

智能电网电力通信数据传输加密防护技术应用

裴金刚 高晨博 杨明飞 金鑫 方超 葛文洁

甘肃同兴智能科技发展有限公司 甘肃 兰州 730050

摘要: 智能电网通信网络具备开放化、动态化、高实时性的运行特点,海量电力数据在交互传输过程中容易遭受各类网络威胁,数据安全防护压力持续增大。本文梳理智能电网电力通信的传输特征与安全防护诉求,系统剖析各类主流加密技术的运行原理与适用场景,结合电网调度、设备运维、用户用电及分布式接入等通信场景的防护要点,从算法轻量化、全链路防护、动态适配及系统融合多个层面完善防护体系,有效提升电力通信数据传输的安全防护能力与运行稳定性。

关键词: 智能电网; 电力通信; 数据传输; 加密技术; 安全防护

引言: 电力通信是智能电网实现数据交互、调度管控与设备运维的核心支撑,网络架构的开放升级与终端接入规模的拓展,让电网数据传输环境愈发复杂。多样化的网络攻击与数据篡改隐患,持续威胁电力数据的保密性与完整性,对电网安全稳定运行形成制约。各类加密防护技术可从数据传输层面构筑安全屏障,适配不同类型电力数据的防护需求。依托通信传输的实际运行特征完善加密防护模式,能够有效规避数据传输隐患,保障电网各类业务平稳开展。

1 智能电网电力通信传输基础特征与防护需求

1.1 智能电网电力通信传输运行特点

智能电网依托网络化、智能化的全新架构完成电力系统的整体调度与运行,电力通信作为数据交互的核心载体,承载电网各类信息的传递工作。电网运行过程中持续产生海量信息,涵盖设备运行状态数据、系统调度指令数据、终端用户用电数据等多种类别,不同数据对应专属的传输形式与承载载体。电力通信网络具备多点接入、双向交互、实时传输的运行属性,能够支撑电网各层级节点之间的信息互通,满足动态调度、设备监测、状态反馈等多项业务的运转需求。电力通信传输链路拥有层级化的结构特征,整体架构分工明确、衔接紧密^[1]。不同作业场景的传输模式存在明显区别,主干网络侧重大批量数据的稳定输送,终端支路侧重零散数据的高频交互,差异化的运行模式构成智能电网通信系统的基本运行形态。

1.2 电力通信数据传输安全风险特征

智能电网打破传统电网封闭独立的运行模式,通信网络具备开放接入的运行特性,大量终端设备的接入拓

展数据传输范围,也让通信链路暴露在复杂的网络环境中,滋生各类安全隐患。数据在通信链路传输的全过程中,会面临多种类型的安全威胁。外部网络攻击可利用通信漏洞完成信息窃取,恶意网络行为能够篡改传输数据内容,链路环境的不稳定因素也会对数据传输进程形成干扰。网络边界管控不严、接入终端管控松散、传输协议存在缺陷,都是各类安全风险的主要诱发原因。电网通信需要保持全天候不间断运行,风险隐患一旦出现在局部链路,会顺着网络节点持续蔓延扩散,引发通信拥堵、数据错乱、信息中断等链路异常问题,影响电网通信体系的稳定运行。

1.3 数据传输加密防护的适配要求

智能电网通信体系对数据传输的实时性、稳定性与保密性具备严格标准,加密防护技术的应用需要贴合电网实际运行工况与传输规范。加密体系建设需要平衡防护能力与传输效率,避免防护操作拖累数据交互节奏,适配电网大容量、高频次的数据传输场景。加密防护需要覆盖数据发送、链路传输、终端接收的完整流程,构建全链条防护体系,杜绝单一环节产生防护漏洞。不同电力数据具备差异化的保密等级,加密防护方式需要结合数据属性灵活调整,适配多样化的防护标准。规范完善的加密布设模式,可以持续维护数据传输完整性,稳固电网通信的安全运行基础。

2 智能电网电力通信用数据传输加密防护技术

2.1 对称加密传输防护技术

对称加密技术依靠单一密钥完成数据加密与解密操作,运行机制简洁清晰。数据发送端通过专属密钥将明文数据转化为不可直接读取的密文,接收端利用相同密

钥完成解码还原,获取完整原始信息。该技术运算逻辑简单,资源消耗更少,能够处理电网海量数据的加密传输任务。密钥配置完成后,加密、传输、解密流程可自动推进,整体运行效率突出。电力通信业务普遍对传输时效要求较高,对称加密的快速运算优势可以适配电网高实时性的通信场景,满足常规电力数据安全、快速传输的实际需求^[2]。

