一种基于访问历史的 BLP 模型*)

李瑞轩　赵战西　王治纲　卢正鼎
(华中科技大学计算机科学与技术学院　武汉 430074)

摘　要　针对经典的 BLP 模型无法控制间接信息流的缺点，借鉴信息流模型的思想，在系统状态中增加记忆分量，记录主体所读的客体，控制信息向安全的方向流动。为了提高 BLP 模型的可用性并增强信息的完整性，将主体的安全级扩充为读写分离的安全级区间。通过这些方法将 BLP 模型改造成为具有记忆能力的新型多级安全模型。

关键词　BLP 模型，信息流模型，访问历史，安全级区间

A BLP Model Based on Access History

LI Rui-Xuan　ZHAO Zhan-Xi　WANG Zhi-Gang　LU Zheng-Ding
(College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan 430074)

Abstract　In order to control the indirect information flow, this paper employs the idea of the information flow model, and adds the memorial factor in the system states to record the read objects and to control the direction of information flow. In order to improve the availability and the information integrity of the model, this paper also extends the security level of the subjects into separated reading and writing security level ranges. By using these methods, we develop the BLP Model into a new Multi-level Security Model with memory ability.

Keywords　BLP model, Information flow model, Access history, Security level range

1　引言

在安全系统的设计和分析中，安全模型是一个重要的概念，它体现了系统中应该执行的安全策略。BLP 模型是著名的安全模型，由 Bell 和 La Padula 在第一次联合设计安全的多用户操作系统时提出[1]。它是定义多级安全性(MLS)的基础，被视作基本安全公理。

在 BLP 模型中，系统元素根据特性被划分为客体和主体。每个主体和客体都被分配了一个安全级，安全级由一个分层的密级和一个非分层的范围组成。主体按照"向下读，向上写"的原则访问客体，即只有当主体的密级不小于客体的密级并且主体的范围包含客体的范围时，主体才能读取客体中的数据；只有当主体的密级不大于客体的密级并且主体的范围包含于客体的范围中时，主体才能向客体中写数据[1,2]。

BLP 模型是以军事部门的安全控制作为其实现基础的，它恰当地体现了军事部门的安全策略，然后被应用到计算机的安全设计中来。BLP 模型也曾显露出某些方面的不足[3]，如不具备记忆性，无法控制间接信息流。此外，BLP 模型在机密性、信息的完整性和可用性等方面也还存在一些缺陷。

本文借鉴 Denning 的信息流模型[4]的思想，提出一个具有记忆性的多级安全模型。该模型对主体的安全级进行扩充，将主体的安全级分离为相互独立的读写区间。在状态中增加记忆性分量，主体读客体时，记录主体所读的客体；主体写客体时，首先判断信息能否从主体已读客体流向所写客体，然后决定是否允许主体向客体写。依据这些方法，提高了信息的完整性和系统的灵活性，并杜绝了隐蔽的信息泄漏。

2　经典 BLP 模型的改进策略

约定 1　$\underline{C}$是等级分类集合，$\underline{C}=\{c_0,c_1,\cdots,c_n\}$，$c_0<c_1<\cdots<c_n$。$K$ 是非等级类别集合。$\underline{L}$ 为所有安全级集合，$\underline{L}=(c,K)$，其中，$c\in\underline{C}$，$K\subseteq\underline{K}$。$\underline{S}$ 是主体集合，$\underline{O}$ 是客体集合。$u\in\underline{S}$，$o\in\underline{O}$，o 的安全级为 $L_o=(c_o,K_o)$，其中，$c_o\in\underline{C}$，$K_o\subseteq\underline{K}$。

对经典 BLP 模型的改进主要依据以下几个方面：

(1)BLP 模型不具备记忆性，没有保留主体的访问历史记录。如果按照经典模型中当前的状态来决定主体能否访问某一客体，则会存在隐秘通道，造成信息泄露。

最初，BLP 模型是模拟计算机的，这里的主体(进程)没有自己的记忆，它们所"知道"的唯一事情是它们被允许查看的客体(文件)的内容。但是当把主体看成人或者特洛伊木马时，这个观点就不合情理了。

