# 一种主动网络管理模型的设计与研究*

马 燕
(重庆师范大学 物理学与信息技术学院, 重庆 400047)

**摘 要**:在分析传统网络管理面临困难的基础之上提出了一种新型的主动网络分布式管理模型,讨论了传统网络管理中存在的问题,分析了主动网络管理体系结构与管理机制。重点研究了节点结构、Smart 的组成、管理机制、包的格式、编程语言和设计目标,以及安全性。

**关键词**:主动网络;网络管理;Smart 包;模型
**中图分类号**:TP393 **文献标识码**:A **文章编号**:1672-6693(2005)03-0037-05

## Design and Study of the Active Network Management System Model

*MA Yan*
(College of Physics and Information Technology, Chongqing Normal University, Chongqing 400047, China)

**Abstract**: Active network is a kind of novel network architecture, it provides for the user a programmable interface where users dynamically inject services into the intermediate nodes. Based on the active network technology, a new distributed management model is designed. This paper analyses the problems of tradition network management and the structure and mechanism of the active network management system. It introduces the structure of active node and Smart packet, the mechanism of management, the packet formats, the language and its design goals, and security.

**Key words**: active network; network management; Smart packet; model

主动网络在网络体系结构的发展上是一次质的飞跃,它使传统的网络成为"运行时可编程、可扩展的网络"。作为一种崭新的网络结构,其应用前景是十分诱人的。主动网络将成为 21 世纪网络体系结构的主流。

基于主动网络的管理技术是将主动网络与网络管理相结合的新型网络管理技术,势必将加大网络管理的现代化进程。本文针对主动网络具有分布式计算的特点,提出了一种基于 Smart Packets(智能包)的主动网络管理模型(ANM, Active Network Management),它改变了过去传统网络集中式管理不足,充分利用了主动节点的计算能力进行分布式管理,使网络管理更趋合理。

## 1 网络管理

### 1.1 传统网络管理

传统的网络管理系统广泛使用的是简单网络管理协议 SNMP。这种网络管理协议是一种集中式的、单序的、反应式的模式,随着网络规模和复杂性的增加以及大量异构网络的存在,这种模式已很难适应当今网络管理的需求。在使用 SNMP 协议的管理系统模型中,被管网络设备由两部分组成:代理进程(Agent)和管理信息库(MIB, Management Information Base)。MIB 是对网络被管对象信息的逻辑描述,它包含被管网络设备的配置、状态、错误和性能等方面的信息;Agent 驻留在被管网络设备中,与远程的网络管理系统(NMS, Network Management Station)通过 SNMP 协议通信,访问、控制 MIB 变量。NMS 是整个网络管理的核心,它通过轮询被管设备获得该设备上管理信息库 MIB 中相关变量的值来获得网络的运行状态[1]。

SNMP 协议在现代网络管理中存在着很多问

* 收稿日期:2005-06-21
资助项目:重庆市教委应用基础研究资助项目(020805);"重庆市高等学校优秀中青年骨干教师资助计划"(重庆市教委[2003]2 号)
作者简介:马燕(1960-),男,云南昭通人,教授,主要研究方向为计算机网络新技术、智能教学系统。

题,其主要原因是:NMS 作为信息汇集的中心,成为网络流量的瓶颈;各被管设备的功能不能动态调整;被管设备必须和 NMS 交换大量信息才能完成网络管理工作,这既加重了网络的负荷又造成了管理任务的延迟。

综上所述,传统的网络管理使用 SNMP 网络管理模型,由于采用集中式管理,无法利用主动网络中节点的计算能力来管理网络。因此,它们不可能对主动网络实施有效的管理。

### 1.2 主动网络管理

为了适应主动网络的特点,主动网络的管理模式应能突破传统网络的非对称管理模式,使网络控制与管理工作站及主动节点之间达到一种对等的关系,从而克服传统网络管理中管理端出现的瓶颈问题,也便于业务的动态加载和动态 MIB 的管理与维护。主动网络管理结构如图1所示。

