基于SDN和Telemetry技术的电力终端管理方案研究

Research on Power Terminal Management Scheme Based on SDN and Telemetry

冯铭能，王　欣，梁辰恺（中讯邮电咨询设计院有限公司广东分公司，广东 广州 510627）
Feng Mingneng，Wang Xin，Liang Chenkai（China Information Technology Designing & Consulting Institute Co.，Ltd. Guangdong Branch，Guangzhou 510627，China）

摘　要：
5G电力终端作为智能电网边缘侧的重要感知节点，对其进行高效的管控必不可少。传统电力终端存在管理复杂、运营困难、安全性差等问题，新方案利用SDN/NFV和软硬件解耦，实现智能化的网络管理；利用Telemetry技术，提供精细化运营手段；利用网络切片、网络加密及二次认证技术打造高安全、高可靠的业务承载，解决现有电力终端存在的业务痛点。

关键词：
电力终端；SDN；遥测；网络切片
doi：10.12045/j.issn.1007-3043.2022.04.014
文章编号：1007-3043（2022）04-0073-07
中图分类号：TN919
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
As an important sensing node on the edge of smart grid，5G power terminal should be efficiently managed and controled. The traditional power terminals have the problems of complex management，difficult operationand poor security. The new scheme uses SDN / NFV and software and hardware decoupling to realize intelligent network management，and uses telemetry technology to provide fine operation means. At the same time，network slicing，network encryption and secondary authentication technology are used to create a highly secure and reliable service bearing，so as to solve the service pain points existing in the existing power terminals.

Keywords：
Power terminal；SDN；Telemetry；Network slicing

引用格式：冯铭能，王欣，梁辰恺. 基于SDN和Telemetry技术的电力终端管理方案研究[J]. 邮电设计技术，2022(4)：73-79.

0 引言

国家发改委和国家能源局在《能源发展“十三五”规划》中强调，积极发展储能，加快推进“互联网+”智慧能源建设，构建21世纪智能化、自动化的电网，实现新型电网的安全、可靠、绿色、高效。5G电力终端作为智能电网边缘侧的重要感知节点，对其进行高效的管控必不可少。

目前电力终端在管理、运营、安全性方面存在诸多问题。在管理方面存在着网络带宽无法动态分配、产品开发周期长，部署难度大等问题；在运营方面，设备复杂多样，且难以满足秒级的精细化监控要求；终端数据采集效率低，速度慢，数据传输过程容易造成网络卡顿；在安全方面，业界的主流方案尚未提供有效的措施对电力终端内部器件与控制软件进行统一的管理与认证，病毒入侵、机密信息泄露、非法代码的恶意篡改等问题频发。

收稿日期：2022-02-25

1 电力终端产品存在的问题和解决思路

传统电力终端产品采用嵌入式实时操作系统，管控结构如图1所示，配置管理系统集成在终端中，采用基于网页的Web管理工具和SNMP协议对终端进行配置管理和状态监控，该管理方式存在开通复杂、采集效率低、速度慢等问题，其主要问题如下。

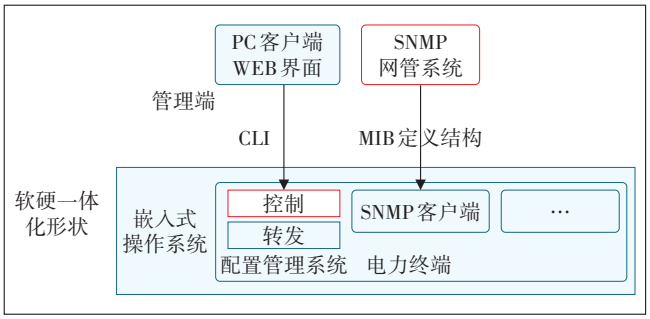

图1　传统电力一体化管控结构

a）网络控制不灵活：目前采用软硬一体化架构，基于网页的Web管理工具对业务的无线、服务、VPN、安全、访问限制、NAT、QoS设置、应用、管理以及状态进行设置操作，其业务开通和业务配置周期长，部署难度大，速度慢。网络带宽无法动态分配，造成网络资源浪费，增加终端管理难度。

b）网络管理效率低：现有技术采用SNMP协议进行业务监控，监控精度是分钟级别，监控周期为5 min，监控精度较差，对网络秒级的波动无法有效感应。

（a）被动运维：SNMP协议采用被动运维模式，通过拉模式（PULL Mode）采集数据，每次查询只有一次响应，设备应答效率低。通过拉模式来获取设备的监控数据，不能监控大量网络节点，限制了网络规模增长。

