

基于 Smart Packets 的主动网络管理模型研究^{*}

马 燕¹ 邹显春² 康 庆¹

(重庆师范大学物理学与信息技术学院 重庆400047)¹

(西南师范大学计算机与信息科学学院 重庆400715)²

摘 要 主动网络是一种新型的网络体系,它不仅可以传送数据包,而且还可以执行数据包中特定的运算任务。主动网络为用户提供了可编程的接口,用户可通过网络中的节点动态地注入所需的服务。Smart Packets 采用紧缩格式和安全代码编写其中的程序,它能够支持主动网络管理。本文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 Smart Packets 的结构、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

The Research of the Active Network Management System Model Based on Smart Packets

MA Yan ZOU Xian-Chun KANG Qing¹

(Faculty of Physics and Information Technology, Chongqing Normal University, Chongqing 400047)¹

(Faculty of Computer and Information Science, Southwest Normal University, Chongqing 400715)²

Abstract Active network is a new framework where network nodes not only forward packets, but also perform customized computation on the packet flowing through them. It provides a programmable interface to the user where users dynamically inject services into the intermediate nodes. Smart Packets programs are written in a tightly-encoded, safe language specifically designed to support network management. This paper analyzes the problems of tradition network management, the structure and mechanism of the active network management system. It introduces Smart Packets and describes the Smart Packets architecture, the mechanism of management, the packet formats, the language and its design goals, and security.

Keywords Active network, Network management, Smart packets, Model

主动网络 AN(Active Network)是针对传统网络发展中所遇到的实际问题而提出来的。主动网络是一种全新的网络计算模型,它赋予网络“编程”能力,允许用户向网络节点插入定制的程序或在报文插入程序代码,以便修改、存储或重定向网络中的数据流。主动网络是一种区别于传统网络的全新体系结构,为网络的快速发展提供了一个契机。

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 ANM 模型(Active Network Management),它改变了过去传统网络集中式管理的不足,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 主动网络

主动网络是由一系列主动节点所构成,其基本思想是利用包含有可执行的代码的主动信包代替传统网络中的信包,利用可编程的主动节点代替传统网络中的中间节点。

目前国际上已认可了三层式的主动网络体系结构方案。主动网络节点可由三个部分组成:

(1)节点操作系统(NOS):NOS 与主动网络节点的硬件资源接口共同管理和控制对主动网络节点的硬件资源的使用,并对资源(如传输、计算、存储)之间进行协调。它包含5个组件:信包仲裁:对信包的类型进行鉴别并设置相应标志,进行相应处理;路由:实现对信包传输的路由选择;策略库:存放

一些安全策略和管理策略,在进行安全和管理检测时调用该库;代码库:存放要加载的 AC(Active Code),执行信包中代码时调用该库,在运行中可以临时加载该库;安全检测:当 AC 需要访问节点资源时进行安全检测。

(2)执行环境(EE):执行环境 EE 定义了一个虚拟机 VM 和可编程接口,它类似于通常计算机系统中的一个“shell”程序。EE 主要完成对主动报文的解释执行,是一个为用户提供端到端网络服务的接口。

所有用户对结点资源的访问都是由 EE 提供的。一个主动结点可有多个 EE,每个 EE 上可定义不同的虚拟机或接口,各个 EE 之间是相互独立的。

(3)主动应用(AA):主动应用 AA 是主动网络提供给用户的服务,用户通过 AA 向主动网络提出请求。一个 AA 由一段程序代码(主动代码)和与主动代码相关的数据、状态参数等组成,它由主动结点上某个特定的 EE 来执行,实现端到端的服务。

2 主动网络管理

2.1 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 Informa-

^{*}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”资助项目([2003]2号)。马 燕 教授,主要研究方向:计算机网络新技术、多媒体数据检索。邹显春,康 庆 副教授,主要研究方向:计算机网络管理、数据挖掘。

tion 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。

SNMP 协议在现代网络管理中存在着很多问题,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。

2.2 主动网络管理系统

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待的关系,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。在主动网络管理 ANM(Active Network Management)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。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)提供了主动信包运行和处理所必需的环境;MEE(Manager EE)负责主动节点的全局管理功能。

对于主动网络而言,网络管理也应完成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。除实现传统的网络管理功能外,主动网络管理主要应实现下述要求:

(1)新的管理业务动态加载:主动网络应具有动态新业务加载的功能。在主动网管系统中,针对新的业务,用户可以编制相应的管理业务代码并将这些管理业务动态地加载到主动节点,不需要变动原有的管理功能、管理信息库等,这有利于新的网管软件、协议的开发。

(2)动态 MIB 的创建与维护:在实际运行中,主动节点的结构和行为可能会发生变化。当一个主动网管系统运行之前,一些被管实体的 MIB 可能还是未知的。为了适应这种特点,主动网管系统必须提供一种可动态创建和维护的 MIB 机制来捕获和表达主动节点的动态结构和行为,可以根据管理业务的需要,动态地构建被管实体的 MIB,并加载到主动节点中,同时动态地进行维护和管理。

