Journal of Theoretical and Applied Information Technology
15th February 2026. Vol.104. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MICROCHAETUS RAPPI-INSPIRED SECURE AND REGENERATIVE ROUTING PROTOCOL (MR-SRRP) FOR ADAPTIVE AND ENERGY-EFFICIENT CLOUD COMMUNICATION NETWORKS

VATCHALA B[1], PREETHI G[2]
[1]Research Scholar, Department of Computer Science, PRIST Deemed University, Thanjaur, India
[2]Associate Professor, Department of Computer Science, PRIST Deemed University, Thanjaur, India
E-mail: [1] vatchala2020@gmailcom, [2]mgpreethi@gmail.com

ABSTRACT
Cloud communication networks require routing mechanisms that sustain security, adaptability, and energy efficiency under rapidly changing virtual workloads and dense topologies. Conventional routing approaches experience route instability, excessive energy usage, and delayed recovery in large-scale cloud environments. This study presents the Microchaetus Rappi-Inspired Secure and Regenerative Routing Protocol (MR-SRRP), a biologically driven framework that models regenerative behavior and energy-conserving movement patterns of Microchaetus rappi within an AODV-based routing structure. The goal of this work is to design a self-healing and secure routing protocol capable of restoring disrupted paths, balancing energy consumption, and maintaining low-latency communication. The underlying hypothesis assumes that embedding biological regeneration and adaptive intelligence into cloud routing decisions enhances route stability, packet reliability, energy utilization, and cryptographic diffusion strength. The protocol integrates encrypted tunneling, trust-driven authentication, regenerative key scheduling, and dynamic route rejuvenation across twelve coordinated phases. Simulation evaluation demonstrates improved delay, packet delivery, throughput, and energy conservation, with an avalanche diffusion strength of 86.14%, validating the protocol's effectiveness for adaptive and secure cloud communication environments.

Keywords: *Routing, Cloud, Encryption, Security, Avalanche, Energy*

1. INTRODUCTION

Cloud computing forms the backbone of today's digital ecosystems, offering scalable computing, networking, and storage services through virtualized infrastructures [1]. It enables seamless data processing and application deployment across distributed environments, including multi-cloud and edge-cloud architectures. Efficient routing plays a crucial role in ensuring seamless communication among virtual nodes, directly impacting data transmission speed, latency, and reliability [2]. As cloud environments expand, routing must evolve beyond static structures to dynamic, adaptive mechanisms that sustain performance across fluctuating workloads and heterogeneous platforms. Intelligent routing ensures continuous coordination among cloud resources, improving overall system responsiveness and operational stability.

Routing protocols in cloud communication networks determine how data is transmitted across interconnected nodes, striking a balance between network efficiency and service quality [3]. Adaptive routing mechanisms dynamically modify data paths based on bandwidth, congestion, and resource availability, ensuring uninterrupted communication under variable conditions. These algorithms enhance performance by maintaining optimal load distribution and reducing latency. They also enhance Quality of Service and Quality of Experience parameters by optimizing throughput and minimizing packet loss [4]. Adaptive routing thereby sustains smooth interaction among cloud services while managing data-intensive workloads. This ability to reorganize communication paths in real-time allows cloud infrastructures to maintain reliable connectivity across large-scale, geographically distributed systems [5], [6].

Energy efficiency has become a defining factor in cloud communication design. Massive data exchanges and continuous server operations significantly contribute to energy consumption across global data centres [7]. Energy-aware routing mitigates this by selecting paths that minimize transmission power while maintaining communication quality. Integrating power-conscious decisions into routing logic supports sustainable computing by reducing operational costs

and extending the equipment's lifespan. Such optimization aligns with green computing principles, ensuring that cloud platforms operate with a smaller energy footprint and improved resource utilization [8]. Energy-efficient routing thus contributes to both environmental sustainability and long-term infrastructure reliability within modern cloud ecosystems.

Secure communication remains an essential aspect of cloud networking. Data traversing virtual environments faces threats from unauthorized access, interception, or alteration. Secure routing frameworks incorporate encryption, authentication, and trust validation to safeguard data integrity and confidentiality [9]. By building trust relationships among nodes, secure routing prevents malicious interference and ensures that routing decisions remain verifiable and tamper-resistant. These frameworks ensure data reliability across multi-tenant architectures, thereby reinforcing privacy and compliance in dynamic network conditions. Security-aware routing thereby enhances dependability and resilience across distributed cloud infrastructures handling sensitive information [10].

The significance of this study emerges from the growing reliance on cloud infrastructures that demand routing mechanisms capable of sustaining security, adaptability, and energy efficiency under continuous environmental variation. The primary goal of this research is to develop a regenerative routing protocol that integrates biological intelligence with on-demand routing logic to maintain reliable and secure cloud communication. The guiding hypothesis states that modeling the regenerative and energy-conserving characteristics of Microchaetus rappi within cloud routing decisions improves route recovery capability, packet delivery reliability, energy utilization balance, and cryptographic diffusion strength in dense and dynamic cloud networks.

This work centers on a single unifying idea: biologically inspired regeneration can be systematically translated into secure and energy-aware routing intelligence for cloud communication networks. The proposed MR-SRRP framework demonstrates how regenerative behavior, adaptive tunneling, and distributed repair can jointly maintain stable communication under dynamic cloud conditions. By structuring routing as a continuous cycle of exploration, recovery, and rejuvenation, the protocol establishes a clear functional link between biological principles and practical cloud networking challenges. This perspective positions the work as a contribution toward resilient, self-sustaining, and security-conscious cloud routing architectures with long-term operational impact.

1.1. Problem Statement

Cloud communication networks demand routing mechanisms that maintain secure, adaptive, and energy-efficient data exchange under dynamic conditions. Fluctuating workloads, latency, and resource availability necessitate that routing systems dynamically adjust communication paths in real-time without compromising stability or trust. Existing frameworks work efficiently in static or small-scale networks but struggle to manage complex, distributed cloud infrastructures. The challenge lies in achieving continuous connectivity, low energy usage, and robust security in dynamic virtual environments. The MR-SRRP addresses this challenge by combining biological adaptability with AODV-based routing logic to create an intelligent framework that ensures secure, regenerative, and energy-aware communication in evolving cloud ecosystems.

1.2. Motivation

Cloud computing environments require routing systems that are self-organising, adaptive, and capable of recovering from disruptions. Biological organisms exhibit exceptional capabilities for self-repair, environmental responsiveness, and energy efficiency traits that are ideal for optimizing cloud routing processes. The Microchaetus rappi earthworm exhibits regenerative and energy-conserving behaviour that mirrors the adaptability required in cloud communication. Incorporating these characteristics into AODV routing enables MR-SRRP to regenerate lost routes, minimize energy waste, and enhance network security. The biological model motivates the development of an intelligent, self-healing routing framework that improves reliability, responsiveness, and sustainability in large-scale cloud infrastructures.

1.3. Objectives

The MR-SRRP develops a secure, regenerative, and energy-efficient routing protocol for adaptive cloud communication networks using AODV principles. The design models Microchaetus rappi-inspired regeneration and adaptability within AODV's route discovery and maintenance processes. The framework introduces energy-aware path selection and trust-driven metrics to enhance security and resource balance. MR-SRRP aims to

improve packet delivery ratio, reduce energy consumption, and shorten route recovery time under dynamic workloads. It evaluates performance in simulated cloud environments to measure gains in efficiency, reliability, and security compared to traditional adaptive routing systems while maintaining scalability and robustness in heterogeneous network conditions.

2. LITERATURE REVIEW

"Parallel Multi-Hop Acceleration" [1] employs simultaneous routing computation across HPC and cloud layers. Network segments process routing tables in parallel threads, synchronizing through a shared controller that merges sub-paths for dense small-cell links. Task partitioning minimizes propagation delay, while adaptive scaling tunes thread allocation based on node density. Parallel cores continuously refine routing states, accelerating decision cycles for massive 5G backhaul data exchanges. "Hybrid Cloud Plane Delegation" [2] splits control and data functions between edge routers and virtualized cloud nodes. Local routers retain essential control logic, while remote cloud agents manage flow processing and route recalculation. Data streams travel through encrypted tunnels, and synchronization feedback dynamically adjusts rule tables. This delegation model enhances routing flexibility and reduces local computational load through cloud-driven coordination. "Federated Deep Fronthaul Routing" [3] applies distributed Deep Q-Learning where edge units train routing agents collaboratively. Each node learns link states and delay costs, transmitting model updates to a federated aggregator. The combined policy selects optimal fronthaul segments for offloaded tasks, balancing delay and computation limits. Continuous updates enable dynamic adaptation to variations in mobility and traffic in Open RAN.

