基于分散组播模式的电能表软件更新技术研究

梁 捷[1],梁广明[2]
(1.广西电网有限责任公司计量中心,广西 南宁 530023;2.南宁百会药业集团有限公司,广西 南宁 530003)

摘 要:针对传统电能表软件远程更新模式在测量点档案与实际不符时会更新失败的问题,首先,分析了传统集中式软件更新模式在档案,信道使用和存储方面存在的问题;然后,提出一种基于分散组播模式的电能表软件更新模式,并给出基于该模式的各过程的软件更新具体方案;接着,研究了原程序拷贝及回滚、更新程序的完整性及安全性的保障等更新过程中遇到的主要问题;最后,通过实例测试,验证了所提升级模式的可行性。

关键词:电能表软件更新;原程序回滚;完整性核验;组播
中图分类号:TM 933 **文献标志码**:A **文章编号**:1003 - 6954(2021)04 - 0090 - 05
DOI:10.16527/j.issn.1003 - 6954.20210418

Research on Energy Meter Software Update Technology Based on Distributed Multicast Mode

Liang Jie[1], Liang Guangming[2]
(1. Electric Power Research Institute of Guangxi Power Grid Corporation, Nanning 530023, Guangxi, China;
2. Nanning Baihui Pharmaceutical Group Co., Ltd., Nanning 530003, Guangxi, China)

Abstract: Aiming at the problems that the traditional remote update mode of watt-hour meter software fails to update when the measurement point file does not conform to the actual situation, firstly, the problems of the traditional centralized software update mode is analyzed in the aspects of archives, channel use and storage. And then, a software update mode of watt-hour meter based on distributed multicast mode is proposed, and the specific scheme of software update for each process based on this mode is given. Then the key problems in the process of updating such as the copy and rollback of the original program, and the protection of the integrity and correctness of the update program, are studied. Finally, the feasibility of the proposed upgrade mode is verified by experiments.

Key words: energy meter software update; original program rollback; integrity check; multicast

0 引 言

随着广西电网低压集抄系统“两覆盖”工作的推进[1],现场发现许多电能表抄表失败的原因是由电能表软件设计缺陷或故障导致的,故障处理时需对故障台区中的大量电能表进行软件更新。此外,随着智能电网的建设,新能源和电动汽车的接入[2]以及非侵入式智能家居设备的推广,对电能表提出更多软件方面的应用功能要求。这些新功能开发应用也需要对现场已安装的电能表进行软件更新来实现测试或应用的目标。

广西电网当前正在推广使用的符合南方电网技术规范的费控电能表,其上行通信协议虽然给出了软件远程升级的报文格式定义,但未给出具体的软件更新方案。为此,针对传统的电能表集中式软件远程更新模式存在的问题,设计了一种新的分散组播模式的电能表软件远程软件更新方案,详细介绍了其软件更新的实现过程并通过实例测试验证了其可行性。

1 软件更新方案设计

1.1 总体方案设计

根据国际法制计量组织(OIML)最新修订的电

能表国际建议 IR46,智能电能表管理芯片的软件升级不应影响计量的准确性和稳定性[3],即要求电能表管理芯片能独立于计量芯片进行软件更新。

由于现场安装的电能表在故障处理以及用户或电网公司有新业务需求时需要进行软件更新;且现场电能表安装数量庞大,安装位置分散,到安装点逐个进行人工更新和由主站进行点对点逐个电能表软件更新的方式工作量大,不能满足实际使用需求:因此要求智能电能表的管理芯支持在线软件更新功能。

传统对批量电能表进行软件更新主要基于主站集中分组的软件更新模式,这里简称集中式软件更新模式。首先,由主站根据自身档案和需求对电能表进行分组;然后,下发软件更新任务,终端根据接收到的更新任务,对电能表进行更新包的组播传输;最后,电能表接收更新包并存储和更新。组播是指根据一定的通信拓扑节点组成的路径将待传输数据进行分布式并发传输的方式,由于通过中间节点进行数据的分布处理,因此该机制的效率比点对点的单播模式高。集中由主站组播的集中更新方式凭借主站的服务器处理能力,数据处理和传输较快,软件更新业务效率高,适用于数据量大的业务过程。

