ICS
M 11

团　　体　　标　　准

T/××××××××—××××

电力无线局域网（EPWL）技术要求

Technical requirements for electric power wireless local area network (EPWL)

××××-××-××发布　　××××-××-××实施

X X X X X X X X发 布

目　　次

前　言

本文件依据GB/T 1.1—2020《标准化工作导则第1部分：标准化文件的结构和起草规则》的要求，按照《国家电网有限公司技术标准管理办法》的规定起草。

本文件由国家电网有限公司数字化工作部提出并解释。

本文件由国家电网有限公司科技创新部归口。

本文件起草单位：中国电力科学研究院有限公司、国网上海市电力公司经济技术研究院、国网江苏省电力有限公司、国网浙江省电力有限公司、国网江西省电力有限公司、中国科学院沈阳自动化研究所、新岸线（北京）科技集团有限公司、北京密码云芯科技有限公司、智芯微电子科技有限公司、沈阳邦粹科技有限公司。

本文件主要起草人：张慧、高凯强、徐高峰、丁慧霞、项栩琛、宋彦斌、汪莞乔、汤婵娟、吕征宇、赵新建、汤亿则、邱兰馨、刘强、傅裕、杨雨沱、刘慎发、崔心发、李鹏、孙马秋、袁艳芳、杨峰、刘立辉。

本文件首次发布。

本文件在执行过程中的意见或建议反馈至国家电网有限公司科技创新部。

引　言

随着新型电力系统建设和电网数字化转型的不断深入，变电站、换流站、无人值守配电房等场景涌现出巡检机器人、智能安全帽、无人机等智能终端，并且这些终端的数量激增，需要无线局域网技术承载。目前可用的WiFi技术存在几方面问题：采用CSMA/CA的竞争机制，会与民用和其他行业WiFi产生空口资源竞争问题；管理帧和控制帧无法进行加密，会存在多种类型攻击；接入认证仍旧存在漏洞。大规模试点的WAPI技术底层协议仍旧基于WiFi，只在安全接入认证方面进行了增强，但仍旧存在WiFi的其他方面问题。当前主流的、公用的无线局域网技术WiFi、WAPI在安全性、可靠性方面都存在问题，因此要制定电力专用的无线局域网技术标准，匹配变电站、换流站、配电房等重要场所实现视频监控类（摄像头等）、远程巡视类（巡检机器人等）、运行监测类（油色谱监测、SF6气体监测、消防监测等）、运维管理类（手持终端、布控球、仪器仪表、智能安全帽等）等业务数据无线接入新需求，支撑新型电力系统建设和电网数字化转型，适应现代设备管理发展新趋势，全面提高变电设备运维感知和管控能力。

电力无线局域网(EPWL)技术要求

1 范围

本文件规定了电力无线局域网（以下简称EPWL）的网络架构、系统功能要求、网络性能要求、频率要求、安全要求、通信协议要求、设备要求。

本文件适用于电力行业所辖变电站、换流站、配电房等生产场所及输电线路、电缆隧道和新能源接入等局域覆盖场景下EPWL的规划、设计、建设。

2 规范性引用文件

下列文件对本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

DL/T 860.3 变电站通信网络和系统 第3部分：总体要求

DL/T 2614-2013 电力行业网络安全等级保护基本要求

YD/T 3168-2016 公众无线局域网设备射频指标技术要求和测试方法

GB/T 2423.3 环境试验 第2部分：试验方法 试验Cab：恒定湿热试验

GB/T 4208 外壳防护等级(IP代码)

GB/T 9254.1 信息技术设备、多媒体设备和接收机 第1部分：发射要求

GB/T 14598.3 电气继电器 第5部分：量度继电器和保护装置的绝缘 配合要求和试验

GB/T 15153.2 远动设备及系统 第2部分：工作条件 第2篇 环境条件（气候、机械和其它非电影响因素）

GB/T 15629-11-2003_信息技术 系统间远程通信和信息交换局域网和城域网 特定要求

GB/T 17626.2 电磁兼容 试验和测量技术 静电放电抗扰度试验

GB/T 17626.3 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验

GB/T 17626.4 电磁兼容 试验和测量技术 电快速瞬变脉冲群抗扰度试验

GB/T 17626.5 电磁兼容 试验和测量技术 浪涌（冲击）抗扰度试验

GB/T 17626.6 电磁兼容 试验和测量技术 射频场感应的传导骚扰抗扰度试验

GB/T 17626.8 电磁兼容 试验和测量技术 工频磁场抗扰度试验

GB/T 17626.9 电磁兼容 试验和测量技术 脉冲磁场抗扰度试验

GB/T 17626.10 电磁兼容 试验和测量技术 阻尼振荡磁场抗扰度试验

GB/T 17626.16 电磁兼容 试验和测量技术 0Hz~150kHz共模传导骚扰抗扰度试验

GB/T 17626.18 电磁兼容 试验和测量技术 阻尼振荡波抗扰度试验

GB/T 17626.29 电磁兼容 试验和测量技术 直流电源输入端口电压暂降、短时中断和电压变化的抗扰度试验

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 26790.2-2015 工业无线网络WIA规范 第2部分：用于工厂自动化的WIA系统 结构与通信规范

GB/T 36454-2018 信息技术 系统间远程通信和信息交换中高速无线局域网媒体访问控制和物理层规范

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

IEEE STD 802.11-2012 信息技术系统间远程通信和信息交换局域网和城域网特定要求第11部分：无线局域网媒体访问控制和物理层规范（Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY) specifications）

3 术语和定义

3.1

业务终端 services terminal

服务于电力生产和企业管理各类业务的终端，包括但不限于电力工控终端、电力物联终端等。

3.2

电力通信终端 electric power communication terminal

连接在电力通信网末端，并与业务终端数据接口相连，为业务终端提供发送和接收信息功能的终端，包括外置式通信终端、内置式通信模组等物理形态。

3.3

无线局域网 wireless local area network

采用无线工作方式，用于局部区域范围内的通信终端无线连通、交换数据的网络。

3.4

电力无线局域网 electric power wireless local area network

通过双向身份鉴别、数据加密保护、电力需求定制等方式实现电力业务稳定可靠、安全传输的电力无线局域网。

3.5

电力无线接入点 electric wireless access point

部署在电力无线局域网应用场所内，发射和接收无线信号，实现对特定区域的无线信号覆盖，提供可靠、高性能的无线连接功能。

3.6

电力鉴别服务单元 electric authentication service unit

EPWL 中为电力通信终端与电力无线接入点的双向认证过程提供数字证书鉴别服务的网元。

3.7

电力无线接入控制单元 electric wireless access control unit

EPWL 中为电力通讯终端与电力无线接入点提供接入控制协议层调度的网元。

3.8

空中接口 air interface

EPWL中，电力通信终端与电力无线接入点之间的通信接口。

3.9

漫游切换 handover

EPWL中，电力通信终端退出当前电力无线接入点、连接到新的电力无线接入点，并保持业务不中断的过程。

4 缩略语

下列缩略语适用于本文件。

CRL：证书吊销列表（Certificate Revocation List）
DTLS：数据包传输层安全协议（Datagram Transport Layer Security）
EAS：电力鉴别服务单元（Electric Authentication Service unit）
EAC：电力无线接入控制单元（Electric wireless Access Control Unit）
EAP：电力无线接入点（Electric wireless Access Point）
ESTA：电力通信终端（Electric power communication Station）
EPWL：电力无线局域网（Electric PowerWireless Local area network）
IP：互联网协议（Internet Protocol）
IPSec：互联网安全协议（Internet Protocol Security）
LTF：长训练序列（Long Training Field）
MAC：媒体访问控制（Medium Access Control）
MCS：调制与编码策略（Modulation and Coding Scheme）
NAT：网络地址转换（Network Address Translator）
PKCS：公钥密码标准（the Public-Key Cryptography Standard）
QoS：服务质量（Quality of Service）
RSSI：接收信号强度指示（Received Signal Strength Indicator）
SINR：信干噪比（Signal-to-Interference-and-Noise Ratio）
STF：短训练序列（Short Training Field）
SIG：信号（Signal）
VPN：虚拟专用网络（Virtual Private Network）

