水质远程监控通讯安全性问题的探讨

——利用现有网络条件确保远程监控通讯安全性的解决方案

王　涛[1]，　张雯宇[2]，　张洪波[1]，　王建军[3]

(1.机械科学研究院,北京　100044；　2.北京大学计算机系,北京　100081；

3.邯郸钢铁集团有限责任公司连铸连轧厂,056015)

摘　要:针对我国总体水质情况不容乐观的现实,提出解决办法之一是对排污口实施大规模远程监控,而远程通讯的安全性又是最直接、最核心的问题。文章着重阐述了如何解决在现有网络条件下实时运行的网络运行速度和数据的加解密等具体问题。

关键词: 远程监控；　污水传感器；　数据安全；　D-H 加解密算法

中图分类号:X84　　**文献标识码**:A　　**文章编号**:1003-6504(2002)03-0027-03

尽管目前我国已经采取措施,对境内主要流域及周边污染源进行了大规模的治理行动,但总体水质情况不容乐观。主要原因之一在于部分企业偷排工业废水,一些地方还存在地方保护主义。解决这一问题的关键是加强监控力度,尤其是上级环保部门对下属环保部门的监督管理,实施排污口远程监控。实施排污口水质远程监控从技术角度讲需解决传感器的可靠性和远程通讯的安全性问题:传感器的可靠性主要依托采购质量信誉较好的产品(如 E + H、ORION 等),而远程通讯的安全性是需解决的最直接也是最核心的问题。如果建立专用讯道,远程通讯系统的安全性可以保证,但投资巨大,不切合实际。那么能否利用现有网络条件解决这一问题呢?

经过研究比较认为:可以利用现有 ISDN Internet 系统进行水质远程监控通讯。目前 ISDN 的流量为 Max(64k/s)的通讯速率,在我们的实验条件下能够达到 Min(15k/s)的对等通讯速率,能够满足我们实时通讯的需求,而且投资低廉。

1　污水监控流程

(1)与远程端(污水口 PLC)进行对接,侦听远程端发送过来的数据并进行相应的安全检查即判断其相连的客户端是否为非法入侵者。

(2)校验远程端发送过来的数据并反馈数据有效性的信息给远程端。

(3)数据库操作,主要进行判断对方传递数据并判断是否是重复数据及相应读写数据库。

(4)按照相应的规则进行专家系统(用于分析污水数据的走向趋势,并保存历史记录用于以后污水处理的研究基础)的建立。由于是与多台 PLC 同时运行并通讯,在服务器端软件设计时要考虑其程序的并发能力。即对于远程端的操作请求要求能够同时响应而不丢失其请求。这种并发(ASCYN)包括对于网络 SOCKET 同时请求的并发与数据库(Expert System Database)操作的并发。

2　服务器端的网络(SOCKET)操作

首先介绍网络通信的协议与标准:在具体运用中,考虑到实际需求的速度与网络流量通信的协议采用 TCP/IP,由于其具有良好的兼容性、可移植性与可扩充性受到了人们欢迎,在系统中着重关注以下三点:

(1)在运用 TCP/IP 时能够满足速度的需求;

(2)在数据传输时要考虑其安全性;

(3)客户端的请求在服务器端的侦听过程中不能有遗漏现象发生。

在此数据传输的方式下采用自定义的一种数据格式,如下图:

数据头	加密帐号	地区号	请求号	实验类型号	数据区	冗于纠错	数据尾

图 1　数据包定义格式

数据头:其中标志了此数据的各数据区的起始地址与相应的各数据区索引模块起始地址。

加密帐号:为每台远程端(PLC)提供自身的帐号与密码,当与服务器对接时检查其身份。

地区号:代表本次请求的被监控的地区。

请求号:标志了本次请求的目的(重发数据/新数据)。

实验类型号:标志了此次请求所发出待实验类型。

数据区:为远程端传送到服务器据解密前的数据。

冗于纠错:采用冗于纠错的正确数据范围标志区。

数据尾:标志了此数据包(PACKAGE)的结尾。

作者简介:王涛(1974-),男,工程师,主要从事水处理工艺与控制技术方面的研究开发工程设计,发表论文 11 篇。

在运行时当远程端提出数据传输请求,首先由远程端的服务程序负责按照图1所示意的数据格式包加密并打成数据包,由SOCKET的程序发送到服务器端由在那里解包并得到水质量参数的各种数据,存储到磁盘阵列中,然后把所要检测的数据进行提取,与所允许最高限度(Max Density)进行比较,这里需要注意的是利用最小二乘法进行直线拟合并分析预测将要超标的污水口,限于篇幅略。数据的传输过程中所关注的是服务器端能够很快的并且接受来自远程端的每一个请求,为此在服务器端的SOCKET程序中采取提高并发的方法:由于可能有不同用户请求,所以在UNIX服务器端开启多个侦听进程,以使不会漏掉每一个客户端SOCKET的请求。过程如下:(a)打开一通信通道并告知本地主机,它愿意在某一公认地址端口上接受客户请求;(b)激活一新进程来处理这个客户请求。新进程处理此客户请求,并不需要对其他请求做出应答。服务完成后,关闭此新进程与客户的通信链路,并终止;(c)返回,等待另外的客户请求,此时值得注意的是要注意收回字进程的运行空间,在消息响应函数中通(waitpid)实现,以避免影响内核的运行效率。在进程间采取信(MESSAGE)与共享存储区(SHARED MEMORY)两种方式通讯,以确保两个进程的协调通讯处理事务。程序采用io端口复用,利用事件驱动方式,即利用FDSET(.)选择自己感兴趣的事件,从而避免了查询或读取的阻塞。通过实际运行通过网络得到的数据与实际现场直接所测量的数据经过比较发现数据丢失率较小能够满足允许的误差范围。见图2。

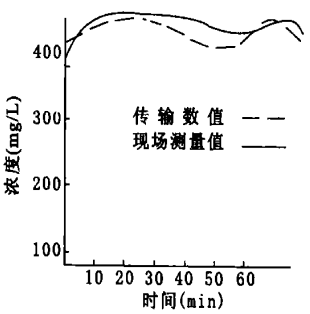

图2 传输数据与测量数据的比较误差

3 远程网络的安全与加解密

由于本系统用于监控,所以系统安全性要求较高,加之采用远程传输(Internet),就其本身安全性较差,如何解决这个问题是系统成功与否的关键。不安全性的因数来自两个方面:(1)远程端内部的安全漏洞;(2)传输过程中的非法入侵者(如被监测用户)。随着网络的快速发展,网络事故也不断发生。在系统的安全性上,主要关注以下两个方面:(a)对于网络互接时所需考虑的安全性;(b)对于数据本身所需考虑的安全性。首先分析其网络拓扑结构(图3):在此拓扑结构中,所需注意的是远程端与中心服务器对接部分即不能有匿名用户由路由器(Router)非法进入中心服务器,同样也不允许由服务器端进入远程端,在网络本身的安全性上有以下两种措施:(1)采用防火墙(Fire Wall)进行隔离一些非法用户的攻击如IP冒用,恶意多连接等。(2)针对每一个远程端采用帐号管理(如图1)的加密帐号。这里采用美国联邦政府公开的加密方法即DES加解密算法因其远程计算机与主服务器的连接具有一定的固定性,所以相对于非对称加解密算法在本系统有其自身的优越性。DES简述如图4所标志:其数据加密的解密过程仅由密钥所决定,目前多采用56位密钥。对于破解的时间将为2^{56}的可能性约为1000年时间。并且由于一位的变化可以引起多位的变化(即雪崩效应),所以对于其破解有非常大的难度。并且这种分散方式的加密方式特别适合可扩展的系统,如可以任意增加被监控的污水口而不需要改变加解密的密文。

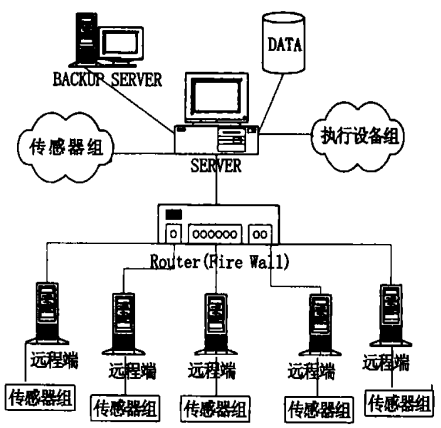

图3 远程网络拓扑图

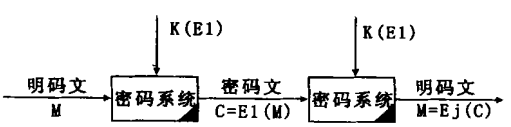

图4 DES加解密算法流程图

加密过程如下:

(1) 系统管理员在服务器端录入密约,并转换成64位二进制码形式。此处录入的密约是明文,是将要被加密的信息。

(2) 64位二进制码进行与密钥无关的初始置换,是增加DES算法安全性的固定置换。该置换依次把密约从第1位到第64位按照一定规律进行置换,形成

置换矩阵。

(3) 行乘积变换。是该算法的核心所在,主要由密钥表计算和加密函数组成。它是由经过初始置换的明文以及用户输入的加密密钥形成。加密密钥是由客户端例如每一污水排放口的数据采集 PLC 中输入的一组字符。乘积变换包括 16 次迭代运算,行迭代 16 次后,将得到形式为 LR(L 和 R 分别代表左右 32 位码组)的输出,然后对左右码组进行互换得到 RL。进行逆置换。它对 RL 进行操作,把初始置换变换的位换回原处,是初始置换的逆过程。

(4) 输出 64 位二进制作为加密的结果,并转换成密文形式。

(5) DES 算法的解密过程和加密过程相仿,不再重述。

4　数据本身涵盖信息的加解密

由于传输的数据要经过 Internet 网络的传输,这样便存在着潜在的不安全性。因此对于数据本身的加解密相当重要。数据加解密的另外一个好处是在服务器端通过解密也可进一步判断整个网络是否有安全隐患,因为根据统计,大部分情况下数据遭到破坏是发生在远程端本身或服务器本身,通过这种对称方式的加解密即可判断在污水口是否有蓄意破坏的发生。

加密过程:

(1) 声明一个 p 整形变量 r,$1 \leq r \leq p$,有 gcd(r,p - 1) = 1,接下来有 $E_i = P_i^r \text{MOD } P$,在这里 P(i) 是 E_i 的公共密钥(PUBLIC KEY),E_i 是(n - 1)次多项式的系数。

(2) 构造函数 $f(x) = A_{n-1}X^{n-1} + A_{n-2}X^{n-2} + A_{n-3}X^{n-3} + \cdots\cdots + A_1X + A_0 \text{Mod } p$,有 $f_{ui} = e_i$ (i = 1,2,3 ……n),在这里 A_i 可由解得 n 的方程所得到,每一个 A_i 是 512 位。A 则为连乘 A_i (i = 0,1,2,3 ……n)所得到。

(3) 构造一数值长度与 A 相等的 M 计算与比较 A 与 M 的大小。(a) 当 A > M 时计算 g (A_i),i = 0,1,……,n - 1) 在这里 g(·) 用于压缩 A_i 的长度,其长度为 $\left[\frac{\text{长度}}{n}\right]$;(b) 当 A < M 时计算 h ($A_i$),i = 0,1,……n - 1) 在这里 h(·) 用于压缩 A_i 的长度,其长度为 $\left[\frac{\text{长度}}{n}\right]$。

(4) 接下来计算 C = A ⊕M。

解密过程:

(1) 计算 $eij = R^{kij}$ 其中 k_{ij} 是每一个数据块 u_{ij} 的公共密钥。

(2) 对于以上构造的多项式 f (i) (i = 1,2,3 ……n),可以计算得到其数值,而由此可以解得其矩阵的正交解即为 A_i 的数值 $A = A_{n-1} \times A_{n-2}A_{n-3} \times \cdots\cdots A_1$ 的数值可以计算得到。

(3) 由 g(·),h(·) 可以计算得到 A′并调整使其长度与 C 相等既 A′= C,最后得到解密钥 M = A′⊕M,对于以上加解密算法,由于生成的多项式具有相对的不确定性,密钥长度为 512 位,所以安全性相对较高。

这种加解密的方法速度相对其它方法速度较快。在系统要求连续运行的情况下不会引起迟滞效应(Delay Response)的发生,作到了对污水口监控数据实时性的要求。

5　结语

通过上述方案,利用现有网络资源,最大程度的确保了远程通讯的安全性,为大规模实施污水排放远程集中监控提供了一个选择。此外,对于污水处理厂的运行状况,也可以采用该模式进行集中管理调配,最大程度的利用现有污水处理能力,降低污水处理成本,提高污水处理率。

[参考文献]

[1] Chin-Chen Changb, Kuo-Feng Hwangb. A threshold decryption scheme without session keys p Min-Shiang Hwanga [J]. Computers and Electrical Engineering, 2001, 27, 29～35.

[2] Vaagn L Zakariana, Mark J Kaiserb. An embedded hybrid neural network and expert system in a computer-aided design system [J]. Expert Systems with Applications, 1999, 16, 233～243.

