智能电表远程升级过程中的通信安全与加密策略研究

康　宣

浙江瑞银电子有限公司 浙江 杭州 311100

【摘　要】：智能电表作为智能电网的关键终端设备，其远程升级功能在提升运维效率的同时，也引入了严峻的通信安全挑战。针对升级过程中可能存在的固件篡改、身份伪造、重放攻击及版本回滚等威胁，本文提出了一套基于端到端加密、双向身份认证、抗重播机制与防回滚保护的多层次安全策略。设计了混合加密与数字签名相结合的升级包保护方案，采用挑战－应答协议与椭圆曲线密钥交换实现双向认证及会话密钥协商，并结合时间戳、随机数与单调计数器抵御重放与回滚攻击。在此基础上，给出了安全升级协议的完整流程，分析了密钥管理、完整性校验及异常恢复等关键实现要点。研究表明，所提方案能够在有限资源条件下有效保障智能电表远程升级过程的机密性、完整性、真实性和可用性，为电力系统终端设备的安全防护提供了理论依据与技术参考。

【关键词】：智能电表；远程升级；通信安全；加密策略

DOI:10.12417/2705-0998.26.05.055

智能电表是智能电网中感知层和用户层的重要组成部分，在完成基本的计费和信息采集任务的基础上，向远方可控制、可调荷、双向通信的方向发展；由于可以远程升级固件和软件程序，供电局可以在不打扰客户的情况下补丁漏洞、增加新功能或者应对新的电费方案，因此极大降低了运维成本、缩短了响应时间。但远程升级带来的便捷是以可靠的安全通讯为前提条件。智能电表多处于户外无人值守场景，并采用无线公网、电力线载波或者射频网等多种信道与主站进行通信，在升级过程中容易形成攻击者入侵与控制的关键环节。当远程升级机制被成功突破后，攻击者可以注入非法固件实现成千上万只计量失真、窃取用户信息、对电网负载进行操纵甚至物理破坏等攻击目标。因而针对低功耗的智能电表终端提出一种能够保证安全性及效率的远程升级通信安全保护机制和安全认证方法是当前智能电网亟待解决的问题之一。为此，首先基于安全性的角度对远程升级过程中的主要潜在威胁以及攻击行为进行研究；在此基础上设计分级加解密及安全保护机制，并进一步提出安全升级协议的具体方案及其实现要点，以期对实际工程应用有所裨益。

1 面向远程升级的分层加密与安全策略设计

1.1 升级包的端到端加密与数字签名机制

针对升级包截获与篡改威胁，必须采用端到端的加密与数字签名组合机制。端到端加密确保从管理中心生成升级包到电表解密之前，升级包的明文内容不在任何中间节点暴露。从智能电表的计算能力考虑，宜采用混合加密方式：用对称加密（例如 AES-128 或 AES-256）加密升级包本体，密钥是每次升级产生的会话密钥，并用电表的公钥（比如 ECDSA 的 secp256r1 密钥）非对称加密后加在升级包头。这就既保证了大量的升级数据加密的高效性，又利用了公钥体制的密钥分配便捷性。管理中心使用自己的私钥对整个加密后的升级包（或对其哈希值）生成数字签名，电表使用管理中心预置的公钥验证签名。签名算法推荐采用基于椭圆曲线的数字签名算法，其在同等安全强度下签名长度更短，适合带宽受限的通信场景。验证通过后，电表才能进入解密与烧写流程。该机制确保任何对升级包的篡改、替换或伪造都会导致签名验证失败。

1.2 双向身份认证与会话密钥协商

为了防范伪造身份及中间人攻击，在每一次升级会话开始的时候进行双向身份认证并根据认证的结果协商本次升级用到的临时会话密钥。单向认证（只有电表认证管理中心）是无法防止中间人攻击的，攻击者在认证过程中可以冒充电表与管理中心通信。双向认证可以采取挑战－应答协议：管理中心发出一个随机数 Nonce_C 给电表；电表用自己的私钥签 Nonce_C 及其它上下文信息后发回；管理中心验证签名来确定电表的身份；同理，电表也可以对管理中心发起挑战，并验证它的签名。完成认证以后，通信双方使用已认证的公钥信息或者预先共享的密钥来协商会话密钥。推荐使用椭圆曲线迪菲-赫尔曼密钥交换协议并引入双主随机数生成密钥，保证每次升级获得新鲜的会话密钥。该会话密钥用于对后续升级包分片的加密或消息认证码计算，从而降低长期密钥在频繁升级中的暴露风险。

