Discover Computing

Research

Intelligent IoT-driven optimization of large-scale healthcare networks: the INRwLF algorithm for adaptive efficiency

Radwan S. Abujassar[1]

Received: 23 December 2024 / Accepted: 9 May 2025
Published online: 25 May 2025

Abstract

Significant research has focused on improving routing performance within centralized Software-Defined Networking (SDN) architectures tailored for Intelligent Internet of Things (I-IoT) environments. With the explosive growth of IoT devices, particularly in expansive and dynamic settings, scalable and energy-conscious routing strategies have become essential. Addressing the limitations of power-constrained nodes, this paper proposes a novel routing algorithm, Interior Neighbors Route with Low Fault (INRwLF), designed for integration within SDN and cloud-enabled infrastructures. Unlike traditional approaches, INRwLF employs an AI-enhanced SDN controller to dynamically construct load-balanced cluster tables and compute fault-tolerant, low-latency paths. Simulation results demonstrate that the protocol reduces energy usage and network delay, while prolonging system lifetime by 50–90%. The proposed approach enhances network efficiency and scalability, particularly in domains such as healthcare, where synchronized data collection and resilient connectivity are critical.

Keywords Intelligent-Internet of Things (I-IoT) · Smart designated node (SDN) · Wireless sensor networks · Adjacent Detective Packets (ADP) · Interior Neighbours Route with Low Fault (INRwLF)

1 Introduction

The Internet of Things (IoT) represents a vast, loosely connected network of intelligent devices with capabilities for sensing, processing, and communication. Advances in Radio Frequency Identification (RFID) and sensor technologies have enabled the integration of information systems into physical environments [1]. These systems continuously generate large volumes of data that must be stored, processed, and analyzed efficiently. IoT solutions focus on reliable data collection and transmission, while cloud computing provides the backend infrastructure for services such as device identification, analytics, and visualization platforms [2]. This cloud-based model enables enterprises and users to access and manage services remotely and on demand.

By linking physical objects with intelligent decision-making systems, IoT facilitates real-time interactions between devices and their environment. IoT nodes are capable of autonomous sensing, processing, and communication. However, Wireless Sensor Networks (WSNs), the core enablers of IoT, often suffer from constrained energy supplies, limited storage, and modest communication capabilities. Since physical maintenance like battery replacement is impractical in many deployments, the adoption of energy-efficient strategies becomes essential for sustaining the overall IoT infrastructure.

✉ Radwan S. Abujassar, r.abujassar@aou.edu.kw | [1]Faculty of Computer Studies, Arab Open University Kuwait, Alardiya Industrial, 830, 92400 Al Farwaniyah, Kuwait.

Converting traditional systems into intelligent IoT environments involves deploying lightweight sensors and actuators, often for functions like automated routing, environmental monitoring, or human-device interaction. Artificial Intelligence (AI) plays a vital role in these applications, allowing systems to perform tasks with minimal human oversight [3]. This progression leads to the concept of the Internet of Intelligent Things (IoIT), which embodies the next stage of IoT evolution [4].

IoIT promotes decentralized intelligence, where decision-making is localized at the node level. Unlike conventional WSNs, these systems can handle time-sensitive operations independently. This architectural shift empowers IoT devices to autonomously react to dynamic situations. Complex metrics such as signal strength, data load, and transmission paths are analyzed in real-time to optimize interactions between users and devices [5].

Such intelligence is derived from advanced data analytics, including machine learning and embedded intelligence (EI), which characterize the symbiotic relationship between human behavior and machine responses [6]. However, IoT still faces challenges in deploying robust, energy-aware routing, maintaining load equilibrium, and ensuring network security. Many legacy models rely on centralized control structures, making them less adaptable to dynamic or large-scale environments.

To overcome these limitations, this work introduces a flexible and scalable network framework that integrates cloud computing with evolutionary algorithms for optimal scheduling and clustering. The approach improves data collection over wide sensor areas using genetic algorithms and cloud resources while ensuring efficient load balancing.

The proposed Interior Neighbors Route with Low Fault (INRwLF) protocol employs Particle Swarm Optimization (PSO) and Artificial Bee Colony (ABC) algorithms to optimize routing paths and cluster formations. This minimizes energy usage, reduces latency, and extends the lifetime of sensor networks. In addition, Ant Colony Optimization (ACO) is utilized to identify reliable, shortest-path routes for both intra- and inter-cluster communication.

IoT technologies are foundational to modern smart environments, from intelligent transportation to responsive healthcare systems. By integrating Narrowband IoT capabilities, the INRwLF protocol effectively handles rerouting during congestion and malicious node activity, ensuring low-latency and fault-tolerant communication. This framework builds upon our previous work on intelligent clustering and leader-based routing in IoT networks [7].

In summary, the INRwLF protocol offers a comprehensive solution for scalable, stable, and energy-efficient IoT communication, with demonstrated benefits for smart healthcare, sustainable cities, and other mission-critical applications.

Relationship with prior work

This work extends our previously published study [7], which introduced the NCIoT protocol-an intelligent, cluster-based routing approach incorporating Smart Designated Nodes and Predictive Inquiry Small Packets (PISP). The original protocol emphasized static topologies and backup path construction to enhance reliability in IoT communications.

The current study advances that foundation with a fully dynamic and scalable routing framework-INRwLF-specifically designed for Software-Defined Networking (SDN)-enabled IoT environments. Key differences include:

- **Algorithmic evolution:** INRwLF employs dynamic topology adaptation using hybrid metaheuristic algorithms-Particle Swarm Optimization (PSO), Artificial Bee Colony (ABC), and Ant Colony Optimization (ACO)-for cluster formation and optimal path discovery.
- **Infrastructure integration:** While the earlier work operated on traditional IoT deployments, this study integrates SDN and cloud-based infrastructures for intelligent, centralized control over routing decisions.
- **Trust-aware routing:** The proposed protocol introduces trust-based neighbor evaluation, a security feature absent in the prior model, enhancing data reliability in hostile environments.
- **Application focus shift:** The current model is tailored to smart healthcare environments, emphasizing low-latency, high-integrity communication, in contrast to the general-purpose IoT applicability of the previous study.

Though the concept of predictive inquiry and clustering remains foundational, the proposed INRwLF algorithm, its architecture, and the performance evaluation have been independently developed and adapted for real-time, large-scale IoT scenarios.

Contributions and novelty

This study makes the following key contributions:

- Proposes the Interior Neighbors Route with Low Fault (INRwLF) algorithm-an AI-driven, energy-efficient routing protocol optimized for SDN-enabled IoT architectures.

- Utilizes a centralized SDN controller to perform adaptive load balancing and routing optimization, reducing computational complexity and energy consumption.
- Introduces a trust-aware neighbor evaluation mechanism to exclude unreliable or malicious nodes, enhancing the security and stability of data transmission paths.
- Develops a network scheduling technique that reduces energy depletion at cluster heads and improves overall node longevity.
- Validates the proposed system through extensive NS2-based simulation, demonstrating 50–90% improvements in network lifetime and significant reductions in end-to-end delays and energy usage.

Novelty: The distinct contributions of the INRwLF protocol lie in its integration of intelligent routing decisions with security-aware clustering in a cloud-integrated SDN environment. Specifically:

- It introduces a hybrid routing mechanism combining PSO, ABC, and ACO for adaptive clustering and shortest-path routing under dynamic network conditions.
- It operates as a scalable, real-time system suited for high-density, energy-constrained IoT deployments with mobility and security challenges.
- It targets healthcare-specific scenarios requiring data precision and transmission continuity-applications where traditional static routing models underperform.
- It offers a comparative performance benchmark against OMS-LB and RM-LB protocols, showing marked improvements in energy-aware path selection and load distribution.

This protocol evaluates energy consumption by analyzing transmission distances, node workload, and residual energy metrics. Unlike conventional fixed-path algorithms, INRwLF dynamically reassigns routing paths in response to network state, thereby minimizing redundant communication and extending network longevity.

2 Improved node clustering in IoT for healthcare

Effective node clustering plays a pivotal role in optimizing Internet of Things (IoT) deployments within smart healthcare systems. In urban health infrastructures, clustering enhances the organization and coordination of IoT-enabled medical devices, enabling real-time monitoring and analysis of patient data. This facilitates faster clinical response, improved diagnostic accuracy, and better resource management in emergency scenarios.

Despite these advantages, the aggregation of sensitive medical data across clustered networks introduces new privacy and security challenges. As data volumes increase, so does the risk of unauthorized access and misuse. Therefore, it is critical to evaluate both the benefits and operational strategies of node clustering in healthcare to ensure patient confidentiality while enabling data-driven decision-making.

Healthcare institutions must implement robust security frameworks to counter potential vulnerabilities associated with large-scale sensor networks. Strategies include encrypted communication, secure authentication protocols, and dynamic trust management to prevent data breaches and preserve patient trust.

Within smart city ecosystems, strategic placement of IoT sensors across hospitals and urban zones supports predictive healthcare management. Enhanced clustering facilitates real-time tracking of health trends, enables early detection of outbreaks, and supports efficient allocation of medical resources. These capabilities are essential for maintaining public health and operational resilience in densely populated areas.

In summary, intelligent node clustering in healthcare-oriented IoT networks enhances the quality and responsiveness of care while supporting broader urban sustainability goals. This is illustrated in Fig. 1.

The remainder of this paper is organized as follows: Sect. 3 reviews existing research in energy-efficient routing within IoT networks, emphasizing recent advances in AI-based approaches and the adoption of Software-Defined Networking (SDN) architectures. It also identifies current research gaps. Section 4 introduces the proposed Interior Neighbors Route with Low Fault (INRwLF) algorithm, detailing its conceptual framework, implementation steps, and the comparative methodology used against benchmarks such as OMS-LB and RM-LB, particularly with respect to network longevity, efficiency, and security. Section 5 describes the simulation environment, followed by an analysis of the results to evaluate INRwLF's impact on data aggregation, energy savings, and latency. Section 6 concludes the paper by highlighting the

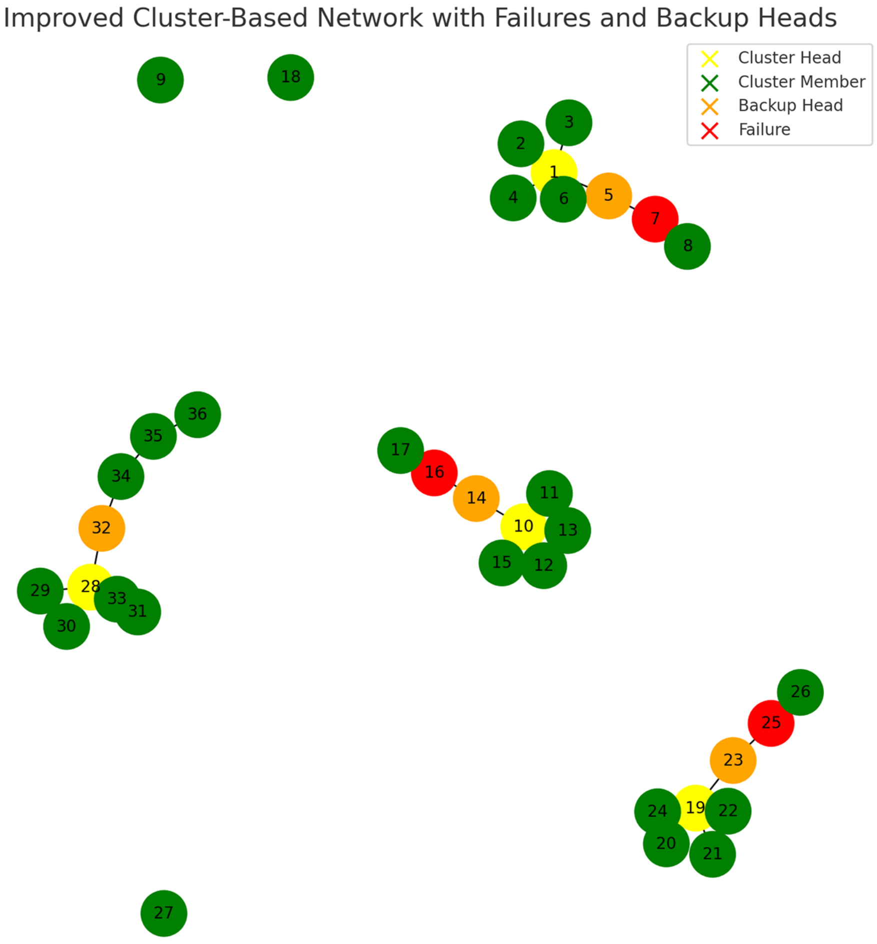


Fig. 1 Clustering characteristics

core contributions and outlining future directions, with an emphasis on enhancing protocol scalability and resilience across varying IoT deployment contexts.

