基于令牌的遥控加密实现方法

曾院辉，徐成斌

（深圳南瑞科技有限公司，广东 深圳 518040）

摘要：变电站综合自动化系统的网络结构目前已广泛采用以太网，以太网良好的开放性带来的网络安全问题已引起人们的极大关注。通过网络的遥控操作，其安全性就更为重要，为了加强遥控的安全性，除规范操作流程、增加防护墙外，将遥控报文进行加密也是一种有效办法。提出了一种基于令牌的遥控加密实现方法，该方法采用改进的RSA-1公开密钥算法，结合一次一密的加密思想，由测控装置产生令牌密文，操作员计算出令牌明文并回传测控装置以检测操作员的合法性。这样合法操作员能进行正常遥控，且能有效防止非法操作员的非法遥控。

关键词：综合自动化； 遥控； 令牌

Method of remote control encryption based on token

ZENG Yuan-hui，XU Cheng-bin

(NARI Science and Technology Co.,Ltd, Shenzhen 518040,China)

Abstract: At present,network configuration of transformer substation automation abroad widely adopts Ethernet,security matter of Ethernet's opening arose people′ s keen attention. Security of remote control across network become even more important. To enhance the security of remote control, there is a good method on remoting control message encryption except for regulating operation flow and enhancing protective wall. This paper brings forward a sort of remote control realization based on token.It adopts ameliorative RSA-1 publicity secret key arithmetic and combines method of encrypting on every operations. The measurement-control device brings up token, the operator calculates encrypted database and feedback measurement-control device to detecting the legitimacy of operator. In this way, legal operator can process normal remote control, and can effectively avoid any illegal remote control of any illegal operator.

Key words: substation automation; remote control; token

中图分类号： TM764 文献标识码： A 文章编号： 1003-4897(2007)01-0051-03

0 引言

目前以CANBUS、LONWORKS、Profibus为代表的现场总线技术得到了快速的发展，但现场总线的标准始终不能统一。已有10多种现场总线的国际标准同时存在，不同总线之间无法实现开放性和互操作性[1]。国内几家大型的电力自动化设备厂家采用了不同的现场总线标准，在一个变电站若将多个厂家的设备连接到综合自动化系统，需采用规约转换器或通信处理单元，给信息的传输带来瓶颈，也增加了成本。电力系统用户迫切希望各厂家采用统一的网络标准。

以太网的网络连接能克服现场总线的不足，目前已成为变电站综合自动化的研究热点，以太网在变电站综合自动化的应用具有如下的特点：

1) 采用国际主流标准，协议开放，不同厂家设备容易互连，具有互操作性；

2) 允许多种通信协议并存共享带宽；

3) 具有高度的可扩展性和良好的开放性，能满足与电力系统专用网络连接及容量扩充的要求，方便子网扩展；

4) 可实现远程访问，远程诊断；

5) 不同的传输介质可以灵活组合，如光纤、电缆、双绞线等；

6) 网络速度快，可采用10 M/100 M的传输速率；

7) 支持冗余连接配置，数据可达性强，数据有多条通路抵达目的地；

8) 网络传输协议采用TCP/IP或UDP，技术成熟，有商业软件开发平台支持。

1 网络安全问题

以太网的开放性带来了数据传输的安全问题。传输的安全保障有两种方式：专用通道技术和信息加密技术。专用通道技术需占用较多的网络资源，并随节点容量的增大而实现复杂。信息加密技术是信息在发出之前进行加密处理，在使用之前要进行解密处理来保证数据的安全。

电力系统的数据传输的安全问题以遥控的安全性最为重要。网络错误或恶意的遥控会影响调度的运行，导致系统供电异常。目前电力供求矛盾日益突出，高电压等级线路的误遥控有可能引起电力系统的连锁反映，包括过负荷跳闸、备自投和过负荷切机，并可能最终导致系统的崩溃[2]。可见提高遥控的可靠性是非常必要的。