但该方式存在的问题是:在对电能表进行分组时,传统软件更新方式由主站来发起,主站根据已经建立的档案信息来进行分组。由于档案更新不及时,会出现本台区的电能表找不到或者其他台区的电能表被划入本台区等主站所建的档案与实际的台区管辖不一致的情况,导致电能表与主站"失联"[4]。

对此,为了在保证电能表软件更新安全可靠的同时提高软件更新效率,设计了一种由各台区的计量终端分解更新任务的分散式更新模式。从主站侧观察,其过程主要可以分为以下 5 个阶段,如图 1 所示。

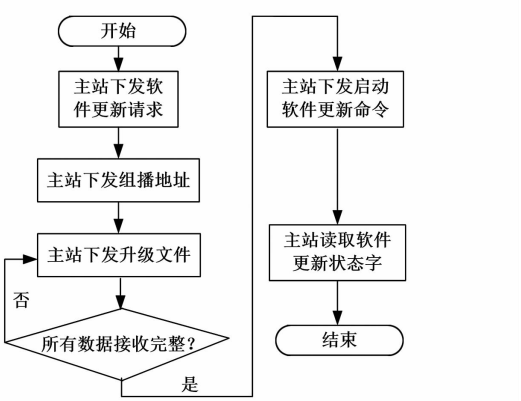

图 1　软件更新主要流程

如图 1,该模式的主要软件更新流程如下:

1)更新请求:软件更新请求由主站发起,主站获取待更新电能表厂家版本信息及待更新的模块信息,并下发更新初始化命令,让电能表或模块做好更新准备。2)更新分组:对电能表进行软件更新分组,分组由集中器或采集器完成,分组完成后根据分组情况下发组地址。3)更新程序下载:软件更新程序的下载由主站下发,为满足南方电网对电能表信息安全防护和完整性的要求,更新程序本身需进行加密和完整性校验。终端通过透传方式[5]直接将更新程序下载到电能表,为了提高更新效率,主站对更新文件采用组播方式下发[6]。4)更新程序下载确认:软件更新文件下发完成后,由集中器或采集器完成下载完整性检测,以点对点方式获取更新文件下载信息,对丢失包重新下发,所有包都接收完成后,对更新程序进行完整性校验,然后费控电能表通过其内置的嵌入式安全控制模块(embedded secure access module,ESAM)芯片进行解密。5)更新程序更新:下载完成主站下发启动更新命令,可选择立即更新和定时更新两种模式,满足更新要求后将下载的新程序更新到电能表管理芯的程序运行区,实现电能表的在线软件更新功能;电能表更新完成后由主站主动读取电能表更新状态字命令,确认是否更新成功。软件更新过程中计量芯正常工作,计量功能正常运行,避免因管理芯更新而导致电量漏记的问题。

该模式可依靠终端的抄表机制实现软件更新对象的实时和准确核对,但业务流程比集中式模式复杂且对终端的处理能力要求较高。适用于待更新电能表规模不大、要求及时进行信息反馈的更新业务。此外,更新文件采用主站分别下载到终端,由终端再对待更新电能表进行更新文件下发的方式,需在终端预留更新文件存放空间,对终端存储要求高。实际应用中可根据具体应用场景和需求选择集中或分散更新的模式。

1.2　更新方案详细设计

1.2.1　更新请求

区别于传统集中软件更新方式,出于如下考虑,不采用主站直接对电能表下发更新请求的模式:

1)主站直接操作电能表,一方面要通过台区识别确定电能表所属的终端;另一方面,在一对一更新时,主站需要知道待更新电能表的通信地址。而实

际主站记录的电能表、终端等的档案信息并不能确保 100% 无误,从而无法保证一定能找到所有需更新的电能表。

2)主站直接操作电能表在更新期间会增加主站与终端之间的信道通信压力。

3)主站获取电能表更新判断结果后,需要对更新的电能表信息进行保存,由于电能表数量庞大,信息存储会占用较多数据存储空间。

故所提模式的更新流程是:首先,由主站发起任务,主站获取更新文件中待更新电能表厂家版本信息及待更新的模块信息;然后,将更新任务信息发送给终端,由终端分别对其所辖电能表进行逐一的更新请求的处理,确定哪些电能表需要进行更新。假设计量终端所辖台区中所有电表组成的集合为 $\boldsymbol{M}=\{m_1,m_2,\cdots,m_{N-1},m_N\}$,则需更新电能表集合 $\boldsymbol{M}_{\mathrm{Q}}$ 定义为

$$\boldsymbol{M}_{\mathrm{Q}}=\{m_n\in\boldsymbol{M}\mid m_n\in\boldsymbol{M}_{\mathrm{T}}\cap\boldsymbol{M}_{\mathrm{C}}\ \text{且}\ R(m_n)<R_{\mathrm{s}}\} \tag{1}$$

式中:$\boldsymbol{M}_{\mathrm{T}}$ 为能与计量终端正常通信的电能表组成的集合;$\boldsymbol{M}_{\mathrm{C}}$ 为与更新文件对应的厂家一致的电能表组成的集合;$R(m_n)$表示序号为 n 的电能表的软件版本日期;R_{s}为更新文件对应的软件版本日期。

将 $\boldsymbol{M}_{\mathrm{Q}}$ 中的电能表通信地址、版本号等信息返回给终端,终端组织所有满足更新条件的电能表信息上传给主站。具体流程如图 2 所示。

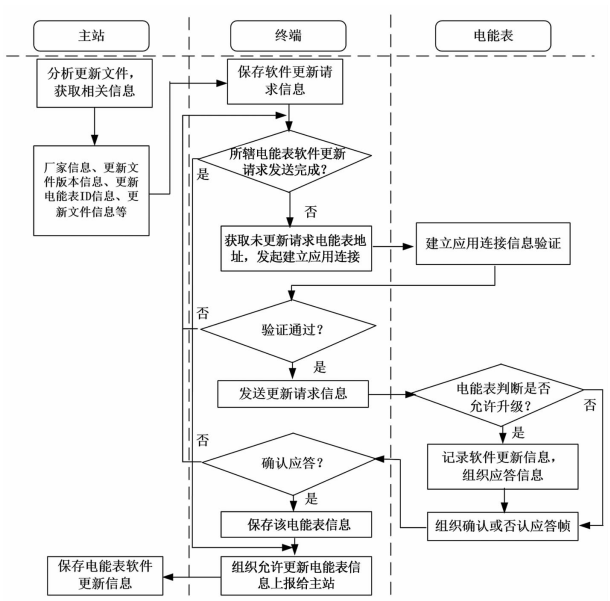

图 2 更新请求流程

从上述过程可见,所提方法的更新请求对于主站来说只需要知道每个终端下面是否有需要进行更新的电能表即可,不需要知道具体哪些电能表需要进行更新。此外,该过程中,终端 ESAM 需具备与电能表建立安全传输的应用连接的功能,若暂不支持,可以采用明文传输的方式。

1.2.2 更新分组

在主站以单播方式进行单个电能表软件更新的时候,不需要进行分组操作。而对批量电能表更新时,根据组播通信技术要求,此时需要对待更新的电能表进行分组。为减少主站与终端之间的交互,最终减少通信压力,所设计更新模式的更新分组不由主站完成,而是由主站发起任务,通过下发分组地址到终端,再由终端将组地址下发到待更新的电能表,实现对待更新电能表的分组。具体流程如图 3 所示。

