NETCONF协议探析

张战杰，王鸿飞
（漯河职业技术学院 计算机工程系，河南 漯河 462002）

摘 要：NETCONF协议是一种最新的基于XML的网络配置和管理协议，NETCONF协议针对之前流行的SNMP协议在功能和构架上的缺陷，并结合时下最流行的XML技术，提出了一套对于网络设备的配置信息和状态信息进行管理的机制。

关键词：NETCONF；RBAC；XML
DOI:10.3969/j.issn.1674-5043.2011.03.014
中图分类号：TP393 **文献标志码**：A **文章编号**：1674-5043(2011)03-0056-06

目前网络管理协议主要是简单网络管理协议(SNMP)，SNMP采用UDP传送，实现简单，技术成熟，但是随着网络规模的日益扩大，网络复杂性的增加、异构性的增强，基于SNMP的传统网络管理协议，由于其过于简单，在配置管理方面上存在着重大的缺陷，正面临着巨大挑战。在安全可靠性、管理操作效率、交互操作和复杂操作实现上还不能满足管理需求。随着网络越来越复杂，新型的网络配置协议(NETCONF)应运而生，NETCONF采用XML作为配置数据和协议消息内容的数据编码方式，采用基于TCP的SSHv2进行传送，以简单的远程过程调用(RPC)方式实现操作和控制。XML语言可以表达复杂的、具有内在逻辑关系的、模型化的管理对象，如端口、协议、业务以及它们之间的关系等，大大提高了操作效率和对象标准化；同时采用SSHv2传送方式，可靠性、安全性、交互性较好。访问控制是NETCONF网络管理中一种必不可少的安全机制，因为NETCONF网络管理中不是任何人都能访问被管设备并读取或修改被管设备数据的，而是指定的人员可以访问被管设备的指定的数据。同时，NETCONF网络管理中存在少量的网络管理站和大量的被管设备。本文对NETC0NF协议的框架进行了简要的介绍，并提出了基于角色的访问控制机制(RBAC)。

1 NETCONF概述

NETCONF协议是一种最新的基于XML的网络配置和管理协议。NETCONF协议针对之前流行的SNMP协议在功能和构架上的缺陷，并结合时下最流行的XML技术，提出了一套对于网络设备的配置信息和状态信息进行管理的机制。NETCONF协议采用XML作为配置数据和协议消息的编码方式，用C/S和RPC方式来获取，更新或删除设备中的相应的部分或所有管理信息。XML可以表达复杂的、具有内在逻辑关系的、模型化的管理对象，大大提高了操作效率和对象标准化。XSD、Xpath、SOAP、XSLT等XML技术都可以应用到NETCONF协议中。另外，协议采用SSHv2、SOAP、BEEP等传输方式，来提高传输的可靠性、安全性和交互性。NETCONF协议分成4层：应用协议层、RPC层、操作层、内容层，如图1所示。协议的应用协议层提供管理端和代理进行安全可靠通信的方案。RPC层为RPC模块的编码提供了一个简单的、传输协议无关的机制。操作层定义了一个基本的操作集并能够通过能力进行操作和功能的扩展。内容层表示的是被管对象的集合，其中RFC4741对NETCONF协议的基本框架，操作层和RPC层以及能力扩展等都做了说明和定义，RFCA742-4744分别对应用协议层的SSH、SOAP/HTTP和BEEP的传输机制进行了阐述。内容层目前还没有定义相应的标准，但是国际组织和研究人员对内容层特别是数据建模以草案的形式提出了很多建议和方案。

收稿日期：2011-06-01

作者简介：张战杰(1970-),男,河南临颍人,硕士,讲师,主要从事计算机网络方面的研究.

