基于 Internet 的远程操作技术研究

唐鸿儒 陈 虹 曹 卫 扬州大学工学院电气工程系(225009)

Abstract

The functions and implementation of remote operation that would be practiced based on Internet are described. The influence of uncertainty and transfer delay of various network transfers on automation system is analyzed. The requirement of network security with remote operation is discussed. Some securetechniques such as Access Control List, Digital Certificate, and SSL used to get safe remote operation are introduced in detail.

Keywords: Internet,network automation,remote operation,transfers delay,network security,SSL

摘 要

本文阐述了基于 Internet 技术的远程操作可完成的功能及其实现方法,分析了各种网络传输的不确定性和延时对自动化系统的影响,分析了远程操作对网络安全性的需求,并详细介绍了利用存取控制、数字证书、SSL 等措施来满足安全性的思路和方法。

关键词:Internet,网络自动化,远程操作,传输延时,网络安全,SSL

远程操纵生产过程技术一直是自动化技术的重要研究内容。实现远程监视、远程控制、远程设备故障诊断、远程调试、远程管理等,不但可以提高企业自动化水平、提高企业生产设备的维护管理水平、实现无人值守, 而且可以为企业合理配置人力资源奠定基础。

1 基于 Internet 网络的远程操作

1.1 企业信息网络性能对远程操作的影响

目前的企业信息网络一般通过现场控制网络(Infranet)、企业内网(Intranet)和 Internet 把分布于各局部现场、独立完成特定功能的计算机互联起来,它是适应企业生产与经营的功能分布和地域分布的特点,达到资源共享、协同工作、远程监控、远程管理等为目的的全分布式网络系统, 是 Internet 技术、Web 技术、数据库技术、TCP/IP 网络通讯技术、浏览器技术发展的产物。图 1 为基于 Internet/Intranet/Infranet 技术的企业信息网络体系示意图。通过 Explore 等通用浏览器进行工业现场生产过程数据的远程浏览已经得到了较多的应用,在企业内网(Intranet)中进行生产现场数据的实时浏览也已经得到一定的应用和发展,国内外许多厂商已经提供不少的商业化的生产监控软件平台,如 FIX、InTouch、组态王等,且都已经能够提供远程浏览功能, 许多人正在研究基于 Web 技术的自动化系统,但是由于基于 Internet/Intranet/Infranet 体系的网络自动化是新兴的研究领域,基于 Web 技术的自动化系统中控制功能的研究更是处于起步阶段,许多存在的问题有待探讨和研究,这是由于网络的固有性能决定的。

对远程操作有直接影响的网络性能包括:①通过网络的操作一般不处于被控现场, 有的可能是远程的,操作人员常常没有眼见为实的感觉。②企业信息网络用途的多样性,网络流量的变化可能很大,且网络传输可能要经过若干环节,因此网络传输存在不确定性,有可能丢失某些关键的信息。③受网络传输协议、网络流量、网络传输路径、以及传输距离的影响,每次数据从源点到目的地的传输延时有很大差别。无法满足有实时性要求的应用。④网络存在许多不安全因素等等。由于网络存在上述所说的性能,使得自动化领域的许多功能不能基于 Internet 实现,那些能够在远程实现的功能, 由于存在空间和时间的差异,也必须重新进行研究,制定出切实可行的实现方案和工作步骤,然后才能加以实现。有些关键问题必须首先解决好,才能实现真正的网络自动化。例如由于网络传输延时时间的不确定性,工业现场的实时闭环控制只能在现场控制器中实现;再如网络安全问题不解决好,远程控制、远程组态和远程维护等工作将是十分

