

浅析光以太网的网络安全

龚羨萍, 任海兰

(武汉邮电科学研究院, 湖北 武汉 430074)

摘要:文章简单介绍了光以太网网络安全的基本技术,根据光以太网的特性分析了其物理安全隐患及可采取的防御措施,并对光以太网中数据的信息安全进行了分析,探讨了采用身份认证和信息加密方法加强信息安全性的具体实现策略。

关键词:光以太网;网络安全;物理安全;信息安全

中图分类号:TN915 **文献标识码:**A **文章编号:**1005- 8788(2006)02- 0035- 04

Security considerations of optical Ethernet

GONG Xian-ping, REN Hai-lan

(Wuhan Research Institute of Post and Telecommunications, Wuhan 430074, China)

Abstract: The basic technologies for the security of optical Ethernet are briefly described and some potential security-related problems in its physical security and the possible preventive measures, and the information security of its data are analyzed in line with its characteristics. Several practical methods for the enhancement of its information security based on the identity authentication and information encryption are proposed.

Key words: optical Ethernet; network security; physical security; information security

随着 IP 数据业务飞速增长和光网络技术尤其是波分复用(WDM)技术的不断成熟完善,如何利用 WDM 带来的超大光纤带宽进行数据业务的传送成为全球的研究热点。而以太网是最常见的 IP 组网方式,所以光以太网将会是 IP 网络和光网络互联的主流技术。由于光以太网技术集中了以太网技术成熟、价格低廉、组网灵活、管理简单和光网络可靠性高、容量大等优点,因而代表了以太网未来的发展方向。

1 光以太网的安全性问题

网络的安全问题是任何一个网络管理者必须重视和研究的问题。网络安全就是通过采用各种技术和管理措施,使网络系统正常运行,从而确保网络数据的可靠性、完整性和保密性。光网络是一种主要以光纤为传输介质的网络,其是否安全,是否有顽强的生存能力,是光网络技术发展的关键。光纤通信线曾被认为是不可以搭线窃听的。光纤没有电磁辐射,因此也不能用电磁感应窃密。但是,光信号在光纤中传输的最长距离受到信噪比、色散等因素的限制,为了实现长距离、高质量的通信能力,在整个网络体系中还包含大量的元器件,而这些元器件则成为光纤通信系统安全上的薄弱环节。经过多年的试验和研究,攻击者已经能通过各种手段和方式窃听和干扰光纤中传输的信息。而以太网是一种媒质共

享的网络,送往任意一个用户的数据包将被同时广播给所有的用户,这些数据包中都包含了目的用户的地址信息,在用户端,用户各自根据地址信息提取出自己的数据。其他用户很容易得到别人的数据。

对于光以太网的安全性能,首先要考虑的就是物理安全。物理安全就是要在物理层面上保证网络中传输的数据具有一定的保密性和服务质量,并且当这种保密性和服务质量无法得到保证时,能采取措施通知用户。同时,在物理安全基础上还要对网络中的传输数据进行进一步的处理,这种安全措施称为信息安全。有了这种安全保障其他用户即使通过各种手段得到了网络中的数据流,也无法知道其真正的含义,这种安全性主要依靠加密技术来实现。以上两种技术体系要相辅相成,加密技术不能保证网络在物理上不受攻击,不能保证信息不被截取,而物理上的绝对安全也是不可能实现的,因此,只有两者相互结合才可能真正实现一个安全的网络体系。本文将从这两个方面讨论光以太网络的安全性问题。

2 光以太网的物理安全分析

在光网络中通常采用的复用方式是 WDM。而现有的光器件性能还不很完善,使得 WDM 信道之间有一定的串扰。串扰可以被利用作搭线通信,也可以把恶意的信号输入到网络中进行恶意干扰造成

收稿日期:2005-07-12
作者简介:龚羨萍(1976-),女,江苏江都人,硕士,主要研究方向为 IP 技术。

服务破坏。在光纤和设备中的非线性变化导致的交叉调制,也会产生服务破坏或搭线攻击。而在系统受攻击时光放大器会受到影响,停止放大,带来服务瓦解。所以很多光器件,如光放大器、波分复用器、光上下复用器等,都可能成为物理安全隐患。