（b）数据分析困难：传统的SNMP协议采用MIB数据结构，数据零散封闭，不利于大数据分析。

（c）安全保障能力弱：业界的主流方案尚未提供有效的措施对电力终端内部器件与控制软件进行统一的管理与认证；电力终端的数据采集未采用安全可靠的保护策略；病毒入侵、机密信息泄露、非法代码的恶意篡改等问题频发；5G用户与网络的认证、密钥与算法的协商更新等过程存在被窃取、攻击的风险。

因此该方案对现有的5G电力终端进行改造，由原有集成的管理系统和SNMP协议改为转控分离的SDN控制和Telemetry管理。

首先通过SDN控制器下发指令给5G电力终端，收集并处理5G电力终端信息，实现批量化的管理，方便管理员集中管理电力终端。除此之外，SDN控制器还可以根据信息数据库对新接入的5G电力终端进行自动化匹配，收集终端的位置变化信息，确保策略跟随用户移动。该方案采用SDN技术对电力终端进行集中控制和业务发放，提升网络管理和业务开展的效率。

其次通过Telemetry能够实现网络设备主动推送状态信息的功能，这样设备的状态信息就更具时效性，可以实现秒级的流量监控和实时的质量监控。一方面监控过程对设备自身功能和性能影响小，另一方面对网络问题的快速定位和网络质量优化调整提供大数据基础，将网络质量分析转换为大数据分析，有力地支撑了智能运维。

最后该方案采用端到端的网络安全管理，对应用系统中的重要数据采取密码机制保护措施，以保证数据的保密性和完整性；通过终端切片技术，将物理网络划分成多个独立的逻辑网络，对各种关键业务进行切片隔离，提升网络安全性。并基于5G的二次认证技术，按照安全接入区的要求，通过灵活的二次认证和密钥管理对电力终端进行安全保护，避免因电力终端USIM卡被盗而引发的对电力网络的攻击。

2　电力终端管理方案研究

传统电力终端存在管理复杂、扩展难度大、安全性差等问题。本文的方案采用SDN、Telemetry和二次认证和国密加密技术，实现电力终端智能管控、精细化管理和安全保障。新的5G电力终端网络控制管理架构如图2所示。

2.1　新的5G电力终端网络控制管理架构

新型的管理架构主要分为控制平面和转发平面2个层次。控制平面包括SDN控制器、Telemetry二次认证、国密加密和网络切片管理等。转发平面包括5G电力终端。转控分离架构如图3所示。

该方案的主要优点如下。

a）转发控制分离：该方案通过控制面逻辑集中的方式来实现统一的策略控制，使流量调度和连接管理更加灵活。转发面实现高速业务数据转发，以满足未来海量移动终端的连接需求。

b）快速灵活：方案采用SDN控制器对网络进行智能化管控，实现网络流量的弹性管理，同时保障灵活和智能的网络控制，实现业务快速响应。

c）安全可靠：方案采用了保密性保护机制，保证了网络传输的安全；同时采用了完整性校检机制，保证了通信网络数据传输的完整性。

d）精细化管理：方案采用Telemetry技术，运维系统能管理更多的设备，监控数据的精度和实时性更高。相比SNMP/CLI，Telemetry能够实现网络设备主动推送状态信息的功能，新的方案更具有时效性，可

