

A Utility-Driven Assessment of LoRaWAN Application for Secure Remote Monitoring in Smart Grid Systems [†]

Zephania Philani Khumalo ^{1,*}  and Resham Singh ²

¹ Electronic and Computer Engineering Department, Steve Biko Campus, Durban University of Technology (DUT), cnr Steve Biko Rd & Botanic Gardens Rd, Durban 4001, South Africa

² SCADA Systems, eThekwin Electricity Durban, Durban 4001, South Africa

* Correspondence: philanik1@dut.ac.za

[†] Presented at the 34th Southern African Universities Power Engineering Conference (SAUPEC 2026), Durban, South Africa, 30 June–1 July 2026.

Abstract

Low Power Wide Area Networks (LPWANs) are essential for enabling Internet-of-Things (IoT) technologies in utility environments. Utilities can leverage these networks to monitor critical remote assets, especially where mobile technologies are unsuitable due to poor power efficiency or insufficient coverage. This paper investigates the use of Long Range (LoRa) Wide Area Network (LoRaWAN) technology as an LPWAN solution for remote grid monitoring within the eThekwin Municipal Area. In addition to evaluating range performance (distance) and the packet reception ratio (PRR) across configurable parameters, such as spreading factor and transmit power, this paper introduces a data-packet security extension for LoRaWAN using NTRU post-quantum cryptography (PQC). The proposed security enhancement provides quantum-resistant encryption for application-layer payloads without violating LoRaWAN duty-cycle constraints or significantly increasing energy consumption. Field tests were performed at 11 geographically dispersed substations using a handheld LoRa device. Test signals were transmitted at four power levels (2 dBm, 8 dBm, 14 dBm, and 20 dBm) and spreading factors (SF7–SF12). Results show that the public LoRaWAN network can achieve communication distances of approximately 30 km in an urban environment, with PRR strongly dependent on SFs and transmit power. The integration of lightweight NTRU-protected payloads was found to be feasible for typical smart grid use cases involving small data packets (1–13 bytes).

Keywords: IoT; LoRa; LPWAN; remote monitoring; SCADA; smart grid; NTRU; post-quantum security



Academic Editor: Akshay Kumar Saha

Published: 9 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

The rapid evolution of the Internet of Things (IoT) has become one of the most influential technological shifts of the modern era. IoT continues to redefine how utilities operate, automate processes, and engage with customers. Global studies project that the economic impact of IoT could reach as high as 12 trillion USD by 2030, highlighting its transformative potential across industries [1].

This technological momentum is driven by continuous progress in electronic miniaturisation, low-power microcontrollers, and advances in long-range wireless communication techniques. As a result, IoT has begun reshaping numerous industrial sectors, including healthcare, electricity, gas, water, and other critical utility domains.

Although machine-to-machine (M2M) communication has been used in industrial systems for decades they often rely on mobile data networks. The widespread application of M2M has historically been constrained by the substantial energy requirements of cellular communication modules. The demand for more energy-efficient field devices has motivated the development of Low Power Wide Area Networks (LPWANs).

A typical LPWAN LoRa Network is depicted in Figure 1. These networks employ highly efficient modulation schemes and simplified radio-layer signalling to reduce energy consumption while significantly extending the communication range. Modern LPWAN technologies can maintain connectivity even when received signals fall well below the noise floor, a capability made possible through sophisticated digital signal processing techniques [2].