[3] James R Nolan. An expert fuzzy classification system for supporting the grading of students writing samples [J]. Expert system with Applications, 1998, 15, 59～68.

(收修改稿日期:2001-12-27)

the measurement results of γ radiation dose rate and ^{222}Rn and its progeny concentrations in outdoor air in this region.

Key words: soil and rock; natural radio-nuclides; Southeast Fujian

Fresh MnO_2: Its Preparation and Application in Paper-making Wastewater Treatment

MA Zi-chuan, ZHANG Su-kun

(Department of Chemistry, Hebei Normal University, Shijiazhuang 050091*)*

Abstract: Four kinds of fresh MnO_2: XS-1, XS-2, XS-3 and XS-4 were prepared and characterized in laboratory scale. Comparative study conducted using them to purify paper-making wastewater showed the best performance of XS-1. Then experiments with XS-1 were carried out to study the effects of pH, dosage and temperature on removals of COD_{cr} and colority. Also studied were the optimum condition for wastewater treatment and the mechanism of fresh MnO_2 to purify paper-making wastewater.

Key words: fresh MnO_2; preparation; treatment; paper-making wastewater

Acid Rain in South Fujian Area: Its Characteristics and Measurement of Nitrite

SUN Xiang-ying, LIU Bin, LIAN Hui-ting, XU Jin-rui

(Department of Environmental Science and Engineering, Overseas Chinese University, Quanzhou 362011*)*

Abstract: Giving a brief description of acid rain in South Fujian area with respect to the characteristics and distribution, this paper highlights some nitrite sensors for acid rain monitoring. Several sensors using different materials have been made in laboratory. Featuring high sensitivity and stability, the sensors are expected to provide a basic tool for establishing automatic acid rain monitoring network.

Key words: acid rain; nitrite; chemically modified electrode

Forms of Heavy Metals Existing in Sediments of Yellow River's Qingshui He Section

YANG Hong-wei, JIAO Xiao-bao, WANG Xiao-li

(Department of Chemistry, Inner Mongolia Normal University, Huhhot 010022*)*

Abstract: Heavy metals on sediments of the Yellow River were analyzed by means of sequential chemical extraction in terms of their distribution characteristics and chemical speciation pertaining to the particles of different sizes. The results indicate that content of heavy metals increases as particle size decreases. Distributions of various forms of 8 heavy metals existing in sediments are described as follows: water-soluble, exchangeable, bound-to-carbonate, Fe-Mn oxides, organic and residual.

Key words: sediment; heavy metal; chemical speciation; the Yellow River

Approaches to Security Problem Relating to Long-distance Supervisory Control of Water Quality

WANG Tao[1], Zhang Wen-yu[2], ZHANG Hong-bo[1], WANG Jian-jun[3]

*(1. Chinese Academy of Mechanical Science & Technology, Beijing*100044*; 2. Department of Computer Science, Peking University, Beijing*100081*;*

*3. Handan Iron and Steel Group Co. Ltd., Handan*056015*)*

Abstract: To enforce monitoring and controlling of wastewater outfalls, long-distance supervisory control becomes more and more important. This paper deals with the ways to tackle the relevant problem of security, elaborating some critical issues such as network running speed under the existing network condition, encipher, decipher algorithm, etc.

Key words: long-distance supervisory control; wastewater monitor; data security; D-H encipher and decipher algorithm

Determination of Trace Organic Pollutants in Coking-plant Wastewater by GC/MS

CHEN Hui, DAI Hui

(Environmental Monitoring Station of Xiangtan City, Xiangtan 411104*)*

Abstract: GC/MS was used to investigate the organic pollutants removal in the activated sludge process for treating coking-plant wastewater. A new C_{18} mini-column was applied for concentration of the trace organics and the analytic results of GC/MS showed that activated sludge process was efficient in removing organic pollutants in coking effluents.

Key words: coking wastewater; trace pollutants; GC/MS; activated sludge process

An Approach to Cost-benefit Analysis in Environmental Impact Assessment

LI Guo-bin[1], LIU Zhuo[1], OUYANG Xian[2]

(1. China University of Geoscience, Wuhan 430074*;*

2. China Wuhuan Chemical Engineering Company, Wuhan 430079*)*

Abstract: This paper highlights the theory relating to seeking for the social optimum pollutant-discharging level, on which cost-benefit analysis of EIA would be made. Concept and procedure of cost-benefit analysis are discussed with emphasis on six fundamental