AUTONOMOUS DATA FERRYING FROM A SELF-ORGANIZING/HEALING WSN IN DISCONNECTED ZONES

25-26J-010

Project Proposal Report

Bandara K.B.O.V.

B.Sc. (Hons) Degree in Information Technology Specializing in Computer Systems & Network Engineering

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

August 2025

AUTONOMOUS CLUSTER FORMATION AND CLUSTER HEAD SELECTION

25-26J-010

Project Proposal Report

B.Sc. (Hons) Degree in Information Technology Specializing in Computer Systems & Network Engineering

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

August 2025

DECLARATION

I declare that this is my own work, and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student ID	Signature
Bandara K.B.O.V.	IT22564986	

The above candidate is carrying out research for the undergraduate Dissertation under my supervision.

Signature of the supervisor:  Date: 28/08/2025

Signature of the co-supervisor:  Date: 28/08/2025

Abstract

Wireless Sensor Networks (WSNs) in disconnected or infrastructure less environments, such as disaster zones, remote fields, offshore platforms, and defence operations, face critical obstacles, including energy constraints, communication unreliability, and susceptibility to compromised nodes. This research introduces a novel, autonomous clustering framework for ESP32 based WSNs, utilising BLE 5.0 Coded PHY for long range, low-power control signalling and ESP Now for rapid intra-cluster data exchange. Each node calculates a dynamic Cluster Head (CH) election score by integrating residual battery level, deep sleep persistent uptime, lightweight trust indicators (including handshake reliability and packet integrity), and link quality. The election process employs HMAC-SHA256 secured BLE extended advertisements to ensure integrity and prevent spoofing attacks. A distinctive feature is the utilisation of RTC memory based uptime retention to guarantee fair, energy balanced CH rotation across multiple cycles. The network supports UAV assisted data ferrying, enabling delay tolerant data transfer from sparsely deployed CHs to remote centres. Furthermore, the split control and data plane, employing BLE for authenticated signalling and ESP-Now for payload exchange, optimizes power usage while maintaining responsiveness. This work addresses gaps in existing clustering models, such as LEACH and HEED, which lack trust, security, and autonomy in disconnected scenarios. Its integrated approach combining energy awareness, security, trust, long-range BLE communications, and UAV-assisted ferrying advances the field by offering a resilient, efficient framework suitable for real world deployments, with potential applications in emergency response systems, remote environmental monitoring, and tactical or military sensor networks where traditional infrastructure is unavailable or unreliable.

Keywords: Autonomous Wireless Sensor Networks; BLE 5.0 Coded PHY; Cluster Head Election; Trust Aware Clustering; UAV Assisted Data Ferrying; Energy Efficient Networking; HMAC-SHA256 Security.

Table of Contents

List Of Figures

List of Tables

1 Introduction

1.1 Background and Literature Survey

Wireless Sensor Networks in Disconnected Environments

Wireless Sensor Networks (WSNs) are critical in scenarios where conventional infrastructure is unavailable or impractical such as disconnected enviornmental monitoring areas, disaster stricken areas, rural regions, or tactical defense zones. These networks rely on clusters to reduce energy consumption and extend operational lifespan through local aggregation and reduced communication overhead. Early influential protocols like LEACH enhance energy efficiency through randomized Cluster Head (CH) rotations, yet neglect node reliability and trustworthiness [1]. HEED improves upon this by selecting CHs based on residual energy and proximity, but still lacks defense against compromised nodes and persistent CH rotation fairness [2].

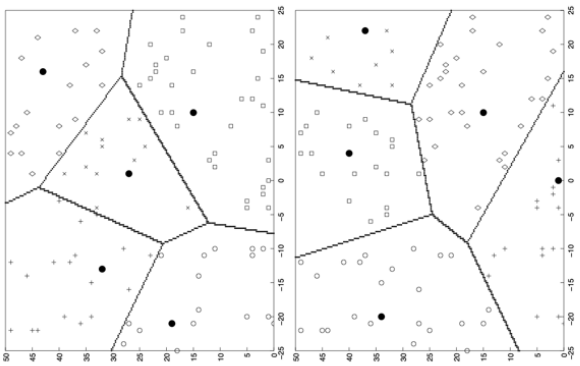

Figure 1.1: Dynamic clusters

Source: Figure 7. Dynamic clusters: W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2005.

I. Initialize

1. $S_{nbr} \leftarrow \{v: v \text{ lies within my cluster range}\}$
2. *Compute and broadcast cost to* $\in S_{nbr}$
3. $CH_{prob} \leftarrow max(C_{prob} \times \frac{E_{residual}}{E_{max}}, p_{min})$
4. *is_final_CH* $\leftarrow$ *FALSE*

III. Finalize

1. *If (is_final_CH = FALSE)*
2. *If* $((S_{CH} \leftarrow \{v: v \text{ is a final cluster head}\}) \neq \phi)$
3. *my_cluster_head* $\leftarrow$ *least_cost*(S_{CH})
4. *join_cluster(cluster_head_ID, NodeID)*
5. *Else Cluster_head_msg(NodeID, final_CH, cost)*
6. *Else Cluster_head_msg(NodeID, final_CH, cost)*

II. Main Processing

Repeat

1. *If* $((S_{CH} \leftarrow \{v: v \text{ is a cluster head}\}) \neq \phi)$
2. *my_cluster_head* $\leftarrow$ *least_cost*(S_{CH})
3. *If (my_cluster_head = NodeID)*
4. *If* $(CH_{prob} = 1)$
5. *Cluster_head_msg(NodeID,final_CH,cost)*
6. *is_final_CH* $\leftarrow$ *TRUE*
7. *Else*
8. *Cluster_head_msg(NodeID, tentative_CH,cost)*
9. *ElseIf* $(CH_{prob} = 1)$
10. *Cluster_head_msg(NodeID,final_CH,cost)*
11. *is_final_CH* $\leftarrow$ *TRUE*
12. *ElseIf Random(0,1)* $\leq CH_{prob}$
13. *Cluster_head_msg(NodeID,tentative_CH,cost)*
14. $CH_{previous} \leftarrow CH_{prob}$
15. $CH_{prob} \leftarrow min(CH_{prob} \times 2, 1)$

Until $CH_{previous} = 1$

Figure 1.2: HEED Protocol pseudocode

Source: Fig.2:O.: O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Trans. Mob. Comput., vol. 3, no. 4, pp. 366–379, 2004.