"RMCF-Driven Request Orchestration" [4] integrates cost-flow optimization for joint service mapping and route control. Nodes estimate resource cost, latency, and bandwidth to assign service routes. The RMCF model updates flow paths using local congestion metrics, redirecting data to underused nodes. Coordinated edge-cloud updates sustain minimal response time under variable demand. "Cognitive Green Routing" [5] establishes adaptive IPv6-based routing through cognitive inference. Each node monitors link reliability, residual energy, and packet success to adjust routing logic. The system encodes behavioural scores into IPv6 headers, thereby forming secure, low-energy routes. Cognitive feedback enables self-learning route repair and energy-balanced transmission across the ad-hoc mesh. "Logical Fault Verifier" [6] constructs a modular verification engine for virtual private cloud setups. The system models network components as logic functions, mapping address translation, routing, and filtering operations. Each configuration undergoes automated reachability and isolation checks across multiple logical layers. Parallel fault localization routines identify conflicts in access rules and connection paths. This verification loop ensures configuration accuracy and rapid fault tracing in large-scale virtualized environments.

"GAVNS-Driven Care Routing" [7] coordinates caregiver assignments and travel paths using a hybrid genetic–neighborhood algorithm. Caregiver skills, time windows, and caretaker preferences form weighted objectives processed through the analytic hierarchy model. The optimiser generates rosters while simultaneously computing vehicle routes to minimise overtime and travel expenses. Each iteration evolves feasible pairings, refining route feasibility and satisfaction scores under real-world caregiving constraints. "Edge-Scale Routing Optimizer" [8] manages workload spikes in multi-edge clusters using two-timescale Lyapunov optimization. Significant timescale decisions adjust cluster scaling, while smaller intervals handle request routing among edge nodes. Resource-aware rounding algorithms solve mixed-integer constraints, aligning cost with latency tolerance. The framework continuously rebalances clusters, minimizing average response delay under fluctuating edge workloads. "Authenticated Task Routing" [9] combines vehicle authentication and fog-based offloading to maintain secure VANET routing. Each vehicle node verifies identity keys before dynamic route computation. Tasks with latency demands shift toward fog layers through adaptive schedulers. Routing and scheduling modules co-optimally integrate authentication, task placement, and link stability, ensuring high accuracy and low delay even under rapid mobility.

"Cooperative Edge Placement" [11] integrates integer linear programming with heuristic rounding for coordinated service deployment. Edge nodes exchange state vectors to assign computation tasks to users near latency-critical locations. The routing controller employs convex set mapping to optimize cache usage and request flow. Cooperative adjustments among base stations distribute workloads evenly, sustaining minimal delay and balanced cloud-edge utilization. "Predictive

Multipath Routing" [12] constructs proactive V2X routes using link prediction and multipath validation. Vehicle mobility and signal strength models forecast link degradation, triggering early rerouting actions. A virtual routing layer evaluates multiple candidate paths, verifying their stability and adherence to hop constraints. Top-ranked paths undergo real-time validation before activation, enabling seamless transitions between vehicle and infrastructure links for stable cloud access in IoV systems. "Self-Organized 5G Routing" [13] formulates a clustering-based routing scheme for intelligent transportation grids. Each vehicle node self-configures communication links using local connectivity metrics and energy feedback. Adaptive clustering reduces routing overhead and maintains strong link reliability at low mobility speeds. Pheromone-inspired updates refine next-hop selection, preserving network lifetime while stabilizing data delivery across connected transport networks.

"Twin-Based Job Routing" [14] integrates digital twin synchronisation with cloud-edge computing for industrial scheduling. Time–space models map production and transportation resources, utilizing a rolling window strategy for dynamic rescheduling. Edge controllers simulate process states while the cloud resolves conflict-free routing via enhanced Dijkstra encoding. Continuous twin feedback corrects disturbances in milliseconds, ensuring energy-efficient scheduling of robotic and automated job systems. "LSTM-MADDPG Flow Routing" [15] employs reinforcement learning for adaptive multi-domain flow control. Each domain hosts autonomous agents that coordinate via long short-term memory and multi-agent deep deterministic policy gradients. Reward-driven updates strike a balance between bandwidth allocation and fairness in response to abrupt traffic shifts. Real topology data drives temporal continuity learning, improving delay convergence and throughput stability across distributed data centers. "Relay-Optimized CN-WAN Routing" [16] designs a latency-aware relay selection method for software-defined WANs. Overlay routes are computed by minimizing the number of intermediate relay nodes while adhering to strict end-to-end delay limits. Scalable algorithms handle varying network sizes through iterative relay pruning. Virtual network controllers coordinate route adjustments in cloud-native environments, ensuring SLA compliance and minimizing overall transmission costs.

"Finite-State Chaotic Compressed Sensing (FSCCS)" [17] employs finite-state chaotic dynamics to capture and rebuild remote sensing images using sparse sampling. Each signal is represented by a reduced coefficient set, compressing spatial data before transmission to the cloud. A chaotic state generator defines sampling patterns, ensuring randomness in measurement while retaining essential features. The reconstruction module reorders sparse coefficients through iterative transformation, synchronizing phase space states to recover the image accurately. This dual-phase mechanism minimizes transmission load, optimizes storage, and maintains coherence in cloud-based image registration workflows. "Conceptual Security Model (CSM)" [18] structures continuous protection across software development through automated phase-wise checkpoints. Security configurations begin at the planning stage, where threat models define control policies. During the build process, secure coding and encryption layers are embedded, followed by vulnerability testing through automated scans. The deployment phase activates real-time log monitoring and adaptive patching cycles. Each feedback loop reinforces security baselines, aligning with open-source integration and continuous verification principles, which enable self-updating defences within evolving development environments.

Bio-inspired intelligence provides a powerful model for designing adaptive and regenerative routing in cloud networks [19]-[31]. Natural organisms exhibit self-organization, environmental responsiveness, and energy-efficient behavior that can be computationally emulated. The Microchaetus rappi, renowned for its regenerative abilities and energy-efficient movement, exemplifies these traits [32]-[41]. Translating its behaviour into algorithmic design results in routing mechanisms that autonomously repair, adapt, and optimize communication paths under fluctuating network conditions. Such biologically inspired strategies enhance the capacity of cloud networks to maintain stability and efficiency in the face of uncertainty [42]-[49]. Integrating these natural principles enables cloud systems to achieve secure, adaptive, and energy-efficient communication, reflecting harmony between computational optimization and biological intelligence.

3. MICROCHAETUS RAPPI-INSPIRED SECURE AND REGENERATIVE ROUTING PROTOCOL (MSRRP)

This section presents the materials and methods employed to design and evaluate the proposed MR-SRRP framework. The methodology

includes biologically inspired routing formulation, mathematical modeling of adaptive behaviors, algorithmic realization through multi-phase operations, and controlled simulation using a cloud-based environment. Each phase contributes to secure route discovery, regeneration, energy regulation, and performance validation.

The proposed Microchaetus Rappi-Inspired Secure and Regenerative Routing Protocol (MR-SRRP) introduces a biologically adaptive routing architecture that merges regenerative behavior and energy-efficient motion patterns of Microchaetus rappi with the dynamic principles of AODV routing. The design aims to deliver secure, stable, and energy-optimized communication across distributed cloud infrastructures. Each operational stage emulates an ecological function—exploration, tunneling, adaptation, and regeneration translated into computational steps that manage route discovery, fault recovery, trust-based authentication, and energy regulation. Security is reinforced through encrypted tunnels and regenerative key scheduling, ensuring continuous confidentiality and integrity within fluctuating environments. The twelve algorithmic phases collectively describe a self-healing routing cycle that sustains connectivity, minimizes latency, and balances energy usage. This biologically grounded model establishes a regenerative foundation for adaptive, secure, and sustainable cloud communication, later validated through delay, throughput, energy, and diffusion performance metrics.

3.1. Surface and Subsurface Exploration

In the first stage of the MR-SRRP, cloud instances embark on a mission to explore the network area, much like the earthworm's surface and subsurface foraging behavior. This exploration involves identifying nodes, which are essential communication points within the network. Each node is denoted by N_i, where i represents its unique identifier.

$$N_i \tag{1}$$

where N_i represents the ith node in the network.

After identifying the nodes, the next step is establishing connections between them. This process involves determining the optimal paths for data transmission based on proximity and signal strength. The connectivity between nodes is represented by the adjacency matrix A, where a_{ij} denotes the connection between nodes N_i and N_j.

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \tag{2}$$

where A is the adjacency matrix representing connections between nodes, a_{ij} is the connectivity between nodes N_i and N_j.

To ensure reliable communication, assessing the signal strength between nodes is crucial for ensuring effective communication. The signal strength S_{ij} between nodes N_i and N_j is determined based on parameters such as distance and interference.

$$S_{ij} = \frac{1}{d_{ij}^2} \tag{3}$$

where S_{ij} represents the signal strength between nodes N_i and N_j, d_{ij} is the distance between nodes N_i and N_j.

After measuring signal strength, MR-SRRP selects the optimal paths for data transmission between nodes. The path selection involves identifying routes with the highest signal strength and the least interference. The optimal path from the node N_i to node N_j is denoted by P_{ij}

$$P_{ij} = argmax_{P_{ij}} S_{ij} \tag{4}$$

where P_{ij} represents the optimal path from the node N_i and N_j, d_{ij} denotes a candidate path from the node N_i and N_j.

