International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/44 Volume 12, Issue 5, September – October (2025)

RESEARCH ARTICLE

Resilient and Self-Healing Wireless Communication Using SQUIMONET for Energy-Efficient and Role-Aware WSNs

R. Karthikeyan
Department of Information Technology, Bharathiar University, Coimbatore, Tamil Nadu, India.
✉ karthikeyanrkrish@gmail.com

R. Vadivel
Department of Information Technology, Bharathiar University, Coimbatore, Tamil Nadu, India.
rvadivelit@buc.edu.in

Received: 27 June 2025 / Revised: 18 September 2025 / Accepted: 29 September 2025 / Published: 30 October 2025

Abstract – Wireless Sensor Networks (WSNs) have become vital in enabling autonomous environmental monitoring, infrastructure management, and mission-critical field operations. These networks often face persistent challenges such as uneven energy usage, frequent node failures, and dynamic topology shifts, which collectively threaten long-term reliability. Addressing these issues, this work introduces Squirrel-Monkey Network (SQUIMONET), a bio-inspired routing methodology that leverages instinctive behaviors observed between Malabar squirrels and forest monkeys to design a role-aware communication framework. In SQUIMONET, sensor nodes dynamically alternate between two primary roles squirrel for sensing and forwarding, and monkey for coordination and routing based on contextual parameters like residual energy and network awareness. This role-driven collaboration enables adaptive routing, self-healing capabilities, and efficient energy management across varying network conditions. The proposed approach operates without centralized control, allowing the network to remain functional and responsive, even in the face of partial failures or unpredictable node behavior. The framework offers a sustainable solution for real-world sensor deployments where robustness and longevity are essential.

Index Terms – Monkey-Squirrel Optimization, Role-Based Communication, Self-Healing Networks, Energy Efficiency, SQUIMONET, WSN.

1. INTRODUCTION

In recent decades, the rise of interconnected digital systems has led to an intensified focus on the design and operation of intelligent networks. A network, in its most basic form, has served as a system of interconnected devices or nodes that have been able to exchange information or share resources efficiently. These networks have typically included computers, sensors, communication protocols, and infrastructure that have enabled seamless interaction [1]. In practical deployments, networks have functioned as backbones for data transmission, allowing real-time updates, remote sensing, control mechanisms, and collaborative computing. From industrial automation to healthcare monitoring, networks have significantly improved operational intelligence, allowing decision-making systems to respond dynamically based on input signals and sensor data. These networks have moved beyond traditional boundaries, incorporating edge-level intelligence and autonomous routing patterns to handle increasingly complex scenarios and highly dynamic environments [2].

One particularly specialized form of such networks has been Wireless Sensor Networks (WSNs), which have comprised low-cost, low-power sensor nodes capable of collecting, processing, and communicating environmental data without fixed infrastructure. These sensor nodes have typically been distributed over geographic regions to monitor physical or environmental conditions such as temperature, humidity, sound, vibration, or pollutants. The applications of WSNs have spanned across diverse fields, including but not limited to, smart agriculture, disaster warning systems, battlefield surveillance, habitat monitoring, and structural health diagnostics [3]. WSNs have served as the sensory foundation that has empowered digital ecosystems to understand, react to, and optimize real-world conditions. Their capacity to function autonomously with minimal human intervention has made them invaluable in locations that are remote, hazardous, or otherwise inaccessible [4].

WSNs have encountered numerous technical and environmental challenges that have restricted their operational potential. Limited battery life, unpredictable node failures, constrained memory, and restricted computational ability have imposed strict limitations on network longevity and resilience. Variable communication ranges, inconsistent signal strength, and dynamic topologies have further complicated the task of maintaining reliable data transmission [5]. Scalability concerns have emerged in large-scale deployments, where increased node count has resulted in higher communication overhead and interference. Environmental obstructions, interference from co-existing wireless systems, and energy-draining re-transmissions have severely affected overall network performance. Fault tolerance and self-healing capabilities have remained underdeveloped in many traditional protocols, especially under harsh or unpredictable deployment conditions. These pressing issues have necessitated adaptive solutions that can sustain network integrity even as components degrade or fail over time [6].

In response to such persistent challenges, a growing body of research has explored biologically inspired computational models that can mimic survival-driven behaviors observed in nature. Bio-inspired computing has drawn its foundations from natural systems such as animal foraging patterns, microbial interactions, and evolutionary development processes and has utilized these principles to develop decentralized, adaptive, and scalable solutions in network engineering [7]. In WSNs, such algorithms have introduced novel ways of achieving clustering, load balancing, fault detection, and routing by emulating the self-organizing intelligence found in biological entities. Unlike conventional deterministic strategies, bio-inspired mechanisms have embraced stochasticity and resilience, allowing sensor networks to remain functional and energy-aware even in dynamically shifting conditions. This line of research has held promise not only for performance enhancement but also for extending the sustainable lifetime of sensor deployments in practical, often hostile, environments [8].

An interesting ecological relationship that has inspired recent computational frameworks is the commensal association observed between the Malabar giant squirrel and forest monkeys in the Western Ghats of India. The Malabar giant squirrel, known for its arboreal agility and strong territorial memory, has often moved silently through the canopy, alert to potential threats and opportunities. Monkeys, on the other hand, have operated in social groups, creating noise and activity that often unwittingly assisted squirrels in avoiding predators.

This interaction, where one species has benefited without negatively impacting the other, has embodied the principle of opportunistic cooperation. Such behavior has illustrated how distinct roles, when loosely coordinated, can lead to increased environmental awareness and mutual survival. By modeling these behavioral insights computationally, networks have begun to simulate this kind of interaction, aiming to achieve smarter, role-differentiated collaboration among nodes. The intention behind such approaches has been to build WSNs that do not rely solely on rigid protocols but instead evolve and adapt based on internal energy states, local neighbor knowledge, and long-term survivability instincts observed in nature.

1.1. Operational Gaps and Constraints

Sensor-based communication systems have consistently faced difficulties in balancing energy efficiency, network longevity, and fault resilience, especially in real-world environments that remain unstable or unpredictable. WSNs deployed in agricultural fields, forest zones, disaster-prone regions, or industrial plants often experience node failures, irregular link behavior, and sudden topology changes that disrupt continuous data flow. Most conventional routing strategies fail to adapt dynamically once network conditions deviate from their designed assumptions, leading to increased packet loss, energy drain, and system downtime. With limited battery life and restricted computational power, sensor nodes cannot afford frequent retransmissions or static role assignments that accelerate depletion. The lack of cooperative communication and situational awareness among neighboring nodes results in inefficient route selection, ignoring localized network context and node status. These challenges are further intensified when critical data needs to be relayed quickly across regions affected by environmental interference or node isolation. The pressing need is to build a communication model where sensor nodes behave adaptively, cooperate opportunistically, and sustain functionality even under partial failures taking cues from real-world systems where decentralized, instinct-driven collaboration enables survival and task continuity under pressure.

1.2. Strategic Intention and Motivation

The primary intention of this work has centered around constructing a self-reliant and adaptive routing mechanism that supports energy-conscious communication, dynamic role distribution, and fault-tolerant coordination in complex sensor-based deployments. The objective has been to design a lightweight strategy where network elements can independently adjust their behavior based on energy reserves, communication quality, and environmental changes, all while ensuring critical data reaches the intended destination with minimal loss or delay. The design encourages node cooperation that is not static but situational, allowing low-power sensing nodes to rely on more capable neighbors for routing, without overburdening any single participant in the network. What has driven this research has been the clear mismatch between static routing solutions and the dynamic, often harsh realities of field deployments. Observing nature's ability to sustain cooperative systems through instinct, awareness, and role differentiation has triggered the motivation to infuse sensor networks with similar characteristics. This pursuit aims to overcome the rigid constraints of conventional protocols by building trust,

RESEARCH ARTICLE

resilience, and longevity into the very logic of sensor-based communication systems.

1.3. Organization of the paper

The paper is organized into Five sections. Section 1 presents the introduction, motivation and background of the proposed bio-inspired routing for WSNs. Section 2 reviews existing role-based and self-healing protocols, highlighting research gaps. Section 3 explains the SQUIMONET architecture, covering role assignment, clustering, fault recovery, and zone analysis. Section 4 describes the simulation environment, setup used for implementation and the results, focusing on delivery ratio, energy efficiency, delay, fault tolerance, and lifetime improvements. Section 5 concludes the study with key insights and outlines future directions for enhancing adaptability through predictive or mobility-aware routing mechanisms.

2. RELATED WORKS

IRIS-Cycle-Route [9] applies a synchronized low duty cycle to extend node life in long-range WSNs. MAC, routing, and sleep scheduling layers cooperate to ensure selective activation based on traffic demand and energy levels. Time-slotted access prevents collisions, and predictive wake-up scheduling aligns with neighbor activity. Trust-Geese-Route [10] combines adaptive trust evaluation with Snow Geese Optimization (SGO) for secure routing in Mobile Ad Hoc Networks. Trust scores, derived from delivery consistency and behavior, influence path formation. SGO simulates coordinated geese flight, refining route discovery by balancing energy and security. Anomaly detection flags suspicious deviations, triggering immediate re-routing. FRR-Smart-GridPath [11] the Fast Routing Recovery (FRR) mechanism ensures immediate rerouting in smart grid WSNs. It maintains standby paths and triggers rapid switchover on link failure without full discovery. Localized fault detection uses signal degradation and neighbor acknowledgments. Control overhead is minimized by avoiding global floods. DDEA-ACO-Data-Route [12] a hybrid routing protocol merges Discrete Differential Evolution Algorithm (DDEA) with Ant Colony Optimization (ACO) for adaptive data collection. DDEA explores global path variations, while ACO reinforces successful paths using pheromone trails. Routing tables are dynamically updated based on feedback from both modules. The collaboration ensures optimal routing under varying network conditions, making the system suitable for structured health monitoring and smart farming applications requiring consistent data aggregation. ZeroTrust-Satellite-Link [13] applies Zero Trust authentication to Low Earth Orbit satellite communication. Continuous verification replaces static credentials using behavior history, cryptographic challenges, and encrypted token exchanges. Access is granted only after real-time trust validation. The approach ensures dynamic, context-aware security without centralized management, supporting autonomous satellite constellations and orbital relay networks that demand high-assurance data integrity in space-based environments. ZeroTrust-AgriSense [14] integrates a Zero Trust framework into precision agriculture via the mySense platform. Each sensor continuously validates peer interactions using behavior scores, encryption tokens, and anomaly detection. Rule-based blocking halts unverified nodes. The lightweight design supports constrained agri-IoT devices. This ensures secure, autonomous operation in monitoring systems where manual oversight is infeasible, enhancing resilience against spoofing, intrusion, and data compromise. DP-MalDetect [15] merges Differential Privacy with malware detection in IoT environments under a Zero Trust paradigm. Machine learning models detect anomalous traffic patterns, while gradient-level noise preserves data privacy during training. Session-based authentication and identity revalidation enforce access control. A localized response system prioritizes alerts and supports edge-level intrusion detection. Instant-Trust-Detect [16] detects Man-in-the-Middle (MITM) attacks by assigning dynamic trust scores to IoT communication sessions. Metrics like encryption anomalies, latency, and signal fluctuations inform the trust model. Real-time scoring triggers session termination or path reassessment when thresholds fall. Cross-validation with historical data reduces false positives.

HERO-ZeroDay [17] utilizes high-dimensional analysis of network traffic for zero-day attack detection. Traffic tensors capture entropy, time, and cross-layer behavior. Dimensionality reduction (t-SNE, autoencoders) extracts latent features. A classifier distinguishes unseen patterns without relying on known signatures. Dynamic windowing enables real-time data ingestion and prioritizes alerts by impact. IAPN-SecureInfra [18] secures IoT infrastructures using a dedicated Private Access Point Network (IAPN). Isolated subnets enforce communication via rotating credentials and device fingerprinting. Elliptic curve encryption secures data, while routing is managed through tunneled paths monitored by edge controllers. Anomaly detection and device quarantine enhance real-time security. By eliminating public IP exposure, this architecture supports privacy-centric deployments in smart cities and healthcare automation, ensuring resilient and confidential communication.

Resilient-TrustEE [19] integrates a trust-driven, energy-aware routing framework for industrial WSNs. Trust is derived from consistent behavior and past data integrity. Energy metrics combine battery status and link stability for route selection. Fault isolation dynamically reconfigures paths when nodes misbehave or fail. Localized decisions minimize overhead while maintaining latency thresholds. Tailored for mission-critical industries, the system aligns with ISA100 and WirelessHART standards for durable and self-healing operation under harsh conditions.

RESEARCH ARTICLE

Renewable-WSN-Integration [20] explores embedding renewable energy sources into WSNs for autonomous long-term deployment. It evaluates solar, wind, and kinetic harvesting integration, redesigning energy management circuits and storage-aware routing. Applications include solar-powered agriculture and wind-driven pollution sensors. The study details challenges in unpredictable supply and sensor miniaturization. Cross-domain insights from embedded electronics and sustainable design drive the framework's direction. HABC-MD [21] applies a Hybrid Artificial Bee Colony algorithm with Multi-Dimensional optimization for WSN routing. Bee roles evaluate paths based on energy, delay, and link quality. Multidimensional fitness ensures no metric is favored at others' expense. Clustering and multi-path support balance energy loads. The protocol avoids retransmissions and enhances robustness through adaptive decision-making. 3DICA-UAV [22] addresses clustering for UAV-based WSNs, using three-dimensional spatial factors like elevation, velocity, and relative distance. Clusters are dynamically formed with stable heads chosen through mobility prediction. Hierarchical routing within 3D zones reduces re-clustering frequency and enhances data integrity. Lie-Hypergraph-Route [23] employs Lie hypergraph theory for WSNs in environmental monitoring. Hyperedges represent dynamic group connections, allowing multi-node communication paths. Edge weights factor in environmental parameters like temperature or emissions, prioritizing critical data. As environmental changes occur, hypergraph topology is reconfigured in real time. The model accommodates flexible and context-sensitive routing, ensuring relevant information is prioritized. 3DTEO [24] addresses three-dimensional WSN deployment challenges by organizing nodes into 3D clusters. Each node uses its spatial coordinates to optimize transmission range and activation schedule. A dynamic neighbor table tracks link viability, enabling energy-aware adjustments. Signal dispersion across altitude is considered in link metrics. Coordinated sleep cycles reduce energy drain without losing coverage.

