主动网络的安全技术探讨*

李一果** 温蜀山 孙海荣 李乐民
(电子科技大学宽带光纤传输与通信系统技术国家重点实验室 成都 610054)

【摘要】 介绍了主动网和网络安全的概念，引入了安全主动网环境的模型，对主动网的安全问题进行了分析和讨论。通过对主动网安全环境的阐述，以及对目前主动网安全方面的研究情况的介绍，论证了安全性在主动网系统中的重要性。说明了对主动网安全性问题的研究及解决，是主动网技术进入大规模实用化的一个先决条件。

关 键 词 主动网； 网络安全； 安全主动网环境
中图分类号 TN913.24

主动网比传统网络具有更大的灵活性，它可以在分布式系统中更好地协调不同设备的工作，将计算所需的负荷和数据传输的负荷合理地分担给不同设备，有效地避免单点故障，并能缩短数据处理和数据传输的时延以及提高数据的端-端可达性。在主动网中可根据网络的当前状态对路由器等交换设备的缓冲进行更为细致的管理，并对数据流所携带的信息进行归类和缓存，更好地利用冗余路径进行数据传输，从而降低拥塞的概率和程度，提高网络的当前性能和可预测性[1]。

在提高灵活性的同时，主动网也对网络的安全性提出了挑战。因此对主动网安全性问题的研究及解决，是主动网技术进入大规模实用化的一个先决条件[2]。

1 主动网

主动网(Active Network)，也称可编程网(Programmable Network)，由于其崭新的思路、强大的功能和广阔的应用前景，已成为通信网领域的一个研究热点。

目前使用的网络只完成信息的传输与交换，各网络节点对信息处理的能力和权限十分有限。在网络传输中，路由器可改写数据包头，但它仅对用户数据进行透明传输，不做任何检查和修改，网络的中间节点只是被动地传输数据包。这种网络可视为“被动网”[3]。

主动网则是一种全新的模式，它将用户数据与一段处理程序一起封装入分组中，在网络节点上运行分组中的程序，完成预定的操作，改变节点状态，使网络能够根据实际情况和用户需求进行变化[4]。

主动网中的交换设备之间以及交换设备和用户之间可以交换程序代码，有利于提高网络协议的适应性，具有比传统网络更为强大的交互能力。同时，用户可以按自己的需要制定程序并交由网络执行，使新的应用和服务更快地完成从构思到实现的转变，而不必受传统网络标准化进展缓慢的限制。由此可见，主动网技术具有广阔的应用前景。

2 主动网的安全问题

2.1 网络安全

计算机信息网的产生和发展，标志着传统的通信保密时代过渡到了信息安全时代，从广义来讲，网络的安全性包括两个方面：1) Safety，指合法用户出错之后系统进行的保护；2) Security，

2000年5月29日收稿
* 国防科研基金资助项目
** 男 24岁 硕士生

指防止非法用户入侵或超越使用权限，这种网络安全可以分为四个相互交织的部分：保密、鉴别、反拒认和完整性控制。

2.2 主动网的安全问题及解决途径

在一个传统网络体系中，大多数的安全问题是在网络的边缘进行解决的。但是位于网络内部的服务如路由和路由更新，也同样会产生安全问题。

在主动网中，主动数据包会产生一些在传统网络中无法遇到的问题，如毁坏资源、拒绝服务、偷取信息等，这些问题有些是由于数据包发生错误所致，有些则是黑客利用主动网的强大功能来达到自己的目的。为了保护节点和数据包不受利用和攻击，可采取主动数据包的安全认证、监测与控制、运行代码认证等措施。即采用容错和加密的技术来保护主动网[5]。

在主动网中，当一个含有可执行代码的数据包到达一个节点时，系统必须进行如下操作：

1) 获取数据包的认证信息；
2) 确认发送网络单元；
3) 确认发送方；
4) 根据确认的用户权限给与相应的资源；
5) 根据确认的用户权限决定是否允许代码运行；
6) 在运行过程中监控代码对系统资源的访问情况；
7) 如果需要，对数据包进行加密以便在传输过程中保护代码和数据。