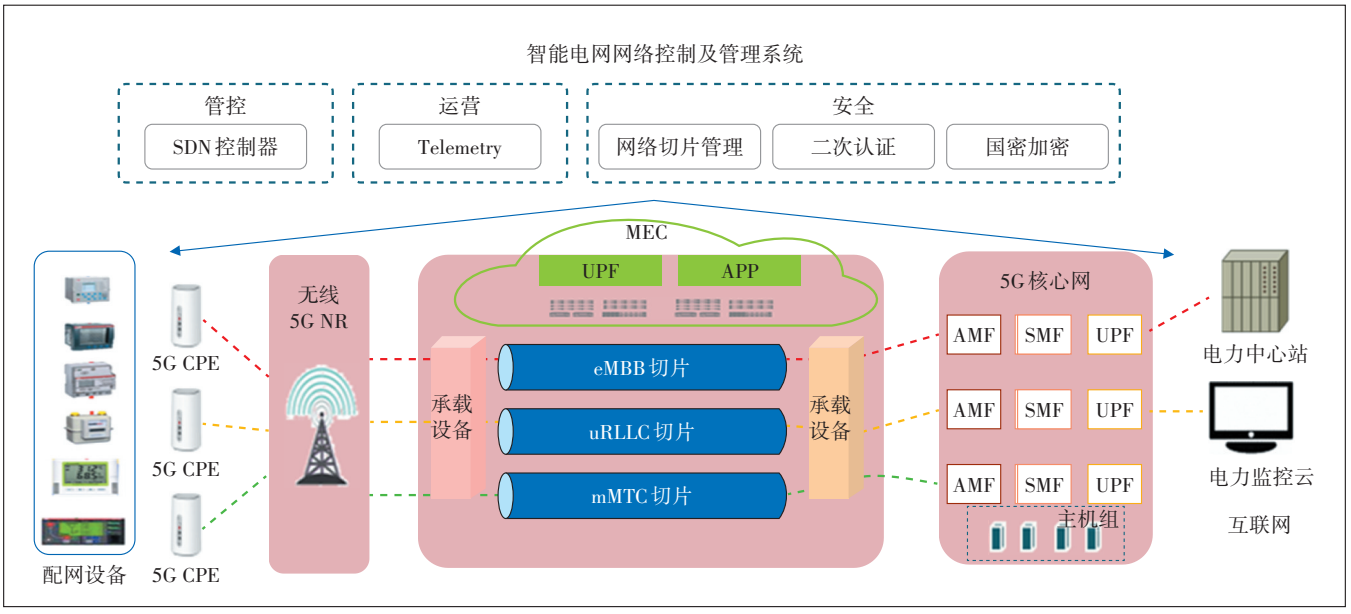

图2　新的5G电力终端网络控制管理架构

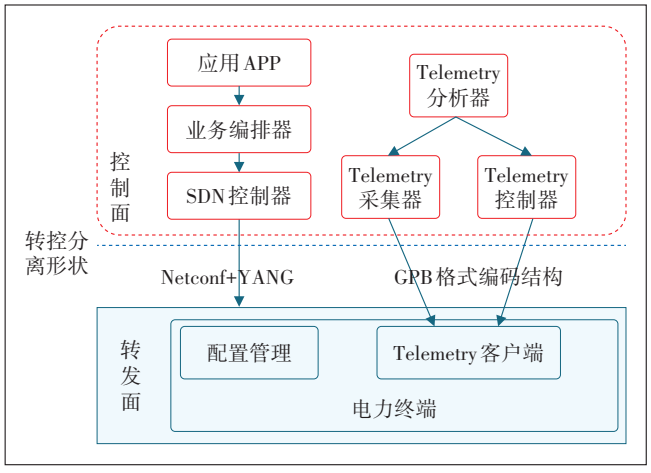

图3　转控分离架构

以实现秒级的流量监控和实时的网络质量监控。

e）差异化运营：方案通过网络切片技术，根据业务需求定制切片，使网络具备良好的可扩展性和业务适应性，满足不同业务之间的QoS需求，如时延、移动性和可靠性等。

新型的管理架构主要基于SDN的网络编排技术、Telemetry技术的运营维护方式、网络切片的差异化服务、二次认证及国密加密方法，实现电力终端的运营和管理。

2.2 SDN的管控技术方案

SDN控制的详细流程说明如图4所示。SDN控制器通过Netconf下发指令给5G电力终端，对全网所有5G电力终端的网络信息进行采集，如IP、MAC、VLAN等。同时，网络信息等通过模板进行批量导入导出操作，简化了管理员的操作。流程上，新的5G电力终端接入前，该方案需要在SDN控制器的信息库注册序列号，SDN控制器将管理者预设的模板数据下发到终端。在接入5G电力终端时，终端会向SDN控制器发送申请上线指令，由SDN控制器匹配信息数据库，判断终端是否合法，如若合法即认证新增设备并且下发相关的网络配置。最后，根据管理者的配置完成电力终端与电力主站之间的组网，从而实现SDN对5G电力终端的智能化控制。

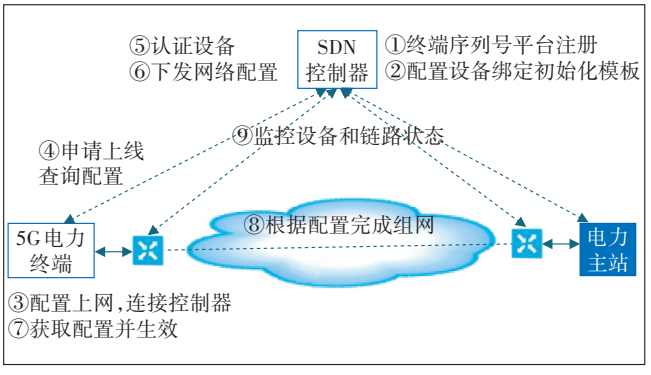

图4　网络SDN管控结构

该方案引入SDN网元实现对5G电力终端的控制和管理，提高了5G电力终端转发与控制的实时性、可靠性；同时有效保障了各类电力业务的稳定运行，以灵活的业务部署方式，满足客户端到端自动化管理运维需求，具备转控分离、快速灵活、安全可靠等优势。

