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) play a crucial role in the Internet of Things (IoT) ecosystem by enabling long-range connectivity with minimal power consumption, which is vital for a diverse range of IoT applications [1]. The progression of LPWAN technologies from design and standardization to commercialization emphasizes their scalability in response to the increasing number of IoT devices [2]. Technologies like LoRa stand out for their ability to facilitate communication over extensive distances while maintaining energy efficiency, thus overcoming the limitations of traditional multihop wireless networks [3]. This capability is particularly important in urban and suburban settings, where physical structures can obstruct signal coverage [4].

LPWAN technologies also enhance network resilience, which is critical in safety-sensitive applications requiring reliable connectivity [5]. For example, they are essential for the development of Vehicular Ad-Hoc Networks (VANETs), contributing significantly to vehicular safety [6]. Additionally, LPWANs such as LoRaWAN are pivotal in supporting massive Machine-Type Communications (mMTC), a fundamental aspect of next-generation wireless systems beyond 5G [7]. They improve network throughput by mitigating packet collisions at gateways, thereby enhancing overall performance [8].

The adoption of LPWAN technologies is evident in Smart Cities, Smart Grids, and the Industrial Internet of Things, where they provide the necessary infrastructure for scalable and efficient communication [9]. Their low-power, long-range connectivity is crucial for various use cases, optimizing communication and routing protocols in IoT environments [10]. Furthermore, LPWANs support a

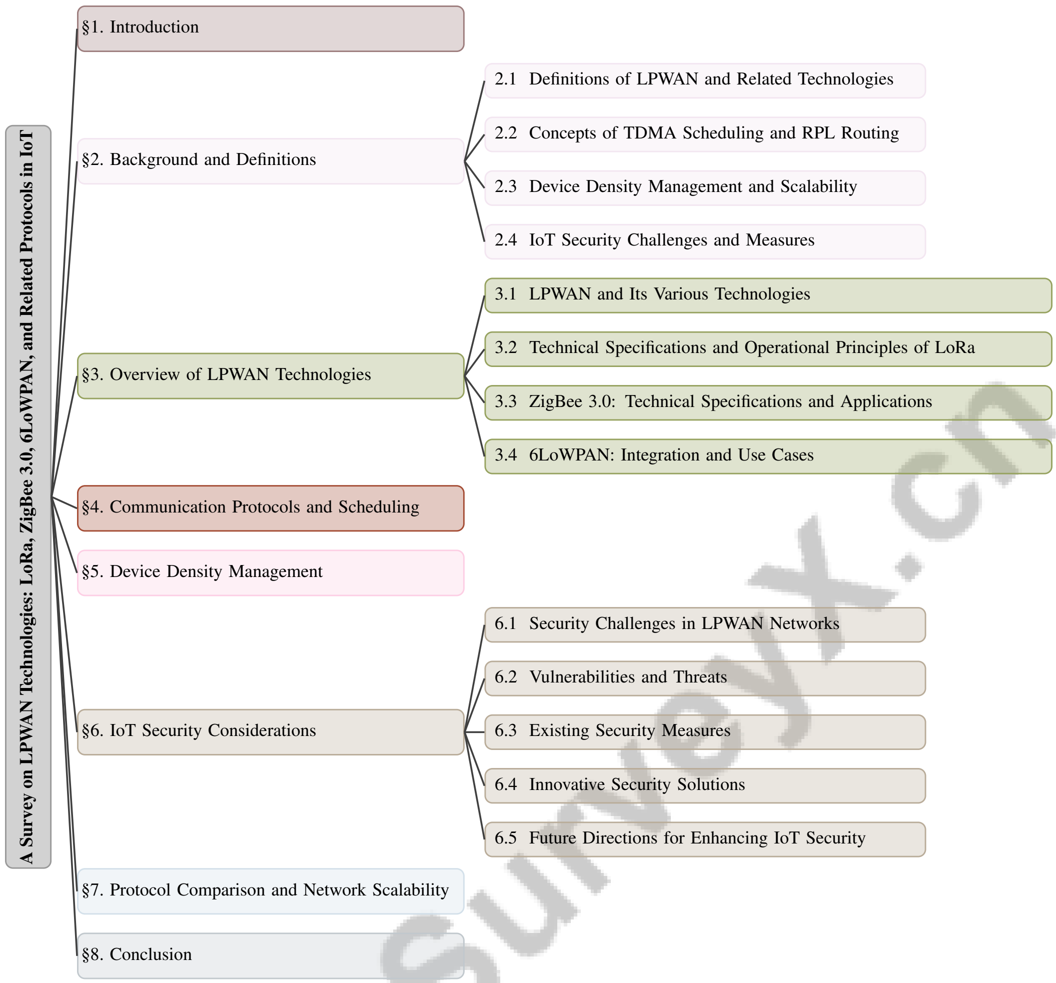

Figure 1: chapter structure

vast number of IoT devices with minimal power requirements, showcasing their advantages across diverse applications [6].

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, a leading LPWAN technology, is recognized for its long-range communication capabilities and low energy consumption, making it ideal for applications such as smart metering and agriculture [11]. The stochastic-geometric model in LoRa networks enhances the analysis of packet reception probabilities, improving our understanding of its applications in IoT [12]. However, LoRa's performance in urban areas is challenged by bandwidth congestion and increased latency, necessitating benchmarks to address these issues [13]. The Data Rate and Channel Control (DRCC) scheme has been proposed to optimize transmission parameters and reduce collision probabilities [14]. Additionally, DSME-LoRa integrates the DSME MAC layer with LoRa technology for seamless long-range communication in IoT networks [15]. Innovations such as using UAVs to assess LoRa signal strength offer new insights into improving coverage [16], while the incorporation of wake-up radios (WuR) enhances energy efficiency during data collection [17].

ZigBee 3.0, designed for low-power, low-data-rate applications, excels in home automation, industrial control, and health monitoring. Its mesh topology enhances reliability and scalability, ensuring robust communication in dense environments. The interoperability of ZigBee 3.0 with other ZigBee devices facilitates seamless integration into existing networks, enhancing deployment flexibility. Comparative

AI-generated, for reference only.

evaluations of ZigBee and LoRa in energy-efficient IoT deployments highlight the practical utility of these technologies [18].

6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) significantly enhances IPv6 capabilities by enabling efficient, IP-based communication among resource-constrained IoT devices. This technology integrates various constrained devices into IPv6 networks, allowing seamless data transmission in diverse environments, even with varying distances and message sizes. Preliminary evaluations indicate that 6LoWPAN can reduce power consumption to one-tenth that of traditional IP over WiFi while addressing mobility management needs for mobile sensor nodes deployed in dynamic scenarios [19, 20]. This is essential for applications requiring consistent connectivity, such as smart cities and environmental monitoring. Moreover, 6LoWPAN facilitates real-time monitoring and control via wireless sensor networks, enhancing user-device interaction and addressing limitations of existing host-based protocols.

Collectively, LoRa, ZigBee 3.0, and 6LoWPAN form the backbone of IoT applications, enhancing scalability, efficiency, and reliability. The integration of advanced communication technologies significantly boosts operational efficiency and scalability within the IoT ecosystem, addressing critical challenges related to interoperability and data management, and fostering the development of smarter, more connected environments across various sectors, including agriculture and urban infrastructure [21, 22, 23, 24].

1.3 Challenges and Opportunities

The LPWAN ecosystem faces several challenges that impede its optimal functionality within the IoT landscape. A primary concern is scalability, exacerbated by interference in heavily loaded networks, which decreases reliability as user numbers increase [25]. This issue is particularly pronounced in LoRaWAN, where the absence of channel sensing leads to increased packet collisions as IoT device density rises [26]. Additionally, the centralized design of LoRaWAN, while facilitating uplink-oriented data sharing, complicates direct communication necessary for distributed applications, increasing costs and inefficiencies [15].

