

Infraestructura de Medición Avanzada (AMI) en Smart Grids: El Rol Fundamental de los Gateways IoT en la Conectividad ISM de Ciudades Inteligentes

Juan Sebastián Giraldo Duque*

*Dept. Ingeniería Electrónica, Universidad Nacional de Colombia, Sede Manizales

Email: jsgiraldod@unal.edu.co

Abstract—This work emphasizes the critical need for IoT Gateways as foundational elements in integrating diverse unlicensed (ISM) band protocols, particularly within the 915 MHz spectrum, into the broader backhaul infrastructure of smart cities. The transition towards Smart Grids in urban environments necessitates not only Advanced Metering Infrastructure (AMI) technologies but also flexible and scalable interconnection systems. This thesis presents an integrated design approach encompassing the hardware, firmware, and software aspects of an IoT Gateway, detailing its modular architecture, radio frequency requirements, interoperability mechanisms, and essential edge services. Specific use cases within AMI are discussed, alongside guidelines for constructing scalable and replicable Gateway prototypes. This integrated perspective highlights how IoT Gateways address the growing demands for data collection, secure communication, and efficient management in modern energy ecosystems.

Index Terms—Infraestructura de Medición Avanzada (AMI) Wi-Fi HaLow Redes Definidas por Software (SDN) Redes Inteligentes (Smart Grids) Internet de las Cosas (IoT) Escalabilidad Eficiencia Energética Ciberseguridad Arquitecturas de Red

I. INTRODUCCIÓN

La transformación de las redes eléctricas tradicionales en *Smart Grids* constituye un cambio de paradigma en la generación, distribución y consumo de energía eléctrica. En el núcleo de esta evolución se encuentra la *Infraestructura de Medición Avanzada* (AMI), que posibilita la medición bidireccional, recolección y análisis de datos de consumo en tiempo real. AMI habilita funciones como respuesta a la demanda, facturación dinámica, detección de fraudes, integración de generación distribuida y gestión de interrupciones, mejorando así la eficiencia operativa y el desempeño económico de las redes de servicios públicos.

La implementación masiva de medidores inteligentes y sensores IoT en entornos urbanos requiere un marco de comunicaciones escalable, seguro y fiable. Para ello, se adopta comúnmente una arquitectura de red jerárquica:

- **Red de Área Doméstica (HAN):** Interconecta electrodomésticos inteligentes y nodos IoT locales con el medidor inteligente mediante tecnologías inalámbricas de baja potencia (p. ej., Bluetooth, ZigBee, 6LoWPAN). Se exigen mecanismos de seguridad rigurosos para proteger los datos del usuario.

- **Red de Área Vecinal (NAN):** Agrega datos de medidores mediante concentradores de datos o enrutadores en malla—frecuentemente basados en IEEE 802.15.4g, WLAN o enlaces celulares ligeros—para realizar pre-procesamiento local y reenviar información resumida hacia arriba.
- **Red de Área Amplia (WAN):** Proporciona la conectividad troncal desde concentradores hasta sistemas centrales de control y SCADA sobre fibra óptica, Internet público o redes dedicadas de operadores, garantizando baja latencia y alta disponibilidad.

A pesar de estos avances, las implementaciones de Smart Grid enfrentan varios retos clave:

- **Escalabilidad y Big Data:** La transición a redes inteligentes implica un despliegue masivo de dispositivos electrónicos inteligentes y sensores que generan volúmenes enormes de datos [17] [3].
 - Miles de sensores en la infraestructura de la Smart Grid monitorizan continuamente la salud del equipo, produciendo grandes cantidades de archivos de registro o series temporales [17].
 - Se prevé que el volumen total de datos generados por dispositivos IoT conectados alcance **175 zettabytes (ZB) en 2025**, lo que exige capacidades robustas de gestión de Big Data [20].
 - Hoy en día, los medidores inteligentes envían solo unos pocos kilobytes de datos cada **15 minutos** [9]; sin embargo, al escalar a 100,000 medidores, muchas arquitecturas de comunicación carecen de ancho de banda suficiente [9].
 - La medición de tensión y corriente de línea puede generar alrededor de **2 kilobits por segundo (kbps) por fase**, lo que equivale a unos **12kbps** en una línea trifásica [9].
 - Si se incluyen otros datos como ángulo de fase y componentes de secuencia, la tasa de datos puede aumentar a entre **200–500 kbps**, y considerando la sobrecarga de los protocolos de comunicación, a menudo se requieren **2–5 Megabits por segundo**

(Mbps) [9].

