文章编号:1671-4598(2019)05-0178-05 DOI:10.16526/j.cnki.11—4762/tp.2019.05.040 中图分类号:TP309 文献标识码:A

面向电压监测终端的远程升级加密通讯方法

包依勤
(南京晓庄学院 信息工程学院,南京 211171)

摘要:随着智能终端应用的日益增长和对其功能需求的不断提高,需要对嵌入式软件进行远程在应用升级;针对电压监测终端远程在线升级的安全性,从前的升级只考虑实现升级功能,而忽视升级效率和安全性,造成升级软件易被第三方窃取等问题,提出了一种在线升级加密通讯方法,通过对电压监测系统的架构、通讯规约、文件结构及加密方法等进行了分析和研究,采用断点续传、Fibonacci 矩阵和 Diffie—Hellman 密钥交换等方法,既保证了升级操作的升级效率,又实现了安全性,容错性;实践结果表明,此种升级加密通讯方法,提高了终端的升级效率和安全。

关键词:在应用升级;断点续传;公开密钥;斐波那契

Remote Upgrading Encryption Communication Method for Voltage Monitoring Terminal

Bao Yiqin
(College of Information Engineering, Nanjing Xiaozhuang University, Nanjing 211171, China)

Abstract: With the increasing application of intelligent terminal and the increasing demand for its functions, it is necessary to remotely upgrade IAP for embedded software. Aiming at the security of remote online upgrade of voltage monitoring terminal, the previous upgrade only considered the upgrade function, but neglected the efficiency and security of the upgrade, which made the upgrade software easy to be stolen by the third party. This paper proposed an online upgrade encryption communication method, through the framework of voltage monitoring system, communication protocol, files. The structure and encryption method are analyzed and studied. The methods of discontinuous transmission, Fibonacci matrix and Diffie—Hellman key exchange are used to ensure the efficiency of upgrade operation, and to achieve security and fault—tolerance. The practice results confirmed the upgraded encryption.

Keywords: IAP; broken—point continuously—transferring; public key; Fibonacc

0 引言

随着国民经济的迅速猛发展,电力负荷急剧增长,特别是非线性、冲击性负荷设备的的不断增长,导致了电网系统产生高次电压和电流谐波,引起线路损耗增加,甚至损坏电气设备,对电网系统造成了严重的污染和干扰。为了对电能质量进行有效的监测与分析,改善电能质量,为了给供电和用电双方提供实时数据依据,需要有一种监测设备对电网质量进行实时监测。

电压监测终端是实时测量和分析电压和电压畸变率等电网质量数据的重要设备,该设备通过 GPRS 接口与主站进行通讯,实现远程监测功能。但是,电压监测终端作为一个监测设备,监测内容和电压质量分析功能会随着供电部门的不断需求而要经常改变和调整,也就需要对电压监测终端中嵌入式软件进行远程升级[1],传统的解决方法是生产厂家技术人员到现场人工重新烧写程序,或者通过串口 ISP 在线编程更新程序,也有通过切换到自己的升级平台进行远程升级的,但升级效率低,可靠性不高,有时异常情况还需到现场维护,特别对大量的地域分散的设备进行升级时,工作量非常大,系统很难管理。钍对这一情况,需要有一个的好的升级手段和升级平台,来提高远程升级的效率。

从前的远程升级,只是简单用密码对数据进行加密,如第三方在通讯时很容易通过监控设备捕获到通讯报文,进行解密,从面造成嵌入式软件被窃取,造成大量的经济损失。

本文通过分析电压监测终端系统总体结构,解析了烧写程序 HEX 文件,统一升级规范和平台,实现了一种远程在线升级的加密通讯方法 DV _ IAP。具有分布式断点续传[2]、容错、安全认证[3]功能,大大提高了远程升级效率和升级的安全性。

1 远程升级系统

1.1 系统架构

电压监测系统主要包括电压监测终端、前置机服务器、数据库和 WEB 服务器,远程监测和远程监测应用系统、WEB 应用终端等,组成分布式系统[4],如图 1 所示。电压监测终端通过 GPRS 与具有固定 IP 地址的前置机服务器连接并实现数据通讯。但是,随着电压监测终端连接前置机数量的增多,达到几万台,就需要在系统中采用负载均衡[5]技术。电压监测终端与前置机的连接是动态的,通过任务调度[6]程序来完成。

