一种主动网络管理框架结构的设计与研究*)

马 燕[1,2] 张小真[1] 李太华[1] 钟国祥[3,1]
(西南大学计算机与信息科学学院 重庆 400715)[1]
(重庆师范大学物理学与信息技术学院 重庆 400047)[2] (重庆教育学院 重庆 400015)[3]

摘 要 随着网络规模的不断扩大,为了提高网络的可靠性和管理水平,需要进一步改进原有的网络管理的体系结构。而基于SNMP协议的传统网络管理体系已不能适应规模日益扩大的网络的需要。本文讨论了一种基于节点的主动网络管理框架体系,分析了该模型的结构、管理机制和设计要点,并对网络拓扑发现和流量进行了分析。

关键词 主动网络管理,ANMS,报文转发,拓扑发现

Design and Study of the Model of the Management System Based on Active Network

MA Yan[1,2] ZHANG Xiao-Zhen[1] LI Tai-Hua[1] ZHONG Guo-Xiang[3,1]
(Faculty of Computer and Information Science, Southwest University, Chongqing 400715)[1] (Faculty of Physics and Information Technology, Chongqing Normal University, Chongqing 400047)[2] (Chongqing Education College, Chongqing 400015)[3]

Abstract With the quick expansion of network, the centralized strategies based on ANMP are not appropriate in large-scale networks. This paper analyzes the structure and mechanism of the active network management system, introduces a pattern of active network management, and studies the structure, management mechanism, design outline and each connection of the management system. The paper also studies the network topology discovery and traffic.

Keywords Active network management, ANMS, Packets transmitting, Topology discovery

网络管理NM(Network management)是一项复杂的系统工程,由于目前网络的规模越来越大、网络的业务种类繁多、流量越来越重,因此原有的网络体系及管理方式已难以胜任当今网络的发展的需要。主动网络的概念是在1995年由DARPA(Defense Advanced Research Projects Agency)研究协会提出来的。它改变了传统网络的体系结构,为网络的快速发展提供了一个契机。从网络管理系统来看,主动网络管理是将主动网络与网络管理相结合的新型网络管理,其最重要的特点在于它可以实现管理应用或工具的分布式处理,势必将加大网络管理的现代化进程。

1 主动网络管理

1.1 主动网络管理体系结构

主动网络管理也应完成诸如传统网络的配置管理、性能管理、故障管理、安全管理和计费管理五大功能。节点是主动网络的核心。在实际运行中,节点的结构、行为和属性都可能会随时发生变化,因此对主动网络的管理也提出了新的要求。

传统的网络管理由于采用集中式管理,无法利用主动网络中的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,无法发挥和体现主动网络的优越性能。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[1],从而克服传统网络管理中Manager端出现的瓶颈问题,也便于业务的动态加载的动态MIB的管理与维护。主动网络管理ANM(Active Network Management)系统结构见图1所示。

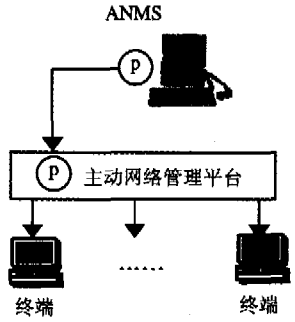

图1 主动网络管理系统的结构

由图1可知,主动网络管理ANM体系结构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工作站(NMS)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。ANMS(Active Network Management Serve)是主动网络管理的服务器,P是由管理信息库MIB和代码服务器生成的一个管理任务。主动节点是网管系统的主要管理对象,负责处理主动包,它通过下载ANMS上的管理应用P到本地执行。ANMS通过定制P的转发例程,使P在各个主动节点上移动,并在访问节点时完成相应的计算。

1.2 主动网络管理的部署与策略

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

*)重庆市教委自然科学基金资助项目(020805);"重庆市高等学校优秀中青年骨干教师资助计划"资助项目([2003]2号)。马 燕 教授,博士生,研究方向:计算机网络系统结构、主动网络、智能教学系统;张小真 教授,博导,主要研究方向:智能教学系统、计算机辅助教学;李太华、钟国祥 博士研究生,研究方向:AI、智能教学系统。

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：$N==\{n_1,n_2,\cdots,n_i\},i\in\infty$；$f$ 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：

$$e_i=f(a_i,n_p) \quad (1)$$

2 一种主动网络管理系统的结构设计

2.1 主动网络管理系统结构

根据主动网络的管理特点及主动网络的结构特征，我们提出了一种主动网络的管理模式。该管理基于节点为管理核心，充分利用了主动网络的主动性、分布性和智能性，以实现主动网络的分布式智能管理，其框图如图 2 所示。