In dynamic network environments, path adjustments may be necessary to accommodate changes in signal strength or network topology. MR-SRRP utilizes a dynamic path adjustment mechanism to reroute data adaptively in response to real-time conditions. The adjusted path P'_{ij} between nodes N_i and N_j is determined iteratively.

$$P'_{ij} = P_{ij} + \Delta P_{ij} \tag{5}$$

where P'_{ij} represents the adjusted path between nodes N_i and N_j, ΔP_{ij} denotes the change in the original path P_{ij} based on dynamic adjustments.

3.2. Adaptive Routing

Adaptive routing in the MR-SRRP begins with initializing routing tables within each node. Each routing table, denoted by R_i for node N_i, stores information about available routes and their associated costs.

$$R_i = \begin{bmatrix} r_{i1} & r_{i2} & \cdots & r_{in} \\ r_{i1} & r_{i2} & \cdots & r_{in} \\ \vdots & \vdots & \cdots & \vdots \\ r_{in} & r_{in} & \cdots & r_{in} \end{bmatrix} \quad (6)$$

where R_i is the routing table for the node N_i, r_{ij} represents the cost associated with the route from the node N_i to node N_j.

To facilitate adaptive routing, MR-SRRP calculates the cost of each route based on factors such as distance, signal strength, and network congestion. The route cost C_{ij} from node N_i to node N_j is determined using a weighted sum of these factors.

$$C_{ij} = \alpha . D_{ij} + \beta . S_{ij} + \gamma . C_{congestion} \quad (7)$$

where C_{ij} represents the cost of the route from the node N_i to node N_j, D_{ij} is the distance between nodes N_i and N_j, S_{ij} is the signal strength between nodes N_i and N_j, $C_{congestion}$ represents the congestion level along the route, α, β, γ are weighting factors that determine the importance of each factor in the cost calculation.

MR-SRRP dynamically adjusts route costs based on real-time network conditions. This adaptive mechanism allows the protocol to respond to changes, such as fluctuations in signal strength or sudden increases in network traffic. The adjusted route cost C'_{ij} between nodes N_i and N_j is recalculated iteratively.

$$C'_{ij} = C_{ij} + \Delta C_{ij} \quad (8)$$

where C'_{ij} represents the adjusted route cost between nodes N_i and N_j, ΔC_{ij} denotes the change in the original route cost C_{ij} based on dynamic adjustments.

After calculating route costs, MR-SRRP selects the optimal route for data transmission based on the criterion of minimum cost. The optimal route P_{ij} from node N_i to node N_j is determined by minimizing the route cost across all available routes.

$$P_{ij} = argmin_{P_{ij}} C_{ij} \quad (9)$$

where P_{ij} represents the optimal route from the node N_i to node N_j, p_{ij} denotes a candidate route from the node N_i to node N_i.

In dynamic network environments, path adjustments may be necessary to maintain optimal routing. MR-SRRP updates routing tables and recalculates route costs periodically to adapt to changes in network conditions. This adaptive path-updating process ensures efficient and reliable data transmission even in fluctuating environments.

3.3. Burrowing and Tunneling

In this step of the MR-SRRP, cloud instances establish virtual tunnels for efficient data transmission inspired by the burrowing behavior of earthworms. This process involves creating pathways through which data packets can travel, optimizing network connectivity, and minimizing latency.

The burrowing and tunneling process in MR-SRRP begins with formulating a tunnel formation strategy. Cloud instances utilize algorithms to determine the optimal locations for tunnel creation, taking into account node density and signal strength.

$$T_i = \sum_{j=1}^{n} t_{ij} \quad (10)$$

where T_i represents the total tunnel formation score for the node N_i, t_{ij} denotes the tunnel formation score contributed by the neighboring node N_j.

Once the optimal locations are identified, cloud instances initiate tunnel construction by establishing direct communication links between adjacent nodes. These links form the basis of the virtual tunnels through which data packets will be transmitted.

$$L_{ij} = \begin{cases} 1, if\ there\ is\ a\ link\ between\ nodes \\ N_i\ and\ N_j \\ 0 \quad otherwise \end{cases} \quad (11)$$

where L_{ij} indicates the presence (1) or absence (0) of a direct link between nodes $N_i$and N_j.

After initial tunnel construction, MR-SRRP optimizes the tunnels to ensure efficient data transmission. This optimization process involves adjusting the tunnel routing paths to minimize transmission delays and maximize network throughput.

$$O_{ij} = \frac{1}{d_{ij}} . \frac{1}{S_{ij}} \quad (12)$$

where O_{ij} represents the optimization score for the route within the tunnel between nodes N_i and N_j, d_{ij} denotes the distance between nodes N_i and N_j, S_{ij}

represents the signal strength between nodes N_i and N_j.

To ensure the reliability of data transmission, MR-SRRP incorporates tunnel maintenance mechanisms. Cloud instances periodically monitor the condition of the tunnels and perform repairs or adjustments as needed to prevent disruptions in communication.

$$M_i = \frac{1}{\sum_{j=1}^{n} m_{ij}} \quad (13)$$

where M_i represents the maintenance score for the node N_i, m_{ij} denotes the maintenance effort required for maintaining the tunnel between nodes N_i and N_j.

In addition to primary tunnels, MR-SRRP establishes redundant tunnels to enhance network resilience and redundancy. These redundant tunnels serve as backup pathways for data transmission, ensuring continuity of communication in the event of tunnel failures.

$$R_i = \sum_{j=1}^{n} r_{ij} \quad (14)$$

where R_i represents the total redundancy score for the node N_i, r_{ij} denotes the redundancy score contributed by the neighboring node N_j.

MR-SRRP incorporates dynamic tunnel adaptation mechanisms to respond to changes in network conditions. Cloud instances adjust tunnel configurations in real-time based on traffic patterns and node availability, optimizing data transmission efficiency.

$$A_{ij} = \frac{1}{t_{ij}} . \frac{1}{c_{ij}} \quad (15)$$

where A_{ij} represents the adaptation score for the tunnel between nodes N_i and N_j, t_{ij} denotes the traffic intensity along the tunnel, c_{ij} represents the congestion level within the tunnel.

3.4. Dynamic Route Restoration

In this phase of the MR-SRRP, the network dynamically restores routing paths in response to failures or disruptions. Like the earthworm's ability to adapt to changing environments, MR-SRRP employs mechanisms to ensure uninterrupted data transmission.

The first step in dynamic route restoration is the detection of route failures. Cloud instances continuously monitor the status of routing paths and detect any abnormalities or interruptions in data transmission.

$$F_i = \sum_{j=1}^{n} f_{ij} \quad (16)$$

where F_i represents the failure score for the node N_i, f_{ij} denotes the failure indication received from a neighboring node N_j.

Upon detecting a route failure, MR-SRRP initiates the process of route recalculation to identify alternative paths for data transmission. This involves evaluating the available routes and selecting the most suitable option based on predefined criteria.

$$R'_{ij} = argmin_{r_{ij}} C_{ij} \quad (17)$$

where R'_{ij} represents the recalculated route from the node $N_i$to node N_j, C_{ij} is the cost associated with the route from the node $N_i$to node N_j.

In parallel with route recalculation, MR-SRRP activates backup routes to ensure continuous data transmission while the primary route is restored. Backup routes are temporary alternatives and help maintain network connectivity during route failures.

$$B_{ij} = \begin{cases} 1, if\ backup\ route\ between\ N_i\ and \\ N_j\ is\ active \\ 0,\ otherwise \end{cases} \quad (18)$$

where B_{ij} indicates the activation status of the backup route between nodes $N_i$and N_j.

Once alternative routes are identified, MR-SRRP employs a route restoration strategy to restore data transmission along the selected paths. This strategy may involve rerouting data packets, adjusting transmission parameters, or prioritizing specific routes over others to optimize network performance.

$$S_{ij} = \frac{1}{r_{ij}} . \frac{1}{d_{ij}} \quad (19)$$

where S_{ij} represents the restoration score for the route between nodes N_i and N_j, r_{ij} denotes the reliability of the route, d_{ij} is the distance between nodes N_i and N_j.

After restoring data transmission along alternative routes, MR-SRRP verifies the integrity and reliability of the restored paths. Cloud instances exchange acknowledgments and status updates to ensure the delivery of data packets without errors or losses.

$$V_{ij} = \frac{1}{\sum_{k=1}^{n} v_{ijk}} \quad (20)$$

where V_{ij} represents the verification score for the route between nodes N_i and N_j, v_{ijk} denotes the verification acknowledgment received from a neighboring node N_k.

Dynamic route restoration in MR-SRRP enhances network resilience by promptly responding to route failures and ensuring continuous data transmission in dynamic environments.

3.5. Redundant Route Establishment

Redundancy is a crucial aspect of network design, enhancing resilience and fault tolerance. In this phase of the MR-SRRP, redundant routes are established to provide backup pathways for data transmission, ensuring continuity of communication in the face of route failures or disruptions.

