第34卷 第10期 计 算 机 工 程 2008年5月
Vol.34 No.10 Computer Engineering May 2008
·软件技术与数据库· 文章编号：1000—3428(2008)10—0055—03 文献标识码：A 中图分类号：TP311.5

基于知识库的智能策略翻译技术

代向东，陈性元，吴 蓓，王永亮
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：提出基于知识库的策略翻译方法，设计策略翻译组成结构，分析策略知识及其表示形式，建立动态可扩展的策略知识库，开发可扩展的策略编译器和策略组装器。实例测试表明，该技术实现了策略翻译的智能化，解决了各种设备的策略不能统一管理的问题。
关键词：知识库；智能；组装；策略翻译

Intelligent Policy Transformation Technique Based on Knowledge Base

DAI Xiang-dong , CHEN Xing-yuan , WU Bei , WANG Yong-liang
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】This paper proposes a policy transformation method based on knowledge base, designs the composing structure of the policy transformation, analyzes the policy knowledge and its specification, builds the dynamic and extensible knowledge base, and develops the flexible policy compiler and policy assembler. Test shows that the technology implements the intelligent policy transformation, and solves the problem that policies of various devices can not be uniformly managed.
【Key words】knowledge base; intelligence; assemble; policy transformation

1 概述

目前，许多研究机构和知名公司正致力于策略管理的研究，并产生了一些基本思路和技术[1]，公布了相关标准。但是，这些标准大多针对服务质量，只是给出了相关草案，没有成熟的RFC文档，策略管理产品也只是对单个厂商的设备来实施策略管理，其面临的问题为：(1)策略描述问题，由于没有统一的策略标准，各设备厂商各自为政，使用自己的协议进行管理，因此无法做到统一的策略描述；(2)策略翻译[2]问题，统一的策略描述语言需要转换为各设备厂商自己的策略表示形式，才能被正确执行，当前，还没有一种很好的解决方法。

针对问题(2)，笔者借鉴人工智能[3]专家系统的一般结构和编译原理[4]的思想，提出了基于知识库的策略翻译思想，科学、合理地设计灵活、通用的策略编译器，编译统一描述的策略；建立动态可扩展的策略知识库，为策略的组装提供依据；构建高效、可靠的策略组装器，将编译的结果和策略知识进行组装，最终实现智能的策略翻译。

2 策略翻译的组成结构

策略翻译主要由人机接口、词法获取机构、知识获取机构、词法库、策略知识库、策略编译器和策略组装器等组成，如图1所示。人机接口是联系策略翻译与管理员间的纽带，它由一组程序组成，用于完成输入工作。用户通过它编辑策略，输入词法和策略知识，更新、完善词法库和策略知识库。词法获取机构的基本任务是扩充词法库，把统一描述策略语言的关键词输入词法库，增强策略翻译的可扩展性，使其能够支持多种类型的网络安全设备的策略。知识获取机构的基本任务是把策略知识输入策略知识库，并负责维持策略知识的一致性、完整性，建立科学的策略知识库。策略编译器对统一描述的策略进行词法和语法检查，生成中间策略。策略组装器将中间策略和策略知识进行组装，最终生成目标策略。目标策略即各设备厂商的策略。

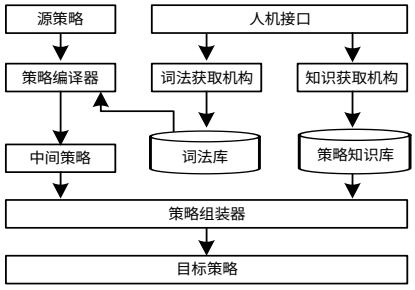

图1 策略翻译组成结构

3 策略知识库的设计

策略知识库是实现智能策略翻译的核心，策略知识是知识库的组成单元。管理员需将各种策略知识输入策略知识库。因此，必须科学合理地表示策略知识，才能使策略的组装准确高效地进行，从而完成目标策略的生成任务，实现智能的策略翻译。