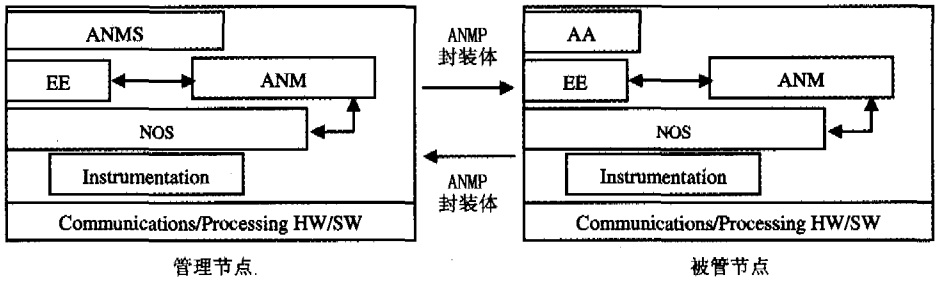

图 2 主动网络管理系统总体结构

图 2 的管理模型就是根据式(1)设计的，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 标准封装成一封装体并送到 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。当封装体到达被管理节点后，其转发例程被自动调用，根据管理节点中发出的管理程序中的转发策略和计算规则，在该节点执行一定的管理功能后根据结果决定后面的动作。

网络中的主动节点根据接收到的封装体的管理程序实现本地的管理功能。为了实现对节点的管理，在 NOS 与 EE 之间增加了主动节点管理器 ANM(ANet Node Mgr)，在节点 NOS(Net OS)与底层之间包含了指令适配器(Instrumentation)，实现了对节点的管理[2]。ANM 是由一系列 SW(SoftWare)组成的。以实现对节点的监视、设置、分析与控制。ANM 通过节点 OS 的 API 发出指令来访问节点的数据、配置节点及操作事件，同时还为 EE 提供一套 API 接口，以使主动应用(App)可以动态地适应与配置网络资源、对网络性能进行监视，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 主动网络管理系统 ANMS

ANMS(Active Network Management System)仅位于管理节点上，它是整个网络管理的核心。ANMS 负责整个系统的控制，将管理员制定的管理策略付诸实现。网络管理员通过 ANMS 启动管理任务，负责网络系统中参数的设置和运行状况的监控。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主动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[3]。

ANMS 应具有的功能有：(1)拓扑探测：ANMS 应具有探测网络拓扑结构、生成结构的视图等功能，并尽可能维护网络的最新拓扑结构；(2)网络资源管理：ANMS 负责网络资源的分配，以保证资源的合理使用；(3)系统的管理和服务；(4)安全控制：一是要保证 ANMS 上存储的信息安全，二是通过对 ANMS 发出的封装体进行数字签名，以证明其合法身份。

ANMS 的结构如图 3 所示，由 4 个模块组成[4]。

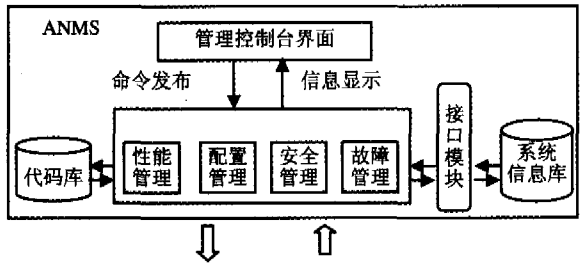

图 3 ANMS 的结构图

(1)用户界面：即网络管理员与 ANMS 之间的接口，它将网络中的资源信息、服务信息、网络运行状况和部署、数据流量等显示给管理员。管理员可以通过此界面发布网络管理命令。

(2)管理功能模块：它是 ANMS 系统的核心，负责整个网络功能的调度和收集信息的处理，它包括对网络的性能、配置、安全和故障等进行调度与管理。

(3)接口模块：提供了访问信息库的方法，可以实现对信息库的打开、创建、查找等功能。

(4)系统信息库：用于记录网络资源信息，如网络配置信息、网络资源列表、当前可用资源等。此外，还要记录网络中各个节点的信息。

2.3 主动节点管理器 ANM

ANM(ANet Node Mgr)作为主动网络管理的一部分，利用与被管理的主动节点之间的 EE 和 NOS 交互行为实现对节点的管理与控制，从而为管理程序提供共享的监视管控制节点的功能[5]。ANM 的主要功能有：(1)提供对节点的监视、控制功能。当 ANMS 为完成某项监控制功能而发出一个封装报文时，ANM 应保证封装体在当前节点上能够正确执行，同时 ANM 在安全允许的范围内应该如实报告本节点的运行状况。(2)安全控制。对 ANMS 发来的封装体和用户的身份进行合法性鉴别，根据本地节点的安全机制决定可以对节点资源实施何种访问与控制等。

