A Survey on LPWAN Technologies: LoRa, ZigBee 3.0, 6LoWPAN, and Related Protocols in IoT

www.surveyx.cn

Abstract

This survey paper provides a comprehensive analysis of Low-Power Wide-Area Networks (LPWANs) and their integral role in the Internet of Things (IoT) ecosystem. Highlighting technologies such as LoRa, ZigBee 3.0, and 6LoWPAN, the paper underscores their contributions to enhancing network scalability, energy efficiency, and communication reliability. Key advancements include DSME-LoRa's superior performance over LoRaWAN in packet reception and transmission delays, and LoRaWAN's effectiveness in urban traffic monitoring. Despite these advancements, challenges in device density management, network scalability, and security persist. The paper discusses the implications of these challenges and explores future research directions, such as refining models for complex traffic patterns, adaptive bitrate allocation, and enhancing simulation models with real-time data. Innovative frameworks like EnvSen for wildfire tracking and design principles for low-power protocols are also examined. The survey concludes that while LPWAN technologies continue to evolve, addressing current challenges is crucial for their future development. By pursuing innovative research and refining existing methodologies, LPWANs can further enhance their scalability, efficiency, and security, ensuring their continued relevance and impact in the dynamic IoT landscape.

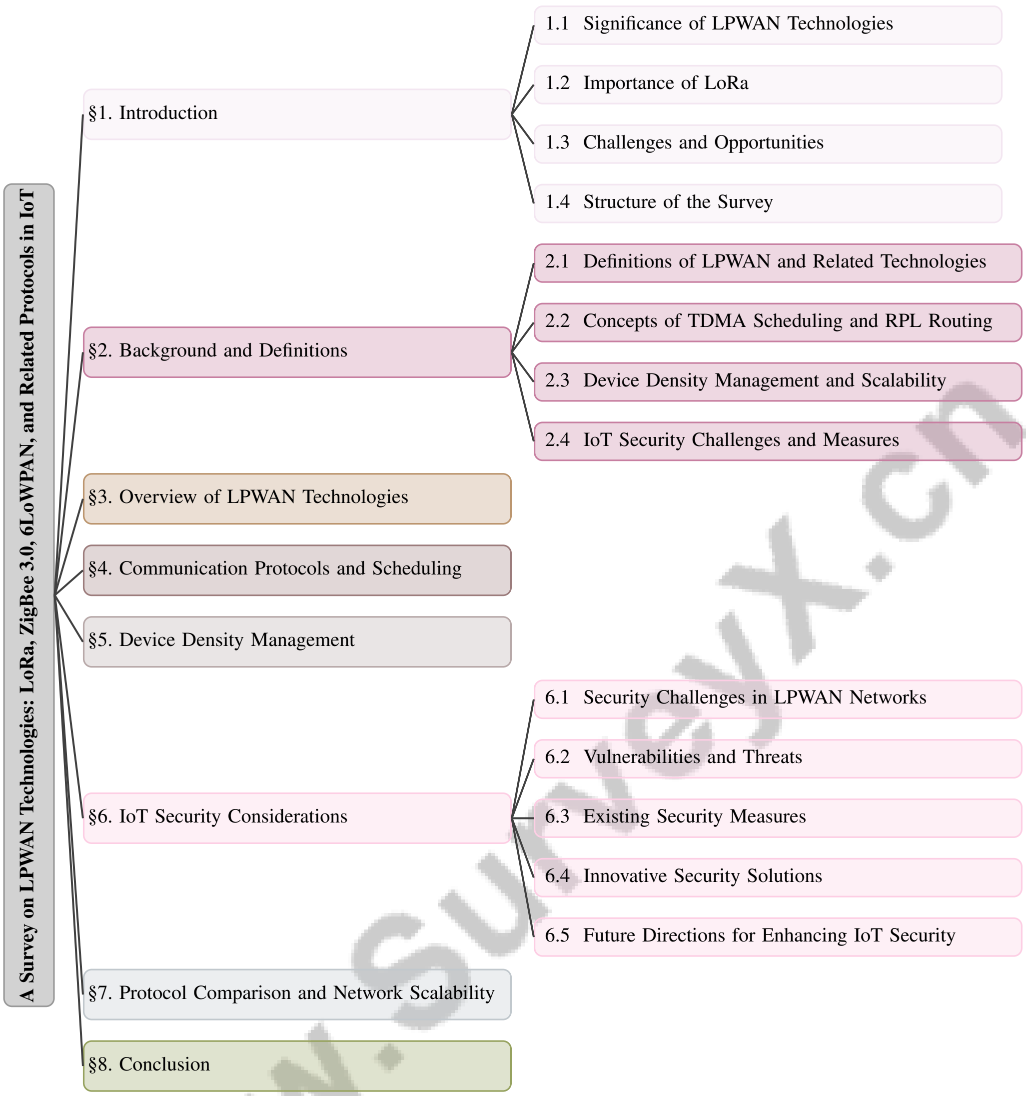
1 Introduction

1.1 Significance of LPWAN Technologies

Low-power wide-area networks (LPWANs) are essential in the Internet of Things (IoT) ecosystem, offering long-range connectivity with minimal power consumption, crucial for diverse IoT applications [1]. The transition from design and standardization to commercialization highlights their scalability as IoT device numbers increase [2]. Technologies like LoRa excel in facilitating communication over vast distances while ensuring energy efficiency, which addresses the limitations of traditional multihop wireless networks [3]. This capability is vital for IoT deployments in urban and suburban settings, where terrestrial structures can obstruct signal coverage [4].

LPWAN technologies also enhance network resiliency, particularly in safety-critical applications that require reliable connectivity [5]. For instance, they are instrumental in vehicular safety through the development of Vehicular Ad-Hoc Networks (VANETs) [6]. Furthermore, LPWANs like LoRaWAN support massive Machine-Type Communications (mMTC), a cornerstone of next-generation wireless systems beyond 5G [7]. They improve network throughput by mitigating packet collisions at gateways, thus enhancing overall network performance [8].

The adoption of LPWAN technologies is evident in Smart Cities, Smart Grids, and the Industrial Internet of Things, providing the infrastructure necessary for scalable and efficient communication [9]. These technologies enable low-power, long-range connectivity essential for various use cases, improving communication and routing protocols in IoT environments [10]. Additionally, LPWANs accommodate a vast number of IoT devices with low power requirements, underscoring their advantages across diverse applications [6].



=0

Figure 1: chapter structure

1.2 Importance of LoRa, ZigBee 3.0, and 6LoWPAN

LoRa, ZigBee 3.0, and 6LoWPAN are integral to the IoT landscape, each offering unique advantages tailored to specific application needs. LoRa is celebrated for its long-range communication and low energy consumption, making it ideal for smart metering and agricultural applications [11]. The stochastic-geometric model in LoRa networks aids in analyzing packet reception probabilities, enhancing understanding of its applications in IoT [12]. However, urban deployments face challenges from bandwidth congestion and latency, prompting the development of benchmarks to address these issues [13]. The Data Rate and Channel Control (DRCC) scheme has been proposed to allocate transmission parameters efficiently, reducing collision probabilities and enhancing network performance [14]. Furthermore, DSME-LoRa integrates the DSME MAC layer with LoRa, promoting seamless long-range communication in IoT networks [15]. Innovative approaches, such as using UAVs to assess LoRa signal strength, provide insights for improving signal coverage [16]. The integration of wake-up radios (WuR) into LoRa networks further boosts energy efficiency during data collection from sensor nodes [17].

ZigBee 3.0 excels in low-power, low-data-rate applications, particularly in home automation, industrial control, and health monitoring. Its mesh network topology enhances reliability and scalability, ensuring robust communication in high-density environments. The interoperability of ZigBee 3.0 with other ZigBee devices allows for seamless integration into existing networks, facilitating deploy-

AI-generated, for reference only.

ment flexibility. A comparative performance evaluation of ZigBee and LoRa in energy-efficient IoT applications within school buildings illustrates the practical utility of these technologies [18].

6LoWPAN extends IPv6 capabilities to resource-constrained IoT devices, enabling efficient IP-based communication across diverse networks. This is crucial for applications requiring consistent connectivity and interoperability, such as smart cities and environmental monitoring. Wireless sensor networks utilizing 6LoWPAN support real-time monitoring and control, enhancing user interaction with devices. Advanced network-based mobility management schemes within 6LoWPAN address limitations of traditional host-based protocols, ensuring seamless connectivity by tackling challenges like handover latency and packet loss, particularly in time-sensitive applications [19, 20].

Collectively, LoRa, ZigBee 3.0, and 6LoWPAN form the backbone of IoT applications, contributing to the ecosystem's scalability, efficiency, and reliability. The integration of advanced wireless communication technologies, such as LoRa, with dedicated sensors enhances the performance and scalability of smart technologies, facilitating innovative applications like integrated sensing and communication (ISAC) in the IoT landscape. This convergence improves data collection and processing capabilities while addressing interoperability challenges among diverse IoT devices, driving advancements in areas like environmental monitoring and smart building automation [21, 22].

1.3 Challenges and Opportunities

The LPWAN ecosystem faces several challenges that impede optimal functionality within the IoT landscape. Scalability issues arise from interference in heavily loaded networks, reducing reliability as user numbers increase [23]. This is particularly pronounced in LoRaWAN, where the absence of channel sensing leads to increased packet collisions as IoT device density rises [24]. Furthermore, the centralized design of LoRaWAN, while facilitating uplink-oriented data sharing, complicates direct communication necessary for distributed applications, resulting in increased costs and inefficiencies [15].

Energy consumption remains a significant challenge, as existing solutions like LoRaWAN grapple with high energy demands and routing inefficiencies in lossy networks, leading to suboptimal performance in IoT applications [9]. The limitations of conventional LoRaWAN data transfer mechanisms exacerbate scalability and energy consumption issues [5]. Optimizing communication decisions of IoT sensors to ensure accurate data collection while adhering to power and bandwidth constraints is essential [1].

Security vulnerabilities are critical concerns, with traditional jamming effects on LoRa networks inadequately explored, highlighting the need for effective mitigation strategies [25]. Regulatory limitations on transmission power, duty cycles, and frequency bands further restrict the potential for massive device deployment [6].

Despite these challenges, the LPWAN ecosystem presents substantial opportunities. Innovations in network architecture and signal processing can enhance overall performance, addressing current limitations. The integration of resilient edge computing solutions can alleviate bandwidth constraints and improve Quality of Service (QoS) [26]. Additionally, tackling mixed-integer non-linear optimization problems related to resource management could yield more efficient strategies, supporting the continued growth and scalability of the LPWAN ecosystem [27].

By addressing mobility-related challenges and leveraging new technological advancements, LPWAN technologies can effectively meet the growing demands of IoT applications, which require low power consumption, reliable connectivity, and extensive range. While LPWAN offers significant advantages in energy efficiency and coverage, its performance can be affected by the mobility of connected devices. Thus, developing mobility-aware LPWAN protocols is crucial for enhancing suitability across a diverse range of IoT scenarios, including industrial applications and smart-city initiatives [28, 23, 29, 30, 31].