2　系统结构

为了兼容现有设备中的网络管理方式，本文提出一种通用的下一代综合网络管理结构，如图2所示。只需要在现有设备代理中加入NETCONF代理即NETCONF管理接口和协议API，在数据库方面可以考虑加入XML数据库便于存储XML数据，设备底层接口和原有的SNMP和CLI接口基本可以保持不变。因为目前大部分设备支持的是SNMP协议和CLI方式，同时设计一个转换网关将其进行报文的转换作为目前传统网络管理系统与下一代综合网络代理的过渡方式，实现下一代网络管理系统的通用网络管理。在图2的结构中，NETCONF代理是目前研究和开发的核心。将

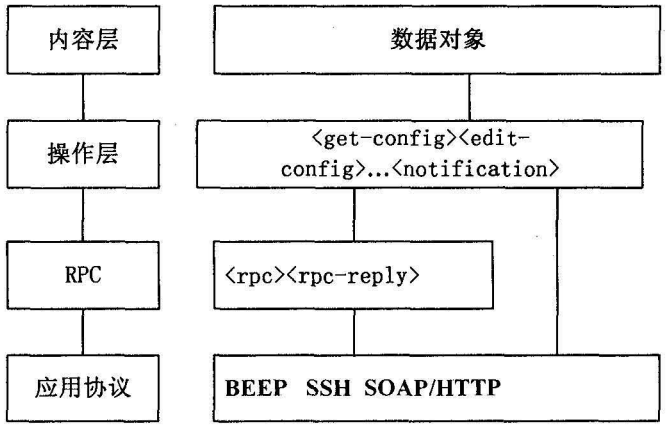

图1　NETCONF四层协议图

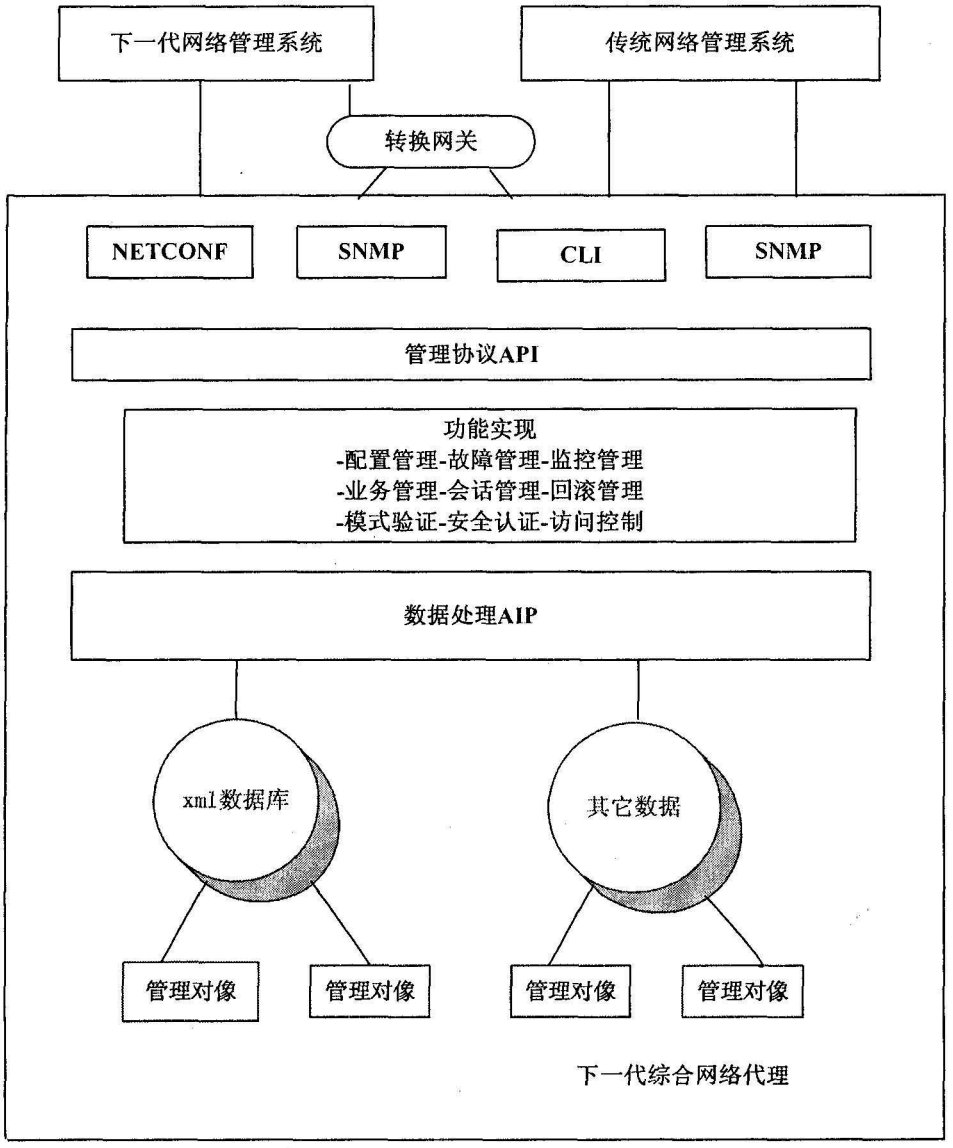

图2　下一代综合网络管理结构图

NETCONF的功能进行分离后，从上到下设计为4大模块：应用协议层模块、RPC层模块、操作层模块、内容层模块。应用协议层模块主要解决连接、会话、安全处理、报文发送和接收等问题。RPC层模块处理压缩解压、加密解密以及RPC处理。操作层和内容层是协议开发和实现的重点。操作层模块需要根据NETCONF操作请求执行相应的操作，通过匹配相应的数据模型，最后通过内容层找到相应的配置模块，在XMLDB中或通过厂商设备接口读取到所需设备配置或状态数据。在此结构中通过模块划分、使用命令、工厂等设计模式来减少模块之间的耦合。同时在处理过程中将重要的配置信息写入日志，并对异常进行处理。