收稿日期:2018-10-26; **修回日期**:2018-11-30。
基金项目:江苏省科技项目(BY2016095—3)。
作者简介:包依勤(1966-),男,江苏南京人,硕士,研究员级高级工程师,主要从事配网自动化和智能终端安全技术方向的研究。

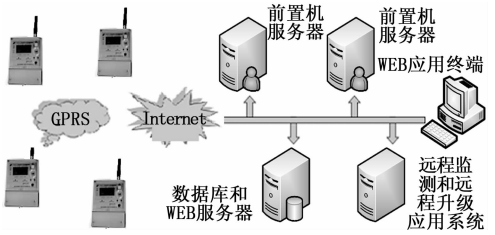

图 1　电压监测系统平台架构

远程监测与远程升级是通过 SOCKET 与前置机服连接、发送和接收报文数据。DV _ IAP 是分布式断点续传和安全论证的远程升级方法，需要升级时，只要将需要升级的电压监测终端 CPU 二制式文件（HEX 文件）放入分布式系统中，系统自动将 HEX 文件解析，并按通讯规约打包成多帧分布发送到前置机，任务管理器进行调度再转发给电压监测终端，从而实现远程升级。

1.2　系统软件

如图 2 所示，系统软件主要分为二个部分：前置机服务器和主站应用平台，前置机服务器向上与主站平台通讯，接收主站发过来的报文，通过规约解析后，前置机服务器向下通过通讯任务调度和通讯接口与电压监测终端连接。

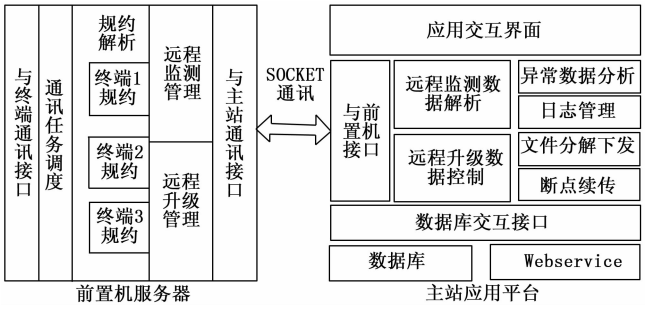

图 2　系统软件结构

由于不同厂家生产电压监测终端在同一平台下运行，所以必须统一通讯规约和升级平台，主站应用平台在需要实现远程升级功能时，首先将不同厂家的待升级文件解析[7]，按照统一的规约通过文件分解下发模块和远程升级数据控制模块发送至前置机服务器，并通过分布式断点续传，解决网络可靠性和多终端同时升级的问题，在安全性方面通过安全论证和报文中数据校验保证了升级文件的完整性。

主站应用平台上可以通过界面看到数据库中各个电压监测终端的升级情况，用户可以通过访问 Webservice 接口查看电压质量信息和电压质量分析结果，并能够对异常数据进行分析，对日志进行管理。

2　系统通讯

2.1　通讯规约

远程升级依靠标准协议《电力负荷管理系统数据传输规约》，协议采用 GB/T18657.1 的 6.2.4FT1.2 异步传输[8]帧格式，规约也采用了类似“会话”的通信协议，每次由负责采集的系统（规约称为“主站”），以通知指定地址码的装置（称为“终端”）准备接收数据，然后向其发送含有不同控制码的数据帧，并等待从站的应答。规约指定的数据帧格式，如表 1 所示。

表 1　帧格式

数据域	标识
起始字符	68H
长度	L
长度	L
起始字符	68H
控制域	C
地址域	A
链路用户数据	DATA
校验和	CS
结束字符	16H

其中 68H 为起始字符，A 为地址域，C 表明消息的来源以及前后消息的关系，并控制消息的功能；L 说明了数据域以双字节为单位的长度，设定 2 个 L 进行比较，增强可靠性，而 CS 则是从帧起始符到校验码之前所有字节模 256 的和，保证传输数据的正确性。