Energy consumption remains a significant challenge, with existing solutions like LoRaWAN experiencing high energy demands and routing inefficiencies in lossy networks, resulting in suboptimal performance in IoT applications [9]. The inefficiencies of conventional LoRaWAN data transfer mechanisms further complicate scalability and energy consumption issues [5]. Moreover, optimizing communication decisions of IoT sensors to ensure accurate data collection while adhering to power and bandwidth constraints is critical [1].

Security vulnerabilities represent another concern, with traditional jamming effects on LoRa networks inadequately explored, highlighting a gap in effective mitigation strategies [27]. 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) [28]. Furthermore, addressing the complexities of mixed-integer non-linear optimization problems related to resource management could lead to more efficient strategies, supporting the growth and scalability of the LPWAN ecosystem [29].

By tackling existing challenges and leveraging emerging opportunities, LPWAN technologies can effectively meet the increasing demands of IoT applications, particularly in sectors requiring energy-efficient, reliable, and long-range communication. Recent studies indicate that LPWAN's capabilities are especially suited for mobile IoT environments, where performance is significantly influenced by node mobility and distance from gateways. As various LPWAN solutions vie for market dominance, their design specifications reveal strengths in battery life, cost-effectiveness, and extensive coverage, positioning them as ideal candidates for future industrial applications within the evolving landscape of Industry 4.0. Additionally, the development of mobility-aware LPWAN protocols is crucial for enhancing effectiveness in dynamic settings, reinforcing their role in advancing IoT connectivity [30, 31, 32].

1.4 Structure of the Survey

This survey is meticulously structured to provide a comprehensive overview of LPWAN technologies and their role in the IoT ecosystem. It is organized into several key sections, each focusing on different aspects of LPWAN and related protocols. The survey begins with an **Introduction**, which highlights the significance of LPWAN technologies and introduces LoRa, ZigBee 3.0, and 6LoWPAN, along with the challenges and opportunities within this domain. Following the introduction, the **Background and Definitions** section provides essential definitions and explanations of core concepts, including LPWAN, TDMA scheduling, RPL routing, and IoT security measures, setting the stage for the 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, offering 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**, where security challenges, potential threats, existing measures, and innovative solutions are discussed, 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. It also addresses scalability challenges and proposes 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 integral to the Internet of Things (IoT), offering extensive coverage with minimal energy usage, crucial for applications across vast areas [33]. These networks provide long-range connectivity at low power, ideal for applications needing widespread connectivity and prolonged battery life [34].

LoRa, a prominent LPWAN technology, employs chirp spread spectrum (CSS) modulation for enhanced interference resistance, enabling reliable long-distance communication [35]. Operating in unlicensed frequency bands, LoRa is effective indoors but faces challenges in urban environments due to signal degradation and packet transmission complexities [12, 4]. Managing transmission parameters in dense environments is crucial to enhance communication performance [14]. The low data rates of LoRa result in longer packet durations, increasing collision risks, especially in dense networks [36]. The inefficiencies of the ALOHA protocol exacerbate collision rates, necessitating solutions for collision resolution among multiple devices [26, 37].

ZigBee 3.0, based on the IEEE 802.15.4 standard, supports low-power, low-data-rate applications, excelling in home automation and industrial control with its mesh network topology ensuring reliable communication and seamless device integration [18].

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) extends IPv6 to constrained devices for efficient IP-based communication [38]. This is vital for applications needing consistent connectivity, such as smart cities and environmental monitoring. By enabling IoT devices to use standard Internet protocols, 6LoWPAN supports applications from environmental monitoring to smart metering. However, interoperability issues among implementations can lead to communication problems, which P6LoWPAN aims to resolve by improving interoperability among low-power devices [39].

Together, LPWAN technologies like LoRa, ZigBee 3.0, and 6LoWPAN address unique IoT deployment challenges, such as energy consumption and network scalability, enabling the integration of

AI-generated, for reference only.

numerous devices into the IoT landscape [40]. These technologies support innovative applications, ensuring reliable data transmission over long distances and enhancing IoT system performance, with standardized localization methods being critical for applications like asset tracking [41].

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 essential for managing LPWAN communications, enhancing network efficiency and reliability. TDMA allocates specific time slots for data transmissions, minimizing collisions and optimizing throughput in high-density networks [42]. This is particularly beneficial for energy efficiency and Quality of Service (QoS) in Wireless Sensor Networks (WSNs) [43]. In LoRa networks, understanding interference and reception probabilities is crucial for optimizing TDMA scheduling, as informed by stochastic geometry analyses.

RPL, a 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. It addresses skewness and load imbalance in the DODAG structure, which can lead to inefficient data transmission [44]. Integrating RPL with IEEE 802.15.4, particularly by encapsulating RPL DIO messages in beacon frames, enhances routing efficiency [45]. Comparisons with other protocols like LOADng demonstrate RPL's suitability for home automation [46].

The synergy between TDMA scheduling and RPL routing is enriched by approaches such as Software-Defined 6LoWPAN (SD-6LoWPAN), which incorporates Software Defined Networking (SDN) principles for dynamic packet forwarding [47]. Leveraging these techniques, LPWAN networks can enhance energy efficiency and link reliability, supporting diverse IoT conditions. The integration of TDMA scheduling and RPL routing offers robust solutions for managing communication, ensuring LPWANs effectively support growing IoT demands.

2.3 Device Density Management and Scalability

Managing device density and scalability in LPWANs is crucial for maintaining performance and reliability as connected devices increase. A major challenge is the bandwidth limitations of the ALOHA protocol, which struggles with high node density due to frequent collisions and lack of synchronization [48]. Duty-cycle regulations further restrict throughput, limiting scalability in dense environments [49].

In LoRaWAN, scalability and capacity are challenged as networks expand to accommodate many devices per gateway [50]. Co-spreading factor interference significantly affects performance under high density [51]. Maintaining synchronization without sacrificing bandwidth is key, as high collision rates can impede scalability and performance [52].

Effective device density management involves optimizing base station placement and frequency assignments, crucial for enhancing LPWAN scalability [53]. Mobility management presents challenges, including high handover latency and packet loss, affecting performance in time-critical applications [20].

Addressing these challenges requires innovative network design and operation approaches, such as advanced synchronization techniques and alternative protocols for high-density environments. By strategically managing device density and scalability, LPWANs can meet increasing IoT demands, ensuring reliable and efficient connectivity. Challenges such as mobility impacts, duty cycle restrictions, and potential bottlenecks must be tackled through new protocols and enhanced technologies to support mobile IoT applications [25, 54, 32, 30, 34].

2.4 IoT Security Challenges and Measures

The security landscape of LPWANs in IoT presents challenges affecting network stability, data integrity, and device authentication. A significant concern is the high rate of missing data due to transmission outages, complicating reliable data analysis and network performance [55]. LoRaWAN's duty cycle limitations restrict downlink transmission frequency, prolonging firmware updates and potentially compromising security [56].

Network stabilization and energy consumption are critical, especially when nodes fail, necessitating RPL tree rebuilding in Wireless Sensor Networks (WSNs) [57]. Dense IoT networks face inefficient management due to device mobility and jamming attacks, impacting packet delivery and energy efficiency [58]. Benchmarks often lack sufficient sample sizes and publicly available data for validation, limiting their applicability [4].

Device authentication remains a critical challenge, requiring scalable solutions for the increasing number of IoT devices [59]. The Decreased Rank Attack in RPL networks poses a threat, where malicious nodes manipulate their rank to mislead traffic routing, degrading performance [60]. Limitations in 6LoWPAN fragmentation strategies pose challenges in real-world setups [61].

Exhaustion attacks exploiting communication protocols to drain device batteries represent a significant security challenge in LPWAN-based IoT networks [62]. These attacks degrade network performance by depleting energy resources. Inefficient fixed quantization methods for key generation may introduce vulnerabilities, necessitating adaptive approaches to enhance security [63].

