NexLattice

Theoretical Study

In recent years, mesh networking has emerged as a vital communication paradigm in the Internet of Things (IoT), enabling distributed, scalable, and fault-tolerant systems. Various studies have explored low-power, long-range, and reliable communication models for embedded devices. Solé *et al.* [1] introduced middleware for distributed applications over LoRa mesh networks, emphasizing decentralized control and robustness but facing bandwidth limitations. Similarly, Berto *et al.* [2] proposed a peer-to-peer LoRa-based mesh design that enhanced coverage while maintaining low power consumption, although it relied heavily on LoRa-specific transceivers. Giménez *et al.* [3] extended this concept by integrating federated learning into LoRa-based systems, showcasing intelligent distributed processing at the network edge but constrained by limited throughput. Sun *et al.* [4] presented a comprehensive survey of LoRa's evolution, underscoring its scalability yet highlighting performance trade-offs in data rate and universality.

Parallel research on WiFi-based mesh networks offers greater bandwidth and interoperability. Akyildiz *et al.* [5] and Bicket *et al.* [6] analyzed IEEE 802.11-based mesh architectures, focusing on routing efficiency, dynamic topology management, and scalability. Espressif's proprietary ESP-MESH [7] provides self-organizing WiFi mesh connectivity but lacks cross-platform compatibility, restricting use to ESP-specific ecosystems. Security studies by Sicari *et al.* [8] and Fernandes *et al.* [9] further emphasize lightweight encryption, authentication, and trust mechanisms for IoT environments.

The literature reveals that while LoRa and WiFi mesh frameworks address communication efficiency, none provide a **universal, hardware-agnostic, WiFi-based secure mesh protocol**. This research gap motivates **NexLattice**, which aims to deliver a modular, lightweight, and secure communication layer for embedded IoT devices using standard WiFi capabilities.

1. LoRa-Based Mesh Networking

Solé *et al.* [1] proposed a middleware solution for distributed applications over a **LoRa Mesh Network**, enabling long-range and low-power communication for IoT devices. However, the system's bandwidth constraints limit real-time and high-throughput applications.

Berto *et al.* [2] developed a **LoRa-based peer-to-peer mesh network** architecture that allows direct communication between nodes without centralized infrastructure. Although the solution demonstrated robustness and low energy consumption, it remained dependent on LoRa-specific transceivers and lacked universal adaptability to common WiFi-enabled devices.

Giménez *et al.* [3] explored **federated learning** over LoRa mesh networks to enable distributed machine learning across embedded devices. This demonstrated the feasibility of collaborative computation across constrained networks, yet performance bottlenecks due to LoRa's limited data rate remained a concern.

Sun *et al.* [4] presented a **comprehensive survey of LoRa technologies**, summarizing advancements in network scalability, adaptive data rates, and energy-efficient routing. Despite these improvements, LoRa's hardware dependency and low throughput restrict its applicability for high-speed, short-range mesh systems.

2. WiFi-Based Mesh Networking

In contrast, WiFi-based mesh networking offers higher bandwidth and wider compatibility. Works like those by ***Akyildiz et al. [5]*** and ***Bicket et al. [6]*** have analyzed the scalability and routing efficiency of wireless mesh networks based on IEEE 802.11 standards. These studies highlight WiFi's advantages in throughput and integration with existing infrastructure but also point out challenges in energy efficiency and interference management.

ESP-based mesh frameworks such as **ESP-MESH** from Espressif [7] provide proprietary solutions for ESP32 devices, enabling automatic node discovery and routing. However, they rely on vendor-specific firmware and are not interoperable with other WiFi microcontrollers or MicroPython environments.

3. IoT Security and Authentication

Security in IoT mesh systems remains a core challenge. Research by ***Sicari et al. [8]*** and ***Fernandes et al. [9]*** emphasizes that lightweight encryption, mutual authentication, and trust management are crucial for securing resource-constrained devices. Protocols like TLS and DTLS, while secure, are often too heavy for microcontrollers without dedicated hardware acceleration.

4. NexLattice’s Distinct Approach

Existing literature demonstrates that **LoRa-based mesh solutions** prioritize range and power efficiency, while **WiFi-based mesh networks** focus on bandwidth and scalability. However, most WiFi-based systems are **hardware-locked** or **lack a universal standard** for embedded environments like ESP32, Raspberry Pi Pico W, and similar boards.

NexLattice aims to bridge this gap by:

- Providing a **universal WiFi-based mesh protocol** implemented in MicroPython.
- Ensuring **plug-and-play compatibility** across various WiFi-capable microcontrollers.
- Incorporating **lightweight encryption and mutual authentication** using standard cryptographic primitives.
- Offering a **dashboard interface** for real-time visualization, monitoring, and device management.

This design leverages the existing WiFi capabilities of embedded devices, eliminating the need for external communication modules like LoRa, ZigBee, or BLE.

References

[1] J. M. Solé, R. P. Centelles, F. Freitag, R. Meseguer, and R. Baig, “Middleware for Distributed Applications in a LoRa Mesh Network,” *ACM Transactions on Embedded Computing Systems*, vol. 24, no. 4, Art. 60, pp. 1–26, Jul. 2025. doi: 10.1145/3747295

[2] R. Berto, P. Napoletano, and M. Savi, “A LoRa-Based Mesh Network for Peer-to-Peer Long-Range Communication,” *Sensors*, vol. 21, no. 13, p. 4314, Jul. 2021. doi: 10.3390/s21134314

[3] N. L. Giménez *et al.*, “Embedded Federated Learning over a LoRa Mesh Network,” *Pervasive and Mobile Computing*, vol. 91, p. 101819, 2023. doi: 10.1016/j.pmcj.2023.101819

[4] Z. Sun *et al.*, “Recent Advances in LoRa: A Comprehensive Survey,” *ACM Computing Surveys*, vol. 55, no. 12, Art. 243, pp. 1–35, Dec. 2022. doi: 10.1145/3543856

[5] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless Mesh Networks: A Survey,” *Computer Networks*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[6] J. Bicket, D. Aguayo, S. Biswas, and R. Morris, “Architecture and Evaluation of an Unplanned 802.11b Mesh Network,” in *Proc. of MobiCom 2005*, Cologne, Germany, Sep. 2005.

[7] Espressif Systems, “ESP-MESH: Networking Solution Based on ESP32,” 2020. [Online]. Available: https://docs.espressif.com

[8] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, Privacy and Trust in Internet of Things: The Road Ahead,” *Computer Networks*, vol. 76, pp. 146–164, 2015.

[9] E. Fernandes, J. Jung, and A. Prakash, “Security Analysis of Emerging Smart Home Applications,” in *Proc. of IEEE Security and Privacy (SP)*, San Jose, CA, 2016.