OPC XML 数据通信安全模型的研究

乔加新

(安徽财经大学 信息工程学院,安徽 蚌埠 233041)

摘 要:在深入分析 IPSec 和 MPLS 的体系结构、工作原理和它们各自优点的基础上,提出了一种基于 IPSec 和 MPLS VPN 的 OPC XML 数据通信安全模型。利用 IPSec 实现数据传输的安全性,应用 MPLS 来保证数据传输的服务质量,从而实现了 OPC XML 数据在企业内部网(Intranet)和企业外部网(Extranet)上实时、高效、安全传输。

关键词:IPSec;MPLS;OPC XML;安全模型

中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2007)07-0148-04

Research on Security Model Used for OPC XML Data Communication

QIAO Jia-xin

(School of Information Engineering, Anhui University of Finance & Economics, Bengbu 233041, China)

Abstract: Through analysis on IPSec and MPLS system architecture, working principle and advantage of themselves, presents a security model used for data transfer based on IPSec and MPLS VPN. Making use of IPSec to realize the safety of data transfer, and making use of MPLS to ensure data transfer quantity of service, accordingly can realize OPC XML data transfer real time, efficiency and safety in Intranet and Extranet.

Key words: IPSec; MPLS; OPC XML; security model

0 引 言

OPC (OLE for Process Control,用于过程控制的OLE)是一个工业标准,OPC 基金会(OPC Foundation, OPC-F)自 1996 年 10 月 7 日在美国的芝加哥正式成立以来,先后发布了不同类型、不同版本的 OPC 规范,用于基于微软平台的 PC 客户应用程序实时数据的交换与共享,通过 COM 的 RPC 接口实现企业底层控制系统的集成。随着 Internet 技术的不断发展,企业规模的不断壮大,出现了将企业总部企业网与分支机构的企业网连接起来的企业内部网(Intranet)和将企业与企业合作伙伴连接起来的企业外部网(Extranet),为了适应基于 Internet 的新的应用,OPC 基金会于 2003 年 7 月 12 日发布了一种新标准——OPC XML-DA Specification Version 1.0[1]。从本质上讲,OPC XML 实际上描述了一个 XML Web 服务。在开放的 Internet 上传输 OPC XML 数据,主要存在以下两个重要问题:

(1) OPC XML 数据的安全性。Internet 是在 TCP/IP 协议体系的基础上建立起来的,TCP/IP 一个开放的体系。建立在相互信任的基础上,协议简单高效,但脆弱的论证机制、容易被窃听和监视、易受欺骗。因此在公用网络上传输企业 OPC XML 数据,同传输其他企业私有秘密数据一样,要采取安全技术,实现 OPC XML 数据安全传输。

(2)OPC XML 数据的实时性。传统的 Internet 中没有传输服务质量的概念,不能保证足够的传输带宽和传输延迟时间要求,网络只是尽最大努力来满足传输要求,而用于工业控制数据的 OPC XML 对时间的实时性要求较高,需要采取服务质量技术,实现 OPC XML 数据实时交换。为了解决上述问题,引入 IPSec 和 MPLS 协议,利用 IPSec 实现 OPC XML 数据传输的安全性,利用 MPLS 来保证 OPC XML 数据传输的服务质量,从而实现了 OPC XML 数据在企业内部网(Intranet)和企业外部网(Extranet)上实时、高效、安全传输。如何结合 IPSec 和 MPLS,建立 OPC XML 的数据传输的安全机制是文中的研究重点。

收稿日期:2006-09-12

基金项目:安徽省教育厅自然科学项目(2006KJ049B);安徽财经大学校青年科研项目(ACKYQ0620);信息工程学院青年科研项目(xgky2006008)

作者简介:乔加新(1975-),男,安徽蚌埠人,讲师,硕士,研究方向为计算机控制、网络安全。

1　IPSec 协议

Internet 工程任务组(IETF)于 1998 年 11 月颁布了 IP 层安全标准 IPSec(IP Security)。IPSec 是一个开放性的标准框架,能为网络层提供一个长期的、稳定的基础。IPSec 是网络层协议,为保障 IP 通信安全而提供的一系列协议簇[2]。它针对数据在通过公共网络时的数据完整性、安全性和合法性等问题,设计了一整套隧道、加密和认证方案。