Addressing these challenges requires efficient TDMA scheduling algorithms that adapt to changing network conditions [64]. Robust security measures must enhance device authentication and mitigate jamming and replay attacks. By adopting these strategies, LPWAN-based IoT networks can achieve enhanced security and reliability, ensuring efficient operation in diverse environments. Sundaram et al. explore vulnerabilities in LoRa networks and present solutions to enhance security, highlighting the need for ongoing research in this area [3].

3 Overview of LPWAN Technologies

The increasing demand for efficient communication technologies in the IoT realm has driven the evolution of various Low-Power Wide-Area Network (LPWAN) solutions. Tailored to address IoT-specific challenges such as range, power efficiency, and data transmission, this section examines LPWAN technologies, focusing on their characteristics, operational principles, and applications. Subsequent subsections delve into specific technologies like LoRa, Sigfox, and Narrowband IoT (NB-IoT), each playing a vital role in the IoT landscape.

3.1 LPWAN and Its Various Technologies

LPWANs are pivotal in the IoT domain, offering long-range communication with minimal power consumption, essential for diverse applications [1]. Key LPWAN technologies include LoRa, Sigfox, and NB-IoT, each tailored for specific environments and use cases. As illustrated in Figure 2, these technologies are categorized based on their distinctive features and research advancements. For instance, LoRa utilizes chirp spread spectrum modulation, enabling effective long-range communication and energy efficiency, particularly beneficial in smart agriculture and rural IoT scenarios [3]. The EnvSen framework, leveraging multi-agent reinforcement learning, exemplifies LoRa's adaptability in dynamic environmental monitoring [1]. Research on LoRa's urban performance highlights its adaptability to different speeds and configurations [4], while multi-sensor localization enhances its IoT applicability [18].

Sigfox, known for ultra-narrowband communication, provides a cost-effective solution for low data rate and long battery life applications. Its fragmentation strategy, coupled with group NACK, improves network goodput and energy efficiency in dense LPWANs, particularly under duty-cycle constraints [34, 65]. Comparative analyses with other LPWAN technologies reveal distinct advantages based on application needs [6].

NB-IoT, a cellular-based LPWAN, excels in robust coverage and high capacity, crucial for reliable data transmission over extended periods. Real-world experiments with various NB-IoT chipsets underscore its urban performance advantages where coverage and capacity are paramount [66]. Its hybrid link adaptation strategies ensure effectiveness across diverse IoT deployments [67].

Together, LPWAN technologies provide a comprehensive framework for IoT applications, facilitating long-range, low-power communication essential for smart devices. Tools like IoT-Scan, compatible with multiple protocols including LoRa and Zigbee, highlight the importance of interoperability in the IoT ecosystem. By leveraging each technology's strengths and addressing their limitations, the IoT ecosystem can expand, supporting innovative applications across various sectors. The integration of non-terrestrial networks (NTNs) enhances coverage and capacity for IoT applications, particularly in underserved areas, broadening LPWAN solutions' reach and impact [68]. An analytical model elucidating the mutual impacts of multiple technologies operating concurrently further clarifies LPWAN performance metrics [69].

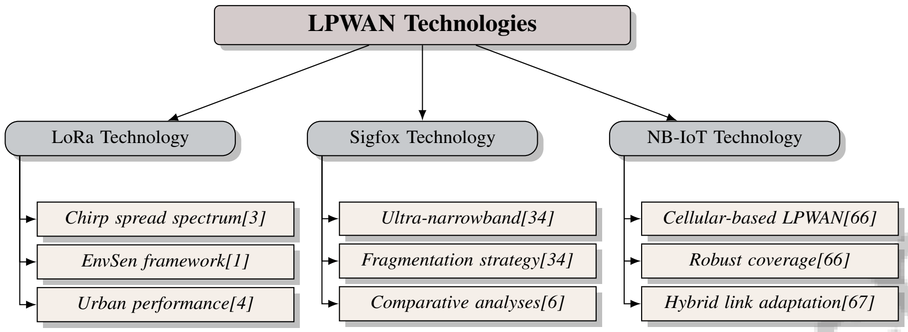

Figure 2: This figure illustrates the key LPWAN technologies, categorizing them into LoRa, Sigfox, and NB-IoT. Each category highlights specific features and research advancements, such as LoRa's chirp spread spectrum and urban performance, Sigfox's ultra-narrowband communication and fragmentation strategy, and NB-IoT's robust coverage and hybrid link adaptation.

3.2 Technical Specifications and Operational Principles of LoRa

LoRa is a cornerstone of LPWANs, engineered for long-range communication with low power consumption, crucial for various IoT applications. Its chirp spread spectrum (CSS) modulation enhances interference resistance, ensuring reliable communication over long distances, vital for data integrity in interference-prone IoT settings [17]. LoRa's technical specifications allow for management of varying node densities and transmission rates, influencing packet reception probabilities. A stochastic geometry model offers insights into uplink coverage in single gateway LoRa networks, addressing unique interference challenges [10]. Additionally, frameworks for computing coverage probability and area spectral efficiency in multi-gateway downlink LoRa networks highlight its adaptability to different interference scenarios [4].

Innovations like the Long-Lived LoRa (LLL) protocol enable dynamic packet offloading from nodes with depleting resources to those with sufficient energy, extending network lifetime and enhancing efficiency [10]. The integration of wake-up radios (WuR) into LoRa networks, such as the WuR-aided Data Collection Scheme (WuR-DCS), further boosts energy efficiency during data collection from sensor nodes [17]. Network performance is optimized through resource management techniques like the LoRaWAN-D2D protocol, which facilitates direct communication links between devices, improving data transfer efficiency [5]. LoRa's urban adaptability is evident as it maintains effective communication under varying speeds and configurations, influenced by the spreading factor used [4].

Security measures are integral to LoRa's operational principles, with resilience against jamming attacks and authenticated preambles countering exhaustion attacks, critical for preserving network integrity [17]. LoRa's technical specifications, including CSS modulation, adaptive resource management, and innovative architectures like LoRaWAN, underscore its effectiveness in diverse IoT applications. Its application in smart city initiatives enables efficient communication for low-power devices in resource-constrained environments, while in smart agriculture, it addresses the unique challenges of agricultural landscapes. The incorporation of edge processing in LoRaWAN enhances scalability, reduces latency, and improves security, making it a robust solution for high-density IoT deployments across various sectors [70, 71, 23]. These capabilities ensure scalable, flexible, and energy-efficient communication solutions, solidifying LoRa's 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 a key technology for low-power, low-data-rate wireless communication, particularly suited for home automation, industrial control, and health monitoring due to its energy efficiency and robust performance in diverse environments. This makes

ZigBee 3.0 suitable for the expanding IoT ecosystem, which demands reliable connectivity for numerous low-power devices across extensive geographical areas [18, 59, 32, 31, 24]. Its design emphasizes a reliable and scalable mesh network topology, enhancing communication robustness even in high device density environments by enabling data to hop from node to node, maintaining connectivity despite node failures or obstructions.

ZigBee 3.0's technical specifications include support for various frequency bands, primarily operating within the 2.4 GHz ISM band, along with sub-GHz frequencies to comply with regional regulations. This flexibility is essential for deploying IoT solutions across different global markets, as the regulatory landscape for unlicensed sub-GHz bands significantly influences the adoption of LPWAN and their interoperability with other wireless technologies, such as RFIDs and mobile devices [6, 24]. ZigBee 3.0 supports data rates up to 250 kbps, sufficient for typical sensor and control data exchanges in its target applications.

A key advantage of ZigBee 3.0 is its exceptionally low power consumption, facilitated by advanced power management protocols and sleep mode capabilities, significantly prolonging battery life. This efficiency aligns with trends in LPWANs, which are increasingly adopted for their ability to support numerous low-power devices over extensive areas while maintaining low operational costs [59, 32, 30, 72, 73]. This feature is particularly beneficial for battery-powered devices in remote locations, where frequent battery replacement is impractical.