3 Background and related work

Node clustering remains a cornerstone in optimizing Internet of Things (IoT) network performance, particularly in large-scale deployments such as healthcare systems within smart cities. Clustering enables more efficient communication, data processing, and energy usage by grouping devices based on relevant attributes. However, it introduces substantial challenges related to scalability, heterogeneity, and real-time adaptability. Our previous work [7] proposed the NCIoT protocol, which leveraged proximity-based clustering to improve routing performance. Building on that foundation, this study incorporates predictive routing and dynamic backup path selection to enhance system robustness and responsiveness.

In high-density IoT environments, conventional clustering methods often fall short in handling large volumes of data, leading to increased latency and degraded performance [8]. Misclassification of nodes, whether due to noise or outliers, can result in suboptimal resource utilization and systemic inefficiencies [9]. Centralized clustering strategies, while effective in static environments, suffer from vulnerabilities such as single points of failure and lack of resilience under dynamic conditions.

To address these drawbacks, decentralized clustering approaches have emerged. These distribute decision-making responsibilities across multiple nodes, improving network fault tolerance and responsiveness [10]. Although beneficial, they bring challenges like inter-node communication delays, coordination complexity, and increased processing time, which may undermine overall efficiency [11].

In healthcare-focused smart city deployments, these limitations are especially critical. Real-time decision-making and accuracy in data collection are vital for timely intervention. Poor clustering decisions in such scenarios can impede patient monitoring and lead to inefficient resource allocation. Additionally, traditional clustering algorithms often overlook the variability within node groups, leading to generalized assumptions and reduced predictive accuracy [12]. Incorporating contextual parameters such as demographic trends or historical behaviors can enhance the relevance and precision of clustering models.

Recent studies have proposed a variety of advanced solutions. For example, sentiment analysis and anomaly detection have been introduced to mitigate misclassification risks and improve model adaptability [13]. In [14], a secure trust-based protocol (SecRPL-MS) was developed to tackle power inefficiencies and high packet loss in IoT networks with mobile sinks, while defending against attacks like Sybil and blackhole. Meanwhile, [15] presented a Deep Learning-based vulnerability detection framework using Pointer Networks, offering performance improvements yet requiring further real-world testing.

Other notable advancements include RISA [16], which utilizes PSO and GA to optimize data collection in cloud-enabled IoT systems, and DAOSVM [17], which enhances mobile sink navigation by accounting for physical obstacles. While these systems improve aspects of IoT routing and data transmission, many still fall short in handling dynamic topologies or fluctuating resource availability.

The work in [18] proposes load balancing using MiniMax stratification and evolutionary algorithms to reduce redundancy. However, its reliance on fixed thresholds limits flexibility. Similarly, Yuan et al. [19] introduced an I-IoT model using a deep learning architecture (EG-CRNN) tailored for healthcare applications, yet lacked scalability and security considerations.

Earlier foundational efforts such as [20, 21] also contributed to energy efficiency and stable routing in WSNs. Nonetheless, these approaches require refinement to address fault tolerance, resource optimization, and real-time responsiveness.

This study builds on the gaps and challenges identified in the existing literature by proposing a more adaptive, resilient, and secure clustering protocol-INRwLF-tailored for energy-efficient, AI-integrated IoT networks, particularly in mission-critical domains such as healthcare.

1. **Energy efficiency:** The INRwLF algorithm is designed to minimize energy consumption, a common bottleneck in IoT deployments. This is achieved through:
   - Intelligent traffic distribution facilitated by an AI-integrated SDN controller, which balances the network load across nodes.
   - Adaptive clustering mechanisms that limit the energy burden on cluster heads (CHs) and reduce unnecessary transmissions among neighboring nodes.
2. **Network scalability:** To ensure effective performance across expansive and heterogeneous IoT environments, the proposed system integrates:
   - A flexible and scalable routing strategy that supports dynamic node density and mobility.
   - Cloud-based resources for efficient computation and data storage, decoupling processing tasks from constrained edge devices.
3. **Delay mitigation:** To overcome latency issues prevalent in traditional IoT protocols, the approach includes:
   - Real-time path computation by the SDN controller to ensure low-latency data delivery.
   - A trust-aware routing process that proactively eliminates unreliable nodes, reducing the need for retransmissions and enhancing overall communication speed.
4. **Trust and security:** Security is strengthened through a decentralized trust evaluation system, where:
   - Nodes assess the credibility of their neighbors before incorporating them into routing paths.
   - Malicious or compromised nodes are systematically excluded, enhancing data integrity and system resilience against threats.
5. **Network lifetime optimization:** The protocol supports long-term network sustainability through:
   - Intelligent load distribution and adaptive clustering that prevent early node failures and balance energy use.

- Efficient scheduling techniques that reduce idle listening and redundant transmissions, thereby extending the overall network lifespan.

Together, these improvements address critical gaps highlighted in existing literature and contribute to the design of a reliable, adaptive, and energy-conscious IoT architecture suitable for diverse application domains.

3.1 Problem statement and aims

This research aims to establish a robust, energy-aware routing framework tailored for Intelligent IoT (I-IoT) networks. Limitations at the physical layer-such as finite battery life, constrained processing capabilities, limited storage, and restricted communication bandwidth-pose significant challenges to maintaining efficient and reliable network operations. These constraints are exacerbated in large-scale deployments, where managing heterogeneous clustering and data aggregation becomes increasingly complex. As such, an intelligent optimization approach is essential for balancing performance and energy efficiency across the network.

At the core of the proposed strategy is a clustering mechanism, wherein nodes are organized into groups led by cluster heads (CHs). These CHs are responsible for aggregating data from their associated cluster members (CMs) and forwarding it to a centralized sink. However, this role imposes a higher energy burden on CHs, causing them to deplete their resources faster than other nodes. The unequal energy consumption leads to instability in the network and can cause early node failures, particularly under static sink configurations. Moreover, fixed sink placements introduce routing bottlenecks and contribute to the hot-spot problem, where certain nodes are overwhelmed with traffic, reducing overall system longevity.

To counter these issues, the proposed routing model incorporates artificial intelligence to support adaptive clustering and route optimization. The specific objectives of this study are as follows:

- Increase the operational lifetime of the network by minimizing premature node failures.
- Reduce overall energy consumption through balanced load distribution.
- Enhance data throughput by optimizing routing paths and reducing packet loss.
- Minimize average communication delay, ensuring timely and reliable data transmission.

3.2 Dynamic adaptation and reliability of INRwLF in high-mobility scenarios

The Interior Neighbors Route with Low Fault (INRwLF) algorithm is engineered to maintain network reliability in dynamic IoT environments characterized by frequent topology changes. It achieves this through adaptive routing and intelligent clustering, allowing the system to respond efficiently to node mobility and shifting network conditions.

A key feature of INRwLF is its ability to continuously assess neighboring nodes based on trust metrics such as energy reserves and link stability. Nodes deemed unreliable are excluded from routing paths, thereby enhancing overall route resilience. Cluster heads (CHs) are selected using real-time indicators including residual energy and spatial proximity, which optimizes cluster composition in mobile settings.

The AI-enabled SDN controller plays a critical role by performing continuous route recalculations, enabling the protocol to dynamically adjust to node movement. INRwLF also maintains redundant routing paths, providing seamless traffic redirection in the event of node displacement or link degradation.

Incorporating velocity and mobility trends into routing logic, the algorithm anticipates disruptions and adjusts paths proactively. It uses compact control messaging to reduce communication overhead, ensuring smooth operation even under high-mobility conditions. Simulation evaluations demonstrate that INRwLF delivers superior performance in terms of packet delivery rate, latency minimization, and network longevity when compared to conventional protocols.

3.3 Cluster head election and energy dissipation minimization

The INRwLF protocol adopts an adaptive approach to cluster head (CH) selection, using a combination of real-time parameters such as residual energy, node centrality, and prior communication reliability. By prioritizing nodes with sufficient energy reserves and favorable positions within the cluster, the system promotes equitable task distribution and limits the need for frequent re-elections, which can otherwise introduce instability and overhead.

This method ensures that no single node is disproportionately tasked with energy-intensive responsibilities, thereby mitigating premature depletion. Moreover, the algorithm supports periodic re-clustering based on updated network metrics, allowing the system to dynamically reassign responsibilities as conditions evolve. This cyclical redistribution of workload not only improves data aggregation efficiency but also significantly contributes to prolonging the operational lifetime of the network.

Table 1 presents a comparative summary of various routing protocols, including the proposed INRwLF algorithm, focusing on key performance indicators such as Quality of Service (QoS) and traffic optimization between source and destination nodes within each cluster. While the evaluation effectively highlights improvements in these areas, the study does not address security-related concerns, which remain a critical component in the design of resilient IoT networks.

Although both simulation and physical test-bed experiments were conducted, the evaluation was limited to a network of 30 nodes. This modest scale restricts the generalizability of the findings, particularly in scenarios involving higher node densities or more dynamic topologies.

Security considerations are acknowledged as a priority for future work. In particular, recent literature emphasizes the integration of emerging technologies, such as blockchain, with IoT infrastructures. For example, research exploring the use of blockchain in demand-side management (DSM) and supply chain (SC) systems suggests that these technologies could play a pivotal role in enhancing data integrity and access control.

Future investigations may expand on this by incorporating blockchain-enabled frameworks to address trust and security challenges in clustered IoT networks. A systematic review of academic databases-including ScienceDirect, JSTOR, Sage, IEEE Xplore, MDPI, and ACM Digital Library-was conducted using keywords such as "blockchain," "IoT-based drug management," "healthcare," and "smart cities." The selected studies were grouped into three major system categories relevant to this emerging interdisciplinary field.

The reviewed literature can be categorized into three primary thematic areas. The first group encompasses research dedicated to the architecture and implementation of demand-side management (DSM) and supply chain (SC) systems that integrate blockchain and IoT technologies. These studies typically propose new models, frameworks, algorithms, and architectural innovations aimed at enhancing system transparency, traceability, and automation.

The second category focuses on the application of behavior change techniques (BCT) and IoT technologies in the context of DSM strategies and smart city implementations. These works emphasize the human-in-the-loop aspect of IoT systems, exploring how behavior modeling can improve sustainability and resource efficiency.

The third category consists of comprehensive reviews that examine how BCT and IoT contribute to decision support systems (DSS) in DSM environments. These studies evaluate the role of intelligent analytics and data-driven decision-making in optimizing resource usage across diverse infrastructure domains.

In [34], the author outlines critical requirements for maintaining secure and efficient communication in energy-aware networks. The study highlights the increasing demand for sustainable energy in modern infrastructures such as homes, transportation, and industry, and underscores the shift from traditional fossil fuels toward renewable sources such as wind and solar power. These alternatives offer benefits in terms of cost efficiency, resilience, and reduced environmental impact.

The same work proposes a blockchain-integrated industrial wireless sensor network to support secure data transmission for smart grid applications. Utilizing a smart contract framework based on the Solana blockchain-referred to as the Advanced Solana Blockchain-the system facilitates real-time monitoring and control of smart grid infrastructure. Experimental results and security evaluations confirm its lightweight nature and reliability in industrial data exchange scenarios.