下面简单介绍一下在光网络中常见的物理攻击破坏方式和相应的解决措施。

2.1 常见的物理攻击类型

典型的物理安全性攻击包括服务破坏攻击和在传输线路上的窃听。光纤、波长选择开关、光放大器等元器件很容易受到该类攻击。

光纤是以不同波长传播光的媒体。当光纤受到弯曲或损坏时,光就可能辐射进或辐射出光纤,因而攻击者使用相关技术就会使服务受到干扰或窃取信息。

波长选择开关将不同波段的信号送至不同的输出线路。它由两部分组成:分波器和多路开关选择器。波长选择开关的主要问题是串扰,串扰会把产生的信号泄漏到无意义的输出上,再通过该部件上的其他光信号造成干扰。攻击者可以利用这种串扰进行干扰。

光通信网中大量使用了各种放大器,尤其是掺铒光纤放大器(EDFA)。而在 WDM 的通信链和节点中,由于各个信道的波长不同,有增益偏差,经过多级放大后,增益偏差累积,如果增益均衡不好,低电平信道信噪比恶化,高电平信道也因光纤非线性效应而使信号特性恶化。这种现象与光纤极低的损耗相互配合,使得 EDFA 对远距离的能量干扰很敏感。而且,如果输入 EDFA 的若干个波长光信号强度相差较大,输入的强信号就会抑制光放大器的增益,使整个增益谱下降,强信号愈强,弱信号愈弱,产生增益冲突现象,导致信噪比过低,破坏 WDM 系统的正常传输。攻击者可以插入一个功率较大、在放大器通带之内的同通信波段的不同波长的信号,剥夺合法通信信号的增益,提高攻击信号的功率进行通信破坏。

2.2 如何加强物理安全

解决物理安全问题可从预防和探测两方面入手。预防可以采用降低硬件内在固有缺陷性的技术,对光器件的性能进行改进和完善,也可以研究适合于全光网络的协议和体系结构设计,采用针对某些服务破坏具有有效保护能力的传输系统等方法。

首先可以从改进光纤物理媒介入手。目前有许多国家都在各类光通信会议上展出、或宣称已设计

出性能更好安全性更高的光纤。例如,日本 NTT 展示了其新研发的超低损耗和长距离光子晶体光纤(PCF),这种 PCF 具有相当低的损耗(0.37 dB/1 550 nm),传输距离长达 10 km。StockYale 宣布了新的弯曲不敏感和保偏光纤。两种弯曲不敏感光纤采用稍高的数值孔径设计,采用 125 或 80 μm 外径,在 1 550 nm 下可以有较小的弯曲损耗。新的保偏光纤针对不同波长应用设计,可以应用到各种光纤传感器中。光纤损耗是光纤的重要特性之一,它在很大程度上决定了在无需信号放大和再生条件下,光发送机和光接收机之间所允许的最大距离。偏振是光信号的一个基本特性,光信号的能量在给定的波长处分解为两个正交的偏振模,光纤固有的双折射现象会使偏振方向发生旋转,产生偏振模色散。损耗和色散都是造成光纤中信号劣化的重要原因,对光纤的传输性能有很大的影响。因而损耗小,传输性能更好的光纤的使用会减少网络中放大器、再生器等元器件的数量,即减少了可能的被攻击点,提高了安全性。

在滤波器改进方面,Auxora 公司已研制出新型可调滤波器。这款可调滤波器是基于 Auxora 独有的技术制造的,该技术可使两信道调制时无阻碍,且不产生串扰。

解决物理安全问题所采用的探测技术,包括对事件的确认、对安全故障的识别和产生相应的报警信号。在发现攻击后迅速隔离也是十分必要的,根据攻击的危害程度,为防止进一步受攻击,需要对攻击源隔离、对元器件进行重新配置、重新选定通信路由。但是,在全光网络中,对攻击的探测远比传统的电光网络要复杂。许多窃取干扰方法都具有接近于零的插入损耗和后向反射,极难发现。

尽管人们逐渐研制出具有更高性能的元器件,但是对于网络的物理保护终究无法尽善尽美,攻击者总是不断想方设法研究先进的仪器和设备来尝试攻击网络的物理漏洞,可以说任何一个网络在物理架构上都不可能有绝对的安全。所以还需要配合信息安全技术,使攻击者即便窃取到网络中的数据,也无法得到正确的信息。

3 光以太网的信息安全分析

基于以太网的光网络在接入网部分是通过光纤光缆连接至用户的。光纤接入网又可分为无源光网络(PON)和有源光网络(AON)。下面的讨论以 PON 的体系结构为基础,但这些信息安全技术同样