Trust-Aware Clustering Mechanisms

To enhance security, recent works integrate trust models into CH election. For example, Researchers proposed a fuzzy logic-based clustering protocol augmented with outlier detection to exclude compromised nodes [3]. Their subsequent study leverages evolutionary game theory to dynamically adjust CH selection using trust and energy metrics [4]. These methods improve resilience but often carry high computational overhead, limiting their deployment in resource-constrained platforms like ESP32.

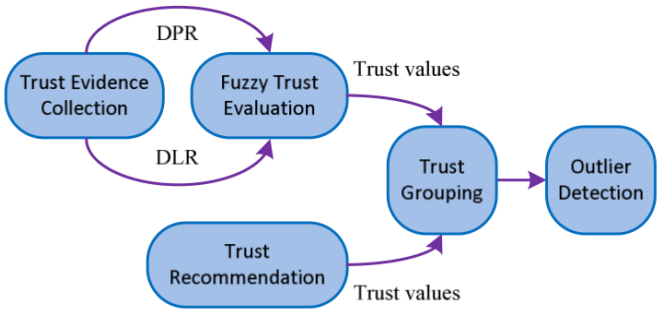

Figure 1.3: Trust Based Security Model in [4]

Source: Fig.3: L. Yang, Y. Lu, S. X. Yang, Y. Zhong, T. Guo, and Z. Liang, "An evolutionary game-based secure clustering protocol with fuzzy trust evaluation and outlier detection for wireless sensor networks," IEEE Sens. J., *vol. 21, no. 12, pp. 13935–13947, 2021.*

UAV Assisted Data Collection in WSNs

Unmanned aerial vehicles (UAVs) increasingly complement wireless sensor networks (WSNs) by serving as mobile data transporters. Reviews of UAV enabled WSNs highlight the importance of synchronising clustering and UAV scheduling for scalable, remote data acquisition [5].

BLE 5.0 Coded PHY and Control Communication

Bluetooth Low Energy (BLE) 5.0 introduces Coded PHY modes (S2, S8) using Forward Error Correction to dramatically extend communication range with moderate energy trade offs. Spork *et al.* experimentally compare BLE 5 PHY modes, revealing that Coded PHY significantly enhances packet reception rates under interference while modestly increasing power draw [6]. BLE's extended advertising provides an efficient, low overhead channel for CH election signaling, supporting infrastructure-free deployments.

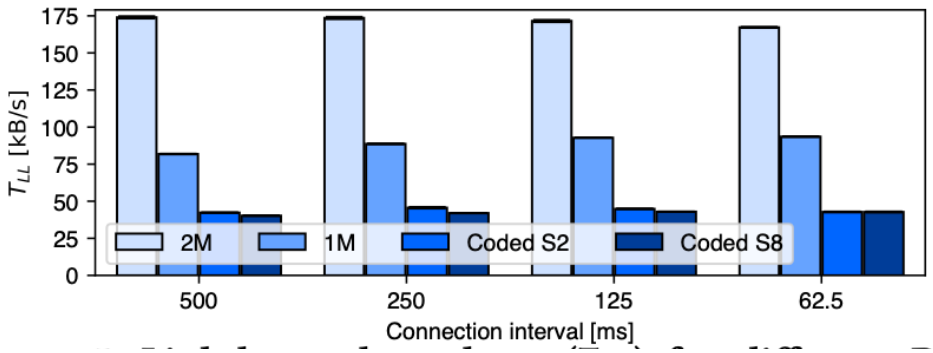

Figure 1.4: Throughput for different PHY modes

Source: Fig.5: M. Spörk, C. A. Boano, and K. Römer, "Performance and Trade-offs of the new PHY Modes of BLE 5," in Proceedings of the ACM MobiHoc Workshop on Pervasive Systems in the IoT Era, 2019, pp. 7–12.

1.2 Research Gap

Despite significant advances in wireless sensor network clustering, trust integration, and UAV assisted data collection, several notable gaps persist that hinder the development of fully autonomous, resilient networks in disconnected environments.

Lack of Integrated Trust, Uptime, and Energy-Aware Clustering

Several clustering strategies have enhanced energy efficiency by considering residual battery levels or network topology (e.g, LEACH [1], HEED [2]). However, these protocols frequently overlook node trustworthiness and operational history. Recent studies incorporate trust evaluation mechanisms utilising fuzzy logic or evolutionary game models to prevent compromised nodes from assuming cluster leadership [3], [4]. While such approaches improve security, they are typically computationally demanding and have not been adapted to the constrained resources of low cost MCUs such as ESP32-S3. Additionally, none of the extant protocols systematically incorporate node uptime or operational reliability into cluster head selection, a crucial factor in optimising energy consumption and guaranteeing fairness in extended deployments.

Missing Secure Long Range Signaling Mechanisms

The integration of BLE 5.0 Coded PHY offers promising improvements in control plane communication combining long-range reach and low power consumption. Spörk *et al.* demonstrate striking improvements in packet reception across challenging environments using BLE Coded PHY [6]. Yet, few clustering protocols exploit BLE 5.0 extended advertising for secure, authenticated cluster head election in infrastructure-less networks.