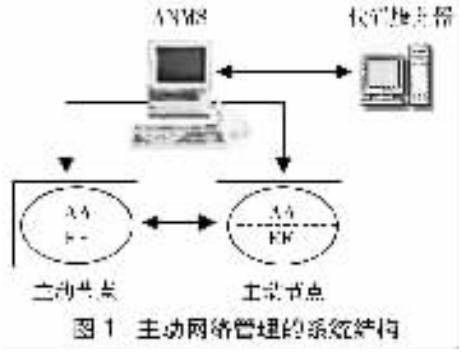


图1 主动网络管理的系统结构

在主动网络管理 ANM 系统中,主动节点是主动网管所要管理的主动对象。主动节点与控制管理站(ANMS)之间的通信是一种对等的关系,而不像 SNMP 中客户端与服务端之间的非对等关系[2]。主动节点是网管系统的主要管理对象,负责处理主动信包;执行环境(EE)提供了主动管理信包运行和处理所必需的环境;主动应用(AA)则执行主动管理信包中的代码。当管理节点需要执行某个管理任务时,它首先启动相应的管理程序,该管理程序创建一封装体报文,然后将它注入到网络中。封装体报文到达主动网络中的节点时,节点根据管理节点发出和管理程序中的策略和计算规则执行相应的程序,并根据程序决定下面的动作,通过调用节点操作系统 OS 来访问各种资源来实施网络配置管理、性能管理、故障管理等功能。

## 2 主动网络管理模型设计与实现

### 2.1 主动节点管理模型

根据主动网络的结构特征,提出了一种基于主动网络的管理模型 ANM。该模型充分利用了主动网络的主动性、动态性和智能性,以实现主动网络的分布式管理。在该模型中,采用了 Smart(精灵包)作为管理调用的程序包,图2显示了主动网络传输模型。

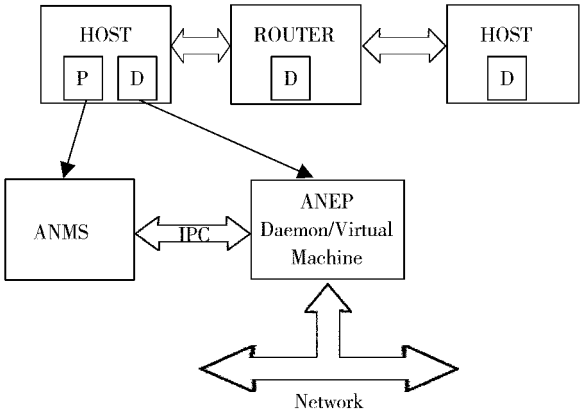


图2 运用 Smart包的主动网络管理结构

**定义** 一个支持主动网络动态管理部署的 ANM 系统是由一个四元组 DANM = $\{A, E, N, f\}$ 组成。

其中,$A$ 为主动应用 AA 的集合,记为 $A = \{a_1, a_2, \cdots, a_i\}, i \in \infty$;$E$ 为 ANM 应用执行环境的集合,记为 $E = \{e_1, e_2, \cdots, e_i\}, i \in \infty$;$N$ 为主动节点的集合,记为 $E = \{n_1, n_2, \cdots, n_i\}, i \in \infty$;$f$ 为 $A$、$E$、$N$ 之间的一种关系,表示对于任何动态的 ANM 应用,在主动节点上,都存在相应的一个环境,即对于 $\forall a_i, n_p$ $(a_i \in A, n_p \in N)$, $\exists e_j (e_j \in E)$,有 $e_i = f(a_i, n_p)$。

