[配电网]

基于域信任管理的配电物联网通信与网络安全防护技术架构研究

文/李毅超[1] 高 毅[2] 刘辛彤[1] 王旭蕊[1]
1. 国网河北省电力有限公司信息通信分公司；2. 国网河北省电力有限公司东光县供电分公司

基于配电物联网的接入技术需求，从电力线载波通信技术、高速载波通信、光纤通信技术和无线通信技术四个角度对配电物联网中采用的主要技术进行分析阐述，对上述技术进行优势、劣势分析，并对其在配电物联网中的应用效能进行对比，同时提出了一种改进型的基于域信任管理的安全防护技术架构。

配电物联网是通过各类信息传感设备，在达到配电网电气设备与人员之间相互连接效果的同时，与现有的网络信息技术、电子技术相结合，最终形成一个规模庞大的智能配电网络，提高配电网的安全性、稳定性及可靠性，为用户提供更优质的配电服务体验。随着电子信息技术和通信技术的快速发展，配电物联网的建设水平也在持续提升。在此背景下，对配电物联网通信技术进行研究分析，进而为配电网的实时控制、在线检测和自动恢复提供一定理论参考，有一定的现实意义。

配电物联网及通信技术概述

1. 配电物联网功能概述

随着我国电力产业迅猛发展，如何提升电力产能及配置系统一直备受关注。电力系统在运行发展中需应用各种新技术、新模式。配电物联网模式是基于传统工业技术，经过网络与物联技术的融合植入，形成一种具有综合性、可控性的新型电力网络形态，实现配电网中设备之间的资源共享、数据传输，并开展实时互通与互动操作。实现整体配电网的全面智能感知、信息互动及数据融合，是推动配电网智能应用与体系建设的重要环节。配电物联网的实际应用实现了配电网的精准、智能管理，从配电物联网整体架构与功能层面分析，主要以“云、管、边、端”架构为主。管理层面负责配电物联网云、边、端各层面的信息传输，是其主要的承载体，并负责配电物联网中的相关项目业务。经分析后发现，配电物联网通信技术是主要以远程通信+本地通信网络为主的设计架构，该设计架构满足边端设备的通信需求，为“即插即用”，可实现配电业务的时效性处理。

2. 配电物联网通信技术架构

现阶段我国配电物联技术与体系建设逐渐向智能化转型，各类业务量的增加与新项目的开展对业务数据的传输稳定和可靠安全提出了更高的要求。基于此，当下对配电物联网通信性能的要求更强。结合实际需求，配电物联网通信架构主要以远程通信接入网、本地通信接入网为主，二者从远程及本地两方面发挥对配电物联网数据传送的作用。配电云平台、边缘计算终端的通信要求相对较高，通常必须满足其安全可靠、低效时延和差异并存的通信要求。从综合角度来讲，远程通信接入网负责对外的全部信息及数据

基金项目：2021—2022年国网河北省电力有限公司科技项目项目《基于多技术融合的实时动态感知的配电网支撑关键技术研究支持》（5204XA20004K）

输送，本地通信接入网是负责边缘计算终端与低压智能设备之间的所有业务数据的传送通信工作，要求稳定可靠、安全快速。在通信方式中，远程通信网以光纤、电力无线专网、无线公网4G/5G、北斗卫星等为主，本地通信网以高速载波通信（HPLC）、微功率无线、HPLC+RF双模通信等为主。

