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

A thesis submitted in partial fulfillment of the requirement for the award of the degree of

Bachelor of Technology

in

Computer Science & Engineering

under

Assam down town University

Submitted by

Vivek Upadhaya

Roll No.: ADTU/2022-26/BCS/048

B.Tech 7th Semester

Debayangshu Sen

Roll No.: ADTU/2022-26/BCS/049

B. Tech 7th Semester

Rajdeep roy

Roll No.: ADTU/2022-26/BCS/046

B.Tech 7th Semester

Under the Guidance of

Dr. Debashis Dev Misra

Associate Professor,

Faculty of Computer Technology
Assam down town University
Guwahati-26, Assam.

Session: Aug-Dec, 2025

CONTENTS

- *Certificate of Approval* *i*
- *Certificate from Guide* *ii*
- *Certificate from External Examiner* *iii*
- *Declaration* *iv*
- *Acknowledgement* *v*
- *Abstract* *vi*

1. INTRODUCTION 1-2
    1.1. Overview of the project 1
    1.2. Motivation 1
    1.3. Scope & Objective 1
    1.4. Existing System 2
    1.5. Problem Definition 2
    1.6. Proposed System 2

2. LITERATURE SURVEY 3

3. LITERATURE REVIEW 4

4. FLOW DIAGRAM 6

5. IMPLEMENTATION 7-9
    5.1. Hardware Setup 7
    5.2. Network Initialization 7
    5.3. Node Discovery Mechanism 8
    5.4. Secure Communication 8
    5.5. Mesh Routing and Data Forwarding 8
    5.6. Self-Healing Capability 9
    5.7. Monitoring and Visualization 9
    5.8. Result Analysis 9

6. TECHNOLOGIES USED 10

7. EXPERIMENTAL RESULTS 11-12
    7.1 Experimental Setup 11
    7.2 Evaluation Metrics 11
    7.3 Experimental Observations 11
    7.4 Result Summary 12

8. CONCLUSION 13

10.REFERENCES 14

Computer Science & Engineering
Faculty of Computer Technology
Assam down town University
Gandhi Nagar, Panikhaiti, Guwahati- 781026, Assam

CERTIFICATE OF APPROVAL

This is to certify that the project report entitle **"NexLattice: Secure, Plug & Play Off-Grid Wi-Fi Mesh for IoT"**submitted by **Vivek Upadhaya** bearing Roll No. **ADTU/2022-26/BCS/048**, **Debayangshu Sen** bearing Roll No. **ADTU/2022-26/BCS/049**, **Rajdeep roy** bearing Roll No. **ADTU/2022-26/BCS/046**, is hereby accorded approval as a project work carried out and presented in a manner required for acceptance in **partial fulfilment for the award of the degree of Bachelor of Technology in Computer Science & Engineering** under **Assam down town University**.

The approval of this project report does not necessarily endorse or accept every statement made, opinion expressed, or conclusion drawn therein. It only signifies the acceptance of the project report for the purpose for which it has been submitted.

Date:

Place: Guwahati

Dr Aniruddha Deka
Dean, Faculty of Computer Technology
Assam down town University
Guwahati 781026

Computer Science & Engineering
Faculty of Computer Technology
Assam down town University
Gandhi Nagar, Panikhaiti, Guwahati- 781026, Assam

CERTIFICATE FROM GUIDE

This is to certify that the project report entitled **"NexLattice: Secure, Plug & Play Off-Grid Wi-Fi Mesh for IoT"** submitted by **Vivek Upadhaya** bearing Roll No. **ADTU/2022-26/BCS/048**, **Debayangshu Sen** bearing Roll No. **ADTU/2022-26/BCS/049**, and **Rajdeep Roy** bearing Roll No. **ADTU/2022-26/BCS/046**, towards the partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science & Engineering** under **Assam down town University**, is a **bonafide project work** carried out by them under my supervision and guidance.

This work has not been submitted previously for the award of any other degree or diploma of this or any other University.

I recommend that the project report may be placed before the examiners for consideration of the award of the degree of this University.