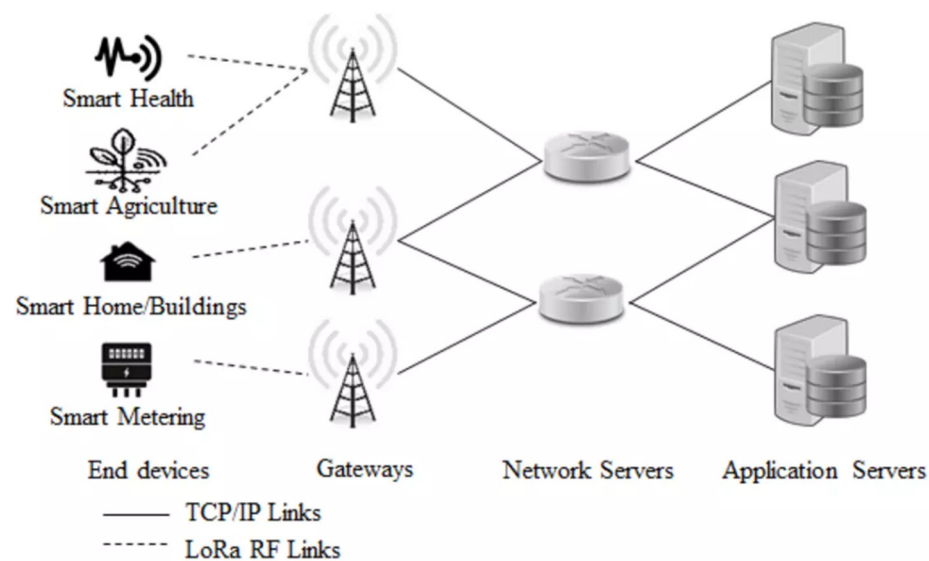


Figure 1. Typical LPWAN LoRa Network.

Within this landscape, LoRa and LoRaWAN have emerged as promising solutions for smart grid telemetry, remote monitoring, and distributed sensing. However, as utilities begin integrating IoT technologies into critical infrastructure, cybersecurity has become an equally important consideration. Standard LoRaWAN provides symmetric encryption at the network and application layers, but rising concerns about long-term cryptographic resilience especially in the face of quantum-enabled adversaries highlight the need for stronger protections. To address this, our work incorporates Nth-degree Truncated Polynomial Ring Units (NTRUs), a lattice-based post-quantum encryption scheme, which enables quantum-resistant security at the application layer. This ensures confidentiality of smart grid telemetry even when public LoRaWAN networks are used for communication.

Against this backdrop, the aim of this paper is to evaluate the real-world performance of LoRa LPWAN technology for smart grid applications at eThekweni Electricity, while additionally assessing the feasibility of integrating lightweight post-quantum (NTRU-based) encryption for secure payload delivery. To achieve this, the study addresses the following research questions (RQs):

- RQ1: What communication distances can be achieved using the public LoRa network within the eThekweni Municipal Area (EMA)?
- RQ2: How reliable is LoRa technology across varying distances, spreading factors (SFs), and transmission power levels (TXps) when deployed within the EMA?
- RQ3: What practical update rates can be supported by the public LoRa network for typical smart grid monitoring applications?

The remainder of this paper is organised as follows: Section 2 introduces the research problem. Section 3 presents an overview of LPWAN technologies and discusses key security considerations, including post-quantum protections. Section 4 details the experimental methodology and field-test design. Section 5 presents the field results and their analysis, while Section 6 describes the setup and evaluation of the Raspberry Pi LoRa testbed. Finally, Section 7 summarises the main findings and outlines directions for future work, including the extension of post-quantum security measures for utility IoT deployments.

2. Research Problem

Modern smart grid networks increasingly rely on remote monitoring to enhance reliability, operational visibility, and responsiveness. However, many utilities still operate in geographically dispersed and infrastructurally constrained environments where traditional communication technologies are either too costly, bandwidth-limited, or lack the coverage required for continuous system monitoring.

LPWAN technologies such as LoRaWAN present an attractive alternative due to their long-range communication capability, low power consumption, and cost-effectiveness. Despite these advantages, utilities face significant challenges when integrating LoRaWAN into smart grid applications, including data security, interference, network scalability, latency concerns, and ensuring end-to-end reliability for mission-critical grid operations.

Furthermore, there is limited research and practical guidance from the utility perspective on how LoRaWAN can be effectively deployed for remote monitoring applications, such as asset management, fault detection, power quality monitoring, meter data acquisition, and predictive maintenance, while maintaining strict cybersecurity and resilience requirements.

3. LPWAN Technologies

3.1. LPWAN IoT Landscape

LPWANs have emerged as a distinct category within the broader IoT communication ecosystem, offering an attractive balance between power consumption, coverage range, and device cost. As illustrated in Figure 2, LPWAN technologies occupy a unique space between short-range high-throughput systems and wide-area mobile broadband solutions, specifically targeting applications where devices must operate for years on constrained batteries while still achieving reliable long-distance communication [3].