改进的方法就是在状态中增加记忆分量。使状态由原来的当前访问集合、访问矩阵集合、敏感标记函数集合和客体层次关系集合 4 个分量，扩展为加上记忆集合的 5 个分量。

主体读客体时，记录主体所读的客体。主体写客体时，首先判断信息能否从已读客体流向所写客体，然后决定是否允许主体向客体写。判断操作就是比较已读客体和当前客体的安全级的大小，如果已读客体的安全级小于当前客体的安全级，允许信息流动，否则不允许。注意：客体的安全级并不是一成不变的。当主体发现客体已经公开时，可以从记忆集合中删除该客体。

(2)BLP 模型中"向上写"的策略使低安全级主体篡改敏感数据成为可能，破坏信息的完整性。必须限制低安全级主

*)国家自然科学基金资助项目(项目编号：60403027)、国家"十五"科技攻关计划项目(项目编号：2002BA103A04)。李瑞轩　博士，副教授，研究方向为分布式异构系统、分布式系统安全；赵战西　硕士研究生，研究方向为分布式异构系统中的安全；王治纲　博士研究生，研究方向为分布系统安全；卢正鼎　教授，博士生导师，主要研究领域为分布式系统、智能信息系统、信息安全。

体向高安全级数据写的能力。“向下读”的策略限制了高安全级主体向非敏感客体写数据的合理要求，降低系统的可用性。必须允许主体可以根据客体的情况，拥有一定范围的写能力。

改进的方法就是将主体的安全级限制在一个区间之内，即限制主体的最低安全级、最高安全级。这样，主体 u 的安全级就是一个安全级区间：$L_u=[L_L,L_H]$，L_L 为 u 的最低安全级，L_H 为 u 的最高安全级，且 $L_L、L_H\in\underline{L}$

(3)BLP 模型中主体的读写权限往往不同，因此读写采用统一安全级的做法不够合理。改进的方法就是将主体的读写权限分开[6]，分别标记为 c_R(读密级)、c_W(写密级)、K_R(读部门集)和 K_W(写部门集)，$c_R、c_W\in\underline{C}$，$K_R、K_W\subseteq\underline{K}$。这样主体 u 就有两个安全级：读安全级 $L_R=(c_R,K_R)$ 和写安全级 $L_W=(c_W,K_W)$，$L_R、L_W\in\underline{L}$。

至此，主体的安全级为：$L_u=(L_{RH},L_{RL},L_{WH},L_{WL})$，$L_{RH}$ 为 u 的最高读安全级，L_{RL} 为 u 的最低读安全级，L_{WH} 为 u 的最高写安全级，L_{WL} 为 u 的最低写安全级，且 $L_{RH}、L_{RL}、L_{WH}、L_{WL}\in\underline{L}$。注意，客体的安全级定义保持不变。

这里设定，$L_{RH}\geqslant L_{RL}$，$L_{WH}\geqslant L_{WL}$，$L_{WH}\geqslant L_{RH}$，$L_{WL}\geqslant L_{RL}$，$L_{RH}\geqslant L_{WL}$。由此可知，主体的只读安全级区间为$[L_{RL},L_{WL}]$，只写安全级区间为$(L_{RH},L_{WH}]$，读写安全级区间为$[L_{WL},L_{RH}]$。

3 改进的 BLP 模型的形式化描述

与经典的 BLP 模型一样，改进的 BLP 模型也是一个有限状态机模型，形式化地定义了系统状态及状态间的转换规则。

约定 2 设 X 和 Y 是任意集合，记 $P(X)$为 X 的幂集，记 $X^Y:=\{f|f:Y\to X\}$为 Y 到 X 的函数集合。

约定 3 $\underline{A}$ 是访问方式集合，$\underline{S}_T$ 是可信主体集合，$\underline{S}'=\underline{S}-\underline{S}_T$ 为不可信主体集合。