Date:

Place: Guwahati

Dr. Debashis Dev Misra
Assistant Professor,
Faculty of Computer Technology
Assam down town University
Guwahati 781026

Computer Science & Engineering
Faculty of Computer Technology
Assam down town University
Gandhi Nagar, Panikhaiti, Guwahati- 781026, Assam

CERTIFICATE FROM EXTERNAL EXAMINER

This is to certify that the project report entitled **"NexLattice: Secure, Plug & Play Off-Grid Wi-Fi Mesh for IoT"** submitted by **Vivek Upadhaya** bearing Roll No. **ADTU/2022-26/BCS/048**, **Debayangshu Sen** bearing Roll No. **ADTU/2022-26/BCS/049**, and **Rajdeep Roy** bearing Roll No. **ADTU/2022-26/BCS/046**, towards the partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science & Engineering** under **Assam down town University**, is a **bonafide project work** carried out by them under the supervision and guidance of **Dr. Arpita Nath Boruah**, **Associate Professor**, Department of Computer Science & Engineering, Assam down town University, Guwahati.

The project work has been examined by me and found to be **satisfactory**.

I recommend the project report for consideration for the award of the degree of **Bachelor of Technology** under **Assam down town University**.

Date:

Place: Guwahati

…….
External Examiner

Assam Down Town University

Faculty of Computer Technology

DECLARATION

This is to certify that the project report entitled **"NexLattice: Secure, Plug & Play Off-Grid Wi-Fi Mesh for IoT"** submitted by **Vivek Upadhaya** bearing Roll No. **ADTU/2022-26/BCS/048**, **Debayangshu Sen** bearing Roll No. **ADTU/2022-26/BCS/049**, and **Rajdeep Roy** bearing Roll No. **ADTU/2022-26/BCS/046**, towards the partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science & Engineering** under **Assam down town University**, is a **bonafide project work** carried out by them under the supervision and guidance of **Dr. Debashis Dev Misra, Associate Professor**, Department of Computer Science & Engineering, Assam down town University, Guwahati.

The project report has been examined by me and found to be satisfactory. I recommend the project report for consideration for the award of the degree of **Bachelor of Technology in Computer Science & Engineering** under **Assam down town University**.

Vivek Upadhaya
Roll No.: ***ADTU/2022-26/BCS/048***
B.Tech CSE , 7th Semester
Session: July – Dec, 2025

Date:
Place: Guwahati

Debayangshu Sen
Roll No.: ***ADTU/2022-26/BCS/049***
B.Tech CSE , 7th Semester
Session: July – Dec, 2025

Date:
Place: Guwahati

Rajdeep Roy
Roll No.: ***ADTU/2022-26/BCS/046***
B.Tech CSE , 7th Semester
Session: July – Dec, 2025

Date:
Place: Guwahati

ACKNOWLEDGEMENT

We would like to express our sincere and heartfelt gratitude to our project guide, **Dr. Debashis Dev Misra**, **Associate Professor**, Department of Computer Science & Engineering, Assam down town University, for his constant guidance, valuable suggestions, and continuous encouragement throughout the duration of this project. His academic support and constructive feedback played a vital role in the successful completion of this work.

We are deeply thankful to the **Faculty of Computer Technology**, **Assam down town University**, for providing us with the necessary facilities, resources, and academic environment required to carry out this project effectively. The support and cooperation of the faculty members greatly contributed to our learning experience.

We would also like to acknowledge our parents and friends for their constant motivation, moral support, and encouragement throughout the project period. Their belief in us helped us remain focused and motivated.

Finally, we extend our sincere thanks to all those who directly or indirectly contributed to the successful completion of this project.

ABSTRACT

With the rapid growth of Internet of Things (IoT) applications, the need for reliable, secure, and infrastructure-independent communication among embedded devices has become increasingly important. Conventional IoT networking solutions such as Zigbee, LoRa, and vendor-specific mesh protocols either require specialized hardware, suffer from low data rates, or lack universality across different devices. This project presents **NexLattice**, a **secure, plug-and-play off-grid Wi-Fi mesh networking framework** designed for IoT environments using standard Wi-Fi capabilities of embedded devices.

NexLattice leverages local Wi-Fi communication, software-based access point (SoftAP) functionality, and lightweight peer discovery to enable autonomous device-to-device communication without reliance on centralized routers or internet connectivity. The system incorporates encryption and authentication mechanisms to ensure secure data exchange while maintaining low latency and minimal resource usage. A multi-node mesh prototype is designed to demonstrate dynamic node discovery, multi-hop message forwarding, and self-healing behavior in the presence of node failures.

