电力监控系统主动防御中数据加密技术的应用研究

张磊 杨伟 张庆 王兵 王宇峰

新疆华电苇湖梁新能源有限公司，新疆省乌鲁木齐市，830000；

摘要：随着电力系统向智能化、网络化方向深度发展，电力监控系统作为保障电网安全稳定运行的核心基础设施，面临的网络安全威胁日益复杂。主动防御作为应对威胁的关键策略，而数据加密技术则是主动防御体系中的核心技术支撑。本文围绕电力监控系统的业务特性与安全需求，首先分析了当前系统面临的主要安全风险及主动防御的重要性，随后探讨了对称加密、非对称加密、哈希算法等主流数据加密技术在电力监控系统数据采集、传输、存储等关键环节的适配性与应用方式，最后针对加密技术应用过程中存在的性能损耗、密钥管理、兼容性等问题提出优化对策，旨在为提升电力监控系统主动防御能力提供技术参考。

关键词：数据加密；网络安全；密钥管理

DOI：10.69979/3060-8767.25.12.006

1 引言

电力工业作为国家能源安全的重要支柱，其稳定运行直接关系到社会经济发展与民生保障。近年来，智能电网建设推动电力监控系统从传统的本地化、封闭式架构，逐步向网络化、开放式架构转型，SCADA（监控与数据采集系统）、EMS（能量管理系统）、DCS（分散控制系统）等核心系统与外部网络的交互日益频繁，这使得系统面临的网络安全威胁从传统的物理攻击、局部故障，扩展到恶意代码注入、数据篡改、中间人攻击等新型网络攻击。

传统的被动防御策略，如防火墙、入侵检测系统等，仅能在威胁发生后进行响应，难以应对提前潜伏、持续渗透的高级威胁。主动防御理念强调在威胁发生前通过技术手段构建安全屏障，从源头降低风险，而数据作为电力监控系统的核心资产，其完整性、机密性、可用性直接决定系统的安全水平。数据加密技术通过对敏感数据进行数学变换，将明文转化为不可直接解读的密文，能够在数据全生命周期内提供安全保护，成为电力监控系统主动防御体系中的关键技术环节。因此，研究数据加密技术在电力监控系统主动防御中的应用，对保障智能电网安全稳定运行具有重要的理论与实践意义。

2 电力监控系统的安全风险与主动防御需求

2.1 电力监控系统的主要安全风险

电力监控系统的安全风险贯穿于数据采集、传输、存储、应用全流程，具体可分为以下三类：

一是数据采集环节的完整性风险。数据采集终端（如 RTU、智能电表、传感器）直接与电网设备连接，若终端被劫持或篡改，采集到的电压、电流、功率等关键运行数据可能被恶意修改，导致监控中心做出错误决策，引发电网负荷失衡、设备过载等故障。

二是数据传输环节的机密性风险。电力监控系统的数据传输多依赖电力调度数据网、无线专网等网络，部分传统传输协议（如 IEC60870-5-101/104）未内置加密机制，数据以明文形式传输，易被攻击者窃听或拦截，导致电网运行状态、调度指令等敏感信息泄露，甚至被篡改后发起虚假调度。

三是数据存储环节的可用性风险。监控系统的历史运行数据、设备参数、调度日志等数据多存储于数据库服务器中，若数据库被入侵或遭受勒索攻击，数据可能被删除、加密或篡改，不仅影响电网运行分析与故障溯源，还可能导致系统瘫痪。

2.2 主动防御的核心需求

主动防御的核心目标是“提前预防、主动阻断”，针对电力监控系统的安全风险，其主动防御需求主要体现在三个方面：

首先是数据全生命周期保护需求。需从数据产生之初即建立安全防护机制，确保数据在采集、传输、存储、使用过程中始终处于安全状态，避免因某一环节的防护缺失导致整体安全防线失效。