(3)与 SNMP 相兼容:主动网管系统应提供动态的 MIB 来实现对节点的管理。因为当主动节点中某些新业务增加使原有的 MIB 信息不够用时,需要增加新的信息来生成一棵新的 MIB 子树,以使网管系统能够从 MIB 中获得管理所需要的信息。

(4)代码移动:主要指网管工作站怎样将主动业务和代码加载进入主动节点。利用主动网络本身技术,实现代码移动的方法有两种:离散型和集成型。这两种方法分别适用于美国 Pennsylvania 大学项目组研制出来的基于可编程的交换节点(Programmable Switch)的离散方案如 Switchware 和 MIT 实验室提出来的基于容器(Capsule)的集成方案如 Active-

ware 的体系结构。

3 基于 Smart Packets 的主动网络管理

3.1 Smart Packets 的结构

Smart Packets(智能包)的管理方案是运用主动网络技术和网络的管理的综合应用方案。Smart Packets 运用主动网络封装协议 ANEP(Active Network Encapsulation Protocol)实现包的封装,它由 IP 包头、ANEP 包头、Smart 包所组成。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报内容。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,其包头有四个域:版本号、类型、上下文和序列号,如图1所示。版本号用来标记语言的升级和包格式的改变。类型域标记下列四种类型之一:程序包、数据包、错误包或消息包。

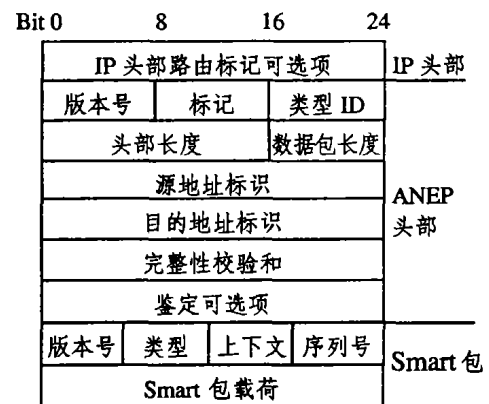


图1 采用 IP 和 ANEP 封装的 Smart 包

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。

为了不给主动结点造成过重的负担,并保证结点自身的安全性,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。

3.2 节点管理模型

根据 Smart 包的特点及主动网络的结构特征,我们提出了一种基于主动网络的管理模型 ANM。该模型运用 Smart 包的特点,将管理工作分散到主动网络的各个节点上。充分利用了主动网络的主动性、动态性和智能性,以实现主动网络的公布式智能管理。图2显示了运用 Smart 包的主动网络传输模型。在该模型中,用户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 即为用户管理程序(Network Management Program),它是可传送的 Smart 包;图中的 D 即为 Daemon,它驻留在网络中的节点中,Smart 包在网络中的传送有端到端(end-by-end)或逐跳转接(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 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。

图3显示了流向主动网络节点的各种包流在节点进行处理和传输的示意图。从图中可以看出,流向节点的包有多种(IP 包、UDP 包、ANEP 包),通过 AN(Active network) Daemon 进行接收、分类处理和传送。ANEP 自适应数据鉴定器和

监视器 Daemon 有两个任务:一是负责对 Smart 包的注入和接收;它同时还包含一个虚拟机(Virtual Machine)以便运行节点所接收到的程序代码。

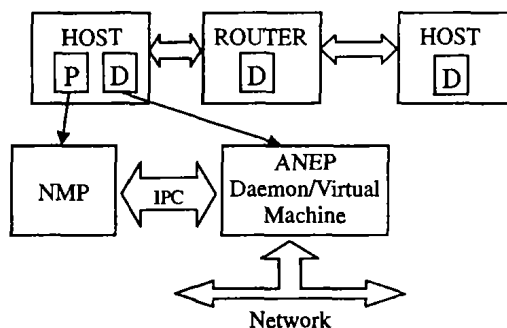


图2 运用 Smart 包的主动网络管理结构

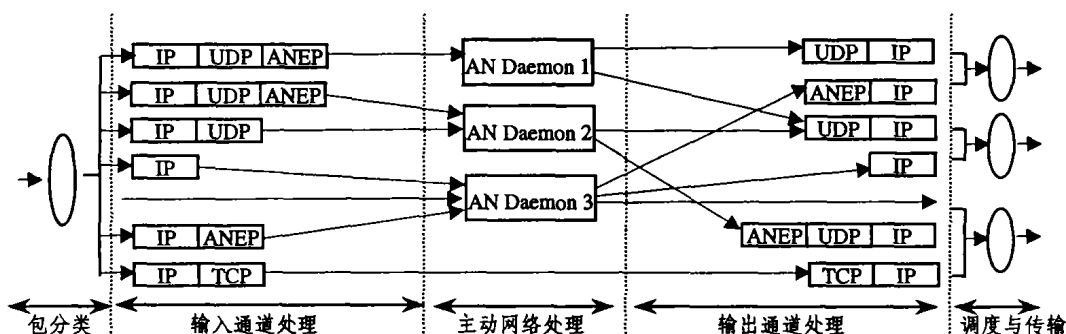


图3 流向主动网络节点的 Smart 包流

在节点中,操作系统中安全策略数据库(Security Policy Database)和安全执行引擎(Security Enforcement Engine)保障了结点的安全。当 AA 或者 EE 中的实体需要结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。结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、代码或结点的安全等。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 类似于一般计算机系统上的“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。

