一个基于网格环境的安全信息流模型

刘益和
(内江师范学院计算机科学学院 内江 641100)

摘 要 网格安全是网格中的一个重要组成部分,它直接影响着网格的发展和网格系统软件的实际应用。为了充分描述网格环境下的信息流动情况,扩展了一般网络环境下的主体、客体,利用客体的组织密级、密级、完整性等级来划分安全类,定义信息流策略,给出了一个基于网格环境的安全信息流模型。经严格的数学证明,新模型满足Denning的信息流模型的有限格和最小上界运算符性质,是合理的、安全的,它是BLP模型、Biba模型对应的信息流模型的扩展,也是一般网络环境下的安全信息流模型的扩展,这对网格安全研究有一定的积极意义。

关键词 网格安全,BLP模型,Biba模型,信息流模型
中图法分类号 TP309 **文献标识码** A

Security Information Flow Model Based on Grid Environment

LIU Yi-he
(College of Computer Science, Neijiang Normal University, Neijiang 641100, China)

Abstract The grid security is an important component, and it directly affects the development of the grid and the practical application of grid system software. In order to fully describe the information flow based on grid environment, a new security information flow model based on grid environment was given, in which the safety class was divided and the information flow policy was defined by using the organization security classifications, classifications, and integrity grade of the object. In this article, the subject and the object were extended, and the concepts of the decomposition of the subject and object, and of organization security classification were defined. The strict mathematics verification shows that this new information flow model satisfies the character of finite lattice and least upper bound operator of the Denning's information flow model, it is reasonable and safe. It is an extension of information flow model contrast to BLP model's and Biba model's, but also the expansion of security information flow model based on the general network environment, and there has some positive significance for the study grid security.

Keywords Grid security, BLP model, Biba model, Information flow model

1 前言

随着互联网技术的迅猛发展,成千上万的各类高性能计算机分布在网上,如何更好地扩展和利用这些网络资源已成为科学家今后研究的方向,这正是网格的发展前景所在。网格安全是网格中的一个重要组成部分,直接影响着网格的发展和网格系统软件的实际应用情况。网格环境下的信息安全是指保密性、完整性和可用性的结合。信息安全模型就是用精确语言描述信息系统的安全策略,正确地综合系统的各类因素,使得系统可以被证明是完整的、反映真实环境的、逻辑上能够实现程序的受控执行的。由此可见,构建合理的信息安全模型既是信息安全的需要,也是完成一个信息安全工程必不可少的手段。目前存在各种信息安全模型,如BLP模型[1]、Biba模型[2]、信息流模型[3]等,它们各有特点,在信息安全形式化描述方面,均起到了非常重要的作用。现有的信息流模型[4-6]主要是在文献[3]的基础上发展起来的,均针对一般网络环境进行安全描述。

目前的网格安全研究主要集中在网格环境中的安全认证、访问控制、数据完整性、通信机密性、用户行为的不可否认性以及单一登录等方面[7-10],在文献[11,12]中讨论了网格工作流等属性,但对网格环境下的信息流研究甚少,针对这一事实,本文利用一般网络环境下的信息流模型特性,引入新的概念,侧重讨论网格环境下信息的安全流动情况。

本文第2节介绍已有的相关概念和已知信息流模型;第3节首先给出新模型所引入的新概念:主客体分解、组织密级、安全函数,其次给出安全类、扩充主客体定义、安全策略、⊕定义等,最后给出模型的描述;第4节给出模型的说明及有关性质的证明;最后是总结。

2 有关概念

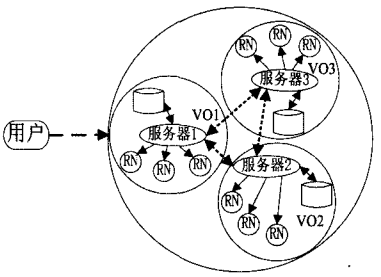
2.1 网格及网格安全

在网格环境中,不同的自治域或虚拟组织组成整个网格计算环境能够对外提供服务,而每个自治域或虚拟组织中的资源节点资源能够协作完成不同的服务,若网格用户所提交

到稿日期:2010-07-28 返修日期:2010-11-12 本文受国家973项目(1999035801),四川省应用基础研究计划课题(04JY029-096),四川省教育厅自然科学重点项目(09ZA055)资助。

