用电采集终端数据安全加密技术的研发与测试分析

郝士军
科大智能科技股份有限公司南京分公司　江苏南京　210000

摘　要：对于用电采集终端数据传输与存储过程中的安全隐患，依托终端内置加密芯片，通过适配优化加密算法应用、完善密钥管理机制，可以实现对整个数据采集、传输和存储的过程加密保护。经过测试可以发现能够抵抗篡改、重放等常见攻击，加解密延迟小于 50ms，CPU 占用率不超过 8%，功耗增加不超过 3%，满足用电采集终端低功耗实时性及硬件适配需求，可以为用电采集终端的数据安全提供保障，支撑智能电网末端数据安全防护体系建设。

关键词：用电采集终端；数据安全；内置加密芯片

1 用电采集终端数据安全现状与需求

1.1 数据安全现状

用电采集终端数据流转涉及采集、传输、存储等多个环节。数据采集软件运行于采集终端，采用模块化设计方法。通信模块主要负责电能表通信，并使用相应的通信协议完成数据传送；数据处理模块负责对采集到的数据进行检验、分析和处理；数据存储模块向数据采集终端的局部存储器存储所处理的数据。但在数据传输环节中，终端与电能表和采集主站通过电力线载波、无线通信等方式连接起来，信道开放导致数据容易被监听窃取 [1]。在存储环节中，终端本地存储以及云端存储的用户用电明细、设备密钥这些敏感信息都有可能遭受非法访问。用电采集终端加密安全这块比较特殊，实际的加解密算法都内置在加密芯片里，终端只要正确调用相关指令与加密芯片交互就可以，终端数据安全防护情况十分严峻。

1.2 安全需求分析

数据机密性需求要求保证终端采集到的原始数据、传输过程中的中间数据以及存储的数据不被非法获取，完整性需求要求在采集、传输、存储的过程中数据不能被篡改，具体可以通过校验机制快速发现异常数据。抗攻击需求要求抵抗篡改、重放、伪造等常见的攻击行为，并且能够抵御内部权限滥用带来的风险。从用户需求角度分析，用户管理模块负责管理、维护用户信息；用电信息查询模块支持用户查询自身用电情况；电费核算模块根据用户所用电量及电价计算具体电费；线损分析模块可对线路损耗进行分析与计算；负荷预测模块利用历史数据预测未来电力负荷。考虑用电采集终端部署于室外容易遭受物理攻击以及数据被篡改等威胁，将其加密算法集成于加密芯片内，以降低软件方面的攻击途径，加密芯片需要支持使用 AES 加密算法，保证用户信息、设备状态的安全，虽然也有部分软件加密，但是仍然存在数据的完整性以及数据的身份验证问题。其 SM3 哈希算法，可以在传输过程中保证数据的完整性，一旦篡改会使哈希值发生变化，通过再次比对保证数据的一致性，能保证数据被篡改之后能及时得到更正。

2 用电采集终端数据安全加密技术研发

2.1 加密算法选型与优化

在用电采集终端数据安全加密技术的研发过程中，应重视加密算法的选择以及优化。用电采集终端可应用于智能电网、智能计量及电力监控等领域，其涉及数据包的内容包括用户的用电信息、设备的状态、传输的命令等，这些数据的安全直接决定了系统的安全和用户的信息安全，而合理地选择加密算法能保证用电采集终端数据的安全性。

由于 AES（高级加密标准）算法用于实现实时数据传输时的数据加解密，能保证数据在网络中处于安全状态，因此被广泛应用。RSA 算法仅适用于初始密钥交换环节的密钥保护，保障初始密钥传输的安全性，将 RSA 进行公钥加密、私钥解密，以防止密钥泄露，也可用于产生数字签名，以判定数据源的真实性和保证数据完整性 [2]。即通过 RSA 传递密钥以产生会话密钥，然后运用 AES 算法完成后续数据加解密，保证数据安全性，使系统效率明显提高。目前，大多数的用电采集终端均采用带有硬件加速的安全模块（TPM 或 FPGA），所以针对其采用并行化处理技术，使用多核处

