)为客体关联度的计算,依据 $assoc_{\min}$获得强关联客体. MAOA_AIP 算法复杂度为 $o(|a|\cdot|b|\cdot k\cdot k)$.

2.2　基于属性频繁集的客体关联发现

第四种关联关系是第三种关联关系的特例,为了提高发现关联客体的效率,针对此关联关系,本文提出了基于属性频繁集的客体关联挖掘方法.

定义 4　令 $A_i^{o_1}$,$A_j^{o_2}$ 分别为客体 O_1,O_2 的一个属性子集,$A_i^{o_1}$ 和 $A_j^{o_2}$ 间的支持度为:

$$sup(A_i^{o_1},A_j^{o_2})=|(A_i^{o_1}\cup A_j^{o_2})|/|O|.$$

支持度是指属性子集 $A_i^{o_1}$ 和 $A_j^{o_2}$ 在所有大于 O_1,O_2 安全级别的客体中出现的频繁程度,并以最小支持度 $sup_{\min}$来进行限定.

定义 5　$A_i^{o_1}$ 和 $A_j^{o_2}$ 间的置信度是指包含 $A_i^{o_1}$ 和 $A_j^{o_2}$

的客体($>\max(C(O_1),C(O_2))$)数量占包含 $A_i^{o_1}$ 的所有客体($>\max(C(O_1),C(O_2))$)数量的百分比.

$$conf(A_i^{o_1},A_j^{o_2})=|A_i^{o_1}\bigcup A_j^{o_2}|/|A_i^{o_1}|.$$

如果置信度太低,那么客体隐含关系的可能越小,难以依据 O_1 和 O_2 推断出更高级别的信息,以最小置信度阈值 $conf_{\min}$ 进行限定.为了获得更可靠的置信度,本文依据领域先验推导知识库进行了修正.

$$conf_R(A_i^{o_1},A_j^{o_2})=\begin{cases}(conf(A_i^{o_1},A_j^{o_2})+\gamma^{A_i^{o_1},A_j^{o_2}})/2, & (A_i^{o_1},A_j^{o_2})\in K\\ conf(A_i^{o_1},A_j^{o_2}), & \text{otherwise}\end{cases}$$

定义 6 n 为强关联属性集个数,O_1 和 O_2 的关联度为:

$$Assoc_4(O_1,O_2)=\sum_{i=1}^{n}\sum_{j=1}^{n}w_{ij}conf_R(A_i^{o_1},A_j^{o_2})$$

其中,$w_{ij}=(C_i^{A_i^{o_1}}I_i^{A_i^{o_1}}+C_j^{A_j^{o_2}}I_j^{A_j^{o_2}})\Big/\left(\sum_{k=1}^{n}C_k^{A_k^{o_1}}I_k^{A_k^{o_1}}+\sum_{l=1}^{n}C_l^{A_l^{o_2}}I_l^{A_l^{o_2}}\right)$,

$$\sum_{i=1}^{n}\sum_{j=1}^{n}w_{ij}=1.$$

据此,本文给出基于属性频繁集的客体关联发现算法 MAOA_HFA(Mining Algorithm of Object Association based on High Frequency Attribute).

算法 2 基于属性频繁集的客体关联发现算法 MAOA_HFA

Input: O_1, O_2, A(information objects; Attribute set)
Output: flg(flag of high association)
(1) $a[\,]=Attr[O_1]$; $b[\,]=Attr[O_2]$;
(2) $k=0$; $d=0$; $l=0$; $Assoc=0$;
(3) for $i=1$ to $|a|$ do
(4) begin
(5) for $j=1$ to $|b|$ do
(6) begin
(7) $p=sup(a[i],b[j])$;//support degree
(8) if $p>=sup_{\min}$ then {
(9) $k=k+1$; $E[k]=\{a[i],b[j]\}$;}
(10) endfor
(11) endfor
(12) for $i=1$ to k do
(13) begin
(14) $f=conf(E(k))$;//confidence degree
(15) if $(E[k,1],E[k,2])\in K$ then
(16) $conf_R(E(k))=(f+\gamma^{E(k)})/2$;
(17) else $conf_R(E(k))=f$;
(18) if $conf_R(E(k))>=conf_{\min}$ then{
(19) $d=d+1$; $G[d]=\{E[k],f\}$;}
(20) endfor
(21) for $j=1$ to d do
(22) begin
(23) compute w_{ij}; $Assoc=+w_{ij}*G[j,3]$;
(24) if$(G[j,1],G[j,2])\notin K$ then $G[j]\Rightarrow K$;//add to K
(25) endfor
(26) if $Assoc>=assoc_{\min}$ then $flg=1$; else $flg=0$;
(27) return flg;