ZigBee 3.0 plays a crucial role in smart home systems by facilitating seamless interconnectivity among devices such as lighting, heating, and security systems. This standard enhances centralized control and automation capabilities while addressing interoperability challenges posed by diverse technologies within the IoT ecosystem. As smart home applications proliferate, ZigBee 3.0's low-power, low-data-rate communication protocol is essential for managing the increasing complexity of interconnected devices, contributing to the vision of an efficient and automated living environment [18, 59, 32, 74, 24]. Its self-healing mesh network capability makes it ideal for industrial environments, facilitating machinery and process monitoring to ensure operational efficiency and safety.

In healthcare systems, the integration of ZigBee 3.0 enhances the reliability of connections among medical devices and sensors, enabling real-time monitoring of patient health metrics. This capability promotes timely interventions and improves healthcare service delivery efficiency, aligning with the trend of utilizing IoT technologies in interconnected healthcare environments. By leveraging standards like ZigBee 3.0, healthcare systems can better manage the interoperability of diverse medical devices, ensuring seamless data transmission across platforms [21, 59, 32, 72, 24]. The technology's low latency and robust communication capabilities ensure accurate and prompt transmission of critical health data.

3.4 6LoWPAN: Integration and Use Cases

6LoWPAN, or IPv6 over Low-Power Wireless Personal Area Networks, significantly advances IP-based communication for constrained IoT devices, bridging low-power networks with the broader Internet. This integration enhances interoperability among diverse IoT devices—such as RFIDs, mobile devices, and wireless sensors—by utilizing established standards like IPv6 and 6LoWPAN, crucial for the widespread adoption of IoT applications across sectors like smart agriculture and edge computing, where reliable communication is essential for performance optimization [21, 23, 28, 24].

6LoWPAN's integration with IPv6 allows for 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 [75]. 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, demonstrated in hospital wireless sensor networks. This capability is essential for real-time patient monitoring, ensuring timely and accurate care delivery [20]. The Enhanced Location-based Routing Protocol (ELBRP) optimizes data transmission in 6LoWPAN networks using link quality and distance as routing metrics, improving performance and reliability [76].

Scalability in 6LoWPAN networks is critical for large-scale deployments. Comparative evaluations of hop-wise reassembly and direct fragment forwarding provide insights into optimizing performance and resource utilization in real-world testbeds [61]. The 6RLR-ABC protocol introduces bio-inspired swarm intelligence for local repair processes, reducing energy consumption and delay while maintaining network efficiency [77].

Innovations like the SD-6LoWPAN method leverage Software Defined Networking (SDN) principles for seamless packet forwarding in multi-hop Wireless Sensor Networks (WSNs). Utilizing a centralized SDN controller, this approach dynamically manages routing rules, enhancing adaptability and performance [47]. Recent designs introduce a capability spectrum providing explicit bounds on resource usage, ensuring 6LoWPAN networks support diverse IoT applications without compromising efficiency [39].

4 Communication Protocols and Scheduling

Effective communication is crucial for optimizing network performance and ensuring reliable data transmission in Low-Power Wide-Area Networks (LPWANs). This section explores the roles of communication protocols, focusing on Time Division Multiple Access (TDMA) scheduling and the Routing Protocol for Low-Power and Lossy Networks (RPL). Understanding these protocols is vital for enhancing communication efficiency and reliability within LPWANs, which are increasingly demanded by Internet of Things (IoT) applications.

Figure 3 illustrates the hierarchical structure of communication protocols and scheduling in LPWANs, highlighting the roles of TDMA scheduling and RPL routing alongside advanced protocols like TurboLoRa and Proteus, as well as adaptive techniques for optimizing data delivery and network efficiency. The following subsection examines TDMA scheduling and RPL routing, illustrating their synergy in creating robust communication networks.

4.1 Communication Protocols: TDMA Scheduling and RPL Routing

TDMA scheduling and RPL play pivotal roles in optimizing communication within LPWANs, significantly enhancing network efficiency and reliability. As illustrated in Figure 4, which presents a hierarchical classification of communication protocols in LPWANs, the focus is on TDMA scheduling, RPL routing, and advanced protocols. This figure highlights key methods and innovations that contribute to enhancing network efficiency and reliability. TDMA manages channel access by allocating specific time slots for data transmission, minimizing packet collisions and improving throughput, especially in high-density environments [42]. Integrating TDMA with advanced algorithms, such as the DRL-based Energy Efficiency Optimization method, allows dynamic adaptation to real-time conditions, optimizing communication management in LoRa networks [78]. The S-ALOHA protocol, which segments the channel into time slots, complements TDMA by further reducing collisions and enhancing throughput [48].

RPL constructs a Destination-Oriented Directed Acyclic Graph (DODAG) to optimize routing paths, ensuring reliable data transmission in resource-constrained networks. The SB-RPL extension enhances RPL by incorporating skewness and subtree size into routing decisions, improving DODAG tree balancing [44]. Approaches like SD-6LoWPAN, employing a mesh-under forwarding mechanism, enhance packet handling compared to traditional route-over methods, improving RPL routing efficiency [47].

The interplay between TDMA and RPL is enriched by advanced protocols. TurboLoRa enables simultaneous transmission from multiple devices, increasing throughput without exceeding channel limits, thus complementing TDMA's structured access [79]. Proteus, a dynamic gateway design, configures data rates and bandwidths per packet based on signal characteristics, optimizing communication efficiency in LPWANs [80].

Techniques like the Multi-Armed Bandit approach maximize frame success rates by independently selecting optimal channels and spreading factors, enhancing protocol adaptability in LPWANs [81]. Redundancy transmission protocols, using fountain coding and message replication, underscore their role in enhancing reliability and efficiency [82]. Additionally, packet fragmentation and group NACK methods significantly boost data transmission efficiency in LPWANs under duty cycle constraints [34].

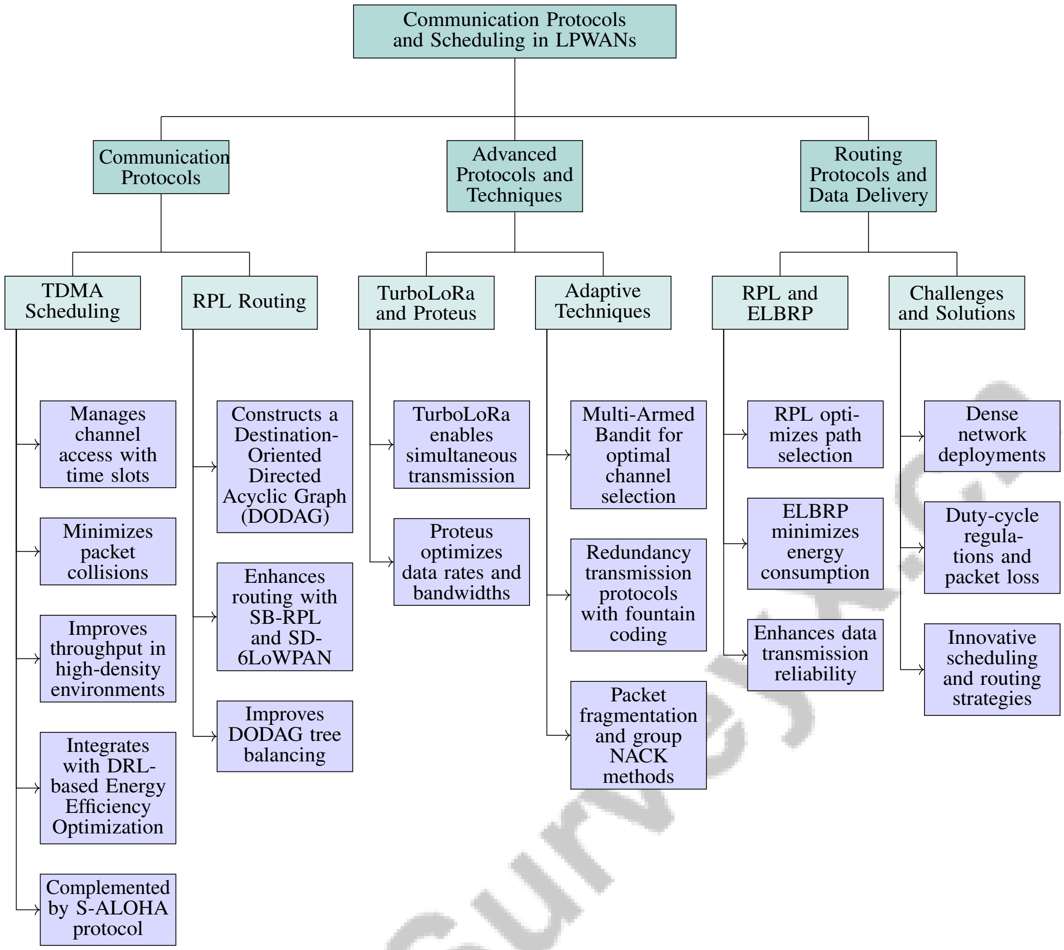

Figure 3: This figure illustrates the hierarchical structure of communication protocols and scheduling in LPWANs, highlighting the roles of TDMA scheduling and RPL routing, advanced protocols like TurboLoRa and Proteus, and adaptive techniques for optimizing data delivery and network efficiency.

