



5G 物联网和边缘计算的智能电网安全方案^{*}

陈旗展

(南方电网广东中山供电局, 中山 528400)

摘要: 智能电网需要高速、可靠的通信, 以通过物联网设备实现实时电网监测, 5G 可以视为将当前电力网基础设施转变为智能电网的催化剂, 因此了解 5G 在基于物联网的智能电网中的网络安全方面的优势对于设计决策和未来的风险分析工作至关重要。本文探讨了一个关于自动电压控制的智能电网用例, 该用例利用 5G 作为具有边缘支持的无线通信基础设施, 确定了 5G 在安全方面带来的优势, 展示了 5G 安全技术如何适用于智能电网, 从而为未来 5G 智能电网系统的安全分析提供基础。

关键词: 5G; 边缘计算; 物联网; 智能电网

中图分类号: TP391

文献标识码: A

Secure Solution for Smart Grid Based on 5G Internet of Things and Edge Computing

Chen Qizhan

(China Southern Power Grid Guangdong Zhongshan Power Supply Bureau, Zhongshan 528400, China)

Abstract: Smart grid requires high-speed and reliable communication to enable real-time monitoring through Internet of Things devices. 5G can be seen as a catalyst for transforming the current power grid infrastructure into a smart grid. Therefore, understanding the advantages of 5G in terms of network security in IoT-based smart grids is crucial for design decisions and future risk analysis. This paper explores a use case of intelligent power grid with automated voltage control, utilizing 5G as a wireless communication infrastructure with edge support. It identifies the advantages of 5G in several security aspects and demonstrates how 5G security technologies can be applied to smart grids, providing a foundation for the security analysis of future 5G smart grid systems.

Keywords: 5G; edge computing; Internet of Things; smart grid

0 引言

电网是国家关键基础设施的重要组成部分, 全球研究人员和能源公司正在将其转变为智能电网, 以实现减排目标。智能电网利用物联网设备提高可靠性、监控功能和资产管理, 并依赖高速通信网络^[1], 然而智能电网领域面临成熟度低、标准差异和安全担忧等挑战^[2]。5G 网络被认为是推动电网数字化的关键, 可提供物联网连接、低延迟和高可靠性^[3], 然而从网络安全角度来看, 相关研究数量仍然有限^[4]。

本文旨在研究 5G 网络对物联网设备安全性和智能电网通信的影响。通过一个智能电网用例的分析, 强调了 5G 连接的重要性, 用例涉及电压调节技术, 并确定了关键的安全需求。通过分析现实挑战, 考虑 5G 技术的缓解作用, 提出了威胁模型, 展示了 5G 如何支持用例并讨论了潜在的新威胁。

1 选择一个现实智能电网用例

本文以智能电网为例, 探讨 5G 在物联网设备与智能电网通信中的安全潜力。在电力系统中, 无功功率调节电网电压, 影响电力流动。无功功率是交流电压作用于电容负载或功率电子器件时产生的。大型发电机组是电网电压的主要控制源, 但其数量正在减少, 而分布式发电机组 (如风力涡轮机) 和太阳能电池板的数量正在增加, 这些分布式发电单元还影响电压水平的快速变化。为维持电压水平, 需要新的无功功率资源、增强输电系统操作者 (TSO) 和配电系统操作者 (DSO) 之间的协作。

参考文献[5]的用例展示了如何优化电力/电压管理方案, 该方案评估无功功率资源, 用于抵消由 RES 引起的电压违规, 并提升分布式网格的 RES 托管能力。若要实现这一目标, 需要在 TSO 和 DSO 控制室之间建立通信基础设施, 并覆盖各自网络中的传感器和控制器。

电力系统辅助服务有质量要求, 通信基础设施需满足延迟、带宽、可靠性和安全性要求。电压控制的反应时间

^{*} 基金项目: 国家自然科学基金项目(61472458)。

约为 2 分钟,延迟不太影响。带宽通常不拥挤,但通信安全性可能存在问题,需防止传感器测量和设定点的恶意更改。除了考虑状态估计相关的测量传感器外,电压控制服务可能涉及到以下参与者:负载和发电预测单元、TSO 最优电力流、TSO SCADA/状态、TSO 分接开关、FACTS、DSOOPF、功率补偿装置、发电机控制器、DSO DG 和 RES 本地控制器。图 1 说明了用例基于物联网的架构。