配电物联网网络架构及主要通信技术

1. 配电物联网网络架构

配电物联网网络架构如图1所示。

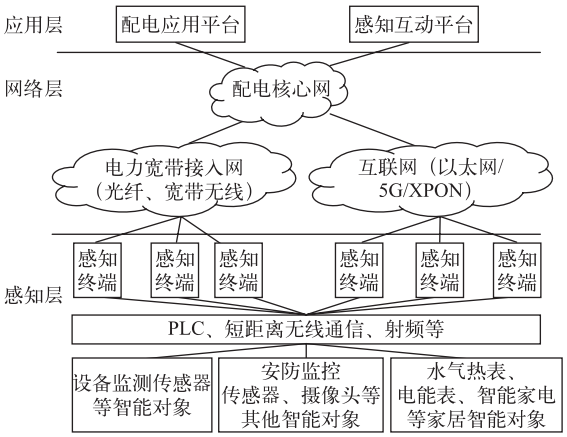

图1　配电物联网网络架构图

2. 配电物联网主要通信技术

（1）电力线载波通信技术

电力线载波通信技术是一种以高压电力线、中压电力线以及低压电力线为信息传输媒介进行语音、图像、数据等业务传输的通信技术，主要应用于电力负荷监控、远程抄表、配电网自动化、需求侧管理等电力生产业务，在应用过程中体现出方便快捷和经济可靠等优势，是实现配电网通信的最佳技术手段之一。在实际应用中需对业务开展的适应性进行明确，低压窄带载波通信技术优势极为明显，如：不必开展额外的布线加设，整体施工周期相对较短；技术本身及操作也相对简单、成熟，建设经济性较高；通信可靠性较高，支持自组网功能。劣势在于其通信带宽相对窄，可能受到窄带宽干扰，导致通信速率不高，无法有效实现低时延支撑，在相对高频次数据传输过程中会发生大功耗情况，受限于电池供电或低功耗情况。

（2）高速载波通信技术

随着配电物联网技术不断发展，通信技术的多元化模式日益突显。高速载波通信技术作为一种新型通信技术，在整个配电物联网数据与信号传送中起着较大作用。其优点如下：高速载波通信技术无须通过额外布线方式开展，在信号传送中通过简单的电力线便可完成；在施工周期方面不存在过度耗时，整个施工期较短，同时在抗电力线噪声、抗信道衰落效果等能力较强；传送与效率及带宽方面也明显提升，在传送延时方面实现毫秒级；在修复方面可满足链路修复需求，使网络可实现自动恢复；在运维方面降低相关成本投入，可进行自动组网等。劣势主要体现在前期成本投入较高，在功耗方面，如控制不合理也会存在高耗量问题，同时对电力连接较为依赖，整体独立性不强。

（3）光纤通信技术

光纤通信技术可以通过光波实现信息感知和信息传输，且两种工作活动可以同时进行。光纤通信技术在配电物联网应用中可以对配电网的线路及设备的温度、压力、电压、电流和振动等多种信息进行采集，并以光波作为媒介进行信息传输。结合实际情况来看，相较于电力线载波通信技术，光纤通信技术常用于更宽的带宽，使其在应用过程中可以将更大数据量的信息进行远程传输，并且由于光纤通信技术的感知媒介和信息媒介均为光波，因此在使用过程中不易受到电磁干扰，使得该技术可以在更为复杂的环境中使用；同时在应用时能量损耗更低，再加上光纤通信技术的制作材料储量相对充足，实际生产成本较低，多角度综合考虑光纤通信技术在配电物联网中应用时的成本更低。

（4）无线通信技术

1）ZigBee技术。ZigBee技术采用IEEE 802.15.4标准，主要应用于自动控制领域和远程控制领域。在具体应用过程中，可在配电物联网中嵌入ZigBee无线通信模块的传感器节点，然后这些节点将会自行组网，具有较强的便捷性，可以实现配电物联网的大规模监测；对于ZigBee技术的远程控制，需要通过树形拓扑结构组网方式构建ZigBee网络，该网络不仅具备ZigBee原本的技术优势，还可以将原有低速短距离传输特点的ZigBee技术用于远距离传输中。在电力领域，基于ZigBee技术所构建的无线网络可以对电力设备运行状态进行实时监测，并表现出一定的应用效果。