ANM 在启动后，需要与 3 个部分进行通信：(1)与节点操作系统 NOS 交互。通过 NOS API 访问本地资源如 CPU、内存使用情况、资源配置、路由表的更改等；(2)与 EE 的交

互。访问 EE 的配置和性能等，掌握每个 EE 占用的 CPU 资源、内存等，从而平衡多个 EE 之间的资源分配；(3)与 ANMS 交互。为 ANMS 提供接口，使 ANMS 通过它完成对节点配置的访问与控制。

图 4 是 ANM 的结构图，当 ANM 启动后，首先要进行初始化工作，主要包括读取配置文件中的数据以配置 ANM 和 MIB 中的变量；注册 ANM 与远程 ANMS，初始化 ANM 的端口等。ANM 的主要组成有：

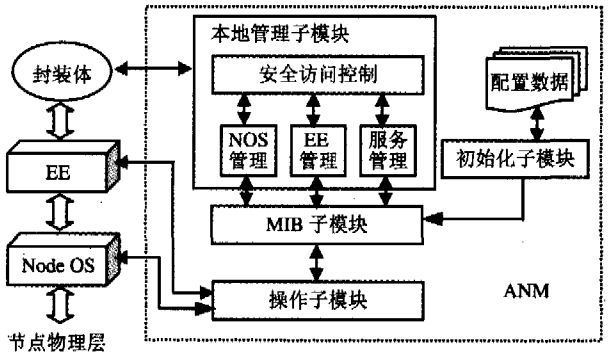

图 4　ANM 的结构图

(1)本地管理子模块。负责对节点 NOS、EE、服务等进行管理，向远程 ANMS 提供访问节点资源的机制并与 ANMS 实现通信。在初始化启动后，它维护节点资源信息，为 ANMS 访问节点资源提供服务原语，接收 ANMS 的服务请求，检测节点性能和配置参数等。它采用了 MIB 的命名方式，以对象标识符来命名被管对象，它提供了两个服务原语：get 和 set 原语，其中 set 原语用于设置被管理资源的值，get 原语用于获得当前被管理的资源值。其格式为：

get 原语：errorStatus＝get(nodeIdentify, digest, objectId, value)

set 原语：errorStatus＝set(nodeIdentify, digest, objectId, value)

其中，errorStatus 是原语执行的返回代码，errorStatus＝0 表示执行原语成功。

(2)安全访问控制子模块。其功能是保护被管理节点上的资源不受到非法访问。ANMS 所发出的封装体报文应提供所访问节点的标识符和经过密钥计算的摘要。该模块通过封装体报文中的标识符搜索访问权限库，利用权限库中的公钥来识别身份，并根据权限库中的权限列表来判断所请求的资源是否允许被访问。

(3)MIB 子模块。沿用 SNMP 中命名的资源管理方式，以对象标识符来命名被管理对象。它将 MIB 对象映射成节点的本地变量，将对外统一的管理功能接口映射成节点内部的管理功能函数。

(4)操作子模块。它通过 NOS 的 API 和 EE 提供的接口来访问它们的配置、性能数据，调用它们的配置函数。

3　ANEP 封装体及转发模式

3.1　ANEP 报文封装格式

封装体是由管理节点的 ANMS 向主动网络中节点所发出的主动报文，其格式采用 ANEP 封装。它使用四个 ANEP 的可选项：源地址、目的地址、完整性校验和和鉴定可选项[6]。鉴定可选项的细节如图 5 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。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 5　ANEP 报文的可选项结构

(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。

3.2　报文的转发

封装体是网络中实现分布式管理的主要元素，它的报文是相当灵活的，可以在传输过程中根据某个节点的状态信息进行计算，决定报文的转发方向、向管理节点返回封装体报文的类型及其携带的数据信息。这种灵活性是通过转发例程来实现的，例程存在于各个节点中，目前将转发例程分为 4 类：