危险的，而这种危险性带来的后果有时是灾难性的，有可能威胁现场工作人员的生命安全，可能比象金融网络这样重要的系统受到攻击时的危害大得多，使得网络自动化毫无意义。

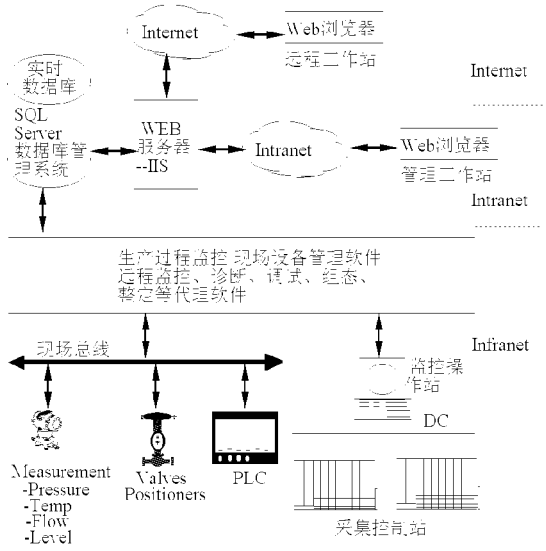

图 1 基于 Internet/Intranet/Infranet 的企业信息网络体系示意图

1.2 基于 Internet 远程操作功能

基于 Internet 网络远程操作生产过程涉及到诸多方面的技术和行为习惯，远程操作可以分为两个部分，一是针对生产过程的远程操作，二是针对生产过程现场测控设备的远程操作。针对生产过程的远程操作包括生产过程现场运行参数和状态的浏览和监督，远程操作生产过程设备，远程调度生产过程，生产过程故障的远程监视、远程诊断和远程处理，生产过程的远程调试等。针对生产过程现场测控设备的远程操作可能包括远程功能组态，远程工作状态监视、故障预测和故障诊断，远程设备调试和工作参数整定等，这是属于现场智能设备远程维护管理方面的内容。

(1) 远程监督

对于无实时性要求或者实时性要求不高、且无须与生产现场进行互动的功能，如生产过程现场运行参数和状态的远程浏览和监督、设备运行状态的远程监视等功能一般是单向的，相对来说比较简单，只要由现场的监控计算机和现场设备管理软件将生产现场的运行数据、设备状态数据等周期性地传送到实时数据库上，在远程用户发出浏览请求时，由 Web 服务器根据这些数据生成动态网页，供远程用户浏览。

(2) 远程故障诊断

对于生产过程的远程故障诊断和现场测控设备的远程故障诊断过程的启动可以分为两种情况：一种情况是由远程的工作人员为了随时掌握生产现场的状态信息而发出诊断命令，由现场的远程故障诊断代理软件自动收集故障信息，故障信息通常是大量动态且连续的反映故障特征的数据（如电力系统发生短路故障时的故障录波）；另一种情况是在故障发生时，由现场的远程故障诊断代理软件自动启动故障数据采集进程，再以一定的机制（如 Email）请求远程的专家、研究机构进行故障诊断。故障诊断过程也可以分成两种情况，一种是由生产现场的远程故障诊断代理软件直接启动本地故障诊断软件利用采集到的故障数据和已有的知识库进行故障推理，将故障可能的原因传送给远程的工作人员，再由远程工作人员进行进一步分析；另一种情况是需要远程专家知识和经验的故障诊断，由现场诊断代理软件将收集到的故障数据以一定的数据结构形式存入实时数据库，远程用户进行故障诊断时，由 Web 服务器以 ActiveX 控件的方式将与一次故障相关的数据提供给远程用户，或者 Web 服务器将这些数据形成可供下载的文件，供远程用户下载，然后在远程进行故障诊断，再将故障原因及其处理方法反馈给现场。

(3) 远程组态

远程组态主要针对现场的测控设备，远程操作人员根据工艺要求进行现场测控设备的功能和工作方式的定义。要实现远程组态，必须研究远程组态的工作范围、组态内容、组态信息的安全性和完整性等。在远程组态时，可先用设备的现行组态信息生成组态页面，远程用户在此基础上修改组态或者重新组态，组态完毕后，提交组态信息，由 Web 服务器对提交的组态信息进行处理并存入实时数据库，生产过程现场的组态代理软件扫描得到组态命令后，将新的组态信息下载到现场智能测控设备，下载完毕后，返回组态完毕信息并通知实施组态工作的远程操作人员。由于现场设备种类繁多，功能差别很大，因此各设备的组态内容千差万别，为了简化组态软件或者组态页面的生成方法，将来对现场设备的功能组态应该由现场测控设备生产厂家提供相应的 ActiveX 组态控件。

(4) 远程控制

通过 Internet 远程对生产现场进行控制的最大障碍是网络传输的不确定性和传输延时，基于目前的 Internet 网，无法进行生产过程的闭环控制。因此这里的远程控制一般仅仅用于远程启停某个设备（如电

力系统的变压器的投切控制)，远程控制进行一次预定的数据采集(如故障数据的采集),远程投入或者切出某一调节控制回路等等。由于从 Internet 远程控制命令发出到现场开始执行,以及执行结果返回的时间间隔无法确切地计算出来,因此,对控制过程异常情况的处理和保护,控制算法的实现只能由现场的远程控制代理软件完成,实施控制的主体在现场,所以,这种基于 Web 技术的远程控制的实现方法倒显得比较简单。