刘益和(1964—),男,博士,教授,主要研究方向为信息安全,E-mail:LIU_YIHE@163.com。

的任务在一个自治域或虚拟组织内不能完成时，则该自治域或虚拟组织的网格服务端就请求其他的自治域或虚拟组织的资源节点协作完成，图 1[13]展现了网格安全的物理视图。



RN—资源结点，VO—虚拟组织，⛁—有关资源与信任信息的数据库

图 1　网格安全视图

本文以网格 Globus 环境中 GSI 安全策略[14,15]为基础进行讨论。

2.2　已知的信息流模型

2.2.1　基本概念

首先给出大家熟知的一些概念。

主体和客体：计算机中存在大量涉及安全的操作。凡实施操作的称为主体，如进程，用 $s_1, s_2, \cdots, s_i, \cdots$，或 s 表示，其集合用 S 表示；被操作的对象称为客体，用 $o_1, o_2, \cdots, o_j, \cdots$，或 o 表示，其集合用 O 表示。

设整个网格 Globus 环境中共有 m 个虚拟组织，在这个环境中一个主体代表一个用户或用户进程。虚拟组织 VO_i 对应的本地资源主体集合记为 S_VO_i，对应的本地资源客体集合记为 $O\_VO_i(i=1,2,\cdots,m)$。

安全密级：主体 s_i 的安全密级用 $T(s_i)$ 表示；客体 o_j 的安全密级用 $T(o_j)$ 表示。将主体、客体的安全密级具体量化[6]。

完整性等级：主体 s_i 的完整性等级用 $I(s_i)$ 表示；客体 o_j 的完整性等级用 $I(o_j)$ 表示，将它们具体量化[6]。

需要说明的是，密级函数/完整性等级函数按何种方式定义对后面的讨论影响不大。

当我们给出了主体、客体的密级等级以及有关访问权限后，根据 BLP 模型最主要思想，系统处于安全状态（机密性），需满足：不读上，不写下，即有：

如果 $T(s)\geqslant T(o)$，则主体 s 能读客体 o；如果 $T(s)\leqslant T(o)$，则主体 s 能写客体 o。

当我们给出了主体、客体的完整性等级以及有关访问权限后，根据 Biba 模型严格完整性策略，系统是处于完整状态的，需要满足：允许主体查看高于或等于其完整性级别的客体；修改低于或等于其完整性级别的客体；调用低于或等于其完整性级别客体，即有：

如果 $I(s)\leqslant I(o)$，则主体 s 能读客体 o；如果 $I(s)\geqslant I(o)$，则主体 s 能写客体 o。

2.2.2　Denning 的信息模型

Denning 把一个信息流模型[3] FM 定义为：

$FM=\langle N,P,SC,\oplus,\rightarrow\rangle$

式中，N,P 分别是客体和进程的有限集，SC 是安全类的有限集，类运算符“$\oplus$”是一个满足结合律和交换律的二进制运算符。对任意两个操作数的类，“$\oplus$”指定了它们之间任意二进制函数产生的结果操作数所属的类。流关系“$\rightarrow$”指定了两个安全类之间的信息流动。当且仅当类型 A 中的信息允许流入类 B，记为 $A\rightarrow B$。

信息流模型的安全策略可简单表述为：当且仅当一个操作序列的执行不会产生违反关系“$\rightarrow$”所规定的信息流，那么流模型 FM 是安全的。这一策略在下面假设下，$\langle SC,\rightarrow,\oplus\rangle$ 形成了一个有限格：

(1)$\langle SC,\rightarrow\rangle$是一个偏序集；

(2)SC 是有限集；

(3)SC 有一个下界 L，$\forall A\in SC, L\rightarrow A$；

(4)$\oplus$ 是在 SC 上的最小上界运算符。

最小上界运算符$\oplus$ 有以下性质：

对于所有 $A,B,C\in SC$

(a)$A\rightarrow A\oplus B$ 和 $B\rightarrow A\oplus B$

(b)$A\rightarrow C$ 且 $B\rightarrow C\Rightarrow A\oplus B\rightarrow C$

3　基于网格环境的安全信息流模型

3.1　新的定义

为了给出网格环境下的安全信息流模型，我们给出以下新的定义。

3.1.1　主体、客体分解

在网格环境中，存在网格用户所提交的任务在一个自治域或虚拟组织内不能完成时，该自治域或虚拟组织的网格服务端就请求其他的自治域或虚拟组织的资源节点协作完成的情况，本文特作如下定义。