Fuzzy-GeoIoT-Route [25] a fuzzy logic-based routing model for IoT-WSNs integrates geographic proximity and energy status to guide data paths. Residual energy, sink distance, and link quality are fuzzified into linguistic variables. Rule sets determine forwarding ranks, while rule weights are adjusted over time for learning. Real-time state updates preserve routing accuracy under dynamic conditions. The lightweight framework minimizes route churn and ensures delivery consistency. LEACH-AHP-Route [26] enhances the classical LEACH model using Analytic Hierarchy Process (AHP) for more deliberate cluster head selection. Multiple criteria energy, proximity to sink, signal quality are assigned weights and evaluated for node suitability. The distributed architecture enables each node to independently compute its priority index, avoiding centralized decision-making. TDMA scheduling reduces idle listening and collisions. NHARSO-IWSN [27] fuses Adaptive-Network-Based Fuzzy Inference Systems (ANFIS) with Reptile Search Optimization (RSO) for energy-aware routing in IoT-based WSNs. ANFIS processes fuzzy inputs such as node delay and link stability to generate route quality scores. RSO refines routing paths by simulating predator-prey search behavior. The system dynamically adapts to changing node density and traffic conditions, triggering re-routing only when performance thresholds are breached.

CR-EH-LIRoute [28] integrates location-aware spectrum mapping and energy-harvesting prediction in cognitive radio WSNs. Nodes select paths based on geographic interference analysis and anticipated energy availability from sources like solar or vibration. Routing decisions prioritize nodes with better spectrum access and higher predicted energy reserves, using a dual-layer decision engine. CBDS2R-UnderRoute [29] Cluster-Based Depth Source Selection Routing (CBDS2R) enhances underwater WSN performance by forming depth-aware clusters. Cluster heads are selected considering vertical sink alignment and residual energy. A source selection mechanism evaluates potential relays to minimize delay and energy drain. Real-time adjustments account for depth shifts and buffer conditions. EE-TLT [30] Energy-Efficient Two-Level Tree-based Clustering (EE-TLT) introduces a dual-hierarchy routing framework in WSNs. Primary clusters contain secondary sub-clusters, reducing long-range transmissions. Primary heads collect from secondary heads, which gather from regular nodes. Dynamic re-clustering responds to energy decay, preventing early failures. Sleep schedules and TDMA-like access reduce idle energy use. WuRx-Fog-Boot-Repair [31] introduces fog-based bootstrapping and failure recovery for Wake-Up Receiver (WuRx)-based WSNs. Fog controllers activate node clusters via wake-up signals, manage routing, and detect failures using real-time network maps. Upon failure, alternate paths are reassigned with minimal control overhead. Rejoining nodes integrate seamlessly. CMR [32] used synchronized sleep-wake scheduling and priority-based multipath routing to support critical traffic in duty-cycled WSNs. Routes have been selected based on urgency, buffer load, and cycle alignment, ensuring time-sensitive data avoids delay. By integrating MAC and network-layer logic, the approach has achieved both energy efficiency and reliable delivery of essential messages in constrained networks. GBOR [33] has applied real-time geo-opportunistic forwarding for underwater WSNs, selecting next hops based on sink distance and link success probability. It has eliminated static routing, adapting dynamically to drift and signal instability. This strategy has reduced retransmissions, supported reliable delivery, and handled disconnections in unpredictable underwater environments. The related existing protocols comparison is shown in Table 1.

RESEARCH ARTICLE

Table 1 Protocols Review Comparison

Name	Methodology	Merit	Gap
IRIS-Cycle-Route [9]	Cross-layer low duty cycle protocol with predictive wakeups	Reduces energy waste and idle time	Lack of evaluation under heavy data loads
Trust-Geese-Route [10]	Trust-based secure routing with Snow Geese Optimization	Combines trust scoring and swarm-based path discovery	Intrusion detection scalability not measured
FRR-Smart-GridPath [11]	Rapid recovery mechanism with pre-computed standby paths	Minimizes delay during link failures	Limited validation in heterogeneous grid nodes
DDEA-ACO-Data-Route [12]	Hybrid DDEA and ACO for data-centric routing	Balances local and global routing decisions	No integration with application-level QoS policies
ZeroTrust-Satellite-Link [13]	Zero Trust model for satellite authentication	Enforces continual identity verification	Not validated on real orbital dynamics
ZeroTrust-AgriSense [14]	Zero-trust model applied to agri-IoT using anomaly scoring	Mitigates sensor spoofing and misuse	Deployment complexity for large farms not studied
DP-Mal-Detect [15]	Differential privacy-enabled malware detection with ML	Protects device data during model training	Real-time detection delay not measured
Instant-Trust-Detect [16]	Trust score assessment for session-level MITM detection	Provides real-time defense against interception	Overhead of session monitoring not benchmarked
HERO-ZeroDay [17]	High-dimensional traffic analysis for zero-day attack detection	Captures previously unseen traffic anomalies	Detection latency under burst traffic not tested
IAPN-SecureInfra [18]	Private APN model for isolated IoT network security	Ensures privacy via traffic isolation and credential rotation	Interoperability with public networks not addressed
Resilient-TrustEE [19]	Trust-based and energy-efficient routing for industrial WSNs	Supports resilient communication in harsh settings	Gap in handling cyber-physical system integration
Renewable-WSN-Integration [20]	Study on linking renewable energy trends with WSN evolution	Aligns WSN development with sustainability goals	No energy model tested under variable conditions
HABC-MD [21]	Hybrid Artificial Bee Colony with multi-dimensional routing	Improves multi-path routing efficiency	Unverified under mobility-constrained environments
3DICA-UAV [22]	3D clustering for UAV networks using spatial improvisation	Handles 3D deployment scenarios effectively	No scalability test under high UAV density

RESEARCH ARTICLE

Lie-Hypergraph-Route [23]	Routing using Lie hypergraph theory with context-based weights	Context-relevant adaptive routing	No comparative study with graph-based methods
3DTEO [24]	3D clustering and topology control using depth metrics	Energy-aware and spatially aware	Unvalidated for vertical mobility
Fuzzy-GeoIoT-Route [25]	Fuzzy logic-based geo-routing using energy and distance	Balances path quality with energy efficiency	No dynamic learning in fuzzy rules
LEACH-AHP-Route [26]	AHP-based cluster head election in distributed LEACH	Improves head selection reliability	No simulation under adversarial noise
NHARSO-IWSN [27]	ANFIS and RSO hybrid for IoT-WSN routing	Combines learning and optimization	No hardware-level simulation
CR-EH-LIRoute [28]	Location-aware, energy-harvesting routing in CR-WSNs	Supports dynamic spectrum and power balancing	Lacks recovery for spectrum handoff failures
CBDS2R-UnderRoute [29]	Depth-aware cluster routing for UWSNs	Minimizes delay and congestion	Tested only in uniform depth zones
EE-TLT [30]	Two-level tree-based clustering for energy saving	Reduces direct transmission cost	No fault-tolerant data merging mechanism
WuRx-Fog-Boot-Repair [31]	Fog-based boot and repair using WuRx triggers	Ultra-low power activation	Fog delay in multi-hop wakeups not benchmarked
CMR [32]	Cross-layer strategy that links MAC sleep scheduling with multipath routing for critical WSN traffic	Delivers urgent data reliably under tight energy constraints using prioritized channel access	Lacks real-time adaptability to sudden topology or traffic pattern changes
GBOR [33]	Geographic and opportunistic routing using proximity and link status for underwater transmission decisions	Minimizes control overhead while increasing reliability in unstable underwater environments	Does not incorporate environmental-aware prediction or adaptive energy balancing for prolonged use

3. THE PROPOSED ROUTING PROTOCOL SQUIMONET

Squirrel-Monkey Network (SQUIMONET) distinctly conveys the underlying ecological dynamics emphasizing opportunistic cooperation, resource efficiency, and adaptability, which mirror the protocol's inherent characteristics such as proactive energy conservation, fault tolerance, self-healing capability, and sustained connectivity.

SQUIMONET the updated version of the BMCVORP for Reliable Data Transmission with Efficient Energy Utilization. The modelling architecture of the proposed SQUIMONET is illustrated pictorially in Figure 1.

3.1. Zone Analysis

Zone analysis in the optimized SQUIMONET routing protocol systematically partitions the entire sensor deployment region into logical subregions, known as zones, to precisely mimic the strategic habitat selection observed in Malabar giant squirrels and monkeys. This partitioning approach ensures optimized connectivity, promoting energy efficiency and simplified management. Inspired by these creatures' natural preference to select distinct and strategic foraging areas, each sensor network zone remains distinctively structured according to node distribution, proximity, available energy, and transmission range. Zones facilitate manageable interactions among nodes, reducing

RESEARCH ARTICLE

energy overhead and communication complexity, resembling how Malabar giant squirrels select secure upper-canopy feeding areas, indirectly influencing monkeys to strategically position themselves beneath, anticipating dropped food.

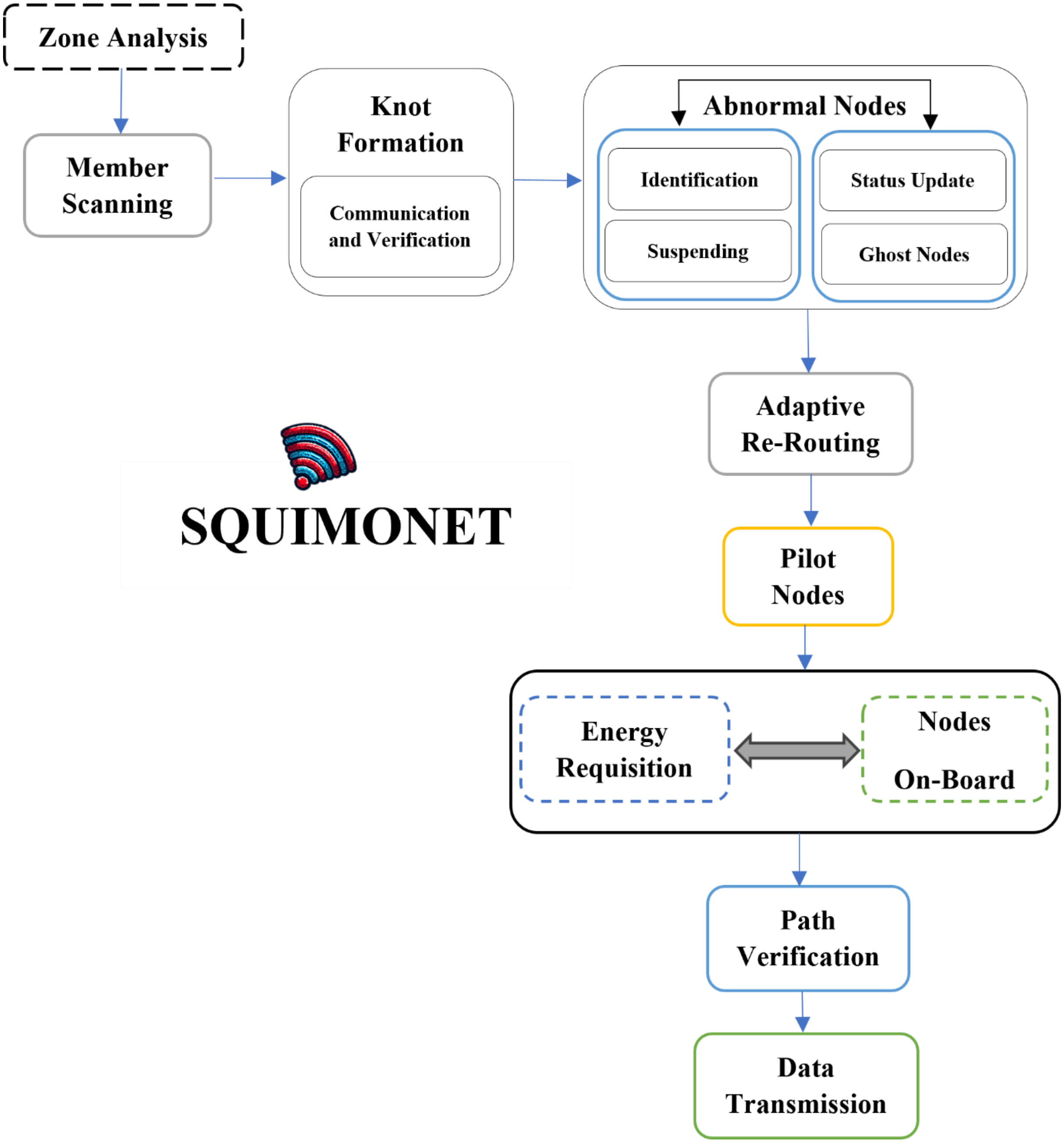

Figure 1 SQUIMONET Architecture

Initially, the total Coverage Area (CA_{total}) of the sensor deployment undergoes precise segmentation into multiple, optimized zones OZ_n.

This segmentation remains directly proportional to network density ρ, communication radius r_c, and network size N_s, expressed mathematically as Equation (1).

$$OZ_n = \frac{CA_{total} \cdot \rho}{N_s \cdot r_c^2} \quad (1)$$

CA_{total} symbolizes the complete physical network coverage area available for sensor deployment, measured in square meters. Network density, represented as ρ, corresponds to the count of active nodes per unit area, reflecting node availability. The communication radius r_c, describes nodes'

RESEARCH ARTICLE

maximum effective communication distance, influencing connectivity among adjacent nodes. The variable N_s denotes the total count of active sensor nodes deployed across the complete network coverage area. Utilizing these parameters, the optimized segmentation strategy ensures each zone effectively facilitates internal node coordination and preserves efficient energy consumption, much like squirrels and monkeys strategically exploit discrete and manageable foraging zones.

After the optimized partitioning, the connectivity factor (F_{Con}) within each zone necessitates calculation to maintain network integrity. Connectivity directly influences energy consumption and communication reliability, significantly impacting routing efficiency. Ensuring high connectivity, the optimized connectivity factor within each zone calculates as shown in Equation (2).

$$F_{Con} = \frac{2 \cdot AcL_{nk}}{Z_n(Z_n - 1)} \quad (2)$$

F_{Con} quantifies the proportion of established direct communication links among nodes relative to the maximum possible direct links within each zone. AcL_{nk} represents the existing active communication links among nodes within the zone. The denominator, $Z_n(Z_n - 1)$, symbolizes the theoretical maximum achievable links, considering every node communicates directly with all other nodes within that zone. Maintaining optimized connectivity mirrors the mutual dependency observed in the commensalism between monkeys and squirrels, ensuring nodes rely effectively on neighbors within a zone, promoting resource sharing, energy efficiency, and robust data transmission paths. The zone analysis thereby strongly aligns with these creatures' adaptive, strategic, and optimized foraging patterns, enhancing network sustainability and resilience.