帧格式中链路地址域包含行政区位码＋终端地址（电压监测终端地址），用于分布式发送数据和接收报的唯一标识；用户数据包含所有用户类型数据，通过功能码和数据单元标识来区分不同类型用户数据，如表 2 所示。

表 2　链路用户数据帧格式

数据域	标识
应用层功能码	AFN
帧序列域	SEQ
数据单元标识(1－N)	DADT
数据单元(1－N)	UNIT

在远程升级中主要用到的应用功能码 AFN 如表 3 所示。

表 3　应用层功能码含义

AFN	含义
00H	确认 / 否认 AFN
06H	身份认证及密钥协商
0FH	文件传输

在 AFN＝0FH 时，数据单元采用 F1 文件传输数据格式如表 4 所示。

表 4　文件传输数据格式

数据内容	数据格式	字节数
文件标识	BIN	1
文件属性	BIN	1
文件指令	BIN	1
总段数 n	BIN	1
第 i 段标识或偏移(i=0～n)	BIN	1
第 i 段数据长度 Lf	BIN	1

2.2 HEX 文件格式解析

电压监测终端采用 ARM7 的 LPC2136，使用 keil 仿真及开发工具，生成烧写文件 HEX 文件，可用记事本可打开，它的每行格式如表 5 所示。

表 5 HEX 文件格式

LEN	ADDR	TYPE	DATA	CS

LEN：记录中的数据字节数目，1 个字节。

ADDR：起始地址，2 个字节。

TYPE：记录类型，1 个字节，04 指 HEX 文件开始，00 指 HEX 文件数据记录，01 指 HEX 文件结束。

DATA：HEX 文件数据，LEN 个字节。

CS：是此行记录的校验和，1 个字节。

例如：一个 HEX 文件

：020000040000FA

：1020000018F09FE518F09FE518F09FE510F09FE5A8

：102010000CF09FE5846FA0B80CF09FE50CF09FE5F5

：102020002C2100003420000038200000942000003

：0CBF900000000000040000040EC1F00001A

：00000001FF

（1）文件头。

：020000040000FA

02：是记录中的数据字节数目。

0000：这个域总是 0000。

04：是记录类型，指文件开始。

0000：是该段的地址。

FA：是效验和。

（2）文件数据。

：1020000018F09FE518F09FE518F09FE510F09FE5A8

10：是此行记录数据的字节数目。

2000：是数据在内存（将要烧写的 eprom 地址）中的起始地址。

00：记录类型 00，指是一条数据记录。

18F0－9FE5：是 HEX 文件数据。

A8：是此行记录的效验和。

（3）文件尾。

：00000001FF

00：是记录中的数据字节数目。

0000：这个域总是 0000。

01：记录类型 01，指文件结束。

FF：是效验和。

2.3 文件升级

烧写到电压监测终端的程序，合并了二个程序：boot.hex 和 main.hex。boot.hex 是启动程序，编译时开始地址从 0x0 开始，主要功能是：上电时看启动标志位（4 个字节），如全是 0xAA，则进入主程序 main.hex，如如全是 0x55，则将通过 GPRS 传来的新的 main.hex 程序覆盖从前的 main.hex。

main.hex 是主程序，是待升级的程序，编译时开始地址从 0x2000 开始（假如不需要升级功能，开始地址从是 0x0 开始，不需要 boot.hex），主要实现电压监测终端的功能，按照 2.2 的文件格式合并二个 HEX 文件 boot.hex 和 main.hex 成一个文件 dy－main.hex，合并如下：

boot 头

boot 体　地址从 0 开始

main 体　地址从 0x2000 开始

main 尾

dy－main.hex 是具有 IAP 功能的电压监测终端程序，要事先烧写到 LPC2136 中，远程升级其实是将 main.hex 通过主站传过来进行升级。

1）文件的传输。

（1）主站按照 2.3 读取 main.hex，读取到总行数 RowNum，计算总报文数 TotalNum，16 行打成一包。

（2）将每行数据 ASC 码字符转换成转成十六进制码，一包 16 行，按表格 5 的格式，文件数据存放 16 行数据，共 16＊16＝256 字节，最后一行可能不足 256 字节。