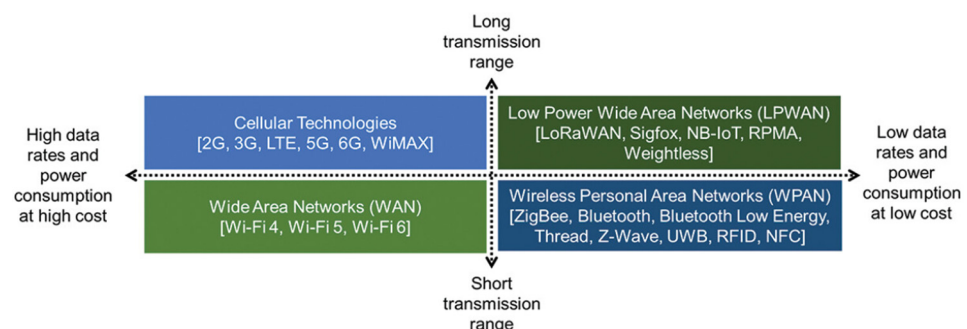


Figure 2. LPWAN value proposition.

Their value proposition is rooted in enabling large-scale sensing and monitoring deployments where minimal bandwidth requirements and long sleep cycles are typical.

Several LPWAN standards and proprietary offerings compete across multiple dimensions, including achievable data rates, operating frequencies, uplink/downlink symmetry, and total cost of ownership. Table 1 summarises key technological differentiators among widely deployed LPWAN technologies, such as LoRa, SigFox, and NB-IoT [4]. LoRa in

particular has gained traction due to its open specification, unlicensed spectrum usage, and support for bidirectional communication, which collectively reduce deployment barriers and eliminate vendor lock-in.

Table 1. LPWAN comparison.

Parameter	LoRa	SigFox	NB-IoT
Data-rate	50 kbps	100 bps	200 kbps
Frequency	Unlicensed	Unlicensed	Licensed
Coverage	Urban: 5 km Rural: 20 km	Urban: 10 km Rural: 40 km	<10 km
Standards	Open standard	Proprietary	3GPP
Communication	Bidirectional	Limited bidirectional	Bidirectional

Beyond functional parameters, security has become a decisive factor in LPWAN adoption for critical infrastructure. As IoT deployments scale, vulnerabilities in symmetric-key systems or traditional public-key cryptography pose long-term risks, especially in smart grid environments with decades-long asset lifecycles. Emerging post-quantum cryptographic schemes, particularly lightweight lattice-based systems, such as NTRUs, provide a compelling foundation to secure LPWAN edge devices against future quantum-capable adversaries. The compact key sizes, low computational overhead, and resilience to both classical and quantum attacks position NTRUs as a strong candidate for securing constrained IoT architectures and utility field assets.

The LPWAN market continues to evolve as new standards integrate improved coverage, energy efficiency, and security, including post-quantum readiness.

3.2. LoRa Technology Overview

LoRa (Long Range) is a spread-spectrum wireless modulation technique engineered to support large-area IoT networks using minimal energy. Operating in sub-GHz licence-free bands, LoRa relies on Chirp Spread Spectrum (CSS) modulation to achieve long communication distances while maintaining robust tolerance to interference. By adjusting the spreading factor (SF) typically ranging from 7 to 12 the transmission time per symbol can be varied, enabling trade-offs between range, link robustness, and throughput [5]. Higher spreading factors increase signal airtime, allowing receivers to decode frames even when received below the noise floor, but at the cost of lower data rates [6].

The flexibility of LoRa is further enhanced through its device classes:

- Class A devices prioritise ultra-low-power operation, opening receive windows only after transmissions.
- Class B introduces beacon-synchronised receive slots, enabling scheduled downlink communication.
- Class C maintains near-continuous receive capability, suitable for grid control applications where latency is more critical.

While LoRa offers an effective communication substrate, ensuring secure device authentication, message integrity, and key management remains a concern, especially when devices are deployed in hostile or hard-to-reach locations. LoRaWAN already utilises AES-based symmetric keys, but as smart grid infrastructure migrates toward long-term cyber-resilience, post-quantum techniques such as NTRUs become increasingly relevant. NTRUs' efficient lattice-based key encapsulation mechanisms provide secure session-key

establishment with lower computational costs than many PQ alternatives, making them suitable for LoRa nodes that operate on microcontrollers with tight energy budgets.