3.2. Member Scanning

Member scanning within the optimized SQUIMONET routing protocol effectively resembles the behavioral patterns of monkeys and Malabar giant squirrels in their natural habitats. This phase precisely imitates the manner monkeys vigilantly observe squirrels' movements to capitalize on accidental food drops. Each node within the predefined and optimized zones regularly initiates a comprehensive scanning process to identify and update the status of active nodes in immediate vicinity. This scanning behavior allows nodes to strategically determine optimal neighbors, promoting energy efficiency, reducing redundant communications, and enabling rapid adaptation to dynamically changing network conditions, just as monkeys efficiently track squirrels' feeding activities to maximize foraging success.

To maintain an optimized balance between node communication range and energy utilization, each node determines its effective communication distance, known as optimized scanning radius (Rad_{scan}), utilizing nodes' residual energy (E_{res}), initial node energy (E_{init}), and maximum communication radius (Rad_{max}).

$$Rad_{scan} = Rad_{max} \cdot \sqrt{\frac{E_{res}}{E_{init}}} \quad (3)$$

In Equation (3), Rad_{scan} describes the calculated effective range for node scanning, influencing connectivity, efficient neighbor discovery, and adaptive resource management. Rad_{max} represents the maximum communication range inherently supported by sensor nodes, while E_{res} indicates the current residual energy available within a node. The term E_{init} refers explicitly to the initial total energy assigned to sensor nodes upon deployment. By continuously adjusting scanning radius proportionally to remaining energy reserves, nodes strategically optimize their energy consumption, mirroring monkeys' cautious resource investment during opportunistic foraging beneath squirrels.

Following optimized radius determination, nodes perform an energy-efficient membership validation (V_{mem}) by evaluating neighboring nodes based on residual energy (E_{nei}), Link Quality Index (LQI), and historical reliability rating (H_{rr}) expressed in Equation (4).

$$V_{mem} = \alpha \cdot \frac{E_{nei}}{E_{init}} + \beta \cdot \frac{LQI}{LQI_{max}} + \gamma \cdot H_{rr} \quad (4)$$

V_{mem} quantifies the optimized suitability of neighboring nodes for participation within communication and data forwarding tasks. The variable E_{nei} explicitly signifies the neighbor nodes' residual energy availability, reflecting their sustained network contributions. LQI accurately denotes the evaluated quality and stability of direct communication links connecting the node and its neighbor, while LQI_{max} signifies the maximum attainable link quality index. The parameter H_{rr} reflects nodes' historically observed reliability in successfully forwarding and transmitting data without significant packet loss or interference. Parameters ($\alpha, \beta,$ and γ) constitute predefined weighting coefficients strategically adjusted based on specific operational scenarios and performance priorities, ensuring accurate neighbor validation closely resembling the cognitive vigilance of monkeys toward squirrels' consistent resource availability.

Member scanning, strategically integrates continuous updates of network node statuses, mirroring the monkeys' vigilant monitoring of squirrels' foraging behaviors. Regular node scanning optimizes energy utilization, enhances adaptive capabilities to changing network dynamics, and supports efficient decision-making processes crucial for maintaining robust connectivity and efficient energy utilization throughout the optimized SQUIMONET routing protocol.

RESEARCH ARTICLE

3.3. Knot Formation

Knot Formation distinctly embodies the adaptive grouping behavior observed among monkeys actively congregating near Malabar giant squirrels during foraging events. Knot formation precisely reflects this strategic grouping, wherein sensor nodes dynamically establish logical clusters (knots) based on the optimized selection of neighboring nodes, determined from previous member scanning processes. The knots ensure robust intra-group connectivity and optimized resource allocation, significantly improving energy efficiency and reducing unnecessary communication overhead. The dynamic and strategic cluster formation of sensor nodes directly parallels monkeys' sophisticated grouping behavior, aiming to minimize energy expenditure while maximizing the benefits derived from squirrels' accidental resource provisioning.

Initially an optimized metric known as Knot Suitability Index (KSI) guides nodes to identify appropriate grouping partners, computed based on Residual Energy Availability (E_{res}), the average Distance to Neighboring Nodes (D_{avg}), and node density within the optimized Scanning Area (δ). The KSI is calculated as depicted in Equation (5).

$$KSI = \lambda \cdot \frac{E_{res}}{E_{max}} - \mu \cdot \frac{D_{avg}}{D_{max}} + \nu \cdot \frac{\delta}{\delta_{max}} \tag{5}$$

The variable E_{res} precisely denotes a node's available residual energy, and E_{max} reflects the maximum possible energy within network nodes. The parameter D_{avg} symbolizes the average Euclidean distance separating the node from its surrounding neighbors, indicating potential communication overhead. D_{max} signifies the maximum distance threshold allowed within a zone. Node density (δ) measures the number of nodes per optimized scanning area, with δ_{max} representing maximum achievable node density. Weighting coefficients $\lambda, \mu,$ and ν strategically balance the influence of energy availability, proximity, and node density, providing a clear indicator of node suitability for optimized knot membership, resembling monkeys' careful selection of locations beneath feeding squirrels. Subsequent to KSI calculation, nodes effectively establish optimized knots by strategically joining with neighbors possessing higher KSI values, ensuring energy-balanced and communication-efficient clusters. The optimized Energy-Balanced Clustering Cost (CC_{eb}) associated with forming these knots evaluates energy consumption and communication reliability which is expressed in Equation (6).

$$CC_{eb} = \frac{1}{n_k} \sum_{i=1}^{n_k} \left(E_{res_i} - \overline{E_{res}}\right)^2 \tag{6}$$

CC_{eb} with lower values indicating more balanced knots. The parameter n_k explicitly denotes the number of nodes within each knot, while E_{res_i} precisely represents residual energy for node i, and E_{res} refers to the average residual energy of nodes within the respective knot. Ensuring low clustering cost directly promotes optimized energy distribution, preventing rapid energy depletion and node failures. Such strategic and optimized knot formation closely mimics the strategic grouping and positioning behavior of monkeys, who select their gathering spots beneath squirrels based on optimized energy expenditure considerations and reliable resource acquisition. Knot formation within SQUIMONET, thus, optimally leverages node energy resources and enhances adaptive communication efficiency, inspired directly by monkeys' calculated and strategic social aggregation around resourceful squirrels.

3.4. Knot Communication / Neighbor Communication

Neighbor Communication within the optimized SQUIMONET routing protocol significantly emulates the vigilant interactions and strategic communication patterns observed among monkeys closely monitoring Malabar giant squirrels during foraging. In natural scenarios, monkeys precisely depend upon indirect communication cues, carefully observing squirrels to optimize their positioning for dropped food resources. Analogously, sensor nodes within each optimized knot systematically perform proactive and optimized neighbor communication. Nodes exchange crucial operational status information, energy availability, and node reliability indicators. The continuous exchange of accurate, updated information effectively reinforces internal connectivity, ensures robust cluster operations, and enhances the overall reliability of data transmissions. This optimized internal communication mirrors monkeys' vigilant monitoring behaviors, effectively minimizing resource wastage through strategic anticipation of optimal opportunities.

To maintain optimized neighbor communication, nodes within a knot compute a precise Neighbor Communication Interval (T_{nci}), directly influenced by the average residual energy ($\overline{E_{res}}$), network load factor (L_f), and communication urgency indicator (U_{com}).

$$T_{nci} = T_{base} \times \left(\frac{\overline{E_{res}}}{E_{max}}\right) \times \frac{1}{L_f \times U_{com}} \tag{7}$$

In Equation (7), the parameter T_{nci} explicitly represents the optimized interval between neighbor communications, ensuring timely data exchange without unnecessary energy depletion. T_{base} denotes the baseline communication interval, serving as an initial reference determined during network deployment. The variable $\overline{E_{res}}$ symbolizes the mean residual energy level across nodes within each optimized knot, while E_{max} indicates the maximum achievable residual energy. The term L_f corresponds to network load factor, accurately reflecting current node workload and communication traffic density. Communication urgency indicator U_{com} explicitly captures the priority or urgency level associated with data

RESEARCH ARTICLE

being transmitted, guiding nodes to strategically adjust their communication intervals, reflecting monkeys' adaptive positioning based on squirrels' behavioral cues.

Subsequently, nodes evaluate Neighbor Reliability Factor (R_{nei}) during each communication cycle, effectively quantifying neighbor node dependability and stability. This optimized factor accounts for Historical Communication Success Rate (C_{sr}), Current Signal Stability (S_{st}), and Average Energy Deviation (E_{dev}).

$$R_{nei} = \sigma \cdot C_{sr} + \emptyset \cdot \frac{S_{st}}{S_{max}} - \psi \cdot \frac{E_{dev}}{E_{avg}} \tag{8}$$

In Equation (8), R_{nei} precisely reflects optimized neighbor stability and dependability, significantly guiding future communication decisions. C_{sr} effectively records past successful transmissions between communicating nodes, directly contributing toward assessing overall reliability. S_{st} distinctly measures real-time link stability and communication strength between neighboring nodes, normalized against Maximum Attainable Stability Value (S_{max}). Energy deviation (E_{dev}) explicitly signifies the variance in residual energy among neighboring nodes, normalized by average energy (E_{avg}), highlighting nodes experiencing critical energy depletion. The weighting coefficients (σ, ϕ, and ψ) strategically balance reliability, stability, and energy factors, thereby assisting nodes in optimized identification of robust communication links, analogous to monkeys identifying optimal foraging positions through precise observational skills.

This optimized neighbor communication mechanism, inspired precisely by monkeys' vigilant behavioral strategies toward Malabar giant squirrels, ensures consistent internal connectivity, efficient energy management, and adaptive responsiveness. Continuous strategic information exchange optimizes data routing pathways, effectively sustaining robust connectivity, reliability, and energy efficiency throughout the optimized SQUIMONET protocol operations.

3.5. Neighbor Verification

Neighbor verification in the optimized SQUIMONET protocol closely emulates the careful vigilance exhibited by monkeys in continuously observing Malabar giant squirrels' reliability during their foraging activities. Just as monkeys methodically gauge squirrels' dependability based on consistent food-dropping patterns, network nodes periodically validate neighbor nodes' operational stability and reliability. This optimized verification process precisely ensures the integrity of neighbor nodes, safeguarding the network from compromised or faulty connections. The consistent execution of neighbor verification significantly strengthens intra-knot communication reliability, preserves energy efficiency, and prevents inadvertent routing errors. In essence, nodes cautiously evaluate neighbors' consistency, mirroring the adaptive assessment monkeys perform toward squirrels' predictable behavior, thereby optimizing network resilience and connectivity.

During neighbor verification, nodes compute an optimized Neighbor Trust Score (N_{trust}) to measure the dependability of adjacent nodes. This trust score incorporates parameters such as neighbor node Availability Rate (A_{rate}), Packet Acknowledgment rate (P_{ack}), and Security Compliance Level (S_{comp}).

$$N_{trust} = \alpha \cdot A_{rate} + \beta \cdot P_{ack} + \gamma \cdot S_{comp} \tag{9}$$

In Equation (9), N_{trust} precisely represents the cumulative optimized trustworthiness evaluation assigned to each neighbor node. A_{rate} measures the percentage of time a neighbor node actively participates in network communications, reflecting its operational consistency. P_{ack} quantifies how frequently a neighbor successfully acknowledges received transmissions, accurately assessing link reliability. S_{comp} indicates nodes' adherence to predefined security protocols, ensuring uncompromised network interactions. The weighting factors (α, β, and γ) strategically balance these considerations, optimizing neighbor selection and preserving robust intra-network connectivity. The evaluation precisely mirrors monkeys' strategic reliance on consistently dependable squirrel behavior, maximizing their resource-acquisition efficiency.

Subsequently, nodes utilize an optimized Neighbor Stability Index (NSI) to ascertain the long-term stability of neighbor relationships. This index strategically accounts for Historical Node Stability (H_{stab}), Recent Energy Consumption Patterns (RE_{cpat}), and Link Fluctuation Frequency (L_{freq}).

$$NSI = \frac{H_{stab}}{H_{max}} - \eta \cdot \frac{RE_{cpat}}{E_{max}} - \theta \cdot \frac{L_{freq}}{L_{max}} \tag{10}$$

In Equation (10), the NSI reflects optimized predictions of nodes' future stability based on historical behaviors. H_{stab} accurately records the consistency and longevity of previous stable interactions with neighbor nodes, normalized by Maximum Stability (H_{max}). RE_{cpat} indicate nodes' ongoing energy utilization trends, normalized by their Maximum Permissible Energy Limit (E_{max}). L_{freq} quantifies the volatility of connection reliability, normalized by the Highest Recorded Link Fluctuations (L_{max}). The parameters (η and θ) tactically adjust the influence of energy and link stability, facilitating precise stability assessments. This optimized index closely aligns with monkeys' adaptive, observational assessments of squirrels' long-term reliability in consistently providing dropped food resources.

Neighbor verification in SQUIMONET, inspired directly by the meticulous vigilance observed between monkeys and

RESEARCH ARTICLE

Malabar giant squirrels, robustly ensures nodes engage exclusively with trustworthy neighbors. This strategic and optimized assessment process inherently sustains high network reliability, preserves communication effectiveness, and significantly strengthens long-term network resilience.

3.6. Identifying Abnormal Nodes

Identifying abnormal or malicious nodes within the optimized SQUIMONET protocol mirrors the cautious behavior of monkeys meticulously observing deviations in Malabar giant squirrels' foraging actions. In natural ecological scenarios, monkeys instinctively notice subtle irregularities in squirrels' behaviors, such as inconsistent feeding patterns or erratic movements, which serve as crucial indicators of resource instability or potential threats. Similarly, sensor nodes within the network vigilantly monitor their neighbors, promptly identifying unusual behaviors, including unexpected energy depletion rates, irregular communication patterns, or malicious activities like intentional packet dropping. This optimized proactive vigilance precisely safeguards the network from disruptions, maintaining the reliability of data transmissions and preserving optimal connectivity. Such careful observation enhances network resilience and integrity, reflecting monkeys' natural adaptations toward behavioral irregularities in squirrels. To effectively detect abnormal nodes, the optimized SQUIMONET protocol utilizes an Abnormal Node Detection Factor ($ANDF$), calculated by evaluating nodes' Energy Consumption Deviation (E_{cd}), Packet Drop Rate (P_{dr}), and Abnormal Communication Frequency (F_{ab}). The optimized Abnormal Node Detection Factor is depicted in Equation (11).

$$ANDF = \xi \cdot \frac{E_{cd}}{E_{th}} + \kappa \cdot P_{dr} + \chi \cdot \frac{F_{ab}}{F_{max}} \quad (11)$$

The optimized factor ANDF precisely quantifies the likelihood of a node exhibiting abnormal or potentially malicious behavior. E_{cd} explicitly measures the difference between a node's observed energy usage and expected energy expenditure, normalized by an Energy Threshold (E_{th}) predefined based on historical averages. P_{dr} accurately assesses the ratio of packets intentionally or unintentionally discarded by nodes, indicative of compromised communication reliability. F_{ab} explicitly captures irregularities in communication patterns, normalized by the Maximum Abnormal Frequency (F_{max}). Parameters ($\xi, \kappa,$ and χ) are optimized weighting coefficients, strategically set based on network security and reliability requirements. These optimized calculations resemble monkeys' instinctive attention to irregular squirrel behaviors, signaling potential instability.