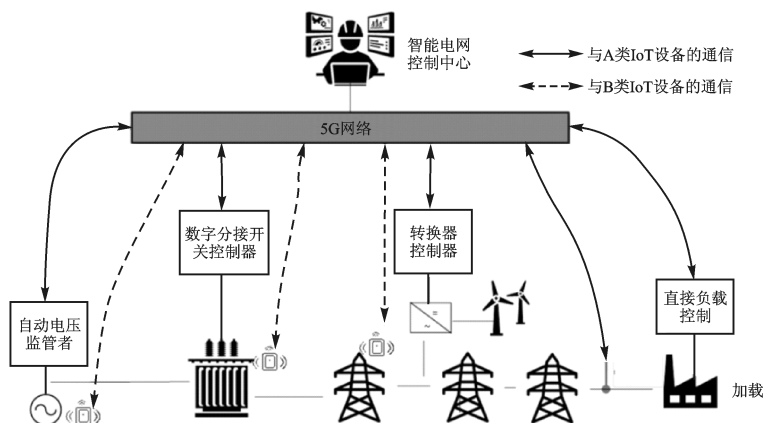


图 1 电压控制用例中 A 型和 B 型物联网设备的通信

2 分析安全要求和威胁

2.1 安全要求

许多研究涵盖了智能电网的网络安全要求,本文重点关注以下无线通信安全需求:①身份验证,物联网设备需要支持轻量级、相互身份验证,需要可扩展的密钥交换机制和数据加密;②隐私,通过各种无线技术通信时,要保护客户和系统数据的隐私;③可用性,为物联网设备提供强大且始终可用的连接;④机密性,通信协议需确保物联网数据的机密性;⑤完整性,保护空中传输数据的完整性。

这些要求对于保护与智能电网相关的主要信息资产至关重要,如电压、电流、温度读数和控制信号。本文专注于通信网络和 5G 的潜在作用,而不涉及针对物联网设备本身的威胁。将物联网设备分为两种类型:类型 A,如自动电压调节器,具备 5G 连接;类型 B,如温度传感器,使用其他无线技术,并通过 5G 网关传输数据。

2.2 威胁模型

潜在的攻击可以分为以下几种类型:需要物理访问的本地攻击、无线攻击和远程攻击。本文主要考虑本地无线攻击和远程攻击。本地无线攻击的主要动机可能包括获取 IoT 设备的精确位置,尝试拦截或修改 5G 无线通信流量,或否认向 IoT 设备提供 5G 无线通信服

务。远程攻击的主要动机可能包括试图破坏与 5G 无线电或核心网络相关的组件,窃取智能电网相关的关键信息,或通过已损坏的 5G 网络元素对 IoT 设备进行攻击。

本文采用 Microsoft 的威胁建模方法,首先根据数据流程图(图 2)对系统进行建模,然后使用 STRIDE(欺骗、篡改、否认、信息泄露、拒绝服务、权限提升)助记符来识别系统的主要威胁。STRIDE 与安全需求相关:欺骗关联到认证,篡改关联到信息完整性,否认与所有需求都有关,信息泄露关联到机密性和隐私,拒绝服务关联到可用性,权限提升涉及攻击者提升其访问权限,可能违反任何安全需求。

本文对每个信任边界都使用 STRIDE,查看穿过该边界的数据流,因此威胁模型是以通信为中心的设计。图 2 确定了 3 个信任边界:在控制室和物联网网关之间(标记①)、在物联网网关和“第三方服务”之间(标记②)、在物联网网关和 DG 控制器之间(标记③)。第三方服务可以是云服务、供应商、其他 IoT GW 或不属于此安装的其他 IoT 设备。

假设攻击者将馈线末端的电压读数降低到被控制室视为欠电压的水平。最佳的无功资源管理系统将计算消除视为欠电压的电压分接开关位置。结果将是当分接开关增加电压时,馈线末端的实际电压增加到导致总停电的严重过电压点。通过协同努力可以创建相同的停电状态,其中电压调节设备的设定点设置为它们所有的过电压点。例如可以通过操纵从控制室(图 2 中的信任边界①)或从 IoT GW(信任边界③)传递的设定点来实现这一点。