3.3. Opportunities for Enhanced Monitoring Within the Smart Grid

Modern power distribution networks rely heavily on remote condition monitoring, status reporting, and event detection to support situational awareness and rapid response. Selecting an appropriate communication technology requires balancing application criticality, allowed latency, bandwidth needs, and power availability at field locations [7].

LPWAN architectures are well suited to applications with:

- Low bandwidth requirements—many grid sensors transmit only a few bytes per message.
- Limited power availability—especially in locations where only medium- or high-voltage lines exist and no low-voltage AC supply is available.
- Infrequent updates or event-triggered communication—typical for supervisory measurements or binary state changes.

Update rates are especially important in utility contexts. Engagement with eThekweni Electricity medium-voltage operations confirms that reporting intervals of around five minutes are acceptable for most monitoring functions, which aligns with recommendations such as Cisco's distribution automation guidelines [8]. Power efficiency can be further optimised through edge-analytics approaches, where transmissions occur only when threshold deviations or binary state transitions are detected.

The analogue quantities generally require around 2 bytes per measurement [9], while binary states can be encoded efficiently using compact bitmasks. When such telemetry is combined with lightweight post-quantum key establishment (NTRU-based KEMs), utilities can ensure long-term confidentiality and integrity without exceeding the processing or energy budgets of LPWAN devices. This is particularly important in smart grid environments where devices are expected to operate securely for 10–20 years.

4. Experimental Research Methodology

To assess the suitability of LoRa technology for smart grid monitoring applications, a structured field evaluation was conducted across eleven substations distributed throughout the eThekweni municipal region. These substations were intentionally selected to represent diverse geographic and environmental conditions, enabling a realistic understanding of link performance across the utility's footprint.

A portable LoRa test terminal, configured as the end-device, was deployed at each site to generate controlled transmission patterns [10]. For every substation, the device transmitted packets using four different transmit power settings, 2 dBm, 8 dBm, 14 dBm, and 20 dBm, combined with six spreading factors (SF7 to SF12). This resulted in a total of 24 unique transmission configurations per location. All tests were conducted using a 125 kHz bandwidth and a coding rate of 4/5, ensuring consistency with common LoRaWAN deployment parameters.

System range was quantified by analysing which gateway nodes across the public LoRaWAN network successfully received each transmitted packet. Each received frame-contained metadata including the transmit power and spreading factor, enabling correlation of performance with radio-layer parameters. The public LoRaWAN infrastructure used for this experiment comprises approximately twelve gateways positioned across the eThekweni area, as documented in [11].

To examine communication reliability more thoroughly, repeated measurements were performed at a single substation. Thirteen full test cycles were executed using the same set

of power levels and spreading factors. The reliability characteristics were quantified using the packet reception ratio (PRR), defined as follows:

$$\text{PRR} = \frac{\# \text{ packets received}}{\# \text{ packets transmitted}} \quad (1)$$

This iterative approach provided statistically meaningful insights into LoRa performance under varying link conditions, including potential interference, multipath fading, and gateway diversity.

From a cybersecurity standpoint, although radio-frequency performance was the primary focus of this study, the testbed architecture reflects real-world IoT deployments where devices must operate securely for extended periods. As utilities migrate toward quantum-resilient communication frameworks, lightweight lattice-based schemes such as NTRUs become increasingly relevant for protecting key exchanges and ensuring long-term confidentiality of telemetry-traversing public LPWAN infrastructures. While encryption was not the central parameter measured in this phase, understanding LoRa performance at different SFs and TX power levels supports future work where NTRU-based secure session establishment and authenticated reporting will be integrated into field-deployed sensors [12].

5. Results and Analysis

The first research question (RQ1) focused on establishing the practical communication distances achievable using LoRa technology within the eThekweni municipal region. Applying the test procedure defined in Section 3, the measured ranges are summarised in Table 2. During the campaign, maximum link distances of approximately 38 km were recorded, with packets from certain substations being simultaneously detected by up to six different gateway sites. A notable observation is that the gateway positioned at the highest elevation (around 950 m above sea level) consistently recorded the longest reception distances, averaging 31 km, highlighting the strong influence of gateway altitude on LoRa propagation performance.

