主动网络及其在电信网中的应用

符云清　梁　柱　梁　忠
(重庆大学计算机学院　重庆400044)

摘　要　本文通过对现有电信网络及其业务的特点,以及主动网络技术的特点等的分析,结合网络技术发展的实际情况,提出了未来基于主动网络的电信网络体系结构。

关键词　电信网络,主动网络

Active Network and it's Application in Telecommunication Network

FU Yun-Qing　LIANG Zhu　LIANG Zhong
(College of Computer Science & Engineering, Chongqing University, Chongqing 400044)

Abstract　This paper analyzes the character of telecommunication network and business, active network and the development of network technology. Then we present the architecture of telecommunication network on the basis of active network in the future.

Keywords　Telecommunication network, Active network

1　电信网络的现状与存在的问题

1.1　我国电信网络的现状

1.1.1　*电信网络的组织形式*　我国电信网络主要由三大网络平台构成:话音网络、基础数据网络和宽带IP数据网络。话音网络包括公共交换电话网(PSTN)和公用陆地移动通信网(PLMN);基础数据网络主要包括分组通信网、数字数据网、帧中继和ATM网络;宽带IP数据网络包括国际互联网和宽带IP城域网等。

目前X.25网已逐渐退出使用,数字数据网和帧中继正逐步与ATM网实现整合,因此电信数据网络主要由ATM网和IP网络组成。

1.1.2　*电信网络所提供的业务*　从整体上看,目前电信网络是业务和网络捆绑的结构,如图1所示,即不同的业务需要不同的业务网络来提供,各种业务网络只能共用传输层以下网络资源。

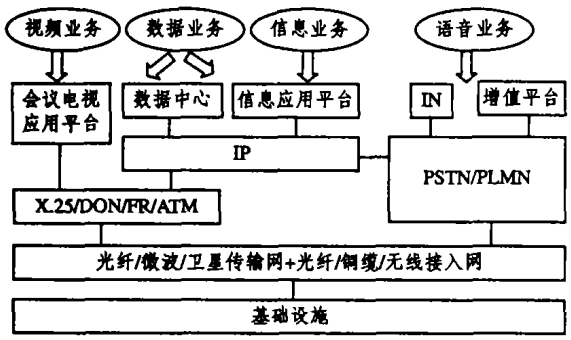

图1　我国电信网络结构状

1.2　电信网存在的问题

电信业的开放与竞争,从根本上改变了电信运营商的运营方式。为了确保未来的持续发展,电信运营商一方面在不断扩大其网络规模,另一方面不断完善运营价值链,进行创新业务的开发。但是目前的网络体系结构将运营价值链分割为设备制造商、网络/业务运营商、内容提供商和用户等几个部分,使得开发新的协议、技术、功能和业务的过程相当复杂。一种新的业务从原型系统的设计到大规模的应用,一般而言,往往需要大约10年的时间。资源预留、MPLS、IPv6等就是因此而不能大范围地进入实际应用的最好佐证。

因此运营商需要建立一种面向应用和用户的、由业务驱动的新的网络体系结构,并以此为基础重构运营价值链,丰富业务种类,保持业务增长。

随着网络技术的发展,特别是主动网络技术的迅速发展,为电信网络的合理化建设、缩短新协议和新技术的应用周期以及丰富电信服务业务种类提供了契机。在这种情况下,我国的电信网络如何演进,如何决定网络的演进策略,本文的目的即提出一些针对性策略,进行一些探讨。

2　主动网络技术

2.1　主动网络技术简介

主动网络(Active Network)的概念是由美国国防部的高级防御研究计划管理处(Defense Advanced Research Projects Agency, DARPA)研究协会于1995年提出的。其主要目就是要解决现有网络体系结构在开发新技术、扩展新应用时存在的诸多不便。在主动网络中,网络节点(路由器、交换机等)不仅能转发报文而且可以执行来自于终端用户、网络管理者、网络服务提供者或其它网络节点的程序。这使主动网络具有"可编程"能力。这种新特性使主动网络能够动态使用新的协议,方便新业务的开展,并用一个平台提供了现有网络需要附加设备才能完成的增值服务。

2.2　主动网络的体系结构

主动网络节点的体系结构可以分为三个部分:节点操作系统(Node OS)、执行环境(Execution Environment, EE)和主动应用(Active Application, AA),如图2所示。