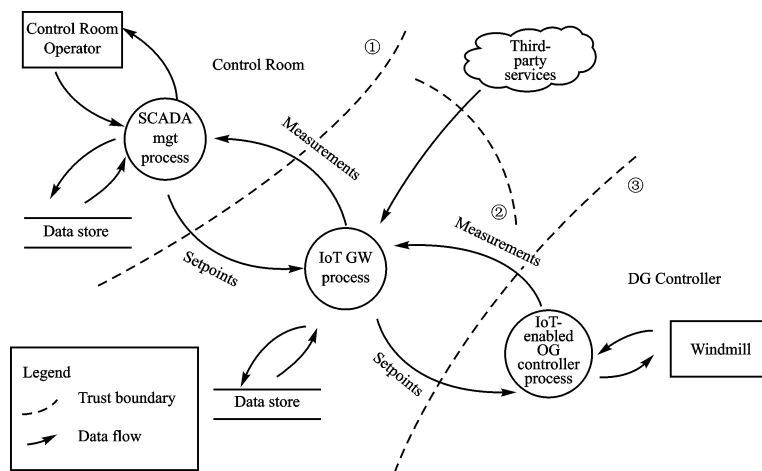


图 2 无功功率用例的数据流程图

3 在智能电网用例中实现 5G 上的安全物联网

A 类和 B 类设备通过多接入边缘计算主机 (MECH) 和 5G 核心网络使用 5G 无线电基站连接到智能电网控制

中心(SGCC)。5G 核心网络由许多不同的元素组成,但大部分不在本文的讨论范围内。我们描述了一些负责向物联网设备提供安全和隐私相关功能的核心网络元素。特别是提到了身份验证服务器功能(AUSF)、统一数据管理(UDM)、网络曝光功能(NEF)、会话管理功能(SMF)和接入/移动性管理功能(AMF)。智能电网控制中心托管在智能电网基础设施中,并通过 5G 核心网络从物联网设备接收数据。SGSC、MECH、5G RAN 和 5G 核心网络之间的接口 I_a 、 I_b 、 I_c 和 I_d 通过专用网络连接(如图 3 所示)或者按照 3GPP 5G 安全规范指定的方式连接。

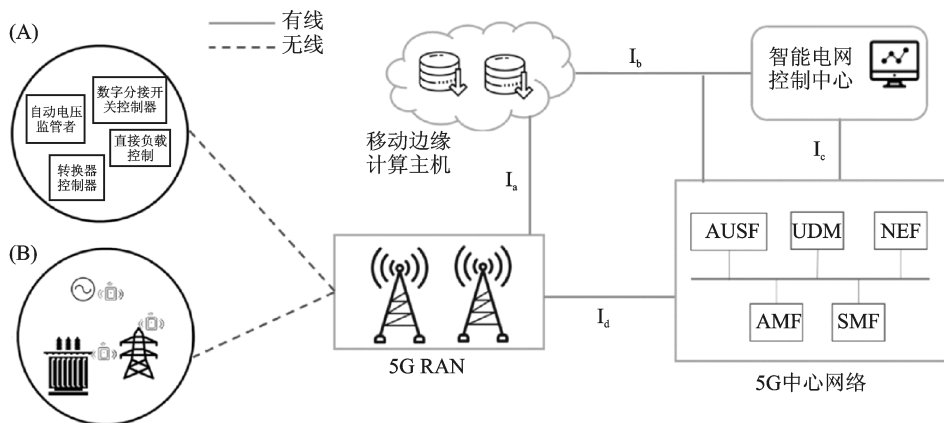


图3 利用5G网络和物联网设备(A类和B类)实现智能电网用例

以下是5G在智能电网基础设施中提供的安全优势:

① 身份验证。5G网络通过通用用户识别模块进行设备身份验证。物联网设备可以使用嵌入式eSIM模块进行身份验证,并向网络服务和智能电网所有者提供独特的身份验证方式^[6]。

② 机密性和完整性。5G网络提供了优化的OTA加密和完整性保护,保障物联网设备与基站之间的通信安全。此外,5G网络还支持128位密钥的加密和完整性保护算法,提供了更强大的数据保护。

③ 弹性和可用性。5G基站提供超可靠、低延迟通信无线电服务,满足智能电网对低延迟和近实时通信的要求。5G网络的分布式架构增加了韧性,提高了对技术或自然灾害相关故障和攻击的抵抗能力。