2.2 非对称加密传输防护技术

非对称加密技术采用相互匹配的双密钥机制,公开密钥用于数据加密处理,私有密钥由接收方专属保管并用于数据解密。公开密钥可对外分发,能够完成原始数据的保密转换,私有密钥具备唯一性,可保障密文解密的专属权限。这套运行模式同时实现数据保密传输与身份核验,阻挡非法主体接入与数据窃取行为。双密钥架构相比单一密钥模式防护等级更高,可搭建更为严谨的传输防护体系。密钥配对验证过程可以识别数据传输中的异常改动,有效保障电力数据完整可信,适配高保密电力业务的传输场景。

2.3 哈希加密校验防护技术

哈希加密依托专属算法对原始数据进行运算处理,生成固定长度的唯一性数据摘要。原始数据内容发生任意改动,对应摘要内容都会出现明显变化,技术特性可用于精准判别数据完整性。电力数据正式传输前,系统生成初始摘要并留存备份。数据完成传输后,终端重新计算摘要信息,通过前后比对判断数据是否存在篡改、缺失等问题。技术核心作用集中在数据校验层面,运算轻便、响应快速,适配电网碎片化、阶段性的数据传输工况,精准识别细微数据异常,为电力通信数据真实性提供可靠技术支撑。

2.4 混合加密协同防护技术

单一加密技术存在应用局限,无法完全适配智能电网复杂多样的通信传输场景。混合加密技术整合多种加密手段的技术优势,形成互补式防护架构,弥补单一技术的应用短板。整体流程分工清晰,利用对称加密完成海量电力数据的高效加密传输,依托非对称加密实现密钥安全传递与身份认证,配合哈希加密完成全流程数据完整性校验。多种技术协同配合,搭建加密、传输、校验、解密一体化的防护链路。复合型防护模式可适配不同体量、不同保密等级的电力数据传输需求,贴合多变的电网通信工况,稳步提升数据传输安全层级。

3 加密防护技术在智能电网通信传输中的应用场景

3.1 电网调度数据传输加密应用

电网调度数据涵盖系统运行参数、调度操控指令、负荷调节信息等关键内容,这类数据的传输质量直接影响电网整体运行秩序。需要针对调度业务专属的传输场景布设适配性更强的加密防护机制,匹配调度数据高精度、高保密的传输标准。对调度数据双向交互的全流程进行标准化加密处理,严格规范数据发送、链路传递与终端接收的各环节操作模式。加密体系可以阻挡外部非法访问与恶意篡改行为,守住调度信息的保密属性与完整状态。稳定可靠的加密防护模式可以维持调度通信链路的运行秩序,规避数据错乱、信息缺失等传输问题引发的调度偏差,为电网精准调控、平稳运行提供基础支撑^[3]。

3.2 电网运维数据传输加密应用

智能电网常态化运维工作依托大量设备监测数据、状态反馈数据、故障告警数据开展,各类运维数据构成设备状态研判与检修决策的核心依据。需要针对运维数据的传输特征落实对应的加密防护处理,覆盖设备状态采集、在线监测、故障信息反馈等全部业务场景。所有设备监测参数与运维交互信息都需要纳入加密传输范围,阻断传输链路中各类干扰与攻击行为,减少数据异常变动的出现概率。规范的加密防护手段可以维持运维数据的原始状态,保障数据传输过程的稳定程度,让运维工作能够依托真实有效的数据开展,提升电网设备运维管理的规范性与精准程度。

3.3 用户用电数据传输加密应用

智能电网终端体系覆盖海量用户设备,日常运行中会持续产生用电计量、用电行为、终端状态等海量隐私数据,通过智能电表完成采集与上传交互。需要针对用户侧数据交互场景搭建完善的加密传输体系,重塑终端与平台之间的数据交互规范。对全部用电采集数据进行专业化加密处理,严格约束终端数据上传、后台平台接收的整套加密流程,杜绝网络漏洞造成的隐私外泄问题。加密防护可以隔绝外部非法窃取与数据窥探行为,维持用户用电数据的私密状态,筑牢电力用户数据安全的防护屏障,保障用户侧通信交互的安全稳定。