1.1　IPSec 体系结构

IPSec 的基本体系结构包括安全协议认证头(AH)和封装安全载荷(ESP)安全关联(SA)、密钥交换(IKE)及加密和认证算法等。身份认证报头(Authentication Header,AH)是 IP 的一个万用型安全服务协议,用于为 IP 提供数据完整性、数据源身份验证和一些可选的、有限的抗重播服务;负载安全封装(Encapsulating Security Payload,ESP)是一个通用的、易于扩展的安全机制。为 IP 提供机密性、数据源验证、抗重播以及数据完整性等安全服务;安全关联和密钥管理协议 ISAKMP/Oakley,在使用 AH 和 ESP 时,协议将与一组安全信息和服务发生关联,称为安全关联(Security Association,SA)。IPSec 使用一种密匙分配和交换协议,即用 ISAKMP 来创建和维护 SA。Internet 密钥交换 IKE 的主要功能是建立和维护 SA。ISAKMP/Oakley 是 IKE 的核心,它确保密钥交换和 IPSec 通信的双方已经通过认证,协商协议、算法和密钥。

1.2　IPSec 工作原理

IPSec 使用传输模式和隧道模式保护通信数据,传输模式用于两台主机之间,保护传输层协议头,实现端到端的安全;隧道模式用于主机与路由器或两台路由器之间,保护整个 IP 数据包,该模式的通信终点由受保护的内部 IP 头指定,而 IPSec 终点则由外部 IP 头指定。IPSec 支持嵌套隧道,即对已隧道化的数据包再进行隧道化处理[2,3]。IPSec 隧道模式如图 1 所示。假设主机 A 与主机 C 通信,主机 A 的数据首先发给路由器 R1。R1 是一个 IPSec 路由器。去往主机 B 所在网络的数据必须被加密,R1 在其 SPD 中查找 SA,如果发现没有有效的 SA,则触发 IKE 进程,对没有 SA 的安全策略建立新的 SA,存入通信双方路由器的 SAD 中,R1 发送这个安全的数据包,R2 接收数据包后,剥去额外的 IP 头,并利用数据包的 AH 或 IP 头,摘录出 SPI(安全策略索引),从被封装的 IP 头中获取源和目的地址及协议,从 SAD 中取出所需的 SA,根据 AH 和 ESP 定义的规则,验证与该包对应的安全策略,进而决定 IPSec 处理方法是否正确,如果验证正确,R2 将数据包传送给主机 C。注意,IPSec 的 SA 是单方向的。

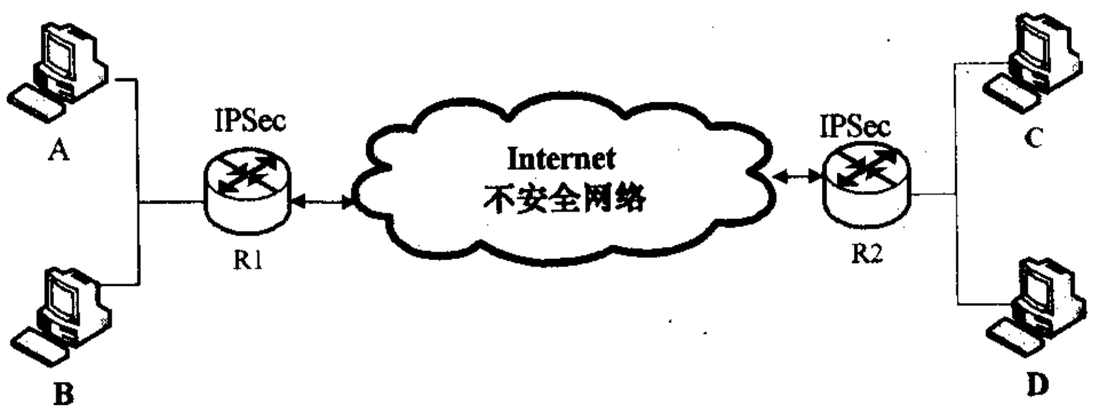

图 1　IPSec 遂道模式

1.3　IPSec 的优点

(1)强大的安全性。IPSec 协议固有的强大的安全特性能使用户进行认证,保证数据的机密性和完整性。用户可以用字证书或者预共享密钥进行认证,与安全策略不一致的包被弃。