④ 多接入边缘计算主机。在智能电网中发挥关键作用,支持边缘计算和实时数据分析,其可以开发用于数据分析和网络威胁检测的应用程序,提高智能电网的安全性和效率。

⑤ 安全标准合规性。5G网络采用符合3GPP/ETSI标准的安全协议和体系结构,为智能电网提供标准化的安全保障。5G网络组件必须符合3GPP标准中的安全认证和保障方案。

⑥ 非公共5G网络。非公共5G网络适用于特定组织

的部署(如工厂或公司办公室),这种网络提供连接和自动化,并能隔离物联网设备流量,减少威胁面和攻击向量。

4 5G网络产生的威胁

本节突出了5G架构中的弱安全接口,并概述了针对智能电网基础设施的相关攻击。如图3所示,5G架构分为无线接入网络(RAN)和核心网络(CN)两部分。受损的RAN和CN可能对智能电网产生以下威胁:

① 虚假基站攻击。虽然5G网络比4G更安全,但物联网设备仍可能受到虚假基站攻击。这种攻击可能导致隐私泄露、拒绝服务和物联网设备电池耗尽。对手需要在物联网设备的覆盖范围内进行攻击,因此攻击范围是有限的。

② 元数据泄露。尽管5G网络为智能电网应用数据提供加密和保密功能,但元数据可能暴露给网络提供商。这些元数据包括设备身份、连接点和加密流量模式,可能涉及AMI基础设施或电池充电站。虚假基站攻击可能危及物联网设备的隐私,降级攻击可能导致数据被攻击者窃取。

③ MECH节点的安全风险。MECH节点及其相关接口存在潜在的安全风险,例如,用户平面攻击、托管的第三方应用程序的风险以及安全敏感数据在边缘节点中的存储。这些安全配置问题可能影响SGCC并危及关键运营数据。

④ 5G核心网络的风险。5G核心网络依赖于保护云基础架构,但存在暴露核心网络元素和安全能力的潜在风险。例如,在智能电网用例中,与物联网设备相关联的身份验证密钥可能通过API暴露给第三方5G核心网络功能。

⑤ 物联网设备的拒绝服务攻击。针对5G上的物联网设备的拒绝服务攻击可能导致设备或传感器无法连接,从而导致智能电网停电。这对于实现自愈和自动化的智能电网概念是一个重要问题。

⑥ MECH相关的威胁,包括恶意网关、服务器过载以及滥用边缘开放应用程序接口等威胁可能涉及MECH。这些威胁可能利用运行在多边缘计算类型应用程序上的漏洞。

5 讨论

自动电压控制为主要的分布式监测和控制技术之一,用于主动配电网络^[7]。这样的应用将显著增加配电网络容量,以承载更多的分布式发电。这是因为在给定的配电

馈线上可以部署的分布式发电的最大量通常受到潜在的电压下降的限制,若沿着馈线的分布式能源资源输出突然下降,则会导致电压下降。此外,实现 TSO-DSO 无功功率管理为未来电力系统的主要挑战之一,因为连接到输电网络的无功功率资源被 DSO 中的分布式发电、负载和储能元件所取代,这需要更多的 TSO 和 DSO 之间的积极操作协调^[8]。因此本文选择了协调的 TSO-DSO 无功功率管理用例作为研究对象,因为它不仅是最有前途的支持因素,而且还是一个高度依赖通信的智能电网应用程序。

电压控制方案被开发成智能电网的一个用例,强调了安全通信的要求。此外,研究确定了适用于 IoT 启用的智能电网用例的 5G 安全规范特征,并讨论了它们实现安全要求的可行性。本文使用 STRIDE 威胁建模方法创建了智能电网用例的威胁模型,揭示了重要的安全挑战,其中一些可以通过 5G 网络来解决。表 1 列出了 5G 如何满足提出的安全要求并应对已识别的威胁。

表 1 利用 5G 应对威胁

安全要求	威胁	5G 贡献
认证方式	欺骗	防止虚假基站, eSIM 支持安全的设备身份验证
机密性	信息泄露	eSIM 密钥交换实现加密通信
可用性	拒绝服务	5G 拆分网络增强了单个基站的弹性, 物联网网络切片可以与其他切片隔离, 5G 支持回退到传统网络
保密性	信息泄露	eSIM 密钥交换实现加密通信
完整性	篡改	eSIM 密钥交换启用消息身份验证码和经过身份验证的加密