表 1 非法遥控的类型及危害

Tab.1 Genre and harm of illegal remote control

类型	危害
修改遥控对象号	将切次要负荷的命令改为切重要负荷
	将送重要负荷的命令改为送次要负荷
修改遥控类型	不能正常遥控，延误调度时机
非法遥合命令	对检修或备用线路送电，有人身安全问题
非法遥跳命令	异常停电，给生产、安全带来问题

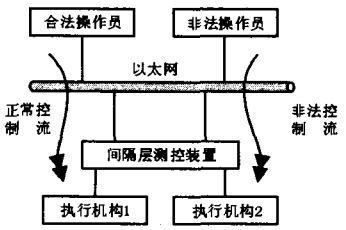

图 1 操作示意图

Fig.1 Sketch map of operation

非法操作员（网络黑客）和合法操作员共享以太网资源，合法操作员对间隔层测控装置的操作命令的格式和报文有可能被非法操作员获取。若不进行信息加密，非法操作员可以发相同的命令来控制测控装置操作执行机构，测控装置无法区分遥控命令的合法性。

传统的加密方式也不能阻止非法操作员发密文（操作命令）来操作执行机构。但如果每次合法操作员下发的密文（操作命令）不一样，且密文只能一次有效，则非法操作员就无法获取操作的命令。本文提出一次性明文的 RSA-1 公开密钥算法，能有效阻止非法操作员的恶意遥控。

2 RSA-1 公开密钥算法

公开密钥算法有两个密钥：一个公开密钥，可供所有人使用，将信息加密传送给使用者；一个秘密密钥，使用者用它来解密消息；

加密算法 E 和解密算法 D 必须满足以下 3 点：

1) D(E (P)) =P;

2) 从 E 导出 D 极其困难;

3) 由一段明文不可能破译出 E（选择明文攻击）。

典型的公开密钥算法是 RSA 算法，安全性建立在难于对大数（如 100 位数）提取因子的基础上，RSA-1 算法由本文提出，在 RSA 算法的基础上进行改进，结合了一次一密的思想，其加密过程如下：

1) 选择两个大质数，p 和 q；典型积为 100 位。

2) 计算 $n=p\cdot q$ 和 $z=(p-1)\cdot(q-1)$。

3) 选择一个与 z 互为质数的数 d。

4) 找出 e，使得 $e\cdot d=kz+1$。

5) 公开密钥为(e,n)，由测控装置使用。

6) 秘密密钥为(d,n)，由合法操作员使用。

7) 测控装置随机生成一个明文，其值 P 落在区间[0，n]内，将 P 加密，密文 $C=P^e \pmod n$；发送给合法操作员。

8) 合法操作员解密 C，明文 $P=C^d \pmod n$；并将明文发回测控装置。

9) 测控装置检查明文是否正确，若正确则确认对方是合法操作员，并删除此明文。

以上的加密过程伴随遥控的进程，非法操作员下发遥控选择后，对应的测控装置上送了返校报文和令牌密文。由于非法操作员没有秘密密钥(d,n)，无法对测控装置送来的密文解密，得不到正确的明文下发测控装置，被测控装置识破，遥控操作被拒绝。RSA-1 算法的安全性还在于明文是一次性的，明文的内容没有含义。一次一密是不能被破译的，所以 RSA-1 算法的安全性和 RSA 算法一样。RSA-1 算法与 RSA 算法的不同点：