(2)支持远程办公和移动办公。IPSec 数据转发设备能够为数万地址上分散的用户提供服务。

(3)易于配置。不需要服务提供商的介入,尽管许多企业为了降低花费、加快服务入门和减轻风险,选择利用服务提供商对区域性或者全局性多个站点配置的管理服务经验。

2　MPLS 协议

多协议标记交换(MPLS, MultiProtocol Label Switching)是一种新出现的技术,旨在解决与当前联网环境中使用的分组转发技术相关的许多问题。IETF 团体的成员针对标记交换领域提出一套适合市场需求的标准[2]。MPLS 体系结构描述了实现标记交换的机制,这种技术兼有基于第二层交换的分组转发技术和第三层路由技术的优点。

2.1　MPLS 体系结构

MPLS 体系结构被分为两个独立的组件:控制组件(也叫控制层面) 和转发组件(也叫数据层面)。控制组件包括路由协议、路由表、LDP 和 LIB。路由协议单元可以使用任何一种路由协议生成路由表,如 OSPF,BGP 等;LIB(标签信息库)是记录标签信息的表格,LDP(标签分发协议)是建立标签交换路径的协议。控制组件负责路由的选择、MPLS 控制协议 LDP 的执行、标签的分配和分发以及标签信息库的构成。转发组件主要包括 LFIB。LFIB(标签转发信息库)是用于标签交换的信息库。转发组件只负责根据标签信息库建立标签转发表和对标签分组进行简单的转发操作。

2.2　MPLS 的工作原理

MPLS 的工作原理如图 2 所示,主要存在三种路由设备:R(Router)为一般路由器,LER(Label Edge Router)标记边缘路由器是用于 MPLS 网络的边缘和 LSR(Label Switching Router)核心标记交换路由器能够迅速处理分组上的标记,并对已打上的标记快速转

发,LER 和 LSR 都必须是符合 MPLS 标准的标签交换路由器[4]。假设 R1 向 R3 发送数据时,IP 数据包到达一个 LER1 时,LER1 会将此 IP 包封装 MPLS 标签,即 LER1 首先要分析 IP 包的信息,并按照它的目的地址和业务等级加以区分,在 LER1 处,数据包分配了一个转发等效类(FEC)后,LER1 就可以根据标签信息库(LIB)为其生成一个标签,然后将数据包用 LSP 的标签封装,从标签信息库所规定的下一个接口发送出去。在网络的核心,当一个带有标签的包到达 LSR1 时,LSR1 提取入局标签,同时以它作为索引在标签信息库中查找,当 LSR1 找到相关信息后,取出出局标签,并由出局标签替代入局标签,从标签信息库中所描述的下一跳接口送出数据包。数据包到达 MPLS 域的另外一端 LER2,在这一点,LER2 剥去封装的标签,仍然按照 IP 包的路由方式将数据包继续传送到目的地 R3。