(5) 远程调试

生产过程或者测控设备的调试过程一般是一个人与被调试对象交互的工作过程,是根据被调试对象的反应决定下一步的工作,生产过程可能存在大惯性滞后，加上网络传输的不确定性和大的传输延时,因此基于网络的远程调试只能是远程发布调试命令,修改工作参数,由现场的远程调试代理软件完成调试操作,实时记录调试过程数据,待一次调试过程稳定后,将调试数据传送给远程工作人员或者专家,由它们分析调试结果、决定是否需要继续调试。

(6) 远程整定

远程整定是远程整定现场测控设备的工作点,只能对现场智能设备中可以直接改变工作参数的场合,如改变电力系统的微机保护装置的保护动作整定值;或者对那些能够自动生成标准信号输入的场合,如现场测控设备中的接受电量输入的输入通道零点整定和校正,对那些需外接标准信号源的场合(如压力变送器的精度校正需要提供标准压力)，则无法远程自动完成,但可以由远程操作人员给出整定命令,由现场操作人员利用现场的整定软件对现场设备进行整定,并记录整定过程数据,再将这些整定数据通过网页送给远方的工作人员进行分析和处理。

2 网络传输的不确定性和延时的分析

自动化系统许多功能的实现都有一定的实时性要求,如数据采集系统、闭环控制系统。不同对象对实时性要求不同,且差别可能很大。影响实时性的主要因素是信号的传输时间和信号的处理时间,早期的控制系统结构简单,传输控制协议简单,传输距离短,因此,传输延时影响较小,实时性主要取决于信号的处理时间。近年来,随着芯片技术的发展(如 DSP 的出现)、计算机速度和精度的提高,信号的处理速度越来越快,而与此同时控制系统体系结构发生了很大的变化,出现了控制网络,因而信号的传输延时对实时性的影响越来越大。

直接数字控制(DDC)的实时性主要取决于输入输出信号的处理时间+算法计算时间,实时性容易得到满足。基于工业控制计算机、PLC 或者单回路智能调节器等的自动控制系统都属于这一类系统。

在集散控制系统(DCS)中,由于采集控制功能是在现场控制站完成的,实时性也容易得到满足,但若某个控制回路需要用到其它采集控制站的参数时,这时就牵涉到网络交换数据,网络交换数据所需时间的长短与传输速率、传输数据量、网络流量以及所用的传输协议直接相关,在采用单主多从或者令牌环协议时,网络传输所需的时间可以定量地计算出来,一般情况下传输是确定的,因此能够满足实时性要求。

现在许多自动化设备厂家已经采用以太网络作为现场通信的主干网，由于 Ethernet 的数据链路层采用 CSMA/CD 协议，它可能因碰撞而导致某站点想发数据时发不出去,影响实时性,很长时间内,人们一直认为它不适合于工业现场,可能不满足实时性要求。但由于工业现场控制系统具有传输的数据报文相对较小、周期性强等特点,研究表明,如果控制网络流量小于网络负载能力的 25%，则可以得到很好的实时性。应用事实也表明,采用 Ethernet 作为现场控制网络的传输链路层,能够满足绝大多数应用的要求。

现场控制系统(FCS)更大程度上依赖于网络交换数据，因为 FCS 中每个 I/O 装置都是现场控制网络中的一个节点(如基于 FF 现场总线的现场总线控制系统),其数据采集、控制算法计算和控制输出可能由若干个现场总线智能设备协同完成,各个节点之间需要频繁交换数据,由于现有的现场总线技术每个网段上的设备数量有限，一般需要传输的数据量不大,且大都采用小报文结构帧和确定性好的链路调度协议,因此,只要适当配置设备和参数,传输延时不会影响系统的实时性。

在图 1 的基于 Internet/Intranet/Infranet 体系结构的企业信息网络示意图中,处于工业现场的控制网络可能是多种总线的集成、多种控制系统的集成,连接于不同总线上的不同设备、不同控制系统协同完成工业现场的控制功能，它们之间可能需要交换数据,因这些数据需要跨总线、跨系统传输,传输延时相对较大,但由于每段总线、每个系统的数据流量相对固定,且总线内或者系统内信息的传输延时时间是可确定的,因此控制网络内的传输延时具有可确定性。

但基于 Internet/Intranet/Infranet 体系的网络自动化系统由于受网络拓扑结构、网络传输协议、网

络流量、网络传输路径、以及传输距离等因素的影响，数据从源点到目的地的传输延时有很大差别。由于操作人员或者控制站点是 Intranet 或 Internet 上的一个站点，从此站点到控制现场可能需要经过若干个传输链路和网络节点，大多数情况下无法预测和控制一个命令或者现场采集的数据在网络上传输所需的实际时间，因此，基于 Internet/Intranet/Infranet 体系的网络自动化系统的功能受到很大的限制。