（3）按 2.1 文件通讯规约发送数据报文。

（4）最后一帧数据包后加上 2 个字节，是整个文件数据校验和 CS。

（5）终端接收所有报文，计算所有报文数据的校验和 CS1，如果 CS1 等于 CS1，则文件传输正确。

2）文件的断点续传

由于数据传输通道是无线信道，难免会有信号干扰和丢包现象，所有升级过程中采用断点续传流程，如图 3 所示。

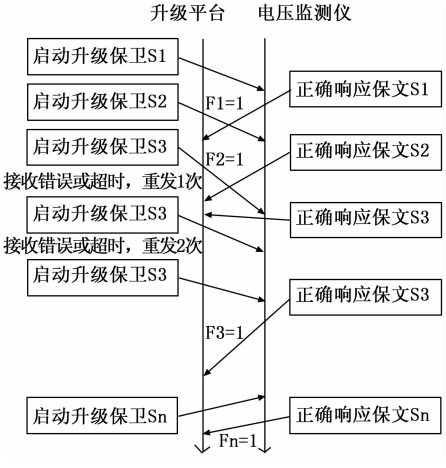

图 3 文件传输和断点续传流程图

实现过程：传输一个文件共有 n 个报文，报文从 $S1$－Sn，报文传送标志从 $F1$－Fn，初始标志 $Fi=0$（$i=1$，n）；升级平台从 $S1$ 开始通过 GPRS 启动下发报文，下发报文 Si，如接收到正确响应报文，则启动下发下一个报文，并

置标志 $Fi=1$；如接收到错误响应报文或接收超时（10 秒），则重新传相同的报文，重传最多三次后如还不能收到正确响应报文，则继续下传下一个报文，并置标志 $Fi=0$；直至下发最后一个报文 Sn，如接收正确响应报文后，升级平台检查所有报文标志 Fi（$i=1$，n）是否为 1，如 Fi 为 0 则 Si 是断点。重复上述过程，进行断点续传，直至所有报文标志为 1；最后比对一下校验和，如正确则更新升级程序。

3　加密通讯方法

3.1　Diffie－Hellman 加密方法

传统的加密方法采用对称密钥来加密和解密数据，很容易被第三方破解，采用 Diffie－Hellman 非对称加密技术又称公开密钥加密技术，通过公开密钥加密数据，抗攻击能力强[9]，可有效防止中间人破译和攻击。Diffie－Hellman 加密方法 DHKE 基本原理和加密过程，即：双方约定一个整数 g，一个素数 N。首先，各自产生一个私有密钥 x 和 y，并计算出各自的公开密钥 X 和 Y，X 和 Y 相互交换。其次，公开密钥交换后，双方计算出用于加密和解密的密钥 $K1$ 和 $K2$，结果是相同的。这样，通讯双方通过密钥 $K1$ 和 $K2$ 来加密和解密报文[10-12]，从而实现数据的加密传输。

它的理论基础是：离散对数计算的复杂性，已知 $X=\bmod N$，直接求 x 是不可行的，例如：已知，$X=146$，$g=15$，$N=197$，求 $x=43$ 是不可能的。

3.2　基于 Fibonacci 和 Diffie－Hellman 加密

无线数据传输难免会有误码，如系统具有容错性，即具有矫正误码能力，可提高升级效率，减少续传频率，而通过斐波那（Fibonacci）矩阵和 Diffie－Hellman 加密方法 FBDH 可实现容错性加密，即：双方约定：公开一个整数 g，一个素数 N，一个 Fibonacci 矩阵 Fn 序列 n，首先，各自产生一个私有密钥向量 x（x_1，x_2，x_3）和 y（y_1，y_2，y_3），并计算出各自的公开密钥向量 X 和 Y，双方对 X 和 Y 进行交换。其次，公开密钥向量交换后，双方计算出用于加密和解密的密钥向量 K 和 G，结果 K 和 G 是相同的。发送方通过密钥 K 加密数据，并通过 Fibonacci 矩阵 F_n 变换，最终获得加密数据向量；接收方接收数据，通过 Fibonacci 逆矩阵变换，再经过 G 解密报文，最终获得三列原文向量；对原文三列向量进行比较，三列中有二列相等，如相同获得原文。通过以上过程，数据获得容错能力，从而实现了数据的加密容错传输。