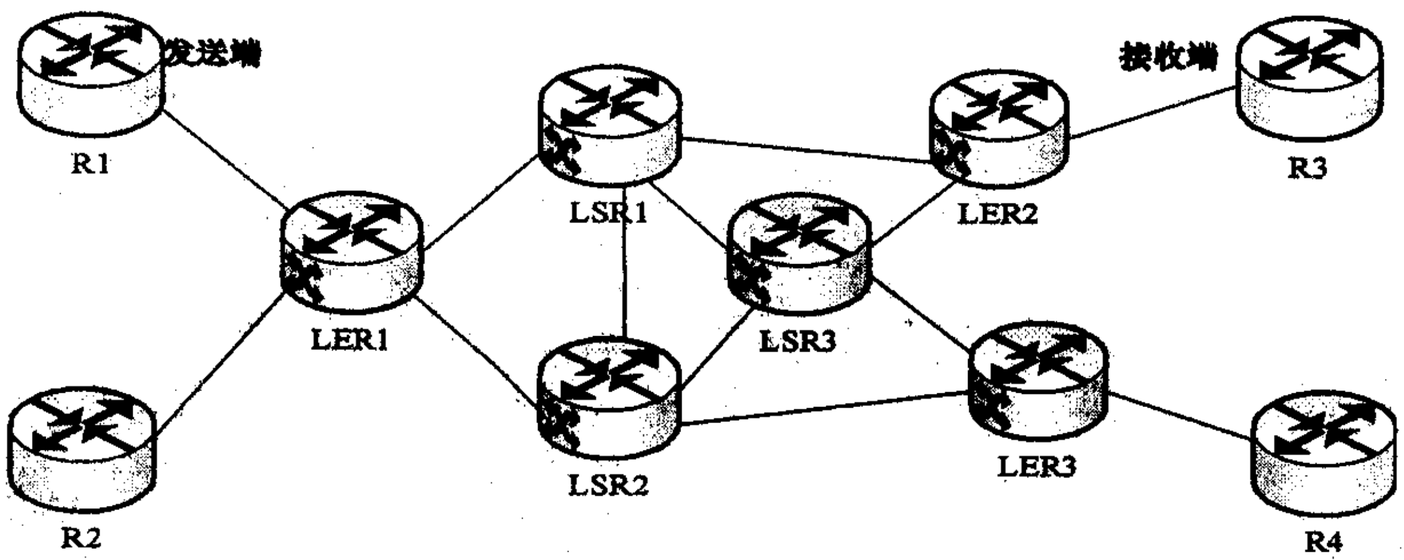

图 2 MPLS 的工作原理

2.3 MPLS 的优点

(1)流量工程。能够提供以往 IP 网中无法保证的流量工程业务,可最佳利用链路和节点,平衡负荷。

(2)MPLS 的服务质量。MPLS 网络的数据传输和路由计算分开,能够以无连接方式或显式路由方式提供面向连接的业务,这使得 MPLS 适用于动态隧道技术,并保证数据传输业务的服务质量需求。

(3)可扩展性和灵活性。MPLS 支持大规模层次化的网络拓扑结构,进一步促进了网络功能的划分,将复杂的事务处理由网络边缘去处理,网络中心只完成传送功能,故 MPLS 具有良好的网络扩展性。

(4)简化控制过程。MPLS 转发可以在能够进行标签查找和替换的交换机和路由器中进行,交换机不需要具有进行 IP 头分析的能力。

3 基于 IPsec 和 MPLS VPN 的 OPC XML 安全模型

因为 Internet 的安全性和实时性无法保证,OPC XML 规范自 2003 年发布以来,其应用进展缓慢,基于 IPSec 的 VPN(虚拟专用网络)和基于 MPLS 的 VPN 的出现为问题的解决提供了可能。从上述研究可以看出 IPSec 本质是一个 IP 层加密协议。它保证特定的通信用户之间数据的私有性、完整性和真实性,并可对相应的数据源进行验证。MPLS 技术在无连接的 IP 网络中引入了面向连接机制,从而既保持了 IP 协议的的灵活性、可靠性和扩展性,又可以充分应用第二层的快速交换能力、服务质量性能、流量控制性能。因此,为了构建既安全又快速的 OPC XML 的安全模型,应集两者之长、优势互补。

3.1 安全模型

结合 IPSec 和 MPLS,构建 OPC XML 的安全模型,如图 3 所示。其中,企业总部和企业客户作为 OPC XML 的客户端,分公司 1 和分公司 2 为 OPC XML 服务器,由企业总部与分公司 1 和分公司 2 构成企业内