节点操作系统(Node OS)类似于一般的操作系统,为执行环境提供了赖以生存的基本功能,如I/O管理、存储器管

理、文件管理等资源管理功能，并为执行环境提供了一个固定接口。因此，节点操作系统把执行环境从资源管理的细节及其它执行环境的行为的影响中分离出来，而执行环境则反过来把与每个具体应用交互的细节从节点操作系统中独立出来。同时节点操作系统具有策略数据库和安全环境引擎。

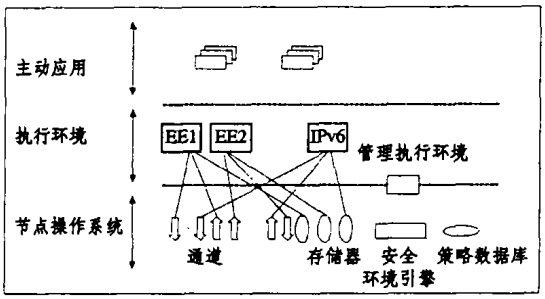

图2 主动节点的体系结构

执行环境(EE)为主动网络中的主动应用在主动节点上提供了一个临时执行环境。一个主动网络节点可以具有多个执行环境。通常，执行环境定义了可编程的网络接口 API 或虚拟机。

主动应用(AA)可以是主动网络用户的主动应用或者是主动网络的主动包，通常由一段主动代码和与主动代码相关的数据、状态参数等组成。主动应用通过执行环境实现用户定制的网络服务。

2.3 主动网络的实施方法

目前，主动网络已有多种实现方案，其中最典型的有三种。

第一种方法是可编程路由器或交换机法(Programmable Switch)，其主要思想是保留现在的报文包格式，而主动程序是由网络管理员预先安装在网络节点上或者是从主动代码服务器或其它网络节点下载得到。在这种方案中要让主动节点执行用户定义的功能就需要先将用户的主动程序发送到节点上，程序会被暂时储存在主动节点的存储空间里。然后用户发送想要处理的数据报文。当报文按照它在现今网络中的传输方式到达中间节点时，节点会根据报文头的信息来确定应该用哪个用户程序来处理。

第二种方法是数据舱法(Capsule)。它改变了现在的报文格式。报文帧不仅仅包含数据，而且还包含了小程序段，即每个报文包都是程序。这种集成法数据和程序的报文被形象地称之为数据舱。数据舱代替了现有网络中的被动数据包，在网络中传输。数据舱到达主动节点时，其中的小程序可以被主动网络的主动节点检查识别并在节点上执行。

第三种方法是将前两种方法的基本思想相结合，根据实现主动应用所需程序代码的大小，将较短的程序段随主动包传送，而将较长的应用程序预先存放在主动节点上。这种方法实现的主动应用的灵活性更高。

3 主动网络技术在电信网中的应用

3.1 基于主动网络的电信业务模型(TBMBA)的体系结构

采用主动网络技术能建立一种面向应用和用户的、由业务驱动的新的网络体系结构——基于主动网络的业务模型(TBMBA)，如图3所示。在该模型中，充分利用了主动网络的主动性、动态性和智能性，以实现电信业务的快速部署。其基本思想是：把业务管理程序发送各个主动节点，在主动节点中运行业务管理程序，实施网络管理、认证计费等管理功能。

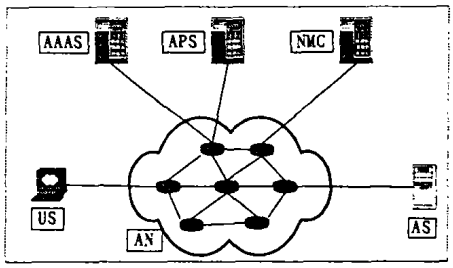

图3 基于主动网络的业务模型(TBMBA)