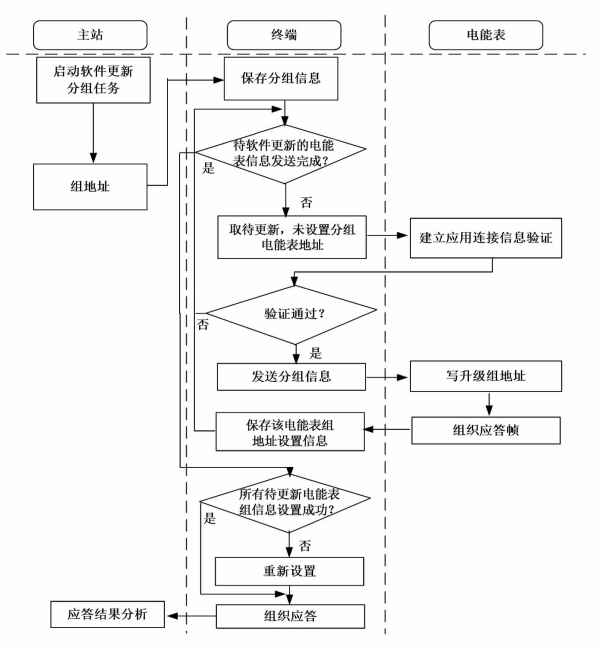

图 3 软件更新分组流程

1.2.3 更新程序下载

更新的程序文件下载采用主站下发到终端的方式。这是考虑到分组后采用组播地址进行文件下发与采用将更新文件下发到终端后再由终端下发到电能表这两种方式相比,虽然主站到终端之间的通信量在理想状态下相差不大,但实际上组播方式进行通讯传输过程中,一次下发成功率比采用主站下发到终端的方式低。当通信失败时,需要对缺失的包进行补发。由于组播机制通常不会预留用于补发的信道资源,故需要补发的电能表通信环境会比其他电能表恶劣。一些电能表可能需要通过多次补发才能实现完成整个更新包的传输,此时如果都通过主站来补发,主站通信量会剧增,从而可能导致通信的

堵塞。故选择采用主站传输更新程序到终端,然后再给电能表进行更新的方式。

更新程序由电能表生产厂家提供。其内容主要包括厂家信息、更新文件版本信息、更新电能表 ID 信息、更新文件信息及更新文件包。更新文件中包括各个模块的可执行程序及整体校验,更新文件通过 AES－128 算法进行加密,作为一个整体的文件,采用分块传输的方式进行下发,文件下载时需要支持链路层分帧,以便后期分块帧的重组。由于是组播下发,电能表不应答,为获得较高的成功率,可适当延长主站下发数据帧时两帧的时间间隔。更新程序下发具体流程如图 4 所示。

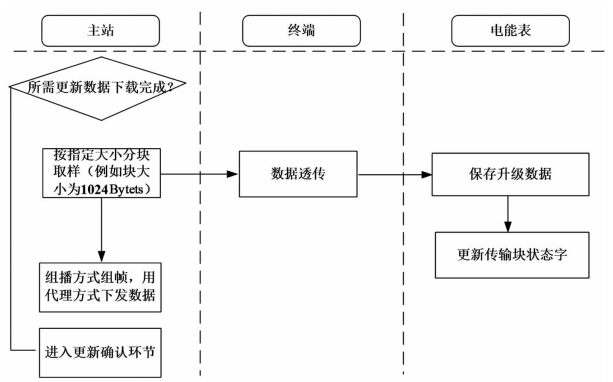

图 4　更新程序下载流程

1.2.4　更新程序下载确认

由于终端对更新文件下载的过程为单方向传输,故为了确保所有电能表均接收到完整的更新文件,终端在文件组播完成后即发起文件下载确认任务,对所辖更新电能表接收信息的确认。更新模式的确认流程如图 5 所示。