5 网络架构

5.1 网络整体架构

EPWL为业务终端与业务系统之间的通信提供服务，由核心层和接入层组成，其中核心层包括证书密钥签发系统、电力鉴别服务单元和设备网管系统，接入层包括电力无线接入控制单元、电力无线接入点、电力通信终端，系统架构如图1所示，基本工作原理如下：

a) 电力通信终端与电力无线接入点建立通信连接,交互由证书密钥签发系统签发的数字证书信息；
b) 电力鉴别服务单元依据数字证书信息对电力通信终端、电力无线接入点进行身份鉴别；
c) 电力无线接入控制单元对电力通信终端、电力无线接入点进行协议层的管理控制功能实现。

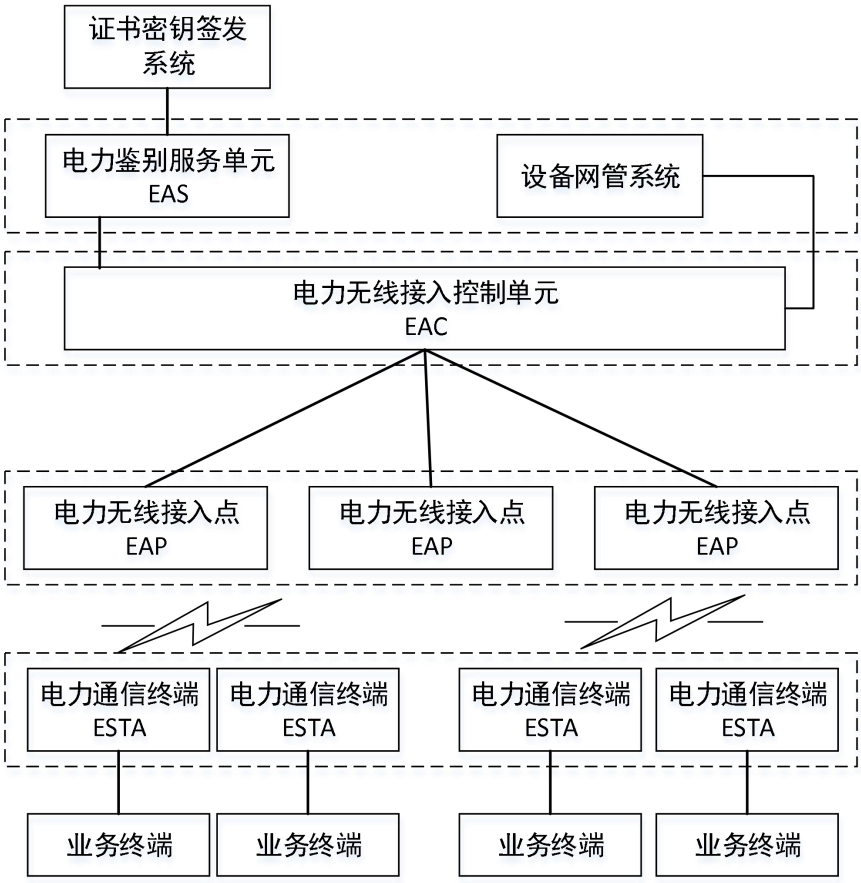

图 1 系统架构图

5.2 组网技术要求

EPWL的各组成部分要求如下：

电力无线接入点应根据应用场景以及信号覆盖范围进行合理部署，并通过设备网管系统进行控制与管理；

a) 电力鉴别服务单元可采用地市公司一级部署或省、市公司二级部署，采用一级部署时，应采用双设备冗余配置；采用省、市二级部署时，应采用 1:N 设备冗余配置；

b) 换流站、特高压变电站等面积较大、电力无线接入点数量较多的场所可单独部署电力鉴别服务单元；

c) 设备网管系统应支持对电力无线接入控制单元、电力无线接入点、电力鉴别服务单元、电力通信终端进行远程配置、管理以及监测；

d) 接入层与核心层之间应通过管理信息大区或专用于 EPWL 的数据通信专网互联。

6 系统功能要求

6.1 电力无线接入控制单元

电力无线接入控制单元用于连接电力无线接入点与其他网元的设备，功能要求包括：

a) 提供与电力无线接入点连接的接口；

b) 应实现对电力无线局域网的通信调度、漫游管理、访问控制，宜支持对不同协议的电力无线局

域网的多网融合接入等；

c) 应提供与现场设备网管系统链接的接口，实现设备网管系统对电力无线接入点以及电力通信终端进行管理；

d) 应实现对电力无线接入点与 EPWL 网络中的其他设备进行通信，交换设备间的信息；

e) 宜实现对直接连接的电力无线接入点的网络时间同步；

f) 应实现对电力通信终端和电力无线接入点的流量控制功能；

g) 应实现对电力无线接入点、电力通信终端等设备与电力鉴别服务单元的鉴权认证信息的交互。

6.2 电力无线接入点

电力无线接入点负责将电力通信终端上的业务数据、告警及网络管理相关信息转发到电力无线接入控制单元，或将电力无线接入控制单元的控制信号、管理信息和配置信息转发给电力通信终端。电力无线接入点功能要求包括：

a) 应支持将电力通信终端采集到的数据发送给电力无线接入控制单元；

b) 应支持将电力无线接入控制单元传输来的信息发送给对应的电力通信终端；

c) 应支持将电力无线接入控制单元的管理、配置和组态信息发送给对应的电力通信终端；

d) 应支持将电力通信终端的告警及网络管理相关信息发送给电力无线接入控制单元；

e) 宜支持空口波形动态配置功能；

f) 宜支持前导序列的实时动态配置功能；

g) 宜支持功率控制，包括固定功率调整及自适应功率动态调整；

h) 宜支持对周围环境无线电磁强度测量；

i) 宜支持无源相控阵天线或带转台的定向天线组控制；

j) 宜支持无线空口级联。

6.3 电力通信终端

电力通信终端连接现场传感器、摄像头等业务终端，负责发送业务终端采集的数据和接收上层控制命令的设备。电力通信终端的功能要求包括：

a) 应支持通过电力无线局域网协议与电力无线接入点通信；

b) 应支持交直流供电、电池供电、太阳能供电；

c) 宜支持空口波形动态配置功能；

d) 宜支持前导序列的实时动态配置功能；

e) 宜支持功率控制，包括固定功率调整及自适应功率动态调整；

f) 宜支持对周围无线电磁环境强度测量；

g) 宜支持以太网接口、RS232、RS485、SPI 等常用业务终端接口；

h) 宜支持无线空口级联；

i) 宜支持对传感器等业务终端的低功耗供电模式。

6.4 电力鉴别服务单元

电力鉴别服务单元的功能要求包括：

a) 应支持与证书密钥签发系统交互，能接收证书密钥签发系统下发的密钥、数字证书和 CRL，并安全存储；

b) 应支持证书验证功能，对于吊销状态中的证书，禁止该设备通过验证；

c) 应支持数字证书管理，包括数字证书的申请、审核、下载、校验等；

d) 应支持对电力通信终端和电力无线接入点的 MAC 地址、数字证书信息进行管理，包括增加、

删除、修改、查询等；

e) 宜支持日志管理功能，可通过 MAC、IP、时间等进行系统日志查询；

f) 宜支持 1:1 热备份或 1:N 热备份，故障切换时不影响业务正常运行，切换时间<500ms。

6.5 设备网管系统

设备网管系统应对电力无线接入控制单元、电力无线接入点、电力通信终端进行管理，功能要求包括：

a) 应支持对与其关联的电力无线接入点设备进行管理，包括配置下发、射频管理和漫游通信管理等功能，以及对非法无线接入点检测、识别；

b) 配置管理，应支持网元配置、网元软件管理、配置数据管理等能力，应支持的配置管理对象为电力无线接入控制单元、电力无线接入点以及电力通信终端，配置参数包括网络标识参数、设备地址参数、射频参数等；