Incomplete Integration of UAV Data Ferrying with Trust and Energy Metrics

UAVs are commonly used to collect data in remote or disconnected WSN scenarios; several comprehensive surveys and studies explains their significance [7], [8], [9]. Some approaches focus on UAV trajectory planning and synchronizing data collection with network topology. However, these models rarely incorporate dynamic trust or energy based cluster head election strategies. As a result, data ferrying may rely on unstable or untrusted network points.

Absence of Persistent, Self-Healing Clustering Architectures

While algorithms such as those proposed by Lewandowski & Płaczek include mechanisms to extend the lifetime of the last surviving sensor through optimized CH rotation [10], they do not incorporate trust, secure signaling, or UAV integration. Modern clustering approaches, such as reinforcement learning models for emission scheduling or self-healing clustering mechanisms, offer resilience but have been studied separately, not as part of a unified framework suitable for resource limited platforms.

1.3 Research Problem

Wireless Sensor Networks (WSNs) are pivotal in facilitating data acquisition in environments devoid of infrastructure, such as disaster zones, remote terrains, and tactical operations. Clustering techniques like LEACH and HEED offer energy efficient management through rotational Cluster Heads (CHs) [1],[2]. However, these approaches overlook crucial aspects such as node trustworthiness, persistent uptime, authenticated signalling, and adaptability in delay-tolerant contexts.

Recent trust-aware clustering models employ fuzzy logic and game theory to secure CH selection [3], [4]. Nevertheless, they impose substantial computational burdens unsuitable for low cost microcontroller platforms like the ESP32. Furthermore, BLE 5.0 Coded PHY (S2, S8) provides long range, low power signalling, but its authenticated usage for CH announcements remains underutilised in clustering literature [6]. The potential of ESP Now for efficient data broadcasting in conjunction with BLE-based control has been demonstrated in official documentation [11], yet formal integrated frameworks leveraging both remain unachieved. While UAV-assisted data ferrying enhances communication in disconnected settings [5], [8], models rarely incorporate trust and uptime into CH selection algorithms, thereby limiting their robustness and deployment viability.

Research Problem Statement

How can we design and implement a lightweight, secure, and adaptive cluster head selection framework on ESP32 platforms that integrates battery level, persistent uptime, trust metrics, and link quality into a unified scoring mechanism; employs authenticated BLE 5.0 extended advertising for control signaling; supports efficient data exchange via ESP-Now; and seamlessly integrates UAV-assisted data ferrying for delay-tolerant deployments.

To address this challenge, we propose the following:

- A multi-parameter CH scoring algorithm that integrates battery level, persistent uptime (via RTC memory), lightweight trust indicators, and link quality, optimised for the hardware constraints of ESP32-S3 devices.
- Secure CH announcements via HMAC-SHA256-protected BLE 5.0 extended advertising.
- Persistent uptime tracking across sleep cycles to ensure equitable CH rotation and balanced energy consumption.
- A dual-plane communication architecture: BLE for secure control signalling and ESP-Now for reliable data transfer.
- Integration of a UAV-assisted ferrying protocol capable of retrieving data from CHs in delay-tolerant, disconnected scenarios.

Expected Outcomes:

- A trustworthy, energy-aware clustering mechanism deployable on ESP32-S3 devices.
- Secure, long-range, authenticated cluster head signalling using BLE 5.0.
- Enhanced fairness in CH rotation through uptime persistence, resulting in improved network longevity.
- Improved energy efficiency by segregating control and payload channels.
- Robust, delay-tolerant data delivery through UAV enabled retrieval in disconnected environments.

2 Objectives

2.1 Main Objective

To design and develop a secure, energy efficient, and trust aware cluster head (CH) selection framework for Wireless Sensor Networks (WSNs) operating in infrastructure less environments. The framework should:

- Leverage ESP32-S3 microcontrollers utilizing BLE 5.0 Coded PHY for long range, low power control signaling.
- Integrate multi parameter CH scoring based on residual battery level, persistent uptime (via RTC memory), trust metrics (e.g., handshake success, packet integrity, reputation), and link quality.
- Ensure secure CH announcements using HMAC-SHA256-protected BLE extended advertising.
- Employ a dual-plane communication architecture combining BLE for control messaging and ESP-Now for efficient intra-cluster data transmission.
- Support UAV-assisted data ferrying to enable reliable data retrieval in delay-tolerant, disconnected zones.

2.2 Specific Objectives

Develop a Lightweight Multi-Parameter Scoring Algorithm

Design and implement a scoring mechanism that dynamically weights battery, uptime, trust, and link quality, optimized for real-time execution on ESP32-S3 MCUs.

Enable Persistent Uptime Tracking for Fair CH Rotation

Utilize RTC memory to store and maintain uptime across sleep cycles, preventing role monopolization and ensuring even energy consumption across nodes.

Secure CH Signaling via BLE 5.0 with HMAC Authentication

Implement BLE extended advertising to broadcast CH status, securing messages via HMAC-SHA256 to ward off spoofing and replay attacks.

Implement Dual-Plane Communication Architecture

Design a communication protocol using BLE for authenticated control messages and ESP-Now for high-throughput data transfer, optimizing energy usage without sacrificing responsiveness.

Integrate UAV-Based Data Ferrying for Delay-Tolerant Operation

Develop a UAV compatible protocol and scanning mechanism so UAVs can efficiently discover CHs, connect via BLE/ESP-Now, and retrieve stored data securely.

Validate Framework through Simulation and Real-World Testing

Conduct NS-3 simulations and hardware experiments to assess performance metrics such as network lifetime, trust reliability, data delivery rate, and energy efficiency compared to baseline protocols like LEACH and HEED [1], [2].