3.4 分布式电网接入数据加密应用

新能源体系不断完善的背景下,分布式电源、储能装置、微电网设备的接入规模持续扩大,多类型终端设备形成繁杂的网络交互节点。这类接入场景的数据交互节点分散、传输形式多样,通信结构具备较强复杂性。需要结合分布式电网的接入特征优化加密防护布设形式,匹配多终端、多节点的数据交互特点。选用轻量化、高适配的加密机制完成多源数据的加密处理,降

低复杂节点交互过程中的安全隐患。针对性的加密模式可以适配分布式电网多变的通信交互模式,保障各类接入数据在传输链路中的安全状态,支撑分布式电网规模化、规范化接入运行。

4 智能电网通信数据加密防护体系优化方向

4.1 加密算法轻量化优化

智能电网终端规模庞大,数据交互频次高、传输总量大,传统加密算法步骤冗余、运算复杂,对设备算力要求偏高,难以适配基层终端的硬件条件。对传统算法开展结构精简,剔除无效运算环节,简化核心加密逻辑,可以降低终端设备的资源消耗。通过合理调整参数配置,平衡加密安全强度与数据传输速率,在保证防护能力的基础上提升加密运算效率。优化后的轻量化算法可以适配电网高频次、高实时性的通信需求,契合终端设备有限的运行算力条件^[4]。

4.2 全链路加密防护体系完善

电力通信数据传输涵盖终端接入、链路传输、平台接收多个关键环节,传统防护模式多聚焦单一环节,存在明显的防护短板与安全漏洞。需要立足数据传输全流程,排查并补齐各阶段防护薄弱点,搭建贯通完整传输链条的加密防护架构。打破局部防护的局限性,构建全方位、无死角的加密防护链路,杜绝单点防护失效引发的整体安全隐患。统一各个传输环节的加密处理规范与技术标准,规整不同节点的防护模式,消除各环节防护差异带来的体系漏洞,有效提升电力通信加密防护体系的完整性与统一性。

4.3 动态加密适配机制升级

智能电网通信场景具备动态多变的特征,不同传输场景、不同类型数据的防护需求存在明显区别。固定单一的加密模式无法适配差异化的防护标准,难以适配复杂多变的电网通信工况。依托场景变化规律与数据属性特征,搭建可自主调整的动态加密防护机制。依据电力数据的重要等级、应用场景的防护等级,匹配对应的加密防护模式与运算强度,实现精细化、差异化的分级防

护管控。灵活可调的加密机制能够适配多元电网通信场景,提升防护体系的环境适配能力与安全防护质量。

4.4 加密与通信系统的融合优化

现阶段多数加密防护模块处于独立运行状态,与电网通信系统的融合程度较低,运行壁垒较为明显。持续推进加密防护技术与智能电网通信系统的深度融合,重构二者的运行适配模式。优化加密程序与通信传输程序的运行架构,梳理两类程序的运行逻辑,减少加密运算对数据传输流程的干扰与阻滞。降低加密防护操作对通信速率、系统资源的占用影响,提升整体通信运行效率^[5]。深度融合的运行模式可以适配智能电网高速化、智能化的通信发展趋势,推动加密防护技术常态化、高效化应用。

结束语

不同类型的加密防护技术具备差异化的应用优势,可分别适配智能电网各类通信传输场景的防护需求,有效解决数据传输过程中的安全隐患。结合当前电力通信加密防护的运行短板,通过优化加密算法结构、搭建全链路防护架构、升级动态适配机制、深化防护系统与通信体系融合,可以补齐传统防护模式的各类不足,强化数据传输全流程安全管控,稳固智能电网电力通信体系的安全运行基础。

参考文献

- [1] 王东,石鑫,胡乃欣.电力通信网络数据传输层属性授权加密方法研究[J].通信电源技术,2025,42(12):151-153.
- [2] 俞震迪,李梦娜,鲍广伟,等.基于加密通信的智能电表数据安全保护方法及系统研究[J].电工技术,2026(5):165-169,173.
- [3] 杜春霞,孙迎臣,邱婷,等.电力通信加密算法在智能电表数据安全传输中的应用研究[J].通信电源技术,2026,43(1):88-90.
- [4] 辛会玲,梁志栋.面向电力工程的通信网络动态加密认证技术研究[J].通信电源技术,2026,43(9):138-140.
- [5] 王容华,王泓.基于非对称加密算法的电力通信安全监测系统研究[J].通信电源技术,2024,41(21):13-15.