主体分解表示：当主体 s_i 需要同时访问虚拟组织 $VO_1, VO_2, \cdots, VO_m$ 时，资源代理需要把一个 Globus 主体映射为一个或多个属于本地资源的主体，称 s_i 在虚拟组织中分解表示为 $s_i=(s_i\_VO_1, s_i\_VO_2, \cdots, s_i\_VO_m)$，其中第 k 个分量($k=1,2,\cdots,m$)表示 Globus 主体映射为第 k 个虚拟组织的主体，当 s_i 不需要映射到虚拟组织 VO_j 中时，则记相应的分量为 $s_i\_VO_j\_\phi$。

为了简单起见，本文记：$s_i\_VO_j\in S\_VO_j$，表示 Globus 主体 s_i 已经映射为具有本地性质的虚拟组织 VO_j 的主体。具体的映射策略可参见文献[14]，这里不做讨论。

客体分解表示：当客体 o_j 需要分解到虚拟组织 $VO_1, VO_2, \cdots, VO_m$ 时，称 o_j 在虚拟组织中分解表示为 $o_j=(o_j\_VO_1, o_j\_VO_2, \cdots, o_j\_VO_m)$，其中第 k 个分量($k=1,2,\cdots,m$)为客体 o_j 分解到虚拟组织 VO_k 的部分，如 o_j 不在虚拟组织 VO_i 时，则记相应的分量为 $o_j\_VO_i\_\phi$。

当主体、客体不在一个虚拟组织，用分解的方式表示时，主/客体密级 $T(s)/T(o)$、完整性等级 $I(s)/I(o)$ 演变为 m 维向量函数，其中向量函数的分量的定义仿前一般网络环境中的相关定义，例如：$T(s)=(T(s\_VO_1), T(s\_VO_2), \cdots, T(s\_VO_m))$。

3.1.2　组织密级

组织密级：设把现有的网格按照访问要求划分为 m 个独立的虚拟组织 $VO_1, VO_2, \cdots, VO_m$，每一个虚拟组织赋予不同的安全等级，称为该组织的密级。记为 $net(Net\_name)$，这里 Net_name 为虚拟组织名。

我们约定：$net(VO_i)=\max\limits_{\forall o\in O\_VO_i}\{T(o)\}(i=1,2,\cdots,m)$，即虚拟组织的组织密级为其该组织中的所有客体密级中的最大者。

显然，同一个虚拟组织的客体对应的组织密级 $net(Net\_$

$name$)是相同的，为了方便，此时的组织密级也简记为 $net(o)$。

当客体 o 不属于同一虚拟组织时，$o=(o\_VO_1, o\_VO_2, \cdots, o\_VO_m)$，我们约定：$o$ 对应的组织密级 $net(o)=\max\{T(o\_VO_1), T(o\_VO_2), \cdots, T(o\_VO_m)\}$。

3.1.3 安全函数

客体安全函数：用于描述客体所在虚拟组织密级、密级和完整性等级的超三维向量函数，记为 $T(net(Net_name), T(o), I(o))$或 $T(net(o), T(o), I(o))$。

我们记集合 U，表示超三维安全函数向量构成的全集，即：对于前面定义的组织密级、客体密级和客体完整性等级的所有可能的取值，超三维安全函数向量构成的集合。

3.2 新模型描述

本文提出的网格安全信息流模型定义如下：

$FM=\langle O, S, SC, \oplus, \rightarrow\rangle$是一个具有网格环境的安全信息流模型，信息只能从低密级虚拟组织流向高密级虚拟组织。

其中 O, S 分别为整个网格的客体和进程(即主体)集合，它们是有限集；SC 为模型的安全类，定义在 3.2.1 节；策略$\rightarrow$定义在 3.2.3 节；运算$\oplus$定义在 3.2.4 节。

下面就有关概念分别进行阐述和讨论。

设 O', S'分别为整个网格实有的客体和进程(即主体)集合，它们是有限集。

U' 是根据 3.1.3 节定义的所有实有的超三维安全函数值向量集合；SC'是根据实有的超三维安全函数值来划分的安全类的集合，显然它是有限集，且 $U'\subseteq U$。