Upon detecting nodes surpassing the abnormality threshold, nodes compute an optimized Malicious Node Probability (MNP), further assessing their trustworthiness. The optimized malicious probability integrates Historical Anomaly Occurrences (A_{hist}), Failed Authentication Count (F_{auth}), and Inconsistency Factor (I_{fac}).

$$MNP = \frac{\rho \cdot A_{hist} + \tau \cdot F_{auth} + \omega \cdot I_{fac}}{A_{max} + F_{max} + I_{max}} \quad (12)$$

In Equation (12), MNP explicitly represents the probability that a node is deliberately malicious or severely compromised. A_{hist} accurately count previous recorded deviations from standard operational behaviors. F_{auth} precisely tallies the number of unsuccessful identity verification attempts, directly implicating potential malicious intent. The I_{fac} quantifies unpredictable behavioral variations observed over time. Normalizing constants A_{max}, F_{max}, and I_{max} reflect maximum thresholds for anomaly occurrences, authentication failures, and inconsistencies, respectively. Weighting coefficients ($\rho, \tau,$ and ω) are optimized according to network conditions, effectively guiding precise assessments of node integrity. These evaluations closely resemble the strategic observational vigilance of monkeys toward Malabar squirrels' unpredictable or suspicious activities, optimizing resource reliability.

This optimized approach toward identifying abnormal and malicious nodes significantly enhances SQUIMONET's defensive capabilities, ensuring continuous vigilance and immediate recognition of threats. The protocol's meticulous evaluation of deviations from expected behavior, directly inspired by the cautious adaptations observed in monkeys toward squirrels, robustly maintains communication reliability, network integrity, and optimized energy utilization throughout network operations.

3.7. Suspending Abnormal Nodes

The suspension of compromised or malicious nodes within the optimized SQUIMONET routing protocol draws direct inspiration from monkeys' instinctive avoidance of areas characterized by unpredictable or abnormal behaviors exhibited by Malabar giant squirrels. Monkeys naturally adapt to avoid unreliable or potentially harmful regions based on squirrels' erratic feeding or irregular movements. Similarly, nodes identified with elevated abnormality indicators from the previous optimized node identification step undergo immediate suspension from active network participation. By strategically suspending these nodes, the network ensures uninterrupted, optimized communication paths and preserves its overall operational stability. Node suspension, thus, maintains continuous, reliable data transmission by proactively mitigating risks associated with compromised nodes, closely resembling monkeys' avoidance strategy towards resource uncertainty.

An optimized Node Suspension Index (NSI_{sus}) determines precisely when a node should be temporarily excluded from

RESEARCH ARTICLE

network operations. This optimized index mathematically integrates factors such as ANDF, MNP, and Energy Depletion Rate (E_{dr}).

$$NSI_{sus} = \alpha_s \cdot ANDF + \beta_s \cdot MNP + \gamma_s \cdot \frac{E_{dr}}{E_{th}} \quad (13)$$

In Equation (13), NSI_{sus} precisely quantifies the suspension readiness of nodes based on comprehensive evaluations of their reliability and operational health. The ANDF represents previously calculated node abnormality likelihood. MNP accurately quantifies nodes' potential malicious intent, as determined earlier. E_{dr} explicitly assesses nodes' ongoing energy reduction speed, normalized by predefined Energy Thresholds (E_{th}), indicating potential imminent node failure. Weighting coefficients ($\alpha_s, \beta_s,$ and γ_s) have been optimized to prioritize network security, energy efficiency, and communication integrity, closely replicating monkeys' decisive avoidance of unpredictable foraging areas exhibiting abnormal squirrel activities.

Subsequent to suspension decisions, nodes initiate an optimized Suspension Duration (T_{sus}), strategically determining the temporary exclusion period necessary for nodes' detailed diagnostics or energy recovery. The suspension duration calculation explicitly considers nodes' Historical Suspension Frequency (F_{hist}), Severity of Recent Abnormal Activities (S_{act}), and Current Network Security Risk (R_{sec}).

$$T_{sus} = T_{min} + \delta_s \cdot F_{hist} + \epsilon_s \cdot S_{act} + \zeta_s \cdot R_{sec} \quad (14)$$

In Equation (14), T_{sus} defines the precise duration of node suspension, ensuring optimized recovery and evaluation intervals. The parameter T_{min} denotes the minimum suspension duration essential for baseline diagnostics. F_{hist} effectively tracks the number of prior suspensions experienced by the node, reflecting habitual irregularities. S_{act} accurately measures the impact level of recent node misbehavior or energy irregularities on network stability. R_{sec} quantifies current overall security threats influencing network operations. The coefficients ($\delta_s, \epsilon_s,$ and ζ_s) have been optimized based on historical network performance and stability requirements, ensuring adaptive suspension durations. Such suspension durations effectively parallel monkeys' strategic intervals between revisiting unreliable feeding sites, enabling sufficient assessment and risk mitigation.

This optimized suspension mechanism significantly preserves network integrity, enhances security, and maintains energy efficiency by temporarily isolating unreliable or compromised nodes. Directly inspired by monkeys' careful behavioral adaptations toward abnormal activities of Malabar giant squirrels, the optimized node suspension strategy ensures uninterrupted, reliable network operations, preserving overall connectivity and robust communication pathways within the optimized SQUIMONET routing protocol.

3.8. Ghost Nodes

The implementation of Ghost Nodes within the optimized SQUIMONET routing protocol distinctively mirrors the cautious behaviors displayed by monkeys toward unreliable foraging areas associated with unpredictable or inconsistent Malabar giant squirrel activities. Just as monkeys temporarily avoid, yet carefully monitor areas where squirrels exhibit inconsistent feeding behaviors, sensor nodes identified and suspended due to abnormal or malicious activities assume a “ghost” state. Ghost Nodes operate under optimized constraints, maintaining minimal network presence to preserve topological awareness without actively participating in data transmission. This state optimally reduces network vulnerability and resource wastage, ensuring nodes remain passively monitored without compromising the network’s operational integrity. The adoption of ghost states strategically reflects monkeys’ cautious yet vigilant observation strategies toward potentially unstable squirrel feeding spots.

Ghost Nodes possess an optimized Communication Suppression Factor (C_{sf}), explicitly governing their reduced interaction level within the network. This optimized factor precisely balances minimal presence for continued monitoring while significantly limiting operational participation.

$$C_{sf} = 1 - \frac{\eta_g \cdot E_{resi}}{E_{init}} - \frac{\theta_g \cdot NR_{risk}}{R_{max}} \quad (15)$$

In Equation (15), C_{sf} explicitly quantifies the suppressed communication participation level of ghost-state nodes. Residual Energy (E_{resi}) precisely denotes ghost nodes’ remaining energy, compared to their Initial Deployment Energy (E_{init}), accurately reflecting nodes' resource capabilities. Network Risk Ratio (NR_{risk}) evaluates ghost nodes' assessed threat level toward network security and communication stability, normalized by Maximum Potential Risk (R_{max}). Optimized Weighting Parameters (η_g, and θ_g) tactically balance residual energy conservation against potential security risks, allowing ghost nodes to remain passively visible but minimally interactive. This optimized management precisely mirrors monkeys’ minimal yet cautious interaction strategy toward unpredictable squirrels' behaviors, ensuring continuous environmental awareness without unnecessary energy expenditure.

To strategically maintain network topological information, ghost nodes periodically broadcast an optimized Status Beacon (B_{gn}), minimally indicating their passive presence. This Optimized Beacon Interval (T_b) directly depends upon ghost nodes’ Abnormality Level (A_{lvl}), Average Energy Reserve within Knot ($\overline{E}_k$), and current Network Load Index

RESEARCH ARTICLE

(L_{idx}). The beacon interval determination is represented as Equation (16).

$$T_b = T_{gmin} + \mu_g + A_{lvl} + \nu_g \cdot \frac{\overline{E}_k}{E_{max}} + \emptyset_g \cdot L_{idx} \quad (16)$$

The T_b precisely defines the strategic frequency at which ghost nodes minimally announce their continued passive presence within the network. The Baseline Interval T_{gmin} denotes a predefined Minimum duration between Beacon Transmissions, ensuring optimized minimal network intrusion. A_{lvl} precisely quantifies ghost nodes' assessed irregular behavior severity. $\overline{E}_k$ indicates the energy state of neighboring active nodes, reflecting their capacity to tolerate minimal ghost node presence. L_{idx} evaluates ongoing network activity levels, influencing nodes' allowable beacon frequency. Weighting parameters (μ_g, ν_g, and $\emptyset_g$) have been optimized strategically, balancing minimal beacon transmissions against network awareness requirements. This strategic minimalistic communication parallels monkeys' subtle yet continuous monitoring of unstable squirrel activities, facilitating vigilant risk assessments.

Thus, ghost nodes, through optimized minimal communication strategies, precisely emulate monkeys' cautious yet vigilant interactions toward unreliable feeding grounds influenced by unpredictable squirrel behavior. The optimized ghost node approach effectively balances passive network participation, continuous monitoring, and resource conservation, significantly enhancing overall network resilience, connectivity, and stability within the optimized SQUIMONET routing protocol.

3.9. Status Updation

Status updation within the optimized SQUIMONET routing protocol meticulously replicates monkeys' persistent monitoring and adaptive reassessment of Malabar giant squirrels' feeding status. Monkeys continuously reassess resource stability by closely observing squirrels' foraging consistency and reliability, dynamically adjusting their positions accordingly. Analogously, network nodes regularly broadcast their updated operational status, energy levels, and security information to neighboring nodes within their respective optimized knots. Regular and optimized status exchanges effectively ensure each node maintains precise, real-time awareness of its environment, facilitating robust decision-making, optimal energy management, and secure communication. These frequent updates strategically sustain network stability, connectivity, and responsiveness, strongly reflecting monkeys' continuous adaptive vigilance toward the squirrels' behavioral changes.

The frequency of optimized status updates, represented as the Status Update Interval (T_{su}), strategically depends upon nodes' Residual Energy Availability (E_{res}), Recent Network Condition Variability (V_{net}), and Security Priority Level (P_{sec}).

$$T_{su} = T_{base} \times \left(\frac{E_{max}}{E_{res}}\right)^{\lambda^u} \times (1 + \mu_u + V_{net} + \nu_u \cdot P_{sec}) \quad (17)$$

In Equation (17), T_{su} precisely signifies the calculated duration between status update transmissions, ensuring optimal frequency without causing energy inefficiency. The Baseline Interval (T_{base}) explicitly provides an initial reference duration. E_{res} explicitly indicates remaining power levels, while E_{max} symbolizes Maximum Node Energy, guiding adaptive adjustments of update intervals. Network Condition Variability (V_{net}) quantifies recent environmental or operational changes, such as topology shifts or fluctuating communication patterns. P_{sec} represents the immediate security sensitivity of the network environment, influencing optimized update frequency. Weighting factors (λ_u, μ_u, and ν_u) have been strategically optimized to balance energy consumption, adaptability, and security considerations. These dynamic adjustments parallel monkeys' continuously adaptive assessments of squirrel behavior changes, optimizing positional decisions.

Further, nodes calculate an optimized Status Relevance Factor (SRF) to precisely quantify the significance of each broadcasted status update. The factor strategically incorporates Recent Status Change Magnitude (M_{chg}), Node Criticality Index (C_{idx}), and Proximity Relevance (P_{rel}). The optimized mathematical expression for calculating Status Relevance Factor is shown in Equation (18).

$$SRF = \alpha_u \cdot \frac{M_{chg}}{M_{max}} + \beta_u \cdot C_{idx} + \gamma_u \cdot \frac{1}{P_{rel}} \quad (18)$$

SRF explicitly evaluates the optimized importance of status updates, ensuring efficient and relevant dissemination of critical information. M_{chg} accurately reflects significant variations in nodes' energy levels, operational status, or security alerts, normalized by the Maximum Observed Change (M_{max}). C_{idx} precisely quantifies nodes' strategic importance in maintaining connectivity and overall knot integrity, assigning higher relevance to pivotal nodes. P_{rel} explicitly considers nodes' spatial closeness, inversely influencing relevance, ensuring updates remain optimized and localized. Weighting coefficients (α_u, β_u, andγ_u) have been strategically optimized, emphasizing significant operational changes, node importance, and spatial proximity. This precise relevance evaluation accurately mirrors monkeys' selective attention towards notable squirrel behavioral cues, optimizing efficient energy usage.

Through frequent and precisely optimized status updation, nodes sustain a consistently adaptive and vigilant network environment, accurately reflecting monkeys' strategic

RESEARCH ARTICLE

behavior monitoring Malabar giant squirrels. These optimized periodic exchanges effectively maintain real-time awareness, robust network stability, and secure, efficient connectivity, strategically reinforcing the operational effectiveness and adaptive reliability of the SQUIMONET protocol.

3.10. Adaptive Re-Routing

Adaptive re-routing within the optimized SQUIMONET routing protocol distinctly mimics monkeys' flexible positioning adjustments triggered by inconsistent behaviors of Malabar giant squirrels during feeding. Naturally, monkeys carefully adapt their locations based on squirrels' unpredictable resource-dropping patterns, swiftly responding to changes for optimized resource acquisition. Similarly, sensor nodes dynamically adapt routing paths whenever network disruptions, such as suspended nodes or energy-depleted neighbors, occur. Optimized adaptive re-routing precisely ensures uninterrupted data transmission, efficient energy management, and sustained network connectivity. Nodes strategically employ updated information from previous optimized status updates, swiftly recalculating alternative routing paths upon detecting abnormal behaviors or network inconsistencies. This adaptive strategy directly parallels monkeys' agile positional adjustments, optimizing both energy expenditure and network robustness.