2.3 秒级的网络监控方式

数据模型从MIB转变为YANG模型：传统电力终端通过SNMP协议与设备的SNMP网管通信，完成对MIB的读取和修改操作，从而实现对网络设备的监控与管理。而Telemetry的YANG模型提供了一套管理网络设备的机制，用户可以使用这套机制增加、修改、删除网络设备的配置，获取网络设备的配置和状态信息。2种数据模型结构变化如图5所示。

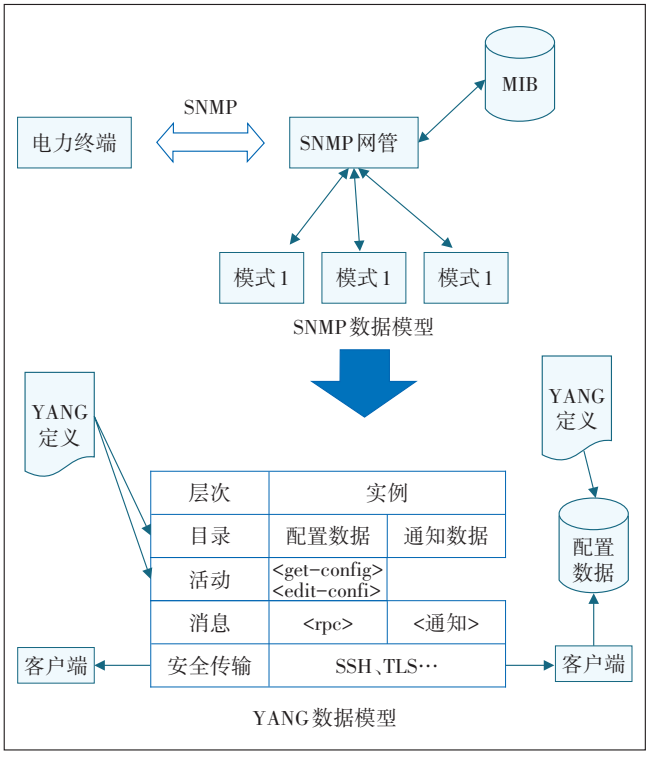

图5　数据模型变化示意图

连接关系从拉模式改为推模式：传统网络连接关系通过拉模式获取数据。如果网络卡顿或者网络获取不及时，就容易造成数据失真。而Telemetry周期性地向网管系统推送数据，避免了网络时延造成的数据不准确。Telemetry采用了“网管定制-设备实时推送”的推模式采集数据。一次定制就可以对应多次响应，减轻了设备处理查询报文的压力。传统的连接关系与Telemetry主动上报的关系对比如图6所示。

数据结构从树状改为分层结构：传统的SNMP协议的MIB以树状结构进行存储，树的叶子节点表示管理对象，而Telemetry的YANG模型采用分层结构。每层分别对协议的某一方面进行包装，并向上层提供相关服务，分层结构使每层只关注协议的一个方面，实现起来更简单，同时使各层之间的依赖关系以及内部