算法分为 4 部分.第 1 部分(1 行)为客体属性子集的获取;第 2 部分(2 – 11 行)为属性子集间支持度的计算;第 3 部分(12 – 20 行)为属性频繁子集置信度的计算;第 4 部分(21 – 27 行)为客体间关联度的计算,依据 $assoc_{\min}$ 来确定高关联度的客体. MAOA_HFA 算法复杂度为 $o(|a|\cdot|b|)$.

3 关联客体聚合信息级别的推演

信息聚合后能否推导出高级别信息,是限定用户访问的关键[8,9].因此,本文在客体关联性发现的基础上,通过关联属性级别模糊集可能性测度对关联客体推导出更高级别信息的可能性进行了评估.

定义 7 设 $F=\{f_{c_1},f_{c_2},\cdots,f_{c_k}\}$ 为属性空间 A 上的模糊集,f_{c_i} 代表不同安全级别属性集合,C_i 为安全级别,令 X 为 A 上取值的变量,与 X 有关的可能性分布,记为 $\prod_x$,$\prod_x$ 的可能性分布函数用 π_X,并在数值上定义等于 F 的隶属度,即 $\forall u\in A$,$\pi_X(u)=F(u)$.

定义 8 设 B 为安全级别 $C(f_{c_i})$ 的 A 上的模糊集,$\prod_x$ 是与变量 X 有关联的可能性分布,而 X 在 A 中取值,则 B 的可能性测度定义为:

$Poss(X\ is\ B)\cong\bigvee_{u\in A}(B(u)\wedge\pi_X(u))$.其中,$B(u)$为 B 的隶属函数;$\pi_X(u)$为与 X 有关的可能性分布函数.

定义 9 关联客体推导出更高安全级别信息的可能性为关联属性子集在高于关联客体最大安全级别的模糊集上的可能性测度与其权值的乘积和.

$$Pro=\sum_{i=1}^{k}w_i(Poss_i(X\ \text{is}\ B\,|\,C(B)>\max(C(A_1),C(A_2),\cdots)).$$

其中,k 为强关联属性子集 A_i 的个数;$Poss(\,)$为高于所有关联属性最高安全级别的模糊集可能性测度;w_i 为关联属性推出更高级别信息的可能性权值,w_i 定义为:

$$w_i=I_i(G[i,1],G[i,2])/\sum_{j=1}^{k}I_j(G[j,1],G[j,2]).$$

其中,$I(G[i,1],G[i,2])$为 $G[i,1]$与 $G[i,2]$的互信息[10].

定义 10 $Pro\geqslant\tau$,则认为这些关联客体为不兼容性客体.τ 指的是关联客体推导出安全级别为 C_i(高于关联客体的最大安全级别)的信息可能性阈值.即关联客体不能被级别 $<C_i$ 的主体同时访问.

据此,本文给出了关联客体聚合信息级别推演算法 LIAAI_AO(Level Inference Algorithm of Aggregated Information on Associated Objects).

算法 3　关联客体聚合信息级别推演算法 LIAAI_AO

Input: $G[d]$(tuple of associated attribute pair)
Output: pro, flg
(1) $flg = C_1$; $p = 0$;
(2) $C = \max(C(G[d]))$; //maximum level of associated attributes
(3) $j = \min(\{i \mid f_{C_i} \in F, C_i > C\})$;
(4) for $i = j$ to k do
(5) begin
(6)　$B = f_{C_j}$; $\prod_x = \{matrix(X) \mid C < j\}$;
(7)　for $s = 1$ to d do
(8)　begin
(9)　　computing w_s by $G[s]$;
(10)　　computing $Poss_s(X \text{ is } B)$ by $\prod_x$ and B;
(11)　$Pro = w_s * Poss_s(X \text{ is } B)$; $p = + Pro$; $s = s + 1$;
(12)　endfor
(13)　for $t = 1$ to $k - 1$ do
(14)　begin
(15)　if $Pro \geqslant \tau_t$ and $C(\tau_t) > C$ then return($flg = j$; pro);
(16)　endfor
(17) endfor

