

Internet/ Intranet 技术应用于 SCADA / EMS 系统中的探讨

梁运华¹, 曾文², 金维香³

(1. 湖南省湘潭电业局, 湖南 湘潭 411104; 2 湘潭技术职业学院, 湖南 湘潭 411102;

3 长沙理工大学电气与信息工程学院, 湖南 长沙 410077)

摘要: 在分析了目前国内 SCADA / EMS 系统的结构以及网络数据安全状况的基础上, 结合现代计算机网络技术 (P2P 计算模型、三层结构技术等), 提出在 SCADA / EMS 系统中采用 Internet/ Intranet 技术的构想, 并给出了新型 SCADA 系统的具体结构、通信模型, 以及应采用的一些相关技术。在对两种 SCADA 系统成本效益分析后, 得出新型系统具有良好的性价比。此外, 为了提高原有设备的利用率, 也提出在传统 SCADA 中增添网关设备, 将其改造成基于 Internet 技术的 SCADA 系统的方法。

关键词: 广域集群技术; P2P; Internet; 三层结构; SCADA / EMS

中图分类号: TM76 **文献标识码:** A **文章编号:** 1003-4897(2005)19-0056-05

0 引言

当 SCADA / EMS 运作在封闭环境前几乎没有人对 SCADA 系统的数据感兴趣。然而, 在电力系统逐步进入市场化后, SCADA 系统中的数据对于许多竞争的电力企业非常重要, 在保证 SCADA 系统原有的安全性、实时性和可靠性前提下, 如何让外界可以方便地访问到 SCADA 系统的数据呢? 随着 Internet 网络有效带宽迅速增加、网络安全及相关技术快速发展, 使得 Internet/ Intranet 技术成为解决该问题的最好途径。对于基于 Internet/ Intranet 技术的 SCADA / EMS 系统, 主要解决的问题仍是电网上、下传数据的实时性、可靠性和完整性。本文所设计的基于 Internet/ Intranet 技术的 SCADA / EMS 系统, 主要包括采用分布式数据库来管理主要的内存数据、P2P 技术、IP 单 / 组播作为通信协议、广域服务器集群系统、网络传输的 QoS 机制以及网络安全技术。该种 SCADA / EMS 系统具有良好的灵活性和扩展性, 它可以集成一些其他的 SCADA 系统, 并减少这些系统的最初创建、后期运行费用。

1 SCADA / EMS 现状

SCADA / EMS 已广泛应用电力系统之中, 目前具体状况主要表现: 有的 EMS 厂家利用前置机进行数据采集和预处理, 其缺点是各个厂家的智能串行通信接口卡、切换板等设备不能通用, 给日后的扩充带来了一定的制约因素; 有的厂家取消前置机, 将 RTU 得来的数据接入终端服务器的不同接口, 终端服务器接入系统的局域网, 将各 RTU 来的数据通过网络设备传输到系统的主服务器或 SCA-

DA 接点机, 而前置处理模块则放在服务器或网上的特定接点机上; 电力企业要求 SCADA / EMS 系统与电力市场技术支持系统、MIS 系统的联系愈来愈紧密; SCADA 主站一旦确定下来之后, 由于传统远动系统的庞大且复杂, 不能随便变动; 电力市场运作之后, 电力系统的商业运作越来越重视, 企业之间需要更频繁的数据交换, 对 SCADA 系统的实时性、扩展性和灵活性要求愈来愈高; IEC60870 - 5 - 104 规约的推广以及 IT 技术的迅速发展, 为 IED 直接接入 WAN, 创造了良好的环境。

2 基于 Internet 技术的 SCADA / EMS 模型

2.1 结构、通信模型^[1-3]