During adaptive re-routing, nodes strategically compute an Optimized Route Recovery Index (RRI) to rapidly select the most suitable alternate routes. This optimized index explicitly integrates critical factors including available Neighbor Node Reliability (R_{nei}), Current Path Latency (L_{cur}), and Remaining Energy Reserves of potential relay nodes (E_{rem}).

$$RRI = \frac{\delta_r \cdot R_{nei}}{R_{max}} - \frac{\epsilon_r \cdot L_{cur}}{L_{max}} + \frac{\zeta_r \cdot E_{rem}}{E_{max}} \tag{19}$$

In Equation (19), the RRI precisely quantifies the suitability and efficiency of candidate paths for adaptive re-routing. R_{nei} indicates trustworthiness and stability of nodes along potential alternate paths, normalized by Maximum Achievable Reliability (R_{max}). L_{cur} explicitly measures delays associated with alternative routes, normalized against Maximum allowable Latency (L_{max}). E_{rem} accurately reflect the collective energy availability of nodes along proposed routes, normalized by the Maximum Node Energy Capacity (E_{max}). The weighting coefficients (δ_r, ϵ_r, and ζ_r) are strategically optimized, prioritizing path reliability, latency minimization, and energy conservation. These calculations precisely parallel monkeys' strategic repositioning in response to squirrels' unpredictable foraging patterns.

An Optimized Alternative Path Stability (APS) calculation ensures selected routes provide sustained reliability. This optimized stability assessment explicitly accounts for Historical Path Success Rate (S_{hist}), Node Density along Alternative Paths (D_{alt}), and Recent Network Stability Fluctuation (F_{stab}).

$$APS = \alpha_r \cdot S_{hist} + \beta_r \cdot \frac{D_{alt}}{D_{max}} - \gamma_r \cdot \frac{F_{stab}}{F_{max}} \tag{20}$$

In Equation (20), APS explicitly measures long-term reliability and robustness of potential adaptive routes. S_{hist} accurately indicates previous routing performance records, guiding future stability predictions. D_{alt} normalized by maximum achievable density D_{max} , directly influences potential route robustness and network coverage. F_{stab} explicitly measures recent variations in communication reliability and route stability, normalized by Maximum Recorded Fluctuations (F_{max}). The optimized weighting coefficients (α_r, β_r, and γ_r) strategically prioritize route dependability, adequate node coverage, and minimal instability, ensuring sustained network reliability. Such optimized calculations strongly resemble monkeys' adaptive behavior to select consistently dependable resource locations based on previous successful experiences.

Through optimized adaptive re-routing, nodes swiftly and strategically adjust to unexpected disruptions or abnormalities, maintaining efficient, reliable network connectivity. The adaptive behavior inspired directly by monkeys' agile responses toward unpredictable Malabar giant squirrels' activities significantly enhances overall robustness, optimized energy utilization, and dependable data transmission within the optimized SQUIMONET protocol framework.

3.11. Pilot Nodes on Duty

Pilot Nodes on Duty within the optimized SQUIMONET routing protocol emulate the decisive roles dominant monkeys adopt during interactions influenced by Malabar giant squirrels' feeding patterns. Observational studies indicate that certain monkeys strategically assume authoritative positions, carefully directing group movement and decision-making when squirrel feeding events occur unpredictably. Similarly, specialized sensor nodes, designated as optimized Pilot Nodes, assume crucial responsibilities within network clusters, dynamically overseeing optimized routing, resource allocation, energy balancing, and security management. These nodes possess enhanced capabilities and strategically positioned roles, carefully managing intra-knot communication and energy resources to maintain optimal connectivity. Inspired directly by monkeys' authoritative decision-making behavior, Pilot Nodes precisely guide network clusters through varying operational conditions, ensuring stability and optimized efficiency.

Pilot Nodes selection employs an optimized Pilot Node Selection Metric (PNSM), computed strategically considering

RESEARCH ARTICLE

Node Residual Energy (E_{res}), Historical Reliability Index (R_{hist}), and Node Connectivity Degree (C_{deg}).

$$PNSM = \lambda_p \cdot \frac{E_{res}}{E_{max}} + \mu_p \cdot R_{hist} + \nu_p \cdot \frac{C_{deg}}{C_{max}} \quad (21)$$

In Equation (21), PNSM explicitly quantifies nodes' suitability and capability to effectively serve as optimized Pilot Nodes. Residual Energy (E_{res}) indicates the available power reserves for extended management duties, normalized by maximum energy capacity (E_{max}). Historical reliability index (R_{hist}) accurately measures nodes' proven stability and successful past performance in managing communications and resource allocation, thus ensuring consistent dependability. C_{deg} assesses nodes' direct communication links within the optimized knot, normalized against maximum possible connectivity (C_{max}). Optimized weighting coefficients (λ_p, μ_p, and ν_p) strategically balance energy sustainability, reliability, and optimal connectivity, resembling dominant monkeys' authoritative selection based on strength, reliability, and central positioning.

Pilot Nodes further employ an optimized Duty Rotation Interval (T_{dri}), managing strategic role rotations among capable nodes, effectively balancing resource utilization and workload distribution. Duty rotation interval explicitly integrates Average Energy Depletion Rate (E_{avgd}), Pilot Node Workload Index (W_{idx}), and Network Condition Variability (V_{cond}).

$$T_{dri} = T_{rotbase} + \delta_p \cdot \frac{E_{avgd}}{E_{th}} + \epsilon_p \cdot W_{idx} + \zeta_p \cdot V_{cond} \quad (22)$$

In Equation (22), T_{dri} defines the optimized duration each Pilot Node remains actively on duty before strategic role reassignment occurs. Base rotation interval ($T_{rotbase}$) denotes minimum duty period, ensuring stability and consistency during management transitions. E_{avgd} explicitly quantifies Pilot Nodes' typical energy consumption levels, normalized by defined Energy Threshold (E_{th}), influencing nodes' operational sustainability. W_{idx} accurately assesses the intensity of management tasks assigned to the node, guiding balanced workload distribution. V_{cond} explicitly measures recent fluctuations in network topology or communication load, impacting nodes' operational intensity. Optimized weighting factors (δ_p, ϵ_p, and ζ_p) carefully prioritize sustainable energy utilization, balanced workload allocation, and adaptive responsiveness, precisely reflecting dominant monkeys' strategic rotation of authoritative roles based on situational demands.

Through optimized Pilot Node management, including strategic selection and efficient duty rotation, nodes effectively replicate dominant monkeys' authoritative behaviors, dynamically guiding network clusters. These Pilot Nodes precisely ensure optimized intra-knot connectivity, strategic energy management, and robust communication stability, significantly enhancing network resilience, reliability, and adaptive efficiency within the optimized SQUIMONET routing protocol.

3.12. Energy Requisition

Energy requisition within the optimized SQUIMONET routing protocol strongly parallels the adaptive behavior displayed by monkeys strategically conserving their energy while closely monitoring Malabar giant squirrels' resource availability. Monkeys precisely evaluate energy expenditure relative to anticipated nutritional gains from squirrels' dropped resources, carefully repositioning themselves to maximize benefits with minimal effort. Likewise, sensor nodes encountering critical energy depletion proactively initiate optimized energy requisition protocols, effectively requesting supplementary energy support from neighboring or designated pilot nodes. This optimized energy-sharing mechanism strategically ensures sustained node functionality, maintains robust communication pathways, and preserves network connectivity. Reflecting monkeys' adaptive conservation strategies, nodes actively balance resource usage against replenishment availability, significantly enhancing overall network efficiency and resilience.

Nodes accurately compute an optimized Energy Requisition Threshold (ERT), triggering proactive energy requests when their Residual Energy (E_{res}) falls below predefined sustainable operational limits. This threshold calculation explicitly integrates current node Workload Intensity (W_{int}), Average Energy Level within the Knot ($\overline{E}_k$), and Predicted Future Energy Consumption (E_{pred}).

$$ERT = E_{base} + \alpha_e \cdot W_{int} - \beta_e \cdot \frac{\overline{E}_k}{E_{max}} + \gamma_e \cdot \frac{E_{pred}}{E_{init}} \quad (23)$$

In Equation (23), the ERT precisely indicates the critical energy level at which nodes must proactively initiate power requisition. Baseline energy threshold (E_{base}) represents minimal energy necessary for essential operational functions. W_{int} explicitly quantifies nodes' current task demands and energy consumption rate. $\overline{E}_k$ normalized against Maximum Node Energy (E_{max}), provides contextual understanding of local network resources available for energy sharing. E_{pred}, normalized by Initial Node Energy (E_{init}), precisely forecasts upcoming energy requirements based on recent operational trends.

Weighting coefficients (α_e, β_e, and γ_e) have been strategically optimized, prioritizing sustainable operation, workload management, and proactive energy planning. This optimized proactive assessment parallels monkeys' adaptive decisions to conserve or expend energy based on anticipated gains from squirrel resource availability.

RESEARCH ARTICLE

Upon exceeding the threshold, nodes initiate an optimized Energy Allocation Request (EAR), efficiently quantifying the precise supplementary energy needed from available neighbors or pilot nodes. This optimized allocation request integrates Residual Energy Deficit (E_{def}), neighbors' Surplus Energy Availability (E_{sur}), and Historical Energy-Sharing Reliability (R_{share}), which is expressed in Equation (24) in mathematical form.

$$EAR = \delta_e \cdot \frac{E_{def}}{E_{max}} + \epsilon_e \cdot \frac{E_{sur}}{E_{max}} + \zeta_e \cdot R_{share} \quad (24)$$

EAR explicitly quantifies the precise energy replenishment level requested by the node. E_{def} explicitly measures the gap between current energy and optimal operational levels, normalized by Maximum Node Energy (E_{max}). E_{sur}, similarly normalized, accurately reflects neighbors' spare energy capacities, guiding realistic energy-sharing expectations. R_{share} explicitly indicates neighbors' past effectiveness in fulfilling energy requisition requests, ensuring dependable transactions. Optimized weighting parameters (δ_e, ϵ_e, and ζ_e) tactically prioritize accurate request sizing, resource availability, and historical reliability, effectively aligning nodes' energy-sharing behaviors with monkeys' carefully calculated reliance upon squirrels' consistent resource provisioning. Optimized energy requisition processes strategically ensure sustained operational effectiveness, balanced energy distribution, and robust network connectivity. The proactive and adaptive nature of these energy-sharing mechanisms, directly inspired by monkeys' calculated decisions toward Malabar giant squirrels' resource availability, precisely enhances the overall reliability, efficiency, and resilience of the optimized SQUIMONET routing protocol operations.

3.13. Node Resume / On-Board Nodes

Node Resume and On-Boarding within the optimized SQUIMONET routing protocol precisely mirror the adaptive behaviors of monkeys cautiously reintegrating themselves into resource-rich areas following careful assessment of Malabar giant squirrels' renewed stability. When monkeys perceive consistent and dependable resource availability from squirrels after prior uncertainties, they strategically resume active participation, carefully reassessing their positioning for optimized resource exploitation. Similarly, network nodes previously suspended or newly introduced actively undergo optimized resumption or onboarding processes, systematically reintegrating into the network. This strategic optimized reintegration ensures robust connectivity, sustained operational efficiency, and balanced resource management across the entire network. Reflecting monkeys' cautious yet strategic approach, nodes precisely evaluate prevailing conditions before resuming active network participation, thus safeguarding reliability and communication effectiveness.

Nodes compute an optimized Node Reintegration Score (NRS) prior to resuming active operations, carefully assessing their suitability based on Updated Residual Energy (E_{upd}), Recent Diagnostic Verification Results (D_{ver}), and Current Network Reliability Status (N_{rel}).

$$NRS = \alpha_n \cdot \frac{E_{upd}}{E_{max}} + \beta_n \cdot D_{ver} + \gamma_n \cdot N_{rel} \quad (25)$$

In Equation (25), the NRS explicitly quantifies nodes' readiness and eligibility for re-entry into active network participation. E_{upd} accurately reflects nodes' current energy status post-suspension, normalized by Maximum Node Energy Capacity (E_{max}). D_{ver} provide explicit assessments of node integrity, operational reliability, and communication readiness. N_{rel} precisely evaluates the current stability of neighboring nodes and overall knot conditions, directly influencing suitability for node reintegration. The strategically optimized weighting parameters (α_n, β_n, and γ_n) balance nodes' energy viability, operational health, and network stability, directly resembling monkeys' adaptive evaluation of environmental stability before resuming resource exploitation activities near squirrels.

Following successful reintegration scoring, nodes determine the optimized Integration Interval (T_{int}), explicitly controlling their phased reintroduction to network communications. This interval calculation explicitly integrates Node Inactivity Duration (D_{ina}), Previous Abnormality Severity Index (S_{abn}), and Current Knot Activity Level (A_{lvl}), represented mathematically in Equation (26).

$$T_{int} = T_{baseint} + \delta_n \cdot \frac{D_{ina}}{D_{max}} + \epsilon_n \cdot S_{abn} + \zeta_n \cdot \frac{A_{lvl}}{A_{max}} \quad (26)$$

T_{int} explicitly defines the strategic duration required for gradual node re-entry, carefully minimizing network disruptions. Baseline interval ($T_{baseint}$) represents minimal initial integration duration, ensuring phased, cautious reintegration. D_{ina}, normalized against maximum permissible inactivity period (D_{max}), influences reintegration pacing based on time away from active participation. S_{abn} precisely quantifies the extent of nodes' prior abnormal or malicious behavior, carefully controlling the cautiousness of their return. A_{lvl}, normalized against Maximum Activity (A_{max}), accurately reflects existing communication and workload conditions within nodes' clusters, guiding adaptive reintegration timing. Weighting factors (δ_n, ϵ_n, and ζ_n) have been strategically optimized, carefully prioritizing phased, secure, and stable reintegration processes, closely replicating monkeys' cautious yet decisive return behaviors toward resource areas after squirrels regain consistent feeding patterns.

Thus, through optimized strategic node resume and onboarding processes, nodes dynamically restore network

RESEARCH ARTICLE

participation, precisely maintaining robust communication and stable energy distribution. This cautious yet optimized reintegration behavior directly mirrors monkeys' adaptive strategies, carefully evaluating Malabar giant squirrels' renewed reliability before actively re-engaging, significantly enhancing network resilience, reliability, and operational stability within the optimized SQUIMONET protocol framework.

3.14. Path Verification

Path Verification within the optimized SQUIMONET routing protocol meticulously mirrors the vigilance and consistent behavioral checks performed by monkeys to ensure reliable access to resources provided by Malabar giant squirrels. Monkeys continuously validate the consistency and safety of pathways leading to resource-rich zones beneath squirrels, cautiously verifying each route's reliability, security, and energy efficiency before moving. Analogously, network nodes systematically perform optimized path verification, continuously evaluating established communication routes' reliability, latency, energy consumption, and security robustness. Nodes carefully assess updated route conditions, ensuring ongoing reliability and optimized performance for data transmission. This optimized continuous validation enhances operational stability and reliability, precisely replicating monkeys' strategic and cautious approach in consistently verifying paths towards reliable feeding grounds provided by squirrels.