理器实现 AES 和 RSA 的计算加速，进一步提升加密性能。

2.2 密钥管理体系设计

为保障用电采集终端数据安全，构建以三级密钥（主密钥、设备密钥、会话密钥）为基础的密钥管理体系，主密钥是体系中最核心的密钥，基于 GM/T0005 的 HSECRNG 算法生成密钥，长度为 256bit，并且此主密钥保存在嵌入式硬件安全模块内部，具有不可拆焊及不可破解的特点，在任何情况下终端硬件如果被破坏，都无法拿到主密钥。设备密钥是由 HKDF 密钥派生函数从主密钥通过终端唯一 ID 和生产批号相结合而成，实现“一机一密”的硬件绑定机制。设备密钥在采用 AES-XTS 加密方式后被存放在终端闪存内，且只有密钥保护模块才能对设备密钥进行解密访问操作，不可以私自破解获取设备密钥。同时，采集主站在集中统一管理分发的前提下，使用正确密钥同采集终端的加密芯片进行对接和验证，包括对接口的状态信息、随机数、MAC 校验值及从中主站各种明文 / 密文报文等解析处理。

2.3 数据传输与存储加密实现

在用电采集终端中，针对不同的通信场景进行数据传输加密的定制化适配。以电力线载波通信为例，在信道噪声较大、带宽受限的情况下，可以通过优化加密适配层的帧结构设计，将加密数据与通信控制字段分离，使该分离模式既可以完成加解密认证的功能，又能减少消息校验开销，将帧长压缩为 512 字节左右，降低延时及丢包率 [3]。数据处理软件以服务器集群为核心，运行于数据处理层，主要完成数据处理、存储、分析等功能。数据处理软件采用 Hadoop、park 等计算架构，以实现数据在不同节点间的并行处理。数据存储加密可以实现“全链路覆盖”，终端本地存储的数据采用透明数据加密，基于文件系统的加密，对文件进行自动加密操作，在写入时采用会话密钥加密，不用改动原来的业务逻辑，采用加密存储以及校验冗余的方式，保证数据不被篡改。

下行采集电表时，可以明文加随机数抄读，返回明文 +MAC，也可密文采集，此时需要下发电表密钥（密文）。终端根据密钥信息生成可识别报文发送到电表，电表收到后解密回复表计数据，表计再重新加签后发回终端，终端再次加签后发往主站。上行时，主站采用不同等级的加密模式，终端则回应相应的加密等级，确保数据传输的安全性和完整性。

3 用电采集终端加密技术测试分析

3.1 测试环境搭建

测试环境尽量模拟用电采集终端的使用场景，选用主流型号的终端硬件进行选型。采集终端用的硬件要求是 专变采集终端（Ⅰ型、ⅢⅢ型），CPU 主频不低于 1GHz，不低于 4 核，内存不低于 1GB，数据存储器不低于 8GB，运行同实际用电采集终端相符的嵌入式系统 FreeRTOS V10.4.3，系统的安全加固已落实，实现进程隔离、端口禁用以及安全启动，启动阶段对引导程序、内核及关键系统文件开展完整性检测并记录日志。终端搭载着国家密码管理局所认可的安全芯片及 ESAM 模块，融入经裁剪适配的 Crypto++8.8 加密算法库，实现密钥安全生成、留存及业务数据加密运作，安全芯片硬件隔离区作为密钥的存储处，达到 Q/GDW 377—2009 电力用户用电信息采集系统安全防护技术准则。装有 SX1278 4G/5G 通信模块连同电力线载波模块，切实遵照 DL/T645-2007《多功能电能表通信协议》，可兼容 Q/GDW 10376 系列通信标准，电力线载波信道数据传输的错误率最大为 10-5，准许在标准帧扩展域添加加密标识、Ⅳ和完整性校验字段，维持原有帧结构的完整性。本地数据存储采用分区加密手段，采集数据、事件记录等敏感信息加密处理后留存，失电情况下数据可存续 10 年，可达成不可篡改的安全审计日志留存，日志至少保存 7 天，支持主站远程调取。

控制中心服务器装配 Intel Core i5-12500 处理器、16GB DDR4 内存连同 512GB SSD，采用 Ubuntu22.04LTS 操作系统，采用 MySQL8.0 作为数据库且开启透明数据加密，协同搭建轻量密钥管理系统，为每个终端配置独特加密密钥。服务器与终端采用密码技术进行身份审定，业务交互数据借密文形式传递，具备对终端上传数据的完整性验证与合法性甄别能力，契合用电信息采集系统安全防护相关标准。

构建电力线载波与 4G/5G 无线双场景通信体系，采用 PL-1000 型电力线信道模拟器，电力线载波场景生成不同噪声环境，信噪比的取值范围是 10dB 到 30dB。4G/5G 情形依靠 4G/5G 信道模拟器对不同信号强度、网络干扰及移动场景进行模拟，涉及实际实施中的信号衰减、切换等状态，测试终端选定为专变采集终端，硬件配置合乎 Q/GDW10374.1—2019 规范规定，即 CPU 主频达 1GHz 及以上、核心数 4 核及以上，内存容量至少 1GB，数据存储空间达 8GB 及以上。