2）WiFi技术。WiFi技术采用IEEE 802.11a/b/g/n/ac/ax等技术标准，采用不同技术标准的WiFi技术的实际速率也不尽相同，其中于2019年发布的IEEE 802.11ax技术标准可使WiFi技术的最高速率达到11 Gbit/s，但无论是采用何种技术标准的WiFi技术，其实际工作频段均为2.4 Hz和5G Hz频段。WiFi技术作为一种短距离无线通信技术，可以实现数十米范围的网络覆盖，其最大优势在于数据传输速率较高，并且可以在信号较弱或者有干扰的情况下自动调整带宽，保障数据传输的稳定性和可靠性。

3）蓝牙技术。蓝牙技术在研发初期主要用于RS 232传感数据线的衍生替补，在后续应用过程中表现出开放性、低成本、支持短距离无线通信等特点，实际工作频段为2.4 Hz频段。传统蓝牙传输距离将近15 m，最新的BLE4.0版本的蓝牙传输距离甚至能够达到150 m，主要应用在标签定位、资产跟踪、运动及健身传感器、医疗传感器、智能手表、遥控器及个人办公手持设备的无线互联等。不同短距离无线通信技术对比见表1，本地通信网通信方式技术参数对比分析见表2。

表1　不同短距离无线通信技术对比

名称	常用频段/GHz	价格	通信距离/m	功耗	安全性	优点	缺点
ZigBee	2.4	低	1～50	低	高	可自行组网	兼容差，普及率低
WiFi	2.4和5	高	1～200	高	低	易实现，受众广	功耗大，体积大
蓝牙	2.4	低	1～15	低	高	体积小，受众广	连接能力弱

表2　本地通信网通信方式技术参数对比分析表

分类	低压宽带载波	高速载波	无线通信技术	光纤通信技术
通信速率/（Kbit/s）	<40	<1	<250	<100
通信时延	百毫秒至秒	<20 ms	<30 ms	<50 ms
传输距离/m	<300	<400	75	<500
接入数量	256～1 024	1 100+	254	1 000
安全性	较高	较高	较高	较高
可靠性	较高	高	高	高
成本	较低	较高	较高	较低
部署周期	短	短	短	短
技术商用程度	成熟	较成熟	成熟	成熟

综上，无线通信技术是未来电力信息化发展的重要手段，在电力行业的应用也越来越深入，目前电力设备逐步多样化，产生了更多新的需求。在如此大规模的接入端中，无线通信技术的优势逐渐体现，解决了用户终端与电力信息网络连接的关键技术问题，也解决了网络用户最后一站的数据采集问题，无线通信技术正逐步成为电力通信网的重要组成部分，在电力传输、电力网络应用等方面逐渐扩大应用。尽管无线通信技术存在很多的优势，但是相对有线通信，它也存在一定的劣势，就是安全接入的问题。在现在电力系统建设中，电力通信要求保密等级高、安全可靠性高，如果接入方式多，且无法统一标准，将直接影响无线通信的稳定性，阻碍无线通信的发展。

无线通信安全技术研究

1. 无线接入安全措施

无线接入技术在不断的发展中日趋完善，伴随工业的发展，无线接入技术也不断发展，接入设备的性能也不断提升，工作协议逐渐规范完善，不断有新的技术涌现，无线接入的安全问题得到了很大的提升。在电力行业，随着无线通信技术逐渐在电力通信领域的广泛应用，针对无线通信的渗透和攻击也越来越多，通常采用的安全措施主要包括以下几个方面。

（1）安全认证与鉴别技术

传统的无线网络主要的安全防护需求包括机密性和完整性，电力无线网络还需要满足电网业务相关的安全防护需求。身份认证技术是通信双方进行的可信身份验证，主要提供身份证明和验证的过程，在实际的操作中，主要是对用户提供的身份数据进行甄别，利用数字签名技术，对密钥进行管理分配，并对各种身份涉及的权限进行精确的设定，允许合法的用户使用相对应的权限，对不合法的用户进行阻断和报警，防止非法用户进一步的入侵。

（2）安全接入技术

协议安全是指利用协议的复杂性对数据加强保护，防止在传输的过程中被入侵者截获并破解。协议之间通过密钥的方式建立通信，并通过密钥来确认发送消息的唯一性、机密性、完整性和非否认性，这都是密码学发展所需要解决的问题。