Further, in [35], the authors advocate for a blockchain-based communication platform tailored for distributed energy resource (DER) management within smart grids. Solana's architecture is identified as particularly suitable due to its high throughput, low latency, and strong scalability features. However, the study also highlights major vulnerabilities in Solana-based industrial wireless sensor networks, including susceptibility to SQL injection, spoofing, and man-in-the-middle (MitM) attacks. These threats compromise the real-time management of DER events and can disrupt operational reliability.

Additionally, the authors identify broader technical challenges such as data transmission overload, misrouted packets, network congestion, and increased system costs. By providing detailed datasets on various cyberattacks, the research contributes to the development of enhanced security frameworks for resilient smart grid infrastructures.

Table 1 Comparison table

Method	Description	Strengths	Weaknesses	Security
Centralized routing using SDN, Particle Swarm Optimization, Genetic Algorithms [22]	Increased network lifespan with reduced delay	Energy-efficient routing, longer network lifespan	Other QoS parameters not considered	Low
SecRPL-MS using Sailfish optimization [23]	Improved malicious node detection accuracy, security against several attacks	High security, efficient performance metrics	Energy depletion, presence of malicious nodes, packet losses	Average
Deep learning with pointer networks and NOC [24]	Efficient in terms of time and solution quality	Scales better than existing AI solutions	Need for real-world testing	Low
DAOSVM with SVM and spanning tree [25]	Balanced network traffic with data fusion	Effective load distribution and network traffic balance	Efficient path construction in the presence of obstacles	Low
AI-driven load optimization, MiniMax, GA, DPSO [26]	Nodes Clustering-Based on IoT	Obstacle-aware data collection path for mobile sinks	Data fusion depends on fixed thresholds; load optimization and migration strategy issues	Low
Intelligent-IoT (I-IoT) with EG-CRNN structure [27]	Faster training, reduced error compared to conventional methods	Obstacle-aware data collection path for mobile sinks	Scalability and real-world adaptability not discussed	Low
Optimizing multi-path routing with PMSO [28]	Average improvement in routing performance	Ensured connectivity among IoT devices with QoS	Centralized network issues like queuing delay	Low
Combined efficient path discovery with ant colony for SDN-based routing [29, 30]	Efficient path discovery	Better combination of parameters like delay and throughput	Parameters like delay not optimized	Low
Deep learning (CNN) for load prediction [31]	Improved throughput, packet loss, and node performance	Efficient channel allocation with less interference	QoS flow concerns not considered	Low
INRwLF	Recover the route or node failure; improved throughput, reduce packet loss	Efficient channel allocation with less interference and energy	Mobility in high speed affects network stability	Low
OMS-LB [32]	Optimal mobile sink with load balancing	Enhanced network lifetime and energy efficiency	Limited adaptability to high mobility scenarios	Low
RM-LB [33]	Random movement with load balancing	Simple implementation, reduced latency in low-density networks	Inefficient energy utilization in dense networks	Low

4 Proposed algorithm: INRwLF

Figure 2 outlines the operational workflow of the proposed INRwLF algorithm, which facilitates dynamic clustering across distributed network segments. The process begins by broadcasting predictive inquiry packets to collect contextual data from each cluster. Based on this data, the algorithm calculates inter-node distances to determine optimal routing paths and construct alternate paths when necessary. Each node's spatial position is defined relative to its zone, enabling localized geographic analysis for precise decision-making.

Algorithm 1 is responsible for determining the Euclidean distances between nodes and identifying all neighbors within a 250-meter radio propagation range. Upon identifying potential neighbors, the algorithm evaluates candidate nodes to construct a route with the fewest intermediate hops. A node is classified as "nearby" if it falls within this propagation radius. When multiple candidates exist, the algorithm selects the next hop based on criteria such as link reliability and trust score, thereby enabling the generation of an efficient primary route.

For fault tolerance, the system computes an alternative path that excludes any nodes present in the primary route. This strategy ensures routing diversity and reduces the risk of repeated node failure along critical paths. The INRwLF algorithm coordinates with the SDN controller to facilitate real-time route computation and disseminate lightweight control packets across the network. These packets retrieve updated trust and availability metrics from adjacent nodes, supporting the dynamic reassignment of routing paths with enhanced reliability.

4.1 Advantages of this model

This clustering approach provides several benefits:

- **Energy efficiency:** Cluster-based architecture reduces direct communication with the base station, saving energy.
- **Scalability:** More sensors can be added without overwhelming the network.
- **Reliability:** If a sensor fails, additional nodes can act as replacements.
- **Better communication:** Cluster heads optimize data transmission, improving efficiency.

Fig. 2 Diagram for collecting info and network clustering

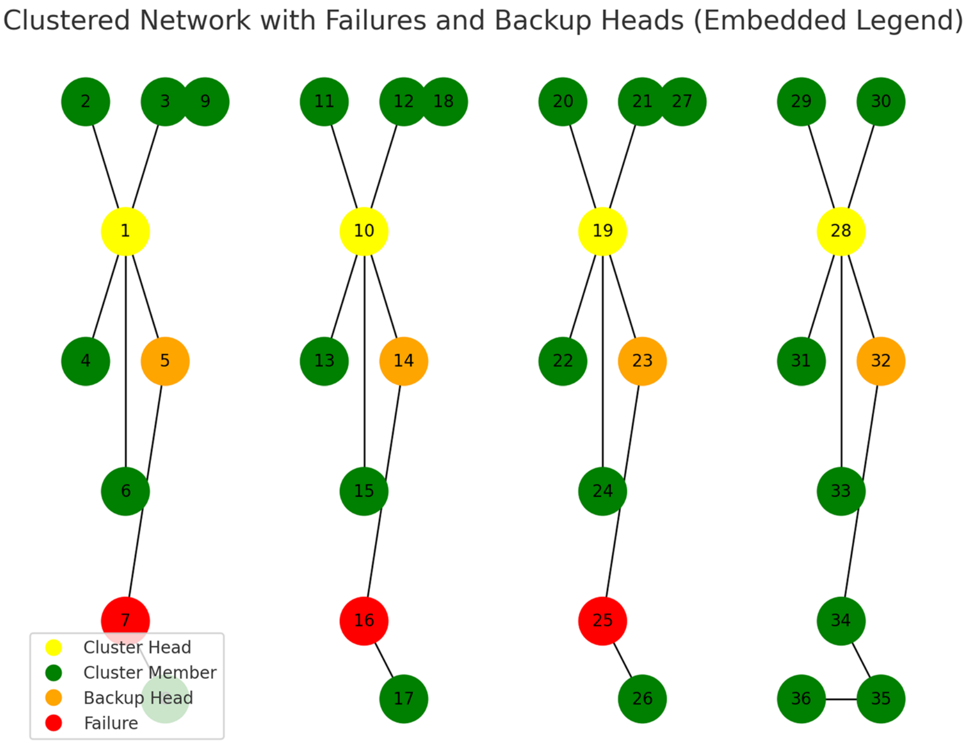


Figure 2 illustrates the communication behavior of nodes within the proposed network architecture. Following the initial transmission phase, each node dispatches a compact control packet to summarize local data and assist in synchronization with designated cluster head (CH) nodes. Within each designated region, head clusters (HCs) initiate the transmission of lightweight packets to probe their surroundings and verify the proximity and membership status of adjacent nodes.

This step is essential in identifying potential overlaps or misclassifications-specifically, nodes that may be geographically located within one cluster but logically belong to another. After validating cluster boundaries, CHs proceed to disseminate data packets across the cluster. Each node operates as part of a modular structure, wherein cluster members monitor local topology changes and assess whether neighboring nodes remain aligned with the CH's route.

Additionally, this stage evaluates cross-cluster communication when a targeted node lies outside the current cluster domain. Member nodes confirm their capacity to relay data upward to the CH, ensuring cohesive intra-cluster communication and supporting dynamic route maintenance in clustered network environments.

Scalability in large-scale IoT networks

The INRwLF protocol is engineered to support the operational demands of large-scale IoT environments characterized by heterogeneous and frequently changing node distributions. Leveraging Particle Swarm Optimization (PSO) for adaptive clustering, the protocol distributes network traffic evenly among cluster heads (CHs), thereby minimizing the impact of node density on system performance.

To ensure routing efficiency at scale, Ant Colony Optimization (ACO) is employed to dynamically compute the most viable communication paths. This enables the protocol to maintain routing stability and low latency even as network size and complexity increase. A centralized Software-Defined Networking (SDN) controller-augmented by AI-driven analytics-coordinates path computation and clustering decisions, offloading intensive tasks to cloud infrastructure. This architecture ensures that processing and storage demands are met without degradation in service quality.

Collectively, these mechanisms allow INRwLF to maintain consistent performance metrics across various deployment scales, rendering it suitable for a broad spectrum of IoT applications, including urban sensing, industrial automation, and healthcare monitoring.

Addressing potential security threats

To enhance the security of data transmission in IoT environments, the INRwLF protocol integrates a continuous trust-based assessment system. This system evaluates the behavior and reliability of neighboring nodes using real-time metrics, enabling the dynamic exclusion of compromised or untrustworthy participants from the routing process. As a result, the protocol mitigates risks associated with packet tampering, selective forwarding, and route hijacking.

The security model is further strengthened through adaptive clustering and the deployment of alternate communication paths. These features not only improve the protocol's resilience to targeted attacks but also ensure service continuity in the face of link failures or node compromise. When potential threats or anomalies are detected, INRwLF automatically recalculates safe routing paths, leveraging trusted nodes to maintain consistent data flow.

By embedding proactive security mechanisms into its core architecture, the INRwLF framework delivers dependable communication capabilities and safeguards data integrity across diverse and dynamic IoT networks.

Algorithm explanation

The INRwLF algorithm is illustrated in Fig. 2, accompanied by a step-by-step breakdown based on Algorithm 1. Designed for dynamic and fault-prone IoT environments, the **Interior Neighbors Route with Low Fault (INRwLF)** algorithm identifies reliable routing paths between a given source node *s* and destination node *d*, while explicitly avoiding unreliable or compromised links.

The process begins with the initialization of key variables: the provisional path $p_a(s, d)$, initially empty, and the edge tracking subset q_{sub}. The source node *s* is enqueued into a processing queue *Q* alongside the empty subset, initiating the route discovery phase.

The algorithm then enters an iterative loop that continues until either a valid path is identified or all routing possibilities have been exhausted. At each iteration, the queue dequeues the current element (q_{sub}, x), where *x* is the node under evaluation. For every neighboring node *k* connected to *x*, the corresponding edge $e = (x, k)$ is assessed. If this edge does not belong to the predefined set of unreliable connections *edges_to_avoid*, and the remaining path from *k* to *d*-denoted $P_r(T_r, k, d)$-is also free of such edges, the path $p_a(s, d)$ is updated accordingly to include *e*.

If no viable edge is found at the current iteration, the algorithm expands the search space by enqueuing $(q_{sub} \cup e, k)$ into *Q*, effectively continuing the path search from a new node while preserving previously explored edge constraints.

This iterative and constraint-aware mechanism ensures that the INRwLF algorithm systematically explores feasible routing paths while avoiding problematic links, ultimately delivering reliable and efficient route construction in highly dynamic network topologies.