2.3 安全主动网环境

SANE (Secure Active Network Environment) 是一个解决主动网安全问题的方案。在 SANE 中，安全性被定义为：静态与动态两类。静态关注的是不需要经常检查的问题，如网络启动；动态关注的是需要经常检查的问题。前者可以很复杂，但必须非常安全；而后者应足够简单实用，以免影响性能。在主动网中主要考虑的是动态问题。

SANE 是一个分层的体系结构。体系的下层确保系统启动到预想的状态，它通过使用一种安全启动结构 AEGIS 来实现的，这属于静态检查。然后进行以每个用户或每个数据包为单位的“动态”检查，这是由高层来实现的。系统按以下方式保持安全性：

1) 系统进行安全认证，如果需要，进行点到点的认证；
2) 提供一个受限的运行环境给接受到的程序；
3) 使用一种新的命名方式在各用户之间区分节点的服务名空间。

如图1所示，安全启动系统(AEGIS)假定系统 BIOS 的最初32 K 字节是不可修改的，存放着加以保护的密钥源。如果系统具有自动恢复功能，那么这个可信赖的密钥源存放在一个可以恢复被损坏部分的位置。有了以上的假设，安全启动进程便可以在用户进入每一级系统之前进行密码认证。

如果认证失败，AEGIS 系统便开始尝试进行恢复。因为安全启动应该是在工作人员无法到达的网络部分，需要远程恢复。如果能够提供一个可以信赖的部分，它会给被损坏的部分提供一份正确的拷贝，安装之后，系统便可以重新启动。AEGIS 系统使用了一种新的技术 CLIC(Chained Layered Integrity Checks)应用于可修改的体系结构。

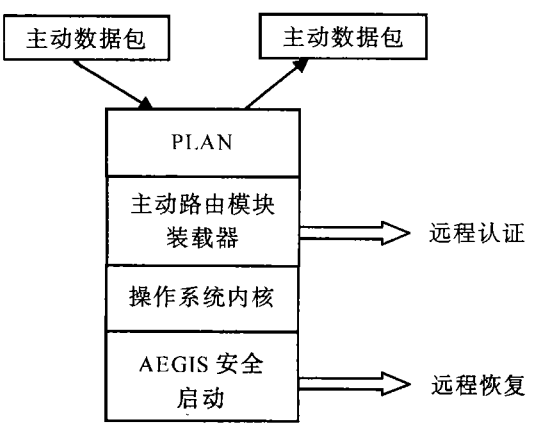

图 1　SANE 与交换设备的关系

3 字数据网远程测试系统

通信网的故障测试是维护网络正常运行及网络故障迅速恢复的关键。传统的故障测试以手工为主，在故障发生后派遣专业人员到故障发生地，利用专业仪器设备进行测试和诊断。随着通信网的发展，网络规模不断扩大，新业务、新技术不断引入以及网络异构性的客观存在，传统方式已不适应现代通信网的要求。国际电信联盟 ITU-T 制定了 X.745建议，提出了通信网自动、远程测试这一新的概念。

在通信网远程测试体系结构的研究过程中，我们引入了主动网的概念，采用 Java 编程，主要完成对网络性能的测试。在安全性方面借鉴了 SANE 等安全主动网络体系的思想。Java 具有安全性、动态性、平台独立、面向对象等特性。其内在的安全机制为主动网的实现提供了安全上的支持；平台独立性使源程序一经编译，便可在各种操作系统之上执行，利于异构网络之间的互连。本文采用 Java 的远程方法调用 RMI，以实现网络测试方法的远程发送、动态加载及运行。Java RMI 是 Sun 公司定义的一套远程调用编程接口，它包含在 Sun JDK1.2中，完全符合 Java 语言规范。使用 Java RMI 能确保在不同操作系统、网络平台上运行。