为了减少传输延时，从工程的角度上我们可以采取一些措施，如减少冗余信息、压缩被传输数据，有些数据只有在变化时传输或者在某个被监督的事件发生时传送相关数据等方法来减少网络传输量和传输时间。但是 Internet 内网络流量可能每个时段都有很大差别，常常有突发报文和大报文出现，因此我们仍然无法控制数据在网络上传输的确定时间。

然而，随着 Internet 网络传输通道的提速、网络交换设备的改进、先进传输协议的使用等措施的实行，也许有一天我们不再为传输延时和传输时间的不确定性问题发愁，远程操纵生产过程如同我们现在在车间控制室内一样方便和有效。事实上 Internet 网络的性能不停地得到改善，我们上网的速度越来越快，我们在校园网络上已经享受到了视频点播的服务，宽带网线也已经进入家庭。

3 远程操作的安全措施

3.1 安全需求

长期以来，由于自动化系统的封闭性，系统的安全性主要通过操作登录和密码来赋予不同操作人员的操作权限，随着主流的计算机网络技术在自动化系统中的应用，自动化系统能和企业生产信息管理网络直至广域范围的 Internet 网络直接连接，自动化系统向着开放系统的方向发展，因而其安全性要求越来越受到重视，如何保证自动化系统的安全是实现网络自动化首要解决的问题，因为如果自动化系统受到恶意攻击，造成生产过程的中断或者危险生产过程的事故（如爆炸），将会造成比金融、电子贸易等网络受到攻击时更严重的灾难。

网络安全性的实现应该以现场测控信息和远程操作信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人利用窃听、冒充、篡改、抵赖等手段侵犯操作人员的利益，同时也避免其它用户的非授权访问和破坏为最终目的。具体来说，网络自动化的安全性需求应包括以下几个方面：①身份认证及访问控制。在网上操纵生产过程中，现场服务器与操作人员进行互相认证，以保证双方身份的正确。现场代理服务器根据操作人员的身份，对其操作权限进行控制。②保密性和完整性：保证网上操作中涉及个人保密信息和生产过程或者测控设备信息在公开网络的传输过程中不被窃取，并保证所传输的信息不被中途篡改或通过重复发送进行虚假传送。③不可抵赖：进行网上操作的人员事后无法因为某种原因否认做过的操作。以便跟踪操作信息和审查。④用户漫游：充分发挥网络互连的优势，保证用户是可以漫游的。即用户在互联网上的任何地方都能够进行远程监视和操纵生产过程，或者对现场测控设备进行管理时，都能享受以上的安全保护。

3.2 安全措施

企业信息网络所需的安全措施可以包括设置防火墙、防治网络病毒、身份辨识、访问控制、信息加密等措施，在此仅讨论与远程操作直接相关的安全措施。

(1) 申请数字证书

首先必须为现场 Web 服务器申请一个数字证书，同样每个要进行远程操作的人员也必须申请一个数字证书。基于数字证书可以实现数字签名、身份鉴别。数字证书是由有一定知名度的、能够被信任的证书授权机构(CA——Certificate Authority)签发的一个电子文档，在该文档中，包含了证书所有者的公共密钥以及和它身份有关的一些信息。申请者在获得证书的同时，还获得它的私有密钥。有很多的证书授权机构，如 Verisign,Thawte 是两个有名的 CA，国内的中国数字认证网、天威诚信也是 PKI/CA。

(2) 定义安全控制表

在基于 Web 服务器的网络自动化系统中，生产过程现场的服务器端通过定义存取控制表 (ACL-Access Control List)等方式，为每个操作人员进行操作权限定义，或者为每个可存取项定义。

(3) 使用 SSL

在客户端(浏览器)和服务器端(web server)均设置要求使用公钥证书的安全套接字层协议 SSL (Security Socket Layer)。SSL 协议处于传输控制层(如 TCP)和应用层(如 HTTP)之间，它以 TCP 为基础，为应用层提供数据加密、信息完整性、客户和服务器认证等服务。SSL 的目标是通过相互利用证书认证、完整性签名和数据加密来提供安全的客户/服务通信。SSL 协议涉及对称加密、公用密匙加密、身份验证、数字签名和信息摘要等。

对称加密就是加密与解密使用相同的关键字进行加密，它的优点是速度很快，在 SSL 中，用于信息在传输过程中的加密，密钥是在客户和服务器端的连接阶段动态产生的。通用的对称加密算法有 DES、RC2、RC4。