The establishment of redundant routes begins with the formulation of a redundancy strategy. Cloud instances analyze network topology and identify critical communication paths that are susceptible to failure. Based on this analysis, redundant routes are strategically deployed to mitigate the impact of potential failures.

$$R_{ij} = \sum_{k=1}^{n} r_{ijk} \quad (21)$$

where R_{ij} represents the redundancy score for the route between nodes N_i and N_j, r_{ijk} denotes the redundancy contribution from a neighboring node N_k.

The selection of redundant routes is based on predefined criteria to optimize network resilience and minimize resource utilization. Cloud instances prioritize routes with low latency, high bandwidth, and minimal interference, ensuring that redundant pathways can effectively handle data transmission in the event of primary route failures.

$$C_{ij} = \alpha . D_{ij} + \beta . B_{ij} + \gamma . S_{ij} \quad (22)$$

where C_{ij} represents the selection criteria score for the route between nodes N_i and N_j, D_{ij} denotes the distance between nodes N_i and N_j, B_{ij} represents the available bandwidth along the route, S_{ij} denotes the signal strength between nodes N_i and N_j, α, β, γ are weighting factors determining the importance of each criterion.

Once redundant routes are selected, MR-SRRP employs an establishment algorithm to configure the backup pathways. This algorithm ensures that redundant routes are efficiently deployed without causing network congestion or resource depletion.

$$E_{ij} = \frac{1}{c_{ij}} . \frac{1}{b_{ij}} \quad (23)$$

where E_{ij} represents the establishment score for the redundant route between nodes N_i and N_j, c_{ij} denotes the congestion level along the route, b_{ij} represents the available bandwidth for the redundant route.

Once established, redundant routes undergo optimization to ensure their effectiveness in handling data transmission. Optimization techniques, such as load balancing and route diversification, are applied to maximize the benefits of redundancy while minimizing resource wastage.

$$O_{ij} = \frac{1}{l_{ij}} . \frac{1}{d_{ij}} \quad (24)$$

where O_{ij} represents the optimization score for the redundant route between nodes N_i and N_j, l_{ij} denotes the load distribution across the redundant route, d_{ij} is the distance between nodes N_i and N_j.

After deployment, redundant routes are continuously monitored to ensure availability and reliability. Cloud instances periodically assess the performance of redundant pathways and perform maintenance activities such as route updates or repairs to preserve their functionality.

$$M_{ij} = \frac{1}{m_{ij}} \quad (25)$$

where M_{ij} represents the maintenance score for the redundant route between nodes N_i and N_j, m_{ij} denotes the maintenance effort required to maintain the route.

Redundant routes are activated or deactivated dynamically based on network conditions and traffic patterns. Cloud instances autonomously manage the redundancy status of routes, ensuring that backup pathways are available when needed while avoiding unnecessary resource consumption during regular operation.

3.6. Fragmented Route Recovery

Fragmentation of routes can occur due to various factors such as node failures, network congestion, or environmental interference. In this phase of the MR-SRRP, mechanisms are implemented to recover fragmented routes and restore seamless data transmission across the network.

The first step in recovering fragmented routes is the detection of these routes. Cloud instances continuously monitor the status of routing paths and identify any segments that have been disrupted or severed.

$$D_i = \sum_{j=1}^{n} d_{ij} \quad (26)$$

where D_i represents the detection score for the node N_i, d_{ij} denotes the detection indication received from a neighboring node N_j.

Once fragmented routes are detected, MR-SRRP initiates the process of route reconstruction to restore connectivity. This involves identifying alternative paths and reassembling the fragmented segments to establish continuous data transmission.

$$R_{ij} = argmax_{r_{ij}} S_{ij} \quad (27)$$

where R_{ij} represents the reconstructed route between nodes N_i and N_j, S_{ij} is the signal strength between nodes N_i and N_j.

MR-SRRP optimizes the newly assembled paths during route reconstruction to ensure efficient data transmission. Optimization techniques such as load balancing and congestion avoidance are applied to maximize network performance.

$$O_{ij} = \frac{1}{l_{ij}} . \frac{1}{c_{ij}} \quad (28)$$

where O_{ij} represents the optimization score for the reconstructed route between nodes N_i and N_j, l_{ij} denotes the load distribution across the route, c_{ij} represents the congestion level along the route.

After route reconstruction, MR-SRRP verifies the integrity and reliability of the restored paths. Cloud instances exchange acknowledgments and status updates to ensure the delivery of data packets without errors or losses.

$$V_{ij} = \frac{1}{\sum_{k=1}^{n} v_{ijk}} \quad (29)$$

where V_{ij} represents the verification score for the reconstructed route between nodes N_i and N_j, v_{ijk} denotes the verification acknowledgment received from a neighboring node N_k.

In dynamic network environments, route adjustments may be necessary to optimize performance and adapt to changing conditions. MR-SRRP dynamically adjusts routing paths based on real-time feedback and network dynamics.

$$A_{ij} = \frac{1}{t_{ij}} . \frac{1}{s_{ij}} \quad (30)$$

where A_{ij} represents the adjustment score for the route between nodes N_i and N_j, t_{ij} denotes the traffic intensity along the route, s_{ij} represents the stability of the route.

MR-SRRP incorporates route maintenance mechanisms to ensure the long-term reliability of reconstructed routes. Cloud instances periodically evaluate the condition of routing paths and perform necessary repairs or adjustments to prevent future fragmentation.

$$M_{ij} = \frac{1}{m_{ij}} \quad (31)$$

where M_{ij} represents the maintenance score for the reconstructed route between nodes N_i and N_j, m_{ij} denotes the maintenance effort required to maintain the route.

Fragmented route recovery in MR-SRRP enhances network resilience by promptly restoring connectivity and ensuring uninterrupted data transmission in dynamic environments.

3.7. Distributed Route Repair

In this phase of the MR-SRRP, the protocol employs distributed mechanisms to repair broken routes in the network. Inspired by the earthworm's decentralized nervous system, MR-SRRP ensures that route repair processes are autonomously managed by individual nodes, enhancing the robustness and fault tolerance of the network.

The distributed route repair process begins with individual nodes detecting route breakages. Each node continuously monitors the status of its neighboring routes and identifies any disruptions or failures in data transmission.

$$B_i = \sum_{j=1}^{n} b_{ij} \quad (32)$$

where B_i represents the breakage score for the node N_i, b_{ij} denotes the breakage indication received from a neighboring node N_j.

Upon detecting a route breakage, the affected node notifies its neighboring nodes about the disruption. This notification includes information about the broken route and the corresponding node identifiers, enabling neighboring nodes to take appropriate action to repair the route.

$$N_{ij} = \begin{cases} 1, & if\ node\ N_i\ notifies\ node\ N_j \\ & about\ route\ breakage \\ 0, & otherwise \end{cases} \quad (33)$$

where N_{ij} indicates whether the node N_i notifies node N_j about a route breakage.

Upon receiving notification of a route breakage, neighboring nodes autonomously attempt to repair the broken route using local repair strategies. These strategies may involve rerouting data packets through alternative paths or establishing temporary connections to bypass the disrupted segment.

$$R_{ij} = argmax_{r_{ij}} S_{ij} \quad (34)$$

where R_{ij} represents the repaired route between nodes N_i and N_j, S_{ij} is the signal strength between nodes N_i and N_j.

After attempting local route repair, neighboring nodes engage in distributed consensus to determine the most effective repair strategy. Through consensus algorithms, nodes collaboratively evaluate the proposed repair solutions and converge on a consensus decision to ensure that the repaired route is stable and reliable.

$$C_{ij} = \frac{1}{\sum_{k=1}^{n} c_{ijk}} \quad (35)$$

where C_{ij} represents the consensus score for the repaired route between nodes N_i and N_j, c_{ijk} denotes the consensus contribution of the neighboring node N_k.

Once a consensus on the repair strategy is reached, the repaired route undergoes validation to ensure its integrity and reliability. Cloud instances exchange verification messages to confirm that data packets can be transmitted along the repaired path without errors or losses.

$$V_{ij} = \frac{1}{\sum_{k=1}^{n} v_{ijk}} \quad (36)$$

where V_{ij} represents the validation score for the repaired route between nodes N_i and N_j, v_{ijk} denotes the verification acknowledgment received from a neighboring node N_k.

The repaired route is restored for data transmission upon successful validation, and regular network operation resumes. The distributed route repair process ensures that route disruptions are promptly addressed, maintaining continuous connectivity and data transmission in the network.

3.8. Responsive to Environmental Cues

In the MR-SRRP, responsiveness to environmental cues is integral to adapting to changing network conditions and optimizing routing decisions. Inspired by the earthworm's ability to sense and respond to environmental stimuli, MR-SRRP incorporates mechanisms that dynamically adjust routing strategies based on real-time ecological cues.

