维普资讯 http://www.cqvip.com

计算机科学 1999Vol. 26№. 1

ATM 局域网安全技术浅探*)

On the Technique in ATM LANs

陈 涛 华 蓓 陈意云 李津生

(中国科技大学计算机科学技术系 合肥 230027)

摘 要 MPOA(Multi-protocol over ATM)集成了 LANE 和 NHRP 技术,不仅继承了 LAN 仿真的优点,使现有网络软件不经修改既可运行于 ATM 网络之上,而且,它允许不同子网内部的 ATM 主机间利用 ATM VCC 直接进行协议层数据通信,使 LAN/WAN 无缝连接有了技术上的保证,但同时,由于 ATM 主机之间可以建立跨越路由器,防火墙的直接连接,引发出了 ATM 局域网的安全问题。笔者在此提出了自己的解决构想:MPOASS—MPC 安全认证模型,该模型可以在最大限度利用 ATM 技术优势的同时,确保 ATM 局域网的安全。

关键词 ATM,局域网,网络安全,MPOA,MPOA 安全服务器,安全认证

一、引言

ATM 论坛于 97 年 5 月推出的 MPOA(Multi-Protocol Over ATM:ATM 上的多协议)规范 1.0,致力于提供一个可以充分利用 ATM 的 QoS 特性,且可以端对端地传送第三层协议的途径。MPOA 规范支持在不同 ATM 子网内部的 ATM 主机间利用 VCC 直接进行通信。

在 MPOA 规范里,两个处于不同的子网或仿真网络中的 MPC(MPOA Client)进行通信的方式有两种。第一种是缺省情况,数据是通过网络仿真而转发至路由器,如果数据是通过缺省的路径传输的,那么此时数据传输并没有使用 MPOA 功能,而仅仅使用的是 MPOA 系统中的网络仿真客户服务功能。第二种方式,当 MPC 通过基于 NHRP 的查询/答复协议来探索它与目标之间存在传输捷径的可能性(关于 MPC 如何发现在它和目标之间存在一个捷径的问题超出了本篇文章的讨论范围),如果捷径存在,MPC 建立一个捷径 VCC,建立完成后,发向同一 ATM 地址的数据不再通过路由功能而直接通过这个端到端的 VCC 连接传输。目标 MPC 从 VCC 捷径收到数据,在数据帧上加入合适的数据链路信息(如:MAC 信息),再将数据传送到高层模块。MPOA 规范里,两个 MPC 可以在已经建立好的一条 VCC 捷径上传输不同协议的数据,而且有关于这两个 MPC 的一切通信数据都可以利用该 VCC 来传递。如图 1 所示,位于两个子网中的 MPOA 客户机间通过缺省路径进行数据传输,而在图 2 中,两个客户机之间存在着捷径路径,那么它们就可以通过捷径 VCC 直接进行数据传输[1]。

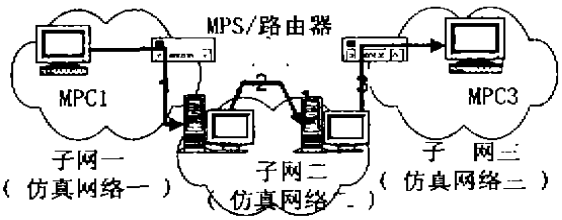

图 1 跨子网的 MPOA 客户之间利用缺省路径传输数据

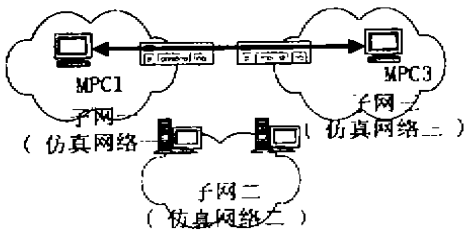

图 2 跨子网的 MPOA 客户之间利用捷径 VCC 传输数据

*) 本课题得到国家"863"重点项目的支持。陈涛 硕士研究生,研究方向为 ATM 网络技术。华蓓 教师,研究方向为网络通信。陈意云 教授,博导,研究方向主要为形式语义学。李津生 教授,博导,承担多项与 ATM 技术有关的"863"攻关项目和国家自然科学基金研究项目。