基于 Internet 技术的 SCADA / EMS 结构模型包括负责传送电网实时数据的 IED、SCADA 主站系统中的服务器 (负责 SCADA 应用程序的执行) 和客户机 (主要应用在主站中心和 WAN 中)。浏览器安装在每个客户机和监控机上, 所有对电网的操作都是通过浏览器来显示的。这种模型具有以下特点: 每个 IED 实时数据上传到主站中服务器都是通过 WAN 来实现的, 数据通信方式主要是采用 IP 单 / 组播方式来完成, 每个服务器都能接收到每个 IED 的数据, 正常时每个区域的服务器只与该区域内 IED 直接进行通信, 当该区域服务器失效后, 可由其他区域的某个服务器接管刚失效服务器的任务; 关键业务应用程序服务器 (如 SCADA 应用服务器、数据库服务器以及 WWW 服务器), 能够互为备份, 彼此之间的数据同步是靠 IP 组播通信方式来实现, 这样每台数据库服务器中都包含了所有整个区域所有厂站的 IED 及相关设备的数据; 每条逻辑数据通信

链路都采用通过 VPN 技术来进行加密和用防火墙进行过滤。其结构通信模型如图 1 所示。

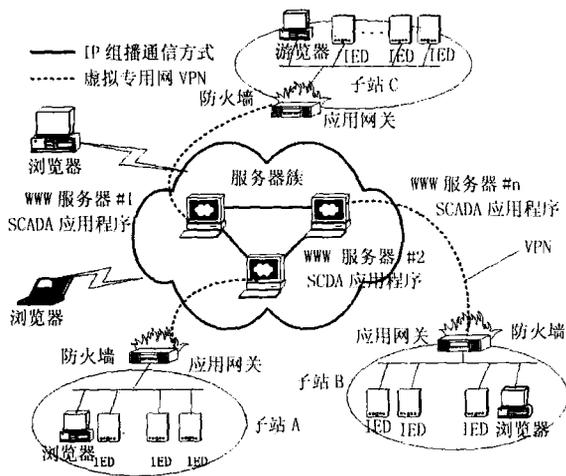


图 1 SCADA 结构通信模型

Fig 1 Architecture of communication model of SCADA

IED 与服务器之间的通信都是通过 WAN 来实现。每个 IED 向服务器发送系统数据是采用 IP 单播传输方式, WAN 上的所有指定服务器都能接收到每个 IED 的上行数据,并能将控制命令下行到每个 IED;而服务器下达给具体 IED 命令时,只有特定的 IED 可以接收到数据,并执行相应命令。在广域群集族中的不同服务器数据同步时,则采用 IP 组播的通信方式,这样可以实现多台(大于 2 台)服务器之间的数据同步。

2.2 点对点 (P2P) 计算模型

点对点 (P2P) 计算模型也正成为当前企业计算应用的主流, P2P 应用程序充分利用了桌面电脑的闲置资源,通过网络把某一任务分布在网络上的其他节点,使得整个网络上的计算机形成一个虚拟的超级计算机,大大扩展了已存在的单独计算机的处理能力。P2P 技术可以被定义成任意支持 PC 间可以直接进行数据交换,且不需依赖某一公共文件服务器的应用程序或网络解决方案。一旦 P2P 计算软件安装在网络上的桌面工作站上,每一台 PC 就变成一个既可以充当客户端,又可以充当服务器的“点”,这样可以减轻当前存在系统的负担,减少费用、系统升级,提高系统的计算效率水平。WebMark 2001 Technology Run 利用 P2P 计算模型,显著性能测试如图 2 所示^[4,5]。

在网络正常情况下, SCADA /EMS 系统中可以运用该技术,来充分利用各主站内的闲置工作站的资源,分担服务器的计算任务,使 EMS 系统中需要

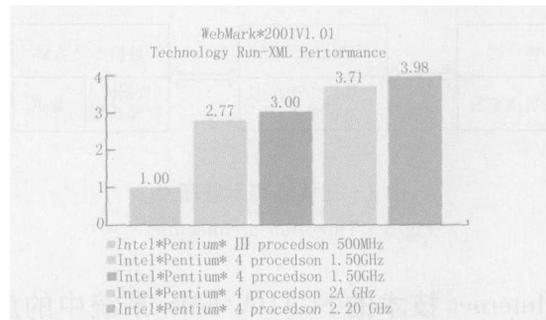


图 2 Intel P4 处理器在 P2P 协作应用程序高性能中示意图

Fig 2 Intel pentium 4 processor provide seceptional performance for XML, which lies at the heart of most P2P applications