基于角色的访问控制机制(RBAC)的最大优势在于其对授权管理的支持。常见的自主型访问控制和强制性访问控制方法都是由主体和访问权限直接发生联系，根据主体/客体的所属关系或主体/客体的安全级来决定主体是否具有对客体的访问权。但是，处于全球网络环境中的计算机或软件系统的访问用户往往种类繁多、数量巨大且动态变化，这使得采用传统的访问控制方法进行安全管理变得非常困难。RBAC方法引入了角色这个中介，安全管理人员根据需要定义各种角色，并设定合适的访问权限，而用户根据其责任和资历再被指派为不同的角色。

3 访问控制机制(RBAC)

3.1 RBAC机制的实现流程

根据RBAC机制的基本原理，NETCONF网络管理系统对具体用户的访问请求进行评估，看该用户是否能够执行该操作。具体的评估过程包含身份认证和权限验证两个部分：根据用户名和密码来判定用户能否访问服务器称为身份认证；而权限验证是根据给用户分配的权限来对访问请求进行验证的过程。

3.2 身份认证

RBAC机制的身份认证既是对用户名和密码的验证，也是为用户分配权限的过程，身份认证流程图如图3所示。用户在身份验证通过时就根据自己担任的不同角色获得权限，否则得不到任何访问权限。