公用密匙加密是采用基于公钥密码理论的公用/私有密匙对进行加密。公用密匙是大家都可以得到的，通过数字证书传递公用密匙，而私有密匙只有拥有者自己知道。用私有密匙进行加密的数据必须用公用密匙来解密，反之亦然。在 SSL 中，采用公用/私有密匙对加密方案可以进行身份验证。公用密匙加密的缺点是速度比较慢。RSA 是常用的公用密匙算法。数字签名实际上是真实签名的电子版，在数字世界中，通过数字签名在文档或者数据上签署自己的标记，既可表明数据发送者身份，又可防止数据发送者否认自己所做的操作。数字签名一般基于公共密钥之上。在 SSL 中，数字签名是用 hash 函数对待传输文档创建一个文档摘要，并用私有密匙加密后添加在文档末尾。采用信息摘要可以保证信息的完整性，采用数字签名可以惟一地标识文档的所有者，通过查看操作日志签名的历史记录，就可以使操作人员和服务器双方都无法抵赖发出过申请或接收到过申请。常用的 hash 算法有 MD2、MD4、MD5、SHA、DES-DM。

基于 SSL 的通信过程分为 2 个基本阶段：连接阶段与数据传输阶段。在连接阶段建立了安全连接，交换信息传输密匙，最后验证身份，然后开始数据传输。

图 2 给出了采用 SSL 的客户端和服务器端的简单通信示例，其中 1-4 为连接阶段，5 为传输阶段。①由客户端首先向服务器端发送“Hello”问候信息。②服务器端收到问候信息后，返回一则问候信息，同时在该信息后添加了自己的数字证书，证书中包含有服务器端的公共密钥。③服务器端随后利用自己的私有密钥对发送的能够表明自己特征的“信息 1”进行加密，通过“信息 1”来证明自己的身份。客户端利用服务器端提供的公共密钥对它发来的密码文本信息“信息 1”进行解码，以确认服务器端身份。④在确认了服务器端的正式身份后，客户端将利用服务器端提供的公共密钥对将要使用于对称加密方法的传输加密密钥进行加密编码，然后将加密编码发送给服务器，服务器端得到了用于传输加密的对称加密密钥。⑤客户端和服务器端都知道了所需的传输加密密钥，双方利用该传输加密密钥对传输的信息进行加密，开始安全的通信过程。在通信过程中，还要对传送的信息进行信息摘要，再用发送信息端的私有密钥进行加密，形成传输信息的数字签名后，附加在传输信息的尾部，这样，既保证了信息传输的完整性，又可以进行抗否认审查。

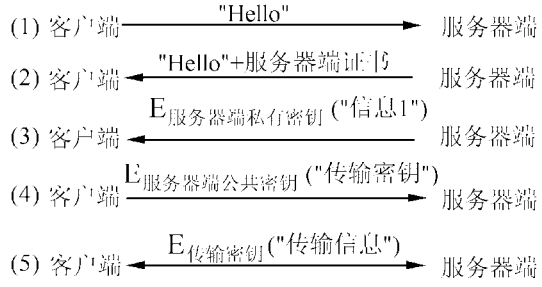

图 2 SSL 客户端和服务器端通信示意图

(4) 用户漫游

用户携带着自己的数字证书和私有密钥，可以在任意一台连接在 Internet 网上计算机上通过浏览器进行远程操作，达到漫游的目的。

4 结束语

远程操作可以提高自动化水平，合理配置企业的人力资源，同时对企业的生产运营模式的改变起着积极的推动作用。但是由于 Internet 网络存在传输延时、传输不确定性和存在安全隐患等固有性能，使得远程操作可实现的功能、实现的方法及其步骤等有待不断地研究和实践。尤其是采用数字签名、加密传输等安全技术，将使得传输效率大幅度降低，如何克服这些不利的影响是研究远程操作技术的重要内容。

参考文献

1 卞正岗.世纪之交论自动化系统工程产业.测控技术，2000.1
2 龚俭，等.计算机网络安全导论.东南大学出版社，2000.8
3 Eric Larson,Brian Stephens,Web 安全、维护及其服务器的管理.机械工业出版社，2000.7
4 李小海，等.基于 WWW 的机器人远程控制的关键技术及典型实现.工业控制计算机，2000.2
5 袁洪芳，等.基于 Internet 的 FMS 远程监测与故障诊断技术研究.制造业自动化，2000.5
6 唐鸿儒，等.企业控制网络技术.工业控制计算机，2001.1
7 来五星，等.远程监测诊断系统中延时问题处理.计算机应用，2000.9
8 陈晋大，等.用数字签名保证网络通信安全，计算机应用研究，2000.9

[收稿日期：2001.8.7]