The integration of TDMA and RPL within LPWANs enhances communication efficiency and supports scalable network management. With advanced protocols, LPWANs effectively address the growing demands of IoT applications, offering long-range, low-power, and cost-effective connectivity suitable for diverse environments. However, node mobility can significantly affect LPWAN performance, particularly in mobile IoT scenarios. This necessitates the development of mobility-aware LPWAN protocols. Technologies such as LoRa, Sigfox, NB-IoT, and LTE-M demonstrate superior energy efficiency and coverage, positioning them as optimal choices for future industrial applications in the evolving IoT landscape [30, 31, 32].

4.2 Routing Protocols and Data Delivery

Routing protocols are crucial for ensuring efficient and reliable data delivery in LPWANs, characterized by constrained resources and diverse deployment scenarios. RPL, designed for such environments, constructs a Destination-Oriented Directed Acyclic Graph (DODAG) to optimize path selection and minimize energy consumption [46]. RPL maintains shorter delays and lower control overhead compared to alternatives like LOADng, 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 [76]. This is particularly beneficial in scenarios emphasizing energy efficiency and data integrity, allowing IoT devices to operate effectively over extended periods.

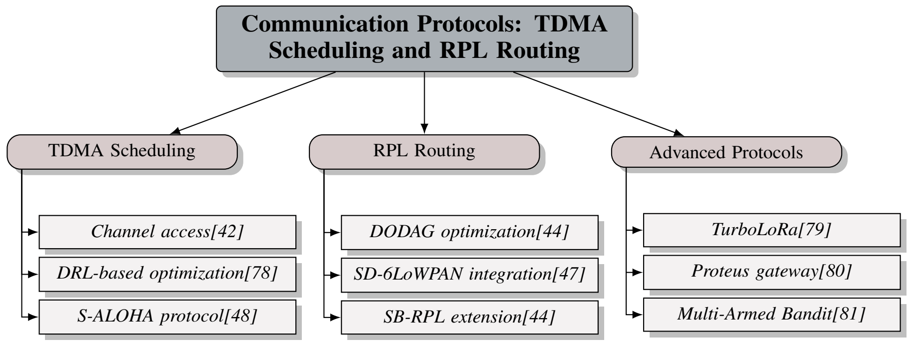

Figure 4: This figure illustrates the hierarchical classification of communication protocols in LPWANs, focusing on TDMA scheduling, RPL routing, and advanced protocols. It highlights key methods and innovations enhancing network efficiency and reliability.

Despite advancements, challenges persist in dense network deployments where duty-cycle regulations and collisions can impact performance, leading to increased packet loss and reduced throughput [54]. Addressing these challenges requires innovative scheduling and routing strategies adaptable to the dynamic conditions of LPWANs.

Integrating TDMA scheduling with routing protocols offers a promising solution by providing structured access to communication channels, thus reducing packet collisions and optimizing throughput. A two-phase scheme for distributed TDMA scheduling, evaluated using the Castalia simulator, demonstrates significant improvements in schedule length and scheduling time compared to existing algorithms, highlighting its potential to enhance data delivery efficiency in LPWANs [64].

5 Device Density Management

5.1 Impact on Network Performance and Scalability

Method Name	Device Density	Energy Efficiency	Innovative Solutions
LTSM[11]	Lorawan End Nodes	Low Power	Lorawan Traffic Sensing
SGM-LN[12]	Node Density	-	Collision Model
WuR-DCS[17]	Sensor Cluster	Wur-aided Approaches	Wake-up Beacons
D2D[5]	Dense Environments	Energy Consumption	D2d Protocol
HARE[7]	Dense Networks	Energy Savings	Hare Protocol Stack
LLL[10]	UP TO 1200	Energy-harvesting Techniques	Dynamic Packet Offloading
DMG-LP[36]	Channel Density	Energy-harvesting Techniques	Closed-form Expressions
DSL[15]	25 Lora Boards	Energy Consumption Reduction	Dsme-LoRa Method
CABF[28]	-	Energy Consumption	Resilient Edge

Table 1: Comparison of various methods addressing device density, energy efficiency, and innovative solutions in LoRa-based Low-Power Wide-Area Networks (LPWANs). The table highlights different approaches to enhance network performance and reliability in dense environments, providing insights into energy-saving techniques and protocol innovations.

Device density significantly impacts the performance and scalability of Low-Power Wide-Area Networks (LPWANs), particularly in LoRa-based systems. Increased device connections elevate the risk of packet collisions and interference, which can degrade network throughput and reliability, especially in urban settings with dense infrastructures like smart meters [11]. The assumption of complete orthogonality among spreading factors often leads to performance issues under high-density conditions, necessitating effective management strategies [12].

As illustrated in Figure 5, the impact of device density on network performance and scalability is multifaceted, highlighting key areas such as the effects of device density, energy efficiency strategies, and innovative solutions. Each category addresses specific challenges and proposes methods to enhance network reliability and efficiency in dense environments. Table 1 presents a comprehensive analysis of methods aimed at improving network performance and scalability in LoRa-based systems, focusing on device density, energy efficiency, and innovative solutions.

Adaptive strategies are essential for mitigating the adverse effects of high device density. The WuR-aided approach allows sensors to conserve power by activating only when needed, thereby improving network performance [17]. Similarly, the D2D communications protocol reduces network load through direct device interactions, addressing high-density challenges [5]. The HARE protocol stack further enhances reliability and energy consumption in dense networks [7].

The Long-Lived LoRa (LLL) protocol evaluates the impact of device density on network performance by addressing rapid battery depletion in energy-harvesting LoRa networks, highlighting the need for energy-efficient strategies in dense deployments [10]. Increasing the duty cycle and transmit power boosts coverage probability and area spectral efficiency, critical for maintaining network performance in dense environments [36].

Innovative solutions like DSME-LoRa minimize gateway reliance, reduce infrastructure costs, and enhance communication efficiency in dense IoT scenarios [15]. The Resilient Edge system ensures reliable message delivery in high-criticality applications, addressing network failure challenges [28].

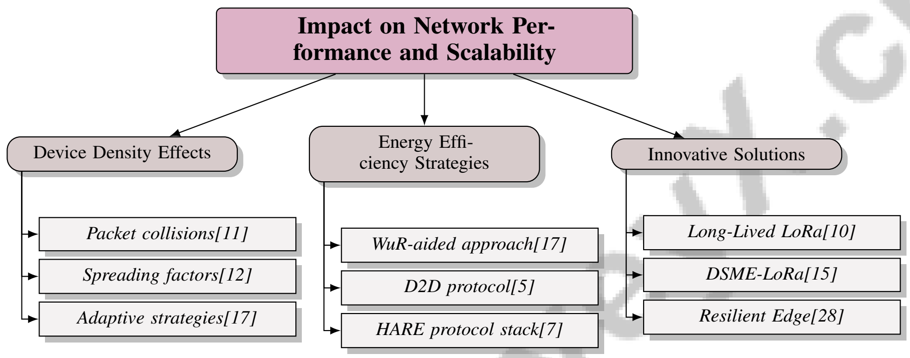

Figure 5: This figure illustrates the impact of device density on network performance and scalability, highlighting key areas such as device density effects, energy efficiency strategies, and innovative solutions. Each category addresses specific challenges and proposes methods to enhance network reliability and efficiency in dense environments.