可用于 AON。

在 PON 中使用 WDM 技术,可同时处理双向信号传输,上、下行信号分别用不同的波长,但在同一根光纤中传送。下行方向,从光线路终端(OLT)传送到光网络单元(ONU)的各数据包是以广播的方式发送的,分光器同时将数据包传送给所有的 ONU。每个数据包中都含有各自的目的地址信息,当数据到达每个 ONU 时,各 ONU 只将发给它的信息包传送给最终用户而丢弃发给其它 ONU 的信息包。上行线路采用时分复用(TDMA)技术,将多个 ONU 的上行信息组织成一个 TDMA 信息流传送到 OLT。在 TDMA 技术中将合路中不同时间隙分配给每个 ONU。这种机制下,每一个连上 OLT 的用户很容易就可以得到其他用户的信息流。保障光以太网中的信息安全主要依靠两种方式:身份认证和信息加密。

3.1 以太网中的身份认证

以太网支持一种简单的密码认证机制。在 OLT 端,建立一个由各 ONU 相关信息构成的用以确认身份的数据库。在该机制下,OLT 将对所有与其相连的 ONU 进行身份确认及身份标识码(ID)注册。注册后,OLT 为已注册的 ONU 分配 ID,各个 ONU 监测到达帧的 ID,如果该帧所含的 ID 与自己的 ID 相同,则接收该帧,反之则丢弃。

3.2 以太网中的信息加密

3.2.1 信息加密算法

现有的以太网一般使用简单易行的扰码加密算法,即以太网通信系统在发送端 OLT 用扰码器来改变原始数字信号的统计特性,而在接受端 ONU 用解扰器恢复出原始数字信号。扰码加密过程是以 4 bit 为单位进行的简单的码置换过程。使用 8 bit 密钥,密钥至少每秒钟更新一次,由 ONU 提供给 OLT。然而,由于在光网络中数据传输速率很高,即使是在短时间内,攻击者也可能截获大量的密文信息,并从中获取密钥,进而破解密文。而且,扰码加密对系统的误码性能会有影响。在传输过程中,如果发送端产生一个误码,在接收端解扰器的输出将会产生多个误码。传输速率越高时对传输质量的影响越大。因此,若只是用扰码加密这样的保密措施,过于简单,并不可靠。现在更多的是采用数据加密标准(DES)和高级加密标准(AES)。

DES 是美国国家标准局 1977 年制定的正式数据加密标准。DES 算法原理如下:加密时,用密钥对数据进行加密,生成新的加密数据(64 位)作为

DES 的输出结果;解密时,则用密钥去把加密过的数据进行解密,还原为原始数据的明文(64 位)作为 DES 的输出结果。

AES 算法是一种性能更好的分组加密方法,信息的内容是以 128 位长度的分组为加密单元的。加密密钥长度有 128、192 或 256 位多种选择。密钥和待加密信息按位做与运算,然后所有要加密的分组都用一个函数 F 进行迭代计算。

因为 DES 算法加密级别也较低,目前已经趋于淘汰。而 AES 128 加密算法,具有比 DES 更好的安全性和更快的速率,是目前更常用的加密算法。

3.2.2 信息加密技术

在计算机网络中,常用的加密技术有节点加密、链路加密和端到端加密 3 种。

节点加密在信息被传入实际通信连接点之前进行,它在 OSI 7 层模型的第 1 层、第 2 层之间进行,是对相邻两节点之间传输的数据进行加密,不过为了便于传输路由的选择,它仅对报文加密,而不对报头加密。节点加密的目的是对源节点到目的节点之间的传输链路提供加密保护。

链路加密在数据链路层进行,是对相邻节点之间的链路上所传输的数据进行加密,不仅对数据加密还对报头加密。链路加密的目的是保护网络节点之间的链路信息安全。在采用链路加密的网络中,每条通信链路路上的加密是独立实现的,使用不同的加密密钥,这样当某条链路受到破坏时不会导致其他链路上传送的信息被破译。但是由于报文是以明文形式在各节点内加密的,所以节点本身必须是安全的。一般认为网络的源节点和目的节点在物理上都是安全的,但所有的中间节点则未必都是安全的,因此链路加密的最大缺点是在中间节点暴露了信息的内容。在网络互连的情况下,仅采用链路加密是不能实现通信安全的。

端到端加密,端到端加密的目的是对源端用户到目的端用户的数据提供加密保护。在始发节点上实施加密,在中间节点以密文形式传输,最后到达目的节点时才进行解密。在端到端加密的情况下,控制信息部分(如源节点地址、目的节点地址、路由信息等)不能被加密,否则中间节点就不能正确选择路由。