- El elevado número de dispositivos conectados y la naturaleza heterogénea de los sistemas IoT (con diversas arquitecturas y diseños) complican cada vez más el procesamiento de datos, las tareas de comunicación y la gestión de energía [20].
- Una gestión eficaz de este volumen de datos es crucial para el mantenimiento de activos y las operaciones de la red [19].
- **Calidad de Servicio (QoS):** Las aplicaciones de Smart Grid presentan requisitos diversos y estrictos de fiabilidad, latencia y ancho de banda, especialmente para operaciones críticas en el tiempo [15] [13].
 - **Aplicaciones en tiempo real**, como el monitoreo sanitario y la detección de desastres naturales (por ejemplo, inundaciones), son sensibles al retraso y no toleran pérdidas de datos [4].
 - En la Red de Área Amplia (WAN), aplicaciones de control, monitoreo y protección a gran escala requieren transmitir puntos de datos a muy alta frecuencia (fracciones de segundo) para mantener la estabilidad del sistema [15]. Estas aplicaciones demandan tasas de datos de **10 Mbps a 1 Gbps** y cobertura de hasta **100 km** [15].
 - Los requisitos de latencia específicos varían:
 - * **Teleprotección:** requiere una latencia menor a **10 ms** [10].
 - * Aplicaciones de **sincronización fasorial (synchrophasors):** ≈ 20 ms [10].
 - * **SCADA y VoIP:** **100–200ms** [10].
 - * **Medición inteligente** y aplicaciones menos urgentes: hasta varios segundos [10].
 - Algunas aplicaciones de Automatización de Distribución (DA) requieren comunicación en menos de un segundo [10].
 - Para AMI, se espera una fiabilidad $>98\%$, con tasas de datos de **100kbps a 10Mbps** para tamaños de mensaje de 100–2400bytes por medidor, muestreados cada **1 o 15 minutos** [6].
 - Los mensajes de evento asíncronos, generados ante sucesos físicos en la red, se producen en ráfagas impredecibles y requieren muy baja latencia [10].
- **Interoperabilidad:** El entorno de Smart Grid es altamente heterogéneo, con diversos dispositivos y sistemas, lo que exige comunicación y intercambio de datos transparentes entre múltiples protocolos y estándares [15] [20].
 - La carencia de estándares de interoperabilidad adecuados es un obstáculo al preferirse soluciones propietarias [15] [11].
 - El objetivo es avanzar hacia **redes basadas en IP** para resolver problemas de compatibilidad [15].
 - Estándares como **IEC 61850** (subestaciones y recursos distribuidos) e **IEC 61970** (Modelo de Información Común, CIM) se armonizan para definir un modelo unificado del sistema de potencia [7].
- Es esencial garantizar el transporte fluido de datos entre dispositivos, mapeando protocolos como DNP3 a **IEC 61850** [7].
- Tecnologías de comunicación como LoRaWAN, Wi-SUN y NB-IoT, cada una con ventajas y limitaciones, complican la estandarización pero hacen imprescindible su integración eficiente [6] [22] [13].
- **Ciberseguridad y Privacidad:** La ampliación de la superficie de ataque por dispositivos interconectados plantea grandes desafíos en seguridad y protección de datos [17] [18] [5].
 - Las Smart Grids son vulnerables a ciberataques que pueden comprometer la disponibilidad y privacidad del sistema [17] [23]. Por ejemplo, el 15 de diciembre de 2015 un ciberataque en una central eléctrica europea provocó un apagón que afectó a 80.000 personas [2].
 - Smart Meters (SM) y Unidades de Medición Fasorial (PMU) pueden ser objetivo de interferencias, suplantación y ataques DDoS; ataques simulados pueden reducir paquetes transmitidos en un 10–20% [17].
 - Muchos dispositivos IoT funcionan con hardware de recursos limitados, lo que hace costoso implementar criptografía compleja (p.ej., RSA) [1] [13] [12].
 - Se requieren sistemas livianos de autenticación y acuerdo de claves que funcionen en entornos con recursos restringidos [13] [1].
 - La seguridad debe integrarse por defecto desde el diseño de dispositivos y protocolos [16] [8].
 - La gestión de claves, tanto para sistemas críticos en tiempo real como para AMI, es un área clave de investigación [16].
 - Proteger datos sensibles de consumidores —como información de consumo y pagos— es crucial para evitar la exposición de identidades y patrones de uso [17].
- **Eficiencia Energética:** Muchos nodos IoT, alimentados por baterías en ubicaciones remotas, exigen protocolos y diseños de red que maximicen la autonomía de los dispositivos [14] [20].
 - Tecnologías como IEEE 802.15.4 (ZigBee) y LoRaWAN permiten 15–20 años de vida útil de batería con pocos envíos diarios [21].
 - La selección de la velocidad de datos en wireless implica un compromiso entre alcance, duración de mensaje y consumo energético [24].
 - El esquema ADR de LoRaWAN optimiza la tasa de datos para cada nodo, maximizando autonomía y capacidad de red [24].
 - El uso eficiente de recursos de comunicación limitados es esencial para ciudades y redes sostenibles [20].
 - Futuras tecnologías (5G/6G) buscan reducir transmisiones siempre activas y optimizar diseños, pero