3.1 策略知识定义

定义1 知识是有关信息关联在一起形成的信息结构。

定义2 策略知识就是把有关各个网络安全设备的策略规范关联在一起所形成的信息结构，它反映了各个网络安全设

基金项目：国家“863”计划基金资助项目(2006AA701110)
作者简介：代向东(1977－)，男，讲师，主研方向：信息安全，策略管理；陈性元，教授、博士、博士生导师；吴 蓓，博士研究生；王永亮，硕士研究生
收稿日期：2007-07-25 **E-mail：**daixiangdong77@126.com

备策略的组织形式。

策略知识主要有以下的基本特点：

(1)模块性。一个策略知识是可以独立存在的，其不会受到外界的影响，可自由地为策略组装器服务。

(2)继承性。子策略知识可继承父策略知识的数据及操作，每个子策略知识的数据被分为 2 个部分：1)从父策略知识那里继承过来的共享数据。2)本策略知识中的私有数据。

(3)易维护性。一个策略知识具有局部性，对其进行修改或删除，不会影响其他策略知识，便于维护。

3.2 选择知识表示方法的一般原则

在其他学科领域，一般都有相应的表示形式，如：数学中的数字表示形式、函数表示形式；化学中的化学元素符号等。可见，任何需要进行交流、处理的对象都需要用适当的形式表示出来才能被应用，知识也不例外。知识表示就是对知识的一种描述，或者说是一组约定，一种计算机可以接受的，并用于描述知识的数据结构。知识表示形式又称为知识表示模式。

目前，表示知识的方法主要有：产生式表示法，Petri 网表示法和面向对象表示法等。对同一知识，一般可以用多种方法进行表示，但其效果却不相同。因为不同领域中的知识都有不同的特点，而每一种表示方法也各有自己的长处与不足。由于当前关于知识表示的理论及规范尚未建立，没有统一的标准，因此不存在一个万能的知识表示模式，但一般来说，在选择知识表示方法时，一般性原则如下：

(1)充分表示领域知识。确定一个知识表示模式时，首先需要考虑它能否充分地表示领域知识。知识表示模式的选择和确定往往要受到领域知识自然结构的制约，要视具体情况而定。

(2)有利于对知识的利用。知识的表示与利用是密切相关的。如果一种表示模式的数据结构过于复杂或者难于理解，使知识不便于进行匹配，那就会影响到求解问题的效率，从而降低求解问题的能力。

(3)便于对知识的组织、维护与管理。为了把知识存储到计算机中，还需要对知识进行合理的组织，这就要求在设计或选择知识表示方法时，能充分考虑知识的组织方式。在确定知识的表示模式时，应充分考虑维护与管理的方便性。

(4)便于理解和实现。一种知识表示模式应是人们容易理解的形式，这就要求它符合人们的思维习惯，便于实现。

3.3 策略知识的表示形式

本文根据策略知识的特点以及选择知识表示法的一般原则，从众多的知识表示方法中，选取最适合的面向对象表示法来表示策略知识。

(1)面向对象表示法。面向对象技术中的对象、类、封装、继承是其基本概念。对象是指客观世界中的任何事物，从实现机制上讲，对象是自动机，有名字、数据和操作，不同对象间的相互作用通过互传消息来实现。类是对一组相似对象的抽象，它也是一个对象，只是它的数据及操作是该类中各具体对象共同的部分。封装是把一切“局部”于对象的信息及操作都局限于对象之内，在外面是不可见的，对象之间除了互递消息之外，不再有其他联系。继承是指父类具有的数据和操作可被子类使用，除非子类对相应数据及操作重新进行了定义。

由此可见，面向对象具有模块性、继承性、封装性、多态性、易维护性和便于增量设计等基本特征。用它表示策略知识最合适。

(2)策略知识描述。在面向对象方法中，类、子类、类的实例构成了一个层次结构，在用其表示策略知识时，需要对其进行描述，以下是一种描述形式：

```
Class    <类名> [:<超类名>]
           [<类变量表>]
         Attribute
             <对象的属性>
         Method
             [<对象的操作>]
         Restraint
             [<限制条件>]
END
```