算法分为 2 部分. 第 1 部分(1 – 2 行)为客体关联属性子集的最大安全级别 C 的获取;第 2 部分(4 – 17 行)为聚合信息推导更高级别信息可能性的评估,若 $Pro \geqslant \tau$,则返回 Pro 和相应的安全级别. LIAAI_AO 算法复杂度为 $o(k * d)$.

4　仿真实验分析

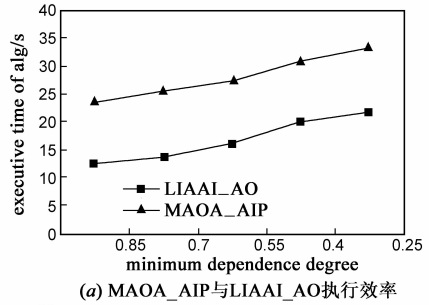
为了说明本文所提出的推演方法的执行效果,我们对推演方法进行了仿真实验,实验数据来源于本单位具有安全级别的科研性文档以及人工合成文件,人工合成文件的目的有两种,一种是为了产生与实际文件内容关联的文件,一种是将实际文件分割为不同的关联文件. 实验评估的指标为算法执行效率、算法推演合理性等.

4.1　算法执行效率分析

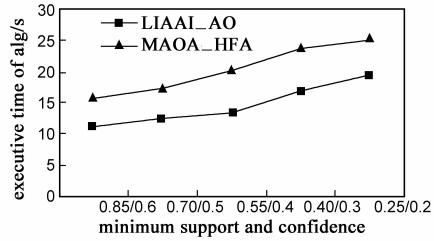
本文从阈值和客体规模变化两个方面对客体关联发现算法以及推演算法进行了性能评估.

图 1 为客体规模 1600 个、阈值变化情况下算法的执行效率. 图 1(a)为第三种关联关系下,MAOA_AIP 和 LIAAI_AO 算法的执行效率,从实验结果看,随着 $\gamma_{\min}$的递减,算法执行时间逐步递增,这是由于关联属性集增多,客体关联度计算量增大. 图 1(b)为第四种关联关系下, MAOA_HFA 和 LIAAI_AO 算法的执行效率,从实验的结果看,随着 $sup_{\min}$和 $conf_{\min}$的递减,算法执行时间增多,这由于属性集频繁项增多的原因. 从图 1 也可看出,当 $\gamma_{\min}$和 $sup_{\min}$相同情况下,MAOA_HFA 执行效率高于 MAOA_AIP,即参数一致的情况下,发现第四类关联关系,MAOA_HFA 优于 MAOA_AIP.

图 2 为 $\gamma_{\min} = 0.4$, $sup_{\min} = 0.4$, $conf_{\min} = 0.6$ 下,三个算法随客体规模变化时的执行效率. 从实验结果看,随着客体数量的增加,算法执行效率相应增加,这是由于客体增多,属性关联复杂度越大,发现的属性关联集越多,计算复杂度就会相应增大.



(a) MAOA_AIP与LIAAI_AO执行效率



(b) MAOA_HFA与LIAAI_AO执行效率

图1　阈值变化情况下算法执行效率

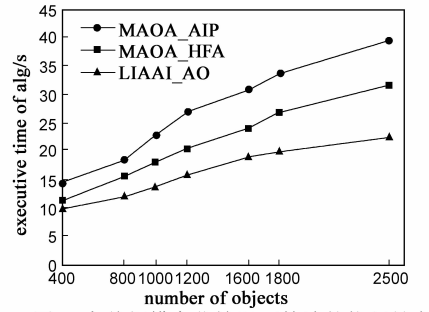


图2　客体规模变化情况下算法的执行效率

4.2　推演方法合理性分析

假定在仿真实验客体中,由人工分析获得的标准不兼容性客体元组集合为 S,推演方法推导出的不兼容性客体元组集合为 T.