Across all substations, the system demonstrated reliable message decoding down to a minimum practical RSSI of -119 dBm. While manufacturer datasheets reference more optimistic limits [12], the measured threshold aligns closely with earlier field studies reported in [13]. For context, traditional 3G and LTE systems typically regard RSSI values below -85 dBm as significantly degraded [14], highlighting LoRa's suitability for low-SNR environments.

5.1. Range, Reliability, and PRR Behaviour

Although the achieved distances are impressive for an urban deployment, it is essential to evaluate how reliably packets are delivered at these ranges. To examine this (RQ2), a detailed reliability assessment was conducted at the Gateway substation, where the entire test sequence was repeated multiple times.

The results indicate that LoRa remains operational even under extremely weak signal conditions, with successful decoding observed at signal-to-noise ratios approaching -16 dB, which is consistent with LoRa's theoretical limits [15]. When examining PRR across the range of test conditions, higher spreading factors (SF11 and SF12) consistently delivered the most stable performance, achieving PRR values of 100% at distances up to 34 km and 21 km, respectively. Among all combinations, SF11 at 14 dBm exhibited the most favourable overall reliability profile.

Conversely, lower spreading factors struggled to maintain consistent delivery at longer ranges, even when SNR values remained within nominal technical limits [16–18].

Table 2. LoRa technology distances (KM) [15].

Substations	Base Stations (BS)												No. of BSs That Received Signals
	Malvern	Glenridge	Alverstone	Umlazi	Wyebank	Westville	Kwa-Mashu	Ballito	Durban CBD	Inanda	Umhlanga	Verulam	
Addington	12				20	11			2				4
Beachwalk									1				1
Berea park	9	3	28		15	6	14						6
Cato street									1				1
Gateway			34		21					13	1		4
Glenashley	19	12	32	30	18	14	12						7
Greenbury			31		18	15	7			10	2	8	7
Jameson park	11		29			7	12	38	3				6
KE Masinga		3	31				15		1				4
La mercy					30			13		16			3
Old fort									1				1
Sunningdale											2		1
Tongaat								11					1
Ave. distance	13	6	31	30	20	11	12	21	2	13	2	8	
Altitude	225	200	950	155	508	280	236	200	180	477	123	100	
Min RSSI (dBm)	−116	−98	−119	−116	−116	−117	−116	−119	−107	−105	−104	−105	

These findings reinforce the importance of carefully selecting SFs and TX power for smart grid IoT deployments, as an inappropriate configuration can significantly degrade field reliability.

5.2. Update-Rate Performance and Smart Grid Suitability

The third research question (RQ3) investigated how frequently LoRa devices can report measurements given typical smart grid payload sizes. Many grid-monitoring applications require only modest payloads, often 1 to 13 bytes. A representative use case consisting of temperature (2 bytes), humidity (2 bytes), and eight digital inputs (1 byte) results in an estimated 5-byte payload.

Using a standard LoRaWAN airtime calculator [19], a total frame size of 18 bytes (5-byte payload plus protocol overhead) yields the update intervals. Under a 1% duty-cycle constraint, update rates range from approximately 5 s (SF7) to around 132 s (SF12). Aligning these results with the reliability findings from RQ2 suggests that SF11 and SF12 are typically offering the highest PRR and would provide update rates of 66 s and 132 s, respectively. These intervals are compatible with the update requirements for most smart grid monitoring assets listed earlier. The trade-off, however, is increased airtime and higher energy consumption at larger spreading factors [20], which must be considered when designing battery-powered field devices.

5.3. Security Considerations: Integrating NTRUs with LoRa Deployments

Although the primary objective of this study was the evaluation of LoRa radio-frequency performance, the results have broader implications for future secure utility IoT architectures [21], as smart grid systems increasingly require cryptographic protection against emerging threats, including quantum-capable adversaries [21–23]. Lightweight post-quantum solutions such as NTRUs have become promising candidates for securing LoRa devices [24,25].

The demonstrated long-range capabilities and achievable update rates suggest that:

- NTRU-based key exchange or periodic re-keying is feasible even for devices operating at higher spreading factors [26,27].
- The 5–132 s reporting cycles accommodate the bandwidth overhead associated with lattice-based signatures or encrypted session metadata.
- A high PRR at longer ranges ensures that secure telemetry and integrity-protected commands can be delivered reliably even at remote installations.