garantizar eficiencia para dispositivos de baja potencia sigue siendo un desafío [13].

- La investigación se centra en lograr un rendimiento óptimo equilibrando las restricciones energéticas de los sensores IoT.

En este contexto, los *Gateways IoT* se erigen como habilitadores críticos para la AMI en ciudades inteligentes. Los gateways realizan la traducción de protocolos y la consolidación de datos entre tecnologías de banda ISM (p. ej., LoRaWAN, Wi-SUN, IEEE 802.15.4g, Sigfox) y proporcionan interfaces seguras y fiables hacia la WAN. Asimismo, implementan gestión local de QoS, filtrado de datos y autenticación ligera antes de transmitir la información a los centros de control de la utilidad o plataformas en la nube. Al unificar las redes de campo heterogéneas con el backhaul de alta capacidad, los Gateways IoT sustentan la operación robusta, eficiente y segura de las Smart Grids de próxima generación [12].

II. PROBLEMA DE INVESTIGACIÓN

El problema de investigación central de esta tesis es: ¿Cómo diseñar un gateway IoT que facilite la integración eficiente y segura de redes de Infraestructura de Medición Avanzada (AMI) en el backhaul de ciudades inteligentes utilizando bandas ISM?

Los gateways IoT son un elemento clave para integrar múltiples protocolos de banda libre (ISM) en el backhaul de ciudades inteligentes. En el contexto de las redes eléctricas inteligentes (Smart Grids) y la AMI, la congestión representa un problema crítico, ya que el desbordamiento de los búferes de los routers puede provocar la pérdida de datos. Las redes de sensores inalámbricos (WSN) y las redes 6LoWPAN se consideran una combinación fundamental para el Internet de las Cosas (IoT). La investigación busca analizar y evaluar las condiciones de congestión en 6LoWPAN y desarrollar esquemas de control de congestión para una implementación exitosa del IoT. Además, la comunicación bidireccional entre el medidor y el centro de control de la empresa es una característica diferenciadora de los sistemas AMI.

III. JUSTIFICACIÓN

La necesidad de esta investigación se justifica por varias razones críticas:

- Alta Dependencia Tecnológica en Infraestructura Propietaria: Existe una preocupación por la dependencia de soluciones propietarias y el "vendor lock-in" en las infraestructuras de Smart Grids, lo que limita la flexibilidad y la integración. Es esencial adoptar una combinación de tecnologías con implementaciones de software y hardware que se adhieran a protocolos abiertos y estándares para lograr interoperabilidad, escalabilidad y seguridad.
- Falta de Estandarización: La ausencia de arquitecturas de referencia estándar y una armonización de estándares de seguridad a nivel europeo es un desafío significativo en las Smart Grids. La interoperabilidad es fundamental para las implementaciones de Smart Grid, que consisten en dispositivos inteligentes conectados con hardware y

software diversos. La normalización de IEC 61850 busca la interoperabilidad e intercambiabilidad de dispositivos de diferentes proveedores.