其次是最小性能损耗需求。电力监控系统对实时性要求极高，如调度指令的传输延迟需控制在毫秒级，因

此主动防御技术需在保障安全的同时，尽可能降低对系统运行效率的影响，避免因加密运算导致数据处理延迟、指令响应缓慢等问题。

最后是兼容性与可扩展性需求。电力监控系统包含不同厂商、不同年代的设备与软件，主动防御技术需兼容现有系统架构，同时具备可扩展性，能够适应未来智能电网对边缘计算、云计算等新技术的融合需求。

3 数据加密技术在电力监控系统主动防御中的应用

数据加密技术按密钥类型可分为对称加密、非对称加密、哈希算法三类，需根据电力监控系统不同环节的安全与性能需求适配应用。

3.1 对称加密技术在数据传输与采集环节的应用

对称加密以相同密钥加解密，具有速度快、开销小的优势，适用于实时性高、数据量大的场景。在数据采集环节，采集终端与区域监控站通过安全通道协商密钥，终端用 AES-128 算法加密电网数据后传输，监控站解密获取明文，既保障完整性，又适配 RTU、智能传感器等计算能力有限的设备。在数据传输环节，SCADA 系统与调度中心通过 IPSecVPN 协议构建通道，以 AES-256 算法加密数据包，结合 ESP 协议防重放、保完整，其长密钥抗暴力破解，硬件实现可降低性能消耗，满足调度指令实时性要求。

3.2 非对称加密技术在密钥协商与身份认证环节的应用

非对称加密采用公钥（公开）与私钥（专属）体系，安全性高且无需预共享密钥。密钥协商时，调度中心生成 RSA 密钥对，将公钥发送至区域监控站；监控站生成 AES 密钥后，用公钥加密传输，调度中心私钥解密，兼顾安全与实时。身份认证中，运维人员终端生成 RSA 密钥对，公钥预注册；登录时终端对请求信息哈希得摘要，私钥加密生成签名；系统用公钥解密摘要并重新哈希，比对一致则认证通过，防止身份篡改。

3.3 哈希算法在数据完整性校验与日志保护环节的应用

哈希算法可将任意数据转为固定长度哈希值，具有单向性与抗碰撞性。数据校验时，智能电表对用电数据 SHA-256 运算得哈希值，与数据一同传输；监控站重新运算比对，一致则数据未篡改，否则触发告警，且算法开销低。日志保护中，数据库服务器对每条操作日志生成 SHA-3 哈希值，采用链式存储（前一条哈希值参与下一条运算），篡改需重构后续所有哈希值，难度极大；定期离线备份哈希值，进一步保障日志完整可用。

4 数据加密技术应用中的问题与优化对策

4.1 主要应用问题

尽管数据加密技术在电力监控系统主动防御中具有显著优势，但在实际应用过程中仍面临以下问题：

一是性能损耗问题。加密与解密运算需要消耗 CPU、内存等计算资源，尤其在数据量较大、实时性要求高的场景（如电网故障时的海量数据传输），加密运算可能导致数据处理延迟增加，影响系统的实时响应能力。例如，部分老旧的 RTU 设备计算能力有限，运行 AES-256 算法时可能出现数据缓存积压，导致监控中心无法实时获取电网运行状态。

二是密钥管理问题。密钥是数据加密技术的核心，若密钥丢失、泄露或被窃取，加密数据将面临安全风险。电力监控系统包含大量终端设备与服务器，密钥数量庞大，且部分设备部署在偏远地区，密钥的生成、分发、更新、销毁等管理环节难度较大；同时，若密钥管理系统被入侵，可能导致全局密钥泄露，引发系统性安全风险。

三是系统兼容性问题。电力监控系统中部分早期设备与软件仅支持传统的加密算法（如 DES、3DES），无法兼容 AES、SHA-256 等新型加密算法；此外，不同厂商的设备采用的加密协议与密钥格式存在差异，导致跨厂商设备之间的加密通信难以实现，形成“安全孤岛”。