大量计算工作的 PAS 或需要实时性很高的操作,获得更好的实时性,如在潮流计算、状态估计等应用。另外,对提高电力系统稳定性分析与控制实时仿真决策系统、电力市场支持系统等实时性都很有实际意义。

2.3 三层结构体系^[6]

随着 Internet 技术的渗透,企业应用正由客户 / 服务器体系的两层结构发展为由客户、应用服务器 (应用层)、数据库服务器 (数据库层) 组成的三层结构。Intranet 主要特点是 B/S 结构,针对大量的数据处理和逻辑分析任务,采用基于 WEB 将客户、逻辑及数据分开的三层结构,客户机采用浏览器进行交互。本系统中的监视 / 控应用模块安装在第二层, SCADA 的数据 (电网的实时数据和历史数据) 安装在第三层。应用层和数据层都安装在服务器上;浏览器安装在第一层,能显示系统的数据,且可以控制电力系统的 IED。为了控制一个设备,用浏览器连接到相应的服务器,然后用执行相应的控制命令,所有这些操作都在浏览器上通过网页方式显示。这种方式可以使得电网操作人员通过 WAN 使用在任何服务器上的应用程序。

使用三层结构在技术层面上的优势: 反应速度快,数据在发送到 LAN 之前首先由功能性服务器过滤,网络通信量会因此而下降,复杂数据访问,分散地来自中间层而不是客户层,也降低了对内存和存储设备容量的需求,提高了系统整体反应速度;由于业务逻辑操作集中在应用层,因此降低网络和各客户端的负荷;安全性强,在中间层功能性服务器中提供加密核心技术,以及在中间层集中应用一些高级网络安全组件,来进一步增加系统的安全性能。该结构如图 3 所示。

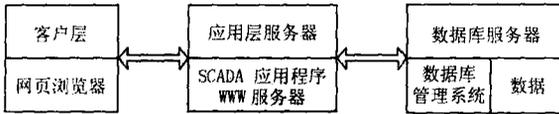


图 3 三层结构示意图

Fig 3 Three-tier architecture

3 Internet技术的 SCADA/EMS 系统中的应用

3.1 SCADA/EMS 系统数据特点

整个网络中主要的数据流有三个特点：动态变化，即系统实时信息、子站上行数据和网络内部的计算机之间的数据交换流，跟动态变化的系统的运行状态和规模、子站的运行状况以及 SCADA/EMS (Supervisory Control and Data Acquisition /Energy Management System) 运行方式有密切的联系；实时性要求不一，其中实时性要求非常严格的有如实时控制、网络分析等；具有突发性，如系统同时发生了多种故障，网络中的数据流在某一时刻会突然变得很大。

3.2 P2P 技术在 SCADA/EMS 系统的应用

基于上述特点和 SCADA/EMS 系统各节点内部互联所用的网络也拥有一定的剩余带宽，SCADA/EMS 系统与 MIS 系统以及 Internet 都已物理隔离，本文利用 P2P 技术来实现 SCADA/EMS 系统的分布式计算，并具体采用 XML 语言来实现。对于 EMS 的 PAS 中对数据计算时间长或实时性高的部分，如网络分析、潮流计算，可以实行分布式计算（数据分布在 PAS 应用服务器以及多台后台机上），专用应用服务器将一个大计算任务分解为许多个小计算任务，并通过网络分发到后台工作站上进行计算，最后将结果统一汇总到一台 PAS 应用服务器上，其工作原理图如图 4 所示。

