电力调度数据的网络传输技术与安全渗透分析

郝一楠
国网西咸新区供电公司，陕西省西安市 712000

摘　要：为了提升电力系统的网络安全性，推动电力系统的智能化发展，本文通过对电力调度数据的网络传输技术与安全渗透问题进行深入探究，引入防火墙技术、加密技术等，有效降低网络攻击风险，保障调度数据的完整性，进而实现高效、安全的电力调度管理。

关键词：电力调度数据；网络传输技术；安全渗透

1 电力调度数据的网络传输技术

1.1 远动通信协议

传统模式大多依靠电路独立的 64kbit/s 专线通道，其主要协议包含 IEC 60870–5–101，DNP 3.0 等。伴随着网络技术的发展，IEC 61850 标准在电力行业慢慢推行，IEC 国际电工委员会便颁布了 IEC 60870–5–104 远动传输规约，从而顺应网络化发展趋向，更好地符合现代电力系统需求。规约依靠 TCP/IP 协议体系，利用平衡通信机制，实现远动数据在复杂网络环境中的有效传输，主要被调度主站（中心站）和子站（远方站）之间的信息交流任务使用。

1.2 电力调度数据网架构与组网技术

1.2.1 网络架构

电力调度数据网依靠电力 SDH 通信传输平台搭建起来，专门用于调度生产的专用数据承载，主要承担实时以及非实时业务数据的传输工作。其网络架构由骨干层和多级接入层组成，骨干层采用 A/B 平面双平面形式，两者在拓扑结构和节点分布方面非常接近，而且具备冗余备份特性。从顶层到底层，依次是国家级调控中心、区域级调度中心、省级调度中心和地市级调度中心，各个层级的作用在于保证各级电网调度机构与接入网络的高效协同运转。

接入网架构分为四个功能区块，实时区充当核心控制中枢，承担着关键业务处理的任务，而非实时区则专注辅助生产职能；管理信息大区由第三、第四区域构成，整个架构的设计目的是改善资源协同以及高效运作状况，各个层级的接入网主要任务是整合所属变电站和直调电厂的资源，并且要保证同不同调度中心之间进行数据交互。单个变电站一般采取双路径接入形式，分别同两个独立的接入网络系统相联结，进而创建上行通信链路的冗余保障机制。

1.2.2 设备配置

中调和地调均配置主、备路由器，形成双冗余和双电源保证体系，在路由器和交换机之间布，置纵向加密装置。变电站以及用户变电站各自安排一台路由器，依靠专门的传输通道，实现主、备路由与地调汇聚层路由器的连接，在路由器之后，依次接入许多业务区域交换机，从而满足各种业务主站或者子站的信息搜集需求。

1.2.3 网络拓扑

电力调度数据网的性能和可靠性由其网络拓扑结构设计所决定，网络架构包括星型、总线型以及环型等模式，在电力调度领域中，分层星型拓扑因其出色的扩展性和故障隔离能力而被普遍采用。以某区域电力调度数据网为例，地调中心充当核心节点，各个变电站以及直调电厂的接入点通过星型结构与之相连，如果某个接入节点发生故障，其他节点依然能够维持正常的通信状态，很好地显示该拓扑设计技术上的优势。

1.2.4 传输网络传送技术

（1）2M 通道

针对 2M 通道，接入层（含变电站及用户变电站）到汇聚层（地调中心）的数据传输大多依靠 2M 链路或者双 2M 捆绑技术来达成，变电站路由器通过 2M 接口接入 SDH 传输网络，通过内部处理之后，汇集到地调 SDH 设备的 STM–1 光口，再通过 STM–1 CPOS 端口，与地调路由器创建联系，以实现信息交流。在汇聚层向核心层的数据转发过程中，利用 STM–4 CPOS 端口去关联 SDH 模块，通过 STM–4 接口把，地调数据网的数据传送至中调系统。此方案凭借 SDH 业务特性，在保障实时性与可靠性的前提下，明显缩减了汇聚节点所需的 SDH 板卡数量，进而改善了整体硬件资源的配置效率。

（2）以太网 Over SDH

在以太网 Over SDH 架构下，接入层与汇聚层的数据传输主要依赖于以太网技术，变电站路由器通过 10M/100M 以太网接口接入 SDH 网络，一般选用 2M 或者 10M 带宽开展数据交换，之后经过 SDH 系统汇总处理，并转发到地调 SDH 设备的以太网端口，再凭借网卡和地调路由器实现通信互动。为了精简配置步骤并简化设备管理，可以利用 EVPLAN 协议搭配 QinQ 技术，在子站通道汇聚层 SDH IP 板卡上指定一个 VLAN 映射规则，然后在汇聚路由器内部通过 QinQ 机制恢复原先的 VLAN 信息，以此达