步骤(10)：接收用户名、密码和角色类型；

步骤(20)：根据用户名，密码和角色类型验证有效性。如果接收信息无效，则转到步骤(30)，否则转到步骤(40)；

步骤(30)：向用户提示授权失败；

步骤(40)：由RBAC 访问控制基本原理，对当前的用户进行权限分配；

步骤(50)：向用户提示授权成功。

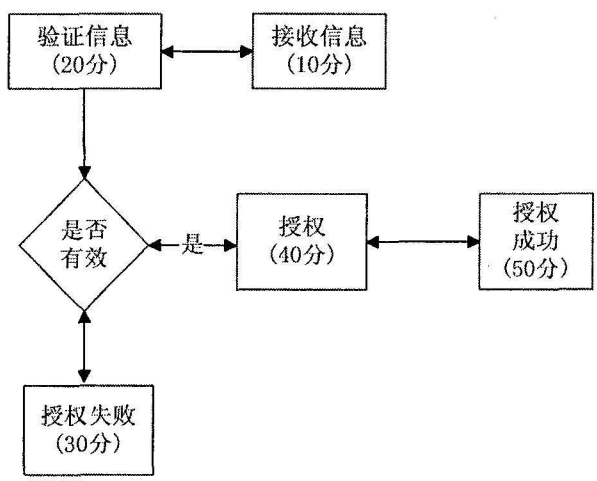

图3 身份认证流程图

3.3 权限验证

NETCONF协议的操作中只有get、get-config 和edit-config操作面向XML节点集，因此，验证过程把NETCONF操作分成两种类型，有节点集操作和无节点集操作。RBAC机制的具体操作验证过程如图4所示。

步骤(10)：等待并接收Manager端发送的操作请求；

步骤(20)：解析请求报文，获取操作名，接着判断是否支持该操作。如果权限中不包含对应的操作名，则表示不支持该操作，将转向步骤(30)，否则继续判断操作类型。如果操作类型为非节点级操作，则转向步骤(40)，否则继续判断是否是可写操作。如果是可写操作，则转向步骤(70)，否则转向步骤(50)。节点级操作表示操作是针对具体节点的操作，如get、get-config、edit-config等操作，其他的操作是非节点级操作。非节点级操作包括lock、unlock、delete-config、copy-config、kill-session、close-session等；