在图2中,ANM 中主动节点执行环境相当于 $e$,主动管理的执行与应用相当于 $a$,$f$ 相当于主动管理部署与策略。对节点的管理程序和监视程序采用 ANEP 标准封装成包并送到 ANEP 自适应数据鉴定器和监视器 Daemon(Data Adaptive Evaluator and Monitor),再由 Daemon 将包注入到网络中。图2中的 P 即为管理程序(Network Management Program),它是可传送的 Smart 包;图中的 D 即为 Daemon,它驻留在网络的节点中。Smart 包在网络中的传送有端到端(end-by-end)或逐段转接(hop-by-hop)两种方式,在前一种方式下,Smart 包中的程序代码仅在目的端被执行。而在后一种方式下,Smart 包中的程序代码可在源端、目的端及中间的所有段被执行。Smart 包中包含代码的程序可以将网络中任何一个主机运行结果带回到源端。

在节点中,操作系统中安全策略数据库(Securi-

ty Policy Database)和安全执行引擎(Security Enforcement Engine)保障了节点的安全。当 AA 或者 EE 中的实体需要节点操作系统提供服务时,由 EE 向 NOS 发出请求消息,该请求消息中带有主体标识符用以指明请求的生成者。节点操作系统收到消息后,将它提交给安全执行引擎,若通过了身份验证,再检查安全策略数据库,最后执行相应操作完成执行环境所请求的服务。

图 3 是 ANMS(主动节点管理站)的结构图。

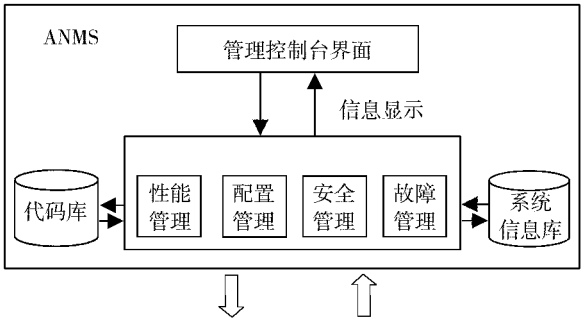


图 3　主动管理 ANMS 结构模型

在 ANMS 中,由管理员通过命令方式,运用主动管理系统的各种 AA,调用相应的模型以生成各种 Smart 包注入到主动网络中,这些 AA 包括主动网络节点信息的获取、网络监控、分析和配置主动网络中各节点的应用程序。

图 4 是基于上述模型的主动网络节点结构。其中 NOS 工作在底层,它主要进行资源管理、存取控制等,还负责基本的网络功能、代码或节点的安全等。NOS 管理 EE 提出的访问请求,为 EE 屏蔽底层资源的分配细节。EE 类似于一般计算系统中的"Shell"程序,提供相应网络服务的可编程接口或虚拟机。EE 主要完成主动包的解释和执行,一个节点中可有多个 EE,各个 EE 之间相互独立。

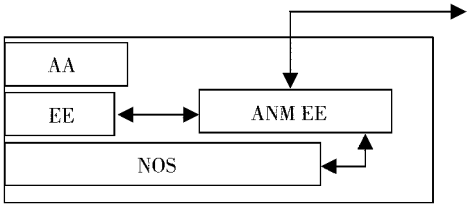


图 4　主动网络管理系统中的主动节点

为实现对节点的管理,在 NOS 与 EE 之间增加了节点管理器 ANM(ANet Node Mgr),它实现主动网络节点的 Daemon 功能,为节点提供一个安全可靠的运行环境。ANM 与本地节点适配器(通过 Node OS API)一起访问相应数据、设置管理功能和控制相应事件。并通过与 EE 的相互协作实现管理节点 EE 设置、性能并处理运行中出现的问题;调整 SW 使其能够动态地适应主动应用的变化;通过其它的 EE 或 AA 实现对节点配置对象的管理。