c) 性能管理，应支持测量数据管理，宜支持测量任务管理。电力无线接入点性能数据包括无线接入点下挂终端数、无线接入点上行速率、无线接入点下行速率、射频信道利用率；

d) 告警管理，应支持告警监视、告警颜色定制、告警声音定制、告警视图定制、告警查询、告警统计与报表生成等告警呈现。应支持告警清除、确认、取消确认、同步、推送、保存等告警操作。应提供的告警信息包括产生告警的设备类型及标识符、告警产生时间、告警清除时间、告警对象、告警编码、告警类型、告警级别、告警确认时间、告警确认状态、告警确认用户标识、告警清除方式，其中告警级别应包括严重告警、主要告警、次要告警、警告告警；

e) 资源管理，应支持电力鉴别服务单元、电力无线接入控制单元、电力无线接入点、电力通信终端资源管理，其中电力鉴别服务单元包括设备资源数据，电力无线接入控制单元包括设备资源数据，电力无线接入点包括设备、射频数据，电力通信终端包括设备资源数据、下挂业务类型、当前附着电力无线接入点等；

f) 系统管理，应支持用户管理、角色管理、认证、鉴权、远程管理；

g) 日志管理，应支持操作日志、用户登录日志和告警日志管理；

h) 宜支持拓扑管理、报表管理等其他功能。

7 网络性能要求

7.1 网络容量要求

EPWL应根据业务需求进行流量分析及容量规划。

7.2 网络性能要求

7.2.1 无线信号覆盖

在覆盖范围内电力无线接入点的信道信号强度RSSI处于[-60dBm,-70dbm]区间。在设计目标覆盖区域内95%以上的区域，电力通信终端的下行信号SINR>13dB，典型的电力无线接入点覆盖方案可参考附录A。

7.2.2 吞吐量

当电力无线接入点覆盖的范围内仅有1个电力通信终端，且电力通信终端的接收信号强度RSSI≥-65dBm、SINR≥13dB时，上下行吞吐量≥100Mbps。

7.2.3 发射功率

电力无线接入点、电力通信终端的最大发射功率应满足国家无线电管理委员会对授权频段以及非授权频段无线信号发射功率的要求。

7.2.4 数据速率

单个电力通信终端平均速率不低于20Mbps，峰值速率不低于200Mbps，应满足多路高速数据业务应用需求。

7.2.5 漫游切换性能

电力通信终端运动速度≤5m/s时，电力通信终端在电力无线接入点之间的漫游切换成功率>99%，漫游切换时延<100ms，漫游切换造成的丢包率<0.1%。

7.2.6 并发容量

单个电力无线接入点可同时联接多个电力通信终端，每个电力无线接入点至少支持25路电力通信终端并发接入。

7.2.7 丢包率

在电力无线接入点设计目标覆盖区域内95%以上的区域，电力通信终端接收到的数据包丢失率<0.1%。

7.2.8 时延

空口传输时延≤20ms，应不影响流媒体、语音等业务的实时性，基本实现用户使用无感知。

7.2.9 可靠性

EPWL承载各类业务的可靠性应满足≥99.99%的要求。

8 频率要求

EPWL的工作频率要求如下：

a) EPWL 的频率使用范围可为 2400MHz~2483.5MHz、5150MHz~5350MHz、5725MHz~5850MHz 等无线电管理部门许可的无线局域网频段；
b) EPWL 应采用同一频点组中的不重叠频点进行频点规划，每个频点的中心频率宜间隔至少 25MHz；
c) EPWL 应规避覆盖区域内其他无线通信系统已使用的频点；
d) 相邻覆盖区的电力无线接入点应使用不同频点；
e) 使用相同频点的电力无线接入点，应间隔 25 米以上距离或通过建筑物隔断增加同频隔离度；
f) 在业务需求密集的局部热点区域，可以在满足信噪比要求的情况下增加电力无线接入点数量，此时工作在 2.4GHz 频段的电力无线接入点宜采用 YD/T 3168—2016 定义的编号为“1、3、6、8、11、13”的频点，如图 2 所示，以紧凑复用的方式减少干扰；

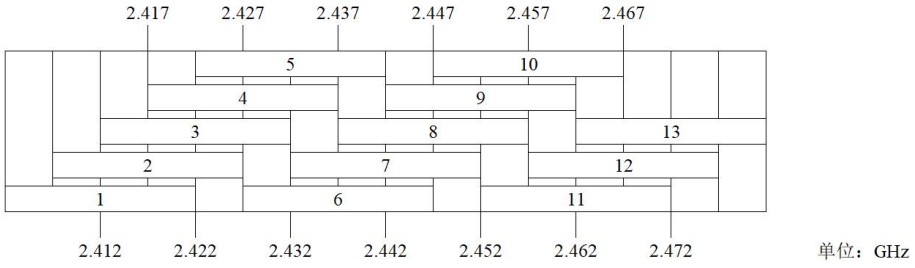

图 2 2.4GHz 信道编号

g) 在电力无线接入点部署密集，使用相同频点的电力无线接入点无法完全隔开时，应降低发射功率，减少干扰影响。

9 安全要求

9.1 总体要求

EPWL安全防护应符合GB/T 22239—2019、GB/T 25070—2019、DL/T 2614—2023对“安全通信网络”的相应等级要求(以下简称“等保要求”)，安全保护等级与业务的安全保护等级一致，其中设备网管系统及电力鉴别服务单元宜满足信息系统安全等级第三级安全防护要求。

9.2 密码应用要求

EPWL空中接口应符合GB/T 39786有关密码应用安全要求，应采用国产密码算法对电力通信终端、电力无线接入点设备、电力无线接入控制单元进行多元双向身份鉴别，保证通信双方设备身份的真实性，应采用国产密码算法保证通信过程中数据的完整性和数据的机密性。

9.3 密钥管理要求

所涉及的密钥应采用国家密码管理部门认可的国密二级及以上等级的安全芯片进行管理。该管理涵盖了密钥的生成、存储、使用、更新、导入、导出以及清除等各个环节。

9.4 鉴别认证要求

9.4.1 基本要求

基本要求如下：

a) 电力无线接入控制单元、电力无线接入点和电力通信终端应搭载支持 SM2、SM3、SM4 算法的硬件芯片作为可信根，且芯片内置公司密码基础设施签发的数字证书；
b) 电力无线接入控制单元、电力无线接入点和电力通信终端应基于数字证书与电力鉴别服务单元进行多元双向认证，在电力鉴别服务单元下通过证书核验后建立通信连接；
c) 鉴别使用的数字证书由电力无线接入控制单元、电力无线接入点、电力通信终端通过电力鉴别服务单元向证书密钥签发系统申请，证书请求文件应符合 PKCS#10 的格式要求；
d) 数字证书的格式定义、颁发和吊销过程应符合 GB 15629.11—2003　8.2 要求，数字签名算法宜采用国产密码算法；
e) 电力无线接入控制单元、电力无线接入点、电力通信终端应支持证书请求文件的导出、数字证书和多级根证书的导入。