1.3 抗重放攻击的时间戳与随机数机制

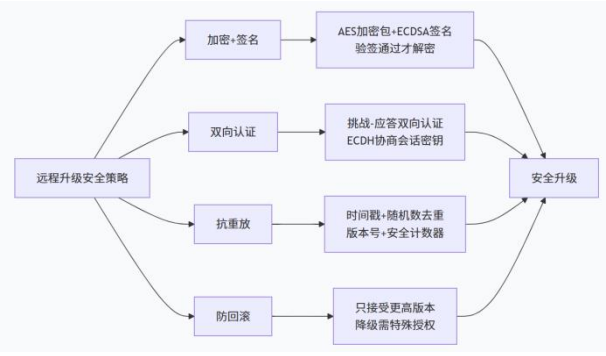
重放攻击和版本回滚攻击的共同特点是攻击者利用合法但过时的消息。抗重放的基本思路是使每条合法消息具有唯一性和时效性。具体策略包括：在每次升级请求和响应中嵌入时间戳与一次性随机数。

作者简介：康宣（1987-），女，汉族，河南商丘人，硕士，中级工程师，研究方向：智能电表的软件开发。

电表和管理中心维护一定的时间同步（可通过网络时间协议或专用的轻量级时间同步协议实现，容忍误差在几分钟内）。接收方检查时间戳是否在可接受的窗口内（例如±5 分钟），并记录最近一段时间内收到的随机数组合，拒绝任何重复的随机数对。针对版本回滚攻击，则需要升级包内明确携带版本号，同时电表需维护一个不被回滚的安全版本计数器，计数器一般存储于电表的防篡改存储区（一次性可编程存储器或者可信执行环境中单调递增的计数器）。在每次升级成功之后，电表将当前固件的版本号写入到计数器，并且此计数器是单调递增的，当升级包到来后，电表将包里的版本号同计数器进行对比，只有比之前记录的最大版本号大才能继续下去。即使旧版本包带有有效签名，也会因版本号过低而被拒绝。

1.4 安全版本管理与防回滚保护策略

防回滚保护不单是电表端简单的版本号比对，还需要一套完整的安全版本管理策略。在管理中心应该维护一份全局版本发布清单，每个版本对应它的安全等级、已知漏洞以及补丁关系；而在签发升级包的时候，在版本号之外还可以将版本链信息绑定到签名中—–例如新的版本签名中隐式或者显式的包含了上一个版本的哈希值，建立一个不可篡改的版本链。电表对新的版本进行校验的时候除了对签名进行校验之外还会校验版本链的连续性，以确保自己的版本是来自于一个合法的状态。对极端情况，比如为了处理严重功能缺陷必须从一个高版本回退到一个旧版本的情况，应该作为例外对待而不视为正常的升级。这种情况下需要采用物理或者带外的安全通道来进行授权，而且必须在管理中心以及电表两端都产生一次降级事件，降级后版本应被视为“过期和危险”。并且在下次连接的时候再进行升级。安全版本控制的一个重要原则就是：不支持降级使用任何版本，除非经过充分的安全性分析并特别批准。



2 安全升级协议设计与实现关键点

2.1 安全升级协议整体流程设计

结合以上方法，一个安全的远升协议应该包括以下几个阶段：初始化与通告阶段、双向认证与密钥协商阶段、升级包传输阶段、完整性校验与版本验证阶段、烧写与切换阶段、确认与激活阶段。管理中心先对目标电表集合进行升级通告，包括升级包大小、版本号、预期时间窗口等。电表在收到后，主动发送双向认证请求消息给管理中心进行互相认证，并协商出本次升级过程中的会话密钥。随后管理中心将加密后的升级包分片传输，每个分片附带基于会话密钥的消息认证码。电表接收完毕后，使用会话密钥解密，再使用管理中心的公钥验证升级包的全局数字签名，同时检查版本号是否高于防回滚计数器。通过所有校验后，电表将升级包写入备份存储区，验证引导加载程序的完整性，然后设置标志位并执行软复位，重新固件启动。新固件首次启动后应向管理中心发送升级成功确认；若启动失败，应自动回滚至旧固件并上报失败信息。