The project includes the development and demonstration of a five-node Wi-Fi mesh network, along with performance evaluation based on packet delivery ratio, latency, and routing stability. Additionally, a theoretical model is proposed to highlight how Wi-Fi-based mesh networking can serve as a universal alternative or complement to existing IoT communication frameworks. The outcomes of this project indicate that NexLattice offers a flexible, secure, and scalable solution for infrastructure-free IoT networking.

INTRODUCTION

1.1 Overview of the Project

The rapid growth of Internet of Things (IoT) devices has created a strong demand for reliable, secure, and infrastructure-independent communication systems. Traditional IoT networking solutions often rely on centralized routers, cloud services, or specialized communication hardware, which limits their usability in off-grid or resource-constrained environments. Mesh networking has emerged as a promising solution by enabling devices to communicate directly and cooperatively without dependence on a central authority.

NexLattice is a secure, plug-and-play, off-grid Wi-Fi mesh networking framework designed for IoT devices. The project leverages the native Wi-Fi capabilities of microcontrollers such as ESP32 and Pico W to establish decentralized peer-to-peer communication. NexLattice focuses on universality, low latency, and security while avoiding the need for additional radio hardware, proprietary protocols, or constant internet connectivity.

1.2 Motivation

Most existing IoT mesh solutions such as Zigbee, LoRa mesh, and vendor-specific ESP mesh protocols require either specialized hardware, low-bandwidth communication, or device-specific implementations. These limitations restrict interoperability and increase deployment complexity and cost. Furthermore, many Wi-Fi-based solutions assume the presence of routers or active internet connections, which are not always available.

The motivation behind NexLattice is to design a **universal Wi-Fi mesh protocol** that works entirely offline, is easy to deploy, and can operate on commonly available IoT hardware. By using standard Wi-Fi features and lightweight software-based routing, NexLattice aims to simplify mesh networking while maintaining security and performance.

1.3 Scope and Objectives

The scope of this project includes the design, development, and demonstration of a Wi-Fi-based mesh networking protocol for IoT devices. The project focuses on protocol design, node discovery, secure communication, routing logic, and performance evaluation through a small-scale prototype.

The primary objectives of NexLattice are:

- To design a secure and decentralized Wi-Fi mesh network for IoT device
- To enable plug-and-play node discovery and authentication
- To ensure off-grid operation without routers or internet
- To evaluate performance metrics such as latency, packet delivery ratio, and routing stability

- 1.4 Existing System

Existing IoT mesh networking systems rely on technologies such as Zigbee, LoRa, Thread, and ESP-MESH. While these systems provide mesh capabilities, they often suffer from limitations such as low data rates, dependency on proprietary hardware, vendor lock-in, or complex protocol stacks. Additionally, many Wi-Fi-based mesh solutions are designed for consumer routers and are not suitable for microcontroller-based IoT devices.

These systems also typically require pre-configured networks, gateways, or centralized controllers, making deployment and scalability challenging in dynamic or remote environments.

1.5 Problem Definition

Despite the availability of multiple mesh networking solutions, there is a lack of a **universal, Wi-Fi-based, lightweight, and secure mesh protocol** that can operate independently of existing infrastructure. Current solutions either compromise on performance, security, or ease of deployment, or require additional hardware and complex configuration.

The problem addressed in this project is the absence of a simple, secure, and hardware-agnostic Wi-Fi mesh networking framework that enables autonomous communication among IoT devices in off-grid scenarios.

1.6 Proposed System

The proposed system, NexLattice, introduces a decentralized Wi-Fi mesh networking framework that uses standard Wi-Fi capabilities in IoT devices to establish peer-to-peer communication. Each node in the network performs automatic discovery, authentication, and routing, allowing data to hop across multiple nodes until it reaches its destination.

NexLattice incorporates lightweight encryption, node authentication, and self-healing routing mechanisms to ensure secure and reliable communication. The system is designed to be plug-and-play, enabling new nodes to join the mesh seamlessly without manual configuration. A small-scale prototype is implemented to demonstrate feasibility and evaluate performance.