5.2 Optimization Techniques for Network Resources

Method Name	Optimization Strategies	Resource Management	Scalability and Performance
MTMA[83]	Adaptive Resource Allocation	Dynamic Bandwidth Allocation	Device Density
LoRaDRL[58]	Deep Reinforcement Learning	Intelligent Resource Allocation	Dense Iot Networks
LCO[84]	Optimization Algorithms	Dynamic Adaptations	User Capacity

Table 2: Comparison of optimization methods for resource management in LoRa networks, highlighting strategies for adaptive resource allocation, dynamic bandwidth management, and scalability. The table outlines the distinct approaches employed by MTMA, LoRaDRL, and LCO methods, demonstrating their effectiveness in enhancing network performance and managing device density.

Optimizing network resources is crucial for maintaining performance and efficiency in LPWANs as the number of connected devices increases. Predictive models are instrumental in managing data efficiently; for instance, in smart campus environments, advanced models predicting occupancy from sensor readings achieved a 95

Adaptive resource allocation strategies are vital for enhancing performance in large-scale LoRa networks. These strategies address near-far fairness and optimize performance indicators like energy efficiency, throughput, and capacity by dynamically adjusting network parameters and employing methods such as Iterative Balancing (IB) and multi-hop routing [85, 86, 87]. Dynamic bandwidth allocation and adaptive duty cycling further enhance efficiency by adjusting resource usage based on real-time conditions.

Advanced scheduling algorithms like Time Division Multiple Access (TDMA) optimize channel access and reduce collision probabilities, improving overall throughput. By assigning specific time slots for data transmission, TDMA enhances resource utilization, minimizes idle time, and fosters reliable communication, particularly in WSNs with dynamic topologies. Recent advancements in

TDMA scheduling techniques offer flexibility in balancing schedule length and generation time, enabling networks to adapt swiftly while maintaining performance efficiency [64, 42, 57].

Edge computing solutions aid in resource optimization by offloading data processing from central servers to edge devices, reducing latency, and alleviating network infrastructure burdens. This approach facilitates efficient resource use by processing data closer to its source, enhancing operations, and addressing scalability challenges while maintaining security and privacy through decentralized architectures [88, 28, 70, 89, 68].

These optimization techniques are essential for sustaining LPWAN performance and scalability. By employing predictive modeling, adaptive resource allocation, sophisticated scheduling algorithms, and edge computing frameworks, networks can effectively optimize resource management to meet the growing demands of IoT applications. These advancements ensure robust communication across diverse environments, addressing challenges related to varying quality of service (QoS) requirements and the need for resiliency in applications ranging from non-critical to safety-critical scenarios. Furthermore, integrating LPWAN technologies with non-terrestrial networks (NTNs) enhances connectivity, particularly in rural areas with limited cellular coverage, facilitating seamless IoT system operation [28, 89, 68, 38, 55].

Table 2 provides a comparative analysis of various optimization techniques employed in LoRa networks, emphasizing their strategies for resource management and scalability enhancement. As illustrated in **??**, managing device density is crucial for enhancing communication network performance and reliability. This example examines three distinct optimization techniques within a LoRa network, each providing unique insights into device density management. The first image depicts the distribution of LoRa gateways and users, visually representing device dispersion and highlighting areas of potential congestion or underutilization. The second image compares the Performance Data Rate (PDR) of three LoRa communication systems—LoRaDRL, LoRaSim, and LoRa-MAB—across varying speeds, demonstrating the impact of mobility on network performance and the effectiveness of different systems in maintaining data integrity. Lastly, the third image presents an algorithm designed to maximize node numbers within a network, given specific reliability targets and coverage constraints. This underscores the importance of strategic planning in network configuration for optimal connectivity and resource allocation. Collectively, these examples emphasize the significance of employing advanced optimization techniques to manage device density and enhance network resource utilization in LoRa networks [83, 58, 84].

6 IoT Security Considerations

6.1 Security Challenges in LPWAN Networks

Low-Power Wide-Area Networks (LPWANs), such as LoRaWAN, confront critical security challenges that impact their functionality in the IoT landscape. A major issue is their susceptibility to jamming attacks exploiting design vulnerabilities, necessitating robust interference management to ensure reliability [27]. In environments with high device density, interference from competing technologies further complicates performance, requiring sophisticated strategies to maintain signal integrity [69, 1]. The complexity of capability discovery mechanisms also poses challenges for maintaining device compatibility [39].

Scalability is a significant concern under heavy network loads, where interference can degrade performance [25]. Inefficiencies in routing and communication exacerbate these issues, particularly in low-power, lossy networks [9]. Accurate signal demodulation is crucial for maintaining reliable communication, as highlighted by synchronization algorithms [8]. However, existing methods do not fully address collision issues, especially in high-density scenarios, revealing ongoing vulnerabilities [26, 37].

Rapid battery depletion underscores the need for energy management strategies to ensure device reliability and security [10]. Multi-hop communication protocols like HARE can enhance resilience against node failures, addressing security concerns related to device reliability [7].

6.2 Vulnerabilities and Threats

LPWANs face numerous vulnerabilities that threaten security and operational stability. LoRaWAN networks are particularly vulnerable to selective jamming attacks, which disrupt communication and degrade performance [90]. The variation in vulnerabilities among nodes complicates the implementation of uniform security measures [91]. The Routing Protocol for Low-Power and Lossy Networks (RPL) is vulnerable to attacks like the Hatchetman attack, which degrade packet delivery ratios, necessitating robust security solutions [92, 93].

Integrating security frameworks such as CSM with 6LoWPAN can mitigate buffer-reservation attacks, emphasizing the importance of such approaches for enhancing network security [94]. However, the dynamic nature of 6LoWPAN presents challenges for existing Intrusion Detection Systems (IDS) [95]. The lack of authentication in protocols like the Semtech Packet Forwarder allows gateway impersonation, posing significant threats [96].

Existing jamming strategies assume prior knowledge of bandwidth and spreading factors, complicating countermeasure development [97]. The transferability of adversarial attacks across models further undermines LPWAN security [98].

6.3 Existing Security Measures

Current security measures in LPWANs address vulnerabilities and challenges posed by resource-constrained IoT devices. Lightweight security approaches avoid heavy cryptographic techniques, making them suitable for environments with limited processing capabilities [92]. A multi-layered security framework for LoRa networks integrates traditional countermeasures with emerging methods, offering comprehensive strategies for mitigating risks [91].

Mitigation techniques for jamming attacks focus on low-cost hardware and detection schemes that maintain low complexity [90, 27]. For RPL-based 6LoWPAN networks, integrating the CSM framework enhances immediate-sender authentication and builds a trust chain, improving overall security [94].

Advanced techniques like device fingerprinting and adaptive IDS strengthen security in LPWANs. Deep learning-based fingerprinting enhances device identification, providing an additional security layer [99]. Adaptive hybrid IDS effectively detect a wide range of RPL attacks, adapting to environmental changes [95].

To mitigate threats like exhaustion attacks, authentication preambles and the AQ-KG protocol enhance communication security [62, 63]. The ChirpOTLE framework offers a practical approach for security evaluation in LoRaWAN, enabling rapid vulnerability testing [100].

6.4 Innovative Security Solutions

Innovative solutions are essential for enhancing LPWAN resilience and reliability. As illustrated in Figure 6, the categorization of innovative security solutions for LPWAN focuses on game-theoretic approaches, mobility and localization solutions, and advanced security frameworks. Each category highlights specific methods and strategies to enhance the security and efficiency of IoT networks. Game-theoretic approaches detect and counteract network attacks like the Hatchetman attack, enhancing security without substantial computational overhead [92]. Secure Objective Functions (Sec-OF) restrict node behavior, mitigating attacks in RPL networks [60].