2.2 密钥管理与存储安全措施

密钥是整个安全系统的基石，管理中心的私钥应当保存于硬件安全模块或者同等强度的高隔离度环境当中以避免泄漏；电表端需存放管理中心的公钥、自己的设备私钥及防回滚计数器，这些关键信息应放置于电表中的安全元件或是可信的平台模块中，而不仅仅是普通的闪存或者电可擦除可编程只读存储器上。在没有硬件安全模块的低价位电表中，至少应该使用软件混淆技术和代码防篡改技术并定期更换密钥。管理中心应该定期（比如每隔 3~5 年）更换签名密钥对，并将新生成的公钥通过安全通道下发至电表中；而电表中的设备私钥则在电表出厂时就已注入电表中，在设计时可以加入远程证书更新功能来处理密钥泄露的情形。所有的密钥操作包括：签名、加密、解密、验证均采用公开验证过的密码学库进行，而不是自己实现密码算法。

2.3 升级包完整性校验与签名验证流程

完整性检验应在整个升级包接收过程中进行，而不是仅仅在传输完成之后。在分片传输方式下，在每次分片传输之后电表都应对该分片的哈希值进行计算，并将其与管理中心发送的期望哈希值相比较，或是利用基于会话密钥的消息认证码进行即时验证，以便尽早地检测出传输错误或是积极的篡改行为，防止将整个升级包丢弃只丢弃最后收到的部分，节省带宽和时间。完整的升级包装配好以后再做最后一步数字签名检查。一般会为升级包的哈希值做数字签名而不是为升级包本身做签名来提升性能。电表计算接收到的明文升级包的哈希值，使用管理中心的公钥解密签名获得预期哈希值，两者一致则验证通过。在验证通过之前，电表不得将升级包写入可执行存储区域，也不得传递给引导加载程序。任何校验失败都应触发安全日志记录，并可选择进入重试或告警状态。

2.4 异常情况下的安全降级与应急恢复

即使有这些多层防护，也有可能出现网络断开、升级包损坏、电表掉电、新的固件启动失败等情况。协议应该具备安全退化以及紧急恢复的能力。所谓安全退化就是在通信状况不好或者设备资源不够充足的时候，能够暂时降低一些非关键性的

安全校验力度，但是一定不可以丧失保密性、完整性及真伪性。比如延长时间戳窗口容忍度，但是不可以跳过签名认证。应急恢复要求电表保存一个最小的、只读的安全引导加载程序，并能从网络或者本地接口载入有签名的紧急恢复固件，这个引导加载程序是独立于主固件的。在主固件不能启动或者校验的时候，安全引导加载程序会接管并进入恢复模式。恢复模式下通信的安全性要求不低于正常的升级，同需身份验证及加密传送。同时管理中心应可远程触发单个或批量电表进入恢复模式，用于大规模升级事故。

3 结论

智能电表远程升级的安全性是智能电网终端安全管理的重要组成部分。本文基于安全需求对升级包截获篡改、身份伪造及中间人攻击、重放和版本回滚、拒绝服务等典型的攻击模型进行了分析，并讨论其带来的危害，在此基础上提出了分层加密与安全策略设计方案，支持端对端加密及数字签名、双因子身份认证及会话密钥交换、基于时间戳与随机数的反重放攻击、安全版本控制与防回退等。

在此基础上，本文给出整体的安全升级协议流程并提出密钥管理、完整性校验、异常恢复等方面的关键实现方法；研究结果表明：在密码技术和协议设计相结合的基础上可以在有限资源条件下保障智能电表的远程升级安全，在机密性、完整性、真实性和可用性方面满足需求。后续的工作还包括：将轻量级密码算法应用于更低价格的电表上、使用区块链技术实现升级包的分发及审计、使用人工智能对升级过程进行异常行为分析等。

参考文献：

[1] 王傲.基于 DLMS__COSEM 的多功能智能电表设计[D].山东科技大学,2022.

[2] 张法瑞.基于指纹解锁的电动汽车交流充电桩设计[D].山东大学,2019.

[3] 吕德勇.基于 STM32 的单相智能电能表设计[D].青岛大学,2019.

[4] 邵氢海.基于 IEC62056 的三相智能电表设计与实现[D].湖南大学,2012.