9.4.2 证书申请认证要求

9.4.2.1 电力通信终端证书申请

电力通信终端证书申请流程如下：

a) 电力通信终端的标识信息在证书密钥签发系统进行预注册；
b) 电力通信终端完成入网和通信能力协商后，向电力无线接入点提交证书申请；
c) 电力无线接入点将证书申请转发至电力鉴别服务单元，电力鉴别服务单元以证书请求文件的格式向证书密钥签发系统申请证书；
d) 证书密钥签发系统审核电力通信终端标识通过后，为其签发设备证书并通过电力鉴别服务单元、电力无线接入点将证书返回给电力通信终端，终端验证证书有效性后，将证书保存至安全芯片中。

9.4.2.2 电力无线接入点证书申请

电力无线接入点的证书申请流程与电力通信终端相同。

9.4.2.3 电力无线接入控制单元证书申请

电力无线接入控制单元的证书申请流程与电力通信终端相同。

9.4.2.4 设备认证流程

a) 电力通信终端使用芯片中的私钥对关键数据进行签名，并将签名信息发送至电力无线接入点；
b) 电力无线接入点使用芯片中的私钥对关键数据进行签名，并将自己的签名信息与电力通信终端的签名信息一起发送至电力鉴别服务单元；
c) 电力鉴别服务单元对终端和接入点的签名及证书有效性进行验证，验证通过后生成鉴别结果并对结果进行完整性保护，将鉴别结果返回电力无线接入点；
d) 电力无线接入点对鉴别结果的来源有效性和完整性验证通过后，判断电力通信终端身份的有效性，有效则将验证结果发送给电力通信终端并进入下一步，无效则终止认证过程；
e) 电力通信终端对鉴别结果的来源有效性和完整性验证通过后来判断电力无线接入点身份的有效性，有效则双向认证通过，无效则双向认证失败。

9.4.3 证书更新申请要求

证书更新申请过程如图 3 所示：

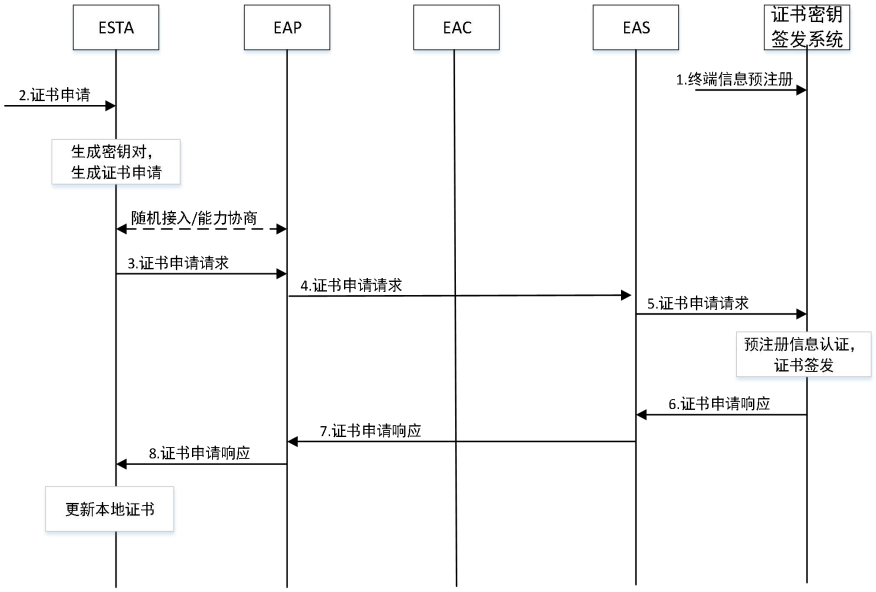

图3 证书更新申请流程

终端证书申请要求如下：

a) 电力通信终端信息预注册，管理员或相关实体通过人工方式将终端信息（如电力通信终端 ID、所有者信息等）在证书密钥签发系统中进行预注册。这是为了确保申请证书的电力通信终端是已知和可信的；

b) 电力通信终端采用自动或人工方式，发起证书申请过程；

c) 电力通信终端入网，向电力无线接入点发出证书申请请求，请求中包含电力通信终端 ID 信息、预注册挑战以及证书申请信息；

d) 电力无线接入点向电力鉴别服务单元转发电力通信终端证书申请请求；

e) 电力鉴别服务单元收到请求后，对其进行打包，转发给证书密钥签发系统；

f) 证书密钥签发系统收到请求后，首先对电力通信终端的预注册信息进行认证。如果预注册认证通过，证书密钥签发系统会签发数字证书。在签发证书后，证书密钥签发系统会构造一个证书申请响应消息发给电力鉴别服务单元，其中包含签发的证书和其他相关信息；

g) 电力鉴别服务单元收到证书申请响应后，会进一步处理并构造一个响应消息，然后将其发送回电力无线接入点；

h) 电力无线接入点将电力鉴别服务单元发送的证书申请响应消息转发给电力通信终端。电力通信终端收到证书响应消息后，提取出其中的数字证书，并更新本地证书安全存储，结束证书申请过程。

9.4.4 初始鉴权认证要求

初始鉴权认证过程如图 4 所示：

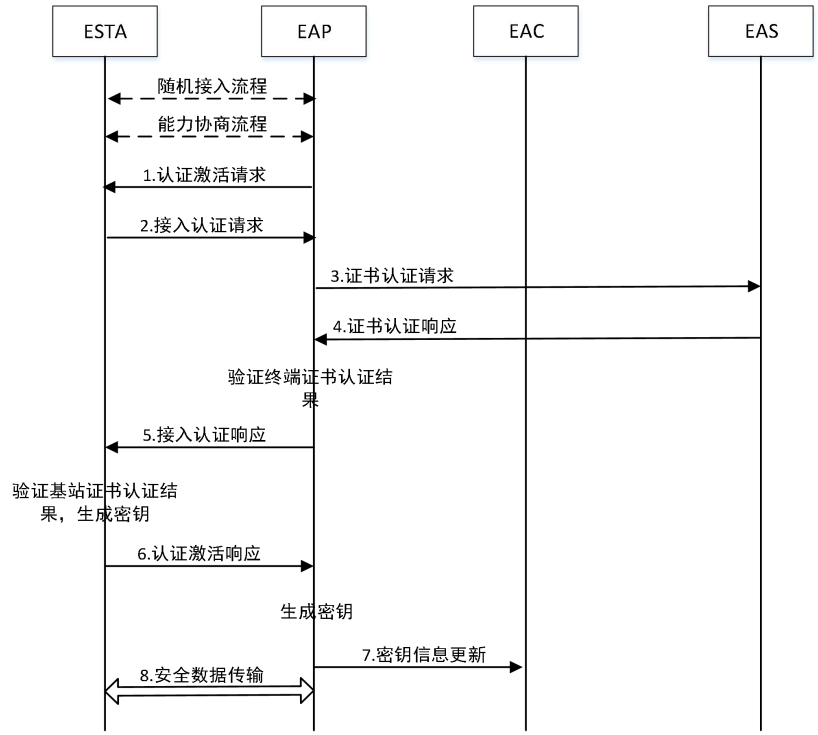

图4 初始鉴权认证流程

初始鉴权认证要求如下：

a) 当电力通信终端空口接入电力无线接入点后，电力无线接入点向电力通信终端发送认证激活请求，以启动整个认证过程；

b) 电力通信终端向电力无线接入点发出接入认证请求，其中包括电力通信终端身份标识、电力通信终端随机数、电力通信终端证书、密钥交换参数等信息；

c) 电力无线接入点在收到电力通信终端的接入认证请求后，向电力鉴别服务单元发出证书认证请求。请求中包含电力通信终端证书、电力无线接入点证书等信息；

d) 电力鉴别服务单元收到电力无线接入点的证书认证请求后，会验证电力无线接入点证书和电力通信终端证书。验证完成后，电力鉴别服务单元将电力通信终端证书认证结果信息、电力无线接入点证书认证结果信息等构成证书认证响应，发送给电力无线接入点；