3.2.1 安全类 $\#o$

为了简便，我们将客体 o 所在的安全类记为 $\#o$，$\#o=\{o|o\in O$且 $T(\text{net}(o), T(o), I(o))$为同一值$\}$，即 $\forall o'\in \#o$，有：

$$T(net(o'), T(o'), I(o'))=T(\text{net}(o), T(o), I(o))$$

则 $SC'=\{\#o|o\in O'\}$。

下面简单讨论一下集合 U', U，并对 O', S', SC' 进行扩充：

如果 $U'\neq U$，则存在向量 $\alpha\in U$，但 $\alpha\notin U'$，这说明实际客体集合中，不存在这样的客体 o，使得 $T(net(o), T(o), I(o))=\alpha$，为了便于以后的讨论我们引入以下概念。

3.2.2 空客体及空主体

空客体：$\forall\alpha\in U$，但 $\alpha\notin U'$，定义新客体 o，使得 $T(\text{net}(o), T(o), I(o))=\alpha$，该客体除了具有名字，超三维安全函数向量外，不具有其他特征，一个主体访问它时，不会泄漏任何有用的信息，如一个只有文件名的空文件，称 o 为一个空客体，所有这样的空客体组成的集合记为 O'。

空主体：凡进行与上述空客体有关的操作，称为空主体，其集合记为 S'。

前面描述的 $s_i\_VO_j\_\phi, o_j\_VO_i\_\phi$ 实际上可以理解为空主体、空客体。

$\forall o\in O'$，记 $SC''=\{\#o|o\in O'\}$

有了上述关于空客体、空主体以及相应的安全类 SC''的定义，我们以后把它们与相应的普通概念一起使用，不加区别，现在重新记：

$$O=O'\cup O'', S=S'\cup S'', SC=SC\cup SC''$$

3.2.3 安全策略描述

下面给出对新模型的安全策略描述。

设有主体 $s=(s\_VO_1, s\_VO_2, \cdots, s\_VO_m), s\_VO_j\in S\_VO_j$ $(j=1,2,\cdots,m)$，客体 o_1 和 o_2是由主体 s 操纵的两个客体，这里 $o_j=(o_j\_VO_1, o_j\_VO_2, \cdots, o_j\_VO_m)(j=1,2)$，如果有信息从 o_1 流向 o_2，则 o_1 的超三维安全函数被 o_2 的超三维安全函数支配或两个超三维安全函数相等，即：

$\forall o_1, o_2\in O, o_1\rightarrow o_2$ 的充要条件为：$net(o_1)\leqslant net(o_2)$且 $T(o_1)\leqslant T(o_2)$且 $I(o_1)\geqslant I(o_2)$。

进一步说明如下：

(1)$\leqslant, \geqslant$操作含义

$\leqslant, \geqslant$分别为实数的小于等于比较、大于等于比较运算。其中 $T(o_1)\leqslant T(o_2), I(o_1)\geqslant I(o_2)$定义为两个 m 维向量的对应分量进行$\leqslant, \geqslant$操作。

(2)客体不在某虚拟组织分解时的定义

1)若源客体 o_1 中的某一分量为

$o_1\_VO_i\_\phi$，本文定义：

当 $i=1$ 时

$T(o_1\_VO_i\_\phi)=\min\{T(o_1\_VO_2), T(o_1\_VO_3), \cdots, T(o_1\_VO_m)\}$；

$I(o_1\_VO_i\_\phi)=\max\{I(o_1\_VO_2), I(o_1\_VO_3), \cdots, I(o_1\_VO_m)\}$。

当 $i=2,3,\cdots,m$ 时

$T(o_1\_VO_i\_\phi)=\min\{(T(o_1\_VO_1), \cdots, T(o_1\_VO_{i-1}), T(o_1\_VO_{i+1}), \cdots, T(o_1\_VO_m)\}$；

$I(o_1\_VO_i\_\phi)=\max\{I(o_1\_VO_1), \cdots, I(o_1\_VO_{i-1}), I(o_1\_VO_{i+1}), \cdots, I(o_1\_VO_m)\}$。