1.4 Structure of the Survey

This survey is structured to provide a comprehensive overview of LPWAN technologies and their role in the IoT ecosystem. It begins with an **Introduction**, highlighting the significance of LPWAN technologies and introducing LoRa, ZigBee 3.0, and 6LoWPAN, along with the challenges and opportunities in this domain. The **Background and Definitions** section follows, offering essential

AI-generated, for reference only.

definitions and explanations of core concepts, including LPWAN, TDMA scheduling, RPL routing, and IoT security measures, setting the stage for subsequent analysis.

The third section, **Overview of LPWAN Technologies**, delves into the technical specifications, operational principles, and applications of LoRa, ZigBee 3.0, and 6LoWPAN, providing insights into their integration and use cases in IoT. The survey then explores **Communication Protocols and Scheduling**, focusing on TDMA scheduling and RPL routing, analyzing their roles in managing communication and data delivery in LPWAN networks.

In the **Device Density Management** section, strategies for managing device density and optimizing network resources are examined, highlighting their impact on network performance and scalability. This is followed by a detailed analysis of **IoT Security Considerations**, discussing security challenges, potential threats, existing measures, and innovative solutions, along with future directions for enhancing IoT security.

The penultimate section, **Protocol Comparison and Network Scalability**, provides a comparative analysis of different communication protocols based on performance metrics such as scalability and efficiency, addressing scalability challenges and proposing potential solutions. Finally, the **Conclusion** summarizes the key findings of the survey and reflects on the future prospects of LPWAN technologies in the evolving IoT landscape.The following sections are organized as shown in Figure 1.

2 Background and Definitions

2.1 Definitions of LPWAN and Related Technologies

Low-power wide-area networks (LPWANs) are fundamental to the Internet of Things (IoT), offering extensive communication coverage with minimal energy use, ideal for applications requiring widespread connectivity and prolonged battery life [28, 32]. LoRa, a prominent LPWAN technology, employs chirp spread spectrum (CSS) modulation for enhanced interference resistance, facilitating reliable long-distance communication [33]. Operating in unlicensed frequency bands, LoRa performs well indoors, but challenges in transmission parameter selection in crowded environments necessitate efficient management strategies [12, 14]. Urban signal degradation and long packet durations due to low data rates increase collision probabilities, particularly in dense networks [4, 34]. The ALOHA protocol used by LoRaWAN's MAC layer leads to high collision rates, with collision resolution among multiple devices being a core challenge [24, 35].

ZigBee 3.0, based on the IEEE 802.15.4 standard, is suited for low-power, low-data-rate applications, excelling in environments like home automation and industrial control through its mesh network topology, ensuring reliable communication even in dense settings. Its interoperability facilitates seamless integration into existing networks, enhancing deployment flexibility. Comparative studies indicate LoRa's superior reliability and performance in educational settings [18].

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) extends IPv6 capabilities to constrained devices, enabling efficient IP-based communication across diverse networks, crucial for smart cities and environmental monitoring [36]. However, interoperability issues among various 6LoWPAN implementations can hinder communication, which P6LoWPAN addresses by enhancing interoperability among low-power devices with differing capabilities [37].

Collectively, LPWAN technologies like LoRa, ZigBee 3.0, and 6LoWPAN address unique IoT challenges, such as energy consumption and network scalability, while supporting the integration of numerous devices into the IoT landscape [38]. They enable reliable data transmission over long distances, enhancing IoT system performance. Developing standardized methods for precise localization in LPWANs is critical for applications like asset tracking, where accurate location data is essential [39].

2.2 Concepts of TDMA Scheduling and RPL Routing

Time Division Multiple Access (TDMA) scheduling and the Routing Protocol for Low-Power and Lossy Networks (RPL) are crucial for managing communication within LPWANs, enhancing network efficiency and reliability. TDMA scheduling allocates specific time slots for data transmissions, minimizing collision probabilities and optimizing throughput in high-density networks [40]. This approach is particularly beneficial where energy efficiency and Quality of Service (QoS) are critical, such as in Wireless Sensor Networks (WSNs) [41]. In LoRa networks, understanding interference effects and packet reception probabilities is essential for optimizing TDMA scheduling, informed by stochastic geometry analyses.

RPL, a widely adopted standard for routing in resource-constrained nodes, constructs a Destination-Oriented Directed Acyclic Graph (DODAG) for efficient data routing in low-power and lossy networks. This protocol addresses issues like skewness and load imbalance in the DODAG structure, which can lead to inefficient data transmission and network disconnections [42]. Integrating RPL with IEEE 802.15.4, particularly by encapsulating RPL DIO messages in beacon frames, enhances routing efficiency [43]. Performance comparisons of RPL with other protocols, such as LOADng, underscore its suitability for home automation and similar applications [44].

The synergy between TDMA scheduling and RPL routing is enriched by innovative approaches like Software-Defined 6LoWPAN (SD-6LoWPAN), which integrates Software Defined Networking (SDN) principles for dynamic multi-hop packet forwarding [45]. This integration allows LPWAN networks to achieve enhanced energy efficiency and link reliability, essential for supporting diverse IoT environments. Together, TDMA scheduling and RPL routing provide robust solutions for managing communication, ensuring LPWANs effectively support the growing demands of IoT applications.

2.3 Device Density Management and Scalability

Managing device density and scalability in LPWANs is crucial for maintaining network performance and reliability as the number of connected devices increases. A primary challenge in LPWAN scalability is the bandwidth limitations of the ALOHA protocol, which struggles with high node density due to frequent packet collisions and lack of synchronization [46]. Duty-cycle regulations further restrict maximum achievable throughput, limiting scalability in dense environments [47].

In LoRaWAN networks, scalability is challenged as networks expand to accommodate hundreds or thousands of end devices per gateway [48]. The effects of co-spreading factor (co-SF) and inter-spreading factor (inter-SF) interference significantly impact performance under high device density [49]. Maintaining synchronization among devices without sacrificing bandwidth is essential, as high collision rates can hinder both scalability and overall network performance [50].

Effective device density management involves optimizing base station placement and frequency assignments, critical for enhancing LPWAN scalability [51]. Mobility management presents challenges such as high handover latency, increased signaling overhead, and packet loss during handovers, affecting performance in time-critical applications [20].

Addressing these challenges requires innovative network design and operation approaches, including advanced synchronization techniques and exploring alternative communication protocols better suited for high-density environments. By strategically managing device density and scalability, LPWANs can meet the increasing demands of IoT applications, providing long-range, low-power, and cost-effective communication for diverse deployments. Recent studies indicate that LPWAN performance, particularly in mobile IoT scenarios, can be adversely affected by varying node mobility and distance from gateways. Advancements such as packet fragmentation and negative acknowledgment strategies have shown potential to enhance network performance in dense environments, improving both goodput and energy efficiency [32, 29, 23].

2.4 IoT Security Challenges and Measures

The security landscape of LPWANs within the IoT ecosystem presents significant challenges affecting network stability, data integrity, and device authentication. A major concern is the high rate of missing data due to transmission outages, complicating reliable data analysis and overall network performance [52]. Additionally, LoRaWAN's duty cycle limitations restrict downlink transmission frequency, prolonging firmware update times and potentially compromising security [53].

Network stabilization and energy consumption are critical issues, particularly when nodes fail, necessitating the rebuilding of the RPL tree in Wireless Sensor Networks (WSNs) [54]. The inefficient management of dense IoT networks is exacerbated by end-device mobility and susceptibility to jamming attacks, which severely impact packet delivery and energy efficiency [55]. Furthermore, existing benchmarks often lack sufficient sample sizes and publicly available data for validation, limiting their applicability for municipalities [4].

Device authentication remains a pressing challenge, highlighting the need for scalable solutions to manage the increasing number of IoT devices [56]. The Decreased Rank Attack in RPL networks poses another significant threat, where malicious nodes manipulate their rank to mislead traffic routing, degrading network performance [57]. Additionally, limitations in existing fragmentation strategies for 6LoWPAN, particularly regarding reliability and latency, present challenges in real-world testbed setups [58].

Exhaustion attacks that exploit communication protocols to drain device batteries represent a significant security challenge in LPWAN-based IoT networks [59], severely affecting network performance by depleting IoT device energy resources. The inefficiency of existing fixed quantization methods for key generation can lead to security vulnerabilities, necessitating adaptive quantization approaches to enhance security [60].

Addressing these challenges requires developing efficient TDMA scheduling algorithms that minimize scheduling time and adapt to dynamically changing network conditions [61]. Robust security measures must also be implemented to enhance device authentication and mitigate the effects of jamming and replay attacks. By adopting these strategies, LPWAN-based IoT networks can achieve enhanced security and reliability, ensuring efficient operation in diverse and evolving environments. The survey by Sundaram et al. explores vulnerabilities in LoRa networks and presents solutions to enhance security, emphasizing the need for ongoing research and development in this area [3].

3 Overview of LPWAN Technologies

3.1 LPWAN and Its Various Technologies

Low-Power Wide-Area Networks (LPWANs) are integral to the Internet of Things (IoT), enabling long-range communication with low power consumption, which is vital for a wide array of IoT applications [1]. Key LPWAN technologies include LoRa, Sigfox, and Narrowband IoT (NB-IoT), each tailored for specific operational contexts and use cases. Figure 2 presents a hierarchical overview of these key LPWAN technologies, highlighting their primary applications and unique features.

LoRa's chirp spread spectrum modulation supports extensive communication ranges and low power usage, making it suitable for smart agriculture and rural IoT scenarios [3]. The EnvSen framework, which utilizes multi-agent reinforcement learning, enhances environmental monitoring via LoRa, showcasing adaptability under dynamic conditions [1]. LoRa's performance in urban environments, adaptable to varying speeds and configurations, is improved through multi-sensor localization methods [4, 18].

Sigfox, with its ultra-narrowband communication, provides a cost-effective solution for low data rate applications requiring extended battery life. Its aggressive fragmentation strategy and group NACK significantly enhance network goodput and energy efficiency in dense LPWANs [32, 62]. Comparative analyses highlight the unique advantages of each LPWAN technology based on specific application needs [6].

NB-IoT offers robust coverage and high capacity, making it ideal for reliable long-term data transmission. Experiments with various NB-IoT chipsets have shown performance advantages in urban settings, where coverage and capacity are critical [63]. Hybrid link adaptation strategies further enhance its effectiveness in diverse IoT deployments [64].

LPWAN technologies form a robust framework for IoT applications, enabling long-range, low-power communication critical for efficient smart device operation. Tools like IoT-Scan, compatible with multiple protocols including LoRa and Zigbee, underscore the importance of interoperability in the IoT landscape. By leveraging each technology's strengths and addressing their limitations, the IoT ecosystem can support innovative applications across sectors. The integration of non-terrestrial networks (NTNs) can significantly enhance IoT coverage and capacity, particularly in underserved areas, expanding the reach and impact of LPWAN solutions [65]. Additionally, analytical models for understanding the mutual impacts of multiple technologies operating simultaneously improve comprehension of LPWAN performance metrics [66].