其中，Class 是类描述的开始标志；<类名>是该类的名字，它是策略知识库中该类的唯一标识；<超类名>是可选的，当该类有父类时，用它指出父类的名字；<类变量表>也是可选的，它是一组变量名构成的序列，该类中所有对象都共享这些变量，对该类对象来说，它们是全局变量，当把这些变量实例化为一组具体的值时，就得到了该类中的一个具体对象，即一个实例。Attribute 后面的<对象的属性>用于描述该类对象所具有的属性。Method 后面的<对象的操作>用于定义对象实例与类成员间的各种操作。Restraint 后面的<限制条件>指出该类元素应满足的限制条件，当它不出现时表示没有限制。

3.4 策略知识库的建立

策略知识库的建立主要由知识获取机构来完成，首先需要获取策略知识，然后按照一定的组织形式，进行存储，在存储过程中，还需要对其进行一致性、完整性检测。

(1)策略知识获取。策略知识获取是为策略翻译获取策略知识，建立起健全、完善、有效的策略知识库，以满足策略翻译的需要。为此，对各个网络安全设备策略的规范进行知识抽取，使之通过知识转换，即将抽取的策略知识转换为用面向对象表示法进行表示，使其能够被计算机识别、运用。

(2)树型策略知识组织形式。策略翻译的性能取决于策略知识的质量和数量、搜索方法、组织形式。由于策略知识采用面向对象表示法进行表示和其层次结构关系，因此策略知识库采用树型结构组织，见图 2。

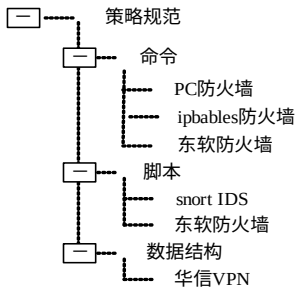

图 2 策略知识树

根节点“策略规范”类具有“策略执行体”、“策略受控体”和“策略行为”3 个属性成员，它是所有分支节点类和叶子节点类的父类，这些类都继承这 3 个属性。命令类定义 3 种操作：“前插”，“后插”和“替换”。前插即对象实例插入命令参数之前，用符号“<<”表示；后插即对象实例插入命令参数之后，用符号“>>”表示；替换即对象实例替换命令参数，用符号“II”表示。命令参数是命令类成员。数据结构类定义五元组：(F,M,T,S,O)，即数据结构大小/数据结构成员/成员类型/成员大小/偏移量。偏移量是指该数据结

构的某个成员相对于该数据结构在内存中起始位置的值，以“位”为单位。脚本类设置一些限制条件，如脚本的最大长度、编写脚本的语言等。

(3)策略知识的一致性和完整性。策略知识库的建立过程是策略知识经过一系列变换进入计算机系统的过程，该过程存在导致策略知识不健全的因素。如对策略知识库进行增加、删除和修改时，没有充分考虑到可能产生的影响，以致在进行这些操作后使得策略知识库出现不完备的情况，甚至产生意想不到的后果。因此，策略知识库经常出现知识冗余、矛盾等情况。

策略知识冗余是指策略知识库中存在多余的策略知识。例如，一个子节点，在继承了其父节点之后，又重新定义与父节点完全相同的属性。此时，则称子节点与父节点产生知识冗余，需要删除子节点重新定义的属性。

如果同一个分支节点或叶子节点从属于不同的分支节点，则称其矛盾。如图 2 中的东软防火墙，既从属于命令节点，又从属于脚本节点，从一个根节点出发，就会得出 2 个不同的结论。但在现实中，有时这是允许的，因为可能存在着一种设备有多种策略配置方式的情况，只不过需要管理员进行分析，选择命令方式配置或脚本配置方式。因此，在进行搜索求解过程前，可预先指明需要哪个知识进行求解，以免引起混乱或者错误。