定义 1

当前访问集合$\underline{B}:=P(\underline{S}\times\underline{O}\times\underline{A})$。

访问矩阵集合$\underline{M}:=\{M|M$ 是矩阵 $\wedge$ M 中元素 M_{ij} 是主体 s_i 对客体 o_j 的访问方式集$\}$。

安全级集合$\underline{L}:=\{(c,K)|\ c\in\underline{C}\wedge K\in\underline{K}\}$，$L_1=(c_1,K_1)\in\underline{L}$，$L_2=(c_2,K_2)\in\underline{L}$，$(L_1\geqslant L_2):=(c_1\geqslant c_2\wedge K_1\supseteq K_2)$。

安全级函数集合$\underline{F}:=\{(f_{RH},f_{RL},f_{WH},f_{WL},f_O)|f_{RH}\in\underline{L}^S\wedge f_{RL}\in\underline{L}^S\wedge f_{WH}\in\underline{L}^S\wedge f_{WL}\in\underline{L}^S\wedge f_O\in\underline{L}^O\wedge(\forall s\in\underline{S}\Rightarrow f_{RH}(s)\geqslant f_{RL}(s)\wedge f_{WH}(s)\geqslant f_{WL}(s)\wedge f_{WH}(s)\geqslant f_{RH}(s)\wedge f_{WL}(s)\geqslant f_{RL}(s)\wedge f_{RH}(s)\geqslant f_{WL}(s))\}$，$f_{RH}$，$f_{RL}$，$f_{WH}$，$f_{WL}$ 称为主体安全级函数，f_O 称为客体安全级函数。

客体层次关系集合$\underline{H}:=\{H|H\in[P(O)]^{\varnothing}\wedge$ 性质 1 $\wedge$ 性质 2$\}$，其中

性质 1：$\forall o_i,o_j\in\underline{O}$ 且 $o_i\neq o_j\Rightarrow H(o_i)\cap H(o_j)=\phi$；

性质 2：$!\ \exists\{o_1,o_2,\cdots,o_n\}\subseteq\underline{O}$，使得 $\forall i(1\leqslant i\leqslant n\Rightarrow o_{i+1}\in H(o_i))\wedge(o_{n+1}\equiv o_1)$。

主体访问记忆集合$\underline{RM}:=\{o|o\in B(s:r,w)\}$，其中，$B(s:r,w)$表示主体 s 以访问权限 r，w 访问过的客体的集合。

状态集合 $V:=\{(b,M,f,H,rm)|\ b\in\underline{B}\wedge M\in\underline{M}\wedge f\in\underline{F}\wedge H\in\underline{H}\wedge rm\in\underline{RM}\}$。

定义 2 设 R 是请求集合，D 是判定集合，V 是状态集合，T 是状态序号集合，定义：

系统$\Sigma(R,D,W,z_0):=\{(x,y,z)|\ x\in R^T\wedge y\in D^T\wedge z\in V^T\wedge(t\in T,(x_t,y_t,z_t,z_{t-1})\in W)\}$，其中，$W\subset R\times D\times V\times V$，$z_0$ 是初始状态，$T=\{1,2,\cdots,i,\cdots\}$，记号 x_t 相当于 $x(t)$，其他类推。

定义 3 $(v\in V)[v$ 是安全状态$:=(v$ 满足 ss-特性$)\wedge(v$ 满足相对于$\underline{S}'$的 $*$-特性$)\wedge(v$ 满足 ds-特性$)]$。