AI-generated, for reference only.

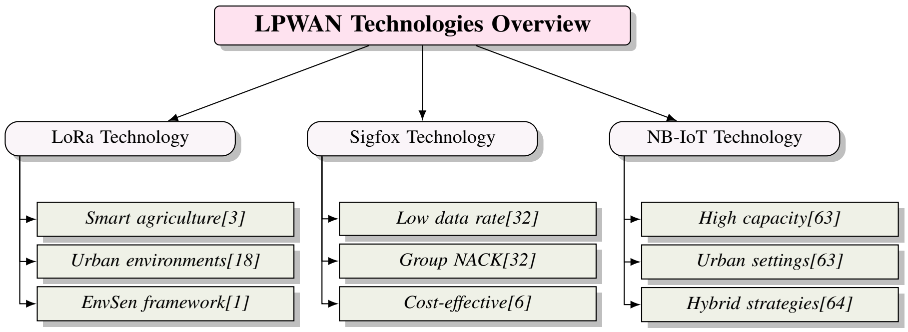


Figure 2: This figure presents a hierarchical overview of key Low-Power Wide-Area Network (LPWAN) technologies, highlighting their primary applications and unique features. The technologies include LoRa, Sigfox, and NB-IoT, each serving distinct operational contexts and use cases within the IoT ecosystem.

3.2 Technical Specifications and Operational Principles of LoRa

LoRa, a key LPWAN technology, is designed for long-range communication with minimal power consumption, essential for diverse IoT applications. Its use of chirp spread spectrum (CSS) modulation enhances resistance to interference, ensuring reliable communication over long distances [17].

LoRa's technical specifications involve managing varying node densities and transmission rates, impacting packet reception probabilities. The stochastic geometry model provides insights into uplink coverage in single gateway LoRa networks, addressing interference conditions [10]. Mathematical frameworks for computing coverage probability and area spectral efficiency in multi-gateway downlink LoRa networks further demonstrate LoRa's adaptability [4].

Innovations in LoRa's operational principles include the Long-Lived LoRa (LLL) protocol, which dynamically offloads packets from nodes with depleting resources to those with sufficient energy, enhancing network lifetime [10]. The integration of wake-up radios (WuR) into LoRa networks, as seen in the WuR-aided Data Collection Scheme (WuR-DCS), improves energy efficiency during data collection from sensor nodes [17].

LoRa's network performance is optimized through resource management techniques, such as the LoRaWAN-D2D protocol, enabling direct device-to-device communication for efficient data transfer [5]. Its adaptability in urban environments is evident, maintaining effective communication at varying speeds and configurations, influenced by the spreading factor used [4].

Security measures are integral to LoRa's operational principles, employing resilience against jamming attacks and implementing authenticated preambles to counter exhaustion attacks, preserving network integrity [17].

LoRa's technical specifications and operational principles, including CSS modulation, adaptive resource management, and innovative network architectures, underscore its potential to support a wide array of IoT applications. LoRaWAN facilitates high-density IoT device deployments by utilizing large coverage cells, optimizing communication even with low-power devices. The integration of edge processing within LoRaWAN architecture enhances performance by reducing latency and bandwidth requirements while ensuring data security and scalability, making it a robust solution for smart city applications and other IoT use cases [67, 68]. These features enable scalable, flexible, and energy-efficient communication solutions, ensuring LoRa's continued relevance in the evolving IoT landscape.

3.3 ZigBee 3.0: Technical Specifications and Applications

ZigBee 3.0, based on the IEEE 802.15.4 standard, is crucial for low-power, low-data-rate wireless communication, particularly in home automation, industrial control, and health monitoring. It emphasizes a reliable and scalable mesh network topology, enabling robust communication in high device density environments. This is facilitated through low-power Internet protocols like 6LoWPAN, which enable efficient IPv6 connectivity and address packet fragmentation challenges [37, 62]. The mesh topology enhances reliability by allowing data to hop between nodes, maintaining connectivity despite failures or obstructions.

ZigBee 3.0 supports various frequency bands, typically operating in the 2.4 GHz ISM band, with sub-GHz options to meet regional regulations and application needs. This flexibility is vital for achieving compatibility among diverse devices and networks, allowing dynamic configuration adjustments for specific communication requirements. Such adaptability facilitates seamless integration into existing systems and enhances network efficiency, as demonstrated by the Proteus gateway's ability to optimize data rates for various IoT devices, resulting in significant throughput improvements in LoRa networks. The integration of open-source platforms like KRATOS fosters innovation across heterogeneous environments [21, 69, 70, 71, 26]. ZigBee 3.0 supports data rates up to 250 kbps, sufficient for typical sensor and control data exchanges in its target applications.

A notable advantage of ZigBee 3.0 is its low power consumption, achieved through efficient power management protocols and sleep modes, significantly extending battery life. This is particularly beneficial for battery-powered devices in remote areas, where frequent replacements are impractical. The low power consumption and long-range capabilities of LPWAN enhance operational lifetime, making ZigBee 3.0 ideal for continuous connectivity in IoT applications, including emergency response during disasters [72, 73, 29, 74].

ZigBee 3.0 plays a crucial role in smart home systems, enabling seamless interconnection of devices such as lights, thermostats, and security systems, enhancing user experience and energy efficiency. It addresses interoperability challenges in the broader IoT ecosystem, supporting wireless sensor networks and contributing to smart environments that optimize resource management [18, 56, 21]. Its self-healing mesh network capability is particularly advantageous in industrial settings, facilitating machinery and process monitoring to ensure operational efficiency and safety.

Moreover, ZigBee 3.0's integration into healthcare systems provides reliable connectivity for medical devices and sensors, enabling real-time patient health monitoring and enhancing healthcare delivery. Its low latency and robust communication capabilities, exemplified by Long Range-Frequency Hopping Spread Spectrum (LR-FHSS) and Heterogeneous Efficient Low Power Radio (HELPER), ensure critical health data is transmitted accurately and promptly, facilitating timely responses in emergencies. These systems optimize packet transmission while maintaining Quality of Service (QoS) standards, enhancing reliability in both disaster scenarios and IoT applications [47, 75, 72, 26].

3.4 6LoWPAN: Integration and Use Cases

6LoWPAN, or IPv6 over Low-Power Wireless Personal Area Networks, advances IP-based communication for constrained IoT devices, bridging low-power networks with the broader Internet. This integration enhances interoperability among various IoT devices—such as RFIDs, mobile handheld devices, and wireless sensors—crucial for widespread IoT application adoption across sectors like smart agriculture, industrial automation, and environmental monitoring. By leveraging established standards like IPv6 and technologies such as LoRa, this integration addresses data transmission complexities, supporting seamless operation of applications requiring varying network resiliency and quality of service [76, 21, 22, 26].

Integrating 6LoWPAN with IPv6 facilitates efficient packet transmission over constrained link-layer technologies, addressing challenges posed by limited device resources and varying network conditions. The ICNLoWPAN framework exemplifies this by mapping Information-Centric Networking (ICN) packets onto 6LoWPAN, enhancing compatibility and performance within existing IoT infrastructures [77]. This approach is vital for applications requiring consistent connectivity and efficient data management, such as smart cities and environmental monitoring.

In healthcare, 6LoWPAN's integration with IPv6 supports low-latency, high-reliability mobility management, crucial for real-time patient monitoring and data transmission, ensuring timely and accurate care [20]. The Enhanced Location-based Routing Protocol (ELBRP) optimizes data transmission in 6LoWPAN networks by utilizing link quality and distance as routing metrics, improving performance and reliability [78].

Scalability is a critical consideration for 6LoWPAN networks, particularly in large-scale deployments. Comparative evaluations of hop-wise reassembly and direct fragment forwarding highlight their practical implications in real-world testbeds, offering insights into optimizing performance and

AI-generated, for reference only.

resource utilization [58]. Additionally, the 6RLR-ABC protocol introduces a bio-inspired swarm intelligence mechanism that enhances local repair processes, reducing energy consumption and delay while maintaining network efficiency [79].

Innovations such as the SD-6LoWPAN method leverage Software Defined Networking (SDN) principles for seamless packet forwarding in multi-hop Wireless Sensor Networks (WSNs). By utilizing a centralized SDN Controller, this approach dynamically manages routing rules, enhancing adaptability and performance [45]. Recent designs also introduce a capability spectrum that provides explicit bounds on resource usage, ensuring 6LoWPAN networks can support diverse IoT applications without compromising efficiency [37].

4 Communication Protocols and Scheduling

Effective communication within Low-Power Wide-Area Networks (LPWANs) is crucial for optimizing network performance and ensuring reliable data transmission, supporting the growing demands of Internet of Things (IoT) applications. This section explores the roles of communication protocols, with a focus on Time Division Multiple Access (TDMA) scheduling and the Routing Protocol for Low-Power and Lossy Networks (RPL). These protocols significantly enhance communication efficiency and reliability in LPWANs. The upcoming subsection will delve into the mechanisms and benefits of TDMA scheduling and RPL routing, highlighting their synergy in establishing robust communication networks.

4.1 Communication Protocols: TDMA Scheduling and RPL Routing

Time Division Multiple Access (TDMA) scheduling and the Routing Protocol for Low-Power and Lossy Networks (RPL) are essential for optimizing communication within LPWANs, enhancing network efficiency and reliability. TDMA scheduling manages channel access by assigning specific time slots for data transmission, reducing packet collisions and improving throughput, especially in high-density environments [40]. Integrating TDMA with advanced algorithms like the DRL-based Energy Efficiency Optimization method allows dynamic adaptation to real-time conditions, further optimizing communication in LoRa networks [80]. The S-ALOHA protocol complements TDMA by segmenting the channel into time slots, reducing collisions and enhancing channel throughput [46].

RPL, tailored for low-power and lossy networks, constructs a Destination-Oriented Directed Acyclic Graph (DODAG) to optimize routing paths, ensuring reliable data transmission even in resource-constrained networks. The SB-RPL extension improves RPL's performance by incorporating skewness and subtree size into routing decisions, enhancing DODAG tree balance [42]. Approaches like SD-6LoWPAN, utilizing mesh-under forwarding below the IP layer, enhance packet handling efficiency compared to traditional route-over methods, improving RPL routing [45].

The synergy between TDMA scheduling and RPL routing is further enriched by advanced communication protocols. For example, TurboLoRa enables simultaneous transmission of multiple devices, increasing throughput without exceeding channel limits, complementing TDMA's structured access [81]. Proteus, a gateway design, allows dynamic, per-packet configuration of data rates and bandwidths based on signal characteristics, optimizing communication efficiency in LPWANs [70].

Figure 3 illustrates the hierarchical structure of communication protocols in LPWANs, focusing on TDMA scheduling, RPL routing, and advanced protocols. It highlights key methods like time slot allocation, DODAG construction, and innovative approaches such as TurboLoRa and the Proteus gateway, which are crucial for enhancing network efficiency and reliability.