借助 Wireshark4.0.8 进行通信数据包采集与分析，

LoadRunner12.57 造就高并发情形，可达到 1000 台终端的并发上限。采用 openssl speed 衡量加密算法速率，keysight N6705B 功率分析仪评估终端能耗水平，依托国家信息安全测评中心渗透测试工具集开展安全防护校验。测试数据集选取某地区实际用电采集数据，含有电压 220V ± 10%、电流 0~60A、用电量 0.01kWh~100kWh 的参数情况，数据量依据 1KB、2KB、3KB、5KB、7KB、10KB 划分层级，对应着不同采集周期的数据收集需求。

3.2 终端数据抄读与存储的测试

功能测试主要是针对加密技术的机密性、完整性、抗攻击以及兼容性的测试。机密性测试中，使用 Wireshark 抓取通信数据，未发现明文，并且解密需要正确的密钥才能恢复数据。完整性测试中对传输的数据进行人为篡改，终端和接收端都可以通过消息认证码准确地识别出异常数据，识别率可以达到 100%。抗攻击测试中模拟重放攻击发送历史通信数据包，终端通过时间戳验证，拒绝处理该数据包。模拟篡改攻击，修改数据字段，完整性校验机制能够有效拦截。兼容性测试中重点测试加密方案与终端内置加密芯片的适配性，不存在兼容性问题。

3.3 功能稳定性测试

性能测试主要考察加密技术对终端运行的影响，如加解密延迟、CPU 占用率和功耗消耗。从实验结果中可以看出，AES–256 算法对于 1KB 数据的加密延迟为 12ms，解密的延迟为 8ms。SM2 算法密钥协商的延迟为 35ms，混合加密模式下，对于 1KB 的数据传输加密总延迟为 42ms。当终端运行加密技术时，其 CPU 平均占用率为 6.2%，最大不超过 8%。功耗相较于未开启加密的情况下增加了 3%，在终端功耗允许范围内。在不同大小的数据量下的加解密延时如下表所示：

表 1 不同数据量下加解密延迟测试结果

数据量（KB）	加密延迟（ms）	解密延迟（ms）
1	12	8
3	18	13
5	29	22
10	45	38

加解密延迟随着数据量的增长呈现线性增长趋势，但都在 50ms 以内，可以满足终端实时的数据传输需求。CPU 占用率测试显示，终端连续对数据进行加密处理时，CPU 的占用率为 4%—8%，不会影响终端其他功能模块的工作。

3.4 安全性测试

为确保用电采集终端安全，首先使用攻防法全面性测试，由第三方安全机构进行渗透测试、密钥破解、算法攻击及协议漏洞检测等工作。经测试，未发现安全隐患，再应用加密技术，可以有效防御一般暴力破解、字典攻击，密钥被破解的难度极大，终端达到了国家信息安全等级保护三级标准。再进行长期稳定性测试，终端连续运行 30 天，均稳定运行加密技术，无加密失效现象，无性能下降问题。接下来进行硬件安全、合规性专项核验。通过对终端内嵌安全芯片和 ESAM 模块密钥生成、密钥存储功能的测试和对硬件隔离区防止密钥被物理接触窃取的测试、暴力拆解测试（对于测试过程中将终端软件和 PC 机硬件并列摆放的情况来说，在这些外加施力作用下仍然无法取得终端主密钥）以及对硬件在线监测审计的安全在线监测审计功能（包括以太网远程端口开放、USB 非法接入、关键目录文件发生变化等 13 种场景）测试来判定终端的安全情况。模拟异常操作，终端会立刻生成事件并报送至主站，其生成的审计日志完整且不可篡改，符合安全审计留档的要求。

4 结束语

研发的用电采集终端数据安全加密技术，根据终端内置加密芯片特性提升混合加密架构、分级密钥管理及全流程加密方案，在解决终端数据安全性问题的同时也解决了资源约束的问题。测试结果表明，其具有良好的机密性、完整性和抗攻击能力，并且加解密延迟和 CPU 占用率等性能满足终端运行需求，同时与现有系统的兼容性良好，可以明显提高用电采集终端的数据安全防护水平，为智能电网末端数据安全提供技术支持。

参考文献：

[1] 李文慧 . 基于联邦学习的智能电网负载预测模型的研究与实现 [D]. 盐城工学院 ,2025.

[2] 吴盼 , 杨洋 . 智能电网数据安全防护策略研究 [J]. 信息与电脑 ,2024,36(24):63–65.

[3] 李新阳 . 智能电网数据安全共享及隐私保护技术研究 [D]. 桂林电子科技大学 ,2024.