LITERATURE SURVEY

Author(s)	Year	Source	Title	Key Findings / Contribution
J. M. Solé et al.	2025	ACM Transactions on Embedded Computing Systems	Middleware for Distributed Applications in a LoRa Mesh Network	Proposed a middleware layer for LoRa mesh networks, highlighting challenges in latency, scalability, and constrained routing for distributed IoT applications.
R. Berto et al.	2021	Sensors Journal	A LoRa-Based Mesh Network for Peer-to-Peer Long-Range Communication	Demonstrated peer-to-peer communication over LoRa mesh networks, emphasizing long-range communication but limited bandwidth and high latency.
N. L. Giménez et al.	2023	Pervasive and Mobile Computing	Embedded Federated Learning over a LoRa Mesh Network	Explored federated learning over LoRa mesh networks, showing feasibility but identifying performance bottlenecks due to low data rates.
Z. Sun et al.	2022	ACM Computing Surveys	Recent Advances in LoRa: A Comprehensive Survey	Provided a detailed survey on LoRa technologies, highlighting trade-offs between range, data rate, and energy efficiency.
W. Wang et al.	2011	ICECE Conference	Research on Zigbee Wireless Communication Technology	Analyzed Zigbee architecture, noting low power consumption but limitations in data rate and dependence on specialized hardware.
J. Bicket et al.	2005	ACM MobiCom	Architecture and Evaluation of an Unplanned 802.11b Mesh Network	Studied early Wi-Fi mesh networks, proving feasibility of infrastructure-less networking but lacking modern security mechanisms.
Espressif Systems	2020	Technical Documentation	ESP-MESH: Networking Solution Based on ESP32	Introduced ESP-MESH for ESP32 devices, offering reliable mesh networking but restricted to ESP hardware ecosystems.
S. Sicari et al.	2015	Computer Networks Journal	Security, Privacy and Trust in Internet of Things	Identified key security challenges in IoT networks, emphasizing the need for encryption, authentication, and trust management.
E. Fernandes et al.	2016	IEEE Security & Privacy	Security Analysis of Emerging Smart Home Applications	Highlighted vulnerabilities in IoT communication protocols, reinforcing the importance of secure data transmission.
A. Aziz et al.	2024	IEEE ATNT Conference	ESP Mesh Network for Security Application	Demonstrated secure ESP-MESH deployment, but noted limited portability and lack of cross-platform support.

LITERATURE REVIEW

Author(s)	Year	Technology / Approach	Key Contribution	Limitations Identified
Solé *et al.*	2025	LoRa-based Mesh Middleware	Proposed middleware for distributed applications over LoRa mesh networks, improving decentralization and scalability.	Very low data rate and high latency; unsuitable for real-time IoT applications.
Berto *et al.*	2021	LoRa Mesh Networking	Demonstrated peer-to-peer long-range communication using LoRa mesh architecture.	Requires additional LoRa hardware; limited bandwidth and slow transmission speed.
Giménez *et al.*	2023	LoRa Mesh with Federated Learning	Showed feasibility of distributed intelligence over LoRa mesh networks.	Performance bottlenecks due to LoRa's constrained throughput.
Wang *et al.*	2011	Zigbee Mesh Networks	Analyzed Zigbee's low-power mesh capabilities for IoT communication.	Low bandwidth, short range, and dependency on specialized hardware.
Ramya *et al.*	2011	Zigbee Communication Systems	Studied Zigbee protocol efficiency and power usage.	Vendor dependency and limited scalability for heterogeneous IoT systems.
Bicket *et al.*	2005	Wi-Fi (IEEE 802.11) Mesh	Demonstrated feasibility of infrastructure-less Wi-Fi mesh networks.	Lacked modern security mechanisms and IoT-specific optimizations.
Espressif Systems	2020	ESP-MESH (Wi-Fi)	Introduced self-healing Wi-Fi mesh networking for ESP32 devices.	Vendor-specific; limited to ESP hardware and not universally compatible.
Sicari *et al.*	2015	IoT Security Frameworks	Identified key security and trust challenges in decentralized IoT systems.	Existing security solutions are heavy for resource-constrained devices.
Fernandes *et al.*	2016	IoT Application Security	Analyzed vulnerabilities in IoT communication protocols.	Highlighted lack of lightweight built-in security in mesh networks.