e) 电力无线接入点收到证书验证响应后，检查电力通信终端证书认证结果，如果证书认证通过，设定电力无线接入点认证结果为成功，构造接入认证响应，发送至电力通信终端；

f) 电力通信终端收到接入认证响应后，检查电力无线接入点证书认证结果。如果证书认证通过，设定电力通信终端认证结果为成功，构造认证激活响应，发送至电力无线接入点。根据密钥导出过程，本地生成密钥；

g) 电力无线接入点将收到认证激活响应后，检查电力通信终端认证结果。如果认证通过，根据密钥导出过程，本地生成密钥，并将相关密钥信息更新到电力鉴别服务单元；

h) 电力通信终端和电力无线接入点之间进行安全数据传输。

9.4.5 漫游切换要求

漫游切换过程如图 5 所示：

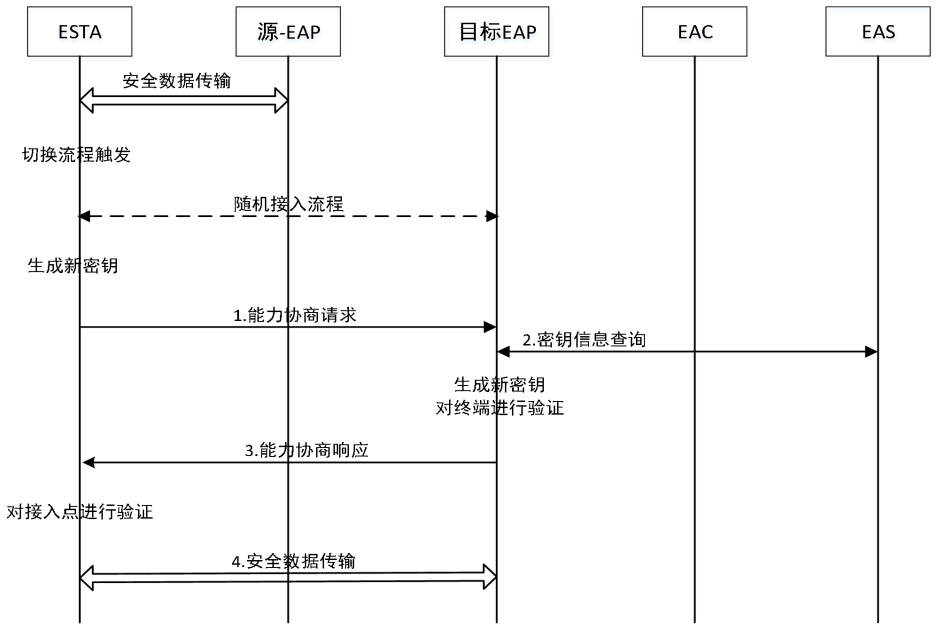

图 5 漫游切换流程

漫游切换要求如下：

a) 当电力通信终端在源电力无线接入点完成认证，进行安全数据传输时，触发漫游切换流程，电力通信终端在与目标电力无线接入点完成随机接入流程后，基于密钥导出算法生成新密钥，向目标电力无线接入点发送能力协商请求消息，其中包括电力通信终端挑战信息；

b) 目标电力无线接入点接收到能力协商请求消息后，向电力鉴别服务单元发起密钥信息查询过程。如果密钥信息查询成功，通过密钥导出算法生成新密钥，并基于电力通信终端挑战对电力通信终端进行认证。如果电力通信终端认证通过，构造并发送能力协商响应消息给电力通信终端；

c) 电力通信终端接收到能力协商响应消息后，基于电力无线接入点挑战对电力无线接入点进行认证。验证通过后，新密钥生效；

d) 电力通信终端和电力无线接入点之间进行安全数据传输。

9.5 访问控制要求

本项要求包括：

a) 电力无线接入点与电力通信终端应具有基于源或目的 IP 地址、MAC 地址、端口号等信息的业务数据白名单访问控制功能；这一功能能够确保只有符合特定条件的数据包才能被允许通过，从而有效防止未经授权的访问和数据泄露；

b) 电力无线通信终端与业务终端之间应采用技术措施进行设备绑定。通过设备绑定，可以确保电力无线通信终端与特定的业务终端之间建立稳定的连接，防止非法设备接入和数据篡改，从而提高系统的整体安全性。

9.6 数据保护要求

9.6.1 安全等级要求

为确保数据交换的安全性和完整性，应采用国家密码管理部门认可的国密二级及以上等级的芯片，并利用芯片提供的国产商用对称密码算法进行数据加密和校验。数据交换双方必须通过鉴别认证，方可进行后续的数据交换操作。

可按照对MAC帧的完整性和机密性保护能力，从低到高分为的三个安全等级，安全等级见表1，分别满足EPWL在不同业务场景下的安全要求：

a) 等级一：仅提供数据帧机密性和完整性保护，可用于不涉及控制信令或敏感信息传输的业务场景；
b) 等级二：可提供数据帧和管理帧的机密性和完整性保护，可用于涉及传输线路和设备参数、地理位置信息等敏感信息的业务场景；
c) 等级三：全面提供数据帧、管理帧和控制帧的机密性和完整性保护，可用于涉及物联器件控制的业务场景。

表 1 EPWL 接口安全等级分类

安全等级	数据帧		管理帧		控制帧	
	机密性	完整性	机密性	完整性	机密性	完整性
等级一	√	√				
等级二	√	√	√	√		
等级三	√	√	√	√	√	√

9.6.2 管理帧、控制帧加密方式

管理帧、控制帧加密采用两阶段加密方式，加密流程如图6所示。

a) 采用预共享密钥方式，确保通信双方在没有进行复杂密钥交换的情况下，能够快速安全地加密管理帧、控制帧。主要包括两部分信令交互过程：一是鉴权认证完成之前的入网管理帧通信过程进行加密，一是对承载初始鉴权认证信令的管理帧、控制帧通信过程进行加密。采用预置加密密钥的方式、加密算法采用 SM4；
b) 当电力通信终端和电力无线接入点双方完成认证，双方协商出主密钥对管理帧、控制帧进行加密。

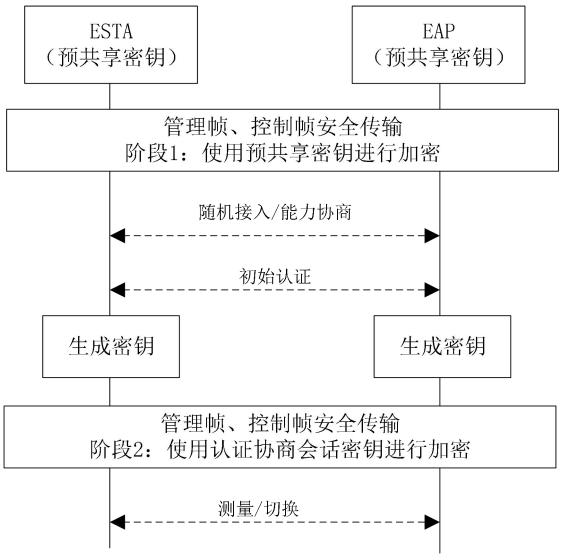

图6 管理帧、控制帧加密流程

9.6.3 数据帧加密方式

认证成功后，通信双方根据相关密钥协商流程，导出基密钥，进而生成会话密钥。采用SM4算法对数据帧进行加密，数据帧加密流程如图7所示。

基密钥可以设置有效期，并在有效期超时后，旧的密钥将不再有效，ESTA和EAP之间应重新进行初始认证过程。新的初始认证过程应对电力通信终端和电力无线接入点的身份进行重新认证，并在重新认证的基础上对基密钥、会话密钥进行更新。