其中：

US 为 TBMBA 中的客户集合，记为 $U=\{u_1,u_2,\cdots,u_i\}$，$i\to\infty$；

AN 为 TBMBA 中的主动节点集合，记为 $AN=\{An_1,An_2,\cdots,An_j\}$，$j\to\infty$；

AS 为 TBMBA 中的各种应服务的集合，记为 $S=\{S_1,S_2,\cdots,S_k\}$，$k\to\infty$；

NMC 为 TBMBA 中的网络管理中心；

APS 为 TBMBA 中的主动代码服务器；

AAAS 为 TBMBA 中的认证、授权、计费服务器。

3.2 TBABM 的组成及工作机制

User System 客户——在需要定制新业务的时候，客户端的业务管理机制发出主动包在相关的主动节点上动态部署业务，客户端的业务管理机制与部署在主动节点上的业务管理机制相互交互实现相应的业务环境，获得所需的业务服务。

Active Node 主动节点——主动网络的中间节点，负责进行主动包的“存储-计算-转发”，有一个或多个主动网络执行环境，可动态部署主动网络服务。基于主动网络的业务机制在主动节点操作系统 NodeOS 的基础上，实现业务执行环境，为开展业务提供支持，包括业务执行环境、动态部署的业务及相关管理、安全机制。

Application Server 应用服务器——在收到应用服务请求后，提供各种应用服务。

Network Manage Center 网络管理中心——负责管理网络平台和网络业务两个层面：网络平台管理主要针对网络本身(包括网络的各个组成部分以及相关软件、规程协议系统)的管理；网络业务管理是对在网络上运行的各种业务进行管理，包括业务特性的监控等。

Active Program Server 主动代码服务器——负责存储由电信运营商提供的可供主动节点使用的主动代码。在收到主动节点的请求后，将开展相应业务所需的主动代码动态部署到主动节点上，为用户提供开展业务所需的网络环境。

AAA Server 认证、授权、计费服务器——实现对用户的认证、计费、用户管理和计费策略管理功能。它是整个模型提供的中央服务器，由 AAA Server 实现对用户的认证，并跟据用户定制的服务灵活计费，完成各个用户的各种服务的计费结算和综合统计功能。

在 TBMBA 中客户可以根据应用所需的网络服务质量，选择运营商提供的相应业务，运营商则按照客户使用的不同业务采取不同的资费标准，对客户进行合理计费。例如：客户在进行一般的网页浏览时可以选择低 QoS 的服务，而在进行网络视频会议等重要的商务活动时，又能方便地选择高 QoS 的服务。

运营商可以在对网络硬件设备不进行改动的情况下，将

开发的新业务快速部署在网络中，而在传统的电信网络，业务是通过事先在中间节点进行业务配置来实现的，即静态的业务配置机制。在 TBMBA 中运营商能以较低的成本实现丰富业务种类、保持业务增长目标。因此与传统的网络模式相比，客户和运营商都获得了满意的结果。

结束语 本文介绍了主动网络的体系结构和电信网络的现状，并遵照主动网络的原则和电信行业发展的趋势，提出了基于主动网络的电信业务模型。利用 TBMBA 运营商能有效地完善运营价值链，进行创新业务的开发，保持业务增长。

AN 提出了一种全新的体系结构，但是 *AN* 离实际应用还有距离，必须解决效率、安全等问题，才能真正推广。因此，面对主动网络提出的挑战，我们还必须作出不断的努力。

参 考 文 献

1 Smith J M, et al. Activating Networks: a progress report. Computer, 1999(324)

2 Merugu S, Bhattacharjee S, Zegura E, Calvert K. Bowman: A Node Os for Active Network . Infocom, 2000

3 Tennenhouse D L, Wetherall D. Towards an Active Network Architecture. In Multimedia Computing and Networking 96, 1996

4 CRA. Research Challenge for the Next Generation Internet. http://www. whitehouse. gov/WH/EOP/OSTP/NSTC/html/97ann-rpt. html.

5 Active storage network. http://www. ece. cmu. edu/~asn/research. html

6 任丰源，任勇，山秀明. 主动网络的研究和发展[J]. 软件学报，2001, 12(11): 1614～1622

(上接第40页)

(2)提供对组播的安全保护。组播的应用能够有效地减少网络流量，特别适用于军事指挥网络。现行大多数的安全方案只停留在如何保护路由信息的完整性，如何实现对单个节点的认证，没有考虑如何实现对组播的安全支持。只有少数如文[19,20]论述了安全的组播，对移动 ad hoc 网络环境下的安全组播的研究还很不完善，需要进一步发展。

(3)如何保护节点通信量和位置的信息。通过通信量的分析能够确定网络中节点的角色，再确定节点的位置，就可将攻击指向网络的要害，如：网控中心、集中的 CA 或军事指挥网中指挥员等。