Advanced techniques like the Multi-Armed Bandit approach maximize frame success rate (FSR) by independently selecting optimal channels and spreading factors (SFs), enhancing communication protocol adaptability in LPWANs [82]. Redundancy transmission protocols, using fountain coding and message replication, improve successful data delivery probability, exemplifying these protocols' role in enhancing reliability and efficiency [83]. Packet fragmentation and group NACK methods significantly enhance data transmission efficiency in LPWANs under duty cycle restrictions [32].

Integrating TDMA scheduling and RPL routing within LPWANs enhances communication efficiency and supports scalable, adaptive network management. By leveraging advanced LPWAN protocols like LoRa, Sigfox, NB-IoT, and LTE-M, these networks effectively address the connectivity demands of

IoT applications. Their long-range, low-power, and cost-efficient communication capabilities ensure robust data transmission across diverse environments. However, LPWAN performance is sensitive to mobility, especially as distance from the gateway increases, necessitating the development of mobility-aware protocols. This adaptability is crucial for the next industrial revolution, where seamless communication among numerous IoT devices is essential for efficient operations [28, 31, 29, 30].

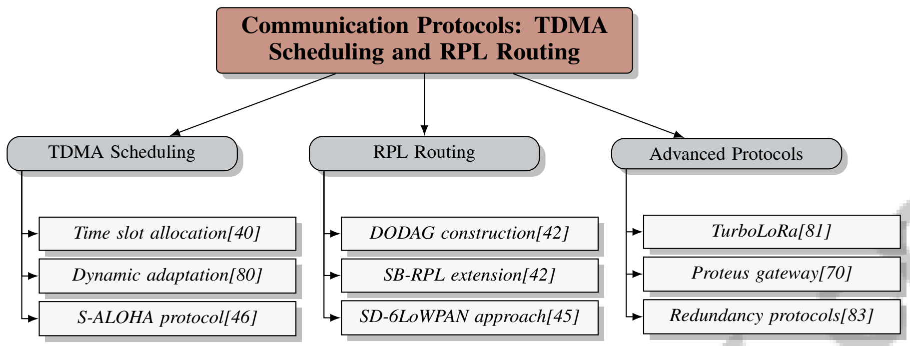


Figure 3: This figure illustrates the hierarchical structure of communication protocols in LPWANs, focusing on TDMA scheduling, RPL routing, and advanced protocols. It highlights key methods like time slot allocation, DODAG construction, and innovative approaches such as TurboLoRa and Proteus gateway, crucial for enhancing network efficiency and reliability.

4.2 Routing Protocols and Data Delivery

Routing protocols are vital for efficient and reliable data delivery in Low-Power Wide-Area Networks (LPWANs), characterized by constrained resources and diverse deployment scenarios. The Routing Protocol for Low-Power and Lossy Networks (RPL) is a prominent protocol for such environments, offering robust solutions for data routing by constructing a Destination-Oriented Directed Acyclic Graph (DODAG) that optimizes path selection and minimizes energy consumption [44]. RPL's ability to maintain shorter delays and lower control overhead than alternatives like LOADng underscores its effectiveness in enhancing network performance and reliability.

The Enhanced Location-Based Routing Protocol (ELBRP) exemplifies advancements in routing strategies by minimizing energy consumption and maximizing data transmission reliability through optimal path selection [78]. This approach is beneficial in scenarios where energy efficiency and data integrity are crucial, ensuring effective IoT device operation over extended periods without frequent energy replenishment.

Despite advancements in routing protocols, challenges remain, particularly in dense network deployments where duty-cycle regulations and network collisions can impact performance. Studies highlight limitations imposed by these factors, leading to increased packet loss and reduced throughput [84]. Addressing these challenges requires innovative scheduling and routing strategies that adapt to LPWANs' dynamic conditions.

Integrating TDMA scheduling with routing protocols offers a promising solution by providing structured access to communication channels, reducing packet collisions, and optimizing throughput. The two-phase scheme for distributed TDMA scheduling, evaluated using the Castalia network simulator, shows significant improvements in schedule length and scheduling time compared to existing algorithms, highlighting its potential to enhance data delivery efficiency in LPWANs [61].

In the context of Low-Power Wide-Area Networks (LPWANs), effective device density management and optimization techniques are critical for enhancing network performance and scalability. Figure 4 illustrates the hierarchical structure of these techniques, highlighting the challenges and solutions associated with improving both performance and scalability, as well as strategies for resource optimization. This visual representation serves not only to clarify the complexities involved but also to underscore the importance of a structured approach in addressing the multifaceted issues that arise in the deployment of LPWANs. By examining this figure, readers can better appreciate the interconnectedness of various optimization strategies and the overarching need for effective management in the context of increasing device density.

AI-generated, for reference only.

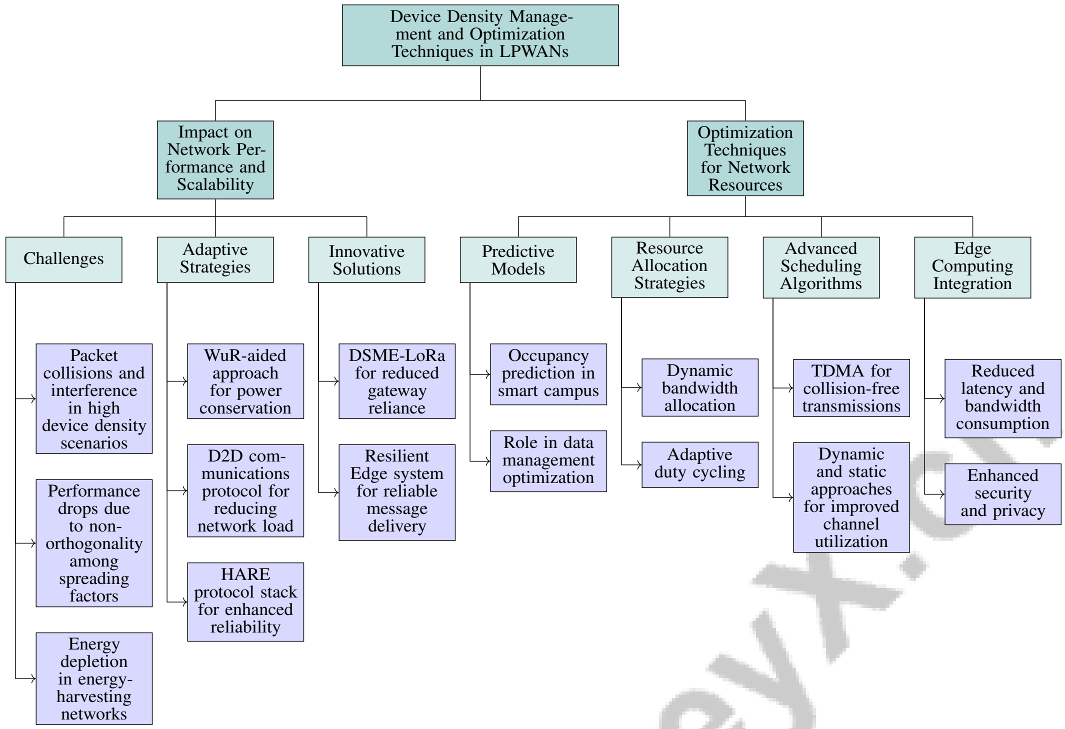


Figure 4: This figure illustrates the hierarchical structure of device density management and optimization techniques in Low-Power Wide-Area Networks (LPWANs), highlighting the challenges and solutions for improving network performance and scalability, as well as resource optimization strategies.

5 Device Density Management

5.1 Impact on Network Performance and Scalability

Device density critically impacts the performance and scalability of Low-Power Wide-Area Networks (LPWANs), especially in LoRa-based systems. As the number of connected devices increases, packet collisions and interference rise, degrading network throughput and reliability. This issue is acute in urban settings with dense infrastructure, such as smart meters, where efficient communication is essential [11]. The assumption of complete orthogonality among spreading factors often results in performance drops in high-density scenarios, necessitating effective management strategies [12].

Adaptive strategies are crucial to mitigate the adverse effects of high device density. The WuR-aided approach enables sensors to activate only when needed, conserving power and improving network performance [17]. The D2D communications protocol supports direct device-to-device interactions, reducing network load and alleviating density-related challenges [5]. Similarly, the HARE protocol stack enhances reliability and energy efficiency in dense networks [7].

The Long-Lived LoRa (LLL) protocol evaluates device density's impact on network performance and scalability, focusing on the rapid battery depletion in energy-harvesting LoRa networks [10]. This highlights the importance of energy-efficient strategies in dense deployments. Increasing the duty cycle and transmit power significantly boosts coverage probability and area spectral efficiency, vital for maintaining network performance in high-density environments [34].

Innovative solutions like DSME-LoRa reduce reliance on gateways, cutting infrastructure costs and enhancing communication efficiency in dense IoT scenarios [15]. The Resilient Edge system ensures reliable message delivery for high-criticality applications, effectively addressing network failure challenges in IoT environments [26].

Figure 5 illustrates the impact of device density on network performance, highlighting challenges and adaptive strategies in LPWANs, and showcasing innovative solutions to enhance scalability and reliability.

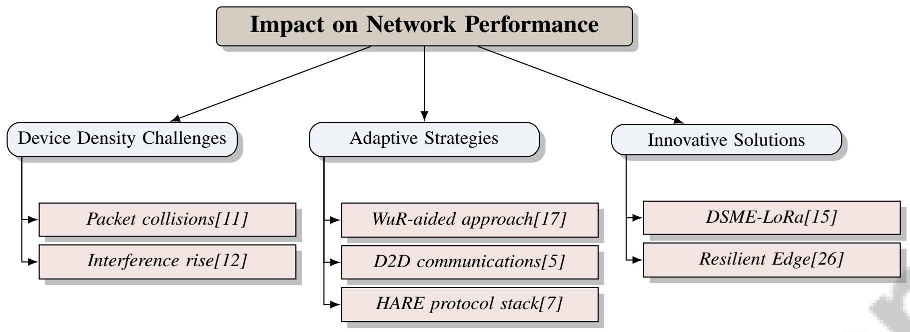


Figure 5: This figure illustrates the impact of device density on network performance, highlighting challenges and adaptive strategies in LPWANs, and showcasing innovative solutions to enhance scalability and reliability.

5.2 Optimization Techniques for Network Resources

Optimizing network resources is essential for maintaining performance as the number of connected devices in LPWANs grows. Predictive models are crucial for efficient data management; for instance, in a smart campus, models predicting occupancy based on sensor data achieved 95% accuracy [52], showcasing predictive analytics' role in optimizing data management and conserving resources.