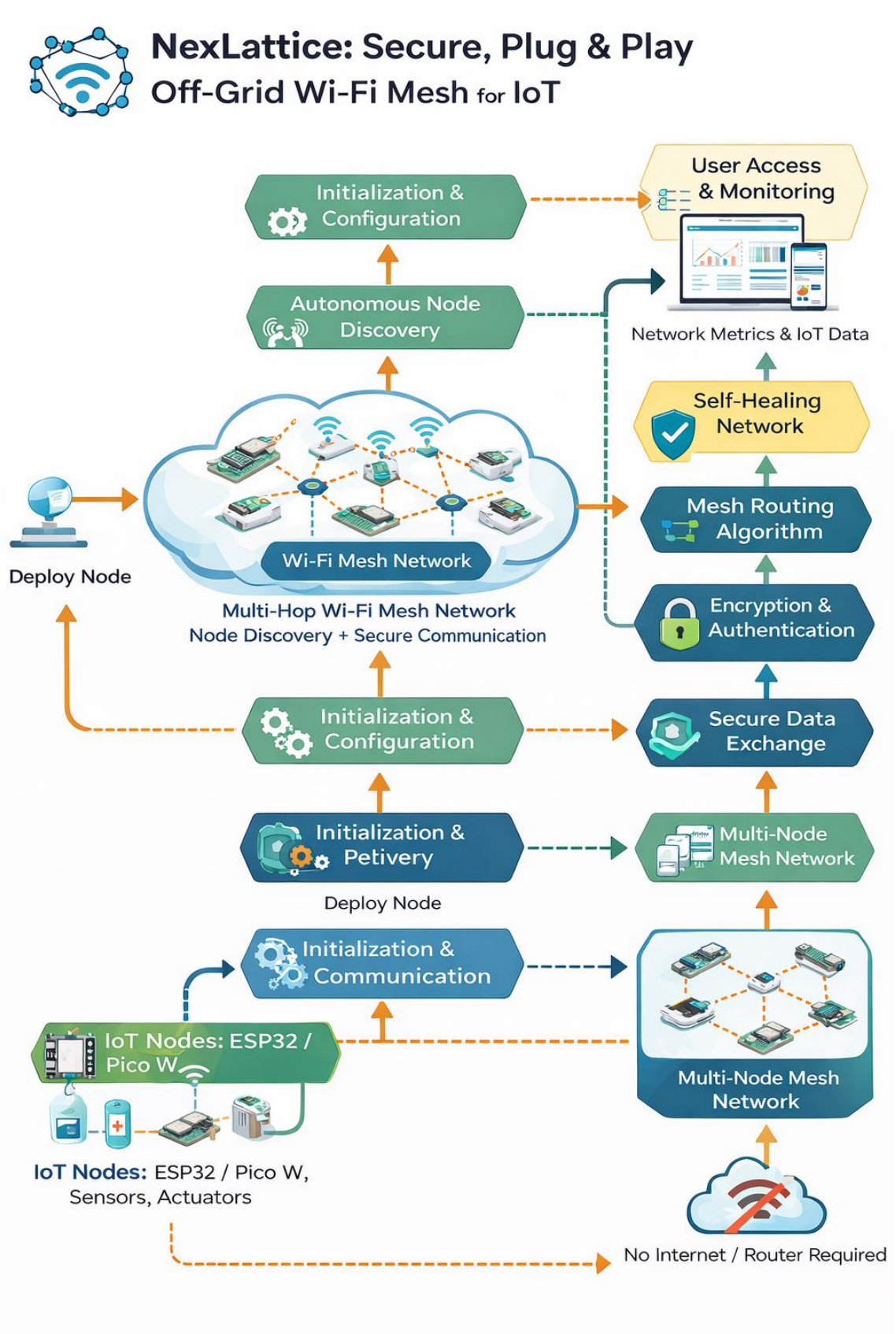
Table 1: Comparative Study of Related Works

LITERATURE REVIEW

Identified Research Gaps	Our Proposed Solution (NexLattice)
Existing mesh protocols such as Zigbee and LoRa require specialized hardware and are not universally supported across IoT devices.	NexLattice uses **standard Wi-Fi hardware**, allowing deployment on common IoT platforms like ESP32 and Pico W without extra modules.
LoRa-based mesh networks suffer from **low data rates and high latency**, making them unsuitable for real-time IoT communication.	NexLattice leverages **Wi-Fi's higher bandwidth** to achieve low-latency, real-time peer-to-peer communication.
Many Wi-Fi mesh solutions rely on **centralized routers or internet connectivity**.	NexLattice operates in a **fully off-grid mode** using SoftAP and local IP networking, eliminating router or internet dependency.
Vendor-specific solutions like ESP-MESH lack **cross-platform compatibility**.	NexLattice is designed as a **device-agnostic software layer**, enabling interoperability across different Wi-Fi-enabled microcontrollers.
Existing mesh networks often involve **complex configuration and deployment procedures**.	NexLattice follows a **plug-and-play approach**, allowing nodes to auto-discover and join the mesh with minimal configuration.
Security mechanisms are either **absent or too heavy** for resource-constrained IoT devices.	NexLattice integrates **lightweight encryption and authentication** suitable for embedded environments.
Limited support for **dynamic node failure handling** in many mesh protocols.	NexLattice supports **self-healing routing**, automatically adapting to node failures or network changes.
Current PGI or IoT studies focus on **evaluation rather than autonomous networking frameworks**.	NexLattice provides a **practical decentralized networking framework**, enabling autonomous IoT communication.