(1)One-One 模式：One-One 的转发模式是一种最简单的转发模式，它又根据包是否在所经过节算分成两种结构。一是所经中间节点不执行，其方式与目前的端到端通信方式类似。二是沿传输路径计算的转发模式，在这种转发模式中，封装体报文按照指定的每到一个中间节点时，就要在该节点执行其携带的程序。通过这种执行方式，管理节点可以把集中的任务分发到沿整个传输路径上去执行。

(2)One-Multi 模式：在这种转发模式中，多个同样的封装体报文同时从一个节点发出，这些封装体报文发向不同的目的节点并且在该节点执行。这种转发模式可以用于信息的广播(如拥塞位置的检测)、子网的控制。

(3)BFST(Breadth First Search Traversing)转发模式：这是一种并行控制模式。当封装体报文到达一个主动节点后，它被转发到与当前节点直接相连的邻居节点。到达下一个节点时同样按照将该报文直接转发给相邻的节点。显然，经过一次转发后，网络中将出现很多该封装体报文的副本。当这些副本到达下一个节点后，它们又被复制，并转发到它们的邻居节点，报文副本依次转发下去，直到遍历完整个网络。

(4)DFST(Depth First Search Traversing)转发模式：这是一种串行控制模式。在该模式中，封装体报文到达一个主动节点后，它被转发到与当前节点直接相连的一个邻居节点。当它到达这个邻居节点后，它又被转发到该邻居节点的一个邻居节点，依次转发下去，直至遍历完整个网络。

4　网络拓扑发现与重构

拓扑发现是主动网络管理中一个重要的问题，其功能是发现管理员设置搜索范围内所有设备以及设备之间的连接关系，管理系统必须为网络管理员提供网络拓扑结构和网络设备的分布情况，以使管理员能够了解网络部署和运行情况。在 ANMS 系统中，网络拓扑发现可以通过 3.2 节的 BFST 转

(下转第 75 页)

7 Labrou Y, Finin T. A proposal for a new KQML specification. In: ARPA Knowledge Sharing Initiative[R]. External Interfaces WorkingGroupPaper. February1997
8 Snapp S, Brentano J, Dias G, et al. DIDS (Distributed Intrusion Detection System)-motivation, architecture, and an early prototype. In: Proceedings of the 14th National Computer Security Conference, October 1991
9 Staniford-Chen S, Cheung S, Crawford R, et al. GrIDS-a graph based intrusion detection system for large networks. In: Proceedings of the 19th National Information Systems Security Conference, September 1996
10 Porras P A, Neumann P G. EMERALD: event monitoring enabling responses to anomalous live disturbances. In: 1997 National Information Systems Security Conference, Oct. 1997
11 李毅,石纯一. 基于 BDI 的对手 BDI 模型[J]. 软件学报,2002,13(4):644~648
12 Northcutt S. Network Intrusion Detection: An Analyst's Handbook. New Riders,1999
13 Tseng C Y, Balasubramanyam P, Ko C, et al. A specification-based intrusion detection system for AODV. In: Proc. of the 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03). Farirfax Virginia,2003. 125~134
14 Vigna G, Kemmerer R. NetSTAT: A network-based intrusion detection system. In: Proc. of the 14th Annual Computer Security Applications Conference. Scottsdale, U S A, Dec. 1998
15 Undercoffer J, Joshi A, Pinkston J. Modeling Computer Attacks: An Ontology for Intrusion Detection. In: RAID 2003, LNCS 2820,2003. 113~135

(上接第 40 页)

发模式即广度优先遍历网格来实现。下面是一种通过 BFST 来获得网络拓扑的算法:

```
if(当前节点地址≠封装体的源地址){
  if(节点深度>0)
    {  count=该节点的相邻节点的个数;
       neighbor 是相邻节点网络地址的数组;
       向该节点中所有相邻且未被访问过的节点发送
       该封装体并设置其访问标记;}
    else
    {  count=0;//该节点是叶子}
     向管理节点返回报文(节点地址、父节点地址、邻节
     点个数及地址);}
else if(当前节点地址≠目的地址){
       向目的节点转发报文;}
```

如果单从封装体的转发例程逻辑上看,上述的拓扑发现是由一种广度优先搜索来实现的,但是整个拓扑发现过程是分布在每个节点上进行的,因此它并不是严格的广度优先搜索。

在生成了拓扑结构后,系统还应以最小代价维护网络最新的拓扑结构,这种功能可以用转发模式为 DFST 的封装体来实现,其转发例程基本上与拓扑发现的例程相似。当封装体到达一个节点后,它首先检查该节点的所有相邻节点是否全部已记录在节点的访问状态中。如果没有,则选择一个未记录的节点并向它转发报文。DFST 可以用最小网络带宽的情况来实现这一功能,但是它的遍历网络速度较慢。