6 结 语

使用物联网设备承诺数字化转型到多个领域,包括当前的电力网络基础设施,然而在智能电网基础设施中,物联网安全仍然面临挑战,部分原因是考虑到成本和性能之间的权衡。本文确定了低压调节智能电网用例中的物联网通信要求,并开发了相关的威胁模型,研究了 5G 规范

并讨论了其在选择的智能电网用例中的安全应用。虽然 5G 网络不能解决所有物联网安全问题,但它们提供了一种可靠的替代通信渠道,具有内置的安全优势,可用于智能电网基础设施。

就科学方面的影响而言,本文总结了使用 5G 进行物联网网络的智能电网安全的现状,记录了一个可用于评估未来安全机制的特定用例,确定了进一步工作的几个领域,尤其是需要对规模部署的 5G 物联网进行实验室研究。对于从业人员,本文提供了威胁模型(DSO 可以利用它来更新它们的变电站通信策略),关于 5G 在安全方面为 DSO 提供的信息,以及需要考虑的限制。

参考文献

- [1] 肖安南,张蔚翔,赵德盛,等. 基于物联网的智能电网监控系统构建方法研究[J]. 信息技术,2020,44(12):86-90,95.
- [2] 彭姣,刘明硕,杨力平面向智能电网的大数据降维管理方案[J]. 计算技术与自动化,2019,38(4):139-143.
- [3] 何立民. 从智能电网、物联网到泛在电力物联网[J]. 单片机与嵌入式系统应用,2022,22(4):3-5,10.
- [4] 瞿水华,郭剑杰,许乐飞. 5G 技术在智能电网中的实践和验证[J]. 供用电,2021,38(5):2-9,34.
- [5] Graditi G, Ciavarella R, Di Somma M, et al. Critical assessment of potential barriers for integrating the emerging technologies in the pan-european network considering the future eu grid scenarios[C]//2019 1st International Conference on Energy Transition in the Mediterranean Area (SyNERGY MED). IEEE,2019:1-6.
- [6] 王旭蕊,孟显,季名扬,等. 序列号同步下配电网 5G 通信的传输[J]. 单片机与嵌入式系统应用,2022,22(10):25-28.
- [7] D'ADAMO C, ABBEY C, BAITCH A, et al. Development and operation of active distribution networks[J]. IRIS,2011(1).
- [8] SUN H, GUO Q, QI J, et al. Review of challenges and research opportunities for voltage control in smart grids[J]. IEEE Transactions on Power Systems,2019,34(4):2790-2801.

陈旗展(高级工程师),主要研究方向为电力系统、人工智能。通信作者:陈旗展,pulouyue621021@163.com。

(责任编辑:薛士然 收稿日期:2023-05-26)

参考文献

- [1] 蒋超,张豪章,恩泽惠,等. 基于改进 YOLOv5s 的行人车辆目标检测算法[J]. 扬州大学学报:自然科学版,2022,25(6):45-49.
- [2] 赵元章,耿生玲. 基于改进 YOLOv5 的人脸遮挡物目标检测算法[J]. 信息通信,2021,34(11):32-35.
- [3] 张德春,李海涛,李勋,等. 基于 CBAM 和 BiFPN 改进 YoloV5 的渔船目标检测[J]. 渔业现代化,2022(3):49.
- [4] 孙丰刚,王云露,兰鹏,等. 基于改进 YOLOv5s 和迁移学习的苹果果实病害识别方法[J]. 农业工程学报,2022(11):38.
- [5] 吕晓玲,杨胜月,张明路,等. 改进 YOLOv5 网络的鱼眼图像

目标检测算法[J]. 计算机工程与应用,2023,59(6):10.

- [6] 向浩,田地. 微型计算机与分析仪器的通信技术研究[J]. 现代科学仪器,2020(6):51-55.
- [7] Xia X, Zhai J. Study on Small Target Detection of Construction Site Helmet Based on YOLOv5[C]//Chinese Intelligent Systems Conference, Springer, Singapore, 2022.

常春雷(高级工程师),主要研究方向为电力信息化、云计算技术。通信作者:常春雷,goufu43396953941@126.com。

(责任编辑:薛士然 收稿日期:2023-05-29)