各种针对中路由协议的攻击及对策。如：wormhole、rushing 攻击等，因为移动 ad hoc 网络的复杂性，也许还存在许多新类型的攻击尚未发现。

(4)路由安全算法研究主要集中在 DSR、AODV、DSDV 路由协议上，还应拓展其范围，设计一些其他路由安全算法，如基于位置的路由安全协议、基于能量的路由安全协议、层次路由安全协议等。

(5)链路层和高层的安全协议的研究。

参 考 文 献

1 Corson S, Macker J. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC 2501, Jan. 1999

2 Hu Y-C, Perrig A, Johnso D B. Wormhole Detection in Wireless Ad Hoc Networks: [Technical Report TR01-384]. Department of Computer Science, Rice University, Dec. 2001

3 Deng Hongmei, Li Wei, Agrawal D P. Routing Security in wireless Ad hoc Networks. IEEE Communications Magazine, Oct. 2002. 70～75

4 Hu Y-C, Perrig A, Johnson D. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. In: Proc. of the ACM Workshop on Wireless Security (WiSe 2003), Westin Horton Plaza Hotel, San Diego, California, U S A, 2003

5 Johnson D B, Maltz D A, Hu Y-H. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), Internet-Draft, draft-ietf-manet-dsr-09. txt, 15 April 2003. http://www. ietf. org/internet-drafts/draft-ietf-manet-dsr-09. txt

6 Perkins C E, Belding-Royer E M, Das S R. Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, July 2003. http://www. ietf. org/rfc/rfc3561. txt

7 Perkins C, Nhagwat P. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. In: Proc. of the ACM SIGCOMM Conf. on Communication Architectures, Protocols, and Applications, Aug. 1994. 234～244

8 Papadimitratos P, Haas Z. Secure routing for mobile ad hoc networks. In: Proc. of the SCS communication Networks and Distributed Systems Modeling and Simulation Conf. San Antonio, TX, Jan. 2002

9 Hu Y C, Perrig A, Johnson D B. Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks. In: Proc. of the MobiCom 2002, Sep. Atlanta, Georgia, USA, 2002

10 Perrig A, Canetti R, Song D, Tygar J D. Efficient and secure source authentication for multicast. In: Proc. of Network and Distributed System Security symposium, Feb. 2001. 35～46

11 Sanzgiri K, et al. A Secure Routing Protocol for Ad Hoc Networks. In: Proc. of 2002 IEEE Intl. Conf. on Network Protocols (ICNP), Nov. 2002

12 Hu Y-C, Johnson D B, Perrig A. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In: Proc. of the 4th IEEE Workshop on Mobile Computing Systems & Applications, WMCSA, IEEE, Calicoon, NY, June 2002 . 3～13

13 Rivest R L. The MD5 Message-Digest Algorithm, RFC1321, April 1992

14 Zapata M G. Secure Ad hoc On-Demand Distance Vector Routing. ACM Mobile Computing and Communications Review (MC2R), 2002, 6(3): 106～107

15 Zapata M Z, Asokan N. Securing Ad-Hoc Routing Protocols. In: Proc. of the 2002 ACM Workshop on Wireless Security (WiSe 2002), Sep. 2002. 1～10

16 Papadimitratos P, Haas Z J. Secure Link State Routing for Mobile Ad Hoc Networks. In: IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 Intl. Symposium on Applications and the Internet, Orlando, FL, Jan. 2003

17 Haas Z J, Pearlman M R. The Performance of query control schemes for the Zone Rounting Protocol, ACM/IEEE Trans. net, 2001, 9(4): 407～438

18 Hu Y-C, Perrig A, Johnso D B. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In: Proc. of the Twenty-second Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM 2003), IEEE, San Francisco, CA, April, 2003

19 Kaya T, Lin G, Noubir G, Yilmaz A. Secure Multicast Groups on Ad Hoc Networks. In: Proc. of the 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), George W. Johnson Center at George Mason University, Fairfax, VA, USA, 2003

20 Lazos L, Poovendran R. Energy-Aware Secure Multicast Communication in Ad-hoc Networks Using Geographic Location Information. In: IEEE Intl. Conf. on Acoustics Speech and Signal Processing, Hong Kong, China 2003