NexLattice: Secure, Plug&play Offgrid Wi-Fi Mesh for IoT

A Project Presentation submitted in partial fulfilment of the requirements for the degree of

Bachelor of Technology in Computer Science and Engineering

By

Vivek Upadhaya

ROLL NO.: ADTU/2022-26/BCS/048

Debayangshu Sen

ROLL NO.: ADTU/2022-26/BCS/049

Rajdeep Roy

ROLL NO.: ADTU/2022-26/BCS/046

Under the guidance of
Dr. Debashis Dev Misra
Associate Professor

FACULTY OF COMPUTER TECHNOLOGY

ASSAM DOWN TOWN UNIVERSITY

GUWAHATI-26, ASSAM.

December 2025

Table of Contents

INTRODUCTION

- **NexLattice** is a **secure, plug-and-play Wi-Fi mesh** network for IoT devices.
- Unlike existing protocols, it **uses standard Wi-Fi** to create a **self-healing, scalable, and offline network**.
- The protocol is designed to be **universal** and works on :
  - **ESP32**
  - **Raspberry Pi Pico W**
  - Other similar microcontrollers.

PROBLEM STATEMENT

- **Issues :** Current mesh networking protocols like **Zigbee, LoRa, and ESP-MESH** are often **vendor-specific**, **low-speed**, or **require special hardware**.
- **Gap :** There's a gap in **universal, secure Wi-Fi mesh networking** that can be used across different IoT devices, without needing a router or internet.

MOTIVATION

- **Universal Compatibility:** Existing mesh protocols (e.g., Zigbee, LoRa) require specific hardware or are not Wi-Fi based. NexLattice aims to fill this gap by using **standard Wi-Fi** that works across various microcontrollers (ESP32, Raspberry Pi Pico, etc.).
- **Offgrid Communication:** Wi-Fi mesh can operate without the need for routers or internet, making it perfect for **offgrid** environments like **disaster zones, rural areas,** or **remote sensor networks**.
- **Secure and Lightweight:** Unlike many mesh protocols, NexLattice ensures **secure data exchange** (encryption) while keeping **low latency** and **minimal power consumption**.
- **Scalable and Fault-Tolerant:** The system is **self-healing** and can scale to a large number of devices, ensuring **reliable communication** even when nodes fail or leave the network.
- **Plug-and-Play Setup: Easy integration** for developers, with a **simple MicroPython library** for quick deployment, allowing anyone to create their own mesh network with minimal configuration.

OBJECTIVES

AIM :

To develop a universal, secure, and scalable Wi-Fi mesh protocol for IoT devices, enabling offline, peer-to-peer communication without reliance on routers or internet access.

Objectives :

- Design and Develop a universal Wi-Fi mesh protocol.
- Ensure secure, encrypted, and peer-to-peer communication.
- Provide plug-and-play support for devices like ESP32.
- Build a dashboard for monitoring and control.

LITERATURE REVIEW

Author(s) & Year	Title	Methodology	Research Purpose	Key Findings
J. M. Solé, R. P. Centelles, F. Freitag, R. Meseguer, R. Baig (2025)	*Middleware for Distributed Applications in a* ***LoRa Mesh Network***	Middleware design, system architecture, experimental evaluation	To enable distributed applications over LoRa-based mesh networks	Middleware abstraction simplifies application development and enables scalable distributed coordination despite LoRa constraints
R. Berto, P. Napoletano, M. Savi (2021)	*A* ***LoRa-Based Mesh Network*** *for Peer-to-Peer Long-Range Communication*	Prototype implementation, field experiments	To investigate peer-to-peer long-range communication using LoRa mesh	LoRa mesh networking supports decentralized communication with extended coverage and acceptable reliability
N. L. Giménez et al. (2023)	*Embedded Federated Learning over a* ***LoRa Mesh Network***	Embedded implementation, federated learning experiments	To assess feasibility of federated learning over LoRa mesh networks	Federated learning is feasible on constrained LoRa meshes with optimized communication strategies
Z. Sun et al. (2022)	*Recent Advances in* ***LoRa****: A Comprehensive Survey*	Systematic literature review	To review state-of-the-art LoRa technologies and applications	Identifies scalability challenges, mesh extensions, and open research problems in LoRa networks
W. Wang, G. He, J. Wan (2011)	*Research on* ***ZigBee Wireless Communication Technology***	Protocol analysis, technical evaluation	To analyze ZigBee communication principles and performance	ZigBee offers low power consumption, self-organizing mesh networking, and reliability for short-range IoT
J. Bicket, D. Aguayo, S. Biswas, R. Morris (2005)	*Architecture and Evaluation of an Unplanned* ***802.11b Mesh Network***	Real-world deployment, performance measurement	To evaluate unplanned Wi-Fi mesh network architectures	Demonstrates robustness, self-configuration, and fault tolerance in real mesh deployments
Espressif Systems (2020)	*ESP-MESH: Networking Solution Based on ESP32*	Technical documentation, system design description	To document ESP-MESH networking architecture	ESP-MESH provides scalable, self-healing Wi-Fi mesh networking for ESP32-based IoT systems
S. Sicari, A. Rizzardi, L. A. Grieco, A. Coen-Porisini (2015)	*Security, Privacy and Trust in Internet of Things: The Road Ahead*	Survey and conceptual analysis	To identify IoT security, privacy, and trust challenges	Highlights major vulnerabilities and calls for holistic, security-by-design IoT architectures
E. Fernandes, J. Jung, A. Prakash (2016)	*Security Analysis of Emerging Smart Home Applications*	Static and dynamic security analysis	To evaluate security of smart home applications	Reveals widespread security weaknesses and insufficient permission controls
C. M. Ramya, M. Shanmugaraj, R. Prabakaran (2011)	*Study on ZigBee Technology*	Comparative study, standards analysis	To study ZigBee standards and use cases	Confirms ZigBee's effectiveness for low-data-rate, low-power wireless sensor networks
A. N. A. A. Aziz, R. A. Rashid, M. N. M. Nasir, M. A. Sarijari (2024)	*ESP Mesh Network for Security Application*	Prototype development, experimental evaluation	To evaluate ESP-MESH for security-related applications	ESP-MESH demonstrates reliable communication and low latency for distributed security systems