3 Methodology

The proposed system centers on a hybrid, autonomous Wireless Sensor Network (WSN) built on micro controller (ESP32) nodes, optimized for disconnected, infrastructure less areas to monitor the environments. It integrates multi parameter cluster head (CH) election, secure BLE 5.0 signaling, ESP Now data communication, and UAV-assisted data ferrying.

3.1 System Design

In the proposed system, sensor nodes initiate cluster formation by periodically broadcasting BLE 5.0 Coded PHY extended advertisements that convey fundamental status information, including residual energy, uptime, and link quality. Each node constructs a neighbour table and computes a Cluster Head (CH) score based on a weighted values of battery level, persistent uptime, trust score, and link quality. Once scores are determined, nodes with enhanced suitability broadcast authenticated candidacy advertisements safeguarded with HMAC, ensuring resilience against spoofing. Neighbouring nodes verify these advertisements and elect the node with the highest validated score as the CH. Subsequently, Main Sets (MSs) formally join the CH and transmit sensor data within their designated time slots utilising ESP-NOW, which avoids collisions and idle listening while optimising energy efficiency. The CH aggregates and stores received data persistently, ensuring continuity even in the event of re elections or failures. When a UAV approaches, the CH detects its presence through BLE beacon exchanges, establishing a secure control handshake. Once proximity is verified, the CH transitions to a high throughput channel ESP-NOW to transfer the aggregated dataset to the UAV. The CH clears its buffer solely after receiving an acknowledgment of successful delivery, ensuring reliability and preventing data loss. This comprehensive flow, spanning from clusterization through secure CH election to UAV assisted data retrieval, establishes a self organising and self-healing network engineered for robust, energy-conscious operation in disconnected environments.

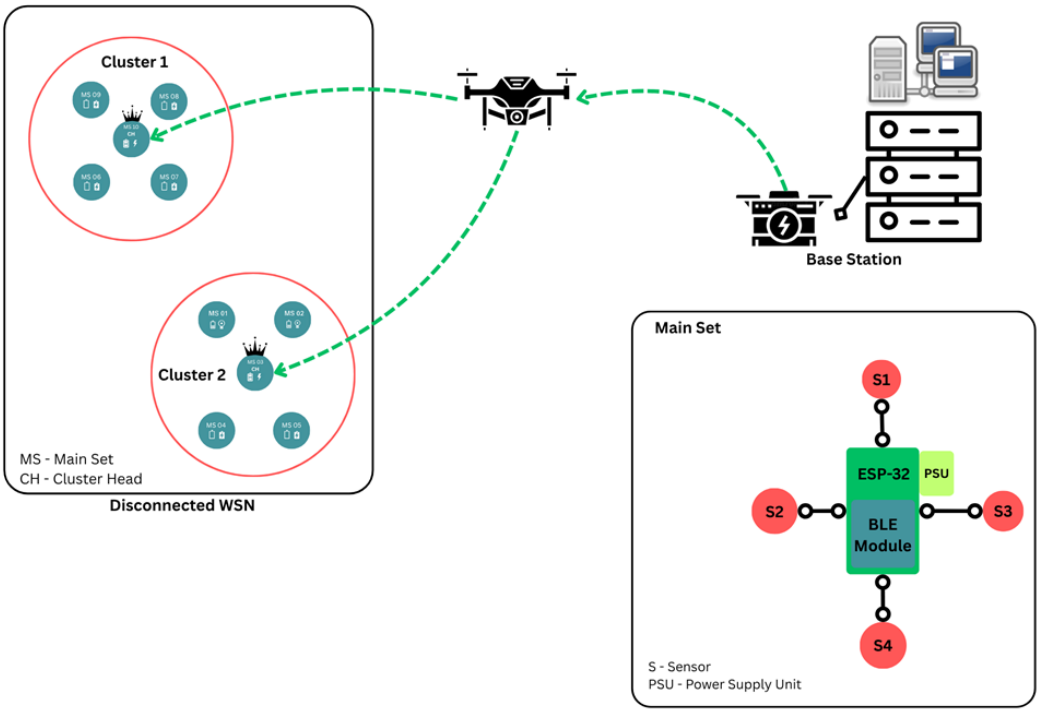

Figure 3.1: Proposed UAV-assisted cluster-based WSN architecture

3.2 Algorithm Design and Framework

Multi metric CH election Algorithm

Each node/ Main Set (MS) computes a composite CH suitability score.

$S = Wb * B + Wu * U + Wt * T + Wl * L$

Where:

- B = Battery level (normalized via ADC)
- U = Uptime (persisted in RTC memory across deep sleep)
- T = Trust score (handshake success, packet integrity)
- L = Link quality (e.g., RSSI average)

Weights ($Wb + Wu + Wt + Wl = 1$) are adaptive and tuned per network context.

Secure Signaling and Candidate Broadcast

Candidate CHs broadcast their score securely using BLE 5.0 extended advertisements (Coded PHY), embedding an HMAC-SHA256 signature to prevent spoofing.

Nodes listen for neighbor announcements, verify HMAC, compare normalized scores, and select CH:

- Highest S value wins.
- Tie-break: Consider Lowest MAC Value.

This decentralized election draws from principles in algorithms like LEACH [1] and HEED [2] but incorporates added trust and persistence mechanisms for resilience.

Simulation and Parameter Tuning

We will simulate the CH selection algorithm in NS-3 or equivalent, modeling ESP32 behavior (BLE 5 Coded PHY, intermittent connectivity, ESP-NOW). Metrics to be captured:

- Network lifetime (first node death, half-node death, last node death)
- Energy balance and fairness across nodes
- Trust resilience: frequency of compromised nodes being elected CHs
- Overhead of secure advertisements and elections

Simulations assess different weighting schemes under varied density, mobility, and threat scenarios.