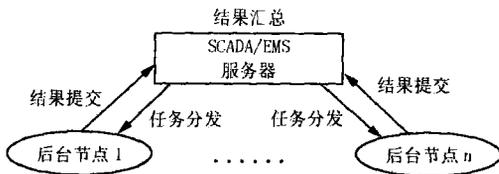


图 4 应用 P2P 技术 SCADA/EMS

Fig 4 Application of SCADA/EMS with P2P technology

P2P 大致的实现方式是：系统特定成员（SCADA/EMS 服务器）要运行一个计算任务，就将在

系统中公告出来，其他相关后台节点在认为自身 CPU 足够空闲的情况下，与特定成员联系，下载计算代码在自身上运行，计算结果返回给该特定成员。在这一过程中，执行任务的成员可根据自身负载变化而主动中止或迁移计算任务。

SCADA/EMS 应用服务器在具体实现过程中，可分为三种工作模式：所用工作组内成员能够在服务器规定时间内，及时将所受理的计算小任务处理完毕，并成功上传到应用服务器；部分工作组内成员不能在服务器规定时间内，将所受理的计算小任务处理完毕或成功上传到服务器；部分工作成员在未将计算结果上传到服务器过程中，就退出应用系统（如人为退出、计算机故障等）。

3.3 嵌入式 Ethernet 技术在 IED 中的应用

Ethernet 是采用冲突检测载波侦听多点访问（CSMA/CD - - - Carrier Sense Multiple Access With Collision Detection）机制解决通信介质层竞争问题的，这造成了以太网通信响应的不确定性，也是长期以来它应用到工业现场设备中的主要障碍。随着嵌入式以太网技术的快速发展，目前通信速率一般达到 10 Mb/s, 100 Mb/s 的快速以太网也已开始广泛应用，使以太网通信实时性得到了增强。使用交换式集线器代替共享式集线器，将网络冲突域细化，各端口发送来的数据报文不会在所有端口上广播发送，减小了冲突的可能性，使以太网通信确定性加强。文献 [7] 对比研究了普通以太网和令牌总线网的性能。

SCADA/EMS 系统内各智能设备（IED）间广泛采用 TCP/IP 协议的嵌入式以太网技术，有助于提高数据传输的效率，从而解决串口通信、现场总线时信息堵塞或时效性差（如发生大量事件），信息容量限制（如故障录波信息的上传）问题，从而提高整个系统自动化的通信性能。引进嵌入式 Ethernet 技术的 IED 设备，对实现上述系统的结构、通信子模型和三层结构体系提供可靠的技术支持。

3.4 网络安全解决策略

由于本系统是采用 Internet 作为网络数据传输平台，因此网络安全是整个系统稳定、可靠的重要保证。解决该安全问题的基本思路是：除了采用支持 P2P 技术的防火墙之外，还采用集中式的安全控制机制。通过建立一个基于比较完善的加密机制而形成的 Workgroup（工作组），对进入该 Workgroup 的计算机加以严格的身份检验、授权以及保存该计算机在网络后的所用动作记录，即实现认证（Authenticat-

tion)、授权 (Authorization)和稽核 (Auditing)的所谓“AAA”安全功能来加强网络安全,以达到保护 Workgroup自身安全的目的。

此外,系统采用扩展性强的 IPSec技术的 VPN安全部件(在选择该安全部件时,需考察其 QoS性能指标),对所经公用链路进行加密,而不采用租用专线方式,降低运行成本。在每个子站和主站接入 Internet口,增添防火墙来过滤非法数据包(过滤规则可以根据 IP地址,端口等)。子站系统有多个节点时,可以应用网关应用代理的方式,来进一步限制子站内的节点访问 Internet,增强系统的网络安全性,同时也降低了子站的运行成本。系统网络安全设计如图 5所示。