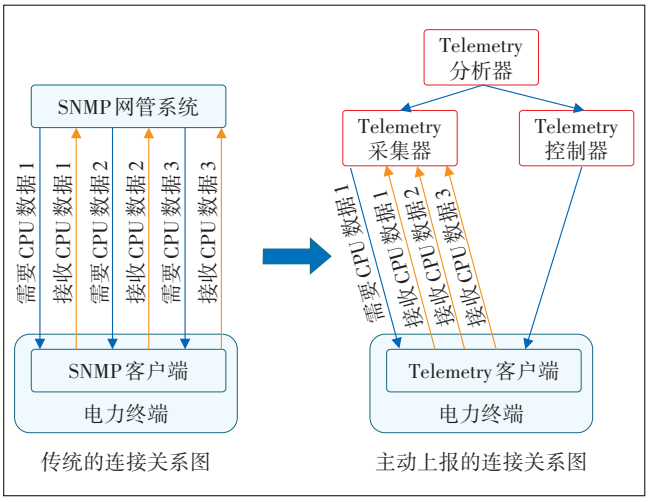

图6　连接关系的变化示意图

实现的变更对其他层的影响降到最低。

Telemetry流程上主要分为数据采集、存储、分析和决策4部分，网络架构上主要分为网元设备、采集器、分析器以及控制器。

a）网元设备：即5G电力终端，接收来自Telemetry网管侧的配置信息，根据Telemetry网管侧指定的规则采集数据，并将采集数据送至采集器。

b）采集器：即数据采集器，用于接收和存储来自数据采集系统的监控数据。

c）分析器：根据数据采集系统收集到的网元监控数据进行分析，并呈现分析结果，为控制器优化相关业务提供依据。

d）控制器：用于配置管理网元设备、优化网络，最终实现优化业务的目的。

Telemetry网管侧和设备侧协同运作，经过以下5个操作步骤完成整体的Telemetry静态订阅。具体流程如图7所示。

a）静态配置：控制器通过命令行配置的方式，使Telemetry的设备能够订阅数据源，完成数据采集。

b）推送采样数据或自定义事件：网络设备根据控制器的配置要求，上报采集完成的数据或自定义事件给采集器进行接收和存储。

c）读取数据：分析器读取采集器存储的采样数据或自定义事件。

d）分析数据：分析器分析读取到的上传数据或自定义事件，控制器根据分析的结果对网络进行配置管理，及时调优网络。

e）调整网络参数：控制器将网络需要调整的配置

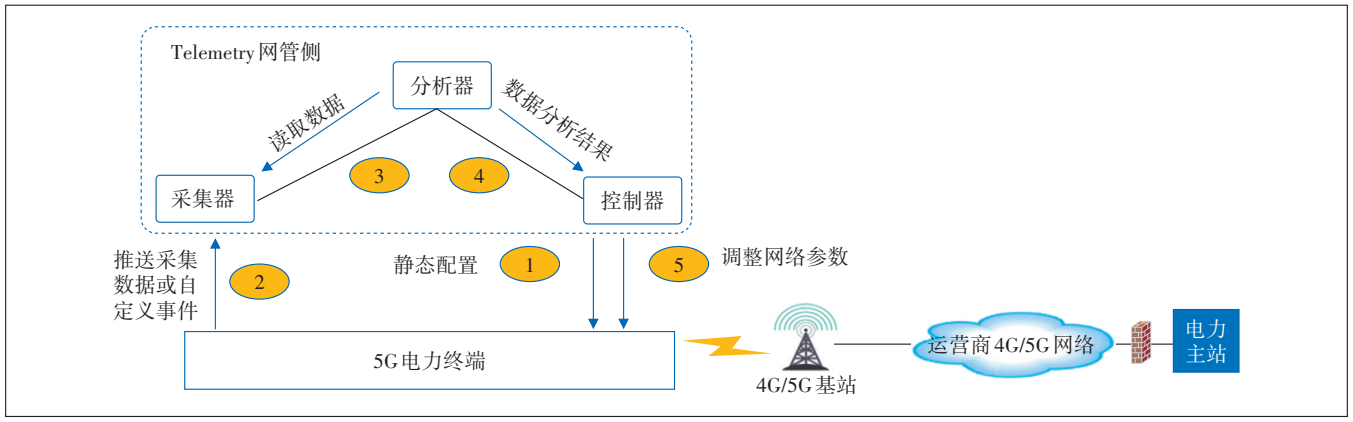

图7　Telemetry流程示意图

下发给网络设备；配置下发完成生效后，新的采样数据或自定义事件上报到采集器。

该方案支持智能运维系统管理更多的5G电力终端设备，监控数据的精度和实时性更高，相比SNMP，Telemetry能够实现终端设备主动推送状态信息的功能，可以实现秒级的流量监控和实时的网络质量监控。该方案一方面监控过程中对设备自身功能和性能影响小，另一方面对出现的网络问题可以快速定位，对网络质量优化调整提供大数据基础，将网络质量分析转换为大数据分析，有力地支撑智能运维。