Fibonacci 数列：又称黄金分割数列，指的是这样一个数列：1、1、2、3、5、8、13、21、34、……在数学上，斐波纳契数列以如下被以递归的方法定义：$F(0)=1$，$F(1)=1$，$F(n)=F(n-1)+F(n-2)$（$n>=2$，$n\in N^*$），在现代物理、准晶体结构、化学等领域，Fibonacci 数列都有直接的应用，为此，美国数学会从 1963 年起出版了以《斐波纳契数列季刊》为名的一份数学杂志，用于专门刊载这方面的研究成果。Fibonacci 数列是使用最为广泛应用的数列，Fibonacci 递推矩阵使 Fibonacci 数列计算容易，使用较多的有二阶 Fibonacci 递推矩阵和三阶 Fibonacc 递推矩阵。

在 FBDH 中，使用三阶 Fibonacc 递推矩阵 Fn 矩阵[13]：

$$Fn=\begin{pmatrix}1&1&1\\1&0&0\\0&1&0\end{pmatrix}^n \quad n=0,1,2,3\cdots\cdots \tag{1}$$

三阶 Fibonacc 逆递推矩阵 Fn^{-1} 矩阵[14]：

$$Fn^{-1}=\begin{pmatrix}0&1&0\\0&0&-1\\1&-1&-1\end{pmatrix} \quad n=0,1,2,3\cdots\cdots \tag{2}$$

从（1）（2）看出，利用 Fibonacc 矩阵和逆矩阵，一方面增强中间人解密的难度，另一方面自身加密解密计算的复杂度低。

3.3　加密算法实现

在传输升级文件时，主站对数据进行加密，终端对数据进行解密。

3.3.1　加密过程

主站做下列步骤：

Step1：公开约定三个参数 g，N，Fn；

Step2：选择自己的私有密钥向量（x_1，x_2，x_3），并计算：

$X=$（gmod N，gmod N，mod N）

X 作为公有密钥向量；

Step3：选择终端的公有密钥：

$Y=$（g^{y_1} mod N，g^{y_2} mod N，mod N）

并计算加密密钥向量：

$K=Y^x=$（$g^{x_1*y_1}$ mod N，$g^{x_2*y_2}$ mod N，mod N）

K 定义为（K_1，K_2，K_3）

Step4：想将数据 M 发给终端

M 如有 5 个字节，$M=$（m_1，m_2，m_3，m_4，m_5）

计算加密矩阵：$C=M^T+K$

Step5：选择三阶斐波纳契数列的递推矩阵 F5

计算加密变换矩阵：

$E=C\times F5=$（E_1，E_2，E_3）

Step6：公开将 E 发送给终端

3.3.2　解密过程

终端做下列步骤。

Step1：公开约定两个参数 g，N，Fn。

Step2：选择自己的私有密钥向量（y_1，y_2，y_3），并计算。

$Y=$（g^{y_1} mod N，g^{y_2} mod N，mod N）

Y 作为公有密钥向量。

Step3：选择主站的公有密钥。

$X=$（g^{x_1} mod N，g^{x_2} mod N，mod N）

并计算加密密钥向量：

$G=Y^{y}=(g^{x_1*y_1} \bmod N, g^{x_2*y_2} \bmod N, \bmod N)$

G 定义为 (G_1, G_2, G_3)

Step4：公开接收主站的数据 E。

$E=\{E_1, E_2, E_3\}$

Step5：选择三阶斐波纳契数列的递推矩阵逆。

计算 $T=E-G=(M_1, M_2, M_3)$

Step6：终端对数据进行比较。

由于：$F5*F5^{-1}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$

$K=G$（根据 Diffie－Hellman 原理）

所以：T 三列是相等，即：$M_1=M_2=M_3$

比较三列，如三列相等，最后获得 $M=(m_1, m_2, m_3, m_4, m_5)$，结束。

如三列中有某一行不等，则进入容错处理。

Step7：容错处理。

一个数据通过密码向量加密 后形成三个加密数据，解密后也是三个数据，如发现三个数据不等，采用循环枚举法，重复解密过程，直至三个数据相等，定位枚举值，就是正确值。选中这个列值，最后获得：$M=(m_1, m_2, m_3, m_4, m_5)$。