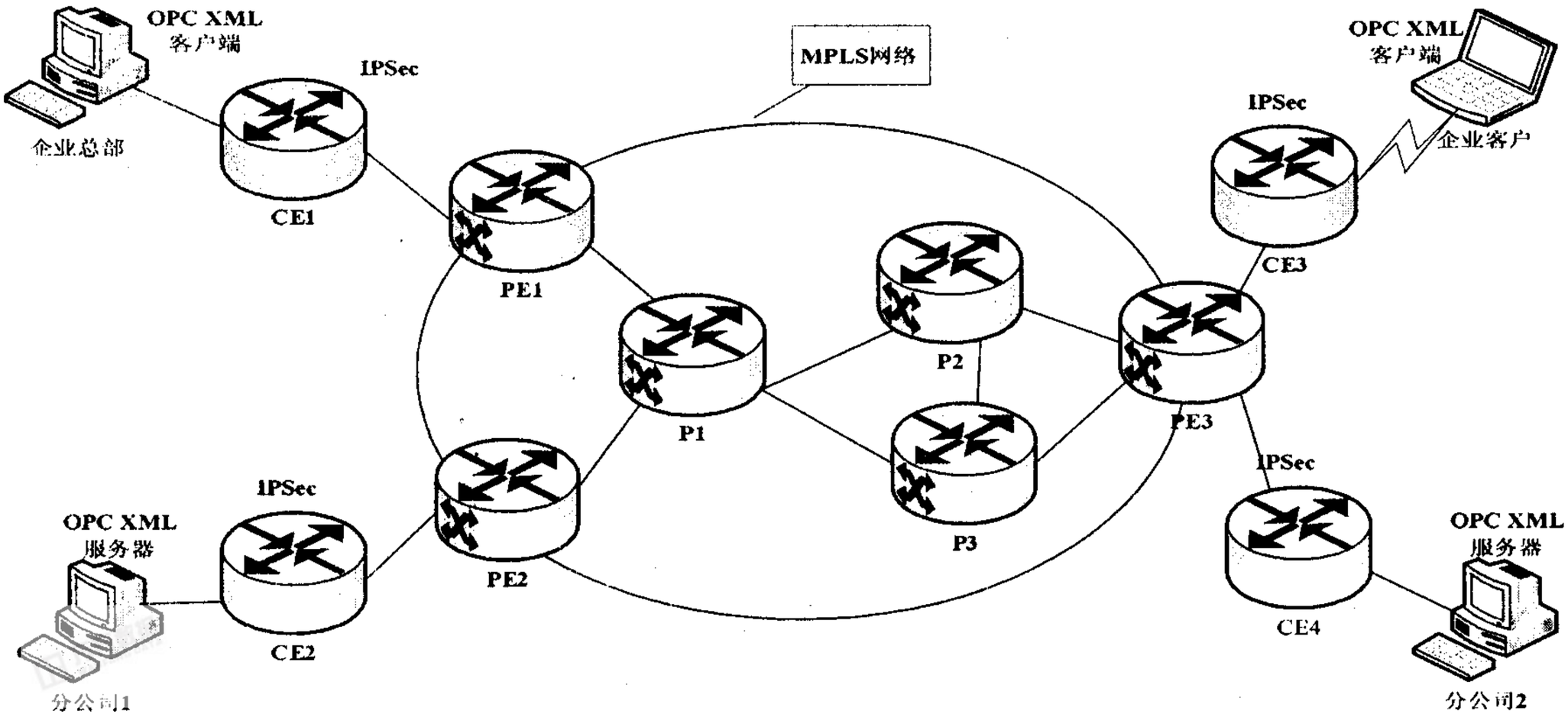

图 3 基于 IPSec 和 MPLS VPN 的 OPC XML 的安全模型

部网(Intranet),企业客户与企业总部及其分公司形成企业外部网(Extranet),OPC XML 客户端通过由 IPSec 和 MPLS 构成的网络与 OPC XML 服务器进行通信,MPLS 作为网络主干部分,根据预留资源,按照标记快速转发。IPSec 与各种用户直接相连,IPSec 模块实施在 CE 路由器上,实施的方式可以采用与操作系统集成,也可以使用堆栈中的块,实施 IPSec 模块的路由器称为安全路由器。

OPC XML 客户端通过 CE 路由器进行 IPSec 安全加密时,根据用户的安全要求不同,可以分为三个级别:

①不作安全要求,无需 IPSec 加密,通过 CE 路由器的 Internet 接口,连接 MPLS 网络,进行快速转发;

②一般安全要求,可以通过 IPSec 的传输模式,保护传输层协议头,实现点到点或端到端的一般安全功能;