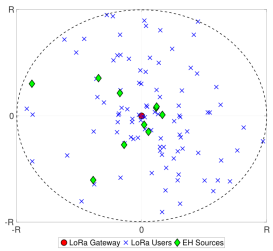
Adaptive resource allocation strategies, such as dynamic bandwidth allocation and adaptive duty cycling, are key to optimizing performance by adjusting resource use to real-time conditions. Studies on RPL with Time Slotted Channel Hopping (TSCH) and LoRaWAN show these methods improve energy efficiency—e.g., the Orchestra method reduces energy consumption by up to one-third during transient states—while optimizing network parameters for better capacity and fairness [54, 85].

Advanced scheduling algorithms, notably Time Division Multiple Access (TDMA), enhance channel access efficiency and minimize collision probabilities, critical for optimizing throughput in wireless sensor networks. TDMA supports energy-efficient, collision-free transmissions, beneficial for periodic traffic patterns and QoS-requiring applications. Recent TDMA scheduling advancements, including dynamic and static approaches, offer a flexible trade-off between schedule length and scheduling time, improving metrics like reduced scheduling time and enhanced channel utilization [61, 40, 86, 54]. By allocating specific time slots for data transmission, TDMA ensures efficient resource use, minimizing idle time and enhancing communication reliability.

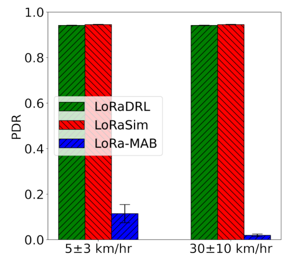
Edge computing integration significantly enhances resource optimization by shifting data processing from centralized servers to edge devices, reducing latency, minimizing bandwidth consumption, and improving scalability. This is particularly beneficial in LoRaWAN environments, where processing large data volumes locally ensures better security, privacy, and efficient resource utilization while maintaining system performance and reliability [87, 67, 26, 88]. Processing data closer to the source enables faster decision-making and more responsive network operations.

The discussed optimization techniques are crucial for enhancing LPWANs' performance and scalability, addressing challenges like energy consumption in multi-hop routing, improving goodput and energy efficiency through packet fragmentation, and facilitating seamless multi-LPWAN integration to extend coverage and manage interference [89, 90, 91, 32]. By employing predictive models, adaptive resource allocation, advanced scheduling algorithms, and edge computing solutions, networks can effectively manage resources and support the growing demands of IoT applications, ensuring reliable and efficient communication across diverse and dynamic environments.

As shown in Figure 6, device density management is crucial for enhancing communication systems' efficiency and performance. The examples illustrate various optimization techniques aimed at effectively managing network resources. The first example, a scatter plot, showcases the spatial distribution of LoRa Gateways and users within a LoRa network, emphasizing strategic placement and density management for optimal connectivity and performance. The second example presents



(a) LoRa Gateway and Users in a LoRa Network[92]



(b) Comparison of PDR performance between LoRaDRL, LoRaSim, and LoRa-MAB at different speeds[55]

Algorithm 2 Maximization of the number of nodes given the target reliability ($\mathcal{T}$) and the minimum coverage radius (R_{min}).

Input: $\mathcal{T}, p, R_{min}, \alpha_z$
Output: result, A, L, N_{max}

$\mathcal{T}_{H_1} \leftarrow \exp\left(-\frac{\mathcal{N}\psi_6}{\mathcal{P}_t g(R_{min})}\right)$
$L \leftarrow \frac{\lambda}{4\pi}\left[-\frac{\mathcal{P}_t \ln(\mathcal{T}_{H_1})}{\mathcal{N}\Psi}\right]^{\frac{1}{\eta}}$ {Equation (1)}
$R \leftarrow L[end]$
$R_z \leftarrow R$
for $i = [1, \ldots, 6]$ **do**
  for $j = [1, \ldots, 6]$ **do**
    $Y[i, j] \leftarrow f(l_i, \delta_{i,j}, l_j, l_{j+1})$
  end for
  $B[i] \leftarrow -\frac{1}{2\pi} \ln \frac{\mathcal{T}}{Z_1(l_i)\mathcal{T}_{H_1}}$
end for
$A \leftarrow Y^{-1} \times B$ {Equation (2)}
$V \leftarrow$ ComputeRingAreas(L)
$N_{max} \leftarrow (Ap) \times V'$
if $A_i \geq 0, \forall A_i$ **then**
  result $\leftarrow 1$
else
  result $\leftarrow -1$
end if
return result, A, L, N_{max}

(c) Algorithm 2: Maximization of the number of nodes given the target reliability (T) and the minimum coverage radius (Rmin).[93]

Figure 6: Examples of Optimization Techniques for Network Resources

a comparative analysis of the Performance Data Rate (PDR) across different LoRa communication systems—LoRaDRL, LoRaSim, and LoRa-MAB—at varying speeds, underscoring the significance of selecting appropriate protocols and configurations to maintain high performance under diverse operational conditions. Lastly, the third example details an algorithm designed to maximize the number of nodes while adhering to specific reliability and coverage constraints, exemplifying the intricate balance required between expanding network capacity and maintaining service quality, thereby emphasizing the role of optimization techniques in device density management [92, 55, 93].

6 IoT Security Considerations

6.1 Security Challenges in LPWAN Networks

LPWANs, including LoRaWAN, face critical security challenges that threaten their functionality within the IoT ecosystem. A significant concern is the vulnerability to jamming attacks, which exploit design weaknesses to disrupt communication [25]. This vulnerability necessitates robust interference management, especially in high-density environments where competing technologies can degrade performance [66]. Channel congestion further exacerbates these issues, leading to data loss and compromised performance [1]. The complexity of implementing capability discovery mechanisms highlights the difficulty in ensuring compliance across devices [37]. Scalability issues, particularly under heavy network loads, limit performance and are often overlooked in literature, emphasizing the need for advanced resource management [23, 9].

Synchronization algorithms are vital for reliable signal demodulation [8], yet limitations persist, such as collisions caused by hidden terminals [35]. Rapid battery depletion is a significant concern, necessitating effective energy management to maintain device reliability and security [10]. The HARE protocol stack's reliance on multi-hop communications enhances resilience against node failures, addressing security challenges related to device reliability [7].

6.2 Vulnerabilities and Threats

LPWANs are susceptible to various vulnerabilities and threats that jeopardize their security and operational stability. LoRaWAN networks are particularly exposed to selective jamming attacks, which disrupt communication between end devices and gateways [94]. The proximity of LoRa nodes to gateways complicates the implementation of uniform security measures [95]. RPL's reliance on resource-constrained nodes makes it vulnerable to attacks like the Hatchetman attack, which significantly degrade packet delivery ratios [96]. Copycat attacks further threaten RPL-based networks, necessitating effective mitigation strategies [97].

Security frameworks, such as CSM with 6LoWPAN, show potential in mitigating buffer-reservation attacks while preserving low power consumption [98]. However, the dynamic nature of 6LoWPAN presents challenges for existing IDS, which struggle to adapt to evolving data streams [99]. The Semtech Packet Forwarder protocol's lack of authentication and confidentiality allows attackers to impersonate gateways, posing significant threats [100]. Adversarial attacks across different models undermine existing classification methods, necessitating improved security measures [101].

6.3 Existing Security Measures

Security measures in LPWANs address unique vulnerabilities posed by resource-constrained IoT devices. Lightweight security approaches avoid heavy cryptographic techniques, ensuring compatibility with limited processing capabilities [96]. A multi-layered security framework categorizes research into traditional countermeasures and emerging strategies like game-theoretic methods and reinforcement learning [95]. Low-cost hardware mitigation techniques counteract jamming attacks while maintaining low complexity [94, 25]. For RPL-based 6LoWPAN networks, tailored security solutions are necessary [102]. The integration of the CSM framework enhances RPL protocol security through immediate-sender authentication and a chain-of-trust for 6LoWPAN fragments [98].

Advanced techniques such as device fingerprinting and adaptive IDS strengthen security in LPWANs. Deep learning-based device fingerprinting enhances device identification, providing an additional layer of security against unauthorized access [103]. The adaptive hybrid IDS effectively detects a wide range of RPL attacks, adapting to environmental changes [99]. Authentication preambles mitigate exhaustion attacks, ensuring device operational security [59]. The AQ-KG protocol improves key generation rates, addressing challenges posed by varying channel conditions [60]. The ChirpOTLE framework enables practical security evaluation in LoRaWAN, facilitating rapid vulnerability identification [104].

These measures underscore the commitment to enhancing the resilience and reliability of LPWANs, particularly LoRa technology, crucial for IoT applications. They address threats, including denial-of-service attacks and vulnerabilities related to packet transmission delays and loss. Recent advancements, such as authentication preambles and game-theoretic approaches, reflect a proactive stance in threat mitigation, ensuring secure communication between end devices and gateways [59, 95, 26].

6.4 Innovative Security Solutions

Innovative security solutions are essential for enhancing the resilience and reliability of LPWANs within the IoT ecosystem. Game-theoretic approaches offer promising methods for detecting and countering network attacks, such as the Hatchetman attack, without imposing significant computational overhead on devices [96]. Secure Objective Functions (Sec-OF) mitigate the Decreased Rank Attack in RPL networks by restricting node behavior [57].

Network-based mobility management solutions improve security and efficiency in 6LoWPAN by addressing the dynamic nature of IoT environments [20]. Enhancing localization accuracy through spreading factor integration contributes to future IoT security improvements [105]. Selective jamming necessitates sophisticated countermeasures to ensure network integrity [94]. Neural networks, including CNNs and FNNs, enhance countermeasure effectiveness against unauthorized jamming signals.

Adaptive security frameworks are crucial for evolving with emerging threats, particularly in RPL-based 6LoWPAN networks. Future research should integrate cross-layer security solutions to address vulnerabilities across multiple network layers [102]. The adaptive hybrid IDS learns from streaming data, detecting a broader range of RPL attacks [99].

Deep learning-based device fingerprinting enhances security against unauthorized access by relying on hardware-specific distortions [103]. The Tweak method facilitates lightweight model calibration for device authentication [106]. Authentication preambles mitigate exhaustion attacks, ensuring device operational security [59]. Identifying significant parameters affecting power consumption in RPL allows for optimization and substantial energy savings [107].

Future research should focus on optimizing blockchain-enabled solutions like HyperLoRa and exploring additional security measures to enhance robustness [87]. The ChirpOTLE framework provides practical means for evaluating LoRaWAN security, enabling rapid testing of vulnerabilities

[104]. The concept of using jamming combined with physical disconnection to disable legitimate gateways highlights the need for countermeasure development against sophisticated attacks [100].

These innovative solutions emphasize adaptive, lightweight, and robust approaches to safeguard LPWAN networks against evolving threats, ensuring secure and reliable operation within IoT applications. Future research will aim to enhance middleware support for a wider range of heterogeneous wireless sensor motes, ensuring flexibility and adaptability in IoT deployments [21]. Developing standardized regulations to facilitate global harmonization and improve spectrum efficiency is crucial for advancing LPWAN technologies [6].