$(z\in V^T)(z$ 是安全状态序列$:=\forall t\in T(z_t$ 是安全状态$))$。

$\Sigma(R,D,W,z_0)$是安全系统$:=\forall(x,y,z)\in\Sigma(R,D,W,z_0)(z$ 是安全状态序列$)$。

约定 4 $b(s:\underline{x},\underline{y},\cdots,\underline{z}):=\{o|(s,o,\underline{x})\in b\vee(s,o,\underline{y})\in b\vee\cdots\vee(s,o,\underline{z})\in b\}$，$s\in\underline{S}$，$o\in\underline{O}$，$\underline{x},\underline{y},\underline{z}\in\underline{A}$。

约定 5 r 为可读不可写方式，a 为可写不可读方式，w 为可读且可写方式，e 为不可读且不可写(可执行)方式。

约定 6 $HIS_S\in\underline{RM}^S$，HIS_S 称为主体访问历史函数。$C_O\in\underline{C}^O$，C_O 称为客体密级函数。

经过上述定义，则公理 1′、2′、3′的形式化描述如下：

公理 1′(ss-特性) 状态 $V:=(b,M,f,H,rm)$满足简单安全特性(ss-特性)：$=s\in\underline{S}\Rightarrow[(o\in b(s:r)\Rightarrow f_{RH}(s)\geqslant f_O(o)\geqslant f_{RL}(s))\wedge(o\in b(s:w)\Rightarrow f_{WH}(s)\geqslant f_O(o)\geqslant f_{WL}(s))]$

公理 2′($*$-特性) 状态 $V:=(b,M,f,H,rm)$满足相对于$\underline{S}'$的 $*$-特性：$=(s\in\underline{S}'\Rightarrow[o\in b(s:a)\Rightarrow f_{WH}(s)\geqslant f_O(o)>f_{RH}(s)\wedge!\ \exists o_i(o_i\in HIS_S(s)\wedge f_O(o_i)>f_O(o))])\wedge$ (1)

$(s\in\underline{S}'\Rightarrow[o\in b(s:w)\Rightarrow f_{RH}(s)\geqslant f_O(o)\geqslant f_{WL}(s)\wedge!\ \exists o_i(o_i\in HIS_S(s)\wedge f_O(o_i)>f_O(o))])\wedge$ (2)

$(s\in\underline{S}'\Rightarrow[o\in b(s:r)\Rightarrow f_{WL}(s)>f_O(o)\geqslant f_{RL}(s)])$。 (3)

公理 3′(ds-特性) 状态 $V:=(b,M,f,H,rm)$满足自主安全特性(ds-特性)：$=(s_i,o_j,x)\in b\Rightarrow x\in M_{ij}$。

公理 1′和公理 2′共同完成强制存取控制部分，即通过安全级来强制性约束主体对客体的存取；公理 3′完成自主存取控制部分，通过存取控制矩阵按用户的意愿来进行存取控制。

4 改进的 BLP 模型规则

经典的 BLP 模型有 10 条规则[1,7]：规则 1、2、3 和 4 分别用于主体请求对客体的 r，a，e 和 w 访问权。规则 5 用于主体释放对某个客体的访问权。规则 6 和规则 7 分别用于主体授予和撤销另一个主体对某客体的访问权。规则 8 用于改变静止客体的安全级。规则 9 和规则 10 分别用于创建和删除(使之成为静止客体)一个客体。

在改进的 BLP 模型中，只有规则 1、规则 2 和规则 4 需要较大的改动(见规则 1′、规则 2′和规则 4′)。其它规则只需在系统状态中增加一个记忆分量，并且要注意安全级函数分量的表示涵义已经改变，状态转换时这两个分量不随状态改变。现说明如下：