依据 S 和 T,则有:①正确率 $VR = |S \cap T| / |S|$;②误差率 $ER = |S - (S \cap T)| / |S|$;③错误率 $FR = |T - (S \cap T)| / |S|$. VR、ER 反映该方法能够推演出不兼容性客体的准确性,且 $ER = 1 - VR$;而 FR 反映方法推演出的假的不兼容性客体的错误率.

表 1、表 2 为阈值、客体规模变化情况下,推演方法正确率、错误率分析. 表的左半部分为 MAOA_ AIP 与 LIAAI_AO 算法对第三(上)、第四(下)种关联关系的分

析;表的右半部分为 MAOA_HFA 与 LIAAI_AO 算法对第四种关联关系的分析;从实验结果看,在本文特定的实验条件下,推演方法均可在一定程度上挖掘出具有关联关系的客体,错误率在 2% 左右,属于可接受的范畴.通过左右两部分实验数据可知,在相同的条件下,针对第四种关联关系的分析,MAOA_HFA 算法要优于 MAOA_AIP 算法,这说明了采用域内支持度来分析,不仅在算法性能方面,而且在准确性方面会更好.通过对比表 1、表 2 可知,阈值降低后,推演方法准确率得到提升,但错误率有所提高.这说明阈值设置越高,放行客体越多,准确率会降低,易于导致泄密;若阈值设置较低,则冗余客体较多,错误率会提升,将影响访问控制系统的执行效率.因此,如何设置合理的阈值,权衡 *VR* 与 *FR* 是分析客体关联性,防止信息聚合泄密的关键,这也是下一步研究的难点.

表 1 $\gamma_{\min}=0.7, sup_{\min}=0.7, conf_{\min}=0.6, assoc_{\min}=0.65$ 下推演方法的 *VR*、*FR*(%)

τ \ n	MAOA_AIP 与 LIAAI_AO 算法						MAOA_HFA 与 LIAAI_AO 算法					
	1200		1600		2500		1200		1600		2500	
	VR	FR	VR	FR	VR	FR	VR	FR	VR	FR	VR	FR
$\tau_{内文}=0.75$	72.92 65.71	2.08 0.00	84.62 70.45	1.54 2.27	86.11 68.52	1.39 1.85	77.14	0.00	81.82	0.00	79.62	1.85
$\tau_{秘密}=0.7$	77.50 67.86	0.00 0.00	76.79 68.42	1.79 2.63	81.82 71.11	1.52 2.22	82.14	0.00	78.95	2.63	77.78	0.00
$\tau_{机密}=0.65$	70.67 67.24	1.33 1.72	81.63 66.67	2.04 1.51	86.26 70.83	1.53 2.08	79.31	1.72	74.24	0.00	81.25	1.04
$\tau_{绝密}=0.5$	85.00 67.50	1.67 0.00	77.94 64.58	1.47 2.08	84.62 71.43	1.28 1.78	77.50	0.00	75.00	2.08	80.35	1.78

表 2 $\gamma_{\min}=0.25, sup_{\min}=0.25, conf_{\min}=0.3, assoc_{\min}=0.4$ 下推演方法的 *VR*、*FR*(%)

τ \ n	MAOA_AIP 与 LIAAI_AO 算法						MAOA_HFA 与 LIAAI_AO 算法					
	1200		1600		2500		1200		1600		2500	
	VR	FR	VR	FR	VR	FR	VR	FR	VR	FR	VR	FR
$\tau_{内文}=0.75$	89.58 85.71	2.08 0.00	92.31 79.55	3.08 2.27	94.44 81.48	4.17 3.71	94.29	0.00	90.09	2.27	88.89	3.71
$\tau_{秘密}=0.7$	87.50 78.57	2.50 0.00	91.07 81.58	5.35 2.63	92.42 84.44	3.03 2.22	89.29	3.57	86.84	2.63	91.11	2.22
$\tau_{机密}=0.65$	93.33 81.03	5.33 3.45	95.91 78.79	5.11 3.03	90.07 83.33	4.58 3.13	89.65	3.45	92.42	3.03	88.54	2.08
$\tau_{绝密}=0.5$	91.67 75.00	1.67 0.00	88.24 77.08	2.94 2.08	93.59 85.71	2.56 1.78	87.50	0.00	91.67	4.16	92.86	1.78

5 结束语

本文通过对客体关联性发现,依据属性子集级别模糊集可能性测度对关联客体能否推导出更高级别信息的可能性进行了推演.该研究将改变多级安全网络边界安全防护的基本原则,使其拓宽到客体关系上来,以有效控制多级安全网络中主体对客体的访问,进一步降低系统失泄密的风险.