到高效的部署目的。虽然该方式可以实现大规模的数据传输，但是传输效率受限于 SDH 设备中的以太网板卡的汇聚能力。随着电网网络规模的增大，地调四级网中主网、配网以及用户站点数量大幅增加（一般在 30 ~ 60 个），需要配置多块以太网板卡，中心节点扩容压力明显。

1.2.5 数据网关键网络技术

（1）OSPF

作为链路状态路由协议的一种典型形式，OSPF 依靠对网络拓扑结构动态变化的即时监控，来启动路由更新机制，其核心在于利用 SPF 算法达成高效路径计算，在链路故障等事件发生时，迅速形成无环路且最优化的转发路径。在 OSPF 架构中，各个区域之间仅仅可以交换本地路由信息，这有效地缩减了全局路由计算的复杂性，并且，边界路由器只会在察觉到路由状态改变时，才向相邻区域发出更新数据包，这样精确的信息流传方式，明显削减了跨区域通信所耗费的资源。

通过把网络划分成三个 OSPF 区域，Area 0 包括主调度中心（中调）和 A 地区调度中心（A 地调）的上行链路接口以及互联接口，而且涵盖 B 地区调度中心（B 地调）的上行链路接口和互联接口；Area 1 由 A 地区调度中心与接入变电站及用户变电站之间的互联接口以及 Loopback 接口构成；Area 2 对应 B 地区调度中心与接入变电站及用户变电站的互联接口及其 Loopback 接口。

（2）BGP

BGP 作为外部网关协议，主要负责路由信息的交互以及最优路径的选择。在路由更新时，采用增量式传输的方式，只发送新增或更改的数据项，大大节省了网络带宽资源，非常适合在互联网环境下的大规模路由信息传播。利用自治系统（AS）路径属性，成功解决了传统路由算法容易产生环路的问题。通过分析某实际系统案例可知，该架构分为核心层、汇聚层两层，其中核心层由中调主备路由器组成，汇聚层由地调 A/B 的主备四台路由器组成，形成了典型的 Cluster 模型。在网络架构设计中，中调及银川 RR 为一级 RR，主要与核心路由器连接的汇聚层及接入层设备通信，充当客户端，汇聚层路由器同时具备一级 RR 客户端及接入层 RR 属性，地调内部汇聚层路由器为二级 RR，与变电站或用户变电站接入层设备（Client）形成独立 Cluster，地调核心骨干路由器为二级 RR，为上述 Cluster 提供服务。

（3）MPLSVPN

多协议标签交换虚拟专用网络（MPLS – VPN）技术凭借优秀的业务隔离能力和 QoS 保证被广泛采用，它依靠骨干网络架构来部署，各个业务系统能够在各自的虚拟专网环境中独立运行，利用标签交换机制，形成安全的通信通道，而且在设备层、链路层以及路由层都加入了冗余设计，这极大提升了网络的可靠性。凭借划分不同的安全级别虚拟专网，可以防止跨域数据泄露，保证用户只能访问到自己被允许的路由信息。在调度数据网的架构体系中，按照自身功能特性，虚拟路由与转发（VRF）划分成实时型和非实时型两种类型。按照电力系统运行规范，各类 VRF 的访问控制策略如下：属于同一个 VRF 的中调节点能够同地调节点、变电站以及用户站开展通信交流；地调节点只能同属于自己管辖范围内的接入层变电站和用户站展开信息交流；原则上不许地调节点之间直接形成连接，而且要严格控制厂站之间的直接链路。

2 电力调度数据网络的安全渗透分析

2.1 安全漏洞与风险分析

电力调度数据网络的安全性遭遇多维度因素的威胁，从网络架构角度出发，如果拓扑结构设计有瑕疵，就会潜藏单点故障隐患，一旦关键节点出现问题，就会造成大量数据传输中断。从协议设计角度来讲，部分传统通信协议由于架构设计瑕疵，存在安全风险隐患。在制定早期远动通信标准时，并没有把网络安全要素考虑进去，这就使它们成了黑客的攻击重点，人为因素是关键风险源，内部运维人员由于技术失误，可能会造成数据泄露或者系统故障，如错误设置防火墙规则，恶意篡改数据、窃取敏感信息等。外部网络攻击的严峻态势日趋严重，黑客常常利用各种网络扫描工具探测电力调度数据网络的安全漏洞，并发起攻击，恶意软件通过感染终端设备，窃取敏感信息，或者控制关键设施。如表 1 所示，为不同漏洞类型以及影响等级。