约定 7 系统的当前状态为 $v=(b,m,f,H,rm)$，请求通过后系统的状态转变为 $v'=(b',m',f',H',rm')$。

规则 1′用于主体 s_i 请求得到对客体 o_j 的 read 访问权，请求的五元组 $R_k=(\phi,g,s_i,o_j,r)$。

rule 1′:get-read $P_1(R_k,v)\equiv$

if $\sigma_1\neq\phi$ or $\gamma\neq g$ or $x\neq r$ or $\sigma_2=\phi$

then $P_1(R_K,v)=(?,v)$

if $r\notin M_{ij}$

then $P_1(R_K,v)=(\text{no},v)$

if $f_{WL}(s_i)>f(o_j)\geqslant f_{RL}(s_i)$

then $P_1(R_K,v)=(yes,(b\cup\{(s_i,o_j,r)\},M,f,H,rm\cup\{o_j\}))$

else $P_1(R_K,v)=(no,v)$

end

规则 $2'$ 用于主体 s_i 请求得到客体 o_j 的 append 访问权请求的五元组 $R_k=(\phi,g,s_i,o_j,a)$。

rule $2'$:get-append: $P_2(R_K,v)\equiv$

if $\sigma_1\neq\phi$ or $\gamma\neq g$ or $x\neq a$ or $\sigma_2=\phi$

then $P_2(R_K,v)=(?,v)$

if $a\notin M_{ij}$

then $P_2(R_K,v)=(no,v)$

if $\exists o_i(o_i\in HIS_S(s_i)\wedge f_O(o_i)>f_O(o_j))$

then $P_2(R_K,v)=(no,v)$

if $f_{WH}(s_i)\geqslant f(o_j)>f_{RH}(s_i)$

then { $P_2(R_K,v)=(yes,(b\cup\{(s_i,o_j,a)\},M,f,H,rm))$

while $\exists o_i(o_i\in HIS_S(s_i)\wedge C_O(o_i)=c_0)$ do

$P_2(R_K,v)=(yes,(b,M,f,H,rm-\{o_i\}))$

end

}

else $P_2(R_K,v)=(no,v)$

end

规则 $4'$ 用于主体 s_i 请求得到对客体 o_j 的 write 访问权，请求五元组 $R_k=(\phi,g,s_i,o_j,w)$。

rule $4'$:get-write: $P_4(R_K,v)\equiv$

if $\sigma_1\neq\phi$ or $\gamma\neq g$ or $x\neq w$ or $\sigma_2=\phi$

then $P_4(R_K,v)=(?,v)$

if $w\notin M_{ij}$

then $P_4(R_K,v)=(no,v)$

if $\exists o_i(o_i\in HIS_S(s_i)\wedge f_O(o_i)>f_O(o_j))$

then $P_4(R_K,v)=(no,v)$

if $f_{RH}(s_i)\geqslant f(o_j)\geqslant f_{WL}(s_i)$

then { $P_4(R_K,v)=(yes,(b\cup\{(s_i,o_j,w)\},M,f,H,rm\cup\{o_j\}))$

while $\exists o_i(o_i\in HIS_S(s_i)\wedge C_O(o_i)=c_0)$

$P_4(R_K,v)=(yes,(b,M,f,H,rm-\{o_i\}))$

end

}

else $P_4(R_K,v)=(no,v)$

end

5 模型正确性证明

因为改进的 BLP 模型是一个有限状态机模型，如果前一状态是安全状态，经过 BLP 模型的规则转变后的状态也是安全状态，则可说明这一转换规则是安全的。因此，新模型正确性证明的方法就是证明 BLP 模型的 10 条规则是否满足 BLP 公理，在这里只需证明修改较大的 3 条规则。

定理 1 若状态(b,m,f,H,rm)满足 BLP 公理，则由规则 $1'$得到的状态(b',m',f',H',rm')满足 BLP 公理。

证明：

(1)证明规则 $1'$满足 BLP 公理 $1'$

A. 设 $o_k\in b'(s_i:r)$

若 $o_k=o_j$，由规则中的条件知 $f_{WL}'(s_i)>f_O'(o_j)=f_O'(o_k)\geqslant f_{RL}'(s_i)$，又因为 $f_{RH}'(s_i)\geqslant f_{WL}'(s_i)$，所以 $f_{RH}'(s_i)\geqslant f_O'(o_k)\geqslant f_{RL}'(s_i)$；