The first aspect of responsiveness to environmental cues involves individual nodes sensing environmental parameters. Cloud instances equipped with sensors continuously monitor ecological factors, including temperature, humidity, and signal interference levels.

$$E_i = \sum_{j=1}^{n} e_{ij} \quad (37)$$

where E_i represents the environmental cue score for the node N_i, e_{ij} denotes the environmental cue indication received from a neighboring node N_j.

Upon sensing environmental cues, nodes analyze the collected data to assess the current state of the network environment. This analysis involves evaluating the impact of ecological factors on routing performance and identifying potential areas for optimization.

$$A_{ij} = argmax_{a_{ij}} E_{ij} \quad (38)$$

where A_{ij} represents the analysis outcome for environmental cues between nodes N_i and N_j, E_{ij} denotes the environmental cue score between nodes N_i and N_j.

Based on the analysis of environmental cues, MR-SRRP dynamically adjusts routing strategies to optimize performance in response to changing conditions. This adjustment mechanism involves rerouting data packets, modifying transmission parameters, or prioritizing specific routes over others to ensure optimal network performance.

$$D_{ij} = \frac{1}{d_{ij}} . \frac{1}{s_{ij}} \quad (39)$$

where D_{ij} represents the dynamic adjustment score for the route between the node N_i and N_j, d_{ij} denotes the distance between nodes N_i and N_j, s_{ij}

represents the signal strength between nodes N_i and N_j.

After adjusting routing strategies, MR-SRRP makes adaptive routing decisions by analyzing environmental cues and implementing dynamic adjustments. These decisions prioritize routes least affected by environmental factors, ensuring robust and reliable data transmission.

$$R_{ij} = argmax_{r_{ij}} D_{ij} \quad (40)$$

where R_{ij} represents the adaptive routing decision for the route between nodes N_i and N_j, D_{ij} denotes the dynamic adjustment score for the route.

To further enhance responsiveness, MR-SRRP incorporates real-time feedback mechanisms that enable nodes to adjust routing decisions in response to immediate network conditions. This feedback loop ensures that routing strategies remain adaptive and responsive to rapidly changing environmental cues.

$$F_{ij} = \frac{1}{f_{ij}} \quad (41)$$

where F_{ij} represents the feedback score for the route between nodes N_i and N_j, f_{ij} denotes the feedback received from a neighboring node N_j.

Responding to environmental cues in MR-SRRP is not a one-time process but a continuous adaptation mechanism. Nodes constantly monitor environmental changes and adjust routing strategies accordingly, ensuring optimal performance and efficiency in dynamic network environments.

3.9. Exploratory Routing

Exploratory routing involves a proactive approach to route discovery and optimization, aiming to enhance network performance and efficiency. Rather than relying solely on predefined routes, MR-SRRP actively explores the network topology to identify alternative paths and adapt to changing conditions. This dynamic exploration enables MR-SRRP to maintain robust and resilient communication pathways, even in dynamic and unpredictable environments.

MR-SRRP employs sophisticated route discovery mechanisms to explore the network topology and identify potential routing paths. These mechanisms may include techniques such as flooding, where nodes broadcast routing queries to their neighboring nodes, or distributed algorithms that collaboratively search for optimal routes based on various metrics, including distance, signal strength, and congestion levels.

$$D_{ij} = \frac{1}{d_{ij}} . \frac{1}{s_{ij}} \quad (42)$$

where D_{ij} represents the exploration score for the route between node N_i and N_j, d_{ij} denotes the distance between nodes N_i and N_j, s_{ij} represents the signal strength between nodes N_i and N_j.

During route exploration, MR-SRRP dynamically adapts path selection criteria based on real-time network conditions and performance metrics. This adaptive approach allows MR-SRRP to prioritize routes with the best reliability, low latency, and minimal resource consumption, ensuring efficient data transmission.

$$P_{ij} = argmax_{P_{ij}} D_{ij} \quad (43)$$

where P_{ij} represents the selected path for exploration between nodes N_i and N_j, D_{ij} denotes the exploration score for the path.

As exploration progresses, MR-SRRP continuously evaluates the performance of discovered routes and adjusts routing decisions accordingly. Routes are dynamically updated based on feedback from neighboring nodes, ensuring the network adapts to changing conditions and maintains optimal communication pathways.

$$E_{ij} = \frac{1}{e_{ij}} \quad (44)$$

where E_{ij} represents the evaluation score for the route between nodes N_i and N_j, e_{ij} denotes the evaluation feedback received from a neighboring node N_j.

During exploration, MR-SRRP utilizes optimization strategies to enhance the efficiency of discovered routes further. These strategies may include load balancing, where traffic is distributed evenly across multiple routes, or route diversification, where redundant paths are established to improve fault tolerance and resilience.

$$O_{ij} = \frac{1}{o_{ij}} \quad (45)$$

where O_{ij} represents the optimization score for the route between nodes N_i and N_j, o_{ij} denotes the optimization effort required for the route.

Exploratory routing in MR-SRRP is not a static process but rather a dynamic and continuous exploration of the network topology. Nodes adapt

routing decisions in real-time based on immediate feedback and environmental cues, ensuring that the network remains responsive and adaptable to changing conditions.

$$A_{ij} = \frac{1}{a_{ij}} \quad (46)$$

where A_{ij} represents the adaptation score for the route between nodes N_i and N_j, a_{ij} denotes the adaptation feedback received from a neighboring node N_j.

3.10. Collaborative Foraging

Collaborative foraging within the MR-SRRP emulates the cooperative behavior observed in earthworm communities. As earthworms work together to optimize their foraging efforts, MR-SRRP nodes collaborate to enhance network efficiency and resilience. This step fosters mutual assistance among nodes, improving routing decisions and overall network performance.

Collaborative foraging in MR-SRRP begins with the sharing of information among nodes. Nodes exchange data regarding network topology, traffic patterns, and routing decisions, enabling them to make informed choices collectively.

$$I_{ij} = \frac{1}{i_{ij}} \quad (52)$$

where I_{ij} represents the information-sharing score between nodes N_i and N_j, i_{ij} denotes the information exchanged between nodes N_i and N_j.

Nodes collaboratively engage in route discovery processes, pooling resources to explore the network topology more efficiently. By sharing route exploration tasks, nodes can cover larger areas of the network, leading to the discovery of diverse routing paths.

$$C_{ij} = \frac{1}{c_{ij}} . \frac{1}{r_{ij}} \quad (53)$$

where C_{ij} represents the collaboration score for route discovery between nodes N_i and N_j, c_{ij} denotes the collaboration between nodes N_i and N_j, r_{ij} represents the reliability of the discovered route.

In collaborative foraging, nodes distribute the traffic load evenly across available routes. By balancing the load, nodes prevent network congestion and ensure optimal resource utilization.

$$L_{ij} = \frac{1}{l_{ij}} . \frac{1}{b_{ij}} \quad (54)$$

where L_{ij} represents the load-balancing score between nodes N_i and N_j, l_{ij} denotes the load distribution across the route, b_{ij} represents the available bandwidth for the route.

Nodes provide feedback to their neighbors regarding route performance and reliability. This information exchange enables nodes to collectively assess the quality of routing paths and make adjustments as needed.

$$F_{ij} = \frac{1}{f_{ij}} \quad (55)$$

where F_{ij} represents the feedback score for the route between nodes N_i and N_j, i_{ij} denotes the feedback received from a neighboring node N_i and N_j.

Collaborative foraging fosters adaptive decision-making processes among nodes. Nodes collectively evaluate routing options and dynamically adjust their decisions based on real-time feedback and environmental cues.

$$D_{ij} = \frac{1}{d_{ij}} . \frac{1}{s_{ij}} \quad (56)$$

where D_{ij} represents the decision-making score for the route between nodes N_i and N_j, d_{ij} denotes the distance between nodes N_i and N_j, s_{ij} represents the signal strength between nodes N_i and N_j.

3.11. Energy-Efficient Routing

Energy-efficient routing is paramount in the MR-SRRP to prolong the operational lifespan of cloud instances in ad-hoc networks. Inspired by the earthworm's energy-efficient burrowing techniques, MR-SRRP aims to minimize energy consumption while ensuring reliable data transmission. This step optimizes routing decisions to conserve energy resources and extend the network lifetime.

MR-SRRP prioritizes routes that consume minimal energy for data transmission. Nodes evaluate potential paths based on energy metrics, such as transmission power and distance, to select routes that minimize energy expenditure.

$$E_{ij} = \frac{1}{e_{ij}} \quad (57)$$

where E_{ij} represents the energy-efficient score for the route between nodes N_i and N_j, e_{ij} denotes the energy consumption along the route.

MR-SRRP utilizes sleep scheduling mechanisms to deactivate idle nodes, conserving energy intermittently. By entering sleep mode during

inactivity, nodes reduce energy consumption while maintaining network connectivity through neighboring nodes.

$$S_{ij} = \frac{1}{s_{ij}} \quad (58)$$

where S_{ij} represents the sleep scheduling score for nodes N_i. e_{ij} denotes the sleep duration for the node N_i.