1) RSA-1 算法针对双向多进程数据传输；RSA 算法针对单向单进程数据传输。

2) RSA-1 算法传输密文和明文；RSA 算法仅传输密文。

3) RSA-1 算法明文内容无实际含义，仅为标识；RSA 算法明文内容就是信息。

4) RSA-1 算法明文仅使用一次；RSA 算法对明文没有限制。

5) RSA-1 算法伴随遥控过程进行加密、解密；RSA 算法与遥控无关，不能防止非法操作员的遥控。

采用 RSA-1 算法的遥控过程见图 2。

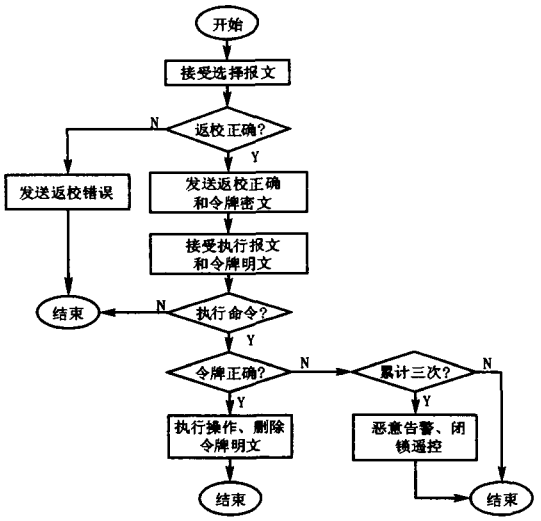

图 2　RSA-1 算法遥控过程

Fig.2　Remote control process of RSA-1

RSA-1 算法遥控过程与普通遥控过程相比，操作员在接受遥控返校报文时，需将令牌密文接受，解密后连同执行报文下发测控装置。加密密钥由操作员通过其他报文传送给测控装置，解密密钥不在以太网传送。测控装置需增加如下功能：

1) 在发送返校正确报文时，产生令牌明文，将明文加密后送操作员；

2) 接受执行报文和操作员发送的解密后的明文；

3) 判断接受的明文是否和产生的令牌明文一样，若一样，执行遥控命令，否则累计三次提示系统有非法操作员，并闭锁遥控进程。

令牌由测控装置生成，由于令牌明文和密文都在网络上传输，非法操作员可以获取令牌明文和密文，一般来说应避免一个网络中出现两次相同的令牌。以免非法操作员照抄密文和明文，进行非法遥控。令牌可以包含单元地址以区分不同测控装置，令牌的长度越长，安全性越高。测控装置可以采用投币法随机产生令牌，也可在令牌中加入一些校验码，对令牌的有效性进行校验，防止如全 0 的令牌产生。

3　示例说明

为了方便，选用 2 位数的密钥来示例说明。先选择 RSA-1 算法的密钥，假设 p=3，q=11，则 n=33，z=20。选取 d=7，求出 e=3，则公开密钥为（3，33），秘密密钥为（7，33）。有

1) 加密过程：$C=P^3 \pmod{33}$；

2) 解密过程：$P=C^7 \pmod{33}$；

若明文为 25，则 $25^3 \pmod{33}=16$，密文为 16，解密时 $16^7 \pmod{33}=25$，得到明文。

以 ISA 通信规约为例，设单元地址为 0x15，遥控通道号为 0x29，合闸操作，其普通遥控过程为：

1) 选择（下行）：0x08 0x00 0x15 0x44 0xCC 0x29 0xCC 0x29

2) 返校（上行）：0x08 0x00 0x15 0xA6 0xCC 0x29 0xCC 0x29

3) 执行（下行）：0x08 0x00 0x15 0x44 0xAA 0x29 0xAA 0x29

普通遥控过程中，非法操作员发送固定的选择和执行报文就可非法遥控。

增加令牌的遥控过程为（选择令牌明文为 25，即 0x19，加密后为 0x10）：

1) 选择（下行）：0x08 0x00 0x15 0x44 0xCC 0x29 0xCC 0x29

2) 返校（上行）：0x08 0x00 0x15 0xA6 0xCC 0x29 0xCC 0x29 0x19

3) 执行（下行）：0x08 0x00 0x15 0x44 0xAA 0x29 0xAA 0x29 0x10

基于令牌的遥控过程增加了遥控报文的长度，一般来说 n 取 100 位的数就不容易通过加密密钥得到解密密钥，此时传输的报文长度增加 50 个字节，这对于高速的以太网来说没有问题。基于令牌的遥控过程同时增加了操作员和测控装置的计算工作量，但对于提高遥控的安全性来讲也是值得的。