5 主动网络管理系统中的流量分析

NMS(Network Management System)的流量是指 NMS 在网络层与所有节点交换的数据量。如果在应用层传送的数据量为 X,则在网络上传送的数据量就为 $\lambda=\xi(X)+\psi(X)X$,式中 $\xi(X)$表示在面向连接方式中建立连接时交换的控制信息,$\psi(X)$由数据包的封装格式决定。为了简单起见,数据量可简化为 $\lambda=k(X)X=kX$,称 k 为加权函数。在后面讨论中,用 M 表示被管理的网络设备的数量,用 Q 表示该任务需要对 MIB 查询的次数。

(1)基于 SNMP 的网络管理系统流量:在 SNMP 系统中,当 NMS 需要请求节点完成一项任务时,NMS 就向节点上的 SNMP 代理发送请求。假定第 i 条请求消息的大小为 Get_i,为了完成该请求任务,这 Q 条请求消息必须全部发送到所有 M 个被管理设备节点上。设备 m 收到第 i 个请求时,会做出响应,向 NMS 发送大小为 R_{im} 的响应消息。因此 NMS 的流量 T_{nms} 就可以表示为

$$T_{nms}=\sum_{m=1}^{M}\sum_{i=1}^{Q}(k_{nms}\mathrm{Get}_i+\tilde{k}_{nms}\tilde{R}_{im})$$

其中 k_{nms} 表示对请求信息 Get_i 封装时的加权函数,$\tilde{k}_{nms}$ 表示对响应信息 $\tilde{R}_{im}$ 封装时的加权函数。

(2)基于 ANMS 的网络管理系统流量:ANMS 向第 1 个节点发送一个主动包,这个包依次访问每一个节点,并在本地得到响应消息,然后带着响应消息传送到下一个节点,最后将所有响应消息传送到 ANMS。我们用 CAN 表示主动包的初始大小,则 ANMS 的流量 T_{AN} 可以表示为

$$T_{AN}=k_{AN}C_{AN}+\tilde{k}_{AN}\sum_{m=1}^{M}\sum_{i=1}^{Q}\tilde{R}_{im}$$

前一部分表示 ANMS 向第 1 个节点发送一个包,后一部分表示最后一个节点上的包将所有的响应消息发送到 ANMS。

通过分析和数据推导(过程略去),可以证明:$T_{nms}\geqslant T_{AN}$。随着网络所管理的节点数的增加,SNMP 的 NMS 流量大于 ANMS 结构的流量。

结束语 在建立原型系统时,我们采用链路层连通模式在局域网中搭建主动网络环境。主动节点的实现采用的是 ANTS 扩展环境—EANTS 以及 Janos,操作系统选用 Linux。非主动节点运行 Windows 作为操作系统。EANTS 系统是用 Java 编写的,所以,在 EANTS 上开发的基于主动网络技术的管理系统也采用 Java 编写。

主动网络管理体现了主动网络的思想,将一部分网络管理功能动态地分布在主动节点上,充分利用了主动节点的计算能力,使节点能够自动发现、解决问题,从而极大地优化了网络管理。本文讨论了一种主动网络的管理模型,该模型中各个模块相互独立、任务明确,而且在每个层都可以动态更新以适应主动网络中主动节点的易变性和主动应用的扩展性,因此网络管理的稳定性和扩展性都大为提高,适应了现代网络管理的需要。

参 考 文 献

1 Kawamura R, Stadler R. Active Distributed Management for IP Networks[J]. IEEE Communications Magazine, 2000, 38(4): 114~121
2 Shaer A E. Active Management Framework for Distributed Multimedia Systems [J]. Journal of Networks and Systems Management, 2000,16(8):49~54
3 Marshall I W, et al. Active management of multiservice networks. In: Proc. IEEE NOMS, 2000. 981~983
4 Shaer A E. Active Management Framework for Distributed Multimedia Systems [J]. Journal of Networks and Systems Management, 2000, 8:49~72
5 Brunner M, Stadler R. Service Management in Multi-Party Active Networks [J]. IEEE Communications Magazine, 2000, 38(3):281~286
6 Kiwior D, Zabele S. Active Resource allocation in Active Networks [J]. IEEE JSAC, 2000,19(3): 452~459