SDN 技术在电力通信网络的研究与应用

张莹[1] 尚铁豪[2]

1 内蒙古电力通信公司，内蒙古呼和浩特市，010000；

2 呼和浩特供电公司，内蒙古呼和浩特市，010000；

摘要：随着电力系统的不断发展和智能化升级，电力通信网络面临着更高的要求。SDN（软件定义网络）技术以其独特的优势，为电力通信网络的发展带来了新的机遇。本文深入研究 SDN 技术在电力通信网络中的应用，分析了 SDN 技术的原理、特点及架构，探讨了其在电力通信网络中的应用优势、面临的挑战以及相应的解决策略，旨在为推动 SDN 技术在电力通信网络中的广泛应用提供理论支持和实践参考。

关键词：SDN 技术；电力通信网络；网络架构；应用策略

DOI：10.69979/3060-8767.25.09.011

引言

电力通信网络作为电力系统的重要支撑，对于保障电力系统的安全、稳定、高效运行起着关键作用。SDN 技术作为一种新型的网络架构，通过将网络的控制平面与数据转发平面分离，实现了网络的集中化控制和可编程性，为解决传统电力通信网络的问题提供了有效的途径。将 SDN 技术应用于电力通信网络，能够提升网络的灵活性、可靠性和资源利用率，满足电力系统智能化发展对通信网络的需求。

1 SDN 技术概述

1.1 SDN 技术原理

SDN 技术关键原理是把网络设备控制平面跟数据转发平面予以解耦，就传统网络的情况而言，网络设备里，控制平面和数据转发平面紧密交融，各个设备分别独立进行路由判断与流量转发，这造成网络配置及管理复杂又不具灵活性，就 SDN 架构这种模式而言，控制平面被聚集到 SDN 控制器那里，交换机、路由器等网络设备承担数据转发平面职责。

1.2 SDN 技术特点

1.2.1 集中控制

SDN 控制器针对整个网络进行集中式管控，可实时获得网络全局情报，实现网络资源统筹调配与优化操作，极大提高网络管控效率及全局掌控水平，与传统所采用的分布式控制方式对比，集中控制可杜绝网络设备相互的协调问题，减少配置方面的错误与冲突。

1.2.2 控制与数据平面分离

此分离架构让数据平面聚焦于数据转发，实现了转发效率的跃升；控制平面承担策略拟定、路由运算等繁杂任务，而且能在脱离数据平面的情况下进行升级与拓展，助力网络在灵活性与可扩展性上更上一层楼。

1.3 SDN 技术架构

SDN 技术架构基本上由应用层、控制层与数据层构成，应用层涵盖基于 SDN 开发的一系列网络应用，各应用按照不同业务方面的需求，依靠北向接口跟 SDN 控制器进行信息交互，采集网络信息且下发管控指令，控制层核心以 SDN 控制器为主，可视为 SDN 架构的智慧中心。控制器担负起收集网络拓扑、设备状态及流量等信息的工作，凭借这些信息进行路由推算、策略编排，而后凭借南向接口向数据层网络设备颁布转发规则，数据层（基础设施层）由诸如交换机、路由器等多样网络设备构成，承担数据转发工作，网络设备依照控制器所下达的转发规则，实现数据包的转递，实现数据在网络布局中的传输作业。

2 SDN 技术在电力通信网络中的应用优势

2.1 提高网络灵活性和可扩展性

电力通信网络的业务需求不断变化，传统网络架构难以快速适应这些变化。而 SDN 技术的应用，使得网络配置可以通过软件编程进行灵活调整。当电力系统新增业务或调整业务优先级时，只需在 SDN 控制器上修改相应的策略和配置，即可快速实现网络资源的重新分配和业务的开通，无需对大量的网络设备进行逐个配置，大大提高了网络的灵活性。同时，SDN 架构的开放性使得新的网络设备和功能模块能够方便地接入和集成到现有网络中，增强了网络的可扩展性，能够更好地满足电力系统未来发展的需求[1]。

2.2 实现高效的网络资源管理

SDN 控制器拥有网络的全局视图，能够实时监测网络流量和资源使用情况。通过对这些信息的分析，控制器可以根据不同业务的需求，动态地分配网络带宽、计算资源等。例如，在电力系统的实时监测和控制业务中，对数据传输的实时性和可靠性要求较高，SDN 控制器可以为这些业务分配高优先级和足够的带宽资源，保障业务的正常运行；而对于一些非实时性的业务，如电力设备的定期巡检数据传输，可以分配相对较低的优先级和带宽，从而实现网络资源的高效利用，提高整个电力通信网络的性能。