6.5 Future Directions for Enhancing IoT Security

Enhancing LPWAN security within the IoT ecosystem demands integrating technological innovations and practical implementations. Future research should prioritize improving wake-up beacon reception probabilities and optimizing resource allocation to enhance network performance and efficiency [17]. Developing dynamic interference management and adaptive access control mechanisms is essential for addressing challenges posed by high-density deployments and diverse environmental conditions.

Integrating real-time environmental data into network benchmarks enhances performance evaluations by providing context-specific insights that account for energy consumption, path loss, and resilience in various scenarios, including urban and battlefield environments. This approach facilitates accurate assessments of network performance and supports efficient operation of emerging technologies like non-terrestrial networks [108, 65, 85, 54, 4]. These advancements lead to robust and scalable LPWAN solutions capable of adapting to changing conditions and maintaining reliable communication in complex environments.

Exploring advanced modulation techniques, such as DLoRa, which increases parallel channels in LoRa networks, alongside detailed topography data integration, will improve prediction accuracy and enable effective network planning. This strategy addresses interference issues in densely populated IoT environments and leverages non-terrestrial networks for reliable communication in remote areas, facilitating a more robust smart IoT ecosystem [65, 109, 22, 110, 111]. These efforts will optimize network configurations, ensuring efficient resource management and improved scalability across various deployment scenarios.

Prioritizing the refinement of security protocols to address the evolving threat landscape is crucial, particularly in enhancing resilience against jamming attacks and other interference forms. By focusing on these research directions, the IoT community can advance LPWAN solutions that are secure, efficient, and scalable to meet the increasing demands of IoT applications. This approach ensures robust protection against evolving threats, such as communication disruptions and data interception, significantly improving the security landscape of LPWAN environments. Addressing challenges posed by mobile IoT applications and varying mobility degrees will lead to the creation of mobility-aware LPWAN protocols, essential for maintaining effective communication in dynamic settings. Leveraging advanced security measures, including game-theoretic approaches and machine learning techniques, will better equip the community to adapt to emerging threats, ensuring uninterrupted and reliable connectivity for diverse IoT use cases [95, 31, 29, 30].

7 Protocol Comparison and Network Scalability

7.1 Comparative Analysis of LPWAN Technologies

Low-Power Wide-Area Networks (LPWANs) are instrumental in supporting diverse IoT applications, each offering unique advantages in scalability, energy efficiency, and cost-effectiveness. This analysis examines leading LPWAN technologies—LoRa, Sigfox, and NarrowBand-IoT (NB-IoT)—focusing on key performance metrics such as scalability, energy efficiency, throughput, and reliability. These metrics highlight the impact of network design, parameter configurations, and interference, underscoring the need for tailored setups to optimize performance [32, 23, 85, 49, 63].

LoRa excels in scalability and adaptability, leveraging chirp spread spectrum (CSS) modulation for spectral efficiency. Optimizing node density enhances reliability and throughput, with non-uniform, concave deployments offering superior coverage [112]. Parameter management, including data rate and bandwidth, significantly affects packet reception and energy use [113]. Tools like LoRaWANSim aid in optimizing network design decisions [114].

In energy efficiency, LoRa employs advanced resource management to minimize consumption while maintaining high packet delivery ratios. S-LoRa synchronizes devices to boost performance, presenting a viable protocol alternative [115]. Deep reinforcement learning (DRL) methods further enhance scalability and efficiency, especially in dense environments [70]. The HARE protocol stack offers up to 15

Sigfox's ultra-narrowband communication is cost-effective for low-data applications, such as asset tracking, due to its long battery life and low operational costs [56]. NB-IoT, a cellular LPWAN, provides robust coverage and high capacity, suitable for reliable long-term data transmission. Comparative studies show NB-IoT's energy efficiency is competitive with LoRa, though it exhibits more variability in energy usage and delays [85].

Innovative approaches like drone-aided localization enhance precision in LoRa networks, surpassing fixed setups [33]. The IoT Cloud-RAN testbed offers cost-effective synchronization and localization using existing LPWAN infrastructure [39]. The CR-MAC protocol outperforms conventional LoRaWAN, demonstrating effective communication management [35].

The comparative analysis of LPWAN technologies highlights their distinct strengths and limitations, guiding their application across various IoT scenarios. By examining performance in both mobile and stationary contexts, alongside innovations like the SNOW platform using TV white spaces, stakeholders can make informed deployment decisions, particularly considering node mobility's impact on communication reliability and efficiency [116, 29].

7.2 Protocol Comparisons and Performance Metrics

Analyzing communication protocols in LPWANs is vital for understanding their scalability, efficiency, and performance in supporting diverse IoT applications. The Routing Protocol for Low-Power and Lossy Networks (RPL) is evaluated using metrics like packet delivery ratio (PDR), latency, and skewness indexes, crucial for assessing communication reliability in resource-constrained networks [42].

The SB-RPL protocol, an RPL extension, addresses load balancing by incorporating skewness and subtree size into routing, enhancing traffic distribution and improving PDR and latency. Experiments show SB-RPL's superior performance over traditional RPL, optimizing network efficiency in dense environments [42].

LoRaWAN and Sigfox are evaluated for scalability and energy efficiency. LoRaWAN supports numerous devices with minimal energy use, aided by the adaptive data rate (ADR) mechanism, which optimizes transmission parameters to enhance capacity and minimize interference. In noisy mobile environments, a link-based ADR approach achieves a PDR 2.8 times higher than the original ADR, ensuring robust communication [117, 118].

Sigfox offers ultra-narrowband communication for low-data applications, competing with LoRaWAN's strengths and challenges in scalability and efficiency [119, 120, 121, 75, 111]. Its energy efficiency and long-range capabilities benefit remote deployments.

These protocols' performance is rigorously evaluated using simulation tools like Contiki OS and COOJA, alongside real-world testbeds, providing insights into operational characteristics across scenarios, including transient states and heterogeneous traffic patterns in dense networks. The Orchestra method significantly reduces energy consumption during RPL network transient states, while RPL generally offers lower delays and control overhead compared to LOADng [54, 44, 9].

Selecting the most suitable LPWAN protocol requires understanding factors like scalability, efficiency, reliability, power consumption, coverage, data rate, security, cost, and Quality of Service (QoS). Protocols like LoRa, Sigfox, NB-IoT, and LTE-M demonstrate superior energy efficiency and coverage, crucial for optimizing performance in diverse IoT and Industrial IoT (IIoT) scenarios. Advancements in routing techniques, such as multi-hop configurations, enhance energy savings and device lifetimes, emphasizing informed protocol selection for operational effectiveness [89, 30]. Leveraging each protocol's strengths allows IoT networks to achieve optimal performance for interconnected devices.

7.3 Scalability Solutions and Future Directions

Addressing scalability challenges in LPWANs is crucial for meeting IoT application demands. Enhancing spectral efficiency and managing interference in dense LPWAN deployments, particularly with LoRa, involves optimizing network configurations using multiple base stations and directional antennae. Research shows multiple base stations significantly improve message reception in interference-prone environments, with simulations indicating a Data Extraction Rate (DER) increase from 0.24 to 0.56 using three base stations. Optimizing end-device spatial arrangements, especially through concave configurations and controlled random access transmission, further enhances coverage and performance [112, 111]. Adaptive resource allocation and dynamic channel management significantly boost capacity, ensuring LPWANs accommodate numerous devices without compromising performance.

Advanced modulation schemes and interference mitigation strategies are vital for scalability. Techniques adjusting transmission parameters based on real-time conditions enable LPWANs to maintain efficient communication in high-density environments, enhancing throughput and extending battery life. LPWANs are suited for remote areas where traditional networks struggle, offering long-range, low-power, cost-effective communication [65, 29, 122].

Future research should refine frameworks like ChirpOTLE to better understand and mitigate LPWAN vulnerabilities [104]. Exploring attack scenarios and developing robust countermeasures are essential for LPWAN security and reliability as they scale. Integrating machine learning to predict network behavior and optimize resource allocation presents a promising scalability direction.

Efforts to standardize protocols and improve interoperability among LPWAN technologies will enhance scalability. Efficient communication across networks facilitates large-scale IoT deployment, improving resource management and utilization. Technologies like LoRa and DSME-LoRa provide long-range, energy-efficient solutions, addressing low-power device constraints while overcoming traditional gateway-centric model limitations. Integrating wireless sensor networks into IoT ecosystems enhances device interoperability, supporting applications in smart cities and agriculture. This approach optimizes data transmission and coverage, paving the way for IoT advancements [21, 15, 68, 76].

8 Conclusion

This survey underscores the pivotal role of Low-Power Wide-Area Networks (LPWANs) in the Internet of Things (IoT) ecosystem, highlighting their ability to facilitate long-range communication with minimal power usage, which is crucial for various IoT applications. Technologies such as LoRa, ZigBee 3.0, and 6LoWPAN have significantly advanced network scalability, energy efficiency, and communication reliability. Notably, DSME-LoRa has demonstrated superior performance over LoRaWAN in terms of packet reception ratios and transmission delays, showcasing its potential to improve long-range communication in IoT deployments. Additionally, the effective use of LoRaWAN end nodes in urban traffic monitoring paves the way for comprehensive traffic management solutions.

However, challenges remain in managing device density, enhancing network scalability, and ensuring security. Existing LPWAN technologies have shown substantial improvements in network throughput and efficiency, particularly with D2D communication protocols that reduce data transfer time and energy consumption, validating their use in smart grids. Future research should focus on refining models to handle complex traffic patterns and developing adaptive bitrate allocation strategies responsive to real-time network conditions. Moreover, exploring adaptive transmission parameter selection strategies is essential to improve scalability and energy efficiency while maintaining high frame success rates.

The EnvSen framework illustrates potential advancements in tracking wildfire spread accuracy while managing communication costs, suggesting future research directions in optimizing communication policies. Further studies should apply design principles to other low-power Internet protocols and seek optimizations for energy efficiency and code size. Enhancing simulation models to incorporate additional variables and real-time data, alongside integrating machine learning techniques for routing and compression optimization, represents crucial avenues for future exploration.

References

[1] Yi Hu, Jinhang Zuo, Bob Iannucci, and Carlee Joe-Wong. Intelligent communication planning for constrained environmental iot sensing with reinforcement learning, 2023.

[2] Orestis Georgiou and Usman Raza. Low power wide area network analysis: Can lora scale?, 2017.

[3] Jothi Prasanna Shanmuga Sundaram, Wan Du, and Zhiwei Zhao. A survey on lora networking: Research problems, current solutions and open issues, 2019.

[4] Michael Rademacher, Hendrik Linka, Thorsten Horstmann, and Martin Henze. Path loss in urban lora networks: A large-scale measurement study, 2021.

[5] Konstantin Mikhaylov, Juha Petäjäjärvi, Jussi Haapola, and Ari Pouttu. D2d communications in lorawan low power wide area network: From idea to empirical validation, 2017.

[6] David Castells-Rufas, Adrià Galin-Pons, and Jordi Carrabina. The regulation of unlicensed sub-ghz bands: Are stronger restrictions required for lpwan-based iot success?, 2018.