MR-SRRP leverages opportunistic routing strategies to exploit transient network conditions and conserve energy. Nodes dynamically adjust routing paths based on real-time opportunities, such as encountering neighboring nodes with sufficient energy reserves or favorable transmission conditions.

$$O_{ij} = \frac{1}{o_{ij}} \quad (59)$$

where O_{ij} represents the opportunistic routing score for the route between nodes N_i and N_j, o_{ij} denotes the energy opportunity along the route.

MR-SRRP integrates energy harvesting capabilities to supplement node power sources and extend operational lifespans. Nodes harness ambient energy sources, such as solar or kinetic energy, to replenish their energy reserves and mitigate the reliance on finite power supplies.

$$H_{ij} = \frac{1}{h_{ij}} \quad (60)$$

where H_{ij} represents the energy harvesting score for the node N_i, o_{ij} denotes the energy harvested by the node N_i.

Through dynamic power management techniques, MR-SRRP optimizes node power usage based on network demands and resource availability. Nodes dynamically adjust transmission power, data processing rates, and sleep schedules to minimize energy consumption without compromising communication reliability.

$$P_{ij} = \frac{1}{p_{ij}} \quad (61)$$

where P_{ij} represents the power management score for the node N_i, p_{ij} denotes the power consumption by the node N_i.

3.12. Route Rejuvenation

MR-SRRP incorporates energy-aware congestion control mechanisms to mitigate energy wastage during periods of network congestion. Nodes regulate data transmission rates and prioritize traffic based on energy efficiency considerations to prevent unnecessary energy depletion.

Route rejuvenation in the MR-SRRP is a crucial mechanism for maintaining the efficiency and reliability of routing paths over time. Like earthworms regenerate and renew their burrows, MR-SRRP rejuvenates routes to counteract degradation and ensure optimal data transmission performance. This step periodically refreshes and optimizes routing paths to adapt to changing network conditions and prevent deterioration.

MR-SRRP continuously monitors the quality and performance of existing routing paths. Nodes assess metrics such as latency, packet loss, and signal strength to detect signs of degradation or deterioration in routing paths.

$$M_{ij} = \frac{1}{m_{ij}} \quad (62)$$

where M_{ij} represents the degradation monitoring score for the route between nodes N_i and N_j, m_{ij} denotes the degradation indication along the route.

Upon detecting signs of route degradation, MR-SRRP evaluates the severity of the degradation against predefined thresholds. Routes that exceed certain degradation thresholds are flagged for rejuvenation to prevent further deterioration and maintain optimal performance.

$$T_{ij} = \begin{cases} 1, & if\ route\ degradation \\ & exceeds\ threshold \\ 0, & otherwise \end{cases} \quad (63)$$

where T_{ij} indicates whether the route between nodes N_i and N_j exceeds the degradation threshold.

When routes surpass degradation thresholds, MR-SRRP triggers rejuvenation to refresh and optimize the affected routing paths. Rejuvenation may also be initiated periodically to prevent route deterioration and proactively ensure long-term network performance.

$$R_{ij} = \frac{1}{r_{ij}} \quad (64)$$

where R_{ij} represents the rejuvenation trigger score for the route between nodes N_i and N_j, r_{ij} denotes the rejuvenation indication for the route.

During route rejuvenation, MR-SRRP optimizes routing paths to improve performance and reliability. This optimization may involve recalculating routing metrics, rerouting traffic through alternative paths, or adjusting transmission parameters to mitigate degradation factors.

$$O_{ij} = \frac{1}{o_{ij}} \quad (65)$$

where O_{ij} represents the optimization score for the route between nodes N_i and N_j, o_{ij} denotes the optimization effort for route rejuvenation.

MR-SRRP dynamically adapts rejuvenation strategies based on real-time network conditions and performance feedback. Nodes continuously assess the effectiveness of rejuvenated routes and adjust as needed to ensure sustained improvements in routing performance.

$$A_{ij} = \frac{1}{a_{ij}} \quad (66)$$

where A_{ij} represents the adaptation score for the route between nodes N_i and N_j, a_{ij} denotes the adaptation feedback received from a neighboring node N_j

After rejuvenation, MR-SRRP verifies the integrity and reliability of the refreshed routing paths. Nodes exchange verification messages to confirm that data packets are successfully transmitted without errors or losses, ensuring that rejuvenated routes meet performance expectations.

Algorithm 1: MR-SRRP

Input:

- Cloud node set $N = \{n_1, n_2, n_3, \ldots, n_k\}$
- Node parameters: distance, signal strength, residual energy, congestion level, and trust score
- Network topology $T(N, E)$representing inter-node connectivity

Output:

- **MR-SRRP Optimized Route ($R_{MR-SRRP}$)** – a secure, adaptive, and energy-efficient communication path

Procedure:

1. **Node Initialization:** Identify active nodes and construct adjacency matrix $A(N, E)$.
2. **Exploration Phase:** Discover neighbors and evaluate link strength
3. **Adaptive Routing:** Compute route cost using weighted metrics of distance, energy, congestion, and trust.
4. **Tunnel Construction:** Form encrypted virtual tunnels between high-trust nodes for secure transmission.
5. **Failure Detection:** Continuously monitor paths and trigger regenerative restoration upon disruption.
6. **Redundant Routing:** Deploy backup tunnels to ensure uninterrupted data flow under node failure.
7. **Environmental Adaptation:** Adjust routes based on interference, temperature, or bandwidth variation.
8. **Energy Regulation:** Activate sleep scheduling, power tuning, and load balancing to conserve energy.
9. **Route Rejuvenation:** Refresh degraded routes, update trust scores, and reinforce tunnel stability.
10. **Return R_{MR-SR} :** Deliver the final secure, regenerative, and energy-aware path for sustained cloud communication.

4. SIMULATION SETTING

The simulation for evaluating MR-SRRP was executed in a controlled cloud environment configured to reflect dynamic virtual communication scenarios. With its unique generic application provisioning method, CloudSim [37], [38] is a crucial factor in addressing this problem. Each simulation entity was tuned to assess adaptive routing, security performance, and energy efficiency. The parameters used are summarized below.

Table 1. Simulation Setting

Simulation Attribute	Configuration Detail
Cloudlet Bandwidth Capacity	12.8 Gbps
Cloudlet Range	250–1200 units
Instruction Length per Cloudlet	1.2×10^3 MI
Processing Cores per Node	4
Data Center Instances	3
Hosts per Data Center	3
Initial Energy per Cloudlet	18 J
Average Packet Volume	512 KB
Memory Allocation per Cloudlet	8 GB
Storage Allocation per Cloudlet	40 GB
Total Simulation Duration	120 s
User Nodes	20
VM Bandwidth Capacity	2 GB
Active Virtual Machines	25
VM Platform	Linux Kernel (64-bit)
VM Memory	2 GB
VM Disk Space	10 GB

5. RESULTS AND DISCUSSIONS

5.1. Delay Analysis

The delay metric measures the average time required for a packet to reach the destination node from the source across the communication path. It determines how efficiently a routing protocol handles end-to-end transmission within varying traffic densities. Figure 1 and Table 2 present the delay variation for

FSCCS, CSM, and MR-SRRP across node densities ranging from 50 to 250. The x-axis indicates the number of nodes deployed in the network, while the y-axis represents the average delay expressed in milliseconds (ms). A smaller delay value demonstrates faster route convergence, reduced congestion, and improved data transfer efficiency under high-load environments.

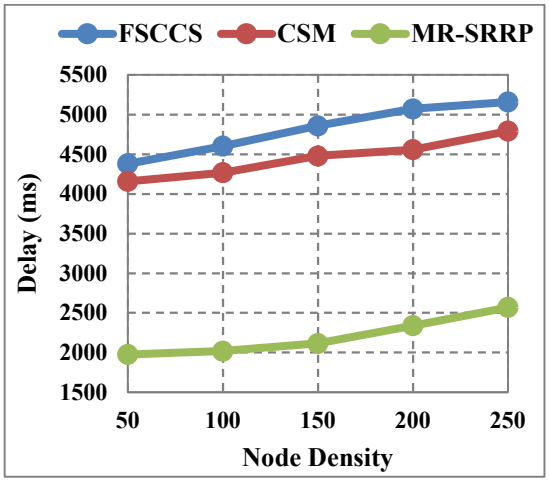

Figure 1. Delay

FSCCS exhibits the highest delay because its finite-state, chaotic compressed sensing framework requires intensive reconstruction of compressed data blocks at every transmission stage. The decompression and re-synchronization steps introduce queuing delay, particularly at higher node densities. CSM reduces the delay marginally, yet multiple verification stages and encryption layers extend the decision time for packet forwarding. MR-SRRP achieves the least delay through adaptive tunnelling, regenerative route repair, and dynamic burrowing behaviour inspired by Microchaetus ruppi. The protocol restores disrupted routes instantly, maintains optimal link strength, and minimizes retransmission overhead. This self-corrective design ensures low propagation time and consistent performance in dense, adaptive cloud networks.