Step 1: Start Begin by taking the following inputs: - T_r: Set of available nodes. - s: Source node. - d: Destination node

Step 2: Initialization - Set the initial path $p_a(s, d)$ to an empty set ($\emptyset$). - Initialize q_{sub}, the subset of edges in the path, to $\emptyset$

Step 3: Queue setup - Enqueue the pair (q_{sub}, s) into the queue Q

Step 4: Queue check - Check if the queue Q is not empty and the final path $p_a(s, d)$ has not been found ($p_a(s, d) = \emptyset$). - If both conditions are satisfied, proceed to extract the next element from the queue. Otherwise, terminate and return the result

Step 5: Dequeue operation - Extract the front element (q_{sub}, x) from the queue Q, where x is the current node being processed

Step 6: Explore adjacent nodes - For each adjacent node k of the current node x, define an edge $e = (x, k)$

Step 7: Avoid restricted edges - Check if the current edge e or the current subset $q_{sub} \cup e$ intersects with the set of edges to avoid. - If $q_{sub} \cup e$ intersects with the restricted edges, skip this edge and continue with the next node. - If it does not intersect, proceed to the next step

Step 8: Check future path feasibility - Determine if the remaining path from node k to the destination d intersects with restricted edges. - If it does not intersect: - Update the path $p_a(s, d)$ with the current path $q_{sub} \cup e$ and the feasible path from k to d. - If it does intersect: - Enqueue the updated subset $(q_{sub} \cup e, k)$ back into the queue for further exploration

Step 9: Repeat or terminate - Repeat steps 4 through 8 until either a valid path $p_a(s, d)$ is found or the queue Q becomes empty

Step 10: End - Return the final path $p_a(s, d)$ if found, or terminate without a solution if no valid path exists

Algorithm 1 INRwLF: Interior Neighbour Routing with Low Fault Tolerance

```
procedure ComputeResilientPath $\mathcal{N}, s, d, \mathcal{B}$
Input:
  $\mathcal{N}$: Set of all active nodes
  $s$: Source node
  $d$: Destination node
  $\mathcal{B}$: Set of blocked edges (to avoid)
Output: $\Pi(s, d)$: Constructed path from $s$ to $d$
$pivot \leftarrow$ SelectNearestNode($s$)
$neighborCount \leftarrow$ EvaluateConnectivity($pivot$)
while $neighborCount \geq$ EvaluateConnectivity($pivot$) do
  if adjMatrix[$pivot$][$neigh$] $\neq \infty$ then
    if routeMap[$pivot$][$neigh$] $=$ $neigh$ & routeMap[$pivot$][$nextHop$] $\neq$ PrimaryNeighbor then
      NextHop[$neigh$] $\leftarrow$ adjMatrix[$pivot + h$][$neigh$]
      $neighborCount \leftarrow neighborCount + 1$
      ClusterPaths[$pivot$][$h$] $\leftarrow$ routeMap[NextHop[$neigh$]][$nextHop$]
    end if
  end if
end while
$\Pi(s, d) \leftarrow \emptyset$
$queue \leftarrow$ InitQueue(($\emptyset, s$))
while $queue \neq \emptyset$ and $\Pi(s, d) = \emptyset$ do
  ($exploredEdges, currentNode$) $\leftarrow$ Dequeue($queue$)
  for all $neighbor \in$ NeighborsOf($currentNode$) do
    $link \leftarrow (currentNode, neighbor)$
    if $(exploredEdges \cup link) \cap \mathcal{B} = \emptyset$ then
      if FindPath($\mathcal{N}, neighbor, d$) $\cap \mathcal{B} = \emptyset$ then
        $\Pi(s, d) \leftarrow exploredEdges \cup link \cup$ FindPath($\mathcal{N}, neighbor, d$)
      else
        AddToQueue($queue, (exploredEdges \cup link, neighbor)$)
      end if
    end if
  end for
end while
end procedure
```

To improve transmission reliability in IoT environments characterized by dense node distributions and high mobility, the INRwLF protocol incorporates a range of adaptive mechanisms:

- **Dynamic clustering:** Nodes are organized into clusters using real-time indicators such as residual energy and geographic proximity. Cluster heads (CHs) are elected based on these metrics to facilitate equitable load distribution and localized data aggregation.
- **Redundant path selection:** The protocol maintains both primary and secondary routing paths. In the event of congestion or link disruption, traffic is autonomously redirected through alternate routes, reducing packet loss and maintaining communication continuity.
- **Mobility-aware routing:** Node velocity and directional movement patterns are integrated into routing decisions, enabling the system to anticipate topology changes and adapt routes proactively to maintain stable links.

- **Trust-based node evaluation:** Nodes continuously evaluate the trustworthiness of their neighbors using behavioral metrics. Unreliable or potentially compromised nodes are excluded from routing decisions, enhancing route integrity and protecting data flows.
- **AI-based load optimization:** The combined use of Particle Swarm Optimization (PSO) for cluster formation and Ant Colony Optimization (ACO) for route determination ensures optimal distribution of communication tasks, preventing traffic congestion and improving resilience.
- **Lightweight control signaling:** The system uses minimal-overhead control packets for maintaining cluster structures and updating route paths. This reduces network overhead while enabling rapid response to dynamic topology shifts.

In support of these mechanisms, the study also analyzes the operational configurations and hardware specifications of the sensor nodes used, as summarized in Table 2. The architecture includes ZigBee coordinators, routers, and end devices, each fulfilling distinct roles within the network. Sensor nodes operate at 3.3–5 V and require voltage regulation components to bridge high-voltage (HV) and low-voltage (LV) domains, ensuring stable power supply and hardware compatibility.

The wavelength λ of the signal is calculated using the formula in Eq. (1):

$$\lambda = \frac{c}{f}, \tag{1}$$

where c is the speed of light (3×10^8 m/s), and f is the frequency of the signal (in Hz). The received power P_r decreases with the square of the distance d between the transmitter and receiver.

The received power P_r is determined using the Friis transmission Eq. (2):

$$P_r = P_t\left(\frac{\lambda}{4\pi d}\right)^2 G_t G_r, \tag{2}$$

where P_t is the transmitted power (in Watts), G_t is the transmitter antenna gain, G_r is the receiver antenna gain, and d is the distance between the transmitter and receiver (in meters). The free-space loss (FSL) in decibels is given by Eq. (3):

$$\text{FSL (dB)} = 20\log_{10}(d) + 20\log_{10}(f) - 27.5. \tag{3}$$

At a frequency of 2450 MHz, the specific free-space loss is show as below in Eq. (4):

$$\text{FSL (2450 MHz)} = -\left(20\log_{10}(d) + 40.3\right). \tag{4}$$

In Eq. (5) the power attenuation in decibels is expressed as:

$$P_{dB} = 10\log_{10}\left(\frac{P_{\text{out}}}{P_{\text{in}}}\right), \tag{5}$$

where P_{out} is the output power and P_{in} is the input power.

Packet forwarding efficiency is evaluated using cumulative route path (CRP) and packet delivery efficiency, as shown in Eqs. (6) and (7), respectively:

Table 2 Mobile node hardware [36]

Hardware	Description
Microcontroller Arduino Pro Mini	Processor with ADC and data serial communication capabilities
XBee S2 C End Device	Sends pulse sensor data to the coordinator node in the wireless sensor network
XBee S2 C Coordinator	Receives pulse sensor data from ZigBee end devices or routers and forwards it to the base station
XBee S2 C Router	Relays pulse sensor data to the coordinator and communicates between routers in a mesh network
Battery (3.7 V, 1000 mAh)	Provides power to the sensor node

$$CRP_{\text{total}} = \sum_{i=1}^{N} CRP_i, \tag{6}$$

$$P_{\text{CRP}} = \frac{CRP_{\text{received}}}{CRP_{\text{sent}}}. \tag{7}$$

The transmission and reception delays for a packet are given by Eqs. (8) and (9) :

$$t_{\text{transmit}} = \frac{\text{packet size (bits)}}{\text{transmission rate (bits/sec)}}, \tag{8}$$

$$t_{\text{receive}} = t_{\text{transmit}} + d \cdot \text{propagation delay}. \tag{9}$$

Cluster routing and node allocation dynamics are evaluated through the routing equation, represented as below in Eq. (10):

$$\begin{aligned} Rout[S][NHop] &= \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}, \\ \text{if } NH \neq Dest, \quad CRP_{\text{Header}} &= \sum_{s=1}^{D} \sum_{i=1}^{N} Routing[i][j]. \end{aligned} \tag{10}$$

The following equations form the basis for optimizing route selection, facilitating efficient data transmission, and improving overall network reliability.

In the initial stage of communication, the source node S initiates a discovery process by querying its immediate neighbors for the most optimal routing path. To prevent circular routing and unnecessary path repetition, the second condition ensures that the selected route remains loop-free. The third condition leverages the underlying cluster-based topology, which governs how nodes are grouped and how inter-cluster communication is managed.

To strengthen network connectivity, each node maintains connections with multiple neighbors, forming a resilient primary route. In parallel, a neighboring cluster node is designated as a backup, ready to assume responsibility in case of failure along the main path. Each adjacent node performs localized route computation for its respective cluster, ensuring that connectivity is maintained even under dynamic conditions.

Intermediate routers reference their respective routing tables to dynamically discover alternate forwarding options. These secondary paths are determined using the hierarchical cluster structure, allowing for flexible adaptation to topology changes. The general path from a given source node S to a destination node D is mathematically represented as:

$$S \rightarrow \text{adjacent\_node} \rightarrow \text{next\_hop} \rightarrow \cdots \rightarrow D.$$

The total weight of the topology is calculated in Eq. (11):

$$W_{\text{total}} = \sum W_{S\ldots\text{to}\ldots D} = X \tag{11}$$

where W_0 represents the weight of an individual arc, and X is the total weight of all arcs. Changes in the network are captured as Eq. (12):

$$\Delta W = W_{\text{final}} - W_{\text{initial}} \tag{12}$$

To ensure routing flexibility, the algorithm computes alternate paths, expressed as:

$$P_s \rightarrow D : S \rightarrow \text{NH} \rightarrow \text{NNH} \rightarrow \cdots \rightarrow D,$$

where NH and NNH are the next hop and next-next hop, respectively.

At the end of each simulation, the total number of **CRP** packets equals the sum of all messages generated. These packets gather routing data, including alternative next-hop options, which are forwarded to the central cluster node (**HEAD**). The **CRP** packet header includes:

- IP source address,
- IP destination address,
- acknowledgment flag,
- identification of the next hop (if altered).

The optimization of transmission and reception durations is represented by the round-trip time as show in Eq. (13):

$$T_{\text{round-trip}} = T_{\text{transmit}} + T_{\text{receive}}, \tag{13}$$

Here, T_{transmit} denotes the transmission duration, while T_{receive} captures the time required for packet reception. These metrics are integral to assessing communication efficiency and reliability throughout the network.

The proposed INRwLF protocol introduces a strategic framework to enhance routing robustness in IoT environments. The process begins with a predefined cluster formation phase, where the network is segmented into geographically or logically bounded zones. A distributed election mechanism, referred to as the **HEAD** cluster process, dynamically identifies the next optimal forwarding node in response to route disruption or link failure. This hierarchical structure facilitates more effective data regulation and monitoring from the source node *S* to the destination *Dest*.

To keep cluster operations synchronized, the designated **HEAD** cluster node periodically receives **CRP** (Cluster Routing Probe) inquiry packets. These packets, designed for minimal overhead, circulate only within their associated clusters and are not propagated to unrelated zones-preserving bandwidth and reducing cross-cluster noise.

For routing optimization, each node adjacent to the primary path maintains a supplementary routing table indexed by destination. This enables the generation of alternate route candidates from *S* to *Dest*, which are assessed based on their physical distance (*Dist*) and divergence from the principal route. The structure of these candidate paths can be formally expressed as (Table 3):

$$S \rightarrow \text{adj1}, \quad \text{or} \quad S \rightarrow \text{adj2}.$$

During the routing process, a neighboring candidate for the target is generated at V_1, as illustrated in Fig. 3. The route selection is based on the financial cost (energy consumption) and the degree to which it aligns with the primary route. The process is detailed as follows:

- V_1: Acts as the first node on the primary path. It evaluates the next hop (*NH*) V_3 for routing towards the destination (*Dest*) V_5. This ensures minimal deviation from the primary path.
- V_2: Functions as an alternative node (*alt*) for V_1 on the backup path. It generates routing information for V_4, which serves as the next hop (*NH*) toward V_5.
- V_3: Operates as an intermediate node on the primary path and determines routing information for its next-next hop (*NNH*) V_5, the final destination.
- V_4: Acts as an alternative to V_3 on the backup path, establishing routing information for V_5 as part of the backup route.