This lays the groundwork for future deployments where LoRa connectivity is combined with post-quantum cryptographic primitives to provide confidentiality, integrity, and long-term resilience for grid-critical monitoring assets.

6. Setup and Test Analysis—Raspberry Pi LoRa Testbed

A Raspberry Pi-based LoRa testbed was developed to validate the performance of LoRa communication under controlled conditions and to supplement the field measurements conducted at the 11 substations. The setup consisted of a Raspberry Pi 4 Model B connected to an SX1276-based LoRa transceiver module operating at 868/915 MHz. Python 3.11-based libraries (e.g., pyLoRa and lorapy) were used to configure the LoRa PHY parameters, including spreading factor (SF7–SF12), bandwidth (125 kHz), coding rate (4/5), and transmit power (2–20 dBm).

The testbed enabled repeatable experiments to assess transmission reliability, the packet reception ratio (PRR), and the impact of different LoRa configurations on airtime and energy consumption. Raspberry Pi also served as the platform for evaluating the integration of NTRU post-quantum encryption at the application layer. Timing measurements were

collected to determine processing delays, CPU utilisation, and additional communication overhead introduced by encrypted payloads, as summarised in Table 3.

Table 3. AES vs. NTRU processing & communication impact.

Factor	LoRa with AES-128 (Standard LoRaWAN Security)	LoRa with NTRU Post-Quantum Encryption
Cryptographic Type	Symmetric block cipher	Lattice-based PQC (public-key)
Processing Time per Packet (Raspberry Pi)	~0.5–1 ms	4–12 ms (key-pair + encrypt)
Payload Size Impact	No increase (16-byte block)	+32–64 bytes depending on ciphertext
Communication Overhead	Very low	Moderate (increased airtime due to larger packets)
Energy Consumption	Lowest; negligible CPU load	~20–40% higher CPU energy per message
LoRa Airtime Impact	Minimal	Airtime increases 10–25% depending on SF
Duty-Cycle Impact	No effect	Slight impact in long-range SF12 mode
Implementation Complexity	Native LoRaWAN standard	Additional application-layer crypto library
Security Strength	Secure against classical attacks	Resistant to classical + quantum attacks
Suitability for IoT Devices	Ideal for ultra-low power sensors	Suitable for fixed or powered smart-grid devices
Long-Term Data Confidentiality	Vulnerable to “store-now, decrypt-later”	Strong; designed for future quantum security

Testing was performed in both indoor and outdoor line-of-sight (LOS) and non-LOS conditions within the eThekweni region. Each configuration was repeated 30–50 times to produce statistically meaningful results. Raspberry Pi recorded transmission timestamps, RSSI, SNR, and processing time, enabling detailed analysis of LoRa performance and overhead under practical utility-oriented conditions.

Analysis of the Raspberry Pi LoRa Testbed Results

The Raspberry Pi testbed results show that standard AES-128 security introduces almost no computational or communication overhead, making it ideal for low-power LoRaWAN Class A devices. The processing latency remained under 1 ms, and the RF airtime was unaffected because AES operates after LoRaWAN frame construction. This confirms why AES is suitable for large-scale utility IoT deployments where battery life is critical.

The integration of NTRU post-quantum encryption produced an expected increase in processing time due to lattice-based mathematical operations. Encryption and key handling still remained within a few milliseconds on Raspberry Pi, which is acceptable for applications with low update intervals, such as transformer monitoring, fault notification, and periodic SCADA telemetry. The ciphertext expansion added 32–64 bytes per packet, resulting in longer airtime at higher spreading factors, especially SF11 and SF12. However, the overhead stayed within LoRaWAN’s duty-cycle limits and did not disrupt communications.

Despite the added computational cost, NTRUs’ application-layer encryption did not interfere with the LoRaWAN MAC layer, preserving interoperability with existing gateways and network servers. This layered approach aligns with best practices for enhancing LoRaWAN security without modifying the protocol stack.

Overall, the analysis demonstrates that NTRU provides strong future-proof security with manageable overhead for smart grid applications that transmit small, infrequent

packets. AES remains optimal for battery-dependent sensors, while an NTRU is best suited for critical infrastructure devices requiring long-term confidentiality and resilience against quantum adversaries.