[7] Toni Adame, Sergio Barrachina, Boris Bellalta, and Albert Bel. Hare: Supporting efficient uplink multi-hop communications in self-organizing lpwans, 2017.

[8] Mathieu Xhonneux, Joachim Tapparel, Orion Afisiadis, Alexios Balatsoukas-Stimming, and Andreas Burg. A maximum-likelihood-based multi-user lora receiver implemented in gnu radio, 2020.

[9] Tayyab Mehmood. Cooja network simulator: Exploring the infinite possible ways to compute the performance metrics of iot based smart devices to understand the working of iot based compression routing protocols, 2017.

[10] Sezana Fahmida, Venkata P Modekurthy, Mahbubur Rahman, Abusayeed Saifullah, and Marco Brocanelli. Long-lived lora: Prolonging the lifetime of a lora network, 2020.

[11] Hannaneh Barahouei Pasandi, Asma Haghighat, Azin Moradbeikie, Ahmad Keshavarz, Habib Rostami, Sara Paiva, and Sergio Ivan Lopes. Low-cost traffic sensing system based on lorawan for urban areas, 2022.

[12] Bartłomiej Błaszczyszyn and Paul Mühlethaler. Analyzing lora long-range, low-power, wide-area networks using stochastic geometry, 2018.

[13] Thenuka Karunathilake and Anna Förster. Using lora communication for urban vanets: Feasibility and challenges, 2023.

[14] Qihao Zhou, Jinyu Xing, Lu Hou, Rongtao Xu, and Kan Zheng. A novel rate and channel control scheme based on data extraction rate for lora networks, 2019.

[15] José Álamos, Peter Kietzmann, Thomas Schmidt, and Matthias Wählisch. Dsme-lora: Seamless long range communication between arbitrary nodes in the constrained iot, 2022.

[16] Vageesh Anand Dambal, Sameer Mohadikar, Abhaykumar Kumbhar, and Ismail Guvenc. Improving lora signal coverage in urban and sub-urban environments with uavs, 2019.

[17] Shashank M. S. Panga and Siddhartha S. Borkotoky. Leveraging wake-up radios in uav-aided lora networks: Some preliminary results on a random-access scheme, 2023.

[18] Lidia Pocero, Stelios Tsampas, Georgios Mylonas, and Dimitrios Amaxilatis. Experiences from using lora and ieee 802.15.4 for iot-enabled classrooms, 2021.

[19] Varat Chawathaworncharoen, Vasaka Visoottiviseth, and Ryousei Takano. Feasibility evaluation of 6lowpan over bluetooth low energy, 2015.

[20] Riaz A Khan and Ajaz Hussain Mir. A study of network based mobility management schemes, 6lowpan mobility, open issues and proposed solutions, 2014.

[21] Nacer Khalil, Mohamed Riduan Abid, Driss Benhaddou, and Michael Gerndt. Wireless sensors networks for internet of things, 2016.

[22] Zhaoxin Chang, Fusang Zhang, and Daqing Zhang. An exploration on integrated sensing and communication for the future smart internet of things, 2023.

[23] Arliones Hoeller, Jean Sant'Ana, Juho Markkula, Konstantin Mikhaylov, Richard Souza, and Hirley Alves. Beyond 5g low-power wide-area networks: A lorawan suitability study, 2020.

[24] Nikos Kouvelas, Vijay Rao, and R. R. Venkatesha Prasad. Employing p-csma on a lora network simulator, 2018.

[25] Clément Demeslay, Roland Gautier, Anthony Fiche, and Gilles Burel. Band tone jamming analysis and detection on lora signals, 2021.

[26] Vijay Kumar, Poonam Yadav, and Leandro Soares Indrusiak. Resilient edge: Can we achieve network resiliency at the iot edge using lpwan and wifi?, 2022.

[27] Licia Amichi, Megumi Kaneko, Ellen Hidemi Fukuda, Nancy El Rachkidy, and Alexandre Guitton. Joint allocation strategies of power and spreading factors with imperfect orthogonality in lora networks, 2019.

[28] Min Chen, Yiming Miao, Xin Jian, Xiaofei Wang, and Iztok Humar. Cognitive-lpwan: Towards intelligent wireless services in hybrid low power wide area networks, 2018.

[29] Dhaval Patel and Myounggyu Won. Experimental study on low power wide area networks (lpwan) for mobile internet of things, 2017.

[30] Mahbubul Islam, Hossain Md. Mubashshir Jamil, Samiul Ahsan Pranto, Rupak Kumar Das, Al Amin, and Arshia Khan. Future industrial applications: Exploring lpwan-driven iot protocols, 2024.

[31] Alexandros-Apostolos A. Boulogeorgos, Panagiotis D. Diamantoulakis, and George K. Karagiannidis. Low power wide area networks (lpwans) for internet of things (iot) applications: Research challenges and future trends, 2016.

[32] Ioana Suciu, Xavier Vilajosana, and Ferran Adelantado. Aggressive fragmentation strategy for enhanced network performance in dense lpwans, 2019.

[33] Victor Delafontaine, Fabrizio Schiano, Giuseppe Cocco, Alexandru Rusu, and Dario Floreano. Drone-aided localization in lora iot networks, 2020.

[34] Lam-Thanh Tu, Abbas Bradai, and Yannis Pousset. Coverage probability and spectral efficiency analysis of multi-gateway downlink lora networks, 2022.

[35] Nancy El Rachkidy, Alexandre Guitton, and Megumi Kaneko. Ss5g: Collision resolution protocol for delay and energy efficient lora networks, 2018.

[36] Emmanuel Baccelli, Christian Mehlis, Oliver Hahm, Thomas C. Schmidt, and Matthias Wählisch. Information centric networking in the iot: Experiments with ndn in the wild, 2014.

[37] Hudson Ayers, Paul Crews, Hubert Teo, Conor McAvity, Amit Levy, and Philip Levis. Design considerations for low power internet protocols, 2020.

[38] Łukasz Marcul, Mateusz Brzozowski, and Artur Janicki. System for measurement of electric energy using beacons with optical sensors and lorawan transmission, 2024.

[39] Thomas Maul, Joerg Robert, and Sebastian Klob. Iot cloud ran testbed for ultra-precise tdoa-based localization in lpwans, 2024.

[40] Ashutosh Bhatia and R. C. Hansdah. A classification framework for tdma scheduling techniques in wsns, 2020.

[41] Xiaofan Jiang, Heng zhang, Edgardo Alberto Barsallo Yi, Nithin Raghunathan, Charilaos Mousoulis, Somali Chaterji, Dimitrios Peroulis, Ali Shakouri, and Saurabh Bagchi. Hybrid low-power wide-area mesh network for iot applications, 2020.

[42] Lam Nguyen and Chong-Kwon Kim. Towards skewness and balancing of rpl trees for the internet of things, 2019.

[43] Malisa Vucinic, Gabriele Romaniello, Laurene Guelorget, Bernard Tourancheau, Franck Rousseau, Olivier Alphand, Andrzej Duda, and Laurent Damon. Topology construction in rpl networks over beacon-enabled 802.15.4, 2014.

[44] Malisa Vucinic, Bernard Tourancheau, and Andrzej Duda. Performance comparison of the rpl and loadng routing protocols in a home automation scenario, 2014.

[45] Giacomo Tanganelli, Antonio Virdis, and Enzo Mingozzi. Enabling multi-hop forwarding in 6lowpans through software-defined networking, 2019.

[46] Tommaso Polonelli, Davide Brunelli, and Luca Benini. Slotted aloha overlay on lorawan: a distributed synchronization approach, 2018.

[47] Guillem Boquet, Pere Tuset-Peiro, Ferran Adelantado, Thomas Watteyne, and Xavier Vilajosana. Lr-fhss: Overview and performance analysis, 2020.

[48] Floris Van den Abeele, Jetmir Haxhibeqiri, Ingrid Moerman, and Jeroen Hoebeke. Scalability analysis of large-scale lorawan networks in ns-3, 2017.

[49] Aamir Mahmood, Emiliano Sisinni, Lakshmikanth Guntupalli, Raúl Rondón, Syed Ali Hassan, and Mikael Gidlund. Scalability analysis of a lora network under imperfect orthogonality, 2018.

[50] Luca Beltramelli, Aamir Mahmood, Paolo Ferrari, Patrik Österberg, Mikael Gidlund, and Emiliano Sisinni. Synchronous lora communication by exploiting large-area out-of-band synchronization, 2020.

[51] Enes Krijestorac, Ghaith Hattab, Petar Popovski, and Danijela Cabric. Multiband massive iot: A learning approach to infrastructure deployment, 2022.

[52] Eslam Eldeeb and Hirley Alves. Lorawan-enabled smart campus: The dataset and a people counter use case, 2023.

[53] Khaled Abdelfadeel, Tom Farrell, David McDonald, and Dirk Pesch. How to make firmware updates over lorawan possible, 2020.

[54] Reza Amini, Mehdi Imani, Petio Ivanov Todorov, and Maaruf Ali. Performance evaluation of orchestra scheduling in time slotted channel hopping networks, 2020.

[55] Inaam Ilahi, Muhammad Usama, Muhammad Omer Farooq, Muhammad Umar Janjua, and Junaid Qadir. Intelligent resource allocation in dense lora networks using deep reinforcement learning, 2021.

[56] Usman Raza, Parag Kulkarni, and Mahesh Sooriyabandara. Low power wide area networks: An overview, 2017.

[57] B. Ghaleb, A. Al-Dubai, A. Hussain, J. Ahmad, I. Romdhani, and Z. Jaroucheh. Resolving the decreased rank attack in rpl's iot networks, 2023.

[58] Martine S. Lenders, Thomas C. Schmidt, and Matthias Wählisch. A lesson in scaling 6lowpan – minimal fragment forwarding in lossy networks, 2019.

[59] Ioana Suciu, Jose Carlos Pacho, Andrea Bartoli, and Xavier Vilajosana. Authenticated preambles for denial of service mitigation in lpwans, 2019.

[60] Chen Chen, Junqing Zhang, and Yingying Chen. Adaptive quantization for key generation in low-power wide-area networks, 2023.

[61] Ashutosh Bhatia and R. C. Hansdah. A two-phase scheme for distributed tdma scheduling in wsns with flexibility to trade-off between schedule length and scheduling time, 2019.

[62] Ioana Suciu, Xavier Vilajosana, and Ferran Adelantado. An analysis of packet fragmentation impact in lpwan, 2018.

[63] Borja Martinez, Ferran Adelantado, Andrea Bartoli, and Xavier Vilajosana. Exploring the performance boundaries of nb-iot, 2019.

[64] Justin Chan, Anran Wang, Arvind Krishnamurthy, and Shyamnath Gollakota. Deepsense: Enabling carrier sense in low-power wide area networks using deep learning, 2019.

[65] Dengke Wang, Alessandro Traspadini, Marco Giordani, Mohamed-Slim Alouini, and Michele Zorzi. On the performance of non-terrestrial networks to support the internet of things, 2022.