表 1 不同漏洞类型以及影响等级

漏洞类型	影响等级	描述
注入	高	攻击者可以通过注入恶意代码来控制目标系统，可能导致系统崩溃或数据泄露。
越界	中	攻击者可以访问或修改超出正常范围的数据，可能影响系统的正常运行。
拒绝服务	高	攻击者通过发送大量的请求或数据包，使目标系统无法正常响应合法请求，导致系统瘫痪。

以某省级电网为例，发生一起调度数据被篡改事件，攻击工具为 BlackEnergy 变种。攻击者先是对该电网调度系统进行侦察，通过钓鱼攻击，获取了一名运维人员的登录凭证，然后利用这些凭证成功登录调度系统的部分节点。之后，攻击者利用协议栈漏洞，篡改调度数据，修改部分发电计划和负荷分配指令，导致电网运行状态异常，还引发了一系列连锁反应。电网系统的异常情况逐渐加剧，最终导致部分区域的电网系统宕机，影响大量用户的正常用电，并且给当地的经济和社会生活带来了严重影响。

2.2 安全防护措施

在上述调度数据被篡改事件中，电网运维人员在发现系统异常后，立即进行应急处理，并采取多种技术手段，经过连续 48 小时的抢修，使电网系统基本恢复正常运行。

2.2.1 防火墙技术

防火墙属于电力调度数据网络安全防护体系的关键部分，被布置在边界区域，依靠预先设定的安全策略对流量进行精准过滤，

从而削减非授权访问的风险。当防火墙置于电力调度数据网与外部网络交汇处时，能够防止非法 IP 地址向内网发起攻击，有效提升系统抵抗威胁的能力和抵御恶意代码侵扰的性能。

在具体部署中，防火墙融合多种访问控制手段，如依靠 IP 地址实施权限划分、针对端口层面的流量控制、应用层的安全防护等，通过合理安排各个模块，外部网络无权访问电力调度数据网核心资源，又可以保障重要业务数据的顺利传输。

2.2.2 入侵检测与防御

入侵检测系统（IDS）通过实时监测网络流量，结合特征匹配、行为分析等技术手段，精准识别出潜藏的安全威胁。当系统察觉到异常数据流，或者符合某种攻击模式的行为模式时，就会启动告警机制，为网络安全管理员提供决策支撑。

入侵防御系统（IPS）是入侵检测系统（IDS）的一种高级形式，能够精准识别入侵行为，并且可以利用其动态阻断功能来抑制潜在的危险。一旦检测到某个 IP 地址存在异常流量，IPS 就会自动进行封禁处理，以此阻止恶意行为继续扩散。在电力调度数据网上，把 IDS 以及 IPS 安排在核心网络层面，如汇聚层或者核心层，可以对整个网络流量实行及时观察，并形成综合安全防范体系。

2.3.3 数据加密技术

数据加密是保障电力调度数据传输安全的关键技术手段，它可以有效地阻止信息被泄露或者改动。在实际应用中，利用加密算法对要传输的数据加以处理，使之变成密文形式，即使遭受非法截取，攻击者也无法得知其真实内容。如图 1 所示，为加密与解密模型。

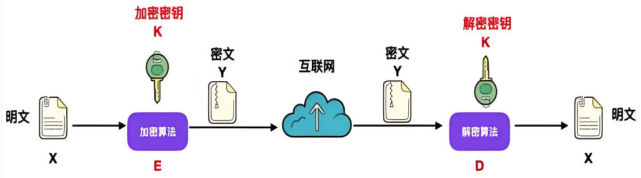

图 1 为加密与解密模型

结语：在电力系统运行中，电力调度数据作为重要支撑平台，主要负责多项核心业务的数据传输任务，其安全性对电力系统的稳定运行有着密切的关系。由于各种网络攻击手段的不断升级，使得电力调度数据面临极大的安全挑战，对此，通过加强安全防护，通过引入防火墙技术、加密认证技术，从而有效保障数据的安全传输。

参考文献：

[1] 凌培根 . 电力调度数据的网络传输技术及安全策略 [J]. 数字通信世界 ,2023(05):170–172.

[2] 马晔 . 云计算环境下电力调度大数据安全传输方法 [J]. 无线互联科技 ,2024(21):10–14.

[3] 刘冬 , 夏新志 , 刘继婷 . 基于量子密钥的电力调度数据安全传输方法 [J]. 微型电脑应用 ,2025(04):126–130.

[4] 吴伊雪 .SDN 技术的电力调度数据安全并行传输方法 [J]. 电子世界 ,2021,(15):168–169.

[5] 潘海捷 , 李韩军 , 吴展 . 探析电力通信网的调度数据网安全传输 [J]. 中国设备工程 ,2021(06):14–15.

[6] 陈博 , 李雅君 , 刘连志 . 基于电力通信网的电力调度数据网安全传输 [J]. 通信电源技术 ,2020(05):197–198.