4.2 优化对策

针对上述问题，结合电力监控系统的特性，可从以下三个方面提出优化对策：

一是基于硬件加速的性能优化。为降低加密运算对系统性能的影响，可采用硬件加密方式替代软件加密。例如，在数据传输网关、服务器中部署专用加密芯片（如国密 SM 系列芯片），通过硬件电路实现 AES、RSA 等算法的并行运算，大幅提升加密速度；对于计算能力有限的终端设备（如智能传感器），可采用轻量化加密算法（如 AES-128 的简化版本、SM4 算法），在保障基本安全的前提下，减少运算开销。同时，可通过数据分类加

密策略，对关键数据（如调度指令、故障数据）采用高强度加密，对非关键数据（如设备状态查询数据）采用轻量化加密或不加密，实现安全性与实时性的平衡。

二是基于分层密钥管理的安全优化。构建分层密钥管理体系，实现密钥的精细化管理。可将密钥分为根密钥、设备密钥、会话密钥三级：根密钥存储于离线的硬件安全模块（HSM）中，用于生成与保护设备密钥；设备密钥由根密钥派生，存储于设备的安全存储区域，用于生成会话密钥；会话密钥由设备密钥动态生成，仅在单次通信会话中有效，会话结束后立即销毁。这种分层结构能够降低单一密钥泄露的影响范围，同时通过 HSM 保障根密钥的绝对安全；此外，可引入密钥自动更新机制，通过远程安全通道定期为设备更新密钥，避免密钥长期使用导致的安全风险。

三是基于协议适配的兼容性优化。针对不同设备的兼容性问题，可构建“协议转换网关+加密适配层”的架构：协议转换网关部署在不同厂商设备的通信节点，支持将传统协议（如 IEC60870-5-101）转换为支持加密功能的标准协议（如 IEC62351）；加密适配层提供多种加密算法的接口，可根据设备支持的算法类型自动选择适配的加密方式，实现跨厂商设备的加密通信。同时，在系统升级改造过程中，应优先选用支持国密算法（如 SM2、SM3、SM4）的设备，推动加密技术的标准化与国产化，降低对国外算法的依赖，提升系统的自主可控能力。

5 结论与展望

本文围绕电力监控系统主动防御需求，研究了数据加密技术在系统中的应用方式，得出以下结论：对称加密技术因高效性适用于数据采集与传输环节，非对称加密技术因安全性适用于密钥协商与身份认证环节，哈希算法因抗篡改特性适用于数据完整性校验与日志保护环节；三种技术的协同应用能够构建覆盖数据全生命周期的主动防御体系，有效提升系统的安全防护能力。同时，针对技术应用中的性能、密钥管理、兼容性问题，提出的硬件加速、分层密钥管理、协议适配等优化对策，可为实际工程应用提供参考。

未来，随着电力监控系统与边缘计算、人工智能等技术的深度融合，数据加密技术的应用将面临新的挑战与机遇：一方面，边缘设备的分布式部署将增加密钥管理的复杂度，需研究分布式密钥管理技术；另一方面，人工智能技术可用于加密算法的动态优化，根据系统运行状态与威胁等级自动调整加密策略，实现“自适应加密”。此外，量子计算技术的发展可能对传统加密算法构成威胁，研究抗量子加密算法在电力监控系统中的应用，将成为未来的重要研究方向。

参考文献

[1]王龙.突破主动防御的网络远程监控系统的研究与设计[J].2010.

[2]张浩,温永亮,孙长春,等.电力监控系统网络安全主动防御研究[J].电气传动自动化,2023,45(4):65-68.

[3]张展阳.系统监控主动防御[J].网络运维与管理,2014(19):1.

[4]吴坡,王丹,宫灿锋,等.面向渗透过程的电力监控系统网络安全防护[J].电力安全技术,2020.

[5]赵迪.电力信息化行业网络安全主动防御技术探讨[J].轻松学电脑,2019.