### 2.2　Smart 包的结构

Smart 采用 ANEP(Active Network Encapsulation Protocol)实现包的封装,它由 IP 包头、ANEP 包头、Smart 包所组成[3]。应用 Smart Packets 的主动网络可以与现有的 IP 网络相兼容,而且可以方便地实现主动网络的管理。在传统网络中,数据包在 IP 路由器上仅仅检查数据报文头部并转发数据报。而对于 Smart 包,路由器必须在转发之前处理包中的内容。因此,只要路由器支持 Smart 包就会检查包中的内容,否则路由器应让数据包通过。

根据上述分析,要达到这个目标可通过修改 IP 报文的可选项来实现。基于在 IP 报文可选项中的一个标签,路由器能决定是否应该处理数据包内容。如果路由器并不支持主动网络,它会忽略选择项并转发这个数据包;如果路由器支持主动网络,它检查 Smart 包中的信息,获知这个数据包是 Smart 包,如果路由器支持这种,它处理这个数据包。

Smart 包结构由 ANEP 作了详细的规定,其包头有 4 个域:版本号、类型、上下文和序列号,如图 5 所示。版本号用来标记语言的升级和包格式的改变。类型域标记下列 4 种类型之一:程序包、数据包、错误包或消息包。

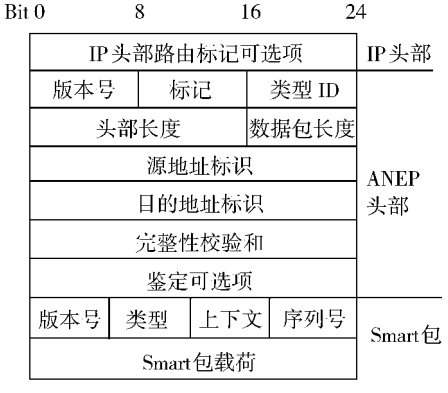


图 5　采用 IP 和 ANEP 封装的 Smart包

程序包将代码传送到某个特定主机执行后由数据包携带其执行结果返回源网络管理程序;消息包所携带报告和消息而非可执行代码;错误包则在程序包传输或是其代码在执行时遇到异常时返回错误结果。

上下文中标记包的发送者,它的值由 ANEP 为

每个客户设置唯一的值。当程序包在网络中传送并产生一个或多个数据包、错误包或消息包时,此值用于标记每个客户所响应的源程序。序列号用于标记相同上下文之间的消息。

为了不给主动节点造成过重的负担,并保证节点自身的安全性,要求将程序代码完整地封装到一个数据包中,因此代码长度不得超过1KB。

### 2.3 Smart Packets 的封装

Smart 包采用 ANEP 标准进行封装。图5已显示了 ANEP 的头部,Smart 包使用4个 ANEP 的可选项:源地址、目的地址、完整性校验和和鉴定可选项。鉴定可选项的细节如图6所示,它主要识别报文的发送者,包含了一个数字签名和一个公开密钥认证[4]。各个域的说明如下。

| ANEP可选项头部 | | | |
|---|---|---|---|
| ID类型 | 签名类型 | 论证类型 | ID长度 |
| 签名长度 | 论证长度 | 负载长度 | |
| ID | | | |
| 签 名 | | | |
| 认 证 | | | |

图6 的Smart包的ANEP可选项

(1)ID 域包含一个 IPv4 或 IPv6 地址,用 ID 类型和长度域标识,其值与在 ANEP 源地址可选项的源地址域中的值相同。

(2)签名域是一个数字签名,用数字签名类型和长度域标识,这个智能包的数字签名算法的有效类型可以是哈希算法或是 MD5(第5类报文摘要算法)。

(3)认证域遵循 X.509 公开密钥认证,用标识类型和长度域标识。该认证域包含有 IPv4 或 IPv6 地址的值。

### 2.4 Smart Packets 的编程语言

目前共有两种程序语言支持 Smart 包中的代码编程。

第一种是 Sprocket 语言,它是一种很类似于 C 的高级语言,但是 Sprocket 取消了像 C 中指针这样的一些威胁安全的结构,增加了一些对 MIB 访问接口和 Smart 包等用于网络和网络管理的新特征。下面的代码定义了一个 Packet 和 address 类型的变量,并指定了一个包的目的地址。

```
packet p;
address a;
a = p.destination();
```