2.4 网络切片管理

该方案通过网络切片将电力终端划分到不同的切片中，以灵活应对不同的电力切片应用场景，配合二次认证和国密加密技术，保障网络安全。终端网络切片系统架构如图8所示。

通过5G网络切片，在为用户提供服务的过程中，

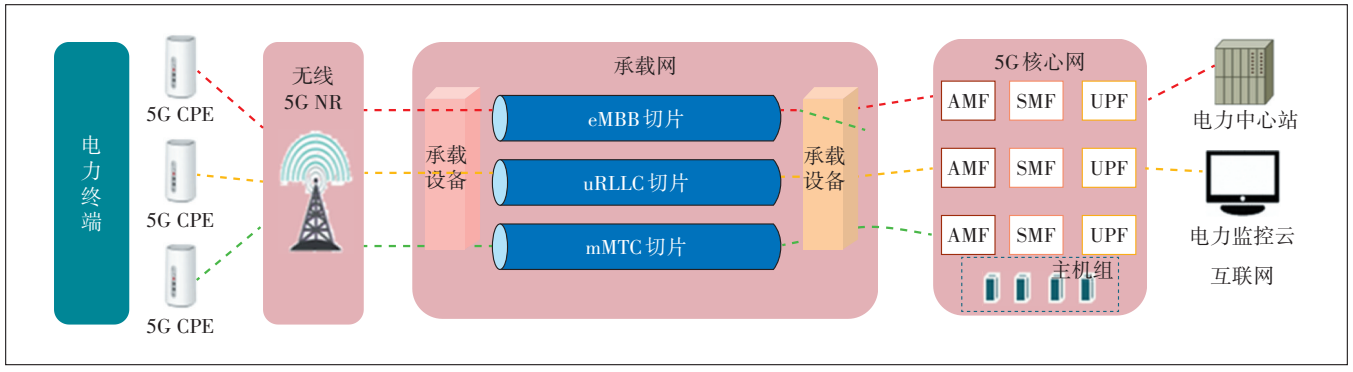

图8　终端网络切片系统架构

将业务分成uRLLC、mMTC、eMBB类切片，通过无线侧、承载网传输侧、核心网侧对5G终端进行统一的管控。无线接入基于电力业务切片和5QI值进行优先级设置。承载网根据业务的时延和可靠性的不同需求，采用FlexE或VPN+QoS隔离技术，实现电力业务的软硬隔离。核心网将电力业务切片分为AMF、SMF、UPF，实现隔离。