Implementation and Validation

The prototype will be developed on ESP32-S3 boards, where the firmware will include dedicated RTOS tasks responsible for periodic score computation, neighbor scanning, BLE announcements, and trust metric updates. To ensure fairness in rotation, uptime values will be stored in RTC memory, enabling persistence across deep sleep cycles. Security will be maintained through HMAC generation and verification implemented using the ESP-IDF cryptographic libraries, while cluster head candidacy will be announced via compact scoring advertisements broadcast over BLE extended advertising. For validation, an experimental setup of approximately ten ESP32 nodes will be deployed to assess multiple performance aspects. This will involve measuring CH rotation fairness enabled by uptime persistence, evaluating the robustness of CH candidacy against spoofing attacks, analyzing energy consumption trends and network longevity, and testing fault recovery behavior when a CH is deliberately removed or fails during operation. This setup will provide comprehensive insights into the reliability, security, and efficiency of the proposed clusterization and CH selection framework in real-world conditions.

Cluster formation and CH election flow

Neighbor discovery: Nodes (MSs) advertise and scan on the BLE 5 Coded PHY. Each node maintains a neighbor table, where each entry is keyed by NodeID and contains rolling RSSI, last-seen, peer's advertised score, and trust values.

Score computation: Every election epoch, nodes recompute S using the current B, U, T, and L values.

Candidacy and verification: Nodes broadcast candidacy advertisements (extended ADV with HMAC). Peers verify the HMAC. invalid frames will be discarded.

Local decision rule: A node elects the neighbor (or itself) with the maximum verified S in its neighborhood as the CH. Ties are broken by considering lower MAC.

Join and schedule: MSs register with the CH, receive a lightweight schedule (ESP-NOW slots or simple TDMA rules), and an encryption seed if used.

Self-healing: If CH beacons are missed for k intervals or trust drops below a threshold, members reenter the election.

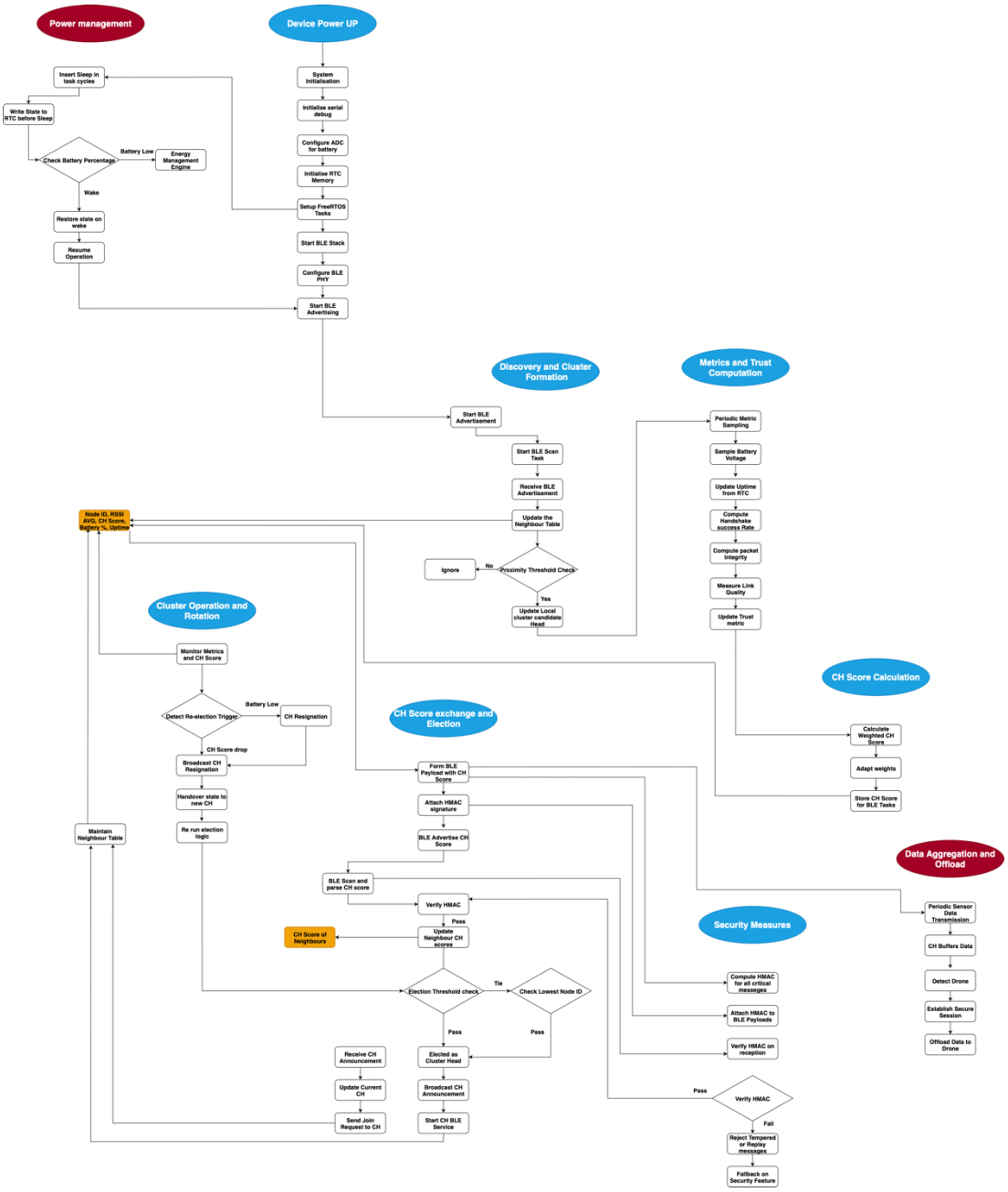

Figure 3.2: CH Election and Rotation process

3.3 Required Materials

To successfully design and validate the Clusterization and CH selection mechanism, both hardware and software resources are required.