第二种是 Spanner 语言,它是一种基于 CISC 的汇编语言,Spanner 的程序通过编译成相应的代码,再通过编译成一个压缩的独立于机器的二进制代码,并将它注入到 Smart 包的程序段中。Spanner 所提供的原语可以实现 Smart 包的发送与传输,由于 Spanner 是为 Smart 包传输路径上路由器执行的程序,因此利用路由器可以鉴别 IP 选项,程序可以控制 Smart 包中的代码是交付节点执行还是沿下一个节点传送。

### 2.5 Smart 包的鉴定与授权

智能包的安全结构由两部分组成:鉴定和授权。使用 ANEP 的鉴定机制可以鉴定数据包的来源和数据的完整性。鉴定可选项规定了对数据报文签名了的实体,它包含签名的类型、认证的类型、标识的长度、认证和在有效负载域中的数据都被签名。

一个重要的问题是如何选择智能包中的数据域进行鉴定与保护,鉴定信息不仅要验证智能包的来源,而且要验证数据包的数据完整性[5]。

在节点收到一个 Smart 包时,通过以下进程实现鉴定和授权。

(1)如果一个鉴定可选项并没有出现在 Smart 包中,该报文不能被鉴定。因此,它被授予在授权数据库中对任何实体最小的访问权限。

(2)如果鉴定可选项存在,公钥认证生效,这个生效处理过程需要认证发行机构的公钥。

(3)以下不进行 ANEP 报文的签名检验:ANEP 数据包的长度是否为零及 Smart 包的载荷域。

(4)如鉴定失败,则数据包被丢弃。如果鉴定无法完成(如认证有效期的超时),数据包被转发。如果验证成功,数据包进入鉴定阶段。

(5)包含在认证中的标识被用于寻找授权数据库的访问权限。数据库中的记录标识着任何一个程序应该具有的约束或特权。

## 3 结束语

主动网络是针对传统网络中新服务实施的困难提出的,它增加了网络的计算能力,在网络的中间节点提供面向用户的编程接口,用户可以通过编程指定节点对数据的处理。这种计算是基于用户或特定应用的,从而使用户能够定制自己的服务,能够对现有各种新型应用提供灵活有效的支持,加速了新网络协议和用户服务在网络中实施和推广的进程。

本文探讨了一种基于 Smart 包的主动网络管理模式,并对其结构、性能与管理机制进行了分析。利用 Smart 包来实现网络管理时,网络的基础结构要足够的简化以适应 Smart 包的传送,网络要足够强壮以适应远程控制,还要足够灵活以允许远程授权和委托。该管理方案满足了主动网络中节点的灵活性和主动应用的扩展性要求,是一种较为理想的网络管理方案,相信它会在将来的网络管理中发挥巨大作用。

## 参考文献:

[1] ZEBIANE D,SERHROUCHNI A,BAKOUR H. Active and Policy Based Management [J]. Telecommunications IEEE, 2003(3):70-76.

[2] RAZ J,SHAVITT Y. Active Network for Efficient Network Distribute Network Management [J]. IEEE Communications Magazine,2000(3):122-124.

[3] SCHWARTZ B. Smart Packets: Applying Active Networks to Network Management[J]. ACM Transactions on Computer Systems,2000,18(1):67-88.

[4] MARSHALL I W. Active Management of Multiservice Networks[J]. Proc. IEEE NOMS,2000,981-983.

[5] FATTA G D,LO RE G. Active Networks: an Evolution of the Internet[C]. Cernobbio, Italy:Proc. of AICA2001-39th Annual Conference,2001.

(责任编辑　游中胜)