电力通信管理平台管理终端卡号，上传切片标识，5GC根据用户签约切片信息，选择相应切片建立会话。具体业务流程如图9所示。

a）PCF把UE路由选择策略通过AMF发放给UE，UE用来建立APP id和S-NSSAI（分片ID）的关联。

b）在PDU激活时核心网把5QI信息发送给gNB，gNB通过配置将5QI与DSCP/VLAN优先级映射，gNB根据nexthop打VLAN tag。

c）不同的VLAN子接口在承载网入不同的VPN，通过VPN选择入相应的切片，承载网与核心网的互通流程也类似，实现端到端的切片互通。

该方案实现网络切片实例与终端服务之间的映射，并将终端注册到正确的网络切片实例上，保障了业务的隔离性。

2.5 安全保障方案

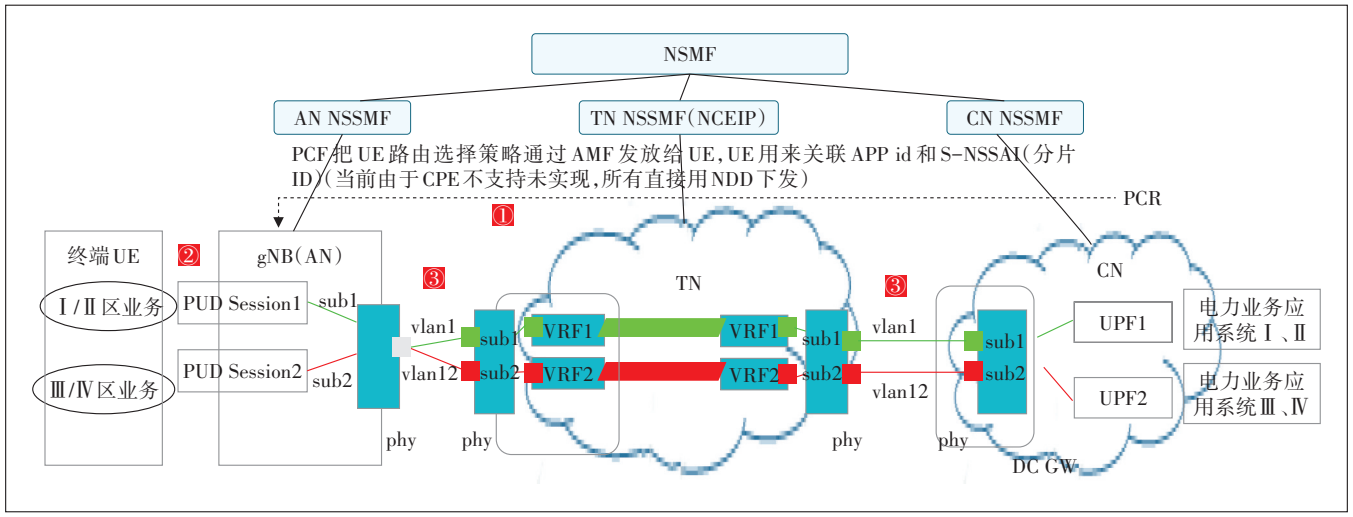

图9　终端切片业务流程图

为保障电力终端业务的安全性，该方案采用二次认证和国密加密技术。电力生产控制类业务通过5G公网进入电力业务平台前，将接入安全接入区，进行必要的网闸隔离。5G智能电网安全手段重点聚焦在管、端两侧，主要通过5G提供的统一认证框架、多层次网络切片安全管理、灵活的二次认证和密钥能力及安全能力开放等，进一步提升安全性。安全保障方案如图10所示。

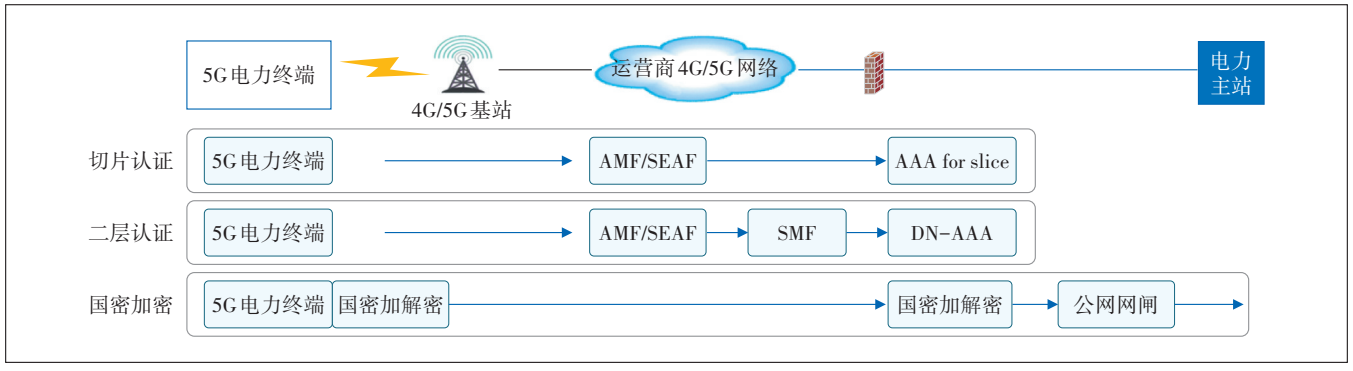

图10　5G通信终端网络安全及认证方案

5G通信终端主要采用物理隔离、安全设备、加密认证、接入控制等方式实现电力数据的安全，具体方案如下。

a）在专用通道上建立电力调度数据网，实现与电力企业数据网的物理隔离，保障在相同安全区进行上下级的纵向互联，避免安全区纵向交叉。

b）采用不同强度的安全隔离设备使各安全区中的业务系统得到有效保护，将生产控制区与管理信息大区进行有效安全隔离，隔离强度应接近或达到物理隔离。

c）采用认证、加密、访问控制等技术实现生产控制数据的远程安全传输以及纵向安全防护。

d）在生产控制大区通过设立安全接入区来实现配电终端的安全接入。配电安全接入网关主要采用国产商用非对称密码算法实现配电安全接入网关与配电终端的双向身份认证。数据加密认证如图11所示。