Table 2: Identified Research Gaps and Proposed solutions

FLOW DIAGRAM



IMPLEMENTATION

The implementation phase of the NexLattice project focuses on translating the proposed architectural design into a functional prototype capable of demonstrating secure, off-grid Wi-Fi mesh communication among IoT devices. This phase involves setting up hardware nodes, implementing communication logic, enabling node discovery, ensuring secure data exchange, and validating multi-hop routing within the mesh network.

MicroPython was chosen as the primary programming environment due to its lightweight nature, portability, and support for Wi-Fi enabled microcontrollers such as ESP32 and Raspberry Pi Pico W.

5.1 Hardware Setup

The implementation uses **five ESP32 development boards** as IoT nodes to demonstrate the mesh network. Each node is equipped with built-in Wi-Fi capability and sufficient computational resources to handle networking, encryption, and routing tasks.

One node is configured to operate in **Software Access Point (SoftAP) mode**, creating a local wireless network, while the remaining nodes connect to this network as stations. This setup enables completely **off-grid communication** without reliance on routers or internet connectivity.

5.2 Network Initialization

Upon powering on, each node initializes its Wi-Fi interface and loads the NexLattice module. The SoftAP node advertises a local Wi-Fi network, allowing nearby nodes to automatically join.

Each node is assigned a **unique Node ID**, which is used for identification and routing within the mesh. The initialization process ensures that all nodes operate on the same local IPv4 network and are ready for discovery and communication.

5.3 Node Discovery Mechanism

NexLattice implements an **autonomous node discovery mechanism** using periodic UDP broadcast messages. Each node broadcasts a discovery packet containing its Node ID and status information.

Neighboring nodes receive these packets and update their **neighbor table**, which stores:

- Node ID
- IP address
- Last-seen timestamp

This dynamic discovery allows nodes to detect new peers, handle node departures, and maintain an updated view of the mesh topology.

5.4 Secure Communication

Security is integrated at the protocol level. All data packets are encrypted using **symmetric key encryption** before transmission. A shared secret key is pre-configured on authorized nodes to prevent unauthorized access.

Each packet includes:

- Source Node ID
- Destination Node ID
- Encrypted payload
- Message ID and Time-to-Live (TTL)

Replay attacks are prevented by tracking recently received message IDs. Only authenticated nodes are allowed to participate in the mesh network.

5.5 Mesh Routing and Data Forwarding

NexLattice employs a **lightweight hop-by-hop routing mechanism**. When a node sends a message:

- If the destination node is a direct neighbor, the packet is delivered immediately.
- Otherwise, the packet is forwarded to the next available neighbor.

TTL values ensure that packets do not circulate indefinitely, preventing routing loops. Nodes do not maintain complex routing tables, which keeps memory usage low and improves performance on resource-constrained devices.

5.6 Self-Healing Capability

The mesh network exhibits **self-healing behavior**. If a node goes offline or becomes unreachable, neighboring nodes automatically remove it from their neighbor tables.

Subsequent packets are rerouted through alternative available nodes without manual intervention. This ensures network reliability even in dynamic or unstable environments.

5.7 Monitoring and Visualization

A gateway node optionally forwards network statistics to a lightweight dashboard for monitoring purposes. The dashboard displays:

- Active nodes
- Neighbor relationships
- Message flow and latency

This visualization aids in debugging and demonstrates real-time mesh behavior during the prototype demonstration.

5.8 Result Analysis

The implemented prototype successfully demonstrated:

- Plug-and-play node integration
- Secure off-grid communication
- Multi-hop data transmission
- Dynamic node discovery and self-healing

The system performed reliably in a five-node setup, validating the feasibility of NexLattice as a universal Wi-Fi mesh networking layer for IoT devices.