This structured routing framework gives precedence to the primary path while maintaining a secondary route to ensure operational continuity. The protocol continuously refreshes each node's routing table based on current

Table 3 Algorithm notations and their definitions

Notation	Definition
NH	Next hop—the immediate node selected for forwarding the packet
ADJ	Adjacent node—a neighboring node directly connected to the current node
Dest	Destination—the intended recipient node of the transmitted data
NNH	Next-next hop—the node that follows the next hop in the route
Dist	Distance—the spatial or hop-based distance between nodes
alt	Alternate node—a fallback node used in case the primary path fails
sim	Simulation time–the duration over which the network is evaluated
S	Source—the origin node of the data transmission
H	Head node—the node responsible for routing and cluster coordination
Point	Evaluation node—the node currently being assessed during routing

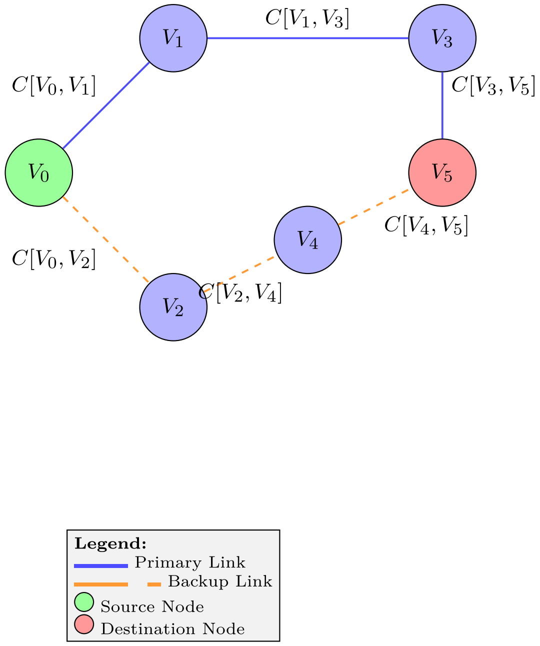


Fig. 3 Illustration of INRwLF routing process showing primary (solid blue) and backup (dashed orange) paths between source and destination

network conditions, allowing for consistent data forwarding even in the presence of node failures or link disruptions. By integrating proactive path management and redundancy, the INRwLF system achieves both robustness and adaptability across diverse IoT scenarios:

1. The primary path ($V_0 \rightarrow V_1 \rightarrow V_3 \rightarrow V_5$) is utilized under normal conditions.
2. The backup path ($V_0 \rightarrow V_2 \rightarrow V_4 \rightarrow V_5$) serves as an alternative when failures or disruptions occur in the primary path.

By leveraging routing information at each node, the INRwLF protocol enhances communication efficiency and minimizes the impact of network failures.

The INRwLF protocol leverages **CRP** packets to gather, relay, and manage routing data. These packets facilitate:

- Monitoring route accessibility between nodes.
- Calculating feasible source-destination paths.
- Managing cluster communication and updates for dynamic routing adjustments.

Each node broadcasts packets containing acknowledgment fields to indicate route status:

- A 1 acknowledgment indicates an available alternative route for backup.
- A 0 acknowledgment signals the unavailability of a backup route.

Upon receiving an acknowledgment, the source node reassesses its neighboring nodes to determine a viable alternate route, thereby sustaining uninterrupted communication with minimal latency. To streamline this process, the protocol constructs a lightweight **CRP** header that encapsulates critical routing information-such as source and destination addresses, acknowledgment flags, and the next-hop identifier. This compact format reduces protocol overhead and enhances overall transmission efficiency.

The process systematically manages clusters by:

- Dynamically updating head nodes (**HEAD**) based on traffic changes.
- Optimizing routes using real-time feedback from adjacent nodes.
- Reducing packet loss by prioritizing nodes closest to the target.

The **CRP** packet mechanism plays a central role in facilitating adaptive cluster operations, supporting dynamic route coordination and scalable communication across IoT infrastructures.

Within this framework, the algorithm targets a selected node-either the designated primary node or a nearby supporting node within the cluster region. The function `search_adjacent` is responsible for initiating CRP packet dissemination, identifying auxiliary nodes that are not currently part of the primary routing pathways utilized by protocols such as OMS-LB, RM-LB, and INRwLF. These auxiliary nodes provide valuable routing flexibility and are instrumental in optimizing intra-cluster forwarding.

To manage information from non-primary nodes, the system utilizes a temporary storage structure, `array_route`, which acts as a buffer for node metadata gathered during the discovery process. This enables the inclusion of alternate forwarding options that would otherwise be overlooked in static routing models. Routing decisions are then based on the contents of this buffer, allowing each node to select the most appropriate next hop (`NextHop`) toward the destination. This process is executed iteratively to ensure progressive data delivery across the cluster.

The CRP-based update system provides continuous routing intelligence by delivering real-time state changes to lead cluster nodes. This mechanism ensures that the `ClusterRoute` remains synchronized with current network conditions, thereby maintaining high routing accuracy. The integration of these operations significantly boosts cluster-level communication efficiency, promoting stability and adaptability in dynamic network environments.

Algorithm 2 Cluster area discovery via CRP packets

```
Input: $S$ (source node), $NearestNode$, $NumberOfAdjacent$
Output: Cluster routing table updated with valid NextHop entries
begin
• Set point ← search_adjacent($S$, $NearestNode$)
• Initialize counter ← NumberOfAdjacent
• while counter $\geq$ NumberOfAdjacent do
    – if array_route[point][adj] $\neq \infty$ then
        * if route[point][adj] = adj and route[point][NextHop] $\neq$ PrimaryAdj then
            · Set NextHop[adj] ← array_route[point + NH][adj]
            · Increment counter ← adj + 1
            · Update ClusterRoute[point][NextHop] ← route[NextHop[adj]][NextHop]
          end if
      end if
  end while
end
```

The total number of **CRP** messages generated during the simulation period is systematically calculated using the formula (14):

$$G_{CRP} = \frac{\sum_{s=i_{to}D}^{N_{Adj}} CRP_s}{\text{Time}} \tag{14}$$

where:

- G_{CRP}: Total number of **CRP** packets generated during the simulation.
- N: Total number of adjacent nodes in the network.
- CRP_s: Number of **CRP** packets generated by node s.

- Time: Total simulation duration.

Each cluster's lead node initiates communication by assigning a default operational state to all member nodes. Initial neighbor discovery and connectivity are established through the transmission of **HELLO** packets, following conventional default routing procedures. However, to reduce signaling overhead, this study introduces an optimization strategy aimed at minimizing **HELLO** packet frequency during the exchange of **CRP** messages.

Simulation outcomes reveal that compact and time-efficient **CRP** packets substantially lower the volume of control traffic, thereby improving protocol efficiency. Nodes located near the cluster perimeter are automatically admitted into the cluster once they satisfy predefined criteria and are detected within the cluster's active range.

Upon receiving a **CRP** message, the node forwards it to the designated cluster head for handling. Two primary scenarios may then follow:

- The cluster head generates a new **CRP** packet in response to internal changes or detected movement within the cluster boundaries.
- If a nearby node enters or exits the cluster area, resulting in a potential connection disruption, the system recalculates route information and redistributes updated control packets accordingly.

Through this responsive mechanism, the protocol not only tracks the volume of control signaling within each cluster but also maintains efficient intra-cluster coordination via a lightweight and adaptive **CRP**-based communication model.

Comparison with prior work (PISP vs. CRP algorithms)

In our previously published work, the PISP focused on predictive packet delivery using lightweight inquiry packets to support route stability in static topologies. While effective, its limitations included the lack of adaptation to dynamic topology changes and absence of real-time cluster feedback.

The current CRP-based Algorithm 2 significantly enhances this foundation. It integrates a cluster-aware discovery mechanism, enabling adaptive route updates and the exclusion of unstable or misbehaving nodes. Unlike PISP, CRP packets gather richer contextual information about node status, adjacency, and route feasibility within active clusters.

As a result, the CRP approach yields improved routing flexibility and network resilience. This is especially critical in large-scale and mobile environments, as reflected in the experimental results, where INRwLF with CRP achieves lower delay and overhead while maintaining higher packet delivery rates compared to the PISP-based method.

5 Simulation experiment

A network simulation was conducted using NS2 to assess the operational efficiency of the proposed **INRwLF** protocol under varying node densities. The simulation environment was tailored to reflect the heterogeneity of real-world IoT deployments, incorporating devices such as ZigBee-enabled sensors, mobile sinks, and IoT gateways-each characterized by unique energy profiles and communication capabilities. These components were clustered in a manner consistent with common configurations used in healthcare monitoring and smart urban infrastructure.

To ensure a realistic evaluation, the simulation incorporated diverse mobility patterns and energy consumption models representative of large-scale IoT ecosystems. The performance of **INRwLF** was benchmarked against established routing protocols, including **OMS-LB** [32] and **RM-LB** [33]. Results indicated that IoT-based nodes running the proposed scheme exhibited improved responsiveness and robustness across multiple connectivity scenarios [37].

Radio propagation was configured with a transmission power of 0.28 watts [38], enabling reliable communication across distances of up to 250 meters. The simulation utilized the IEEE 802.11b standard for multimedia data exchange at the physical and data-link layers. Node mobility followed the Random WayPoint model within a 500×500 m^2 area, reflecting real-time environmental variability. During simulation runtime, nodes dynamically formed clusters, mirroring the adaptive behavior of real-world smart systems.

The simulation was configured with an initial node velocity of 1 m/s, representing a relatively low mobility scenario. While this modest speed yielded limited variability in the current study, its impact will be explored further in future work involving comparative mobility analyses. Each simulation session spanned 500 s and was repeated ten times to ensure statistical consistency, with final results based on average values. Data packets ranged in size from 512 bytes to a maximum of 1024 bytes, and the transmission bitrate was maintained at 2 Mb/s.

Table 4 Simulation parameter

Parameter	Value
Wireless LAN medium access control (MAC)	IEEE 802.11
Maximum range distance between mobile nodes	Up to 550 m
Roaming area	500×500 m^2
Number of nodes test	25,50,100 up to 300
Minimum node speed movement	0 to 40 km/s

A key characteristic of wireless ad hoc networks is the distributed sharing of communication capacity among participating devices. In the first experimental setup, between 200 and 300 nodes were uniformly deployed across the simulation field, ensuring equal distribution within defined cluster zones. The data exchange between source and destination nodes followed a fixed traffic rate of 512 Kb/s. Performance results are visualized in subsequent line graphs, and the associated simulation parameters are summarized in Table 4.

Network efficiency metrics included the packet loss ratio, defined as the fraction of unsuccessfully delivered packets relative to the total packets transmitted, and the average end-to-end delay, representing the mean transmission duration from source to sink.

Prior to evaluating the computational overhead and route reconstruction strategies under dynamic network conditions, it is important to consider the primary contributors to video Quality of Service (QoS). This study highlights three specific factors influencing the delivery and stability of video traffic. Notably, higher node densities were associated with prolonged network lifetime due to more consistent path discovery and maintenance, whereas intermediate and low-density scenarios were more prone to network fragmentation. Furthermore, regions with slower node movement exhibited greater connection stability, supporting extended service continuity.

Once the simulated networks were segmented into clusters, the analysis focused on latency, throughput, and packet delivery ratio as core performance indicators.

Impact of increased device heterogeneity

In our simulation setup (Sect. 5.1), device heterogeneity was modeled within the range of 1–50%, where a portion of nodes possess distinct capabilities in terms of energy, mobility, or communication range. This configuration reflects common real-world IoT deployments. However, increasing heterogeneity to levels such as 60 or 65% may introduce additional routing challenges. In particular, it may lead to less balanced cluster formation, with lower-capability nodes contributing to route instability, increased delay, or localized congestion.

Despite these challenges, the INRwLF protocol is designed with adaptability in mind. Its use of swarm intelligence (PSO, ACO) and trust-based node evaluation enables it to respond to fluctuations in node capability and density. While performance may slightly degrade in extreme heterogeneity, the system is expected to maintain reliable operation. Future work may include a focused empirical analysis on higher heterogeneity scenarios to validate this robustness under more diverse configurations.