若 $o_k\neq o_j$，则 $o_k\in b(s_i:r)$，由定理 1 的条件知 $f_{RH}'(s_i)\geqslant f_O'(o_k)\geqslant f_{RL}'(s_i)$。

总之，若 $o_k\in b'(s_i:r)$，则 $f_{RH}'(s_i)\geqslant f_O'(o_k)\geqslant f_{RL}'(s_i)$。

B. 设 $o_k\in b'(s_i:w)$

若 $o_k=o_j$，因为规则 $1'$不改变主体 s_i 对客体 o_k 的 w 访问权，所以在规则 $1'$执行之前必有 s_i 对 o_k 的 w 访问权的授权，即 $o_k\in b(s_i:w)$，由定理 1 的条件知 $f_{WH}'(s_i)\geqslant f'_O(ok)\geqslant f_{WL}'(s_i)$；

若 $o_k\neq o_j$，则 $o_k\in b(s_i:r)$，同上 $f_{WH}'(s_i)\geqslant f_O'(o_k)\geqslant f_{WL}'(s_i)$。

总之，若 $o_k\in b'(s_i:w)$，则 $f_{WH}'(s_i)\geqslant f_O'(o_k)\geqslant f_{WL}'(s_i)$。

由 A 和 B 可知，规则 $1'$满足 BLP 公理 $1'$。

(2)证明规则 $1'$满足 BLP 公理 $2'$

A. 设 $o_k\in b'(s_i:a)$

若 $o_k=o_j$，因为规则 $1'$不改变主体 s_i 对客体 o_k 的 a 访问权，所以在规则 $1'$执行之前必有 s_i 对 o_k 的 a 访问权的授权，即 $o_k\in b(s_i:a)$，由定理 1 的条件知 $f_{WH}'(s)\geqslant f_O'(o)>f_{RH}'(s)\wedge !\exists o_i(o_i\in HIS_S'(s)\wedge f_O'(o_i)>f_O'(o))$；

若 $o_k\neq o_j$，则 $o_k\in b(s_i:a)$，同上 $f_{WH}'(s)\geqslant f_O'(o)>f_{RH}'(s)\wedge !\exists o_i(o_i\in HIS_S'(s)\wedge f_O'(o_i)>f_O'(o))$。

所以，满足公理 $2'$的式(1)。

B. 设 $o_k\in b'(s_i:w)$

若 $o_k=o_j$，因为规则 $1'$不改变主体 s_i 对客体 o_k 的 w 访问权，所以在规则 $1'$执行之前必有 s_i 对 o_k 的 w 访问权的授权，即 $o_k\in b(s_i:w)$，由定理 1 的条件知 $f_{RH}'(s)\geqslant f_O'(o)\geqslant f_{WL}'(s)\wedge !\exists o_i(o_i\in HIS_S'(s)\wedge f_O'(o_i)>f_O'(o))$；

若 $o_k\neq o_j$，则 $o_k\in b(s_i:w)$，同上 $f_{RH}'(s)\geqslant f_O'(o)\geqslant f_{WL}'(s)\wedge !\exists o_i(o_i\in HIS_S'(s)\wedge f_O'(o_i)>f_O'(o))$。

所以，满足公理 $2'$的式(2)。

C. 设 $o_k\in b'(s_i:r)$

若 $o_k=o_j$，由规则中的条件知 $f_{WL}'(s_i)>f_O'(o_j)=f_O'(o_k)\geqslant f_{RL}'(s_i)$，所以 $f_{WL}'(s_i)\geqslant f_O'(o_k)\geqslant f_{RL}'(s_i)$；

若 $o_k\neq o_j$，则 $o_k\in b(s_i:r)$，由定理 1 的条件知 $f_{WL}'(s_i)\geqslant f_O'(o_k)\geqslant f_{RL}'(s_i)$。