2)若目的客体 o_2 中的某一分量为

$o_2\_VO_j\_\phi$，本文定义：

当 $j=1$ 时

$T(o_2\_VO_j\_\phi)=\max\{T(o_2\_VO_2), T(o_2\_VO_3), \cdots, T(o_2\_VO_m)\}$；

$I(o_2\_VO_j\_\phi)=\text{mim}\{I(o_2\_VO_2), I(o_2\_VO_3), \cdots, I(o_2\_VO_m)\}$。

当 $j=2,3,4,\cdots,m$ 时

$T(o_2\_VO_j\_\phi)=\max\{T(o_2\_VO_1), \cdots, T(o_2\_VO_{j-1}), T(o_2\_VO_{j+1}), \cdots, T(o_2\_VO_m)\}$；

$I(o_2\_VO_j\_\phi)=\text{mim}\{I(o_2\_VO_1), \cdots, I(o_2\_VO_{j-1}), I(o_2\_VO_{j+1}), \cdots, I(o_2\_VO_m)\}$。

3.2.4 $\oplus$的定义

根据 $\#o$ 的定义，上面的 $o_1\rightarrow o_2$ 也可以写成 $\#o_1\rightarrow\#o_2$。

“$\oplus$”定义如下：

$\forall o_1, o_2\in O, \#o_1\oplus\#o_2=\{o|\ T(net(o), T(o), I(o))=T(\max(net(o_1), net(o_2)), \max(T(o_1), T(o_2)), \min(I(o_1), I(o_2)))\}$，其中 $o\in O$。

其中 $\max(net(o_1), net(o_2))$为两个实数的最大者，$\max(T(o_1), T(o_2))$定义如下：

$$\max(T(o_1), T(o_2))=(\max(T(O_1\_VO_1), T(O_2\_VO_1)), \max(T(O_1\_VO_2), T(O_2\_VO_2)), \cdots, \max(T(O_1\_VO_m), T(O_2\_VO_m)))$$

$\min(I(o_1), I(o_2))$类似定义。

对于上面的假设，3.2 节描述的模型 $FM=\langle O, S, SC, \oplus, \rightarrow\rangle$是一个具有网格环境的安全信息流模型。

4 新模型的说明

下面从几个方面说明新模型的合理性。

4.1 "→"的定义的合理性

首先根据假设，操作客体 o_1 和 o_2 的主体 $s=(s\_VO_1, s\_VO_2, \cdots, s\_VO_m)$，满足 $s\_VO_j \in S\_VO_j$，表示主体有关策略，把主体映射为一个或多个属于本地资源的主体，符合网格安全的最基本的要求。

当 $o_1, o_2 \in O$ 且属于同一个虚拟组织时，$net(o_1)=net(o_2)$，这时 o_1, o_2 的流动方向只需根据这两个客体的密级和完整性等级大小来决定，根据文献[4]的描述，用 $T(o_1)\leqslant T(o_2)$ 和 $I(o_1)\geqslant I(o_2)$ 来定义 $o_1 \rightarrow o_2$，符合一般网络环境安全要求，此时由于信息没有流出虚拟组织，因此符合整个网络设计要求。

当 $o_1, o_2 \in O$ 且不属于同一个虚拟组织时，根据定义只有 $net(o_1) \leqslant net(o_2)$ 且 $T(o_1) \leqslant T(o_2)$ 和 $I(o_1) \geqslant I(o_2)$ 才有 $o_1 \rightarrow o_2$，据 $net(o)$ 的假设，o_1, o_2 只有分别在低密级虚拟组织，高密级虚拟组织内时才满足第一个条件，且 o_1, o_2 还应该满足第二条件即作为普通信息流应具有的条件，才能从低密级虚拟组织流到高密级虚拟组织，这符合一般网络安全设计要求。所以也符合整个网格安全设计要求。

另外，当源客体或目的客体不在某虚拟组织分解时，按其主体、客体密级、完整性等级定义，也符合上述安全讨论要求。

由上分析可知 3.2 节"→"的定义是合理的。

4.2 〈SC,→〉是一个偏序集

定理 〈SC,→〉是一个偏序集。

证明：下面从〈SC,→〉具有自反性、传递性和反对称性 3 方面进行验证。

自反性：$\forall o \in O, o \rightarrow o$。

由于 $T(o\_VO_i) \leqslant T(o\_VO_i), I(o\_VO_i) \geqslant I(o\_VO_i)$ $(i=1,2,\cdots,m)$。