维普资讯 http://www.cqvip.com

二、MPOA 技术带来的网络安全问题

假设在某个企业的 ATM 子网(如图 3,子网一)中有一个同时对内部和外部提供服务的高性能服务器 UltraX,在这个服务器上运行有 MPC,在它与其它的 MPC 之间可以建立 VCC 连接——无论另一方是在该子网内部还是在子网的外部。该服务器的某些服务只是面向企业内部员工的——如:HTTP 代理服务,FTP 服务,EMAIL 服务和 WWW 服务等等,而来自子网外部的用户只可以使用 WWW 服务。现在有来自企业网外部的一台 ATM 主机 Y(在它上面同样运行有 MPC)正在使用 UltraX 的 WWW 服务,并且该 MPC 检测出了它和 UltraX 之间存在一个传输捷径,就与 UltraX 建立了一条 VCC 捷径。在建立完捷径 VCC 后,有关于这两个 MPC 的一切通信数据都可以利用这个 VCC 来传递。我们不难发现,Y 可以不加任何限制地使用由 UltraX 提供的一切服务。在有防火墙的时候,非法访问可以被防火墙过滤掉,但现在的情况是:如果使用了防火墙,那么 UltraX 与 ATM 主机 Y 之间就不可能建立 VCC 捷径连接。但如果不使用防火墙,则不只是类似 UltraX 之类的服务器会被非法使用,所有可以和其它 MPC 建立 VCC 捷径连接的 MPC 都在受到非法访问的威胁之中。

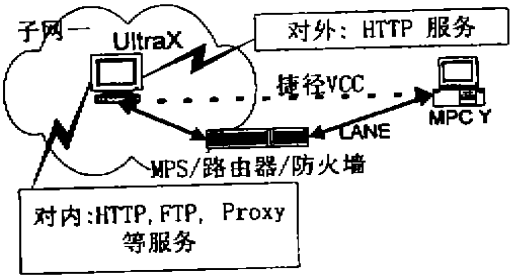

图 3 捷径 VCC 使得传统防火墙失效,特权资源受到非法访问

为什么会允许非法访问的情况发生呢?原因就在于通过 VCC 捷径传输的数据将不经由路由器或防火墙过滤功能而直接发送给了 ATM 主机的高层。

网络的安全,信息的保护,无论是在现在,还是在将来都是人们极为关注的焦点之一。人们在提出对网络带宽,服务质量的要求的同时,也提出了对网络安全的要求;特别是与国际互联网相联的用户,他们希望在充分利用互联网络资源的同时,也能保护自己的子网和主机不受到未经许可的使用和访问。我们在享受 ATM 技术所带来的优质服务的同时,必须考虑如何保护我们基于 ATM 技术的企业网,子网的安全。

三、MPOASS—MPC 安全认证模型

在我们所承担的国家"863"攻关项目中,需要解决跨子网的 ATM 主机间进行直接数据通信的问题。在 ATM 论坛推出 MPOA 规范之前,我们提出过通过扩展 LANE1.0 规范来实现这一技术。与此同时,我们就考虑到了允许 ATM 主机间进行直接通信会给 ATM 仿真网络带来的安全问题。

研究了 MPOA 规范之后,肯定了在 MPOA 技术下 ATM 局域网可能会出现的安全问题。在分析了产生安全问题的原因后,我们认为,可以通过以下 MPOASS—MPC 安全认证机制来实现保护 ATM 局域网安全的目的。(由于 MPS 往往运行在具有路由功能的 LEC 上,所以经由它们传送的数据仍然可以通过传统的防火墙进行数据过滤。所以在以下的探讨中将不再考虑由 MPS(在上面提到过的缺省路径)传输数据的情况。)

必须根据与 MPC 建立起捷径 VCC 的 MPOA 主机的不同,来限制可以通过捷径 VCC 向高层模块传送的数据。这需要设立一个 MPOA 网络安全服务器(MPOA Security Server,MPOASS),并在 MPC 模块中增加 MPC 安全检测模块和 VCC 安全管理模块。

MPOASS 统一管理一个或几个仿真网络的安全事宜。MPC 安全检测模块与 MPOASS 通信,对经由它传送给上层的数据进行安全检测,确认哪些数据可以传送至上层,哪些数据应该被丢弃;VCC 安全管理模块通过向 MPOASS 查询,标识捷径 VCC 的可信任程度,确认从哪些捷径 VCC 连接进入的数据是需要进行送给安全检测模块进行检测,哪些数据无需经过安全检测模块而可以直接送至更高层。图 4 是 MPOASS—MPC 安全认证模型的示意图。

对 MPOASS 来说,所有的 MPOA 主机可以根据可信任程度分为几个级别,如 A 类为永久可信任 MPOA 主机,B 类为临时可信任 MPOA 主机,C 类为不可信任主机。信任关系不存在传递关系。在子网内部的所有 MPC 可以设定为 A 类 MPOA 主机,即为永久可信任主机,一些特殊的 MPOA 主机可以临时成为 MPOASS 的临时可信任主机,但 B 级的 MPOA 主机可能会因为可信任时间超时而丧失