Table 1: Comparative Study of Related Works

LITERATURE REVIEW

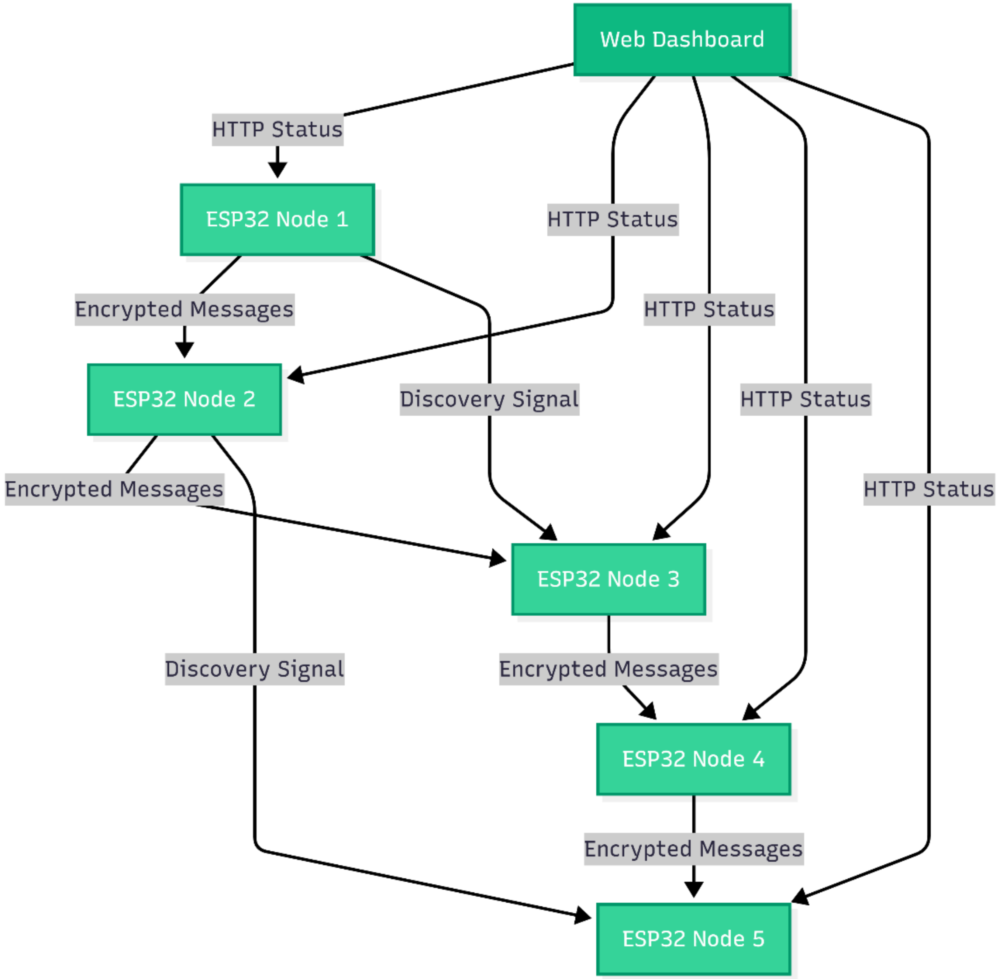
Identified Research Gaps	Limitations in existing work	Our Proposed Solution
Limited support for true multi-hop, application-level LoRa mesh networking	Most LoRa solutions focus on star topology or basic routing without application abstraction	NexLattice introduces a modular mesh framework with application-aware routing and middleware support
High communication overhead in constrained LoRa mesh environments	Existing systems suffer from latency and packet loss under dense or multi-hop scenarios	NexLattice uses lightweight messaging, adaptive forwarding, and duty-cycle–aware scheduling
Poor integration of edge intelligence in low-power mesh networks	Federated learning and analytics are rarely optimized for extreme bandwidth limits	NexLattice enables optional edge intelligence with ultra-lightweight data aggregation and model updates
Limited security mechanisms in ESP/Wi-Fi mesh and LPWAN hybrids	Security is often add-on and not end-to-end across heterogeneous nodes	NexLattice embeds secure node authentication and encrypted mesh communication by design
Lack of unified framework across LoRa, ESP-MESH, and heterogeneous IoT nodes	Prior work targets single technologies in isolation	NexLattice provides a unified, extensible lattice-style architecture supporting heterogeneous mesh nodes