Table 2. Delay Results

Node Density	FSCCS (ms)	CSM (ms)	MR-SRRP (ms)
50	4379	4156	1977
100	4600	4265	2016
150	4856	4478	2113
200	5071	4557	2338
250	5157	4793	2567
Average	**4812.6**	**4449.8**	**2202.2**

5.2. Packet Delivery Ratio Analysis

The Packet Delivery Ratio (PDR) metric quantifies the percentage of data packets that reach the intended destination out of the total packets transmitted. It directly indicates the reliability, stability, and consistency of the routing protocol under varying network loads. Figure 2 and Table 3 present the PDR results for FSCCS, CSM, and MR-SRRP, covering node densities ranging from 50 to 250. The x-axis indicates node density, while the y-axis represents packet delivery percentage (%). A higher PDR reflects improved network dependability, reduced packet loss, and stable path recovery across dynamic communication layers. FSCCS exhibits poor PDR because its compressed sensing mechanism suffers from synchronization loss and packet distortion during reconstruction, reducing successful data transmission under heavy load. CSM shows better but unstable delivery rates due to the delay introduced by repeated security validation and policy enforcement cycles, which disrupt transmission continuity.

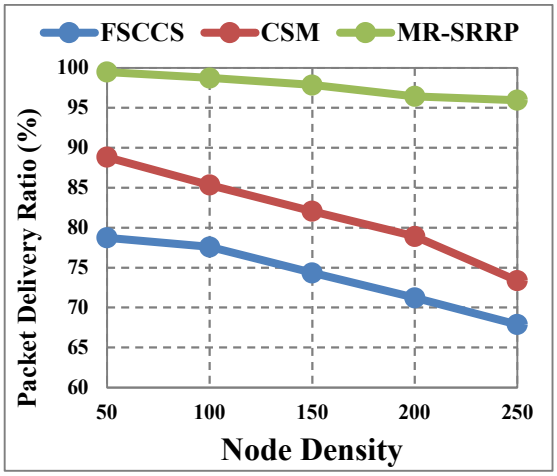

Figure 2. Packet Delivery Ratio

MR-SRRP achieves superior PDR through regenerative route rejuvenation, collaborative tunnelling, and adaptive restoration mechanisms inspired by Microchaetus rappi. The protocol instantly reconstructs damaged routes, prioritizes reliable paths, and maintains energy-balanced communication. Its self-healing and context-sensitive decision-making ensure uninterrupted packet forwarding across dense topologies, sustaining a near-perfect delivery rate that demonstrates robustness and security-driven adaptability.

Table 3. Packet Delivery Ratio Results

Node Density	FSCCS (%)	CSM (%)	MR-SRRP (%)
50	78.744	88.802	99.465
100	77.580	85.322	98.727
150	74.326	82.046	97.846
200	71.215	78.891	96.413
250	67.874	73.357	95.955
Average	**73.948**	**81.684**	**95.667**

5.3. Packet Loss Ratio Analysis

The Packet Loss Ratio (PLR) defines the proportion of packets that fail to reach the destination compared to the total transmitted. It serves as a direct indicator of transmission stability and routing resilience under diverse traffic conditions. Figure 3 and Table 4 present PLR values for FSCCS, CSM, and MR-SRRP across node densities ranging from 50 to 250. The x-axis represents node density, and the y-axis displays the packet loss ratio as a percentage (%). A lower PLR denotes effective route maintenance, minimal retransmission overhead, and improved packet integrity within the cloud network.

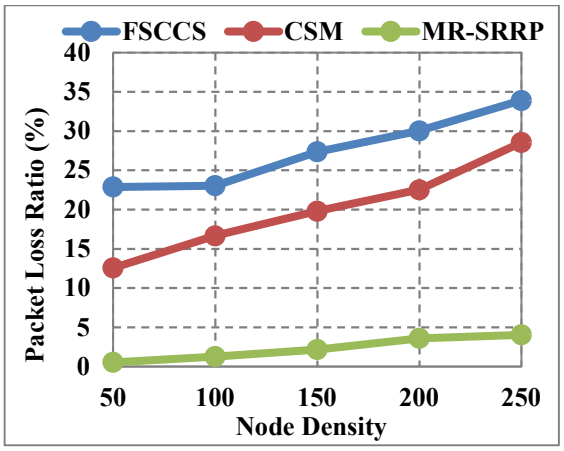

Figure 3. Packet Delivery Ratio

FSCCS records a high PLR because its compressed sensing and chaotic mapping produce decoding mismatches that increase packet drop probability, particularly under high node density. CSM reduces loss slightly through authentication and controlled routing; however, its layered verification delays routing responses, resulting in missed packet acknowledgements. MR-SRRP maintains an extremely low PLR through proactive detection of weak routes, instantaneous repair of broken paths, and redundant tunnelling. Its regenerative routing ensures continuous link reformation without dependency on retransmission. By balancing traffic and preserving node stability, MR-SRRP minimizes packet deterioration, confirming its superior capacity to sustain error-free transmission in dynamic cloud-based environments.

Table 4. Packet Delivery Ratio Results

Node Density	FSCCS (%)	CSM (%)	MR-SRRP (%)
50	22.869	12.577	0.535
100	23.025	16.647	1.273
150	27.355	19.788	2.154
200	30.014	22.513	3.587
250	33.898	28.537	4.045
Average	**27.432**	**20.012**	**2.319**

5.4. Throughput Analysis

The throughput metric determines the average volume of data successfully transmitted per unit time, expressed in kilobits per second (Kbps). It reflects the network's capacity to sustain continuous data flow under variable traffic and node density. Figure 4 and Table 5 show throughput variations for FSCCS, CSM, and MR-SRRP at densities from 50 to 250 nodes. The x-axis indicates node density, and the y-axis represents throughput, measured in kilobits per second (Kbps). Higher throughput demonstrates efficient channel utilization, stable routing decisions, and reduced congestion in packet delivery. FSCCS achieves low throughput because its data compression and chaotic reconstruction consume processing cycles that limit transmission rate and restrict bandwidth usage.

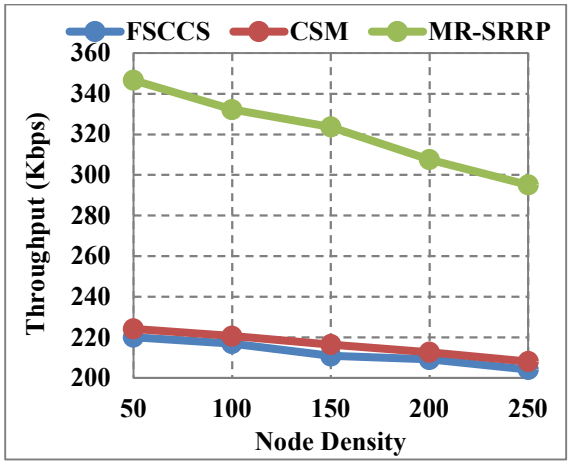

Figure 4. Throughput

CSM performs marginally better through controlled routing but loses efficiency due to the

constant validation of encryption and resource locking. MR-SRRP achieves the highest throughput by integrating adaptive tunnelling, dynamic regeneration, and cooperative load distribution among cloud nodes. Its self-organizing behaviour eliminates redundant retransmissions, balances energy expenditure, and stabilizes route convergence. The continuous path optimization within MR-SRRP ensures smooth packet scheduling, resulting in consistently higher data transfer rates and superior channel utilization across adaptive and energy-sensitive cloud infrastructures.

Table 5. Throughput Results

Node Density	FSCCS (Kbps)	CSM (Kbps)	MR-SRRP (Kbps)
50	220.142	224.221	346.698
100	216.863	220.557	332.154
150	210.790	216.391	323.573
200	209.084	212.613	307.479
250	204.177	208.125	295.147
Average	**212.211**	**216.381**	**321.010**

5.5. Energy Consumption Analysis

The energy consumption metric defines the proportion of total node energy utilized for packet transmission, reception, and routing control within the cloud environment. It serves as a key indicator of the sustainability and operational longevity of a routing protocol. Figure 5 and Table 6 present the comparative energy performance of FSCCS, CSM, and MR-SRRP across node densities from 50 to 250. The x-axis represents node density, and the y-axis shows energy usage in percentage (%). A smaller value denotes higher energy efficiency and better management of transmission power across dynamic communication paths.

FSCCS consumes excessive energy due to its chaotic compression and decompression cycles, which repeatedly activate processing units, leading to a power drain across the sensing nodes. The limited synchronization between encoding and reconstruction further increases retransmission effort, intensifying power demand. CSM performs slightly better, yet its continuous validation checkpoints and frequent encryption routines increase CPU cycles and radio usage. MR-SRRP maintains minimum energy consumption through intelligent route rejuvenation, energy-driven tunnelling, and adaptive sleep scheduling. Its regenerative routing reduces redundant transmissions and balances workload among active nodes. The biologically modelled behaviour, inspired by Microchaetus rappi, ensures that MR-SRRP sustains optimal energy distribution, prolongs node lifetime, and delivers consistent efficiency across complex cloud communication environments.