终端安全模块通常具有双向认证加密能力，能够对来自上级的控制命令和参数设置进行鉴别，对相关数据的来源进行认证，并对相关数据的完整性进行验证。上传至调度中心的数据，通过终端安全模块后生成校验密钥，供调度中心使用相关计算机算法进行校验。

从数据加密方向提高传输数据的安全性，能够从根本上消除安全隐患，即使截获了数据也无法破解，保证了数据的安全。目前数据加密的主要算法有数据加密标准（DES算法）和公开密钥加密算法（RSA算法）两种。另外还有Fertzza、Elgama 加密等。但这些算法都没有在电力行业大规模的应用，只用于密钥分配和数字签名等部分领域。

2. 基于域信任管理的网络安全防护架构研究

根据配电网电压等级和电网公司运营管理特点，结合电网运行、设备运维、客户服务等分立体系将配电网划分为主站域、线路域、台区域、应用域和用户域五个信息域。通过信任管理，将五个域结合建立一个信任空间。该信任空间既能满足各类用户的合法需求，又能实现各域的信息交流，如图2所示。

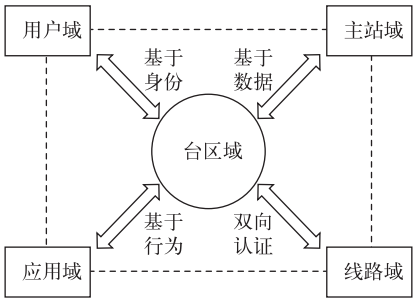

图2　基于域信任管理的网络安全防护架构

各域之间使用用户口令、指纹等多种方式实现信任，该信任是基于身份认证的方式实现的。应用域上的各种应用根据数据加密等方式与各域之间建立信任关系，这种信任是建立在基于行为认证的方式实现。台区域与线路域之间通过双向认证的方式建立信任机制，避免冒名攻击、假冒基站的可能性。主站域同台区域使用加密算法对数据进行加密，建立信任关系。最终实现对配电网的信任管理。

结束语

综上所述，通过对上述通信技术进行比较，从配电物联网构建及功能应用层面分析，保障电力数据传输的稳定性及信号安全性尤为关键。在该基础上可提升网络信号传输的强度适应性，将自动化与智能化进行体现，对传统通信技术进行创新升级。经过分析与对比后得出，无线通信技术整体效果较好，在通信速率、通信时延、传输距离、接入数量、安全可靠性、成本、部署周期和技术商用程度等方面适应性较强，可满足配电物联网整体传送及实时通信要求。针对电力系统建设中电力通信要求保密等级高、安全可靠性高等安全接入问题，提出了一种基于域信任管理的网络安全防护架构。在主站域、线路域、台区域、应用域和用户域之间实现数据的可信聚合，以扁平、灵活和高效的软件定义方式快速满足形态多样的业务融合和快速变化的安全服务要求。在此架构下最大程度实现业务功能的前提下，如何提供有效的安全保障是下一步需要研究的课题。EA

（收稿日期：2022-11-23）

参考文献

[1] 高雁．基于ZigBee技术的无线传感网络定位系统的研究[D]．南京：南京邮电大学，2019．

[2] 陈士龙，陈浩．基于物联网的智能变电站在线监测系统研究[J]．山东工业技术，2017(5)：116-117．

[3] 李宜才．物联网技术在配电网运维管理中的应用及研究[J]．南方农机，2020，356(16)：168-169．

[4] 王鹏，林佳颖，宁昕，等．配电网全景信息感知架构设计 [J]．高电压技术，2021，47(7)：2 293-2 302．

[5] 庞继福．基于CPS的区域能源网络信息安全防护技术研究[D]．保定：华北电力大学，2018．

[6] 赵辉，支瑞峰，徐保红，等．基于窄带物联网(NB-IOT)的低压配电用户侧状态评估技术研究[J]．电气应用，2022，41(1)：41-46．