Hardware:

- ESP32-S3-DevKitC-1 boards (10–12 units) equipped with BLE 5.0 and ESP-NOW support.
- External 2.4 GHz antennas (ACS4057 or equivalent) to enhance range and ensure stable communication.
- Power sources: 3.7 V Li-ion batteries with charging modules for long-term deployments.
- Environmental sensors (temperature, humidity, or application-specific) for realistic test data.
- UAV platform or Raspberry Pi-based receiver capable of BLE scanning and ESP-NOW/Wi-Fi data collection.

Software and Tools:

- ESP-IDF SDK with FreeRTOS for firmware development and task scheduling.
- MbedTLS libraries for HMAC-SHA256 authentication.
- Arduino IDE or PlatformIO for iterative prototyping.
- Draw.io for system diagrams and workflow illustrations.
- GitHub for version control and collaborative development.

3.4 Anticipated Outcomes

The proposed Clusterization and CH selection methodology is expected to achieve the following:

- **Energy Efficiency**: Fair distribution of CH roles through uptime tracking and battery-aware scoring, leading to extended network lifetime compared to LEACH and HEED.
- **Security and Trust**: Reduced vulnerability to malicious or compromised nodes due to the integration of trust metrics and HMAC-based authentication.
- **Resilience and Self-Healing**: Robust fault recovery with rapid re-election when CHs fail or leave the network, maintaining data flow without significant disruption.
- **Reliability of Data Delivery**: Persistent local storage ensures that no sensor data is lost during CH rotation, while UAV-based collection guarantees eventual delivery in disconnected environments.
- **Scalability**: The algorithm is expected to remain effective as the number of nodes increases, with negligible election overhead due to lightweight BLE advertisements.

4 Project Requirements

4.1 Functional requirements

Cluster Formation and Maintenance

- Sensor nodes must self-organize into clusters using BLE 5.0 advertisements.
- Neighbor discovery and maintenance of a local neighbor table should be continuous.

Cluster Head (CH) Election

- Each node must compute a composite CH score using battery, uptime, trust, and link quality.
- Election results must be securely broadcast using HMAC-authenticated BLE extended advertisements.
- Tie-breaking mechanisms must exist (based on node ID/MAC).

Trust Evaluation

- Nodes must evaluate neighbors based on handshake success rate, packet delivery ratio, and peer reputation.
- Malicious or low trust nodes must be excluded from CH candidacy.

Persistent Uptime Tracking

- Each node should store uptime in RTC memory across deep sleep cycles.
- Uptime must contribute to fair CH rotation and prevent role monopolization.

CH – to – CH and Re Election Handling

- If a CH fails, remaining nodes must trigger reelection within a bounded time.
- The outgoing CH, if still alive, must forward buffered data to the new CH.

4.2 Non-Functional Requirements

These define the quality attributes and operational constraints:

Energy Efficiency

- Nodes must minimize idle listening via slot scheduling and duty cycling.
- Election and signaling overhead must consume <10% of node energy per cycle.

Scalability

- The framework must support deployment without excessive control overhead.

Security

- All CH announcements should be HMAC-authenticated to prevent spoofing.
- Trust mechanisms must reduce false CH selections compared to non-trust models.

Reliability & Resilience

- Network must recover from CH failure within two election cycles.
- Data delivery success rate to UAV should be under normal conditions.

Latency & Throughput

- Intra-cluster data transmission must complete within allocated slots without collisions.
- CH-to-UAV handover must succeed within defined intervals after UAV arrival.

Storage & Persistence

- CHs must store data persistently until UAV acknowledgment is received.
- Data loss tolerance should be minimal even under node or CH failure scenarios.

Maintainability & Extensibility

- Firmware must be modular, separating radio tasks, scoring, trust, and data handling.
- System must allow weight reconfiguration (Wb, Wu, Wt, Wl) without code rewrites.

Usability

- Logs, telemetry, and debugging interfaces must be accessible via UART/serial.
- Neighbor tables and scores should be exportable for analysis during testing.

4.3 System Requirements

- Autonomous Cluster Management and Fair Cluster-Head Rotation

The distributed clustering system will implement autonomous network organization capabilities, enabling individual sensor nodes to self-discover neighboring nodes through Bluetooth Low Energy (BLE) 5.0 advertisement mechanisms. Upon neighbor discovery, nodes will participate in a distributed cluster formation process and execute a weighted scoring algorithm for cluster-head election. The scoring function will

incorporate multiple quality metrics, including residual battery capacity (B), operational uptime (U), trust coefficient (T), and link quality indicator (L).

To ensure equitable resource utilization and prevent cluster-head monopolization, the system will implement a fair rotation mechanism based on persistent uptime tracking. This mechanism will distribute the computational and communication overhead of cluster-head responsibilities across all eligible nodes in the network, thereby promoting balanced energy consumption and extending the overall network lifetime.

- Secure Control Signaling and Robust Network Operations

The clustering protocol shall implement comprehensive security measures to safeguard against malicious attacks and preserve network integrity. All cluster-head candidacy announcements and control messages shall be authenticated through Hash-based Message Authentication Code (HMAC) cryptographic signatures. The system shall incorporate replay attack prevention mechanisms and maintain the capability to detect and reject spoofed or replayed advertisement packets with high reliability.