③较高安全要求,利用 IPSec 的隧道模式,保护整个 IP 数据包,实现较高级别的安全功能。

下面分析数据在 OPC XML 的安全模型的转发过程。在企业内部网中,企业总部作为 OPC XML 的客户端,访问分公司的 OPC XML 服务器时,通过 OPC XML 客户端发送数据到 CE1 路由器上,根据安全级别,进行加密,保护数据传输的安全性,加密后的数据到达 MPLS 网络的边缘标记路由器 PE1,数据包分配一个转发等效类(FEC),打下标签,然后执照标记在 MPLS 网络中进行快速转发,到达 MPLS 网络另一端边缘后,去掉标签,发送连接目标主机相连的 CE 路由器,进行数据解密后,发送到具体的 OPC XML 服务器,OPC XML 服务器接收数据并处理。在企业外部网中,如企业客户(OPC XML 客户端)与分公司(OPC XML 服务器)访问流程与上述过程相似。

3.2　性能分析

(1)满足数据传输的安全性要求。在 CE 路由器设置 IPSec 模块,同时根据安全要求的不同,实行三级分类。因此支持按照用户需求的不同的安全级别保障。

(2)保证数据传输的实时性。在 MPLS 网络实施包括 InterServ,DiffServ 和流量工程等技术,可以提供比较高的服务质量保证[5]。

(3)具有很强的网络扩展能力。该方案业务实施支持多运营商提供端到端的业务。能支持多种用户连接接入,随着企业网点的增多可以通过 ISP 网络服务提供商实施网络的配置和管理。

(4)支持多种实施模式。可以实现企业内部(Intranet)的安全传输,如企业总部与分公司,也可以实现企业外部(Extranet)安全访问,如企业客户与分公司。支持企业内部网、企业外部网和移动用户等多种组网方式。

(5)支持多协议传输和多种用户信息流。MPLS 承载的信息流允许采用多种协议如 IPX、IP,在整个网络中用户信息流可以是 IPv4、IPv6、单播和组播。

4　结束语

IPSec 与 MPLS 结合,有利于把 IPSec 的高度安全、可靠的优势与 MPLS 的高速交换、服务质量保证、流量控制以及灵活性、可扩展性发挥出来,提供设计优良、运行正常和综合性的 OPC XML 数据通信安全模型。通过现有的公用网络,建立企业各级安全互连的企业内部网和企业外部网,不仅会节省网络的建设和运行维护费用,而且增强了网络的可靠性和安全性。同时也为 OPC XML 规范的安全部分提出了自己的设计方案。

参考文献:

[1] OPC Foundation. OPC XML - DA Specification Version 1.0 [EB/OL]. 2003 - 07 - 12. http://www.opcfoundation.org/.

[2] 胡越明. Internet 技术及其实现[M]. 北京:高等教育出版社,2003.

[3] Doraswamy N, Harkins D. IPSec Implementation[EB/OL]. 2004 - 08. http:// www. microsoft. com/technet/itsolutions/network/security.

[4] Rosen E, Viswanathan A, Callon R. Multi protocol Label Switching Architecture[S]. RFC3031. 2001.

[5] Le Faucheur F. Multi Protocol Label Switching(MPLS) Support of Differentiated Services[S]. RFC3270. 2002.

(上接第 147 页)

参考文献:

[1] 刘九芬,黄达人,黄继武. 图像水印抗几何攻击研究综述[J]. 电子与信息学报,2004,26(9):1496 - 1503.

[2] 飞思科技产品研发中心. 小波分析理论与 MATLAB7 实现[M]. 北京:电子工业出版社,2005:363 - 364.

[3] 吴永宏,潘　泉,张鸿才,等. 基于提升框架的整数小波变换[J]. 电子与信息学报,2004,26(4):659 - 663.

[4] Gonzalez R C, Woods R E, Eddins S L. 数字图像处理(英文版)[M]. 北京:电子工业出版社,2004:108 - 112.

[5] 台莉春,高　珍,张志浩. 基于小波变换的数字水印最佳嵌入位置的研究[J]. 微型电脑应用,2005,21(4):11 - 14.