维普资讯 http://www.cqvip.com

MPOASS的信任成为C类。在子网外部的MPOA

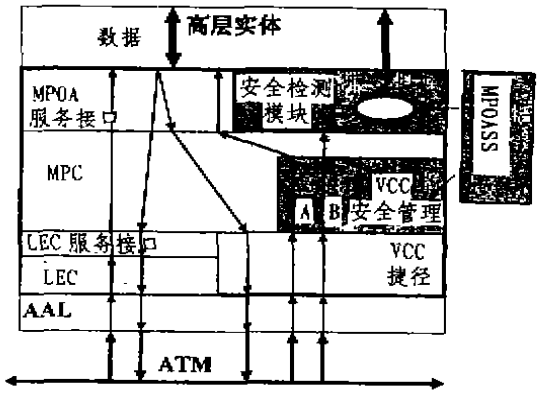

图4 MPOASS—MPC 安全认证模型

主机(已知的和未知的)被设定为C类主机。C类主机可以在一定条件下成为B类主机。

根据与子网内部MPC建立VCC连接的MPC信任级别不同,设定建立的VCC连接的两种安全类别:可信任连接和不可信任连接。与A类主机(例如:一个子网内部的MPC)之间建立的VCC捷径,是可信任连接;而与C类主机(例如:子网外部的MPC)建立的VCC连接,是不可信任连接;MPC与B类主机之间建立的VCC连接,在当MPOASS与之维持着可信任关系阶段,该连接属于可信任连接,如果信任关系超时或解除,随着该主机成为了C类主机,与它建立的连接也降为不可信任连接。

可信任连接与不可信任连接的区别在于:从可信任捷径VCC连接中传送到MPC的数据,MPC将不做任何安全性检查;而从不可信任捷径VCC连接传送来的数据,将会触发一个安全检查事件,MPC检测该数据是否属于敏感数据,对TCP/IP协议来说,敏感数据是指TCP的连接请求数据包。MPC将传统网络层防火墙所关心的数据信息(如:TCP连接端口号,对方ATM地址等)发送到MPOASS,由MPOASS根据传统防火墙的办法决定是否允许MPC将该数据传送给上层。

当MPC与其它MPC建立连接后(包括主动地建立连接和被动地建立连接),MPC向MPOASS查询连接另一端MPC的安全类别。MPOASS接收到查询请求后,查询本地数据库,根据对方的ATM地址,确定连接是可信任连接还是不可信任连接。MPOASS同时将记录连接的其它信息。例如VPI/VCI值等。发出请求的MPC根据MPOASS返回的指示,标识当前连接为可信任连接或不可信任连接。

由于有B类MPOA主机的存在,MPOASS在B类主机的信任关系取消后,将依据本地数据库的连接记录,向目前仍与该MPOA主机保持连接的MPC发送取消信任通知。

现实中存在允许个别用户先登录到网络防火墙上,再登录到子网内部的其它主机上,使用子网内部资源的情况。在MPOASS—MPC安全认证机制下,可以允许用户登录到一个传统的防火墙上,通过登录,身份认证,确认该用户可以使用子网内部资源。此时该用户使用的MPC主机对MPOASS来说仍然是C类主机。可以通过手动或自动的方式,向MPOASS申请,使用户所使用的主机由C类主机升级为B类主机。那么在用户活动的一段时间里,或在系统默认的某段时间内,用户使用的主机可以和子网内部的MPC之间建立可信任捷径VCC连接。最后,系统可以通过用户登录退出,或信任超时解除对用户使用主机的信任关系。

四、比较

我们还考虑过一种容易想到的解决方案,即在每一个MPC上运行一个类似网络防火墙功能的模块,我们称之为MPCLFW(MPC Local Firewall)模型,该模型检测从MPC传送给上层的所有数据,利用传统防火墙的功能数据进行过滤以达到保护MPC的作用。通过建立软件模拟环境,在分析了两种模型的性能和其它特性后,我们得出的结论是使用MPOASS—MPC认证方式来实现ATM局域网安全管理,其性能与MPCLFW方式基本一样,但MPOASS—MPC安全认证模型在以下几个方面有更明显的优势:

1. 可实现性 MPCLFW模型需要针对不同的操作系统,实现包含于系统内核级的功能类似的防火墙功能,这存在着重复开发的弊端。而MPOASS—MPC认证模型只要在MPOASS方实现功能全面的防火墙,MPC方实现数据分练功能,就可以完成保护MPC安全的工作。ATM子网防火墙功能更新的工作大多数情况只要更新MPOASS上的软件就可以完成。

2. 实用性 防火墙不仅要提供网络安全的保障,而且有必要向系统管理者提供有关网络安全状况,网络资源访问情况、访问记录等信息。MPCLFW模型属于各MPC分散,单独管理本机安全,通过这种形式难以搜集和了解ATM局域网或子网的总体的网络安全状况,网络资源访问情况,访问记录等信