During optimized path verification, nodes precisely compute an Optimized Path Reliability Metric (PRM), carefully assessing route dependability by integrating factors such as Link Stability (L_{stab}), Historical Success Rate (H_{sr}), and Residual Energy Balance (E_{bal}).

$$PRM = \frac{\lambda_v \cdot L_{stab}}{L_{max}} + \mu_v \cdot H_{sr} + \nu_v \cdot \frac{E_{bal}}{E_{max}} \quad (27)$$

In Equation (27), PRM explicitly quantifies the reliability and operational dependability of communication pathways. L_{stab} accurately measures current communication consistency and signal strength along verified paths, normalized by Maximum Achievable Stability (L_{max}). H_{sr} explicitly records past successful data transmissions along evaluated routes, reinforcing predictions of future reliability. E_{bal} precisely indicates the evenly distributed energy availability among nodes within the verified route, normalized against maximum node energy (E_{max}). The optimized weighting parameters ($\lambda_v, \mu_v,$ and ν_v) strategically balance link stability, historical reliability, and energy distribution, closely resembling monkeys' cautious reliance on historically dependable pathways under squirrels' consistent behavioral patterns.

Further, nodes accurately calculate an Optimized Path Security Index (PSI), continuously verifying route security through assessing the Security Compliance Rate (S_{cr}), Recent Detected Threats Count (T_{cnt}), and Route Abnormality Indicator (A_{ind}).

$$PSI = \alpha_v \cdot S_{cr} - \beta_v \cdot \frac{T_{cnt}}{T_{max}} - \gamma_v \cdot A_{ind} \quad (28)$$

In Equation (28), the PSI explicitly quantifies security, integrity, and vulnerability along evaluated paths. S_{cr} explicitly indicates nodes' adherence to predefined security protocols along the communication pathway, ensuring consistent and secure interactions. T_{cnt}, normalized against Maximum Possible Threats (T_{max}), explicitly assesses current security vulnerabilities, guiding cautious route utilization. A_{ind} quantifies unusual behavior occurrences along paths, providing additional security awareness for optimized path selection. Optimized weighting coefficients ($\alpha_v, \beta_v,$ and γ_v) precisely balance security compliance, threat minimization, and behavioral normality, accurately paralleling monkeys' strategic decisions to cautiously avoid potentially risky or unpredictable pathways influenced by irregular squirrel activities. Optimized path verification ensures continuous assessment, enhanced reliability, and strengthened security for active routing paths within the network. Inspired directly by monkeys' consistent vigilance and cautious pathway validation behaviors toward resources provided by Malabar giant squirrels, this optimized verification mechanism strategically reinforces SQUIMONET's communication stability, energy efficiency, and secure connectivity, significantly enhancing the overall resilience, reliability, and operational robustness of the network.

3.15. Data Transmission

Data transmission within the optimized SQUIMONET routing protocol closely mirrors monkeys' strategic behaviors when positioning themselves optimally to receive resources efficiently dropped by Malabar giant squirrels. Monkeys consistently choose precise locations beneath the squirrels to ensure reliable acquisition of food, thus minimizing energy expenditure and maximizing nutritional gains. Similarly, network nodes engage in optimized data transmission, strategically transmitting information through paths carefully verified for reliability, energy efficiency, and security. This careful selection of optimized transmission routes significantly enhances the likelihood of successful data delivery, maintains energy conservation, and ensures consistent communication reliability across the network. Such optimized transmission mechanisms directly parallel monkeys' calculated decisions in positioning beneath resource-dropping squirrels, strategically optimizing resource acquisition and conserving energy.

Nodes calculate an optimized Data Delivery Success Probability (DDSP) during each transmission cycle, carefully assessing the likelihood of successful data transmission based

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/44 Volume 12, Issue 5, September – October (2025)

RESEARCH ARTICLE

on optimized Link Reliability (L_{rel}), Current Path Congestion Rate (C_{rate}), and Intermediate Node Energy Availability (E_{int}).

$$DDSP = \frac{\sigma_d \cdot L_{rel}}{L_{max}} - \frac{\emptyset_{dd} \cdot C_{rate}}{C_{max}} + \frac{\psi_d \cdot E_{int}}{E_{max}} \quad (29)$$

In Equation (29), DDSP explicitly measures the likelihood of accurate and timely data transmission across the selected path. L_{rel}, normalized against Maximum Achievable Reliability (L_{max}), quantifies the dependability and stability of communication links along the path. C_{rate}, precisely normalized by Maximum Permissible Congestion (C_{max}), indicates current communication load, influencing path availability and responsiveness. E_{int}, accurately normalized by Maximum Energy Capacity (E_{max}), reflects nodes' collective capability to sustain transmission duties without interruption. Weighting parameters (σ_d, ϕ_d, and ψ_d) are strategically optimized, balancing reliability, congestion management, and energy sufficiency. These calculations precisely reflect monkeys' strategic positioning behaviors beneath squirrels for optimized resource retrieval.

Nodes utilize an optimized Transmission Energy Efficiency (TEE) metric, strategically assessing the energy conservation effectiveness of selected communication routes. This optimized efficiency metric incorporates Transmission Power Required (P_{tx}), Data Packet Size (S_{pkt}), and Total Energy Consumed along the Path (E_{path}), which is represented as Equation (30).

$$TEE = \frac{S_{pkt}}{P_{tx} \cdot E_{path}} \quad (30)$$

TEE explicitly quantifies data transmission effectiveness relative to the energy utilized. P_{tx} precisely signifies the optimized energy expenditure required for reliable signal propagation across network links. S_{pkt} explicitly indicates the volume of information transmitted during each communication session. E_{path} accurately quantifies cumulative energy expenditure across intermediate nodes facilitating data delivery. This optimized assessment ensures communication efficiency remains consistently high, reflecting monkeys' carefully optimized energy expenditures in resource acquisition beneath squirrels. Lower transmission power and energy consumption combined with effective data packet management strategically enhance nodes' operational longevity and overall network resilience. Through carefully optimized data transmission processes, the network precisely maintains robust connectivity, ensures reliable and secure information delivery, and sustains energy efficiency. Nodes dynamically and adaptively select routes verified for optimal reliability and minimal congestion, directly emulating monkeys' strategic and energy-conscious decisions to position optimally beneath consistently resourceful Malabar giant squirrels. This optimized approach within SQUIMONET protocol operations significantly strengthens data integrity, minimizes resource wastage, and maximizes operational longevity, effectively reflecting strategic behaviors derived from careful observation of natural ecological interactions. The process of SQUIMONET is expressed in pseudocode in Algorithm 1.

```
BEGIN SQUIMONET_CORE()
FOR EACH node IN Network
INIT(node):
node.status ← ACTIVE
node.energy ← INITIAL
node.role ← UNASSIGNED
node.neighbors ← FILTER_BY(RSSI AND DISTANCE)
END FOR
FORM_CLUSTERS():
ASSIGN cluster_id BASED ON neighbor energy
                > THRESHOLD
ASSIGN_ROLES():
FOR EACH cluster
SELECT MAX_ENERGY node → role ← MONKEY
OTHERS → role ← SQUIRREL
WHILE network is functional
FOR EACH SQUIRREL
IF node.energy < MIN_THRESHOLD THEN
SEND ENERGY_REQUEST TO MONKEY
PAUSE SENSING
ELSE
DATA ← SENSE()
SEND TO MONKEY
FOR EACH MONKEY
packet ← RECEIVE()
IF packet.id NOT IN BROADCAST_CACHE THEN
IF packet IS NORMAL → FORWARD_TO_BASE()
IF packet IS EVENT → BROADCAST_TO_MONKEYS()
ADD packet.id TO BROADCAST_CACHE
UPDATE_ENERGY_AND_STATUS()
```

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/44 Volume 12, Issue 5, September – October (2025)

RESEARCH ARTICLE

```
REFRESH_ROLES_AND_DEMOTE()
REBALANCE_CLUSTERS()
HANDLE_FAULTS()
END WHILE
END SQUIMONET_CORE
```

Algorithm 1 SQUIMONET

4. SIMULATIONS AND OUTCOME EVALUATIONS

Simulation has represented a controlled experimental technique that has enabled researchers to model, examine, and predict the behavior of systems in virtual settings. Within the scope of WSNs, simulation has provided a valuable means to understand complex interactions among nodes, evaluate routing decisions, and measure performance under fluctuating energy levels, mobility constraints, and data delivery demands. WSNs have comprised spatially distributed sensor nodes deployed to observe physical or environmental parameters and relay this information toward a central base station or sink. In these networks, constraints on energy, bandwidth, and processing power have made the evaluation of new routing frameworks critical prior to real-world deployment.

One such framework, SQUIMONET, has introduced a queue-priority and mobility-aware routing strategy that has been aligned with quality-of-service (QoS) objectives in cloud-integrated sensor systems. For evaluating SQUIMONET in a 3D WSN setting, the NS-3 simulator has been employed due to its capacity to support mobility models, energy-aware behavior, and cloud synchronization. The simulation design has emphasized queue length balancing, efficient retransmissions, and energy conservation across multiple node densities. This setup has facilitated the examination of fault recovery time, packet delivery ratio, and end-to-end delay in varied topological and traffic scenarios. The simulation settings tailored for SQUIMONET have been curated to match realistic IoT applications involving dynamic sensors and adaptive routing responses in harsh environmental conditions, shown in Table 2.

Table 2 Simulation Table

Simulation Parameter	Value
State Power Consumption	Idle: 168 mW
Bandwidth	99 Hz
Network Boundary	1.6 km × 1.6 km × 1.6 km
MAC Protocol	CW-MAC02.11DCF
Layer Width	≤ 150 meters
Simulation Runtime	1000 seconds
Packet Size	85 bytes
Packet Header Size	16 bytes
Initial Node Energy	410 Joules
Transmission Radius	320 meters
Data Transmission Rate	24 kbps
Total Number of Nodes	500
Number of Sink Nodes	≥ 4
Operating Voltage per Node	3.2 Volts

4.1. Packet Delivery Ratio and Packet Loss Ratio

Packet Delivery Ratio (PDR) has been one of the most essential performance indicators in WSNs evaluations, as it reflects the reliability and completeness of packet transmission between sensor nodes and the base station. This metric has been particularly critical in determining whether a routing protocol is capable of sustaining stable communication across various network sizes. In this evaluation, the PDR values of three protocols CMR, GBOR, and the proposed SQUIMONET have been analyzed over increasing node densities ranging from 50 to 500 nodes. It has been clearly observed that SQUIMONET has consistently maintained a higher PDR across all node configurations, starting from 97.51% at 50 nodes and sustaining 81.45% even when scaled to 500 nodes.

In contrast, both CMR and GBOR have shown declining trends with PDR values dropping below 65% at higher node counts. The average PDR for SQUIMONET has reached 89.779%, which has notably surpassed GBOR's 73.518% and CMR's 71.261%. This reliable delivery rate underlines the role-based and adaptive routing behavior of SQUIMONET that has helped reduce congestion, reroute around failures, and preserve communication fidelity under increasing load conditions.

Packet Loss Ratio (PLR) has served as a critical metric for evaluating the resilience and dependability of WSNs, particularly under varying node densities. PLR measures the percentage of data packets that have failed to reach the intended destination, which often arises due to link failures, congestion, or routing inefficiencies.

Lower PLR values have indicated a more reliable and robust routing behavior, which is especially important in real-world environments where uninterrupted communication plays a central role in mission-critical applications. The PLR performance of the proposed SQUIMONET protocol has been compared with existing protocols such as CMR and GBOR over a range of node counts. SQUIMONET has demonstrated

RESEARCH ARTICLE

an exceptionally low PLR starting at 2.49% for 50 nodes and gradually increasing to only 18.55% at 500 nodes. In contrast, both CMR and GBOR have shown much higher PLR values throughout the experiment, averaging 28.74% and 26.482% respectively, while SQUIMONET has maintained an average PLR of just 10.221%. These values have confirmed that the adaptive role-switching and fault-tolerant design of SQUIMONET has substantially minimized data loss even under dense and dynamic network conditions. The PDR and PLR results were exhibited in textual form using Table 3 and pictorial form in Figure 2.

Table 3 PDR and PLR

No. of Nodes		50	100	150	200	250	300	350	400	450	500
CMR	PDR	78.87	76.82	76.56	74.95	72.95	70.72	67.86	66.76	64.12	63.01
	PLR	21.13	23.18	23.44	25.05	27.05	29.28	32.14	33.24	35.88	36.99
GBOR	PDR	81.37	79.25	78.98	77.32	75.26	72.96	70.01	68.87	66.15	65.01
	PLR	18.63	20.75	21.02	22.68	24.74	27.04	29.99	31.13	33.85	34.99
SQUIMONET	PDR	97.51	96.98	94.46	92.34	90.5	88.78	86.84	85.77	83.16	81.45
	PLR	2.49	3.02	5.54	7.66	9.5	11.22	13.16	14.23	16.84	18.55

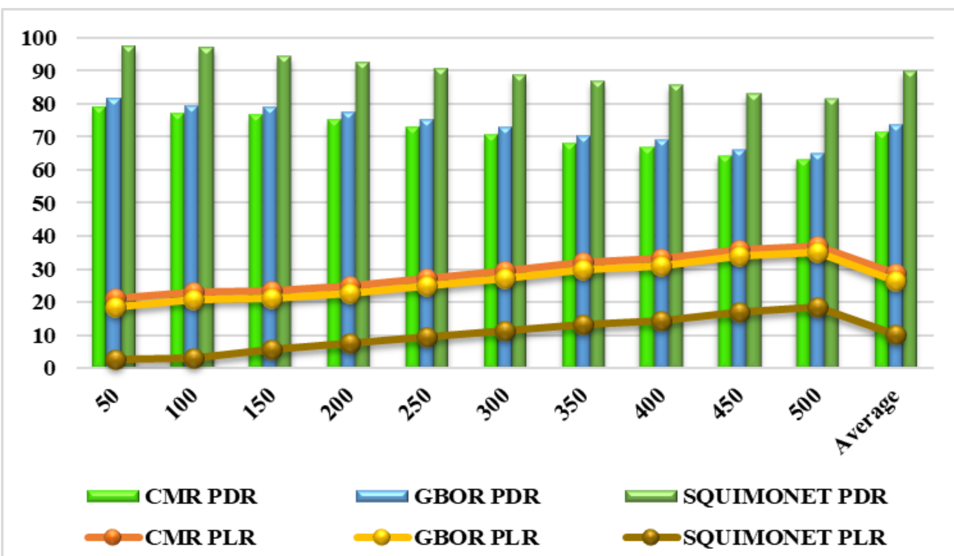

Figure 2 PDR and PLR

4.2. Throughput

Throughput has been recognized as a key performance indicator in WSNs evaluations, reflecting the overall efficiency with which a routing protocol can transfer data across the network. It has measured the total amount of successfully delivered data within a given time frame and has

RESEARCH ARTICLE

played an essential role in applications that demand steady and high-volume communication. A higher throughput value has indicated that the routing framework has been capable of handling more data traffic without delay or loss, even as network conditions become more complex with increased node density. In this comparative study, the throughput performance of the proposed SQUIMONET protocol has been analyzed against CMR and GBOR across node counts ranging from 50 to 500.