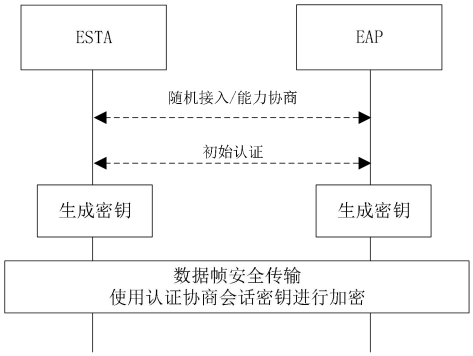

图7 数据帧加密流程

10 空口通信协议要求

10.1 物理层要求

10.1.1 物理层基本要求

EPWL物理层可采用不同编码、调制方式，物理层基本要求：

a) EPWL 物理层在数据加扰、信道编码、速率匹配、空间映射、比特交织、星座调制、空时编码宜采用 GB／T 36454-2018 规范章节 9.2 内容或 GBT26790.2-2015 8 标准中内容；

b) EPWL 调制方式宜采用 GB／T 36454-2018 标准或 GBT26790.2-2015 8 标准中 FHSS/DSSS/OFDM 的调制技术；

c) EPWL 物理层宜采用频分、时分或码分等技术；

d) EPWL 应具备无线信号功率、频率可调节能力。应根据实际应用场景，降低信号发射功率或调整工作频率；

e) EPWL 应支持对物理帧长、上下行配比、工作带宽、前导格式、编码调制方式（MCS）、MIMO 天线模式等等序列的参数动态实时可配置功能；

f) EPWL 宜对调制方式中 FHSS 调频序列、DSSS 扩频码长度、OFDM 循环前缀时隙长度、子载波数量等参数进行动态实时调整。

10.1.2 物理层帧格式

a) EPWL 物理层宜采用 GB／T 36454-2018 标准或 GB/T 26790.2-2015 标准中帧格式；

b) EPWL 物理层宜根据场景需求配置短导码、长导码，形成普通、低时延、广覆盖等模式帧格式。普通模式宜采用图8中格式：

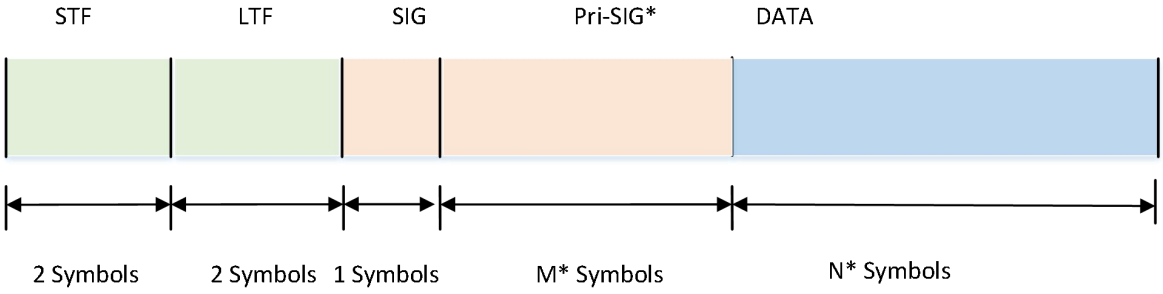

图8 EPWL普通模式帧格式

低时延模式宜采用图9格式：

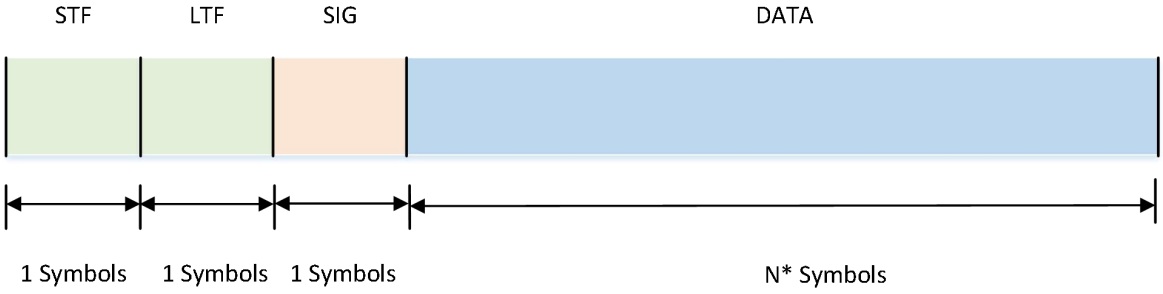

图9 EPWL低时延模式帧格式

广覆盖模式宜采用图10格式：

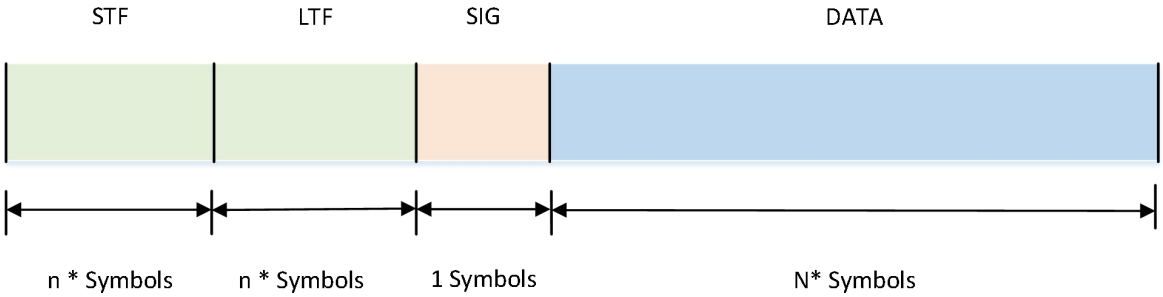

图10 EPWL广覆盖模式帧格式

10.1.3 物理层编码要求

a) EPWL 物理层宜采用 GB／T 36454-2018 标准或 GBT26790.2-2015 标准中编码定义；

b) EPWL 物理层宜根据场景需求配置编码方案 MCS，适应普通、低时延、广覆盖等模式需求。普通模式宜在表2中选择MCS：

表2 EPWL普通模式下MCS配置表

MCS 索引号	调制方式	空间流数量	编码码率	子载波承载编码比特数
0	BPSK	1	1/2	1
1	QPSK	1	1/2	2
2	QPSK	1	3/4	2
3	16-QAM	1	1/2	4
4	16-QAM	1	5/8	4

表 2 （续）

MCS 索引号	调制方式	空间流数量	编码码率	子载波承载编码比特数
6	16-QAM	1	7/8	4
7	64-QAM	1	2/3	6
8	64-QAM	1	3/4	6
9	64-QAM	1	5/6	6
10	64-QAM	1	7/8	6
11	256-QAM	1	3/4	8
12	256-QAM	1	5/6	8
13	256-QAM	1	7/8	8
14	BPSK	2	1/2	2
15	QPSK	2	1/2	4
16	QPSK	2	3/4	4
17	16-QAM	2	1/2	8
18	16-QAM	2	5/8	8
19	16-QAM	2	3/4	8
20	16-QAM	2	7/8	8
21	64-QAM	2	2/3	12
22	64-QAM	2	3/4	12
23	64-QAM	2	5/6	12
24	64-QAM	2	7/8	12
25	256-QAM	2	3/4	16
26	256-QAM	2	5/6	16
27	256-QAM	2	7/8	16
28	BPSK	3	1/2	3
29	QPSK	3	1/2	6
30	QPSK	3	3/4	6
31	16-QAM	3	1/2	12
32	16-QAM	3	5/8	12
33	16-QAM	3	3/4	12
34	16-QAM	3	7/8	12
35	64-QAM	3	2/3	18
36	64-QAM	3	3/4	18
37	64-QAM	3	5/6	18
38	64-QAM	3	7/8	18
39	256-QAM	3	3/4	24
40	256-QAM	3	5/6	24
41	256-QAM	3	7/8	24
42	BPSK	4	1/2	4
43	QPSK	4	1/2	8
44	QPSK	4	3/4	8
45	16-QAM	4	1/2	16