维普资讯 http://www.cqvip.com

息。而 MPOASS 上记录了子网中，或局域网中所有 MPC 的不可信任访问的记录。所以 MPOASS—MPC 模型更具实用性。

3. 可维护性　MPOASS—MPC 认证模型为系统管理人员提供一个统一的界面，来配置网络安全的所有设置，对某台 MPC 的特殊配置也可以在 MPOASS 上完成，整个安全系统维护性很好，在 MPCLFW 中，需要对每个 MPC 进行单独设置，维护性差。

4. 灵活性　MPOASS—MPC 通过对 ATM 主机按信任级别分类的方法，在对不同的主机提供不同的安全策略方面，较 MPCLFW 模型有明显的灵活性，特别是我们在原型系统中，圆满地处理了用户先登录到网络防火墙上，利用 ATM C 类主机的 CheckIn，CheckOut 方式，使该主机由 C 类变为 B 类主机，再登录到子网内部的其它主机上，使该主机充分使用子网提供的优质服务的情况。在 MPCLFW 模型下是难以实现的。

参 考 文 献

1　ATM Forum Multi-Protocol Over ATM Version 1.0. 1997.5

2　Amxter. 1996, ATM Update Ⅱ

3　吴定一，等．异步传递模式的理论与应用．1997

4　ATM Forum. LAN Emulation Over ATM Version 2.0. 1997.7

5　Paul Wernick. British Telecom URI Security: Project Outline. 1995

6　Anthony Alles. ATM Internetworking 1995

7　Routing over Large Clouds Working Group. NBMA Next Hop Resolution Protocol(NHRP)

8　Cisco, Amxter, ATM Forum, UB Networks 等公司. 组织的主页

（上接第 49 页）

一个分组旁路的概率之和：

$$q_i=\frac{P(1)}{4}+\frac{P(1)+\cdots+P(i-1)}{2}=\frac{P(1)}{4}+\frac{\pi(i-1)}{2}\quad 1\leqslant i\leqslant n \tag{8}$$

将(8)代入(5)，经推导可得：

$$\pi(i-1)=[\pi(i)-\pi(1)]\left\{1-\frac{\pi(1)}{2}-\left[\frac{\pi(i)-\pi(1)}{4}\right]\right\}\quad 2\leqslant i\leqslant n \tag{9}$$

一个分组在状态 1 不被旁路的概率为 $1-\pi(1)/4$，不被旁路意味着此令牌携带的分组到达其目标结点。因此网络的吞吐率为：

$$\Lambda=2N\pi(1)\left[1-\frac{\pi(1)}{4}\right] \tag{10}$$

虽然我们无法从(7)和(9)解出 $\pi(1)$，但可以证明系统不存在不稳定区域。

证明：$\frac{d\Lambda}{d\pi(1)}=2N\left[1-\frac{\pi(1)}{2}\right]>0$ (11)

据(9) $\frac{d\pi(i)}{d\pi(i-1)}=\frac{\left\{1-\left[1-\frac{\pi(1)}{2}\right]\frac{d\pi(1)}{d\pi(i-1)}\right\}}{1-\frac{\pi(i)}{2}}$

$2\leqslant i\leqslant n$ (12)

令 $i=2$ 可得 $\frac{d\pi(2)}{d\pi(1)}>0$

据(12)可推出 $\frac{d\pi(i)}{d\pi(1)}>0$，$1\leqslant i\leqslant n$

因此 $\frac{d\Lambda}{d\varphi}=\frac{d\Lambda}{d\pi(n)}=\frac{d\Lambda}{d\pi(1)}\times\frac{d\pi(1)}{d\pi(n)}>0$ (13)

图 5(b)示出了每结点对应于 n=5，10，15，20 的吞吐率---链负荷曲线，在可达到的最大吞吐率方面与随机竞争策略相比有明显的提高，而且使系统工作在稳定区域。

结语　通过上面的分析可知，在混洗交换网络中，如果使用随机旁路算法解决竞争冲突，当网络规模较大($n\geqslant 5$)时，系统存在不稳定性，性能得不到保障；而使用最短距离优先旁路算法时，较好地解决了系统的稳定性问题，提高了系统的整体性能。但最短距离优先策略较随机旁路策略复杂，在选取获胜者时需比较两个分组已走过的步数，增加了实现的难度。因此，在实际的系统中，应具体情况具体分析，根据需要适当选择冲突解决算法。

参 考 文 献

1　童调，程代杰．多处理机及智能多机系统．重庆大学出版社，1988

2　杨宗凯．ATM 理论及应用．西安电子科技大学出版社，1996

3　Krishna A, et al. Performance of shuffle-like swirching networks with deflection. In: Proc. IEEE INFOCOM'90. 1990. 473～480

4　Bertsekas D, et al. Data Networks, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 1992