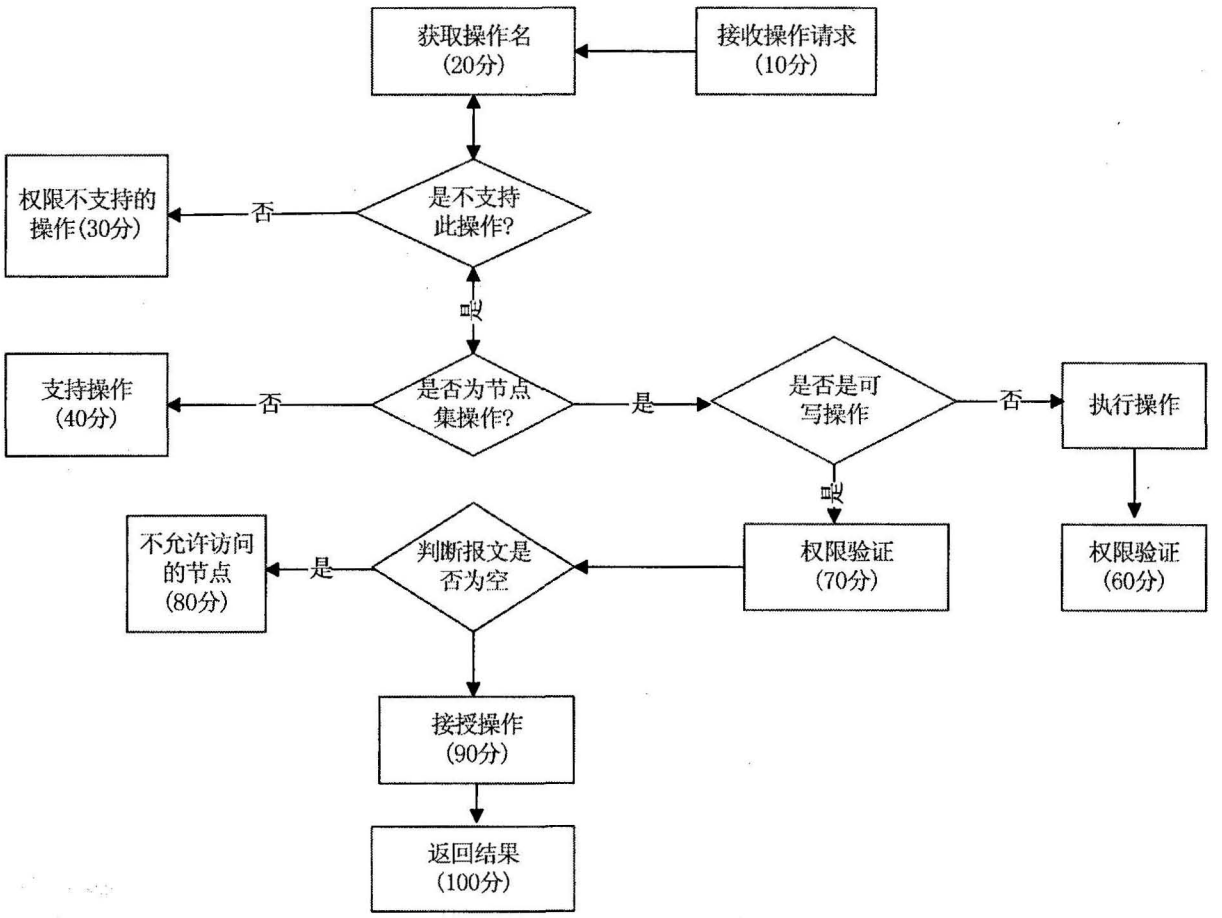

图4　RBAC的操作验证过程

步骤(30)：表示权限不支持此操作，生成错误信息；

步骤(40)：执行非节点级操作，生成结果；

步骤(50)：对于节点的不可写操作是get 操作和get-config 操作。根据操作请求执行操作，生成结果；

步骤(60)：根据权限从结果集中删除不可访问的节点；

步骤(70)：对于节点的可写操作是edit-config操作。根据权限判断请求报文是否允许执行，如果允许，则转向步骤(90)，否则转向步骤(80)；

步骤(80)：表示请求报文中存在权限不允许访问的节点，生成错误信息；

步骤(90)：执行edit-config 操作，生成结果；

步骤(100)：向用户返回结果，进入等待状态，准备接受下一次访问请求。

3.3.1　只读操作的权限验证

在NETCONF协议中只读操作包括get操作和get-config操作。对于只读操作，首先执行操作获取结果，然后权限验证得到最后的结果。这种先执行后验证方法的好处是：支持xpath过滤、子树过滤以及扩展子树过滤；对以上三种过滤方式，可以统一考虑；支持对多个模块的过滤；如果有其他过滤方式时不会影响权限验证。坏处是：结果集越大，验证时间越长。只读操作的权限验证过程如图5所示。