Table 4 Throughput

No. of Nodes	50	100	150	200	250	300	350	400	450	500	Average
CMR	74	132	187	229	268	289	295	297	284	265	232.0
GBOR	77	145	202	248	287	311	320	325	312	300	252.70
SQUIMONET	109	211	305	368	414	445	462	469	456	437	367.60

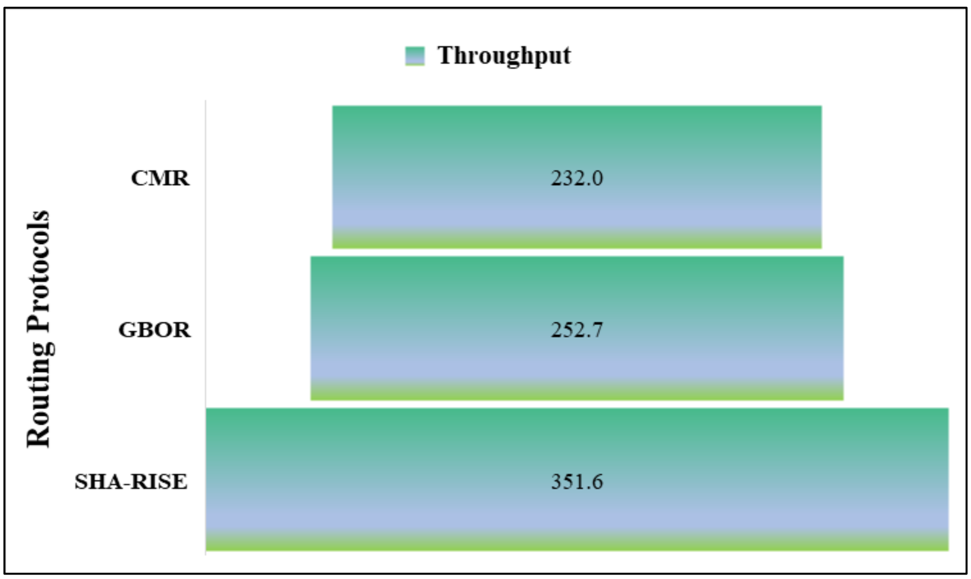

Figure 3 Throughput

It has been observed that SQUIMONET has maintained consistently higher throughput values across all scenarios, beginning at 109 units with 50 nodes and reaching up to 469 units at 400 nodes. The average throughput of SQUIMONET has been recorded as 367.60, which has been significantly higher than that of GBOR at 252.70 and CMR at 232.00. This consistent advantage has demonstrated the capacity of SQUIMONET to manage data flow efficiently through its adaptive routing and reduced packet collisions. The obtained Throughput results were exhibited in textual form using Table 4 and pictorial form in Figure 3.

4.3. Delay

Delay has represented the time taken for a data packet to travel from its source to the destination within a WSNs. It has included all intermediate processing, queuing, transmission, and propagation intervals experienced along the communication path. In real-time or time-sensitive applications, minimizing delay has been essential to ensure that the data remains relevant and actionable by the time it reaches the sink node or base station.

Lower delay values indicate the ability of a routing protocol to efficiently handle transmissions without introducing bottlenecks or waiting times. In this assessment, the proposed protocol SQUIMONET has been compared with CMR and GBOR under increasing node densities from 50 to 500. SQUIMONET has consistently achieved lower delay across all tested configurations, starting at 4512 ms with 50 nodes and maintaining 4967 ms even at the highest density of 500 nodes. In contrast, both CMR and GBOR have recorded significantly higher delay values, with their averages reaching 5907.6 ms and 6044.2 ms respectively. SQUIMONET's average delay has remained at 4779.5 ms, which has clearly shown the protocol's effectiveness in reducing transmission latency through adaptive clustering, role awareness, and efficient route selection. The obtained Delay results were exhibited in textual form using Table 5 and pictorial form in Figure 4.

Table 5 Delay

No. of Nodes	50	100	150	200	250	300	350	400	450	500	Average
CMR	5671	5701	5747	5803	5851	5963	5992	6032	6112	6204	5907.6
GBOR	5782	5821	5874	5925	6003	6099	6148	6201	6287	6302	6044.2
SQUIMONET	4512	4661	4734	4753	4771	4791	4839	4843	4924	4967	4779.5

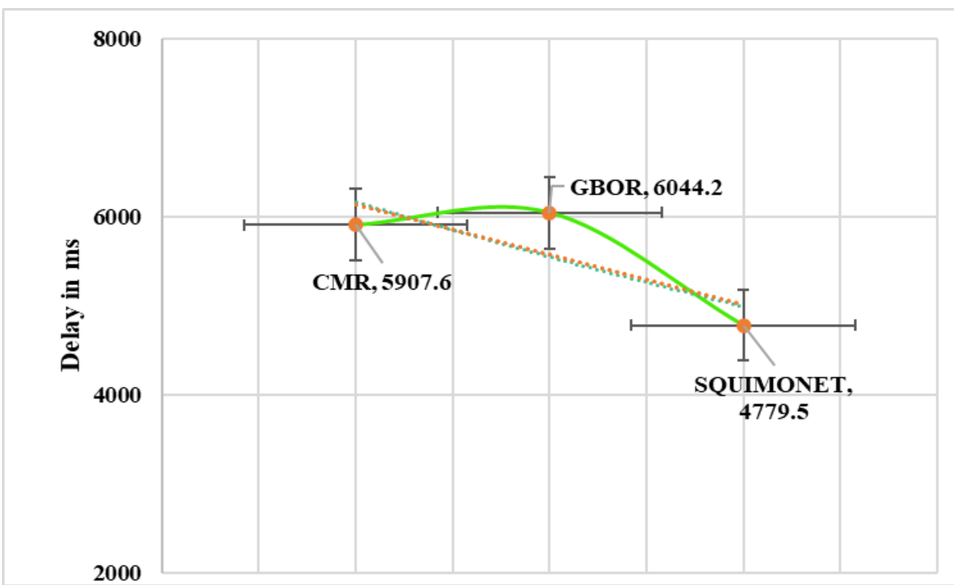

Figure 4 Delay

4.4. Energy Consumption

Energy consumption has remained one of the most vital performance indicators in WSNs, especially considering the constrained battery capacities of sensor nodes deployed in remote or inaccessible environments. This metric has indicated the percentage of total energy depleted during the network operation and has been crucial for assessing the longevity and sustainability of any proposed routing protocol. Lower energy consumption has signified more efficient use of resources, which has directly contributed to extending the overall network lifetime. The energy consumption of SQUIMONET has been compared with that of CMR and GBOR over increasing node densities from 50 to 500. SQUIMONET has consistently exhibited lower energy usage

RESEARCH ARTICLE

across all scenarios, starting at 26.47% for 50 nodes and gradually increasing to only 46.51% at 500 nodes. On the other hand, both CMR and GBOR have shown significantly higher consumption patterns, averaging 50.5005% and 48.2005% respectively.

SQUIMONET has maintained an average energy consumption of just 36.720%, highlighting its ability to conserve node power through optimized role distribution and reduced communication redundancy. This efficient energy behavior has validated the protocol's suitability for long-term, sustainable WSN deployments in real-world conditions. The obtained Energy Consumption results were exhibited in textual form using Table 6 and pictorial form in Figure 5.

Table 6 Energy Consumption

No. of Nodes	50	100	150	200	250	300	350	400	450	500	Average
CMR	41.32	42.40	43.17	46.55	48.88	50.31	54.31	56.28	59.74	62.04	50.50
GBOR	39.20	41.25	42.07	44.28	46.03	48.67	51.44	53.72	56.92	58.44	48.20
SQUIMONET	26.47	28.34	31.35	34.11	35.71	38.33	40.20	42.23	43.96	46.51	36.72

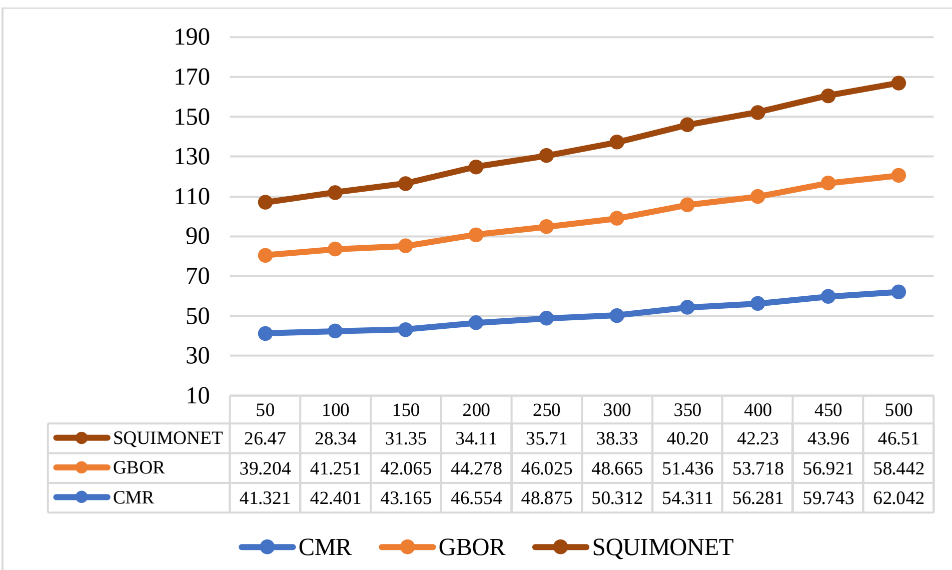

Figure 5 Energy Consumption

4.5. Fault Recovery Time

Fault Recovery Time (FRT) has served as a crucial performance metric in evaluating the responsiveness and adaptability of routing protocols in WSNs. This metric has quantified the duration required by the network to restore communication following a node or link failure, which is particularly important in mobile and dynamic environments. A shorter FRT has reflected the protocol's ability to detect faults quickly, reconfigure routes, and maintain data flow with minimal disruption.

In this evaluation, the FRT performance of the proposed SQUIMONET protocol has been assessed across increasing node densities and mobility speeds. As the number of nodes rose from 50 to 500 and mobility speeds ranged from 1 ms to 5.5 ms, the FRT values have ranged from 439 ms to 771 ms.

RESEARCH ARTICLE

Table 7 Fault Recovery Time

Node Count	Mobility Speed (ms)	T_1 (ms)	T_2 (ms)	Fault Recovery Time (FRT in ms)
50	1	120.084	120.523	439
100	1.5	181.2	181.696	496
150	2	226.438	227.012	574
200	2.5	234.518	235.019	501
250	3	298.112	298.749	637
300	3.5	378.043	378.672	629
350	4	395.107	395.798	691
400	4.5	452.101	452.739	638
450	5	483.9	484.671	771
500	5.5	521.445	522.196	751
Average				612.7

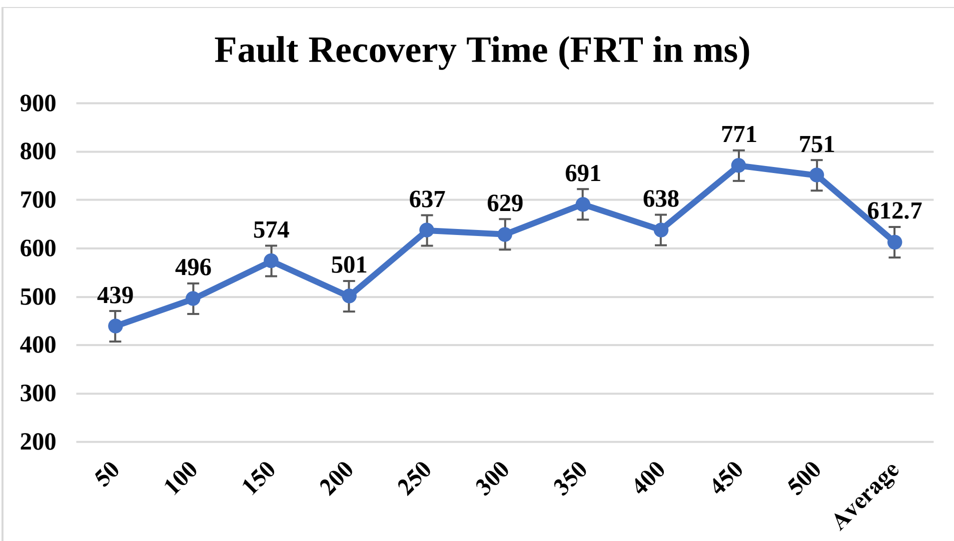

Figure 6 Fault Recovery Time

The recovery process has remained consistent and efficient, even as mobility introduced unpredictability into the network. SQUIMONET has achieved an average FRT of 612.7 ms, which has demonstrated its ability to promptly adapt to failures without requiring extensive overhead.

This consistent performance under varying speeds and node counts has confirmed the protocol's suitability for applications where continuity of communication and minimal downtime are mission critical. The obtained FRT results were exhibited in textual form using Table 7 and pictorial form in Figure 6.

4.6. Network Lifetime

Network Lifetime (NLT) has represented the duration for which a WSNs remains functionally active before a significant portion of its nodes become inoperative. This metric has been especially relevant in scenarios where battery-powered nodes are deployed in unattended environments, as it directly influences the sustainability and practicality of the routing protocol. A longer network lifetime has indicated that the protocol has efficiently managed energy consumption, balanced load among nodes, and responded well to environmental dynamics and node failures.