所以，满足公理 $2'$的式(3)。

故由 A、B、C 可知，规则 $1'$满足 BLP 公理 $2'$。

(3)证明规则 $1'$满足 BLP 公理 $3'$

设$(s_i,o_k,x)\in b'$，若 $o_k=o_j$，且 $x=r$，则由规则 $1'$中的条件知 $x=r\in M_{ij}=M_{ik}$；若 $o_k\neq o_j$，或 $x\neq r$，则由定理 1 中的条件知 $x\in M_{ik}$，所以规则 $1'$满足 BLP 公理 $3'$。

综上所述，规则 $1'$满足 BLP 公理。证毕。

根据新模型正确性证明的方法，以下两个定理可以使用类似的方法证明。

定理 2 若状态(b,m,f,H,rm)满足 BLP 公理，则由规则 $2'$得到的状态(b',m',f',H',rm')满足 BLP 公理。

定理 3 若状态(b,m,f,H,rm)满足 BLP 公理，则由规则 $3'$得到的状态(b',m',f',H',rm')满足 BLP 公理。

结论 本文通过引入信息流模型的基本思想，提出了一

(下转封三)

一旦源节点收到消息 S_B'，则路径 B 建立成功。

(5)如果路径 A 和 B 建立成功，则建立 RMP 成功，标记 m_g 的状态为 minimal，返回；否则，消息 S_A(或者 S_B)沿原路返回源节点，建立 RMP 失败，标记 m_g 的状态为 misrouting，返回。

下面给出自适应最小容错路由算法：

算法 2 Route()：设源节点为(0,0)，目的节点为(i,j)，$i,j=0$，m_g 为需要路由的消息。

(1)如果 $i=j=0$，销毁消息 m_g，返回。

(2)Set-RMP(m_g)。

(3)如果 m_g 的状态为 minimal，则使用自适应最小路由算法，一旦消息遇到路径 A(或者 B)的边界，则剩下的路由应该沿着路径 A(或者 B)到达目的节点。

(4)如果 m_g 的状态为 misrouting，则使用多阶段最小容错路由算法。

为了使算法满足无死锁，我们可以把整个二维网格分成 4 个虚拟网络：X+Y+，X+Y−，X−Y+，X−Y−。根据源节点和目的节点的相对位置，消息只能选择其中的一个虚拟网络进行路由，不会使用任何其他的虚拟网络。这样，任何网络内部的环相关就被避免，从而使算法满足无死锁的特点。

5 算法性能讨论

提出的算法只需要知道每个节点的局部信息，是分布式的。由于在发送消息前要建立最小通路区，故这个算法在源节点到目的节点需要发送大量信息的时候性能会比较好，而两个路径的建立确保消息能在最小通路区里路由。用来建立最小通路区的时间将被后来的最小路由所弥补。这种方法很像电路交换，电路交换就是在传递消息之前先建立一条通路。

结论 本文研究了二维网格结构的多处理器系统中存在故障情况下的最小容错路由问题，根据最小通路区，提出了存在最小通路的一个充分必要条件，解决了文[4]中未解决的问题，并在此基础上，提出一种启发式自适应最小容错路由算法。本文试图从容错路由算法的最优性上去讨论，尽量使消息能走最优路径，当然为此需要付出一定的代价。我们提出的算法为容错路由提供了重要的选择。

参 考 文 献

1 Dally W J. The J-Machine: System support for actors. Actors: Knowledge-Based Concurrent Computing. MIT Press, 1989

2 Dally W J, Aoki H. Deadlock-free Adaptive Routing in Multicomputer Networks Using Virtual Channel. IEEE Trans Parallel Distrib Syst, 1993. 466～475

3 Boppana R V, Chalasani S. Fault-tolerant Wormhole Routing Algorithms for Mesh Networks. IEEE Trans Comput, 1995, 44(7): 848～864