表 2 （续）

MCS 索引号	调制方式	空间流数量	编码码率	子载波承载编码比特数
47	16-QAM	4	3/4	16
48	16-QAM	4	7/8	16
49	64-QAM	4	2/3	24
50	64-QAM	4	3/4	24
51	64-QAM	4	5/6	24
52	64-QAM	4	7/8	24
53	256-QAM	4	3/4	32
54	256-QAM	4	5/6	32
55	256-QAM	4	7/8	32

低时延模式宜在表3中选择MCS：

表3 EPWL低时延模式下MCS配置表

MCS 索引号	调制方式	空间流数量	编码码率	子载波承载编码比特数
7	64-QAM	1	2/3	6
8	64-QAM	1	3/4	6
9	64-QAM	1	5/6	6
10	64-QAM	1	7/8	6
11	256-QAM	1	3/4	8
12	256-QAM	1	5/6	8
13	256-QAM	1	7/8	8
21	64-QAM	2	2/3	12
22	64-QAM	2	3/4	12
23	64-QAM	2	5/6	12
24	64-QAM	2	7/8	12
25	256-QAM	2	3/4	16
26	256-QAM	2	5/6	16
27	256-QAM	2	7/8	16
49	64-QAM	4	2/3	24
50	64-QAM	4	3/4	24
51	64-QAM	4	5/6	24
52	64-QAM	4	7/8	24
53	256-QAM	4	3/4	32
54	256-QAM	4	5/6	32
55	256-QAM	4	7/8	32

广覆盖模式宜在表4中选择MCS：

表4 EPWL广覆盖模式下MCS配置表

MCS 索引号	调制方式	空间流数量	编码码率	子载波承载编码比特数
0	BPSK	1	1/2	1
1	QPSK	1	1/2	2
2	QPSK	1	3/4	2

表 4 （续）

MCS 索引号	调制方式	空间流数量	编码码率	子载波承载编码比特数
4	16-QAM	1	5/8	4
5	16-QAM	1	3/4	4
6	16-QAM	1	7/8	4
14	BPSK	2	1/2	2
15	QPSK	2	1/2	4
16	QPSK	2	3/4	4
17	16-QAM	2	1/2	8
18	16-QAM	2	5/8	8
19	16-QAM	2	3/4	8
20	16-QAM	2	7/8	8

10.2 媒体接入层要求

10.2.1 媒体接入层基本要求

EPWL媒体接入层（MAC）的主要功能是保证EPWL无线设备之间的实时、可靠、安全地传输，媒体接入层的基本要求：

a) 宜采用 TDMA 机制，按照时分模式分配给不同的 ESTA，避免 ESTA 接入碰撞，支持帧聚合/解聚；
b) 媒体接入层管理功能：定义设备加入、离开、时间同步、属性读写等功能；
c) 媒体接入层数据帧格式以及上下行交互协议宜采用 GB／T 36454-2018 标准或 GBT26790.2-2015 8 标准中要求；
d) EPWL 应基于媒体接入层在帧格式、接入机制等方面做安全增强改造，支持管理和控制帧、数据帧加密能力，支持 EPWL 鉴权认证流程，保证协议隐蔽性与安全性；
e) EPWL 应具有基于帧序列号、源地址、目的地址、时序等信息的协议数据安全校验及非法数据检测功能；
f) EPWL 应具有业务 QoS 保障能力。

10.2.2 媒体接入层协议要求

10.2.2.1 寻呼要求

EPWL在采用TDMA机制情况下多电力通信终端同时加入时，网络宜支持对ESTA接入时的时隙分配，宜支持对ESTA的寻呼接入功能，寻呼接入流程如图11所示。

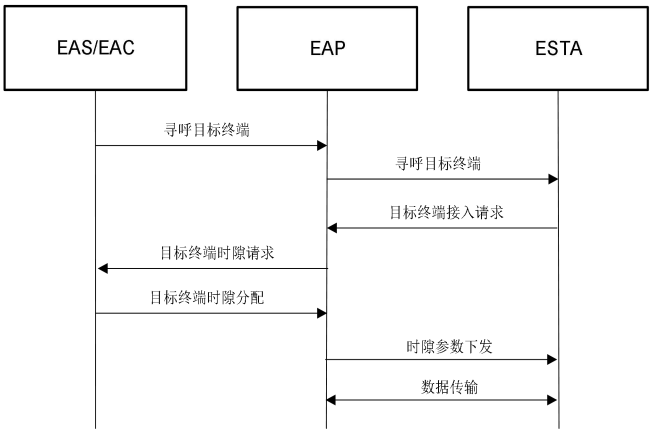

图11 寻呼接入时隙分配流程

寻呼接入流程要求如下：

a) EPWL 网络侧 EAS/EAC 按照业务需求对目标电力通信终端进行寻呼，发送寻呼目标终端命令到电力无线接入控制单元下所有的电力无线接入点；

b) 电力无线接入点接收到寻呼目标终端消息后，向电力通讯终端发起寻呼目标终端的过程；

c) 电力通信终端接收到寻呼目标终端消息后，对消息中的目标终端的身份进行确认验证，确认本终端是寻呼目标终端，则发起电力通信终端接入请求要求到电力无线接入点；

d) 电力无线接入点收到目标终端的接入请求后，向相应的网络侧 EAS/EAC 发起时隙申请请求；

e) 网络侧 EAS/EAC 收到相应的电力无线接入点的时隙申请请求后，根据系统现有资源对电力通讯终端进行时隙分配，并下发时隙参数给电力无线接入点；

f) 电力无线接入点根据时隙参数设置自身配置参数，并下发时隙参数给对应的电力通信终端；

g) 电力通信终端根据下发的时隙参数完成时隙参数配置并进行数据传输。

10.2.2.2 无线级联要求

EPWL宜支持EAP、ESTA之间通过无线方式实现多点级联数据传输功能，级联长度不小于4节点。级联数据传输流程如图12所示。

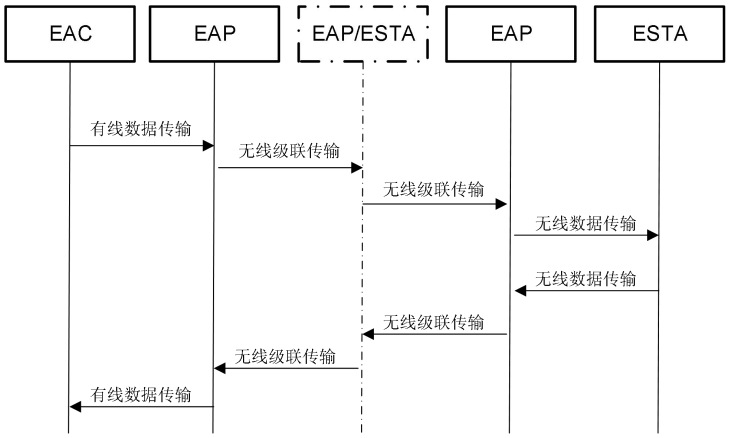

图12 EAP、ESTA无线多点级联数据传输

10.2.2.3 帧内应答要求

EPWL 系统采用 TDD 双工机制时，宜采用具有在本帧内含有数据传输应答功能的帧结构。实现帧内符号级的调度控制、帧内快速反馈和确认、流水线式信号处理，实现数据本帧内的数据重传，提升系统数据传输的可靠性，帧内应答机制如图 13 所示。