TECHNOLOGIES USED

Technology	Purpose
MicroPython	Embedded programming for IoT nodes
ESP32	Wi-Fi enabled microcontroller for mesh nodes
Wi-Fi (IEEE 802.11)	Wireless communication medium
UDP Sockets	Lightweight, low-latency data transmission
AES Encryption	Secure data encryption
HMAC / Hashing	Message integrity and authentication
SoftAP (Wi-Fi Access Point Mode)	Off-grid local network creation
Python	Backend and dashboard development
Flask	Web framework for dashboard
WebSockets	Real-time network monitoring
HTML / CSS / JavaScript	Dashboard user interface
VS Code / Cursor AI	Development environment
Serial Monitor	Debugging and logging

EXPERIMENTAL RESULTS

The experimental evaluation of **NexLattice** was conducted using a small-scale prototype consisting of **five Wi-Fi enabled IoT nodes (ESP32)** operating in an off-grid environment. The experiments were designed to validate secure peer-to-peer communication, routing efficiency, network stability, and plug-and-play behavior without reliance on external routers or internet connectivity.

The results demonstrate that NexLattice successfully forms a **self-organizing, secure Wi-Fi mesh network** where nodes can dynamically discover peers, authenticate each other, and exchange encrypted data packets. Multi-hop communication was achieved with low latency, and the network continued to operate reliably even when intermediate nodes were temporarily disconnected.

7.1 Experimental Setup

The experimental setup included the following components:
I. Five ESP32 nodes running MicroPython
II. NexLattice communication library
III. Local SoftAP-based Wi-Fi mesh environment
IV. Encrypted UDP-based message exchange
V. Monitoring through serial logs and dashboard visualization

Each node was configured with a unique identifier and shared authentication key to validate secure entry into the mesh network.

7.2 Evaluation Metrics

The performance of NexLattice was evaluated using the following metrics:

- **Packet Delivery Ratio (PDR)** – Measures the percentage of successfully delivered packets
- **Latency** – Measures end-to-end delay in multi-hop communication
- **Routing Stability** – Evaluates network behavior during node failure or removal
- **Discovery Time** – Measures time taken for a new node to join the mesh
- **Security Validation** – Confirms rejection of unauthorized nodes

7.3 Experimental Observations

The experimental results indicate that:

- NexLattice achieved a **high packet delivery ratio** under normal operating conditions.

- **Multi-hop routing** worked effectively with minimal additional latency.
- The network exhibited **self-healing behavior**, automatically rerouting data when a node was disconnected.
- New nodes were able to **join the network seamlessly** within a short discovery window after authentication.
- Unauthorized nodes without valid credentials were **successfully blocked**, validating the security mechanism.

Overall, NexLattice proved to be **reliable, secure, and efficient** for small to medium-scale IoT deployments.

7.4 Result Summary

The experimental evaluation confirms that NexLattice can serve as a **practical and scalable off-grid Wi-Fi mesh solution for IoT devices**. The combination of lightweight routing, encryption, and plug-and-play deployment makes it suitable for applications such as smart environments, disaster recovery networks, and decentralized IoT systems.

CONCLUSION

This project successfully presents **NexLattice**, a secure, plug-and-play, off-grid Wi-Fi mesh networking framework designed for IoT devices. The study demonstrates that reliable, decentralized, and encrypted peer-to-peer communication can be achieved using standard Wi-Fi capabilities without relying on internet connectivity, centralized routers, or vendor-specific protocols.

Through theoretical analysis and a prototype-level demonstration, NexLattice proves the feasibility of forming a **self-organizing and self-healing mesh network** using Wi-Fi enabled microcontrollers such as ESP32 and Pico W. The implemented mechanisms for node discovery, authentication, secure data exchange, and multi-hop routing ensure robustness, low latency, and resistance to single-point failures.

The project highlights the advantages of using a **universal software-based approach** over existing mesh technologies like Zigbee, LoRa, and ESP-MESH, which are often hardware-dependent or limited in interoperability. NexLattice stands out by offering device independence, ease of deployment, and enhanced security while remaining lightweight and suitable for embedded environments.

In conclusion, NexLattice provides a strong foundation for **future decentralized IoT communication systems**, particularly in scenarios such as smart cities, disaster recovery, remote monitoring, and off-grid applications. With further enhancements such as optimized routing algorithms, dynamic key management, and large-scale deployment testing, NexLattice has the potential to evolve into a scalable and widely adoptable IoT mesh networking solution.

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.