7. Conclusions and Future Considerations

This study examined the practicality of employing LoRa technology as a communication platform within modern smart grid environments. Several representative use cases were explored, particularly those involving remote field devices that operate without convenient access to a.c. power and only require periodic data exchanges. These characteristics align well with the low-power and long-range advantages inherent to LoRa systems.

Field measurements conducted across multiple substations within the eThekwinini region showed that LoRa is capable of sustaining communication links over distances exceeding 30 kilometres, even within a densely built urban landscape. The analysis further revealed that packet delivery performance is highly sensitive to the selected spreading factor and transmit power, with different combinations producing varying levels of reception success across the network. Despite this variability, the results confirm that LoRa can achieve reliable communication at ranges approaching 34 km when parameters are optimally configured.

For typical monitoring and status-reporting applications in the smart grid, the observed update intervals at approximately 66 s for SF11 and 136 s for SF12 were found to be acceptable. However, the improved range offered by higher spreading factors comes at the cost of increased energy consumption, highlighting a necessary trade-off for battery-powered devices. Overall, the findings indicate that LoRa presents a technically viable and operationally efficient option for the types of remote monitoring applications currently under consideration by eThekwinini Electricity.

The study also observed that public LoRaWAN networks may provide enhanced performance due to the wider distribution of gateways, which increases the likelihood of successful packet reception. Nevertheless, integrating critical smart grid systems with public communication infrastructure introduces cybersecurity and resilience challenges. Future work should therefore focus on designing a comprehensive security framework for linking SCADA and other grid-control environments with public LoRa networks, including measures for authentication, data protection, secure gateway handling, and system hardening.

The Raspberry Pi LoRa testbed validated that integrating post-quantum NTRU encryption at the application layer is feasible for smart grid devices, providing long-term confidentiality without compromising communication reliability. AES remains suitable for standard battery-powered sensors, while an NTRU offers future-proof security for critical infrastructure devices, demonstrating the potential for layered security approaches in operational LoRa deployments.

Author Contributions: Conceptualization, Z.P.K.; methodology, Z.P.K.; software, Z.P.K.; validation, Z.P.K.; formal analysis, Z.P.K.; investigation, Z.P.K. and R.S.; resources, Z.P.K.; data curation, R.S.; writing—original draft preparation, Z.P.K.; writing, Z.P.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All original contributions are included in the article, and further inquiries should be directed to the corresponding author.

Conflicts of Interest: Author Resham Singh was employed by eThekweni Electricity Durban. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