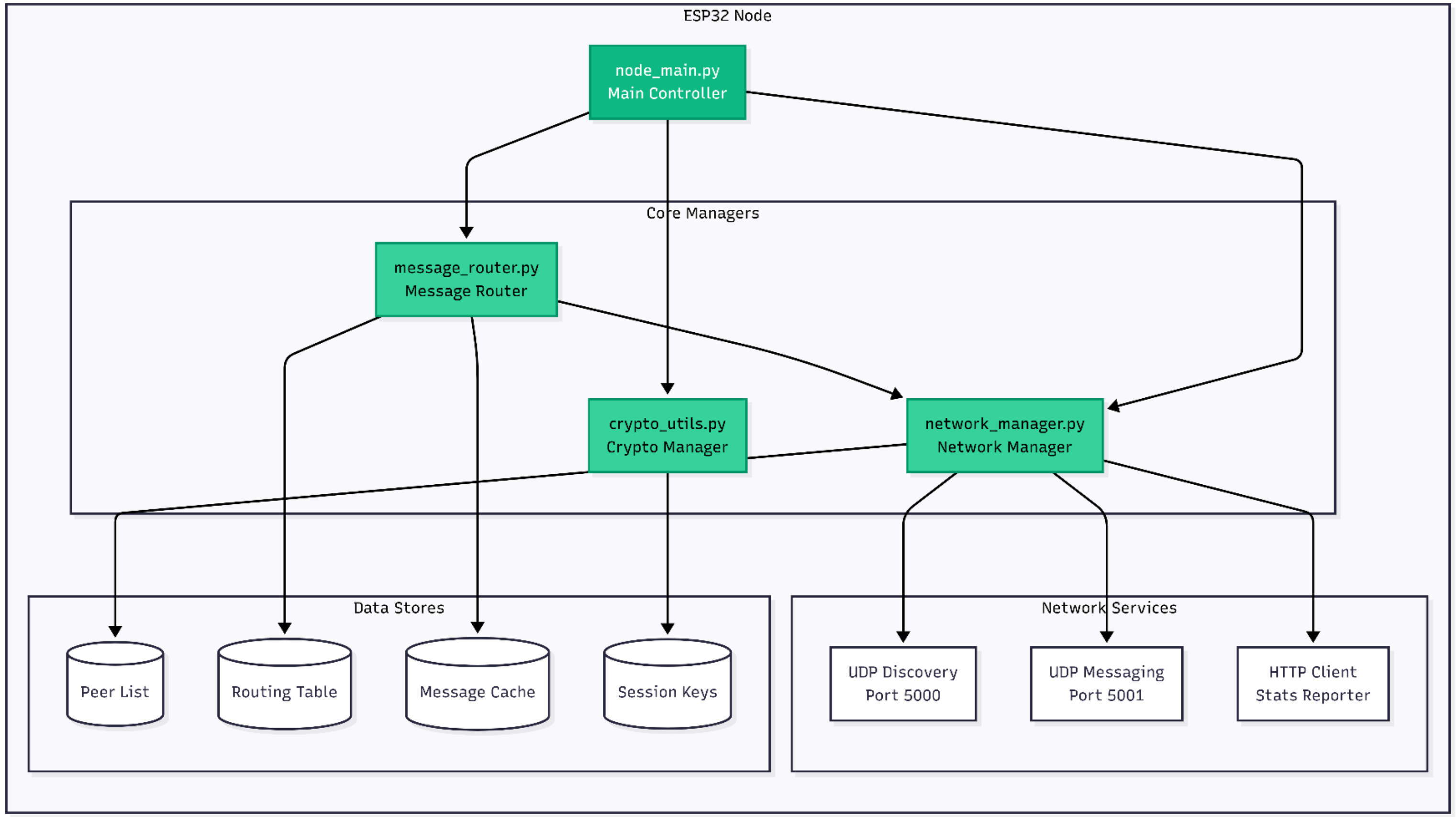
Table 2: Identified Research Gaps and Proposed solutions