- Cobertura Efectiva en Zonas Urbanas y Suburbanas: Las redes IoT requieren una planificación cuidadosa basada en la geografía y la cobertura. Las tecnologías de comunicación inalámbrica son esenciales para las Smart Grids, pero las tecnologías con alcance y tasas de datos limitadas pueden causar dificultades y congestión. Las tecnologías LPWAN, como LoRaWAN y NB-IoT, ofrecen una mayor cobertura. LoRaWAN, en particular, demuestra una notable penetración de señal en ubicaciones de difícil acceso, como sótanos, lo que la hace adecuada para áreas de medidores dispersas. Wi-Fi HaLow también se destaca por su alcance mejorado en entornos urbanos inteligentes. La AMI para Smart Grids implica una arquitectura de red jerárquica que incluye redes de área doméstica (HAN), redes de área de vecindario (NAN) y redes de área amplia (WAN). La comunicación entre estas redes y con los centros de control es crucial para la eficiencia y la seguridad.

IV. OBJETIVO GENERAL

El objetivo general de esta tesis es: Diseñar y evaluar un gateway IoT modular, enfocado en protocolos abiertos en bandas ISM, con énfasis en la integración AMI para ciudades inteligentes.

Este objetivo aborda la necesidad de infraestructuras de interconexión flexibles y escalables para la migración hacia las Smart Grids en el contexto urbano. El diseño integral propuesto abarca el hardware, el firmware y el software del Gateway IoT, definiendo su arquitectura modular y los servicios de borde necesarios.

V. OBJETIVOS ESPECÍFICOS

Para lograr el objetivo general, se plantean los siguientes objetivos específicos:

A. Analizar los requerimientos regulatorios y técnicos de las bandas ISM.

Esto implica una descripción detallada de las bandas ISM, incluyendo 433 MHz, 868/915 MHz y 2.4 GHz, y la selección de la banda de 915 MHz por sus ventajas en alcance, penetración y densidad de nodos. Se considerará la aplicación de diferentes bandas de frecuencia para la comunicación en Smart Grids, como los 2.4 GHz para ZigBee y LoRa, y las bandas sub-GHz para LPWAN.

B. Diseñar hardware de gateway compatible con múltiples protocolos de 433/868/915 MHz y 2.4 GHz.

El diseño de hardware del Gateway IoT es un componente clave de la tesis. El gateway debe ser capaz de manejar mensajes de dispositivos heterogéneos y soportar la compatibilidad multiprotocolo, como lo ejemplifica un solo gateway que adquiere señales de diversos medidores de calidad de energía mediante diferentes protocolos como Modbus, Profibus,

Ethernet/IP e IEC 61850. Los gateways actúan como un puente transparente entre los dispositivos finales y el servidor de red central.

C. Desarrollar firmware y software orientado a interoperabilidad y seguridad.

- Esto abarca la arquitectura de firmware, incluyendo el kernel, el sistema de archivos, los drivers de RF, los pilotos de radio y la adaptación a múltiples protocolos. En cuanto al software, se explorará el sistema operativo embebido (Linux, RTOS), el middleware para la integración de protocolos y los servicios de edge computing como filtrado, agregación y analítica básica. Las comunicaciones con la nube utilizarán protocolos como MQTT, CoAP y REST.
- La seguridad embebida se centrará en el arranque seguro y el cifrado ligero, esenciales para dispositivos con recursos limitados. La interoperabilidad se garantizará mediante modelos de datos comunes (JSON, CBOR, DLMS/COSEM), mecanismos de autenticación y autorización, cifrado y protocolos seguros (DTLS, TLS), políticas de firewall y segmentación de red, y actualizaciones de seguridad.

D. Validar un prototipo mediante pruebas de campo.

Se realizará una implementación de prototipo y una evaluación exhaustiva. La metodología de pruebas incluirá la evaluación de la cobertura de radio, la latencia y el rendimiento. Los resultados se obtendrán en un entorno real de ciudad inteligente (por ejemplo, Manizales). Se realizará una comparativa con soluciones existentes como LoRaWAN y Wi-SUN. La validación en campo es crucial para asegurar la aplicabilidad en el mundo real, superando las limitaciones de los estudios de simulación.

VI. MARCO TEÓRICO

Esta investigación se apoya en los siguientes pilares teóricos:

A. Comunicación Máquina a Máquina (M2M):

El IoT se define por la comunicación M2M, donde dispositivos, sensores y actuadores interactúan sin intervención humana. Esta comunicación es vital para el monitoreo en tiempo real de los sistemas de Smart Grid.

B. Arquitecturas AMI:

Los sistemas AMI son una parte fundamental de las Smart Grids y típicamente emplean una arquitectura de red jerárquica compuesta por Redes de Área Doméstica (HAN), Redes de Área de Vecindario (NAN) y Redes de Área Amplia (WAN).