故 $net(o) \leqslant net(o), T(o) \leqslant T(o)$ 和 $I(o) \geqslant I(o)$，所以 $o \rightarrow o$。

传递性：$\forall o_1, o_2, o_3 \in O, o_1 \rightarrow o_2$ 且 $o_2 \rightarrow o_3$，有 $o_1 \rightarrow o_3$。

由 $\forall o_1, o_2, o_3 \in O, o_1 \rightarrow o_2$ 且 $o_2 \rightarrow o_3$

得 $net(o_1) \leqslant net(o_2), T(o_1) \leqslant T(o_2)$ 和 $I(o_1) \geqslant I(o_2)$ 且 $net(o_2) \leqslant net(o_3); T(o_2) \leqslant T(o_3)$ 和 $I(o_2) \geqslant I(o_3)$ 于是有：

$T(o_1\_VO_i) \leqslant T(o_2\_VO_i), I(o_1\_VO_i) \geqslant I(o_2\_VO_i)$ 且 $T(o_2\_VO_i) \leqslant T(o_3\_VO_i), I(o_2\_VO_i) \geqslant I(o_3\_VO_i)$ $(i=1,2,\cdots,m)$。

则 $T(o_1\_VO_i) \leqslant T(o_3\_VO_i), I(o_1\_VO_i) \geqslant I(o_3\_VO_i)$ $(i=1,2,\cdots,m)$。

根据安全策略描述中关于客体不在某虚拟组织分解时的定义，上述讨论适合所有情况下的客体 o_1, o_2, o_3。

从而有 $T(o_1) \leqslant T(o_3)$ 和 $I(o_1) \geqslant I(o_3)$，且显然有 $net(o_1) \leqslant net(o_3)$，故 $o_1 \rightarrow o_3$。

反对称性：$\forall o_1, o_2 \in O, o_1 \rightarrow o_2$，且 $o_2 \rightarrow o_1$，则 $\#o_1 = \#o_2$。

由假设有 $net(o_1) \leqslant net(o_2); T(o_1) \leqslant T(o_2)$ 和 $I(o_1) \geqslant I(o_2)$ 且 $net(o_2) \leqslant net(o_1); T(o_2) \leqslant T(o_1)$ 和 $I(o_2) \geqslant I(o_1)$，于是有：

$T(o_1\_VO_i) \leqslant T(o_2\_VO_i), I(o_1\_VO_i) \geqslant I(o_2\_VO_i)$ 且 $T(o_2\_VO_i) \leqslant T(o_1\_VO_i), I(o_2\_VO_i) \geqslant I(o_1\_VO_i)$ $(i=1,2,\cdots,m)$。

则 $T(o_1\_VO_i)=T(o_2\_VO_i), I(o_1\_VO_i)=I(o_2\_VO_i)$ $(i=1,2,\cdots,m)$。

故 $T(o_1)=T(o_2)$ 和 $I(o_1)=I(o_2)$，而显然有 $net(o_1)=net(o_2)$；根据安全策略描述中关于客体不在某虚拟组织分解时的定义，上述讨论适合所有情况下的客体 o_1, o_2，这说明 o_1, o_2 是同一安全类，即 $\#o_1=\#o_2$。

由上可见〈SC,→〉是一个偏序集。

4.3 SC 的下界

SC 有下界，记为 $\#o_{lowest}$，这里：

$\#o_{lowest}=\{o \mid T(net(o), T(o), I(o)) = T(\min(net(o), \min(T(o)), \max(I(o))), o \in O\}$

其中，$\min(net(Net(o))$ 为所有组织密级中的最小值，$\min(T(o))$，$\max(I(o))$ 分别为客体密级最小值、完整性等级的最大值。

根据扩充的客体、主体和安全类的定义，$\#o_{lowest}$ 始终存在。

由安全策略定义，容易证明：$\forall o \in O, \#o_{lowest} \rightarrow \#o$。

4.4 运算⊕的性质

性质 1 $\forall o_1, o_2, o_3 \in O, \#o_1 \rightarrow \#o_1 \oplus \#o_2, \#o_2 \rightarrow \#o_1 \oplus \#o_2$