4 Wu J. Fault-tolerant Adaptive and Minimal Routing in Mesh-connected Multicomputers Using Extended Safety Levels. IEEE Trans Parallel Distrib. Syst, 2000, 11(2): 149～159

5 Wu J. A Fault-tolerant and Deadlock-free Routing in 2D Meshes Based on Odd-even Turn Model. IEEE Trans Comput, 2003, 52(9): 1154～1169

6 Chang H, Chiu G. An Improved Fault-tolerant Routing Algorithm in Meshes with Convex Faults. Parallel Computing, 2002, 28: 133～149

7 Xiang D, Chen A. Flult-tolerant Routing in 2D Tori or Meshes Using Limited-gobal-safety Information. In: Proc. of Int'l Conf on Parallel Processing, 2002

8 Yoshinaga T, Hosogoshi H, Sowa M. Design and Evaluation of a Fault-tolerant Adaptive Router for Parallel Computers. In: Proc. of the Innovative Architecture for Future Generation High-Performance Processors and Systems, 2003

9 Zhou J P, Lau F C M. Multi-phase Minimal Fault-tolerant Wormhole Routing in Meshes. Parallel Computing, 2004, 30: 423～442

10 Boura Y M, Das C R. Fault-Tolerant Routing in Mesh Networks. In: Proc. 1995 Int'l Conf Parallel Processing. IL: Urbana Champion, 1995: I 106～I 109

11 Su C C, Shin K G. Adpative Fault-Tolerant Deadlock-Free Routing in Meshes and Hypercubes. IEEE Trans Computers, 1996, 45(6): 672～683

12 Duato J, Yalamanchili S, Ni L. Interconnection Networks: An Engineering Approach. Elsevier Science Press, 2004

(上接第 288 页)

个改进的具有记忆性的多级安全模型。该模型将主体的安全级分离为相互独立的读写区间，在状态中增加记忆性分量。与经典的 BLP 模型相比，基于访问历史的改进的 BLP 模型有以下优点：

(1)在状态中增加记忆分量。主体读客体时，记录主体所读的客体；主体写客体时，首先判断信息流向是否合法，然后再决定是否接受主体的请求。

(2)将主体安全级变为读写分开的安全级区间。这一区间内含只读区间、读写区间和只写区间。主体本身不能改变自己的安全级。

基于访问历史的多级安全模型可以满足多种实际应用的需要。例如，在安全的企业级信息管理系统和安全的操作系统中采用这种方法，可以增强信息的完整性，提高系统的安全性和系统安全配置的灵活性。在未来的工作中，我们将在分布异构环境的信息共享与交换中应用该模型，以期解决分布异构信息交换中的安全问题。

参 考 文 献

1 Bell D E, LaPadula L J. Secure computer system: Unified exposition and MULTICS interpretation: [Tech Rep]. The MITRE Corporation, MTR-2997 Revision 1, 1976

2 Gligor V D, Burch E L, Chandersekaran C S, et al. On the design and the implementation of secure Xenix work stations. In: Proc. of the 1986 IEEE Symposium on Security and Privacy. Oakland, California: IEEE Computer Society Press, 1986. 102～117

3 Lin T Y. Bell and LaPadula axioms: A "new" paradigm for an "old" model. In: Proc. 1992 ACM SIGSAC New Security Paradigms Workshop. Little Compton, Rhode Island, USA, 1992. 82～93

4 Denning D E. A lattice model of secure information flow. Communications of the ACM, 1976, 19(5): 236～243

5 Bell D E. Secure computer systems: A network interpretation. In: Proceedings of the 2nd Aerospace Computer Security Conference, McLean, 1986, 32～39

6 朱国华，卢正鼎，洪帆. BLP 模型主体敏感标记动态调整方案及其正确性证明. 小型微型计算机系统，2003，24(11)：2012～2015

7 石文昌，孙玉芳，梁洪亮. 经典 BLP 安全公理的一种适应性标记实施方法及其正确性. 计算机研究与发展，2001，38(11)：1366～1372