步骤(61)：获取操作结果，接着判断结果是否为错误信息，如果是错误信息，则转向步骤(66)，否则转向步骤(62)。

步骤(62)：从操作结果中获取结果所涉及到的模块个数，接着每个模块都进行权限验证。当所有的模块都验证完以后转向步骤(65)。

步骤(63)：根据模块名从权限集中过滤出对应的权限，接着判断过滤出的权限中是否存在权限，如果

存在则转向步骤(64)，否则处理下一个模块的结果。

步骤(64)：删除相关模块的结果，处理下一个模块的结果。

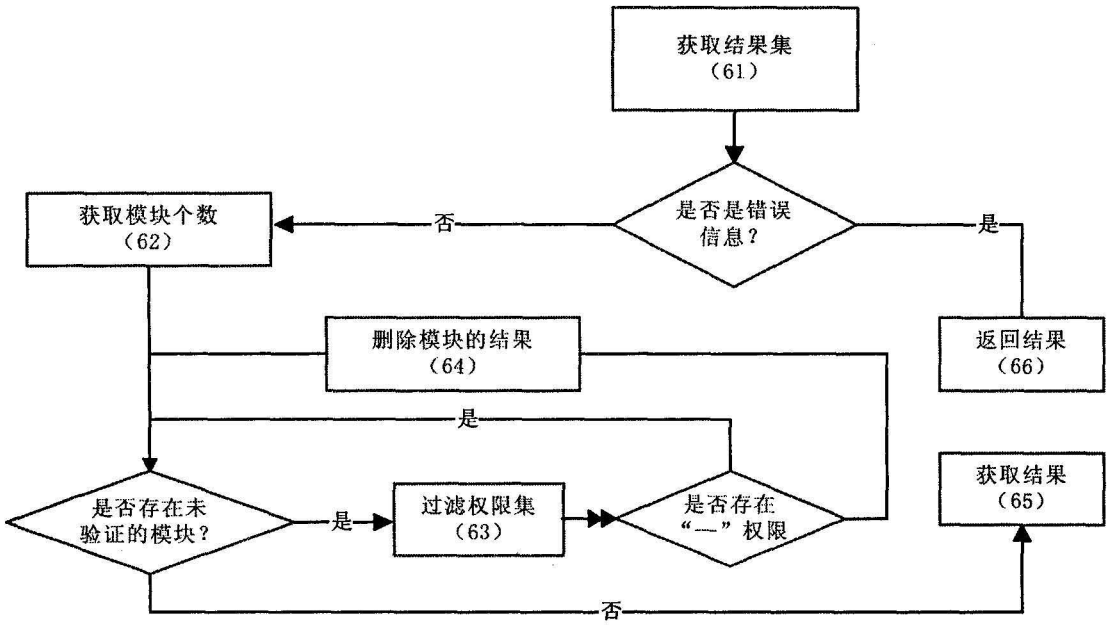

图5 只读操作的权限验证过程图

3.3.2 可写操作的权限验证

在NETCONF协议中可写操是edit-config操作，可写操作包括修改、替换、创建、删除等。对edit-config 操作存在以下特点：edit-config操作报文使用绝对路径，根据绝对路径可以定位到具体节点；权限列表中把一个节点的权限设置为W时，该节点的子节点的权限都是W。采用先验证后执行的方法，能提高edit-config操作的效率。可写操作的权限验证过程如图6所示。

步骤(71)：根据请求报文获取模块名。

步骤(72)：根据模块名过滤权限集。接着判断在过滤出的权限集中是否存在“一”权限权限，如果存在则转向步骤(80)，否则继续判断带有operation属性的节点是否设置了权限。如果是则根据权限类型判断操作的可行性，否则定位到该节点的上一级节点。

步骤(73)：判断对当前节点是否设置了权限，如果是则根据权限的类型判断操作的可行性，否则判断是否存在父节点。如果存在则转向步骤(73)，否则转向步骤(90)。

4 结 语

在NETCONF网络配置协议的基础上对RBAC机制的基本原理和实现做了全面的分析，并且对访问资源为XML格式数据的访问控制机制做出了新的探索。该机制利用角色不仅支持大量用户的管理和认证，而且实现了用户和权限之间的松耦合，大大提高了访问控制的灵活性。但是，该机制仍存在一些不足，验证面向底层数据使得验证效率会随着数据模型不断变大而降低，这也在一定层度上降低了XML大数据量的处理能力，考虑到XML具有schema文档，它的大小不会随着XML的变化而变化。

参考文献：

[1] Jan van Bon.IT服务管理——基于ITIL的全球最佳实践[M].北京:清华大学出版社,2006:71-73.

[2] 高志鹏.新的基于SID的管理信息建模方法[J].北京邮电大学学报,2006(S1):112-115.

[3] 肖德宝.下一代网络配置管理协议NETCONF的研究与实现[J].华中师范学报,2008(4):50-53.

[4] 徐慧.基于NETCONF协议的新一代网络管理[J].北京邮电大学学报,2009(4):10-14.

[5] 王晓军.基于NETCONF的网络管理系统设计[J].南京邮电大学学报,2006(3):62-67.