证明：(1)由 $net(o_1), net(o_2)$ 定义

$net(o_1)=\max\{T(o_1\_VO_1), T(o_1\_VO_2), \cdots, T(o_1\_VO_m)\}$，

$net(o_2)=\max\{T(o_2\_VO_1), T(o_2\_VO_2), \cdots, T(o_2\_VO_m)\}$

显然 $net(o_1) \leqslant \max(net(o_1), net(o_2)), net(o_2) \leqslant \max(net(o_1), net(o_2))$

(2)由 $\max(T(o_1), T(o_2))$ 定义

$\max(T(o_1), T(o_2)) = (\max(T(o_1\_VO_1), T(o_2\_VO_1)), \max(T(o_1\_VO_2), T(o_2\_VO_2)), \cdots, \max(T(o_1\_VO_m), T(o_2\_VO_m)))$

显然：$T(o_1\_VO_i) \leqslant \max(T(o_1\_VO_i), T(o_2\_VO_i)), T(o_2\_VO_i) \leqslant \max(T(o_1\_VO_i), T(o_2\_VO_i))$ $(i=1,2,\cdots,m)$

则 $T(o_1) \leqslant \max(T(o_1), T(o_2)), T(o_2) \leqslant \max(T(o_1), T(o_2))$。

(3)同理 $I(o_1) \geqslant \min(I(o_1), I(o_2)), I(o_2) \geqslant \min(I(o_1), I(o_2))$。

由⊕定义及上面(1)－(3)的讨论得：$\#o_1 \rightarrow \#o_1 \oplus \#o_2$，$\#o_2 \rightarrow \#o_1 \oplus \#o_2$。

性质 2 $\forall o_1, o_2, o_3 \in O, \#o_1 \rightarrow \#o_3, \#o_2 \rightarrow \#o_3$，则 $\#o_1 \oplus \#o_2 \rightarrow \#o_3$。

证明：(1)由已知有：$net(o_1) \leqslant net(o_3), net(o_2) \leqslant net(o_3)$ 得：

$\max(net(o_1), net(o_2)) \leqslant net(o_3)$

(2)由已知有；$T(o_1) \leqslant T(o_3), T(o_2) \leqslant T(o_3)$，由"≤"定义得：

$\max(T(o_1\_VO_i), T(o_2\_VO_i)) \leqslant T(o_3\_VO_i)$ $(i=1,2,\cdots,m)$

于是有：$\max(T(o_1), T(o_2)) \leqslant T(o_3)$

(3)同理得：$\min(I(o_1), I(o_2)) \geqslant I(o_3)$

由⊕定义及上面(1)－(3)的讨论得：

$\#o_1 \oplus \#o_2 \rightarrow \#o_3$。

结束语 本文利用一般网络环境的安全信息流模型特点，基于网格安全的要素，定义了主体、客体分解表示、组织密级、客体的超三维安全函数等概念，利用客体的超三维安全函

(下转第 199 页)

理、营运管理中心，是整个系统的核心。其具有对全国的物流车辆进行实时监控调度管理，并对有关营运情况的考核和数据的集中管理的功能。总调度指挥中心主要由地理信息系统、监控管理系统、物流运营管理系统、大屏幕显示系统、数据库系统和通信系统等组成。

营运管理平台：通过 2M 数字电路等各种方式与总控制中心互联，在授权范围内对所辖车辆及业务进行管理，查看本部门或公司内部所管辖车辆的营运情况、计划数据、实际数据、各种报表等各种信息。

线路调度室基础平台：通过 ADSL 与总控制中心互联，主要承担对本车队车辆的监控工作。

实时数据处理分析平台：通过对调度信息总控中心的数据库系统中的数据进行分析，并结合采集到的实时数据，可以成功地实现流量统计分析、实时路径规划分析、动态目标的聚类、运动模式分析、动态目标的趋势分类、动态目标的异常点挖掘、基于约束的时空挖掘、分析与预测等功能。因此该平台是整个高效智能物流系统的智能分析核心。

通过这个高效智能物流系统平台，能科学地验证我们提出的各种动态目标模型与算法，为最终找到最佳的解决方案奠定基础。

结束语 目前我国在动态目标管理与分析方面的研究还处于起步阶段，从事这方面研究的人员还不是很多，理论与方法研究的内容基本上还是引进国外的东西多，自己创新的结果少，研究成果的推广应用也不广泛。本文对动态目标的相关研究进行了分析，提出了一个总体框架来建模、管理与分析动态目标，同时对框架进行了深入的分析，最后提出了一个原型系统。未来可在这个框架的基础上，在 GPS 和 RFID 等技术的支持下，丰富传统物流系统在数据分析上的功能，实现物流中动态目标的实时监控与远程信息交换，确保物流中对动态目标高效、及时地查询和检索，突破传统物流管理模式，建立高效的物流管理与跟踪系统。