Network-based mobility management solutions improve security and efficiency in 6LoWPAN mobility, addressing IoT environment dynamics [20]. Enhancing localization accuracy through spreading factor integration presents an innovative solution for IoT security [101].

Selective jamming requires sophisticated countermeasures to ensure network integrity [90]. Neural networks offer novel approaches for generating countermeasures against unauthorized signals. Adaptive security frameworks evolve with threats, focusing on cross-layer solutions for RPL-based networks [102, 95].

Deep learning-based device fingerprinting enhances authentication by relying on hardware-specific distortions [99]. The Tweak method complements this by enabling lightweight model calibration

[103]. Authentication preambles mitigate exhaustion attacks, ensuring operational security [62]. Optimizing parameters like DIO_MIN_INTERVAL can lead to substantial energy savings [104].

Future research should optimize blockchain-enabled solutions like HyperLoRa and explore additional security measures for robustness [88]. The ChirpOTLE framework bridges the gap between research and application, highlighting the need for countermeasures against sophisticated attacks [100, 96].

These solutions emphasize adaptive, lightweight, and robust approaches to safeguarding LPWAN networks, ensuring secure IoT operations. Future research should enhance middleware for heterogeneous sensor motes and develop standardized regulations for global harmonization and spectrum efficiency [24, 6].

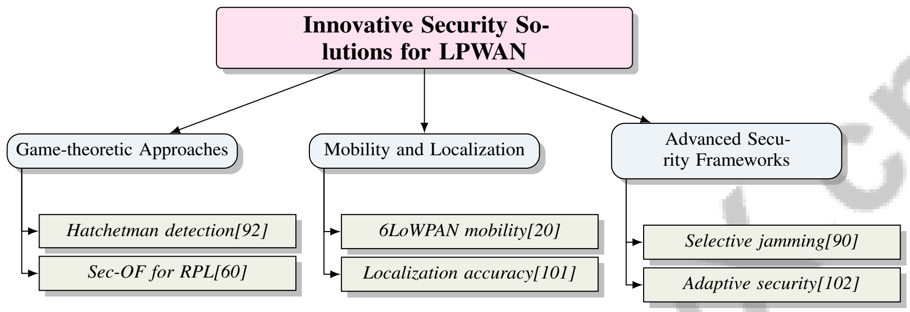

Figure 6: This figure illustrates the categorization of innovative security solutions for LPWAN, focusing on game-theoretic approaches, mobility and localization solutions, and advanced security frameworks. Each category highlights specific methods and strategies to enhance the security and efficiency of IoT networks.

6.5 Future Directions for Enhancing IoT Security

Enhancing LPWAN security within IoT requires integrating technological innovations with practical implementations. Future research should focus on improving wake-up beacon reception and optimizing resource allocation [17]. Developing dynamic interference management and adaptive access control mechanisms is crucial for high-density deployments.

Integrating real-time environmental data into benchmarks will enhance performance evaluation, leading to resilient LPWAN solutions. Mobility-aware protocols are needed for mobile IoT applications, as exemplified by the SNOW platform's effective urban deployment [30, 105].

Advanced modulation techniques like DLoRa can improve channel capacity, while integrating topography data enhances prediction accuracy for network planning [21, 106]. Leveraging non-terrestrial networks optimizes traffic management in rural areas [107, 68].

Future research should refine security protocols to address evolving threats, focusing on resilience against jamming and interference. By advancing these directions, the IoT community can develop secure, efficient, and scalable LPWAN solutions that meet diverse application demands, ensuring robust protection against cyber threats and addressing challenges like mobility and long-range communication [30, 32].

7 Protocol Comparison and Network Scalability

7.1 Comparative Analysis of LPWAN Technologies

Low-Power Wide-Area Networks (LPWANs) are integral to IoT applications, providing extensive connectivity, low energy usage, and cost-effective deployment. These networks are designed to support numerous devices over long ranges with minimal power consumption, addressing mobility and environmental challenges. Various LPWAN technologies, including LoRa, Sigfox, and NB-IoT, offer unique features tailored to specific use cases, with ongoing research optimizing their performance for smart cities and machine-to-machine communications [30, 25, 59, 32]. This analysis evaluates these technologies, focusing on scalability, energy efficiency, throughput, and reliability.

LoRa technology is noted for its adaptability and scalability across deployments, using chirp spread spectrum (CSS) modulation to maintain spectral efficiency. Optimizing node density around receivers enhances reliability and throughput, with non-uniform deployments offering superior coverage over traditional methods [108]. Adjusting parameters like data rate and bandwidth significantly affects packet reception and energy consumption [109]. Tools like LoRaWANSim enable optimization of network design based on performance metrics [110].

LoRa networks employ advanced resource management to minimize energy use while maintaining high packet delivery ratios. The S-LoRa method synchronizes devices to improve performance, presenting a viable alternative to existing protocols [111]. Deep reinforcement learning (DRL) methods enhance LoRa's scalability and efficiency, especially in dense environments [80]. The HARE protocol stack achieves up to 15

Sigfox, characterized by ultra-narrowband communication, provides a cost-effective solution for applications with minimal data needs, such as asset tracking and environmental monitoring, offering long battery life and low operational costs [59].

NB-IoT, a cellular-based LPWAN, excels in robust coverage and high capacity, ideal for applications requiring reliable data transmission over extended periods. Comparative studies show NB-IoT's energy efficiency is comparable to LoRa, though with greater variability in energy use and delays, impacting its suitability for certain applications [86].

Innovations like drone-aided localization in LoRa networks improve localization precision over traditional setups [35]. The IoT Cloud-RAN testbed offers ultra-precise synchronization and localization using existing LPWAN infrastructure [41]. The CR-MAC protocol outperforms conventional LoRaWAN in various scenarios, effectively managing communication protocols [37].

This comparative analysis highlights the distinct advantages and limitations of LPWAN technologies, emphasizing critical factors like energy efficiency, coverage, data rate, and security. Understanding these differences is crucial for selecting the most suitable technology for specific IoT applications, particularly in industrial settings where connectivity requirements are evolving [30, 31, 54, 32]. This knowledge enables stakeholders to make informed deployment decisions tailored to application needs and operational conditions.

7.2 Protocol Comparisons and Performance Metrics

Benchmark	Size	Domain	Task Format	Metric
Multi-RAT[112]	4,597	Environmental Monitoring	Energy Consumption Measurement	Packet Delivery Ratio, Energy Consumption per Byte
LoRaTM[113]	54	Smart Metering	Performance Evaluation	Packet Error Rate, Received Signal Strength Indication
LoRaWAN-IE[114]	2,500,000	Wireless Communication	Packet Delivery Evaluation	Packet Error Rate, Signal-to-Interference Ratio
NELORA-BENCH[115]	27,329	Wireless Communication	Classification	SER, SNR gain
SCDB[55]	462	Occupancy Estimation	Classification	Accuracy, RMSE
Orchestra[57]	6	Wireless Sensor Networks	Performance Evaluation	Energy Consumption, Stabilization Time
CC-RPL[93]	30	Networking	Performance Evaluation	PDR, AE2ED
6LoWPAN[61]	50	Embedded Networks	Performance Evaluation	PDR, Latency

Table 3: This table presents a comprehensive comparison of various benchmarks utilized for evaluating communication protocols in diverse IoT domains. It includes detailed information on the benchmark size, domain of application, task format, and the specific metrics used for performance evaluation. This comparison aids in understanding the operational characteristics and effectiveness of each protocol under different conditions.