在这个测试系统中，我们引入管理员/代理的模式，管理员(测试指导者)向代理(测试执行者)发送测试命令，测试执行者对被测对象进行测试并将测试结果报告给测试指导者。通信网实现自动、远程测试对于提高军用网的生存性具有十分重要的意义。

我们设计了一个演示网络远程测试的模型，在校园网上建立一个虚拟网，完成上网络远程测试功能。其基本思路是各网络节点通过多线程方式与其他节点维持一条虚电路，该虚电路以隧道方式建立在 TCP/IP 套接字之上。各网络节点包含一系列运行于 Java 虚拟机上的线程，节点的核心提供最主要的功能(包括消息传递、处理，虚电路的维持等)和动态执行程序(网络服务)的功能。主动网网络应用(数据汇总、处理，网络测试等)作为一系列的服务运行于网络之上。各节点被限制为只能访问本地资源，如内存、处理器，并能与其他节点交换消息。在研究过程中借鉴 TMN、SNMP 等方面的成果，将网络管理协议的思路引入到通信网测试体系结构中。

具体测试功能作为主动网应用运行于虚拟网之上，主要测试图1所示的测试指导者和测试执行者之间的协议、原语和协议数据单元；测试执行者与被测对象之间的协议；被测对象的测试数据库[6,7]。

4 结 束 语

随着分布式应用的迅速发展，主动网开始出现以满足在网络中定制服务的需求。主动网的主要优势在于它的灵活性。但如果没有处理好灵活性和安全性的关系，主动网无法得到广泛的实际应用。在实际工作中，灵活性和安全性常常是相互矛盾的，只有根据具体的情况在两者之间做出合理的权衡。

SANE 体系为我们建立安全主动网提供了一个很好的参考，我们可以参照其思路，根据具体情况，将主动网的优势和安全性很好地结合起来。

参 考 文 献

1 Tennenhouse D L. A survey of active network research. IEEE Comm Mag, 1997, 35(1): 80~86

2 Psounis K. Active network: applications, security, safety and architectures. IEEE Comm Surveys, 1999, 2(1): 445~457

3 Tannendaum A S. Computer networks (3rd Ed). New York: Prentice Hall, 1998

4 Wetherall D. Introducing new Internet services: why and how. IEEE Network, 1998, 12(3): 12~19

5 Alexander D S. Safety and security of programmable network infrastructures. IEEE Comm Mag, 1998, 36(10): 84~92

6 李立忠, 李乐民. 截短 RS/混合 II 型 ARQ 在衰落信道上的性能分析. 电子科技大学学报, 1999, 28(1): 1~5

7 许　都, 李乐民. ATM 网络中长相关业务排队性能的分析. 电子科技大学学报, 1998, 27(4): 357~361

Discussion About Security and Safety of Active Networks

Li Yiguo　Wen Shushan　Sun Hairong　Li Lemin

(National Key Lab of Optical Fiber Transmission and Communication Networks, UEST of China　Chengdu　610054)

Abstract　This paper introduced the concepts of active networks, network security, and security active network environment (SANE), and analyzes the security of active networks. With the describing of SANE and current developing status in this field, this paper emphasizes the importance of safety and security in active networks. It is shown that the research and solution of active networks are the precondition of its applications.

Key words　active networks;　network security;　secure active network environment

·科研成果介绍·

155 Mb/s $LiNbO_3$光开关阵列

主研人员：陆荣鑫　杨德伟　杨亚培　曹泽煌　刘永智　蒲天春等

155 Mb/s $LiNbO_3$光开关阵列为四只全封装4×4光开关阵列，具有插入损耗低、开关速率高、驱动电压低、有较好的串音衰减等特点，可用于光交换系统中。其主要技术指标为：

1) 光纤-器件-光纤的总插入损耗分别为6.5 dB、5.5 dB、5.5 dB、5.6 dB;

2) 串音衰减分别为：21.80 dB、20.66 dB;

3) 开关电源分别为：11.92 V、11.18 V;

4) 3 dB 小信号带宽大于500 MHz。