参 考 文 献

[1] http://www.iso.org/iso/catalogue_detail.htm?csnumber=41445

[2] Sistla A P, Wolfson O, Chamberlain S, et al. Modeling and querying moving objects[C]// Proceedings of the 13th International Conference on Data Engineering (ICDE). Birmingham, UK, April, 1997: 422-432

[3] Beller A. Spatial/Temporal Events in a GIS[C]// Proceedings of GIS/LIS 91. Atlanta, Georgia, 1991

[4] Armstrong M P. Temporality in Spatial Databases[C]// Proceedings of GIS/LIS 88. San Antonio. Texas, November 1988

[5] Worboys M F. Object-Oriented Models of Spatiotemporal Information[C]// Proceedings of GIS/LIS 92. San Jose, California, November 1992

[6] Pitoura E, Samaras G. Locating objects in mobile computing [J]. IEEE Transactions on Knowledge and Data Engineering, 2001, 13(4): 571-592

[7] Sistla A P, Wolfson O, Chamberlain S, et al. Querying the uncertain position of moving objects, Temporal databases: Research and Practice[C]// Lecture Notes in Computer Science. Springer Verlag, 1998: 310-337

[8] Chon H D. Storage and retrieval of moving objects[C]// LNCS. 2001: 173-184

[9] Gaede V, Günther O. Multidimensional access methods [J]. ACM Computing Surveys, 1998, 30(2): 170-231

[10] Betty S, Tsotras V J. A comparison of access methods for temporal data[J]. ACM Computing Survey, 1999, 31(2): 158-221

(上接第 160 页)

数值来定义信息流策略，描述了一个基于网格环境下的新的信息流模型，通过分析和证明可以看出，它是安全的、合理的，利用该模型可以较好地反映网格环境下的信息流动情况，这有利于网格安全环境下的信息流动描述。由于网格环境过于复杂，加之版面篇幅所限，本文所描述的信息流模型的应用实例将另文研究。

参 考 文 献

[1] Bell D E, Lapadula L J. Secure compter system: Mathematical foundation[R]. MTR-2527. Mitrecorp, Bedford, MA, 1973

[2] Biba K. Integrity Considerations for Secure Computing Systems [R]. MTR-3153. Mitre Corporation, Bedford, MA, 1975

[3] Denning D E. A lattice model of secure information flow[J]. Communications of the ACM, 1976, 19(5): 236-243

[4] Ravi S. Sandhu. Lattic-Based Access Control Model[J]. IEEE computer, 1993, 26(11): 9-19

[5] 刘益和，沈昌祥. 一个信息安全函数及应用模型[J]. 计算机辅助设计与图形学学报，2005，17(12)：2734-2738

[6] 李焕洲，刘益和，李华. 基于信任和安全等级的 P2P 信息流模型[J]. 计算机应用，2008，28(12)：2168-3170

[7] 靳楠. 网格安全认证关键技术研究[D]. 南京：南京邮电大学，2006

[8] Oo M P, Naing T T. Access Control System for Grid Security Infrastructure[C]// 2007 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology-Workshops. 2007: 299-302

[9] 韩兵. 网格环境下的数据管理及安全问题研究[D]. 合肥：中国科技大学，2006

[10] Huang Xiao-qin, et al. An Identity-Based Model for Grid Security Infrastructure[C]// ISSADS2005, LNCS3563. Berlin Heidelberg: Springer-Verlag, 2005: 258-266

[11] Bivens H. Grid work flow[R]. Albuquerque: Sandia National Laboratory, 2001

[12] 周建涛，叶新铭. 网格工作流及其关键技术研究综述[J]. 内蒙古大学学报：自然科学版，2008，39(5)：581-589

[13] 王芳. 网格环境下的信任机制研究[D]. 南京：南京邮电大学，2009：52-53

[14] 都志辉，陈渝，刘鹏. 网格计算[M]. 北京：清华大学出版社，2002

[15] The Globus Project [EB/OL]. http://www.globus.org/