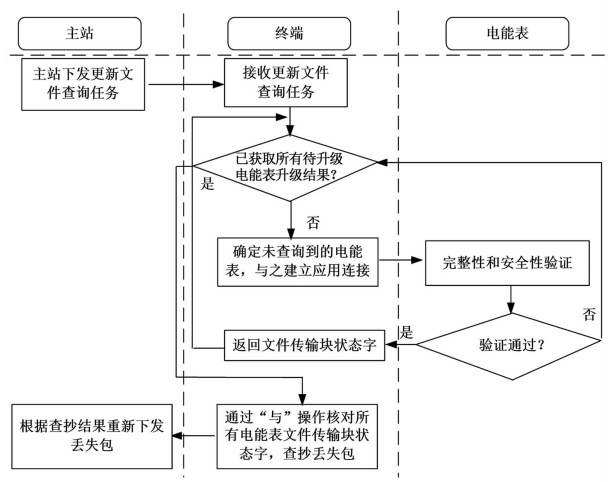

图 5　更新程序下载确认流程

图 5 中,电能表更新文件是否接收完整,由终端查询电能表文件传输块状态字进行判断。对于丢包的数据,集中器通过对块状态字进行分析,按下述两种补发策略进行更新程序补发:对大批量电能表都丢失的数据块,采用组播方式补;对于少量电能表丢失的数据块,采用单播方式进行补发。在进行下载文件的确认时,如果有某些包补发不成功,终端会进行有限次数的重复补发,若超过补发次数,则放弃该电能表的补发,继续更新流程。上述异常情况下,后续电能表收到更新启动命令时若数据包接收不完整,则返回异常应答给主站,主站再进一步的处理。

1.2.5　软件更新程序安装

升级程序安装时,首先由主站下发启动安装更新任务;为了确保接收电能表均能接收到完整的更新文件,由终端采用点对点方式下发该命令到电能表,电能表应答启动更新结果传给终端,终端再透传给主站,流程如图 6 所示。

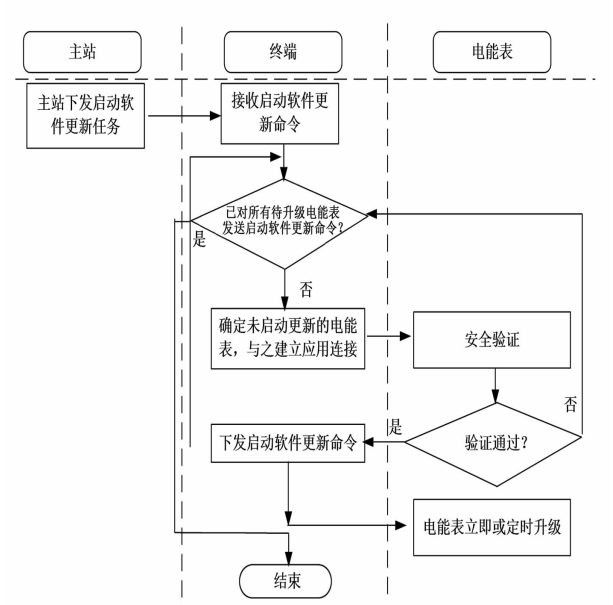

图 6　更新程序更新流程

更新任务有两种模式:一种为下载完成并校验后立即进行管理芯片程序安装的立即安装模式;另一种为通过设置时间参数进行定时更新程序安装的模式,可根据具体应用场景选择不同方式,大批量现场软件更新通常采用定时安装模式,避免更新时和重要采集任务冲突。

2　更新过程关键问题

2.1　原程序拷贝及回滚

相对于将要更新的程序,这里将电能表微处理器(MCU)内正在运行的应用程序称为当前应用程序。相对地,当前下载到外部闪存(FLASH)内、比

当前版本高一个版本、还未更新到MCU的应用程序称为待更新应用程序。

该应用程序在出厂前会烧录在电能表的管理芯内,同时还会额外下载一个同样的应用程序到电能表的外部FLASH内;更新程序更新前应将电能表内的原应用程序拷贝到MCU外部的FLASH芯片中。更新后,则将新的应用程序和外部存储芯片中的原应用程序进行功能核验。若核验不一致,则用该拷贝的程序进行回滚覆盖。若更新后有其他异常情况时,例如新应用程序频繁异常复位、复位超过门限次数,电能表自检到这种异常后也将回滚恢复至原应用程序。