当然,客体聚合还有许多方面待于研究,如主体共谋泄密等,我们也将在此做进一步的研究.

参考文献

[1] 秦超,陈钟,等.中国墙策略及其在多级安全中的应用[J].北京大学学报,2002,38(3):369 – 374.
Qin chao, Chen zhong, et al. Chinese wall policy and its extension in multilevel security system[J]. Acta Scientiarum Naturalium Universitatis Pekinensis, 2002, 38(3): 369 – 374. (In Chinese)

[2] Q Ni, E Bertino, J Lobo. Risk-based access control systems built on fuzzy inferences[A]. Proceedings of the 5th ACM

Symposium on Information, Computer and Communications Security[C]. New York: ACM, 2010. 250 – 260.

[3] Vasilios Katos, Dimitrios Vrakas, et al. A framework for access control with inference constraints[A]. Proceedings of the 35th IEEE Annual Computer Software and Applications Conference [C]. Munich: IEEE, 2011. 289 – 297.

[4] J Threet. Designing secure relational databases[D]. Oklahoma, USA: University of Tulsa. 1993.

[5] Emilin C, Swamynathan S. Reason based access control for privacy protection in object relational database systems[J]. International Journal of Computer Theory and Engineering, 2011, 3 (1): 32 – 37.

[6] 曹利峰,陈性元,杜学绘,等.基于聚类分析的客体聚合信息级别推演方法[J].电子与信息学报,2012,34(6):1432 – 1437.
Cao Li-feng, Chen Xing-yuan, Du Xue-hui, et al. A level inference method for aggregated information of objects based on clustering analysis [J]. Journal of Electronics & Information Technology, 2012, 34(6): 1432 – 1437. (in Chinese)

[7] 苗夺谦,李道国.粗糙集理论、算法与应用[M].北京:清华大学出版社.2008. 2 – 7.
Miao Duo-qian, Li Dao-guo. Rough Sets Theory, Algorithms and Applications [M]. Beijing: Tsinghua University Press. 2008. 2 – 7. (in Chinese)

[8] 刘雄,卓雪君,汤永利,戴一奇.一种基于通道容量的多级安全模型[J].电子学报,2010,38(10):2460 – 2464.
Liu Xiong, ZHUO Xue-jun, TANG Yong-Li, DAI Yi-qi. A Multilevel Security Model Based on Communication Channel Capacity[J]. Acta Electronica Sinica, 2010, 38 (10): 2460 – 2464. (in Chinese)

[9] 李凤华,苏 ▮,等.访问控制模型的研究进展与发展趋势[J].电子学报,2012,40(4):805 – 813.
LI Feng-hua, Su Mang, et al. Research status and develop ment trends of access control model[J]. Acta Electronica Sinica, 2012, 40(4): 805 – 813. (in Chinese)

[10] 付钰,吴晓平,等.基于模糊集与熵权理论的信息系统安全风险评估研究[J].电子学报,2010,38(7):1489 – 1494.
FU Yu, WU Xiao-ping, et al. An approach for information system security risk assessment on fuzzy set and entropy-weight[J]. Acta Electronica Sinica, 2010, 38 (7): 1489 – 1494. (in Chinese)

作者简介

曹利峰　男,1981 年 7 月出生,河南禹州人.2005 年获解放军信息工程大学硕士学位,现为解放军信息工程大学讲师、博士生.研究方向为网络安全.
E-mail: caolf302@sina.com

陈性元　男,1963 年 11 月出生,安徽无为人.教授,博士生导师.2003 年获解放军信息工程大学博士学位,现为解放军信息工程大学三院院长,研究方向为信息安全、分布式操作系统.