5.1 Performance and analyses evaluation

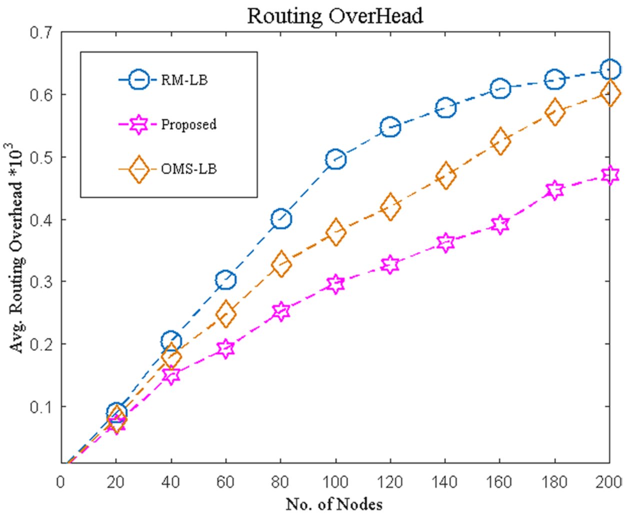
The evaluation environment comprises *N* IoT nodes deployed within a 500 m × 500 m simulation space. The network architecture includes a mixture of static and mobile devices, with mobility introduced in 1–50% of the node population to reflect realistic heterogeneity across operational tiers.

For each cluster, the proposed INRwLF protocol is benchmarked against comparable clustering-based approaches to assess end-to-end route reliability between source and destination nodes. INRwLF determines the effective clustered area by computing inter-node connectivity across the deployment region. Cluster head selection is driven by cumulative node intelligence gathered through **CRP** dissemination, historical node behavior, energy longevity, and database records.

Each node is treated as an autonomous participant within its cluster, enabling localized coordination. When CRP packets detect abnormal conditions-such as instability or connectivity degradation-these updates are relayed to neighboring nodes and processed by the cluster head. The INRwLF protocol incorporates a real-time path validation mechanism to ensure route consistency across multiple clusters, even under rapidly shifting topologies.

A distinguishing feature of INRwLF is its recursive propagation mechanism. As a packet enters a new cluster, the protocol is automatically reinitialized by the receiving head node, extending fault-tolerant routing throughout the communication chain.

Fig. 4 Routing over head



This evaluation compares INRwLF with two established routing strategies: OMS-LB [39] and RM-LB [40], focusing on their relative effectiveness in managing cluster stability and maintaining reliable data transmission paths.

Average routing overhead analysis

Figure 4 compares the average routing overhead for the proposed INRwLF protocol against OMS-LB and RM-LB, across varying node populations. As the number of participating devices increases, INRwLF consistently demonstrates the lowest overhead, attributed to its use of intelligent optimization strategies. Specifically, the integration of Particle Swarm Optimization (PSO) for cluster construction and Optimal Data Gathering (ODG) point selection, combined with Ant Colony Optimization (ACO) for route identification, reduces excess signaling.

By coordinating Mobile Sink (MS) movements through ODG points via an AI-enabled SDN controller, the protocol ensures streamlined path usage and avoids redundant routing decisions. OMS-LB and RM-LB, by contrast, incur higher overhead due to static cluster head configurations and less adaptive route planning. As node count scales from 20 to 200, INRwLF overhead remains within 0.2×10^3 to 0.4×10^3, while OMS-LB ranges from 0.25×10^3 to 0.5×10^3 and RM-LB reaches 0.3×10^3 to 0.6×10^3.

Quantitatively, INRwLF achieves:

- **21% reduction** in routing overhead compared to OMS-LB and **26%** versus RM-LB.
- **20% efficiency gain** over OMS-LB and **31%** over RM-LB in distance-sensitive overhead.

Routing overhead is defined as:

$$RO = \frac{\text{Total Control Packets Exchanged}}{\text{Total Data Packets Delivered}} \tag{15}$$

Where:

- *RO* denotes the routing overhead ratio.
- *Total Control Packets Exchanged* includes all routing-related messages such as **HELLO**, updates, and acknowledgments.
- *Total Data Packets Delivered* counts the packets successfully reaching their destination.

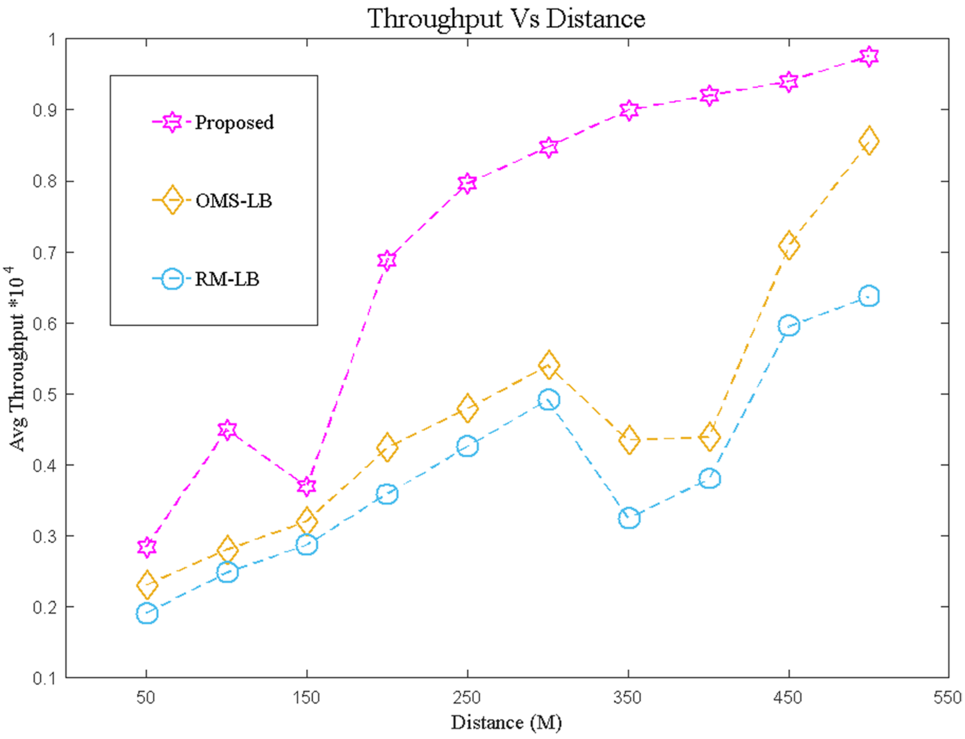
This metric reflects protocol efficiency: lower values indicate more effective network resource utilization.

Average throughput analysis

Figure 5 presents the average throughput measurements for INRwLF in comparison with OMS-LB and RM-LB across a range of communication distances. INRwLF demonstrates superior data transmission performance due to its adaptive Mobile Sink (MS) routing and dynamic cluster head (CH) coordination, augmented by Artificial Bee Colony (ABC) optimization.

Throughput is measured using:

Fig. 5 Throughput comparison



$$T = \frac{\text{Total Data Transferred (bits)}}{\text{Simulation Time (seconds)}} \tag{16}$$

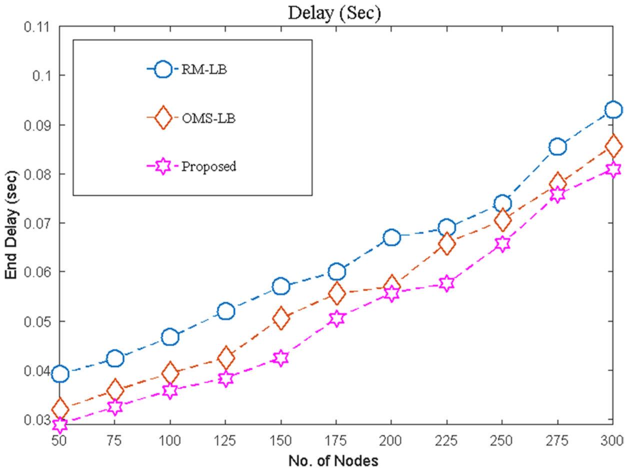
This metric captures the protocol's capacity to deliver data efficiently across the network during the simulation window.

The use of AI-driven control allows INRwLF to prevent congestion at CHs and direct MS movements to optimize data collection. As communication range increases from 50 m to 500 m, INRwLF maintains throughput between 0.4×10^4 and 0.9×10^4, outperforming OMS-LB (0.3×10^4 to 0.7×10^4) and RM-LB (0.2×10^4 to 0.6×10^4).

Performance improvements at maximum distance include:

- **28.6% increase** in throughput over OMS-LB.
- **50% increase** in throughput over RM-LB.

Fig. 6 End-to-end delay comparison



These findings confirm that INRwLF supports higher data rates and more efficient channel usage, making it an effective routing strategy for dense and large-scale IoT deployments.

End-to-end delay analysis

Figure 6 presents a comparative evaluation of end-to-end delay across the INRwLF protocol, OMS-LB, and RM-LB as the node count in the network scales. The proposed **INRwLF: Neighbours Route with Low Fault** framework consistently exhibits reduced latency relative to the baseline protocols. This performance gain is primarily due to the integration of Particle Swarm Optimization (PSO) for Optimal Data Gathering (ODG) point selection and Ant Colony Optimization (ACO) for dynamic path resolution.

The INRwLF algorithm reduces retransmissions and route reinitializations by proactively identifying stable paths, resulting in improved packet delivery efficiency. In contrast, OMS-LB and RM-LB rely on fixed cluster head (CH) assignments and static aggregation points, which often lead to inefficient Mobile Sink (MS) traversal paths and contribute to greater transmission delays.

As network size increases from 50 to 300 nodes, the INRwLF protocol maintains a delay window ranging from approximately 0.03 to 0.08 s, outperforming OMS-LB (0.04 to 0.09 s) and RM-LB (0.04 to 0.10 s). These results emphasize the protocol's ability to uphold low-latency performance under scaling network conditions, making it a strong candidate for delay-sensitive IoT applications such as real-time healthcare monitoring or emergency response systems.

The average end-to-end delay is calculated using Eq. (17):

$$D = \frac{\sum_{i=1}^{N} \left(T_{\text{received},i} - T_{\text{sent},i}\right)}{N} \tag{17}$$

where:

- D is the average end-to-end delay.
- $T_{\text{received},i}$ and $T_{\text{sent},i}$ represent the reception and transmission times of the ith packet, respectively.
- N is the total number of packets transmitted during the simulation.

Network lifetime analysis

The lifetime of a node is defined as the duration for which it remains operational, beginning from the network's initialization until energy depletion. This lifetime is categorized into two distinct phases:

1. **Steady stage:** The interval during which all nodes remain active and no failures are observed.
2. **Unstable stage:** Initiated when the first node exhausts its energy, extending until the final node ceases operation.

Figure 7 depicts the progression of active nodes across simulation rounds, providing insight into the sustainability of the proposed system. The INRwLF protocol demonstrates a prolonged steady stage and slower transition into the unstable phase compared to benchmark protocols. These improvements are primarily driven by integrated load-balancing mechanisms, energy-aware network scheduling, and adaptive clustering based on the INRwLF routing framework.

Formally, network lifetime is defined as:

$$L = T_{\text{first node failure}}$$

where L represents the time elapsed until the initial node depletes its energy reserves.

To quantify overall energy usage, the total consumption across all nodes is evaluated using:

$$E = \sum_{i=1}^{N} \left(P_t \cdot t_t + P_r \cdot t_r\right) \tag{18}$$

where:

- E denotes total energy consumption.
- N is the number of active nodes.
- P_t and P_r represent the transmission and reception power, respectively.
- t_t and t_r denote the duration of transmission and reception phases.