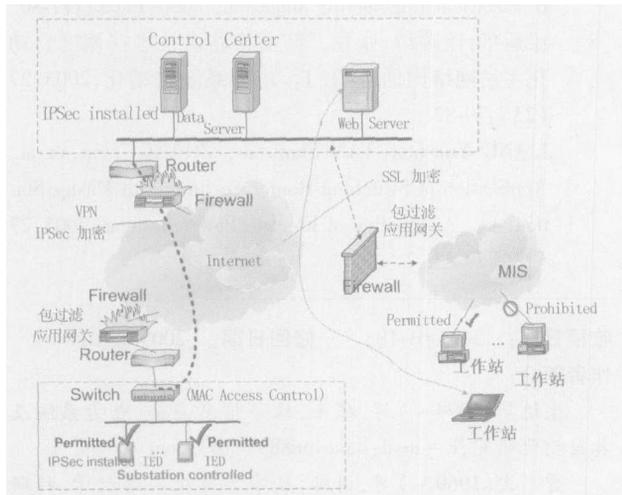


图 5 网络安全结构示意图

Fig 5 Architecture of network security

在浏览器和 WWW 服务器通信时,我们采用了 SSL对数据进行加密。对系统内的操作员都分配访问权,但具体操作时需结合 IC卡技术(将已创建好的用户名及其密码保存在 IC卡中),来进一步对每个操作者进行身份认证。

当然,如果要实现比较坚实的 Internet安全体系,还需要许多安全技术的配合,不是简单一两种技术就可以完成的。又由于当前大多电力企业将 SCADA /EMS系统与其它(如 MIS,计量计费)之间采用了物理隔离,所以采用了该策略系统的网络安全状况应该和传统模式的 SCADA /EMS系统一样。

4 其他主要相关问题

4.1 网络的实时性

由于 SCADA /EMS系统的数据具有动态变化、

实时性要求不同以及具有突发性等特点,所以对网络数据有必要应用 QoS技术来满足一些数据流高实时性的要求。QoS技术为网络注入了必要的智能因素,确保对延迟敏感的流量和关键任务型的流量即使在拥挤的网络中也能被优先传递。在调度自动化主站内的 LAN中,也可以利用交换机的四层交换技术,结合 LAN中数据流的特点,利用 QoS技术来进一步提高系统的实时性^[8]。

4.2 网络管理

网络管理的目的是保证整个网络达到尽可能高的运行效率,对复杂的网络环境进行控制,保证网络传输的可靠性、网络数据的安全性,网络整体性能的稳定性,另外还需实现对网络性能监控和有关参数的设置。

5 对传统模式的 SCADA 系统的改造和合并设计

对于一些旧 SCADA系统改造为基于 Internet技术的 SCADA系统,原有的 IED设备仍可利用,只需另增加一个网关设备,用它直接用 WAN进行连接,子站中的 IED采集到的电网实时数据,需通过网关设备才能与 WAN进行通信,即网关向主站服务器转发上传电网实时数据,同时它也可接受主站下行的命令后,再将命令转发给相应的 IED,由 IED执行具体命令。

6 效益分析

表 1 SCADA 包含的项目

Tab 1 Items included in SCADA

项目	传统的 SCADA	基于 Internet的 SCADA
服务器的数量	每个子站中心和区域主站中心都需一套	子站不需要;区域主站中心需一套;或几个区域主站中心合用一套
客户机的数量	两者相同	两者相同
客户端业务软件	每个客户端需安装	任何客户端不需安装
WAN	不需要	要
IED	两者相同	两者相同
专用机房	每个子站和主站中心都需	需一个
通信协议	DN3.0/Polling/CDT等	IEC60870-5-101/104
网络数据安全要求	一般	严格
网络通信 bit/s	1 200~9 600	10M

从表 1可以看出,采用基于 Internet的 SCADA系统,其最初的安装和日后的运行费用,相对传统而言要少,更具有良好的性价比。其次,整个 WAN具有相对传统系统几十倍的速率,因此使得新的系统拥有更好的实时性。另外,新系统的客户端不需要

安装客户端业务软件,因而使得新的系统的安装和日后维护量,都得到简化。由于整个 WAN 只利用一套服务器,因此主站中心所需的计算机服务器硬件配置要求比传统的主站中心要高些。