为了获得更好的安全性,可将链路加密与端到端加密结合在一起使用(如图 1 所示)。链路加密用来对数据报的目的地址进行加密,而端到端加密则提供了对端到端的数据的保护。

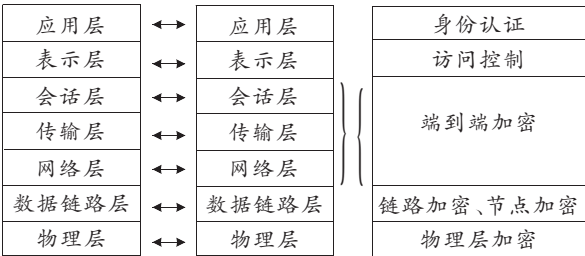


图 1 常用的各种加密技术和安全机制与网络各层次的对应关系

还可以采用在物理层进行加密的方式,封装整个比特流,包括帧头信息和循环冗余校验(CRC)。在接收端,物理层解密数据,并把它传到上层做确认。但是使用这种方式需要解决面向连接的问题,以保证能给不同 ONU 以不同的密钥,使其只对需要的帧进行正确解密。常用的各种加密技术和安全机制与网络各层次的对应关系如图 1 所示。

4 结束语

光以太网的发展趋势是逐渐向全光网络演进,

目前全光网络的发展还处在初级阶段,而全光以太网的实现和推广应用,不仅与光器件和光交换技术的发展和完善相关,也与光以太网的网络安全技术的发展密切相关。本文对光以太网网络安全的基本技术进行了探讨,从物理安全和信息安全的角度提出了加强光以太网安全性的策略,相信这些安全策略会随着光以太网技术的发展而逐步走向成熟并推向应用。

参考文献:

[1] 梁亚声,汪永益,刘京菊,等. 计算机网络安全技术教程 [M]. 北京:机械工业出版社,2004。
[2] Kramer G. IPACT: A dynamic protocol for an Ethernet PON(EPON) [J]. Lightwave, 2002, 16(10):74-79.
[3] Kramer G, Mukherjee B, Pesavento G. Ethernet PON: Design and analysis of an optical access network [J]. Phot. Net. Commun., 2001, 3(3): 307-309.
[4] Gerd Keiser. Optical fiber communications (Third Edition) [M]. 北京:电子工业出版社,2002。

(上接第 19 页)

另一种直接映射方式虽然头部简单,传输效率高,但适用性不是太好,和其它网络如 VoATM、VoFR 等的互通也比较复杂。两种传输方式的互通性也是急待解决的问题。比如将 VoIP over MPLS 的端口和 VoMPLS 的 CID 如何映射,如何实现语音的跨网。这些问题在 2005 年 2 月的世界 MPLS 大会上仍在探讨,估计不久将能够得到很好的解决。

VoMPLS 正逐步由理想变为现实,虽然它将有广泛的应用,但目前运营商希望实现的仍是各网络的互通,以保护现有网络的投资,并能实现网络 and 业务的平滑升级等。要实现这些要求还有一些问题需要解决,但 VoMPLS 对网络的管理功能是其它分组网络无法相比的,用可管理的网络提供可靠的服务是对运营商最有吸引力的。

目前中国几大电信运营商都已建设了各自的 MPLS 网络,未来几年 MPLS 会逐渐由核心向接入转变。到时运营商将不会满足于 MPLS 只能负载数据业务的状况,基于语音、视频等实时多媒体业务

将会得到迅猛发展。MPLS 将会作为通用载体而具有更大的用武之地。

参考文献:

[1] Kankkunen A. draft-kankkunen-vompls-fw-00. txt [DB/OL]. ftp://ftp.ietf.org/internet-drafts/draft-kankkunen-vompls-fw-00. txt, 2000- 03.
[2] MPLS-Forum 1. 0-July 2001, Voice over MPLS-bearer transport implementation greement [S].
[3] ITU-T Recommendation Y. 1261-2002, Service requirements and architecture for voice services over multi-protocol label switching [S].
[4] George Swallow. draft-swallow-mpls-simple-hdr-compress-00. txt [DB/OL]. http://www.ietf.org/internet-drafts/draft-swallow-mpls-simple-hdr-compress-00. txt, 2000-03.
[5] RFC 3550-2003, RTP: A Transport Protocol for Real-Time Applications [S].