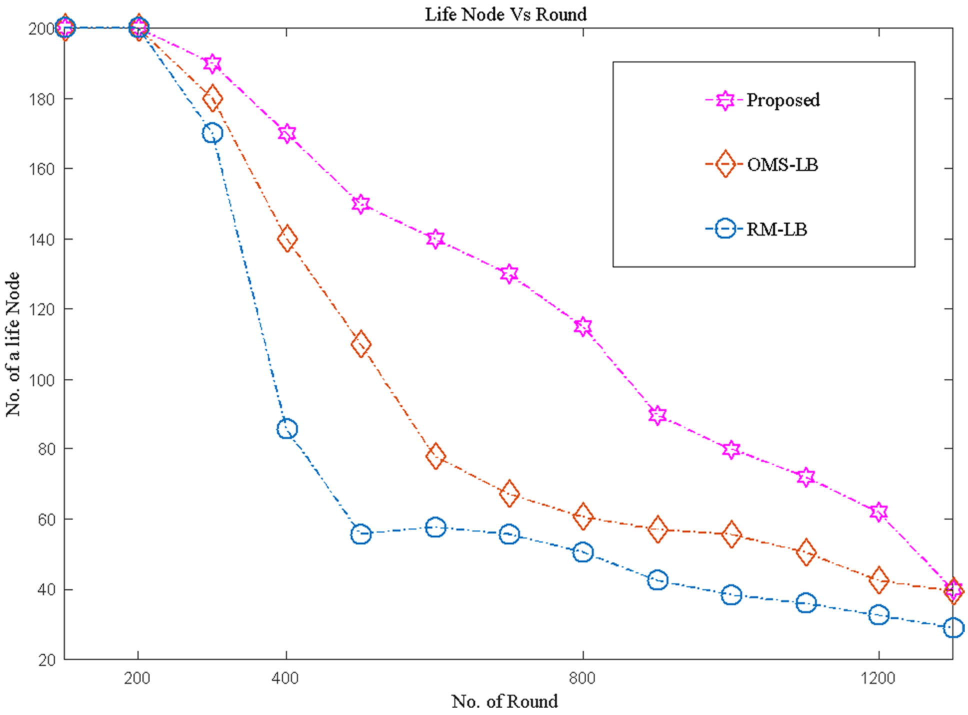


Fig. 7 Number of active nodes over time

Additionally, protocol reliability is evaluated using the packet delivery ratio (PDR), defined as:

$$PDR = \frac{\text{Total Packets Received}}{\text{Total Packets Sent}} \times 100 \tag{19}$$

This metric captures the effectiveness of the routing process in delivering packets to their intended destinations.

Figure 8 presents the continuity of successful data delivery across simulation rounds. The proposed INRwLF protocol delays the first node failure until approximately the 1580 th round, extending the steady operational window significantly. In comparison, OMS-LB exhibits a shorter stable duration, while RM-LB experiences a more rapid decline in node availability.

The INRwLF approach demonstrates improved energy distribution and prolongs overall system function, especially in dense network configurations. The protocol surpasses OMS-LB and RM-LB in terms of longevity, with recorded gains of approximately **50% over OMS-LB** and **90% over RM-LB** in terms of sustained network activity.

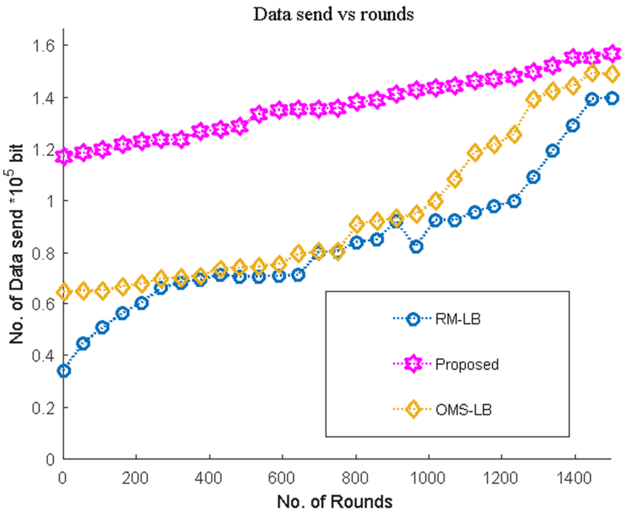


Fig. 8 Continuity of data packet reception

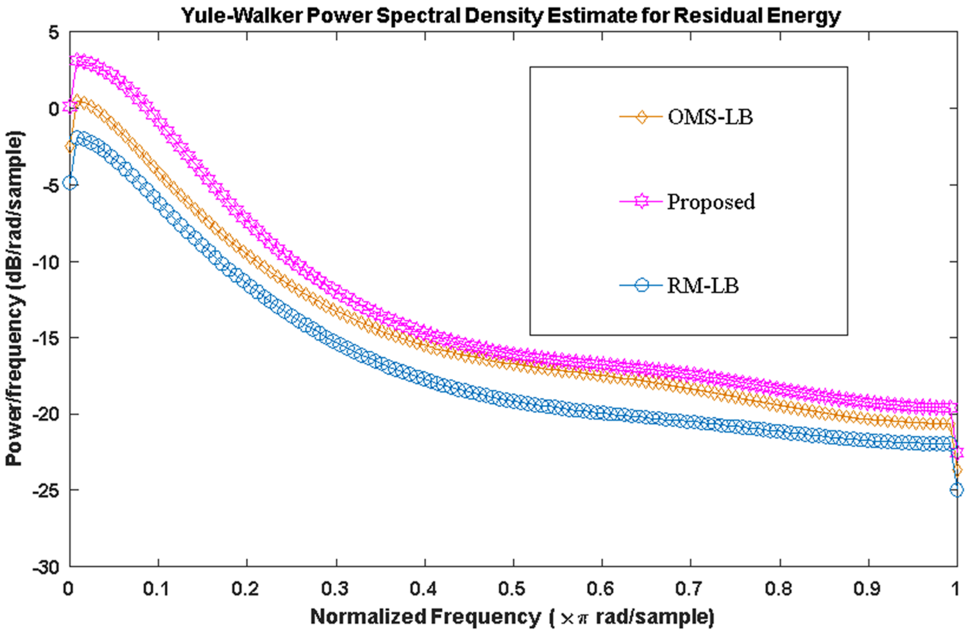


Fig. 9 Comparison energy

Moreover, the data presented in Fig. 8 highlights the protocol's ability to deliver a higher volume of packets successfully, reinforcing its role in supporting reliable and energy-efficient communication over extended operational lifetimes.

Clarification of Yule–Walker power spectral density estimation for residual energy

Figure 9 depicts the Yule–Walker power spectral density (PSD) estimate for the residual energy inside the network. This analysis evaluates the efficacy of three methodologies: OMS-LB, proposed, and RM-LB, concerning normalized frequency ($x\pi$ rad/sample) and their corresponding power/frequency levels (dB/rad/sample). Residual energy trends: The Proposed Method regularly demonstrates superior power spectrum density, signifying enhanced energy retention and utilization optimization relative to other techniques. The OMS-LB Method has middling performance, demonstrating superior energy efficiency compared to RM-LB, although inferior to the Proposed Method. The RM-LB Method has the lowest power spectral density, indicating more energy consumption or less efficiency in energy use.The suggested solution employs an effective energy distribution mechanism, guaranteeing equitable energy usage across all devices and network nodes. This mitigates premature energy depletion at certain nodes, enhancing system lifespan. Effect on system longevity; The suggested strategy enhances system performance by preserving more residual energy, ensuring extended network operation without substantial deterioration. Frequency The PSD curves have a declining tendency as frequency increases, which is characteristic of such systems. The elevated PSD levels of the suggested technique signify enhanced energy distribution and retention over time. Enditemize In conclusion, the suggested technique enhances residual energy efficiency via the uniform distribution of energy consumption, hence prolonging the system's operational lifetime in comparison to OMS-LB and RM-LB.

Throughput vs. mobility analysis

Figure 10 depicts the correlation between throughput and node mobility for the proposed INRwLF method in comparison to the OMS-LB and RM-LB approaches. The findings indicate that the proposed INRwLF system attains markedly superior throughput at diverse mobility speeds, from 0 to 40 km/sec, surpassing both OMS-LB and RM-LB. The graph indicates that when mobility speed escalates, the throughput for all protocols diminishes owing to the heightened difficulty of sustaining stable connections and optimizing routing patterns. Nevertheless, the suggested INRwLF system demonstrates a more progressive reduction in throughput in comparison to OMS-LB and RM-LB. This enhancement is ascribed to the efficient use of AI-driven methodologies, specifically Particle Swarm Optimization (PSO) for dynamic cluster head (CH) administration and Ant Colony Optimization (ACO) for resilient route selection. These systems provide effective data gathering and transmission, even in high-mobility scenarios.

The throughput trends indicate that:

- At low mobility speeds (0–10 km/s), the INRwLF system achieves a throughput of approximately 0.9, compared to 0.8 for OMS-LB and 0.5 for RM-LB.

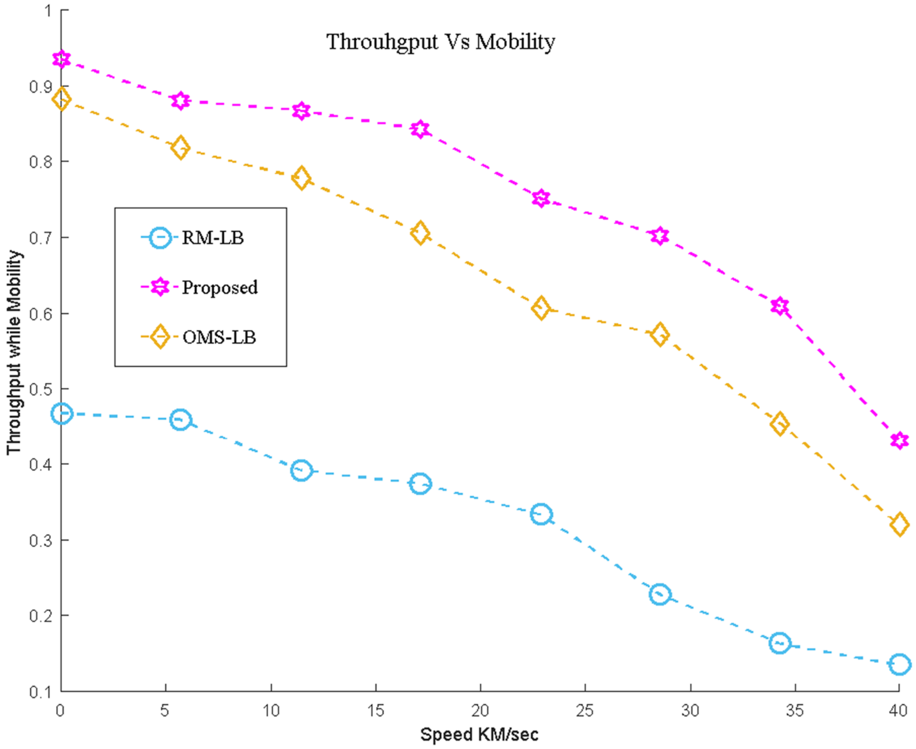


Fig. 10 Nodes with mobility

- At high mobility speeds (35–40 km/sec), the INRwLF system maintains a throughput of approximately 0.7, whereas OMS-LB and RM-LB drop to 0.6 and 0.4, respectively.

The findings underscore the robustness and efficacy of the INRwLF algorithm in managing high-mobility situations, rendering it particularly appropriate for dynamic and extensive IoT networks. The suggested system's capacity to maintain elevated throughput against rising mobility illustrates its resilience in practical situations where node movement is unavoidable.

Comparison with prior work (PISP vs. CRP algorithms)

To provide a comprehensive comparison, Fig. 11 illustrates the average performance of the current CRP-based approach against the previously developed PISP method and a baseline representing other common packet types (e.g., HELLO packets and control packets used in traditional cluster maintenance).