7 结论

随着计算机网络技术和厂站自动化水平的提高,电力系统中的传统 SCADA 模式也有必要改变。本文所设计基于 Internet 技术的 SCADA 系统,利用现在流行的分布式结构、三层结构,降低了整个系统网络数据的流量;客户端只需浏览器不需安装业务应用软件,降低了系统的日后维护工作量。P2P 计算模型使得 SCADA/EMS 能够充分利用各客户端的剩余资源,形成一个虚拟超级计算机,使得原来费时的计算任务,得到了有效的缓解,提高了整个系统的设备利用率。基于 Internet 技术的 SCADA 系统拥有比传统远动系统多几十倍的网络带宽,使得 SCADA 系统的数据通信实时性,得到显著提高。基于 Internet/Intranet 技术的 SCADA/EMS 系统良好的扩展性、灵活性以及性价比,使得它将成为 SCADA/EMS 系统的主要结构模式。

参考文献:

- [1] Ebata Y, Hayashi H, Hasugawa Y, et al Development of Intranet-based SCADA [J]. IEEE, 2000: 1656-1661.
- [2] Serizawa Y, Ohba E, Ohba T, et al Conceptual Design for Distributed Real-time Computer Network Architecture [J]. IEEE, 2002: 26-31.
- [3] Srinivas M, Sreekumar N, Krishna V P. SCADA-EMS on the Internet [J]. IEEE, 1998: 656-660.

- [4] <http://www.intel.com/business/newstech/peertopeer.pdf> [EB/OL].
- [5] <http://www.intel.com/procs/perf/limits.htm> [EB/OL].
- [6] 朱文凯,丁汉,杨学平. 三层分布式数据库在联网售票系统中的应用 [J]. 计算机工程与应用, 2002, (15): 195-197.
ZHU Wen-kai, DING Han, YANG Xue-ping. The Application of Three-tier Architecture Distributed Database in Online Booking System [J]. Computer Engineering and Application, 2002, (15): 195-197.
- [7] 黄文君,冯卫标,葛毅,等. 实时控制系统网络设计 [J]. 机电工程, 2000, 17(3): 77-80.
HUANG Wen-jun, FENG Wei-biao, GE Yi, et al Design of Real-time Control System Network [J]. Mechanical & Electrical Engineering Magazine, 2000, 17(3): 77-80.
- [8] 梁运华,谈顺涛,张颖,等. 交换路由技术在调度自动化主站网络内的应用 [J]. 电力系统自动化, 2003, 27(23): 79-82.
LIANG Yun-hua, TAN Shun-tao, ZHANG Ying, et al Application of Switching Router Technique to Master Station [J]. Automation of Electric Power Systems, 2003, 27(23): 79-82.

收稿日期: 2005-01-18; 修回日期: 2005-05-07

作者简介:

梁运华 (1974 -)男,硕士,从事信息安全、电力系统及其自动化研究; E-mail: liangyun889@163.com

曾文 (1969 -)男,讲师,从事计算机网络教学、科研工作;

金维香 (1965 -)女,高级试验师,主要从事电子信息技术、计算仿真技术等方面的教学研究。

Applying Internet/Intranet technology to SCADA/EMS system

LIANG Yun-hua¹, ZENG Wen², JIN Wei-xiang³

(1. Xiangtan Electric Power Supply Bureau, Xiangtan 411104, China;

2. Xiangtan Technical Vocational College, Xiangtan 411102, China;

3. School of Electrical & Information Engineering, Changsha University of Science & Technology, Changsha 410077, China)

Abstract: On the basis of analyzing the structure of domestic SCADA/EMS system and the safety state of network data at present, the paper puts forward the proposition of adopting the Internet/Intranet technique in SCADA/EMS system by considering the modern computer network technology (current 3-tier technology, P2P calculating model). SCADA/EMS system's concept based on the Internet/Intranet technique and a new structure of SCADA and communication model and some correlated technique which should be adopted are detailed. The new model has a better cost performance after the two kinds of SCADA system are analysed. In addition, to further improve the utilization ratio of the old equipment, a method to refit it into a SCADA system based on Internet technique by adding up gateway equipment on the traditional SCADA system is put forward.

Key words: clustered technique of WAN; P2P; Internet; 3-tier architecture; SCADA/EMS