METHODOLOGY

- **Protocol Design :**
  - Develop a lightweight Wi-Fi mesh protocol using UDP packets for low-latency communication and integrate AES encryption for secure data exchange.
- **Node Discovery & Network Formation :**
  - Implement discovery signals to allow devices to find each other and form a self-healing mesh network. Nodes forward messages to the destination via hop-based routing.
- **Security :**
  - Use AES-128 encryption and authentication to ensure secure, peer-to-peer communication. Each message will include a nonce and timestamp to prevent replay attacks.
- **Plug-and-Play Setup :**
  - Provide a MicroPython library for easy integration with IoT devices, enabling automatic setup of the mesh network without additional configurations.
- **Dashboard :**
  - Develop a web-based dashboard to visualize the mesh network, monitor node status, and track performance metrics like latency and packet delivery ratio.

SYSTEM ARCHITECTURE & NODE ARCHITECTURE





IMPLEMENTATION

The **NexLattice protocol** enables **Wi-Fi-based mesh networking** for IoT devices, allowing them to communicate **securely** without the need for routers or internet.

- **Wi-Fi Mesh Protocol**:
  - Uses **UDP** for communication and **AES-128 encryption** for secure data transfer.
  - Allows devices to form a **self-healing mesh network**.
- **Node Discovery**:
  - Nodes send **discovery signals** (UDP broadcast) to find nearby devices and form connections.
- **Routing**:
  - **Hop-based routing** forwards messages to the destination through intermediate nodes, using **local routing tables**.
- **Plug-and-Play Setup**:
  - Integrated via **MicroPython**, enabling easy **plug-and-play** setup for devices like **ESP32**.
- **Security**:
  - **AES encryption** and **device authentication** ensure secure and trusted communication.
- **Monitoring Dashboard**:
  - A **web dashboard** tracks **node status**, **latency**, and **packet delivery**.

CHALLENGES

- **Scalability:**
  - **Challenge:** Increased nodes could lead to congestion.
  - **Solution:** Efficient hop-based routing and dynamic path recalculation.
- **Latency:**
  - **Challenge:** Maintaining low latency in a mesh network.
  - **Solution:** Optimized UDP messaging with minimal overhead.
- **Network Instability:**
  - **Challenge:** Nodes joining/leaving the network.
  - **Solution:** Self-healing network with automatic reconnection.
- **Energy Consumption:**
  - **Challenge:** Low power usage for battery-operated devices.
  - **Solution:** Efficient routing and sleep modes for nodes when inactive.
- **Security:**
  - **Challenge:** Ensuring secure communication without performance loss.
  - **Solution:** Lightweight AES encryption and node authentication.
- **Device Compatibility:**
  - **Challenge:** Supporting various IoT devices.
  - **Solution:** MicroPython library for easy plug-and-play integration.

CURRENT FINDINGS

- **Novel Approach**:
  - **NexLattice** is a **unique Wi-Fi mesh protocol** that works across a wide range of IoT devices, providing **secure, decentralized communication** without relying on external infrastructure like routers.
- **No Existing Alternatives**:
  - Unlike existing protocols (e.g., **Zigbee**, **LoRa**, or **ESP-MESH**), which often depend on specialized hardware or require **centralized management**, **NexLattice** is based purely on **Wi-Fi** and operates without **centralized control**.
- **Self-Healing Network**:
  - The **self-healing mesh network** allows nodes to join or leave dynamically, offering **scalability and flexibility** that most other mesh networks lack.
- **Plug-and-Play Integration**:
  - The protocol's integration into devices like **ESP32** through **MicroPython** makes it **easy to set up** and use, something not commonly seen in existing mesh protocols.

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] W. Wang, G. He and J. Wan, "**Research on Zigbee wireless communication technology**," 2011 International Conference on Electrical and Control Engineering, Yichang, China, 2011, pp. 1245-1249, doi: 10.1109/ICECENG.2011.6057961.

[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.

[10] C. M. Ramya, M. Shanmugaraj and R. Prabakaran, "**Study on ZigBee technology**," 2011 3rd International Conference on Electronics Computer Technology, Kanyakumari, India, 2011, pp. 297-301, doi: 10.1109/ICECTECH.2011.5942102.

[11] A. N. A. A. Aziz, R. A. Rashid, M. N. M. Nasir and M. A. Sarijari, "**ESP Mesh Network for Security Application**," 2024 IEEE International Conference on Advanced Telecommunication and Networking Technologies (ATNT), Johor Bahru, Malaysia, 2024, pp. 1-4, doi: 10.1109/ATNT61688.2024.10719207.

THANK YOU