- McKinsey & Co. Accelerating the Value of the Internet of Things. 2020. Available online: <https://www.mckinsey.com> (accessed on 23 August 2025).
- Lima, W.G.; Lopes, A.V.; Cardoso, C.M.; Araújo, J.P.; Neto, M.C.; Tostes, M.E.; Nascimento, A.A.; Rodriguez, M.; Barros, F.J. LoRa Technology Propagation Models for IoT Network Planning in the Amazon Regions. *Sensors* **2024**, *24*, 1621. [CrossRef] [PubMed]
- Kadusic, E.; Zivic, N.; Ruland, C.; Hadzajlic, N. A Smart Parking Solution by Integrating NB-IoT Radio Communication Technology into the Core IoT Platform. *Future Internet* **2022**, *14*, 219. [CrossRef]
- Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT. In *Proceedings of the IEEE PerCom Workshops*; IEEE: New York, NY, USA, 2018; pp. 197–202. [CrossRef]
- Semtech. What Are LoRa and LoRaWAN? 2024. Available online: <https://lora-developers.semtech.com> (accessed on 25 August 2025).
- Tulka, T. LoRa Spreading Factor Explained. 2024. Available online: <https://blog.ttulka.com> (accessed on 5 September 2025).
- Krug, S.; O’Nils, M. IoT Communication Introduced Limitations for High Sampling Rate Applications. In *GI/ITG KuVS Fachgespräch Sensornetze (FGSN 2018)*; Technische Universität Braunschweig: Braunschweig, Germany, 2018. [CrossRef]
- Cisco. Distribution Automation—Feeder Automation: Design Guide. 2020. Available online: <https://www.cisco.com> (accessed on 16 September 2025).
- IEEE. P1815 Standard for Electric Power Systems Communications—Distributed Network Protocol (DNP3). 2012. Available online: <https://standards.ieee.org> (accessed on 22 September 2025).
- Multitech. MultiTech mDot Box. 2024. Available online: <https://multitech.com> (accessed on 26 September 2025).
- The Things Network. The Things Network Coverage Map. 2024. Available online: <https://www.thethingsnetwork.org/map> (accessed on 4 October 2025).
- Semtech. SEMTECH SX1276/77/78/79. 2020. Available online: <https://semtech.com> (accessed on 16 October 2025).
- Augustin, A.; Yi, J.; Clausen, T.; Townsley, W.M. A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. *Sensors* **2016**, *16*, 1466. [CrossRef] [PubMed]
- Nexitivity. Understanding LTE Signal Strength Values. 2022. Available online: <https://support.cel-fi.com/hc/en-us/articles/1260805036129-Understanding-LTE-Signal-Strength-Values> (accessed on 20 October 2025).
- Singh, R. LoRaWAN for Remote Monitoring Applications in the Smart Grid-A Utility Perspective. In *2024 IEEE PES/IAS PowerAfrica*; IEEE: New York, NY, USA, 2024.
- Semtech. IPv6 Officially Enters the LoRaWAN® Ecosystem. 2024. Available online: <https://blog.semtech.com/ipv6-officially-enters-the-lorawan-ecosystem> (accessed on 25 October 2025).
- Fehér, M.; Rötter, D.E.L.; Hansen, M.T.; Vester, F.E. Stream Compression of DLMS Smart Meter Readings. In *Proceedings of the ICC 2022-IEEE International Conference on Communications*; IEEE: New York, NY, USA, 2022; pp. 5517–5522. [CrossRef]
- Elshabrawy, T.; Robert, J. Analysis of BER and Coverage Performance of LoRa Modulation under Same Spreading Factor Interference. In *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*; IEEE: New York, NY, USA, 2018; pp. 1–6.
- Avbentem. Airtime Calculator for LoRaWAN. 2024. Available online: <https://avbentem.github.io/airtime-calculator> (accessed on 27 October 2025).
- Mnguni, S.; Mudali, P.; Abu-Mahfouz, A.M.; Adigun, M. Performance Evaluation of Spreading Factors in LoRa Networks. In *Towards New e-Infrastructure and e-Services for Developing Countries: 12th EAI International Conference, AFRICOMM 2020, Proceedings*; Springer: Cham, Switzerland, 2021; pp. 203–215. [CrossRef]
- Mosca, M. Cybersecurity in an Era with Quantum Computers: Will We Be Ready? *IEEE Secur. Priv.* **2018**, *16*, 38–41. [CrossRef]
- Hoffstein, J.; Pipher, J.; Silverman, J.H.; Whyte, W. NTRUEncrypt: A Description of the Encryption Scheme. In *NTRU Cryptosystems Technical Report*; NTRU Cryptosystems, Inc.: Burlington, MA, USA, 2001.
- NIST. Post-Quantum Cryptography Standardization—Finalists and Standards. 2024. Available online: <https://csrc.nist.gov/projects/post-quantum-cryptography> (accessed on 28 October 2025).
- Singh, A.K. Evaluating Lightweight Post-Quantum Cryptography for IoT and LPWAN Devices. *IEEE Internet Things J.* **2023**, *10*, 13500–13512.
- Khumalo, Z.P.; Ngongoma, M.S.; Sibabda, E.; Malele, V.; Singh, N.R.; Maswanganyi, R.C.; Mbatha, C.N. Lightweight secured power line communication based network for advanced metering in smart grids. In *Proceedings of the IEEE PES/IAS Power Africa, Cairo, Egypt, 28 September–2 October 2025*; IEEE: New York, NY, USA, 2025; pp. 1–6. [CrossRef]

26. Khumalo, P.; Tsoeu, M.S.; Moloi, K. Lightweight scheme for security and privacy in smart grids applications. In *International Conference on Intelligent and Innovative Computing Applications*; Pearle Beach Resort & Spa: Flic en Flac, Mauritius, 2024; pp. 190–204. [[CrossRef](#)]
27. Bopape, L.P.; Nleya, B.; Khumalo, P. A Privacy and Security Preservation Framework for D2D Communication Based Smart Grid Services. In *Proceedings of the IEEE Conference on Information Communications Technology and Society (ICTAS)*, Durban, South Africa, 11–12 March 2020; pp. 1–6. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.