C. Protocolos LPWAN (Low-Power Wide Area Network):

Incluyen LoRaWAN y NB-IoT. Estos protocolos son una alternativa prometedora para la conectividad IoT a largo alcance y baja tasa de datos en bandas sub-GHz sin licencia.

D. Estándares IEEE 802.15.4g:

Es un protocolo abierto para bandas ISM. IEEE 802.15.4 (Zigbee) es un protocolo de comunicación de corto alcance y baja velocidad de bits adecuado para redes de área personal inalámbricas (WPAN) y puede formar la base de WSNs en IoT.

E. LoRaWAN:

Es una especificación clave para redes de baja potencia y área amplia, diseñada para dispositivos de bajo consumo, conexiones bidireccionales seguras, largo alcance y bajas velocidades de datos. Utiliza una arquitectura de red en estrella de estrellas con dispositivos finales, gateways y un servidor de red central. Destaca por su eficiencia energética, permitiendo una vida útil de la batería de los medidores de hasta 15-20 años.

F. Wi-SUN:

Es otro protocolo abierto en bandas ISM, recomendado para estrategias de comunicación AMI, especialmente en NANs.

VII. METODOLOGÍA

La metodología de la tesis seguirá un enfoque riguroso:

A. Diseño Basado en Ciclos Iterativos (V-modelo o Scrum Embebido):

Aunque los documentos no mencionan explícitamente "V-modelo" o "Scrum", la estructura de la tesis (Diseño de Hardware, Desarrollo de Firmware, Plataforma de Software, e Implementación y Evaluación) sugiere un proceso de diseño sistemático e iterativo.

B. Simulación RF:

Se utilizarán simulaciones para explorar acciones y prever resultados. Se realizarán análisis de congestión basados en simulaciones y pruebas con testbed. Herramientas como TOSSIM (un simulador de eventos discretos para redes de sensores TinyOS) permitirán examinar y depurar algoritmos en un entorno controlado. También se emplearán simulaciones Monte Carlo para evaluar el rendimiento de NB-IoT en comunicaciones inteligentes a gran escala.

C. Validación en Campo:

La validación del prototipo se realizará a través de pruebas de campo, empleando experimentos en redes reales para validar el trabajo de simulación. Esto incluye un análisis de congestión basado en testbeds para 6LoWPAN, utilizando nodos sensores CM5000 TelosB en escenarios interiores y exteriores. Las pruebas de campo son cruciales para obtener datos del mundo real que guíen las implementaciones IoT. La creación de testbeds es imperativa para la implementación real de las Smart Grids.

D. Métricas de Desempeño:

La evaluación incluirá métricas clave como la cobertura de radio, la latencia y el rendimiento del gateway. Para las redes inalámbricas de sensores (WSN) y 6LoWPAN, se considerarán la pérdida de paquetes, el rendimiento, el retardo, el índice de equidad ponderada y el consumo de energía. Las Smart Grids requieren una infraestructura de comunicación con baja latencia, flujo rápido, gran ancho de banda, bajo ruido y altas tasas de datos.

Esta estructura proporciona una hoja de ruta clara para abordar el problema de investigación y sus objetivos, basándose en un marco teórico sólido y una metodología de investigación exhaustiva.