The network shall exhibit robust self-healing capabilities through automatic detection of cluster-head failures, trust degradation, or link quality deterioration. Upon detection of such conditions, the system shall initiate re-election procedures within predefined time frames, ensuring the completion of recovery operations within two election cycles to preserve network connectivity and data flow continuity.

- Energy Aware, Low Overhead Control Plane Design

The clustering system will optimize energy consumption by employing lightweight control plane operations. The combined overhead of neighbor discovery procedures, scoring computations, and election processes will not exceed node’s energy budget per operational cycle. This objective will be achieved through the implementation of duty cycling mechanisms for radio operations and the utilization of compact BLE extended advertisement formats to minimize transmission energy costs.

The system architecture will prioritize computational efficiency in scoring algorithms, thereby minimizing the frequency of control message exchanges while ensuring adequate network responsiveness and adaptation capabilities.

- Reliable Intra Cluster Data Handling and Persistence

Cluster member nodes shall transmit sensor readings and telemetry data to their designated cluster head via reliable communication protocols, particularly employing ESP-NOW for low-latency, high-throughput data transfer. The cluster head shall implement data aggregation functions and provide persistent storage capabilities using flash memory to guarantee data durability across system events.

The data management system shall preserve data integrity and continuity during cluster head transitions and re-election events. Committed data records shall not be lost during leadership changes, ensuring complete data preservation throughout the network's operational lifespan.

4.4 Test Cases

- Election Convergence and Security Validation

This test assesses the distributed election algorithm's ability to converge to a single cluster head and verifies the security framework against malicious activities. A network of six to ten heterogeneous nodes is deployed with variations in battery, uptime, trust, and link quality. HMAC authentication is enabled for all control messages. The test commences by initiating the election process across all nodes. Subsequently, crafted spoofed and replayed cluster-head advertisements are injected into the network. The system is monitored to ensure that only one cluster head is elected, all nodes agree on the result, invalid advertisements are rejected with a respectable accuracy, and the election process concludes within predefined election windows.

- Fair Rotation and Energy Balance Assessment

This test focuses on validating the fairness of CH rotation and energy balance across the network. A network of 6 nodes is established with Real-Time Clock (RTC) based uptime persistence enabled, and the system is operated for election cycles. Throughout this period, the CH identity for each cycle is logged, and battery levels are monitored across all nodes. The results are analyzed to confirm that no node monopolizes the CH role, energy consumption is balanced across nodes, and control overhead remains below the energy level.

- Self-Healing Capabilities Under Failure Conditions

This test assesses the network's resilience in the event of cluster-head failures. A stable cluster is initially established, followed by controlled failure scenarios such as cluster-head power loss, trust degradation, or link quality deterioration. The system's re-election process is monitored to verify that a new cluster-head is elected within two election cycles, all nodes successfully rejoin the reconfigured cluster, and previously stored data records are preserved without any loss.

- Intra Cluster Communication Reliability and Data Persistence

This test validates the reliability of intra-cluster communication and the persistence of data during cluster-head transitions. A cluster of five to eight nodes is deployed with periodic sensor transmissions scheduled. During active data exchange, cluster head re-election is intentionally triggered. The system is evaluated to ensure that data is successfully delivered from members to the cluster head, data integrity is preserved during transitions, and no sequence identifiers are lost in the stored data.

- Link Quality Sensitivity and Tie Breaking Logic

This test assesses the election algorithm's sensitivity to link quality and validates tie-breaking mechanisms. Two candidate nodes are configured with nearly identical CH scores. The algorithm is anticipated to select the node with the lowest MAC address in tie scenarios, thereby ensuring stable and consistent election outcomes.

5 Description of Personal and Facilities

5.1 Work Breakdown Structure

Table 5.1.1: Work Breakdown Structure

WBS	Task
1	Research & Planning
1.1	Literature Review
1.1.1	Collect academic papers on LEACH, HEED, trust-based clustering
1.1.2	Review BLE 5.0 (Coded PHY, extended adverts) and ESP-NOW use cases
1.1.3	Summarize UAV-assisted WSN data ferrying studies
1.1.4	Document gaps in existing clustering/security mechanisms
1.2	Problem Definition
1.2.1	Define research problem & disconnected environment scenario
1.2.2	Identify security, trust, and energy limitations in existing CH schemes
1.2.3	Write research problem statement
1.3	Objective Setting
1.3.1	Define main objective: Secure, fair CH election
1.3.2	Define specific objectives (energy balancing, trust, UAV handover)
1.4	Requirements Gathering
1.4.1	Define functional requirements (clusterization, CH election, persistence)
1.4.2	Define non-functional requirements (energy efficiency, reliability, scalability)
1.4.3	Identify system requirements (ESP32-S3 boards, antennas, UAV, sensors)
2	System Design
2.1	Architecture Design
2.1.1	Select hardware platform (ESP32-S3, external antenna, batteries)
2.1.2	Select UAV data ferry hardware/software (Raspberry Pi BLE/Wi-Fi)
2.1.3	Define network topology (clusters, CH roles, UAV ferry route)
2.2	Clusterization & CH Election Design
2.2.1	Define multi-parameter score formula (Battery, Uptime, Trust, Link Quality)
2.2.2	Design trust evaluation sub-metrics (HSR, PDR, reputation)
2.2.3	Specify HMAC-based security for adverts
2.2.4	Define tie-breaking logic
2.3	System Models & Diagrams
2.3.1	Clusterization workflow diagram
2.3.2	Sequence diagram for CH election
2.3.3	System workflow diagram (Node → CH → UAV)
3	Implementation
3.1	Firmware Development
3.1.1	Set up ESP-IDF toolchain and FreeRTOS environment
3.1.2	Implement RTOS tasks (radio, scoring, trust, storage)
3.1.3	Implement BLE Coded PHY advertisements (extended ADV)
3.1.4	Implement HMAC authentication with mbedTLS