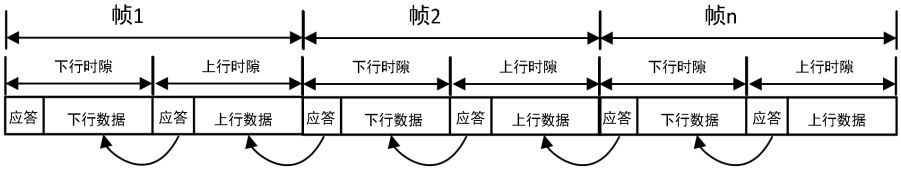

图 13 EWPL 帧内应答机制

11 设备要求

11.1 接口要求

11.1.1 接口类型

电力通信终端的接口类型包括以太网接口、RS232、RS485接口等。其中基于以太网接口的电力通信终端具体要求包括：

a) 设备地址设置应满足唯一性、可管理性、连续性和可扩展性的要求；
b) 设备地址包括网络设备管理地址、通信终端地址两类，每台网络设备应设置 1 个设备管理设备地址；
c) 电力鉴别服务单元应分配数据通信网信息 VPN 或通信专网 IP 地址；接入点控制单元、无线接入点应分配数据通信网信息 VPN 的 IP 地址，接入层与核心层之间通过通信专网互联时，还应分配通信专网 IP 地址；
d) 可统一规划数据通信网信息 VPN 的 IP 地址，也可自行规划其他可用的私网 IP 地址。采用私网 IP 地址时，应支持通过 NAT 协议完成私网地址与数据通信网信息 VPN 地址的转换。

11.1.2 接口安全

本项要求包括：

a) 应能够通过安全技术手段或管理手段，按最小化原则开放接口，并对开放的接口采取安全管控措施；
b) 应禁用所有无关的无线通信模块；
c) 应采取技术措施实现通信终端与业务终端的绑定。

11.2 环境要求

规定EPWL系统工作于变电站、换流站等场景的温度、湿度、电磁干扰等环境要求。

11.2.1 环境适应性

设备环境适应性应满足GB/T 15153.2的贮存和使用气候条件分级C2及以上级别要求，在规定的气候条件下应能正常工作。

11.2.2 湿热

室外型的电力无线接入点应能承受GB/T 2423.3规定的恒定湿热试验，在30℃温度、95%湿度条件下，试验后各导电回路对外露非带点导电部位及外壳之间、电气上无联系的各回路之间的绝缘电阻不应小于1.5MΩ。

11.2.3 绝缘性能

设备绝缘性能应满足GB/T 14598.3中规定要求，绝缘性能试验结束后设备应能正常工作。

11.2.4 机械性能

设备机械性能要求应符合GB/T 15153.2中Cm等级的要求，试验结束后设备应无损伤，应能正常工作。

11.2.5 电磁兼容

11.2.5.1 抗干扰性能

抗电磁干扰能力应满足DL/T 860.3的相关要求，设备至少应通过表5所包含的电磁兼容类试验。

表 5 抗干扰性能要求和试验

序号	试验	参考标准	严酷等级	
			室外设备	室内设备
1	静电放电抗扰度	GB/T 17626.2	4 级	3 级
2	射频电磁场辐射抗扰度	GB/T 17626.3	3 级	3 级
3	电快速瞬变脉冲群抗扰度	GB/T 17626.4	4 级	3 级
4	浪涌（冲击）抗扰度	GB/T 17626.5	4 级	3 级
5	射频场感应的传导骚扰抗扰度	GB/T 17626.6	3 级	3 级
6	工频磁场抗扰度	GB/T 17626.8	5 级	5 级
7	脉冲磁场抗扰度	GB/T 17626.9	5 级	5 级
8	阻尼振荡磁场抗扰度	GB/T 17626.10	5 级	5 级
9	交流电源暂时中断抗扰度	GB/T 17626.11	500ms	500ms
10	振荡波抗扰度	GB/T 17626.18	3 级	3 级
11	0Hz~150kHz 共模传导骚扰抗扰度	GB/T 17626.16	3 级	3 级
12	直流电源暂降、暂时中断抗扰度	GB/T 17626.29	100ms	100ms
注 1：评价等级均采用 A 类判据。 注 2：室内设备适用于机房和办公室环境，室外设备适用于楼道和室外等应用环境。 注 3：序号为 5、6、7、8、11 的试验为在变电站环境下增加的测试项目。				

11.2.5.2 无线电骚扰限值

无线电骚扰限值应符合GB/T 9254.1对B级设备的相关规定。

11.2.6 外壳防护

室外型设备应满足GB/T 4208标准中定义的IP67等级。

室内型设备应满足GB/T 4208标准中定义的IP20等级。

附 录 A
（资料性）
无线接入点覆盖方案

A.1 室外开阔地

室外开阔地可采用全向天线或定向天线，典型覆盖方案见表A.1，频宽宜使用20MHz。

表 A.1 室外开阔地典型覆盖方案

场景	推荐天线类型	安装方式	覆盖方案
立杆部署	全向天线、定向天线	落地抱杆	全向天线挂高 2m~3m，覆盖半径约 40m~50m，部署间隔约 70m~90m； 定向天线挂高 3m~5m，覆盖距离约 80m~100m。
		楼顶抱杆	全向天线挂高 2m~3m，覆盖半径约 50m~70m； 定向天线挂高 3m~5m，覆盖距离约 90m~110m。
墙壁部署	全向天线、定向天线	挂壁	全向天线挂高 2m~3m，覆盖半径约 40m~50m，部署间隔约 70m~90m； 定向天线挂高 3m~5m，覆盖距离约 80m~100m。
注：覆盖半径和覆盖距离按照无线电管理部门规定的发射功率限值计算。			

A.2 室外遮蔽区域

室外遮蔽区域可采用全向天线或定向天线，典型覆盖方案见表A.2，频宽宜使用20MHz。

表 A.2 室外遮蔽区域典型覆盖方案

场景	推荐天线类型	安装方式	覆盖方案
立杆部署	全向天线、定向天线	落地抱杆	全向天线挂高 2m~3m，覆盖半径约 20-30 米，部署间隔约 30-40 米。
		楼顶抱杆	全向天线挂高 2m~3m，覆盖半径约 40-50 米；定向天线覆盖距离约 50-60 米。
墙壁部署	全向天线、定向天线	挂壁	全向天线挂高 2m~3m，覆盖半径约 20-30 米，部署间隔约 30-40 米。
注：覆盖半径和覆盖距离按照无线电管理部门规定的发射功率限值计算。			

A.3 室内区域

室内区域采用内置全向天线，典型覆盖方案见表A.3。室内覆盖场景下宜使用40MHz频宽，室内多隔断覆盖场景下可使用80MHz频宽。

表 A.3 室内区域典型覆盖方案

场景	推荐天线类型	安装方式	覆盖方案
室内设备区域	室内内置全向天线	挂壁	天线挂高≥2m，部署间距约 25m~30m。
室内办公区域	室内内置全向天线	吸顶	天线挂高≥2m，部署间距约 10m~12m。
注：部署间距按照无线电管理部门规定的发射功率限值计算。			