Analyzing communication protocols within LPWANs is essential for understanding scalability, efficiency, and performance in diverse IoT applications. A key protocol is the Routing Protocol for Low-Power and Lossy Networks (RPL), evaluated using metrics like packet delivery ratio (PDR), latency, and skewness indexes [44]. These metrics assess the protocol's effectiveness in maintaining reliable communication across resource-constrained networks. Table 3 provides a comparative overview of benchmarks used to assess communication protocols across various IoT applications, highlighting their size, domain, task format, and performance metrics.

The SB-RPL protocol, an RPL extension, addresses load balancing by incorporating skewness and subtree size into routing decisions, enhancing PDR and reducing latency. Experiments demonstrate SB-RPL's superior performance over traditional RPL, optimizing network efficiency in dense environments [44].

Protocols like LoRaWAN and Sigfox are evaluated for scalability and energy efficiency. LoRaWAN supports numerous devices while maintaining low energy consumption, crucial for emerging IoT applications requiring massive Machine-Type Communications (mMTC). Its flexible network parameter configuration allows optimization for specific applications, enhancing energy efficiency and performance. However, understanding these parameters is necessary to fully leverage LoRaWAN's strengths and mitigate inefficiencies [25, 86]. Its scalability is further enhanced by an adaptive data rate mechanism that optimizes capacity and reduces interference.

Sigfox's ultra-narrowband communication offers a cost-effective solution for low data transmission applications, with energy efficiency and long-range capabilities suitable for remote areas with limited cellular coverage. Leveraging non-terrestrial networks (NTNs) like UAVs and satellites, Sigfox effectively aggregates, processes, and relays IoT traffic, addressing sparse network infrastructure challenges [25, 68].

Performance benchmarking with simulation tools and real-world testbeds provides insights into operational characteristics under various conditions. Analyzing throughput, latency, and energy consumption helps assess IoT communication protocols' advantages and limitations. This analysis informs stakeholders about protocol suitability for specific applications in environments like rural or urban settings, empowering decision-makers to optimize IoT solution deployment [116, 68, 112, 66, 65].

Comparative analysis underscores the need for selecting suitable protocols tailored to application requirements, considering scalability, energy efficiency, reliability, coverage, cost-effectiveness, and Quality of Service (QoS). Understanding each protocol's strengths and weaknesses is essential for optimizing performance in diverse scenarios, particularly for industrial IoT applications [31, 117, 87]. Leveraging protocol strengths enables optimal network performance to meet interconnected devices' growing demands.

7.3 Scalability Solutions and Future Directions

Addressing scalability challenges in LPWANs is vital for supporting increasing IoT application demands. Enhancing spectral efficiency and managing interference in dense deployments, such as those using LoRa, involves optimizing network configurations with multiple base stations and directional antennas. Research shows multiple base stations significantly improve data extraction rates in interference-prone environments, outperforming directional antennas. Optimal non-uniform deployment and uplink random access schemes enhance coverage and performance. Stochastic geometry analysis of interference distribution and packet success probability aids in developing policies for joint spreading factor allocation, power control, and duty cycle adjustments, addressing fairness and maximizing throughput in high-density environments [85, 108, 107]. Adaptive resource allocation and dynamic channel management improve capacity, ensuring LPWANs accommodate many devices without compromising performance.

Advanced modulation schemes and interference mitigation strategies are crucial for scalability. Techniques that adjust transmission parameters based on real-time conditions maintain efficient communication in dense environments, enhancing throughput and extending IoT device battery life, essential for remote operations. Leveraging LPWAN and NTNs like satellites and UAVs addresses mobility and gateway distance challenges, ensuring reliable performance and energy efficiency for various applications [30, 68].

Future research should refine frameworks like ChirpOTLE to better understand and mitigate LPWAN vulnerabilities [100]. Exploring attack scenarios and developing robust countermeasures are essential for ensuring security and reliability as LPWANs scale. Integrating machine learning to predict network behavior and optimize resource allocation presents a promising direction for scalability enhancement.

Standardizing protocols and improving interoperability among LPWAN technologies will also contribute to scalability. Efficient communication across network types, as seen in LoRaWAN and DSME-LoRa, facilitates large-scale IoT application deployment. These technologies address low-power, resource-constrained device challenges while ensuring wide-area coverage, leading to effective network resource utilization, demonstrated by smart city projects and evaluations highlighting their capabilities and limitations in managing diverse IoT ecosystems [15, 71, 24].

8 Conclusion

Low-Power Wide-Area Networks (LPWANs) are pivotal in advancing the Internet of Things (IoT) by providing efficient, long-range connectivity with low energy consumption, which is crucial for a wide array of applications. Technologies such as LoRa, ZigBee 3.0, and 6LoWPAN have significantly contributed to enhancing the scalability, energy efficiency, and reliability of IoT networks. DSME-LoRa, for example, has demonstrated superior performance over LoRaWAN in terms of packet reception and transmission delays, suggesting its potential to optimize long-range communications in IoT contexts. Additionally, LoRaWAN's capability to monitor urban traffic effectively underscores its utility in developing large-scale traffic management solutions.

Despite these technological strides, challenges remain, notably in managing device density, ensuring network scalability, and addressing security concerns. Current advancements in LPWANs have led to improvements in throughput and efficiency, exemplified by the D2D communications protocol's success in reducing data transfer times and energy usage, thereby proving its relevance for smart grid applications. Future research should focus on refining models to better handle complex traffic patterns and developing adaptive bitrate allocation strategies that respond to real-time network conditions. Moreover, exploring adaptive transmission parameter selection is essential for enhancing scalability and energy efficiency, while maintaining high frame success rates.

The potential of frameworks like EnvSen in accurately tracking wildfire spread while managing communication costs opens new research avenues in optimizing communication strategies. Further investigation into design principles for other low-power Internet protocols, along with optimizations for energy efficiency and code size, is necessary. Enhancing simulation models to include more variables and real-time data, and integrating machine learning techniques for routing and compression optimization, represent critical future research directions.

AI-generated, for reference only.

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

[22] Kazım Rıfat Özyılmaz and Arda Yurdakul. Designing a blockchain-based iot infrastructure with ethereum, swarm and lora, 2018.

[23] 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.

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

[25] 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.

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

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

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

[29] 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.

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

[31] 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.

[32] 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.

[33] 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.

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

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

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

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

[38] 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.

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

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

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

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

[43] 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.

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

[45] 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.

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

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

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

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

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

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

[52] 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.

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

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

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

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

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

[58] 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.

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

[60] 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.

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

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

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

[64] 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.

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

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

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

[68] 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.

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

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

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

[72] Mohieddine El Soussi, Pouria Zand, Frank Pasveer, and Guido Dolmans. Evaluating the performance of emtc and nb-iot for smart city applications, 2017.

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

[74] Zhibang Xie and Qingjin Deng. Loongson iot gateway: A technical review, 2017.

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

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

[77] 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.

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

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

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

[81] 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.

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

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

[84] 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.

[85] Jiangbin Lyu, Dan Yu, and Liqun Fu. Analysis and optimization for large-scale lora networks: Throughput fairness and scalability, 2021.

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

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

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

[89] 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.

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

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

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

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

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

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

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

[97] Tarun Rao Keshabhoina and Marcos M. Vasconcelos. Data-driven classification of low-power communication signals by an unauthenticated user using a software-defined radio, 2023.

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

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

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

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

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

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

[104] 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.

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

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

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

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

[109] 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.

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

[111] 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.

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

[113] Muhammad Nouman Rafi and Muhammad Muaaz. Performance evaluation of the lora protocol in the context of smart meter, 2019.

[114] Konstantin Mikhaylov, Juha Petajajarvi, and Janne Janhunen. On lorawan scalability: Empirical evaluation of susceptibility to inter-network interference, 2017.

[115] Jialuo Du, Yidong Ren, Mi Zhang, Yunhao Liu, and Zhichao Cao. Nelora-bench: A benchmark for neural-enhanced lora demodulation, 2023.

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

[117] Maxim S. Ilderyakov and Nikita V. Stepanov. Using a small number of devices to experimentally estimate the packet delivery ratio on a lorawan network with a large number of end devices, 2019.

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.