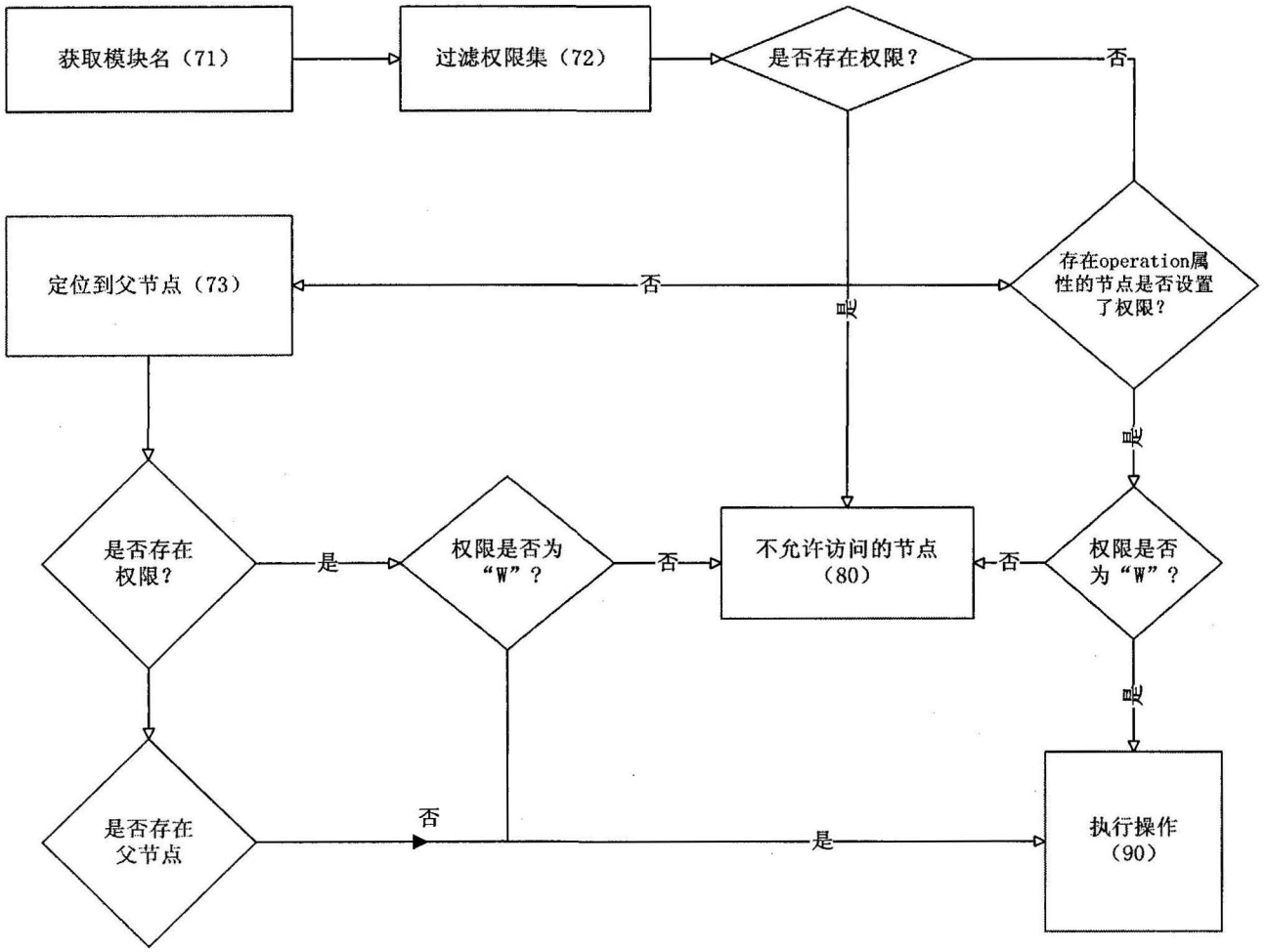

图6 可写操作的权限验证过程图

NETCONF Protocol Exploration

ZHANG Zhan-jie, WANG Hong-fei

(Luohe Vocational and Technical College, Luohe 462002, China)

Abstract: NETCONF protocol is a new XML-based network configuration and management protocol. In view of the function and structure defects of the ex-popular SNMP protocol, combined with the prevalent XML technique, NETCONF protocol presents a set of mechanics to manage the configuration information and stated information of the network devices.

Key words: NETCONF; RBAC; XML