还有的策略知识可能是管理员在进行知识获取时，由于疏忽，而把对象的一些属性等内容输入错误或没有输入，导致策略知识不完整，致使求解错误。

4 应用测试

以iptables防火墙[5]2 条统一描述的策略为例，进行测试。

4.1 iptables 防火墙策略知识

策略知识库中对应的 iptables 防火墙策略知识为：

```
Class   <iptables 防火墙> : <命令>
<“iptables”>
        Attribute
<
(D_Operate,-),
(C_ ActPoint),
(C_Protocol,–p),
(C_S_IP,–s),
(C_S_Port,—sport),
(C_D_IP,–d),
(C_D_Port,—dport),
(P_Action,–j)
>
        Method
              < “>>” >
END
```

4.2 策略编译器输出

策略编译器将统一描述的策略通过词法分析和语法分析后，输出双向链表。

4.3 策略组装器输出

策略组装器在策略知识库中搜索，找到 iptables 的策略知识，并根据策略知识生成如下策略：

```
iptables -A OUTPUT -j ACCEPT -p tcp -s 192.168.0.1 -d 25.20.188.129/30 --dport 80:1024 --sport 1050
iptables -A OUTPUT -p udp -s 192.168.0.1 --sport 1050:2000 -d 25.20.188.2/32 --dport 8008 -j REJECT
```

4.4 验证结果

将策略组装器输出的结果传送给 iptables 防火墙，假设为文件 iptables_policy。通过 iptables 命令查询防火墙当前是否有策略正在执行，操作为 ipables –L。如果有策略，将其清除。操作为 ipables –F。当前防火墙内核将没有策略正在执行，可以通过命令 iptables –L 再次查询策略，将发现内核已没有策略执行。这时，执行该文件，操作为 ipables iptables_policy。此时，可以通过命令 iptables –L 再次查询策略，可以发现内核的 OUTPUT 链已多了 2 条策略。在搭建的实验环境中进行数据包的测试，得出预期的正确结果。说明在 iptables 防火墙上测试通过，策略的翻译是正确的。

策略编译器双向链表输出见图 3，其中，2 条双向链表表示 2 条策略。

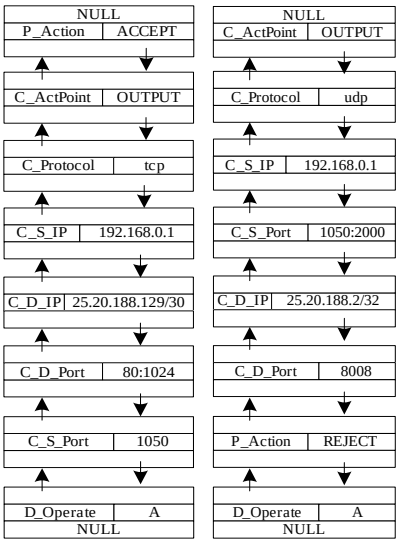

图 3　策略编译器双向链表输出

5 结束语

策略知识库可以存储如 iptables 防火墙、PC 防火墙、Snort 入侵检测系统等设备的策略知识，管理员只需选择设备类型，就可以自动地翻译为相应的策略，实现对不同厂商设备策略的管理，体现了策略翻译的智能化，减轻了管理员的工作负担。因此，策略知识的表示形式和策略知识库将直接影响策略翻译的效果，必须科学地规划策略知识，合理地建立策略知识库，才能达到策略智能翻译的目的，更好地实现策略管理。

参考文献

[1] Nicodemos C D. A Policy Framework for Management of Distributed Systems[D]. London, England: Imperial College of Science, Technology and Medicine University of London, 2002-02.

[2] Beigi M S. Policy Transformation Techniques in Policy-based Systems Management[M]. [S. l.]: Watson Res. Center Press, 2004: 13-22.

[3] 王永庆. 人工智能原理与方法[M]. 西安: 西安交通大学出版社, 1998.

[4] 胡元义. 编译原理教程[M]. 西安: 西安电子科技大学出版社, 2003.

[5] 李忠宪. iptables 指令详解[EB/OL]. (2006-03-16). http://www.i170.com/article/18839.