RESEARCH ARTICLE

Table 8 Network Life Time

No. of Nodes	50	100	150	200	250	300	350	400	450	500	Average
CMR	43.45	41.30	38.95	34.73	30.54	29.10	27.41	24.43	21.20	19.08	31.02
GBOR	50.53	48.03	45.30	40.40	35.52	33.85	31.88	28.41	24.65	22.19	36.07
SQUIMONET	92.25	89.22	85.55	81.36	71.89	60.81	59.76	57.74	56.85	55.67	71.11

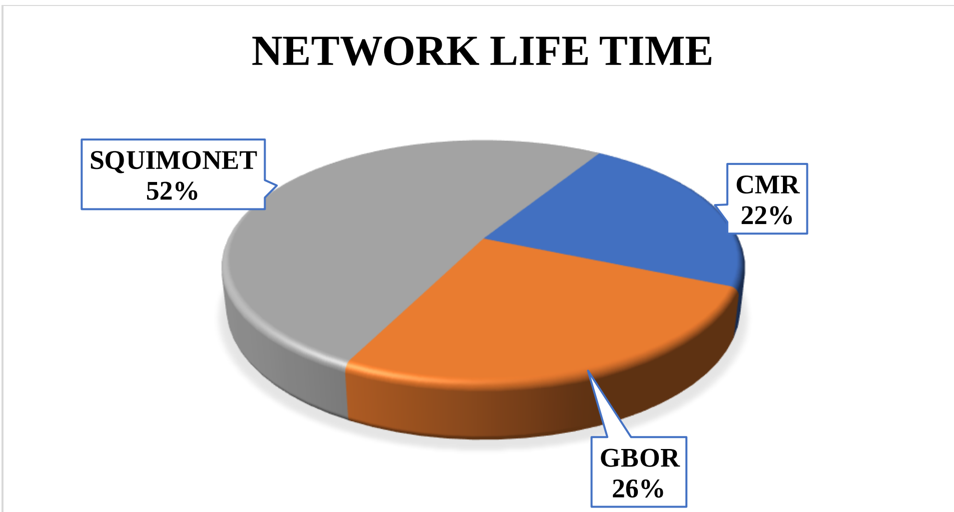

Figure 7 Network Lifetime

The proposed SQUIMONET protocol has been evaluated against existing approaches like CMR and GBOR over node densities ranging from 50 to 500. SQUIMONET has shown a clear advantage by sustaining higher lifetime values across all test cases, with 92.250 units at 50 nodes and maintaining 55.670 units even at 500 nodes. In contrast, GBOR and CMR have demonstrated a steady decline, averaging 36.074 and 31.018 units respectively. SQUIMONET has maintained an average network lifetime of 71.111, significantly outperforming both benchmarks. This improvement has been attributed to its energy-aware role distribution and adaptive rerouting strategy, which together have reduced early node exhaustion and supported prolonged network activity in dense deployments. The obtained NLT results were exhibited in textual form using Table 8 and pictorial form in Figure 7.

5. CONCLUSION

The proposed SQUIMONET has been developed with the intention of addressing the persistent challenges found in WSNs, especially those associated with energy efficiency, scalability, and communication reliability. Inspired by the instinct-driven cooperation between Malabar squirrels and forest monkeys, SQUIMONET has introduced an adaptive, role-based routing framework in which nodes dynamically assume the roles of either data-gathering squirrels or coordination-centric monkeys. This division has not only distributed responsibilities intelligently but also balanced energy usage across the network, allowing it to operate sustainably even under high node densities and mobile conditions. Based on the evaluated metrics PDR, PLR, Throughput, Delay, FRT, Energy Consumption, and NLT it has become evident that SQUIMONET has consistently outperformed conventional approaches like CMR and GBOR. The observed improvements in delivery accuracy, energy savings, and fault responsiveness have confirmed that biologically inspired role coordination has offered a reliable alternative to rigid routing models. The protocol's strength has resided in its minimalistic but powerful adaptation mechanism. While its responsiveness and role transitions have been effective under increasing load, certain areas such as

RESEARCH ARTICLE

overhead management during extreme failures or node mobility transitions may benefit from future enhancements. It would be meaningful to integrate predictive learning models to further refine monkey role election and anticipate energy drops. Overall, SQUIMONET has stood out as a resilient and scalable routing strategy grounded in natural behavior, capable of extending network longevity and improving communication stability across diverse real-world sensor deployments.

REFERENCES

[1] M. Shahid et al., "Link-Quality-Based Energy-Efficient Routing Protocol for WSN in IoT," IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 4645–4653, 2024, doi: 10.1109/TCE.2024.3356195.

[2] S. Sangeetha, A. A. V. T., P. M., and R. and Sowmya, "Segment routing for WSN using hybrid optimization with energy-efficient game theory-based clustering technique," Automatika, vol. 66, no. 1, pp. 24–42, Jan. 2025, doi: 10.1080/00051144.2024.2431750.

[3] J. R. Nishanth and B. and Senthilkumar, "Hybrid energy harvesting by reverse di-electric on a piezo-electric generator with thermo-couple and monitoring in WSN," Automatika, vol. 65, no. 3, pp. 738–748, Jul. 2024, doi: 10.1080/00051144.2024.2315407.

[4] A. K. Rao, K. K. Nagwanshi, and M. K. Shukla, "An optimized secure cluster-based routing protocol for IoT-based WSN structures in smart agriculture with blockchain-based integrity checking," Peer Peer Netw Appl, vol. 17, no. 5, pp. 3159–3181, 2024, doi: 10.1007/s12083-024-01748-1.

[5] S. K. Sharma and M. Chawla, "Compatibility Analysis of Cluster-Based WSN Framework for IoT Applications," Wirel Pers Commun, vol. 131, no. 2, pp. 1365–1380, 2023, doi: 10.1007/s11277-023-10486-1.

[6] J. Zhang, "WSN Network Node Malicious Intrusion Detection Method Based on Reputation Score," Journal of Cyber Security and Mobility, vol. 12, no. 1, pp. 55–76, 2025, doi: 10.13052/jcsm2245-1439.1213.

[7] T. R. Beegum, M. Y. I. Idris, M. N. B. Ayub, and H. A. Shehadeh, "Optimized Routing of UAVs Using Bio-Inspired Algorithm in FANET: A Systematic Review," IEEE Access, vol. 11, pp. 15588–15622, 2023, doi: 10.1109/ACCESS.2023.3244067.

[8] Y. Azzoug and A. Boukra, "Improved junction-based routing for VANETs using a Bio-inspired route stability approach," Ad Hoc Networks, vol. 153, p. 103346, 2024, doi: https://doi.org/10.1016/j.adhoc.2023.103346.

[9] Y. Chu, P. Mitchell, D. Grace, J. Roberts, D. White, and T. Mickus, "IRIS: A low duty cycle cross-layer protocol for long-range wireless sensor networks with low power budget," Computer Networks, vol. 225, p. 109666, 2023, doi: https://doi.org/10.1016/j.comnet.2023.109666.

[10] V. Nivedita, C.-S. Shieh, and M.-F. Horng, "An integrated trust-based secure routing with intrusion detection for mobile Ad Hoc network using adaptive snow geese optimization algorithm," Ain Shams Engineering Journal, vol. 16, no. 7, p. 103385, 2025, doi: https://doi.org/10.1016/j.asej.2025.103385.

[11] G. C. Heck, A. A. Quispe, P. H. da Fonseca, O. S. Junior, R. A. Hexsel, and L. C. P. Albini, "FRR: A Fast Routing Recovery mechanism minimizing network formation time in smart grids," International Journal of Electrical Power & Energy Systems, vol. 164, p. 110364, 2025, doi: https://doi.org/10.1016/j.ijepes.2024.110364.

[12] M. A. Alqarni, M. H. Mousa, M. K. Hussein, and M. A. Mead, "Improved wireless sensor network data collection using discrete differential evolution and ant colony optimization," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 8, p. 101725, 2023, doi: https://doi.org/10.1016/j.jksuci.2023.101725.

[13] K. A. Farrea, Z. Baig, R. Doss, and D. Liu, "Zero trust-based authentication for Inter-Satellite Links in NextGen Low Earth Orbit networks," Ad Hoc Networks, vol. 174, p. 103817, 2025, doi: https://doi.org/10.1016/j.adhoc.2025.103817.

[14] R. Ferreira, T. Adão, R. Morais, A. R. Costa, and E. Peres, "Zero Trust-based preventative detection of vulnerabilities for IoT-based precision agriculture: a case-study on the mySense platform," Procedia Comput Sci, vol. 256, pp. 267–275, 2025, doi: https://doi.org/10.1016/j.procs.2025.02.120.

[15] F. Nawshin, D. Unal, M. Hammoudeh, and P. N. Suganthan, "AI-powered malware detection with Differential Privacy for zero trust security in Internet of Things networks," Ad Hoc Networks, vol. 161, p. 103523, 2024, doi: https://doi.org/10.1016/j.adhoc.2024.103523.

[16] R. Basri et al., "Enhancing IoT security: Assessing instantaneous communication trust to detect man-in-the-middle attacks," Future Generation Computer Systems, vol. 166, p. 107714, 2025, doi: https://doi.org/10.1016/j.future.2025.107714.

[17] J. F. Cevallos-Moreno, A. Rizzardi, S. Sicari, and A. Coen-Porisini, "HERO: From High-dimensional network traffic to zERO-Day attack detection," Computer Networks, p. 111264, 2025, doi: https://doi.org/10.1016/j.comnet.2025.111264.

[18] N. Alsharabi, A. Bhardwaj, T. Alshammari, S. alotaibi, D. Alshammari, and A. Jadi, "IAPN: Framework to secure IoT-based infrastructures using Private APN," Egyptian Informatics Journal, vol. 30, p. 100671, 2025, doi: https://doi.org/10.1016/j.eij.2025.100671.

[19] A. Singh et al., "Resilient wireless sensor networks in industrial contexts via energy-efficient optimization and trust-based secure routing," Peer Peer Netw Appl, vol. 18, no. 3, p. 132, 2025, doi: 10.1007/s12083-025-01946-5.

[20] O. I. Khalaf and G. M. Abdulsahib, "Renewable Energy Relationship with Technology and Application to Develop New Generation of Wireless Sensor Networks," SN Comput Sci, vol. 6, no. 2, p. 123, 2025, doi: 10.1007/s42979-024-03614-6.

[21] J. Dev, P. Pradhan, and J. Mishra, "HABC-MD: a novel routing algorithm for wireless sensor network," Microsystem Technologies, pp. 1–10, May 2023, doi: 10.1007/S00542-023-05461-6/METRICS.

[22] V. Gupta and D. Seth, "3Dimensional improvise clustering algorithm for unmanned aerial vehicles: 3DICA," International Journal of Information Technology, vol. 16, no. 4, pp. 2563–2576, 2024, doi: 10.1007/s41870-024-01748-7.

[23] S. Sridharan, S. Venkatraman, and S. P. Raja, "A Novel Lie Hypergraph Based Lifetime Enhancement Routing Protocol for Environmental Monitoring in Wireless Sensor Networks," IEEE Trans Comput Soc Syst, vol. 11, no. 2, pp. 2070–2080, 2024, doi: 10.1109/TCSS.2023.3262273.

[24] M. Thammawichai and T. Luangwilai, "An energy-optimization topology control for three-dimensional wireless sensor networks," Journal of Communications and Networks, vol. 25, no. 6, pp. 778–788, 2023, doi: 10.23919/JCN.2023.000050.

[25] K. Aravind and P. K. R. M, "Optimized Fuzzy Logic Based Energy-Efficient Geographical Data Routing in Internet of Things," IEEE Access, vol. 12, pp. 18913–18930, 2024, doi: 10.1109/ACCESS.2024.3354174.

[26] V. Gangal, I. Cinemre, and G. Hacioglu, "A Distributed Leach-AHP Routing for Wireless Sensor Networks," IEEE Access, vol. 12, pp. 19307–19319, 2024, doi: 10.1109/ACCESS.2024.3359750.

[27] P. Sharma, M. Sharma, R. Singh, V. Kumar, R. Agarwal, and P. K. Malik, "NHARSO-IWSN: A Novel Hybridized Adaptive-Network-Based Fuzzy Inference System With Reptile Search Optimization Algorithm-Based Routing Protocol for Internet of Things-Enabled Wireless Sensor Networks," IEEE Transactions on Consumer Electronics, vol. 70, no. 3, pp. 6293–6302, 2024, doi: 10.1109/TCE.2024.3418845.

[28] M.-R. Mortada, A. Nasser, A. Ramadan, K.-C. Yao, and A. Mansour, "Location Information-Based Routing Protocol for Energy Harvesting Cognitive Radio Wireless Sensor Network," IEEE Access, vol. 13, pp. 9965–9980, 2025, doi: 10.1109/ACCESS.2024.3517741.

[29] S. Vahabi, A. Daneshvar, M. Eslaminejad, and S. E. Dashti, "CBDS2R: A Cluster-Based Depth Source Selection Routing for

RESEARCH ARTICLE

Underwater Wireless Sensor Network," IEEE Trans Signal Inf Process Netw, vol. 9, pp. 468–476, 2023, doi: 10.1109/TSIPN.2023.3299108.

[30] N. D. Tan and V.-H. Nguyen, "EE-TLT: Energy-efficient routing protocol using two-level tree-based clustering in wireless sensor network," Journal of Communications and Networks, vol. 25, no. 6, pp. 734–749, 2023, doi: 10.23919/JCN.2023.000038.

[31] M. Weber, G. Fersi, and F. Derbel, "Fog-Based Bootstrapping and Failure Repair Protocols for Wake-Up Receiver (WuRx)-Based Wireless Sensor Networks," IEEE Access, vol. 12, pp. 90073–90083, 2024, doi: 10.1109/ACCESS.2024.3419813.

[32] I. Jemili, D. Ghrab, A. Belghith, M. Mosbah, and S. Al-Ahmadi, "Cross-layer multipath approach for critical traffic in duty-cycled wireless sensor networks," Journal of Network and Computer Applications, vol. 191, p. 103154, 2021, doi: https://doi.org/10.1016/j.jnca.2021.103154.

[33] N. Kanthimathi and Dejey, "Void handling using Geo-Opportunistic Routing in underwater wireless sensor networks," Computers & Electrical Engineering, vol. 64, pp. 365–379, 2017, doi: https://doi.org/10.1016/j.compeleceng.2017.07.016.

Authors

R. Karthikeyan pursuing his Ph.D in Bharathiar University. Currently, he is working as Assistant Professor in the Department of Computer Technology at Sri Krishna Adithya College of Arts and Science, Coimbatore, Tamil Nadu, India.

R. Vadivel Completed his B.E. in Periyar University. M.E. in Annamalai University. He obtained his PhD degree from Manonmaniam Sundaranar University. At present, he is working as an Assistant Professor in the Department of Information Technology, Bharathiar University, Coimbatore. He has published more than 45 research papers in National, International Journals and Conferences. His research interest lies in the area of Computer Networks & Security, Mobile Computing, Mobile Ad-Hoc Networks, Wireless Sensor Networks, Data mining and Digital Signal Processing. He is a life member of CSI, ISTE, ACS, ISCA, AMIE, IACSIT and IAENG.

How to cite this article:

R. Karthikeyan, R. Vadivel, "Resilient and Self-Healing Wireless Communication Using SQUIMONET for Energy-Efficient and Role-Aware WSNs", International Journal of Computer Networks and Applications (IJCNA), 12(5), PP: 737-763, 2025, DOI: 10.22247/ijcna/2025/44.