4　结论

基于 RSA-1 算法的遥控操作尽管计算工作量较大，但对令牌没有特殊要求，不增加电力自动化系统的运行管理难度。

用于加密的密钥是公开的，测控装置的厂家无需了解解密密钥，实现比较容易。测控装置和监控系统（包括调度系统）可以是不同的厂家，对电力系统的招标和选型没有限制。

电力系统的安全事关重大，在电站自动化大量采用开放的以太网的今天，遥控的安全问题已日益引起人们的重视，将密钥系统的研究成果应用到遥控的安全防误具有重要的意义。

（下转第 62 页　continued on page 62）

和可行性。建立在通信服务商基础上的信息传输稳定性有待提高，在此基础上不断改进，这种技术将会得到更广泛的应用。

参考文献

[1] 韩绍甫，杜树新. 电能质量监测系统设计及实现[J]. 电力自动化设备，2006, 26(4)：80-84.
HAN Shao-fu，DU Shu-xin. Design and Realization of Power Quality Monitoring System [J]. Electric Power Automation Equipment，2006,26(4)：80-84.

[2] 肖湘宁. 电能质量分析与控制[M]. 北京：中国电力出版社， 2004. 54-121.
XIAO Xiang-ning. Analysis and Control of Power Quality Monitoring[M]. Beijing: China Electric Power Press, 2004.54-121.

[3] 段成刚，欧阳森，宋政湘, 等. 新型在线实时电能质量监测设备的设计[J]. 电网技术，2004, 28(1)：60-63.
DUAN Cheng-gang,OUYANG Sen,SONG Zheng-xiang,et al.Design of a New Online and Real-time Power Quality Monitor[J].Power System Technology,2004,28(1):60-63.

[4] Technical Documents for MSC1210Y5[Z]. Texas Instruments,2004.

[5] The Measurement and Automation Catalog 2000[Z]. Texas (USA): National Instrument Corporation，2000.

[6] 邓焱，王磊. LabVIEW7.1 测试技术与仪器应用[M]. 北京：机械工业出版社，2004. 296-317.
DENG Yan, WANG Lei.LabVIEW7.1 Test Technology and Instrument Application[M].Beijing:China Machine Press,2004.296-317.

收稿日期：2006-08-04； 修回日期：2006-11-16

作者简介：
孙鹤林(1981-)，男，硕士研究生，研究方向为电力系统在线监测技术； E-mail:helin_sun@126.com

（上接第 53 页 continued from page 53）

参考文献

[1] 林功平. 配电网馈线自动化技术及应用[J]. 电力系统自动化, 1998, 22(4):64-68.
LIN Gong-ping.Distribution Network Feeder Automation Technology and Its Application[J].Automation of Electric Power Systems, 1998,22(4):64-68.

[2] 陆俊，李军，吴涛. 华北东北联网后华北主网安全稳定性的研究[J]. 华北电力技术, 2000, 29(1):3-4, 7.
LU Jun,LI JUN,WU Tao.Study on Stability of North China Main Power Network When North and Northeast Power Network Interconnected[J].Technology of North China, 2000,29(1):3-4,7.

收稿日期：2006-07-17； 修回日期：2006-09-22

作者简介：
曾院辉（1968-），男，硕士，从事电力系统综合自动化领域的研究与技术开发； E-mail:zengyh@sznari.com
徐成斌（1972-），男，硕士，从事电力系统综合自动化领域的研究与技术开发。

（上接第 58 页 continued from page 58）

[10] Ooi B T, Joos G, HUANG Xiao-gang.Operating Principle of Shunt STATCOM Based on 3-level Diode-clamped Converter[J]. IEEE Trans on Power Delivery, 1999,14(4): 1504-1510.

收稿日期：2005-12-31； 修回日期：2006-01-24

作者简介：
云平平(1980-)，男，硕士研究生，研究方向为电力电子技术及其应用; E-mail:yppinverter@sina.com
刘永和(1953-)，博士，男，教授，研究生导师，研究方向为大功率静止变换装置及其控制技术；
杨宝峰(1976-)，男，博士研究生，研究方向为电力电子技术及其应用。