3.4 加密算法实现举例

主站：

约定两个参数 $g=15$，$N=197$，$n=5$

$x=(x_1, x_2, x_3)=(196, 46, 178)$

$X=(1, 53, 70)$

$K=(1, 105, 171)$

$M=(104, 101, 108, 108, 111)$

$$\boldsymbol{C}=\begin{pmatrix}105&12&78\\102&9&75\\109&16&82\\109&16&82\\112&19&85\end{pmatrix}$$

$$\boldsymbol{F}5=\begin{pmatrix}1&1&1\\1&0&0\\0&1&0\end{pmatrix}^{5}=\begin{pmatrix}13&11&7\\7&6&4\\4&3&2\end{pmatrix}$$

$$\boldsymbol{E}=\boldsymbol{C}\times\boldsymbol{F}5=\begin{pmatrix}185&82&151\\113&22&112\\84&162&6\\84&162&6\\156&25&45\end{pmatrix}$$

终端：

约定两个参数 $g=15$，$N=197$，$n=5$

$y=(y_1, y_2, y_3)=(45, 180, 8)$

$\boldsymbol{Y}=(148, 187, 16)$

$\boldsymbol{G}=(1, 105.71)$

$$E=\begin{pmatrix}185&82&151\\113&22&112\\84&162&6\\84&162&6\\156&25&45\end{pmatrix}$$

$$\boldsymbol{F}5^{-1}=\begin{pmatrix}0&1&0\\0&0&1\\1&-1&-1\end{pmatrix}^{5}=\begin{pmatrix}0&-1&2\\2&-2&-3\\-3&5&1\end{pmatrix}$$

$$\boldsymbol{T}=\boldsymbol{E}\times\boldsymbol{F}5^{-1}-\boldsymbol{G}=\begin{pmatrix}104&104&104\\101&101&101\\108&108&108\\108&108&108\\111&111&111\end{pmatrix}$$

$M=(104, 101, 108, 108, 111)$

上述数据分析：假设在没有干扰的情况下，主站欲将报文将 M 传送到终端。首先，主站对 M 加密加密和变换，生成 E，然后通过 2.1 传输规约断点续传传输给终端，终端对 E 进行解密和容错处理还原成 M。最终结果，通过此方法实现了终端远程升级的容错和安全。

4 测试对比

本文针对电压监测终端远程升级功能，采用了二种方法进行了测试，一种是传统的 IAP 方法，另一种是采用了新的加密通讯的方法 DV－IAP。测试结果比较，如表 6 如示。

表 6 远程升级方法测试结果比较

IAP 升级方法	升级数量	文件大小	掉包率	耗时	成功率
传统的 IAP	40	212KB	15.6%	200Min	95%
DV－IAP	50	287KB	1.5%	98Min	100%

从测试结果可以看出，新方法电压监测终端 DV _ IAP，具有容错加密功能。测试中，升级 50 台终端只用了 98 分钟，而传统的电压监测终端 IAP 升级 40 台终端却用了 200 分钟，DV _ IAP 升级效率大幅度提高，更重要的是：成功率从 95%到提高达到 100%，而且安全性也很好，达到远程升级可靠安全的目标。

5 结束语

智能电网的不断发展，使得对配电网遥测终端要求不断提高，需要升级终端的功能。对面向电压监测终端的远程升级加密通讯方法进行了研究与实现，阐述了远程升级软件平台、芯片 HEX 文件的生成、通讯规约、断点续传，重点研究了组合 Fibonacci 矩阵和 Diffie－Hellman 技术的加密通讯方法。应用结果表明，系统不仅实现了文件远程升级功能，而且解决了在传输过程中的保密性和容错性，具备了矫正误码的能力和防止中间人破解的能力，提高了电压监测系统的可靠性与安全性。此外，本文所采用的 DV _ IAP 升级方法对其他嵌入式系统远程升级有一定的借鉴和参考作用。

（下转第 187 页）