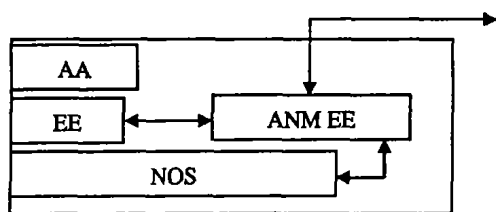


图4 主网络管理系统中的节点

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。

3.3 Smart Packets 的封装

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 Smart 包的 ANEP 可选项

Smart 包采用 ANEP 标准进行封装。图1已显示了 ANEP 的头部,Smart 包使用四个 ANEP 的可选项:源地址、目的地址、完整性校验和和鉴定可选项。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:

(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。

3.4 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。

(下转第46页)

S 负责。

小结 本文主要分析讨论了 H. Kim 等人提出的移动 Agent 中的一次代理签名体制所存在的安全性问题。该体制应用故障-停止签名保证代理签名的一次性要求。但是它不满足抗伪造攻击这一性质。而在移动 Agent 中,为保证代理签名以及秘密计算的安全性需求,要求系统能够抵抗伪造攻击。通过我们的分析,可以看到 H. Kim 等人提出的一次代理签名方案中不诚实的原始签名人即不诚实的客户可以成功地伪造有效的代理签名。因此该方案需要进一步改进以保证移动 Agent 的安全运行。

参考文献

1 Kim H, Baek J, Lee B, Kim K. Secret Computation with Secrets for

Mobile Agent using One-time Proxy Signature. In: Cryptography and Information Security 2001, 2001

- 2 Okamoto T, Tada M, Okamoto E. Extended proxy signatures for smart cards. In: Information Security Workshop (ISW'99), LNCS 1729, Springer-Verlag, 1999. 247~258
- 3 Lee B, Kim H, Kim K. Strong proxy signature and its applications. In: Proc. of SCIS, 2001. 603~608
- 4 Park H-U, Lee I-Y. A digital nominative proxy signature scheme for mobile communications. In: Information and Communications Security (ICICS'01), LNCS 2229, Springer-Verlag, 2001. 451~455
- 5 Sun H-M, Hsieh B-T. On the Security of Some Proxy Signature Schemes. Available at: <http://eprint.iacr.org/2003/068>
- 6 Yi Lijiang, Bai Guoqiang, Xiao Guozhen. Proxy multi-signature scheme. Electronics Letters, 2000, 36: 527~528

(上接第39页)

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新的特征。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。

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

第二种是 Spanner 语言,它是一个基于 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。

4 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完整性。鉴定可选项规定了对数据报文签名的实体,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。包含在 Smart 包中的授权是安全结构的第二部分,有两个主要的授权因素:

(1)控制 MIB 访问,它包含 MIB 的视图与读/写权限。

(2)在虚拟主机中进行时间环境限制了每次调用被发送数据包的最大数量,能够被分配的最大内存数,每次调用能被执行的最大指令数。

用户标识的获取来自于鉴定组件,用来获得在数据库中的程序的资源限制,这些限制被设定在虚拟机当中,虚拟机实施这些限制在主机资源和对特权指令的访问控制上。

一个被鉴定的智能包携带了 X.509 公钥认证来标识智能包的发送者。数据签名用来验证数据完整性,使用数字签名防止了恶意篡改数据包的这些部分。

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。

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。

要实现上述的服务,就需要增加 Smart 包中证书域所占用的空间大小。例如, X.509 公钥认证包含有长度约为 400 bytes。另外一个问题就是验证证书所需要的时间与资源,很多的减少处理证书时间的方法都是通过增加数据包中的附加验证信息来实现的,因此这些方法都有一定的局限性。

结束语 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地简化以适应 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的作用。

参考文献

- 1 Fry M, Ghosh A. Application Layer Active Networking. Computer Networks, 1999, 31(7): 655~667
- 2 Marshall I W, et al. Application Layer Programmable Internet work Environment. British Telecom. Technol. J., 1999, 17(2): 82~94
- 3 Fatta G D, Gaglio S, Re G L, Ortolani M. Adaptive Routing in Active Networks. IEEE Openarch 2000, Tel Aviv Israel, March 2000
- 4 Schwartz B, et al. Smart Packets: Applying Active Networks to Network Management. ACM Transactions on Computer Systems, 2000, 18(1): 67~88
- 5 Wetherall D, Legedza U, Gutttag J. Introducing New Internet Services: Why and How. IEEE Networks Magazine, May/June 1998
- 6 Marshall I W, et al. Active management of multiservice networks. In: Proc. IEEE NOMS, 2000. 981~983
- 7 Fatta G D, Re G L. Active Networks: an Evolution of the Internet. In: Proc. of AICA2001 - 39th Annual Conf. Cernobbio, Italy, Sept. 2001