2.3 增强网络可靠性和稳定性

在传统电力通信网络中，当某个网络设备或链路出现故障时，故障的检测和恢复往往依赖于设备自身的协议和算法，恢复时间较长，可能会对电力系统的运行产生影响。SDN 技术应用后，SDN 控制器可以实时监测网络设备和链路的状态，一旦检测到故障，能够迅速根据预先设定的策略进行故障切换和流量重路由。例如，当某条链路出现故障时，控制器可以立即将流量切换到备用链路，确保电力业务数据的不间断传输，大大提高了网络的可靠性和稳定性，保障了电力系统的安全运行[2]。

3 SDN 技术在电力通信网络应用中面临的挑战

3.1 技术标准和规范不完善

目前，SDN 技术在电力通信网络中的应用还处于发展阶段，相关的技术标准和规范尚未完全统一和完善。不同厂家的 SDN 设备和控制器在接口、协议和功能实现上存在差异，这给多厂家设备的互联互通和网络的集成带来了困难。例如，在电力通信网络的建设中，可能需要使用多个厂家的网络设备和 SDN 控制器，如果它们之间的兼容性不好，就会导致网络配置复杂、运行不稳定等问题，影响SDN技术在电力通信网络中的推广和应用。

3.2 网络安全问题

SDN 技术的集中控制特性使得网络安全风险相对集中。一旦 SDN 控制器受到攻击，整个电力通信网络可能会陷入瘫痪，对电力系统的运行造成严重影响。此外，由于 SDN 网络的开放性和可编程性，网络攻击的手段和途径也更加多样化，如恶意软件通过北向接口入侵控制器，篡改网络配置和策略；或者攻击者利用南向接口漏洞，对网络设备进行控制和破坏等。因此，如何保障 SDN 网络的安全，是其在电力通信网络应用中需要解决的重要问题。

4 SDN 技术在电力通信网络中的应用策略

4.1 推动技术标准的统一和完善

推动SDN技术在电力通信网络中技术标准的统一和完善，是一项系统且长期的工作，需要行业上下游协同发力，从标准体系构建、跨厂商兼容测试、场景化标准细化等多个维度展开。

首先，应构建多层次的标准体系框架。电力通信网络具有业务类型多样、安全性要求高、运行环境复杂等特点，SDN 技术标准需覆盖从基础架构到业务应用的全链条。在基础架构层面，需明确控制层与数据层的接口协议标准，例如南向接口应统一采用 OpenFlow 协议的扩展版本，针对电力通信的实时性需求优化报文结构，减少控制指令的传输延迟；北向接口则需制定标准化的 API（应用程序编程接口），确保不同厂商开发的电力业务应用（如调度自动化系统、配网自动化系统）能与 SDN 控制器无缝对接，实现网络资源的按需调用。在业务支撑层面，需针对电力通信的典型业务（如继电保护信号传输、远程抄表数据上传、视频监控流等）制定差异化的服务质量（QoS）标准，明确各类业务的带宽、时延、抖动等关键指标在 SDN 网络中的保障机制，例如为继电保护业务分配专用的转发路径和最高优先级，确保其端到端时延不超过 10ms[3]。

其次，建立跨厂商的兼容测试机制。由于电力通信网络通常采用多厂商设备组网，设备间的兼容性是标准落地的关键。可由行业协会或电力企业牵头，搭建第三方兼容性测试平台，制定严格的测试规范和流程。测试内容应包括控制器与不同厂商交换机的协议交互兼容性、多控制器协同工作时的状态同步准确性、业务配置指令在跨厂商设备间的执行一致性等。例如，在测试 OpenFlow 协议兼容性时，需验证控制器下发的流表项能否被不同品牌的交换机正确解析和执行，以及交换机上报的端口状态、流量统计等信息能否被控制器准确识别。对于通过测试的设备，颁发兼容性认证证书，引导电力企业在网络建设中优先选用认证设备，逐步解决“厂商壁垒”问题。同时，定期组织厂商参与兼容性互操作演练，针对发现的问题推动标准修订，形成“测试-反馈-优化”的闭环机制。

4.2 加强网络安全防护

SDN 技术在电力通信网络中的集中控制特性，虽然提升了网络管理效率，但也使安全风险高度集中，需构建覆盖“控制器-接口-设备-业务”的多层次安全防护体系，结合电力行业的安全需求制定针对性的防护策略。