REFERENCES

- [1] A lightweight and safe method for authenticating and establishing keys in smart grid systems. Source is from 'Insights2TechInfo'; specific authors and publication year not provided in the excerpt [9].
- [2] Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach. *J. Comput. Des. Eng.*, 7(3):352, 2020. Authors not explicitly stated in excerpt; publication details inferred from provided URL and content [25, 26].
- [3] Optimal Placement of Data Concentrators for Expansion of the Smart Grid Communications Network. Undated. Authors and full journal details not explicitly provided in the excerpt; internal references range from 2004 to 2018 [28-30].
- [4] Hayder Al-Kashoash. *Congestion Control for 6LoWPAN Wireless Sensor Networks: Toward the Internet of Things*. Springer Theses. Springer Nature Switzerland AG, 2020. Doctoral Thesis accepted by the University of Leeds, Leeds, UK [1-3].
- [5] Massimo Bernaschi, Emanuele Gabrielli, and Luca Verzichelli. Methodology for the identification of critical communication networks links and components. *Computer Standards & Interfaces*, 41:31–38, 2015.
- [6] Rupam Bhattacharya, Subhankar Dhar, and Ishwar Holla. Leveraging IoT for utility transformation. In *Proceedings of the 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pages 303–307. IEEE, 2019.
- [7] Christoph Brunner. Iec 61850 blog (until 2020-03-01), 2020. Accessed: 2025-07-28.
- [8] European Commission. Cyber Security of the Smart Grids. Technical report, Undated. Produced with input from the Expert Group on the Security and Resilience of Communications Networks and Information Systems for Smart Grids. Year not explicitly stated for the document, but internal references indicate around 2011 [17, 18].
- [9] Prem Chand Jain. Recent advances in smart grid communication and networking. *AKGEC International Journal of Technology*, 15(2):28–34, 2022. ISSN: 0975-9514.
- [10] Yong-Hee Jeon. Qos requirements for the smart grid communications system. *International Journal of Computer Science and Network Security (IJCSNS)*, 11(3):86–94, March 2011. ISSN: 1738-7906.
- [11] Luke Kane. Investigation into cybersecurity within the smart grid. Master's thesis, Technological University Dublin, 2021.
- [12] Luke Kane. *PhD Thesis by Luke Kane*. PhD thesis, Queensland University of Technology (QUT), 2023. Full thesis title not explicitly provided in excerpt. Year inferred from included chapter publication dates (latest is 2023) [34-37].
- [13] D. Kanellopoulos, V. K. Sharma, T. Panagiotakopoulos, and A. Kameas. Networking Architectures and Protocols for IoT Applications in Smart Cities: Recent Developments and Perspectives. *Electronics*, 12(2490), 2023. Received 28 April 2023, Published 31 May 2023 [27].
- [14] Evgeny Khorov, Andrey Lyakhov, Alexander Krotov, and Andrey Guschin. A survey on IEEE 802.11ah: An enabling networking technology for smart cities. *Computer Communications*, xxx, 2014. Volume number 'xxx' is a placeholder from the source [10, 11].
- [15] M. Kuzlu, M. Pipattanasomporn, and S. Rahman. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks*, 67:74–88, 2014. Work supported in part by the U.S. National Science Foundation [16].
- [16] Rossella Mattioli and Konstantinos Moulinos. Methodology for the identification of critical communication networks links and components – annexes. Technical report, European Union Agency for Network and Information Security (ENISA), Heraklion, Greece, 2015. Annexes to the ENISA report on communication network interdependencies in smart grids.
- [17] T. Mazhar, H. M. Irfan, S. Khan, I. Haq, I. Ullah, M. Iqbal, and H. Hamam. Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods. *Future Internet*, 15(83), 2023. Published 19 February 2023 [15].
- [18] Mehmet Hazar Cintuglu and A. Chakraborty. A Survey on Smart Grid Cyber-Physical System Testbeds. *IEEE Communications Surveys & Tutorials*, 2016. Authors identified from affiliations mentioned in the provided excerpt; full author list not explicitly stated for the paper itself [6-8].
- [19] National Energy Technology Laboratory. Advanced Metering Infrastructure. Technical report, National Energy Technology Laboratory, 2021. Version V1.0, part of 'NETL MGS - Powering Our 21st-Century Economy'. Year cited from another source [12, 13].
- [20] Iqra Rafiq, Anzar Mahmood, Sohail Razzaq, S. Hassan M. Jafri, and Imran Aziz. IoT applications and challenges in smart cities and services. *J. Eng.*, pages 1–25, 2023. Article available on Wiley Online Library [21-23].
- [21] Adithya Shreyas. ANALYSIS OF COMMUNICATION PROTOCOLS FOR NEIGHBORHOOD AREA NETWORK FOR SMART GRID. Master's thesis, The Oxford College of Engineering, Undated. Master's project from ScholarWorks; year not specified in excerpt [14].
- [22] Smart Energy. Breaking barriers in smart metering with wi-fi hallow. <https://www.smartenergy.com/industrysectors/smartmeters/breakingbarriersinasmartmeteringwithwifihallow/>, 2025. Accessed: 2025-07-28.
- [23] John Smith. Design and simulation of smart grids for improved energy distribution. *American Journal of Mechanical Engineering and Technology*, 5(4):10–17, 2024.
- [24] Wikipedia contributors. LoRaWAN, Undated. Content from Wikipedia; retrieval date and URL not provided in excerpt [24].