[66] Meysam Masoudi, Amin Azari, Emre Altug Yavuz, and Cicek Cavdar. Grant-free radio access iot networks: Scalability analysis in coexistence scenarios, 2017.

[67] Stefano Milani, Ioannis Chatzigiannakis, Domenico Garlisi, Matteo Di Fraia, and Patrizio Pisani. Enabling edge processing on lorawan architecture, 2024.

[68] Sebastian Meiling and Thomas C. Schmidt. Lora in the field: Insights from networking the smart city hamburg with riot, 2020.

[69] Batuhan Mekiker, Mike Wittie, Jefferson Jones, and Michael Monaghan. Beartooth relay protocol: Supporting real-time application streams over lora, 2020.

[70] Zerina Kapetanovic, Deepak Vasisht, Tusher Chakraborty, Joshua R. Smith, and Ranveer Chandra. No size fits all: Automated radio configuration for lpwans, 2021.

[71] Rajeev Piyare, Amy L. Murphy, Michele Magno, and Luca Benini. Kratos: An open source hardware-software platform for rapid research in lpwans, 2018.

[72] Jithin Jagannath, Sean Furman, Anu Jagannath, Luther Ling, Andrew Burger, and Andrew Drozd. Helper: Heterogeneous efficient low power radio for enabling ad hoc emergency public safety networks, 2019.

[73] Adria Galin-Pons. Technology independent method for defining battery powered lpwan end-point lifetime estimation, 2019.

[74] You Li, Yuan Zhuang, Xin Hu, Zhouzheng Gao, Jia Hu, Long Chen, Zhe He, Ling Pei, Kejie Chen, Maosong Wang, Xiaoji Niu, Ruizhi Chen, John Thompson, Fadhel Ghannouchi, and Naser El-Sheimy. Location-enabled iot (le-iot): A survey of positioning techniques, error sources, and mitigation, 2020.

[75] Diego Maldonado, Megumi Kaneko, Juan A. Fraire, Alexandre Guitton, Oana Iova, and Herve Rivano. Enhancing lr-fhss scalability through advanced sequence design and demodulator allocation, 2024.

[76] Lameya Aldhaheri, Noor Alshehhi, Irfana Ilyas Jameela Manzil, Ruhul Amin Khalil, Shumaila Javaid, Nasir Saeed, and Mohamed-Slim Alouini. Lora communication for agriculture 4.0: Opportunities, challenges, and future directions, 2024.

[77] Cenk Gündoğan, Peter Kietzmann, Thomas C. Schmidt, and Matthias Wählisch. Icnlowpan – named-data networking for low power iot networks, 2018.

[78] M. Rehenasulthana, P. T. V. Bhuvaneswari, and N. Rama. Enhanced location based routing protocol for 6lowpan, 2012.

[79] Nurul Halimatul Asmak Ismail, Samer A. B. Awwad, and Rosilah Hassan. 6rlr-abc: 6lowpan routing protocol with local repair using bio inspired artificial bee colony, 2020.

[80] Mohammed Jouhari, Khalil Ibrahimi, Jalel Ben Othman, and El Mehdi Amhoud. Deep reinforcement learning-based energy efficiency optimization for flying lora gateways, 2023.

[81] Moez Altayeb, Marco Zennaro, Ermanno Pietrosemoli, and Pietro Manzoni. Turbolora: enhancing lorawan data rate via device synchronization, 2020.

[82] Aohan Li, Ikumi Urabe, Minoru Fujisawa, So Hasegawa, Hiroyuki Yasuda, Song-Ju Kim, and Mikio Hasegawa. A lightweight transmission parameter selection scheme using reinforcement learning for lorawan, 2022.

[83] Siddhartha S. Borkotoky. Redundancy transmission in uav-aided lora networks featuring wake-up radios, 2024.

[84] Ferran Adelantado, Xavier Vilajosana, Pere Tuset-Peiro, Borja Martinez, Joan Melia, and Thomas Watteyne. Understanding the limits of lorawan, 2017.

[85] Davide Magrin, Martina Capuzzo, and Andrea Zanella. A thorough study of lorawan performance under different parameter settings, 2019.

[86] Qipeng Song, Xavier Lagrange, and Loutfi Nuaymi. An analytical model for s-aloha performance evaluation in m2m networks, 2016.

[87] Lu Hou, Kan Zheng, Zhiming Liu, and Xiaojun Xu. Design and prototype implementation of a blockchain-enabled lora system with edge computing, 2021.

[88] Wesley dos Reis Bezerra, Fernando Luiz Koch, and Carlos Becker Westphall. Models of computing as a service and iot: an analysis of the current scenario with applications using lpwan, 2021.

[89] Sergio Barrachina-Muñoz and Boris Bellalta. Learning optimal routing for the uplink in lpwans using similarity-enhanced epsilon-greedy, 2017.

[90] Mahbubur Rahman and Abusayeed Saifullah. Integrating low-power wide-area networks for enhanced scalability and extended coverage, 2020.

[91] Sergio Barrachina-Muñoz, Toni Adame, Albert Bel, and Boris Bellalta. Towards energy efficient lpwans through learning-based multi-hop routing, 2018.

[92] Fatma Benkhelifa, Zhijin Qin, and Julie McCann. Minimum throughput maximization in lora networks powered by ambient energy harvesting, 2019.

[93] Arliones Hoeller-Jr., Richard Demo Souza, Hirley Alves, Onel L. Alcaraz López, Samuel Montejo-Sánchez, and Marcelo Eduardo Pellenz. Optimum lorawan configuration under wi-sun interference, 2019.

[94] Emekcan Aras, Nicolas Small, Gowri Sankar Ramachandran, Stéphane Delbruel, Wouter Joosen, and Danny Hughes. Selective jamming of lorawan using commodity hardware, 2017.

[95] Debraj Basu, Tianbo Gu, and Prasant Mohapatra. Security issues of low power wide area networks in the context of lora networks, 2020.

[96] Girish Sharma, Jyoti Grover, and Abhishek Verma. A lightweight security solution for mitigation of hatchetman attack in rpl-based 6lowpan, 2024.

[97] Abhishek Verma and Virender Ranga. The impact of copycat attack on rpl based 6lowpan networks in internet of things, 2023.

[98] Ahmed Raoof, Chung-Horng Lung, and Ashraf Matrawy. Integrating 6lowpan security with rpl using the chained secure mode framework, 2021.

[99] Aryan Mohammadi Pasikhani, John A Clark, and Prosanta Gope. Adaptive hybrid heterogeneous ids for 6lowpan, 2022.

[100] Lukas Simon Laufenberg. Impersonating lorawan gateways using semtech packet forwarder, 2019.

[101] Yalin E. Sagduyu and Tugba Erpek. Adversarial attacks on lora device identification and rogue signal detection with deep learning, 2023.

[102] Abhishek Verma and Virender Ranga. Security of rpl based 6lowpan networks in the internet of things: A review, 2023.

[103] Bechir Hamdaoui and Abdurrahman Elmaghbub. Deep-learning-based device fingerprinting for increased lora-iot security: Sensitivity to network deployment changes, 2022.

[104] Frank Hessel, Lars Almon, and Flor Álvarez. Chirpotle: A framework for practical lorawan security evaluation, 2020.

[105] Yaya Etiabi, Mohammed JOUHARI, Andreas Burg, and El Mehdi Amhoud. Spreading factor assisted lora localization with deep reinforcement learning, 2023.

[106] Jared Gaskin, Bechir Hamdaoui, and Weng-Keen Wong. Tweak: Towards portable deep learning models for domain-agnostic lora device authentication, 2022.

[107] Chandra Sekhar Sanaboina and Pallamsetty Sanaboina. Identification of the most significant parameter for optimizing the performance of rpl routing protocol in iot using taguchi design of experiments, 2023.

[108] Guilherme Rotth Zibetti, Juliano Araujo Wickboldt, and Edison Pignaton de Freitas. Context-aware environment monitoring to support lpwan-based battlefield applications, 2022.

[109] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R. Smith, and Shyamnath Gollakota. Lora backscatter: Enabling the vision of ubiquitous connectivity, 2017.

[110] Lorenzo Vangelista and Alessandro Cattapan. Extending the lora modulation to add further parallel channels and improve the lorawan network performance, 2020.

[111] Thiemo Voigt, Martin Bor, Utz Roedig, and Juan Alonso. Mitigating inter-network interference in lora networks, 2016.

[112] Orestis Georgiou, Constantinos Psomas, Christodoulos Skouroumounis, and Ioannis Krikidis. Optimal non-uniform deployments of lora networks, 2021.

[113] Weitao Xu, Jun Young Kim, Walter Huang, Salil Kanhere, Sanjay Jha, and Wen Hu. Measurement, characterization and modeling of lora technology in multi-floor buildings, 2019.

[114] Alexandru-Ioan Pop, Usman Raza, Parag Kulkarni, and Mahesh Sooriyabandara. Does bidirectional traffic do more harm than good in lorawan based lpwa networks?, 2017.

[115] Luca Beltramelli, Aamir Mahmood, Patrik Österberg, Mikael Gidlund, Paolo Ferrari, and Emiliano Sisinni. Energy efficiency of slotted lorawan communication with out-of-band synchronization, 2020.

[116] Mahbubur Rahman, Dali Ismail, Venkata P Modekurthy, and Abusayeed Saifullah. Lpwan in the tv white spaces: A practical implementation and deployment experiences, 2021.

[117] Reza Serati, Benyamin Teymuri, Nikolaos Athanasios Anagnostopoulos, and Mehdi Rasti. Adr-lite: A low-complexity adaptive data rate scheme for the lora network, 2022.

[118] Khaled Q. Abdelfadeel, Victor Cionca, and Dirk Pesch. Fair adaptive data rate allocation and power control in lorawan, 2018.

[119] Guus Leenders, Gilles Callebaut, Liesbet Van der Perre, and Lieven De Strycker. Multi-rat iot – what's to gain? an energy-monitoring platform, 2022.

[120] Dmitry Bankov, Evgeny Khorov, and Andrey Lyakhov. Mathematical model of lorawan channel access, 2020.

[121] Antoine Waret, Megumi Kaneko, Alexandre Guitton, and Nancy El Rachkidy. Lora throughput analysis with imperfect spreading factor orthogonality, 2018.

[122] Zhijin Qin, Frank Y. Li, Geoffrey Ye Li, Julie A. McCann, and Qiang Ni. Low-power wide-area networks for sustainable iot, 2018.

Disclaimer:

SurveyX is an AI-powered system designed to automate the generation of surveys. While it aims to produce high-quality, coherent, and comprehensive surveys with accurate citations, the final output is derived from the AI's synthesis of pre-processed materials, which may contain limitations or inaccuracies. As such, the generated content should not be used for academic publication or formal submissions and must be independently reviewed and verified. The developers of SurveyX do not assume responsibility for any errors or consequences arising from the use of the generated surveys.