该方案通过网络数据通信的身份认证和传输数据的加密与解密，保障系统连接的合法性和数据传输的机密性、完整性。

3　技术方案的优势分析

3.1　SDN转控分离

该方案基于SDN转控分离的理念，实现智能化控制管理。转控分离后，转发面将具备简单、稳定和高效的业务数据路由转发功能，满足未来流量大幅增长

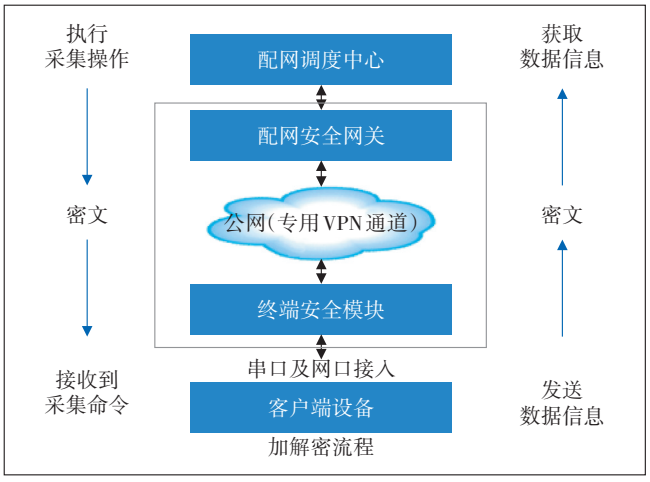

图11　5G通信终端网络安全加密流程

的需求。该方案采用SDN控制器对网络进行智能化管控，实现对网络流量的弹性管理，同时，保障灵活和智能的网络控制，实现业务快速响应。由于转发面和控制面的分离，网络变得更加扁平化，网络相关设备的部署将更加灵活。

3.2 秒级精度的监控

网络传输过程中普遍存在微突发现象，超过设备转发能力的报文将被丢弃，导致通信双方需要重传报文，严重影响通信质量。该方案通过Telemetry高精度采样，可以检测到网络的微突发流量。

传统的网络监控手段无法有效监控网络中的缓存、丢包、时延。Telemetry技术与传统的方式相比，监控数据的精度更高，可快速检测和处理微突发流量。在SNMP协议方面，如果要获取网络状态信息的SNMP，则需要由外部应用发起请求，无法反映网络的实时状态，而Telemetry采用主动上报方式，可实时获取网络微突发流量信息。

3.3 主动运维

与传统的sFlow、NetStream或者NetFlow的采样技术相比，该方案中采用Telemetry技术，实现秒级的数据采样，时效性更高。该方案依靠INT技术采集网元信息，支持高采样颗粒度，并且可采集更多的过程数据，比如设备的buffer、队列等数据。该方案依靠gRPC技术，能够实时反馈数据。在分析方面，Telemetry方案支持多种分析，例如，无线用户接入故障定位、RDMA状态可视和拥塞分析、业务异常检测及分析、音视频应用体验分析、应用质量分析等。而且Telemetry技术能够支持多方面流量、故障预测以及质量差等的预测。

3.4 提供安全保障的手段

该方案采用多种技术结合的安全保障手段，包括网络切片、安全加密、二次认证等。网络切片技术具备优化网络资源分配，满足未来多元新业务的网络需求等特点。该方案的网络切片方案一方面提供端到端的网络切片能力，另一方面能够将控制5G电力终端的网络进行安全隔离，电力业务与基础网络实现分离。该方案由安全加密、二层认证和切片认证共同构建了5G终端的安全保障体系，为电网的密码提供全方位的保障，提高电网外网环境下的数据产生、采集、传输、存储、使用、销毁等全生命周期过程的机密性、真实性、完整性，达到业务处理过程的数据信息的可管可控。除此之外，该方案为电网外网上的终端运行提供统一认证、访问控制、数字签名验签、数据加密等服务。

4 结束语

本文分析了传统电力终端存在的问题，主要基于SDN和Telemetry技术研究5G电力终端的网络控制和管理方法，运用SDN/NFV、Telemetry技术、网络切片、网络加密及二次认证等技术，解决当前传统电力终端存在的管理复杂、运营困难、安全性差等问题。该方案具备智能化管控、精细化运营、安全可靠、边缘计算、终端软硬件解耦等优势。该方案可持续为南方电网、国家电网等电力行业提供端到端的5G电力智能化解决方案，助力电网企业实现数字化转型升级。

参考文献：

[1] 张传福，赵立英，张宇. 5G移动通信系统及关键技术[M]. 北京：电子工业出版社，2018.
[2] 郭铭，文志成，刘向东. 5G空口特性与关键技术[M]. 北京：人民邮电出版社，2019.
[3] 陶志强，王劲，汪梦云. 5G在智能电网中的应用[M]. 北京：人民邮电出版社，2019.
[4] 陈允鹏，黄晓莉，杜忠明. 能源转型与智能电网[M]. 北京：中国电力出版社，2017.
[5] 刘韶林. 物联网技术在智能配电网中的应用[M]. 北京：中国电力出版社，2019.

作者简介：
冯铭能，高级工程师，博士，主要从事数据网、核心网、电力通信网的相关咨询设计工作；
王欣，高级工程师，本科，主要从事数据网、核心网、电力通信网的相关咨询设计工作；
梁辰恺，工程师，硕士，主要从事数据网、网络安全、电力通信网相关咨询设计工作。