3.1.5	Implement RTC uptime persistence
3.1.6	Implement CH election and tie-break logic
3.2	Experimental Setup
3.2.1	Deploy 8–10 ESP32-S3 nodes with sensors
3.2.2	Configure UAV/gateway with BLE scanning and Wi-Fi/ESP-NOW
3.2.3	Set up power monitoring for energy profiling
3.2.4	Configure logging and debugging interfaces (UART/CSV export)
4	Testing & Validation
4.1	Test Case Development
4.1.1	Define election convergence and spoofing rejection test
4.1.2	Define fairness/rotation test
4.1.3	Define self-healing test on CH loss
4.1.4	Define intra-cluster reliability test
4.1.5	Define UAV interoperability test
4.2	Test Execution
4.2.1	Perform unit tests (score computation, HMAC, uptime storage)
4.2.2	Perform integration tests (neighbor discovery, CH election, rotation)
4.2.3	Perform system tests (UAV data pickup, persistence validation)
4.3	Performance Evaluation
4.3.1	Measure election latency and convergence time
4.3.2	Measure control overhead vs. node energy budget
4.3.3	Analyze fairness of CH rotation
4.3.4	Measure data delivery success rate (CM→CH and CH→UAV)
5	Analysis & Documentation
5.1	Data Analysis
5.1.1	Compare test results against LEACH and HEED benchmarks
5.1.2	Evaluate improvements in lifetime, trust filtering, UAV delivery
5.2	Report Writing
5.2.1	Document methodology and experimental results
5.2.2	Write discussion and conclusion sections
5.2.3	Compile references in IEEE style
5.3	Presentation & Defense
5.3.1	Prepare slides (architecture, algorithm, test results)
5.3.2	Practice and rehearse presentation
5.3.3	Submit dissertation and defend
6	Project Management & Deliverables
6.1	Weekly Logbook Updates
6.2	Gantt Chart Maintenance
6.3	Budget Tracking (ESP32 boards, antennas, sensors, UAV parts)
6.4	Risk Assessment (hardware availability, testbed failures, UAV battery limits)
6.5	Final Dissertation Submission

5.2 Timeline

Figure 5.1: Gantt Chart

5.3 Estimated Budget

Table 5.3. 1: Estimated Budget

Component	Prize (Rs.)
UAV (Estimated)	60,000.00
ESP32-S3-DevKitC-1U (8MB Flash, 8MB PSRAM) x 7	1,850.00
18650 Li-ion 3500 mAh battery (Samsung)	780.00
3x18650 Battery Holder (parallel wiring)	120.00
CN3065 Solar Li-ion Charger module	350.00
INA219 Current sensor (I²C)	350.00
Mini Solar Panel 6V 1W (110x60mm)	350.00
SMA antenna + IPEX to SMA cable	690.00
ENS160 + AHT21 air quality sensor module x 6	7,100.00
INMP441 I²S MEMS microphone module x 6	5,040.00
HMC5883L 3-axis magnetometer module x 6	2,700.00
BME280 pressure/temperature/humidity sensor x 6	5,700.00
Total	**85,030.00**

References

[1] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, 2005.

[2] O. Younis and S. Fahmy, “HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks,” *IEEE Trans. Mob. Comput.*, vol. 3, no. 4, pp. 366–379, 2004.

[3] L. Yang, Y. Lu, S. X. Yang, T. Guo, and Z. Liang, “A secure clustering protocol with fuzzy trust evaluation and outlier detection for industrial wireless sensor networks,” *IEEE Trans. Industr. Inform.*, vol. 17, no. 7, pp. 4837–4847, 2021.

[4] L. Yang, Y. Lu, S. X. Yang, Y. Zhong, T. Guo, and Z. Liang, “An evolutionary game-based secure clustering protocol with fuzzy trust evaluation and outlier detection for wireless sensor networks,” *IEEE Sens. J.*, vol. 21, no. 12, pp. 13935–13947, 2021.

[5] M. Chodnicki, B. Siemiatkowska, W. Stecz, and S. Stępień, “Energy efficient UAV flight control method in an environment with obstacles and gusts of wind,” *Energies*, vol. 15, no. 10, p. 3730, 2022.

[6] M. Spörk, C. A. Boano, and K. Römer, “Performance and Trade-offs of the new PHY Modes of BLE 5,” in *Proceedings of the ACM MobiHoc Workshop on Pervasive Systems in the IoT Era*, 2019, pp. 7–12.

[7] M. T. Nguyen *et al.*, “UAV-assisted data collection in wireless sensor networks: A comprehensive survey,” *Electronics (Basel)*, vol. 10, no. 21, p. 2603, 2021.

[8] D. Popescu, F. Stoican, G. Stamatescu, O. Chenaru, and L. Ichim, “A survey of collaborative UAV-WSN systems for efficient monitoring,” *Sensors (Basel)*, vol. 19, no. 21, p. 4690, 2019.

[9] P. A. Karegar, D. Z. Al-Hamid, and P. H. J. Chong, “Deep Reinforcement Learning for UAV-based SDWSN data collection,” *Future Internet*, vol. 16, no. 11, p. 398, 2024.

[10] M. Lewandowski and B. Płaczek, “A cluster head selection algorithm for extending last node lifetime in wireless sensor networks,” *Sensors (Basel)*, vol. 25, no. 11, p. 3466, 2025.

[11] “RF Coexistence - ESP32-S3 - — ESP-IDF Programming Guide latest documentation,” *Espressif.com*. [Online]. Available: https://docs.espressif.com/projects/esp-idf/en/latest/esp32s3/api-guides/coexist.html. [Accessed: 26-Aug-2025].