在控制器安全防护方面，需从硬件、软件、数据三

个维度构建防护屏障。硬件层面，SDN 控制器应部署在物理隔离的电力专用机房，采用冗余架构设计（如主备控制器热备份），确保单点故障时能快速切换，避免控制器失效导致整个网络瘫痪；同时，控制器服务器需具备防物理篡改功能，如通过硬盘加密、BIOS 密码保护等手段，防止未经授权的物理访问。软件层面，需对控制器操作系统和应用程序进行深度安全加固，关闭不必要的服务和端口，定期进行漏洞扫描和补丁更新，例如采用 Linux 操作系统时，需启用 SELinux（安全增强型 Linux）进行强制访问控制，限制进程的权限范围；针对控制器的核心模块（如路由计算模块、流表管理模块），需采用代码审计和静态分析工具排查潜在的安全漏洞，防止攻击者通过恶意输入触发程序崩溃或权限提升。数据层面，控制器存储的网络拓扑、配置策略、流量统计等敏感数据需进行加密存储，采用 AES-256 等高强度加密算法；数据传输过程中，需启用 TLS（传输层安全协议）加密控制器与其他设备的通信，防止数据被窃听或篡改；同时，建立数据备份与恢复机制，定期将关键数据备份至离线存储介质，确保数据损坏或丢失时能快速恢复。

在接口安全防护方面，需强化北向接口和南向接口的访问控制与安全监测。北向接口作为业务应用与控制器的交互通道，需采用严格的身份认证机制，例如基于数字证书的双向认证，业务应用需向控制器提交包含公钥的证书，控制器验证证书的有效性后才能建立连接；同时，通过细粒度的权限管理，为不同的业务应用分配差异化的操作权限（如只读权限、配置权限、管理权限），例如调度自动化系统可拥有配置 QoS 策略的权限，而普通监测系统仅能获取网络状态信息。南向接口作为控制器与网络设备的指令传输通道，需采用安全的协议栈，例如对 OpenFlow 协议进行扩展，增加报文完整性校验和源地址验证字段，防止攻击者伪造控制指令；同时，在接口处部署入侵检测系统（IDS），实时监测异常的报文交互，如短时间内大量重复的流表删除指令、异常的控制器 IP 地址发起的连接请求等，一旦发现攻击行为立即触发告警并阻断连接。

在网络设备安全防护方面，需提升数据转发平面的抗攻击能力。交换机、路由器等网络设备应支持硬件级别的安全功能，例如内置可信执行环境（TEE），确保转发逻辑的代码和配置不被恶意篡改；启用端口安全功能，限制每个端口允许接入的 MAC 地址数量，防止 MAC 地址泛洪攻击。对于电力通信网络中的关键设备（如骨干网核心交换机），需部署异常流量清洗功能，通过深度包检测（DPI）技术识别恶意流量（如 DDoS 攻击流量、SQL 注入攻击报文），并实时过滤或引流至清洗中心，避免攻击流量占用网络资源。此外，定期对网络设备进行安全配置核查，确保设备的默认密码已修改、不必要的服务已关闭、固件版本为最新安全版本，从配置层面减少安全漏洞。

在业务安全防护方面，需结合电力业务的特性实施差异化防护。针对继电保护、安控系统等关键业务，需采用“专用通道+加密传输”的双重保障机制，通过 SDN 控制器为其划分独立的 VLAN（虚拟局域网）或切片，与其他业务完全隔离；业务数据传输时采用国密算法（如 SM4）进行加密，确保数据的机密性和完整性。对于远程控制类业务（如变电站远程操作），需在 SDN 网络中嵌入操作鉴权机制，控制器在转发控制指令前，需验证操作指令的数字签名和操作权限，防止未授权的远程操作；同时，通过流量镜像技术将控制指令的传输过程实时镜像至审计系统，实现操作行为的全程可追溯。此外，建立业务安全态势感知系统，整合控制器、网络设备、业务系统的安全日志，通过大数据分析识别潜在的业务安全风险，如某一区域的配网终端突然出现大量异常的连接请求，可能预示着终端被恶意控制，系统可自动触发 SDN 控制器切断该区域的网络连接，防止风险扩散。

5 结论

SDN 技术作为一种具有创新性的网络技术，为电力通信网络的发展带来了新的契机。然而，SDN 技术在应用过程中也面临着技术标准不完善、网络安全风险和人才短缺等挑战。为了推动 SDN 技术在电力通信网络中的广泛应用，需要行业各方共同努力，完善技术标准，加强网络安全防护，加大人才培养和引进力度。

参考文献

[1]杜荣良,余修成,陈浩.基于 SDN 的电力通信网络技术分析[J].中国电子商情,2024,(02):112-114.DOI:10.19584/j.cnki.11-3648/f.2024.02.008.

[2]夏桂兵,赵艳,岳曲,等.基于SDN技术的电力系统通信网络数据包获取方法[J].电子元器件与信息技术,2024,8(01):167-169+174.DOI:10.19772/j.cnki.2096-4455.2024.1.043.

[3]苏辉,买合木提·吐尼牙孜,王海鹏.基于 SDN 的电力通信网络技术应用[J].集成电路应用,2023,40(11):294-295.DOI:10.19339/j.issn.1674-2583.2023.11.135.