2.2 更新程序的完整性及安全性核验

更新程序的软件完整性和安全性分别通过CRC校验和国标加密算法AES-128[7]保证。先对更新程序整体做循环见余校验码(cyclic redundancy check,CRC)校验。CRC校验是发送方通过对待发送数据进行多项式计算,并将计算结果附在报文中,接收方根据同一算法进行查错的数据传输检错方法。通过这种方法来保证软件的完整性和正确性。然后,根据南方电网费控电能表信息交换安全认证技术要求,再使用AES-128加密算法对包含CRC的更新程序整体进行加密,避免报文的核心数据域以及CRC被篡改。

2.3 更新相关事件记录

在电能表更新程序过程中,更新初始化事件、更新校验成功事件、更新校验失败事件、更新激活成功事件、回滚事件,每个事件都会记录相应时标及对应固件版本号便于后续的软件管理和故障分析。

3 实验验证

为验证所设计的电能表更新模式的可行性,搭建模拟测试平台进行测试,由测试主站通过该模式给61只同一厂家同一批次的费控电能表进行远程软件更新。结果显示1024 kB的应用程序更新时间为16 min左右。

在该更新程序下载过程中,由于采用分块传输,每个程序更新块大小为512 Bytes,则共需传2000块。每个更新块组帧时作为数据域,然后加上帧头、帧尾、地址等上行通讯规约定义的帧结构部件,则更新报文每条的长度为551 Bytes。采用窄带载波方式以1200 bit/s速率传输。实测通信传输时间需要983 s,即约16 min,基本满足现场应用需求。该时间包含电能表回复帧传输时间、收发双方通信延时、电能表接收到更新块后进行存储和更新的时间。

4 结 语

所设计的电能表远程管理芯片软件的分散式更新方案,在案例测试时,观察到其更新程序下载过程中未影响电能表计量芯的正常工作。程序更新期间,峰平谷各费率的电量累积的准确性也可得到保证,电能表程序更新前后也未引起表内基本参数和底度等重要数据的改变,在测试环境中验证了其可行性。如何进一步提高该方案在发送大文件时的传输效率和稳定性,解决大批量电能表组播更新时的"广播风暴"问题,值得进一步研究。

参考文献

[1] 万忠兵,谢智,王韬. 基于本征时间尺度分解和时间序列分析的电能计量误差预测方法[J]. 电气应用,2017(2):79-84.

[2] 刘文华,梁永全,冯 政等. 基于加权均方残差的改进双聚类算法[J]. 模式识别与人工智能,2016,29(6):519-526.

[3] 陈杜琳,陈魁,张国玉. 一种针对含稀疏误差向量的线性多变量系统递归辨识算法[J]. 工业控制计算机,2016,29(11):114-116.

[4] 高金兰,康迪,雷星宇. 基于改进模糊聚类分析的电力系统不良数据辨识[J]. 电气自动化,2018,40(5):30-33.

[5] 王晶. 电力系统异常数据检测辨识方法综述[J]. 电力与能源,2015,36(6):813-817.

[6] 杨海涛,牟婷婷,杨海滔,等. 基于序列光滑性分析的集抄数据缺陷判定[J]. 电网与清洁能源,2016,32(8):73-78.

[7] 梁捷,李刚. 基于节点特征分类的配电网重构辐射约束处理法[J]. 广东电力,2016,29(8):91-95.

[8] 张瑞琴. 基于信息熵聚类的异常检测方法研究[D]. 北京:北京交通大学,2016.

[9] 梁捷. 基于禁忌动态规划的含电动汽车机组组合研究[J]. 电力工程技术,2018,37(2):67-72.

[10] 李亦非,宋玮琼,彭放,等. 基于局部异常点检测算法的电能表飞走异常智能分析[J]. 电测与仪表,2016,53(18):69-73.

作者简介:

梁 捷(1987),男,工学硕士,工程师,主要从事电能计量管理方面工作。

(收稿日期:2021-01-08)