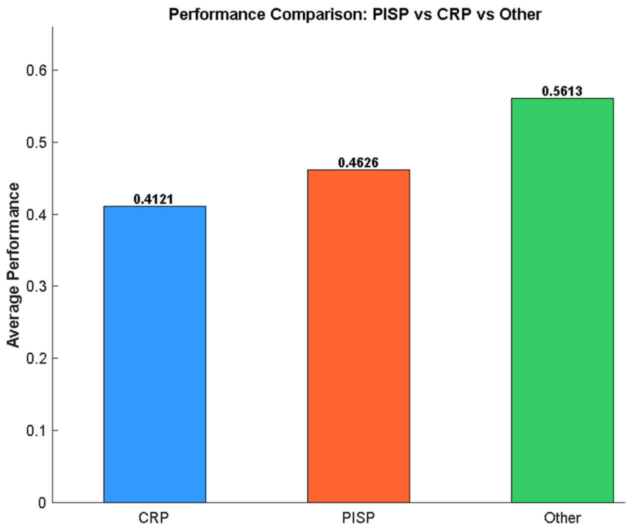


Fig. 11 CRP Vs PISP & other

The PISP strategy, introduced in our earlier work, performed well in static environments where predictive packet transmission ensured low overhead. However, the newly proposed CRP approach outperforms under more realistic dynamic conditions. It enables real-time rerouting and improves fault tolerance by updating cluster route tables in response to link changes and node mobility.

In contrast, the HELLO and control packet-based methods show reduced efficiency, as they lack predictive intelligence and require frequent broadcasts, which increases network overhead. These findings validate CRP's applicability in modern large-scale IoT environments.

6 Conclusion and future work

This paper introduces the INRwLF protocol, a novel energy-efficient routing approach for large-scale IoT networks. By leveraging intelligent clustering, load balancing, and AI-driven optimization, the protocol significantly improves energy efficiency, extends network lifetime, and enhances data reliability. Simulation results demonstrate that INRwLF outperforms existing methods, such as OMS-LB and RM-LB, in terms of throughput, latency, and fault tolerance, making it highly effective in dynamic, resource-constrained environments. While the protocol shows great promise in healthcare and smart city applications, it can also be extended to other critical domains, including industrial automation, agriculture, disaster management, and environmental monitoring.

Future work will build on these findings by addressing emerging challenges and expanding the protocol's capabilities. Integrating 5G technology could enhance scalability, reduce latency, and support massive device connectivity in dense IoT environments. Advanced AI techniques, such as reinforcement learning, may improve real-time decision-making, particularly in dynamic, time-sensitive applications. Strengthening security through the incorporation of blockchain or zero-trust frameworks will help mitigate threats like rank, blackhole, and Sybil attacks. Cross-layer optimization techniques will be explored to improve coordination across network layers, boosting energy efficiency and reducing latency.

Additionally, future efforts will focus on IoT heterogeneity by developing mechanisms to handle diverse device characteristics, ensuring consistent performance across the network. Practical applications beyond healthcare and smart cities-such as industrial automation, precision agriculture, disaster recovery, and environmental monitoring will be explored to validate the protocol's versatility. The integration of edge computing resources will further enhance responsiveness by reducing reliance on centralized systems. Finally, real-world implementations in these domains will provide valuable insights, solidifying INRwLF as a resilient and scalable solution for next-generation IoT systems.

Acknowledgements This research was supported and funded by Arab Open University-Kuwait under decision number 25072.

Author Contributions The author, Radwan S. Abujassar, solely contributed to the conceptualization, methodology, algorithm development, data collection, experimental setup, simulations, result analysis, manuscript writing, editing, and final approval of this work.

Funding No funding available.

Data availability The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Code availability Available upon request.

Declarations

Ethics approval and Consent to participate I have approved there is no conflicts of interest for this study. Not applicable.

Consent for publication Not applicable.

Competing interests The authors declare no competing interests.

References

1. Atzori L, Iera A, Morabito G. The internet of things: a survey. Comput Netw. 2010;54(15):2787–805.
2. Botta A, De Donato W, Persico V, Pescapé A. Integration of cloud computing and internet of things: a survey. Future Gener Comput Syst. 2016;56:684–700.
3. Jin J, Gubbi J, Marusic S, Palaniswami M. An information framework for creating a smart city through internet of things. IEEE Internet Things J. 2014;1(2):112–21.
4. Priyadarshini I, Barik R, Dubey H, Sahoo G. Internet of robotic things: driving intelligent robotics of future-concepts, architecture, applications and technologies. Int J Adv Comput Sci Appl (IJACSA). 2019;10(1):533–41.
5. Oktian YE, Witanto EN, Lee S. A conceptual architecture in decentralizing computing, storage, and networking aspect of IoT infrastructure. Sensors. 2021;21(5):1–20.
6. Venkateshwari P, Subramaniam S. A survey and challenges: embedded system on IoT. In: IoT Based Smart Applications, EAI/Springer Innovations in Communication and Computing. Springer International Publishing; 2022. p. 113–29.
7. Abujassar RS. Enhancing traffic routing inside a network through IoT technology & network clustering by selecting smart leader nodes. Int J Comput Netw Commun (IJCNC). 2024;16(2):1–20.
8. Subramani M, Devi M, Vignesh R, Balaji S, Vimal J. Controlling of embedded based industrial monitoring system using IoT. Mater Today Proc. 2022;62:2928–33.
9. Roberts MK, Ramasamy P. An improved high performance clustering based routing protocol for wireless sensor networks in IoT. Telecommun Syst. 2023;82(1):45–59.
10. Taami T, Azizi S, Yarinezhad R. An efficient route selection mechanism based on network topology in battery-powered internet of things networks. Peer-to-Peer Netw Appl. 2023;16(1):450–65.
11. Ananthi JV, Jose PSH. Performance analysis of clustered routing protocol for wearable sensor devices in an IoT-based WBAN environment. In: Kannadhasan S, Nagarajan R, Karthick A, editors. Intelligent Technologies for Sensors: Applications, Design, and Optimization for a Smart World. Apple Academic Press; 2023. p. 253–70.
12. Anbullam NG, Mary JPP. A survey: energy efficient routing protocols in internet of things (IoT). AIP Conf Proc. 2023;2854(1): 040002.
13. Yalçın S, Erdem E. TEO-MCRP: thermal exchange optimization-based clustering routing protocol with a mobile sink for wireless sensor networks. J King Saud Univ Comput Inf Sci. 2022;34(8):5333–48.
14. Rakesh K, Sharma S, Singh A. SECRPLMS: secure and energy-efficient cluster-based routing protocol for large-scale mobile sensor networks. Wirel Pers Commun. 2023;131(3):2045–63.
15. Sheng Z, Yu B, Liang C, Zhang Y. VPNet: a vulnerability prioritization approach using pointer network and deep reinforcement learning. In: Digital Forensics and Cyber Crime (ICDF2C 2022), vol 489. Springer; 2023. p. 307–25.
16. Jazebi SJ, Risa AG. Routing scheme for internet of things using shuffled frog leaping optimization algorithm. J Ambient Intell Humaniz Comput. 2020;11(11):4457–73.
17. Sulakshana G, Kamatam GR. Data acquisition through mobile sink for WSNs with obstacles using support vector machine. J Sens. 2022;2022:1–12 (**Retracted paper**).
18. Smith T, Zotta R-M, Boulton CA, Lenton TM, Dorigo W, Boers N. Reliability of resilience estimation based on multi-instrument time series. Earth Syst Dyn. 2023;14(1):173–83.
19. Yuan F, Zhang Y, Zhang J. IoT technology for intelligent management of energy, equipment and security in smart house. Int J Adv Comput Sci Appl. 2023;14(1). https://doi.org/10.14569/IJACSA.2023.0140118
20. Jafri MR, Javaid N, Javaid A, Khan ZA. Maximizing the lifetime of multi-chain PEGASIS using sink mobility. World Appl Sci J. 2013;21(9):1283–9.
21. Simaremare H, Syarif A, Abouaissa A, Sari RF, Lorenz P. Performance comparison of modified AODV in reference point group mobility and random waypoint mobility models. In: 2013 IEEE International Conference on Communications (ICC). IEEE; 2013. p. 2135–9.
22. Kao C-C, Yeh C-N, Lai Y-T. Low-energy cluster head selection for clustering communication protocols in wireless sensor network. Int J Comput Appl. 2011;33(1):9–14.
23. Al-Shaikh A, Khattab H, Al-Sharaeh S. Performance comparison of LEACH and LEACH-C protocols in wireless sensor networks. J ICT Res Appl. 2018;12(3):219–36.
24. Shafiq M, Ashraf H, Ullah A, Masud M, Azeem M, Jhanjhi NZ, Humayun M. Robust cluster-based routing protocol for IoT-assisted smart devices in WSN. Comput Mater Continua. 2021;67(3):3505–21.
25. Udayaprasad PK, Shreyas J, Srinidhi NN, Dilip Kumar SMN, Dayananda P, Askar SS, Abouhawwash M. Energy efficient optimized routing technique with distributed SDN-AI to large scale I-IoT networks. IEEE Access. 2024;12:2742–59.
26. Tuli S, Mirhakimi F, Pallewatta S, Zawad S, Casale G, Javadi B, Yan F, Buyya R, Jennings NR. Ai augmented edge and fog computing: trends and challenges. J Netw Comput Appl. 2023;216: 103648.
27. Al-Jamali NAS, Al-Raweshidy HS. Smart IoT network based convolutional recurrent neural network with element-wise prediction system. IEEE Access. 2021;9:47864–73.
28. Shinde R, Shinde SN. Hybrid optimization technique for multipath routing mechanism in internet of things. In: Proceedings of the International Conference on Artificial Intelligence and Cyber Security (IACIDS). EAI; 2024.
29. Chatterjee C, Ghosh S, Buyya R. Multi-path routing based on ant colony optimization in satellite networks for SDN. IEEE Access. 2021;9:45678–89.
30. Torkzadeh S, Soltanizadeh H, Orouji AA. Energy-aware routing considering load balancing for SDN: a minimum graph-based ant colony optimization. Clust Comput. 2021;24(3):2293–312.

31. Farsi B, Amayri M, Bouguila N, Eicker U. On short-term load forecasting using machine learning techniques and a novel parallel deep LSTM-CNN approach. IEEE Access. 2021;9:31191–212.
32. Mohammed MA. Energy optimization approach in wireless sensor network. J Al-Qadisiyah Comput Sci Math. 2024;16(3):111–27.
33. Al-Obady ASH, Al-Janabi T, Mutlag AH. Development of an energy efficient routing protocol based on the diversity of site temperature and recent technologies for IoT applications. Int J Wirel Microwave Technol. 2022;12(1):1–11.
34. Faheem M, Kuusniemi H, Eltahawy B, Bhutta MS, Raza B. A lightweight smart contracts framework for blockchain-based secure communication in smart grid applications. IET Gener Transm Distrib. 2024;18(3):625–38.
35. Faheem M, Al-Khasawneh MA, Khan AA, Madni SHH. Cyberattack patterns in blockchain-based communication networks for distributed renewable energy systems: a study on big datasets. Data Brief. 2024;53: 110212.
36. Adi PDP, Kitagawa A. Quality of service and power consumption optimization on the IEEE 802.15.4 pulse sensor node based on internet of things. Int J Adv Comput Sci Appl. 2019;10(5):144–53.
37. Ali AA, Hussein MK, Subhi MA. A classifier-driven deep learning clustering approach to enhance data collection in MANETs. J Cybersecur Privacy. 2024;3(3):45–60.
38. Sathish K, Hamdi M, Chinthaginjala R, Pau G, Ksibi A, Anbazhagan R, Abbas M, Usman M. Reliable data transmission in underwater wireless sensor networks using a cluster-based routing protocol endorsed by member nodes. Electronics. 2023;12(6):1287.
39. Al-Turjman F, Malekloo A. A centralised routing protocol with a scheduled mobile sink-based ai for large scale I-IoT networks. J Netw Comput Appl. 2018;123:1–11.
40. Kumar P, Lee HJ. Reliable multipath load balancing protocol for wireless sensor networks. Int J Distrib Sens Netw. 2014;10(5):1–11.