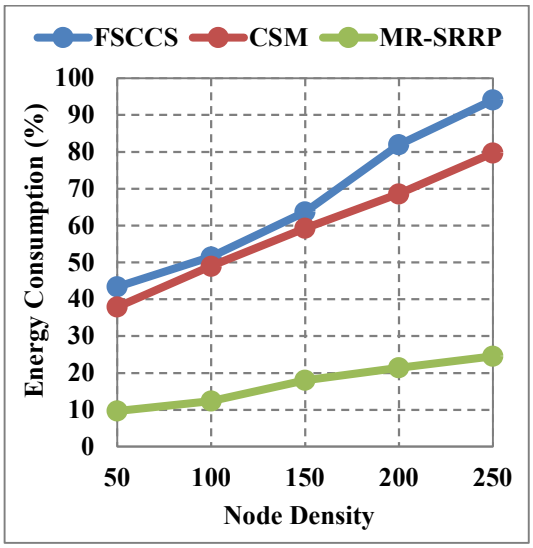

Figure 5. Energy Consumption

Table 6. Energy Consumption Results

Node Density	FSCCS (%)	CSM (%)	MR-SRRP (%)
50	43.396	37.889	9.623
100	51.447	48.929	12.327
150	63.680	59.228	17.968
200	81.887	68.565	21.364
250	94.060	79.665	24.479
Average	**66.894**	**58.855**	**17.152**

5.6. Avalanche Effect Analysis

The avalanche effect metric evaluates how effectively a protocol propagates diffusion in encrypted data whenever a single input bit changes. It reflects encryption strength, sensitivity, and resistance to cryptanalytic prediction. Figure 6 and Table 7 show the avalanche performance of FSCCS, CSM, and MR-SRRP. The x-axis lists the evaluated routing protocols, and the y-axis represents the avalanche effect measured in percentage (%). A higher value indicates stronger diffusion, meaning that minor alterations in input generate significant variations in output, ensuring better data confidentiality. FSCCS exhibits limited diffusion since its compressed sensing relies on deterministic transformations, producing predictable bit transitions under repetitive data patterns. CSM improves diffusion slightly by embedding security checks and open-source encryption policies, yet its

multi-layer validation weakens uniform randomness in ciphertext propagation. MR-SRRP, derived from regenerative encryption sequencing, displays a robust avalanche effect reaching 86.146%. Its multi-phase encryption integrates adaptive key scheduling, dual-segment cipher layering, and regenerative route-based security reinforcement. This architecture ensures that every bit alteration triggers widespread cipher transformation, achieving high entropy across cloud transmissions. The enhanced avalanche property confirms MR-SRRP's superior cryptographic resilience and reliability against unauthorized inference in adaptive communication networks.

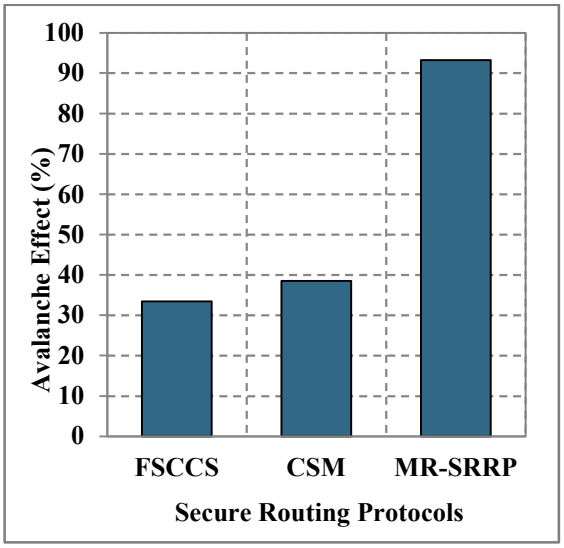

Figure 6. Avalanche Effect

Table 7. Avalanche Effect Results

Protocols	FSCCS (%)	CSM (%)	RGWOSR (%)
Avalanche Effect	33.471	38.472	86.146

The observed performance improvements across delay, packet delivery, packet loss, throughput, energy consumption, and encryption diffusion are directly attributable to the regenerative and adaptive mechanisms embedded within the MR-SRRP framework. Continuous route rejuvenation and distributed repair explain stable packet delivery and reduced transmission delay under increasing node density. Energy-aware tunneling and adaptive sleep regulation justify the sustained reduction in power consumption across cloud nodes. Strong avalanche diffusion behavior is supported by regenerative key scheduling and trust-based encrypted routing paths, ensuring robust confidentiality under dynamic conditions. These findings demonstrate practical relevance for real-world cloud infrastructures, including virtual data centers, multi-tenant platforms, and adaptive service networks where secure communication, rapid fault recovery, and energy sustainability remain critical operational requirements.

The collective performance trends across delay, packet delivery, packet loss, throughput, energy consumption, and avalanche diffusion highlight the systemic impact of regenerative routing intelligence within cloud environments. The results indicate that coupling biological regeneration with adaptive tunneling and distributed repair stabilizes routing behavior under increasing node density. Energy-aware path rejuvenation limits unnecessary retransmissions, while trust-driven encryption ensures confidentiality without imposing excessive overhead. These observations demonstrate that MR-SRRP functions as an integrated adaptive system rather than a metric-specific optimization, reinforcing its suitability for large-scale, security-sensitive cloud communication infrastructures.

6. CONCLUSION

Microchaetus Rappi-Inspired Secure and Regenerative Routing Protocol (MR-SRRP) establishes a biologically adaptive framework for secure, energy-efficient, and self-regenerative cloud communication. Inspired by the regenerative behavior of Microchaetus rappi, the protocol ensures autonomous route restoration, adaptive tunneling, and intelligent energy regulation across distributed virtual infrastructures. Its multi-phase operation maintains continuous connectivity, balanced load distribution, and reliable transmission under dynamic network conditions. Security is reinforced through trust-based authentication, encrypted tunneling, and regenerative key scheduling supported by high-diffusion avalanche encryption, achieving an 86.14% diffusion strength. The energy-aware logic minimizes redundant transmissions, extends node longevity, and sustains stable performance. For future enhancement, MR-SRRP can integrate quantum-resilient cryptography, AI-based predictive routing, blockchain-assisted trust validation, and fog-to-cloud coordination to advance transparency, scalability, and adaptability for next-generation autonomous cloud ecosystems.

REFERENCES:

[1] S. A. Aboulrous *et al.*, "Parallel Deployment and Performance Analysis of a Multi-Hop Routing Protocol for 5G Backhaul Networks

Using Cloud and HPC Platforms," *IEEE Access*, vol. 12, pp. 16696–16714, 2024, doi: 10.1109/ACCESS.2024.3355130.

[2] P. K. Dey and M. Yuksel, "Delegating Data Plane With Cloud-Assisted Routing," *IEEE Trans. Netw. Serv. Manag.*, vol. 20, no. 3, pp. 3190–3204, 2023, doi: 10.1109/TNSM.2023.3239802.

[3] A. Ndikumana, K. K. Nguyen, and M. Cheriet, "Federated Learning Assisted Deep Q-Learning for Joint Task Offloading and Fronthaul Segment Routing in Open RAN," *IEEE Trans. Netw. Serv. Manag.*, vol. 20, no. 3, pp. 3261–3273, 2023, doi: 10.1109/TNSM.2023.3245544.

[4] B. Tang, W. Xu, L. Zhang, B. Cao, Q. Yang, and K. Li, "Joint Optimization of Dynamic Service Selection and Request Routing in Cloud-Edge Collaborative Environments," *IEEE Internet Things J.*, vol. 12, no. 14, pp. 27222–27236, 2025, doi: 10.1109/JIOT.2025.3565469.

[5] M. S. Javed and R. A. Bakar, "A Secure and Green Cognitive Routing Protocol for Wireless Ad-Hoc Networks," *IEEE Access*, vol. 12, pp. 194989–195004, 2024, doi: 10.1109/ACCESS.2024.3519976.

[6] K. Wang *et al.*, "LFVeri: Network Configuration Verification for Virtual Private Cloud Networks," *IEEE/ACM Trans. Netw.*, vol. 32, no. 6, pp. 5475–5490, 2024, doi: 10.1109/TNET.2024.3469386.

[7] C.-C. Lin, Y.-C. Peng, Z.-Y. A. Chen, and P.-Y. Liu, "Crowdsourcing Home Healthcare Service: Matching Caretakers With Caregivers for Jointly Rostering and Routing," *IEEE Trans. Serv. Comput.*, vol. 18, no. 1, pp. 126–139, 2025, doi: 10.1109/TSC.2024.3517344.

[8] P. Wang, T. Ouyang, J. Gong, C. Hong, and X. Chen, "Adaptive Dynamic Scaling and Request Routing Optimization in the Multi-Edge Cluster Collaboration," *IEEE Trans. Mob. Comput.*, vol. 24, no. 10, pp. 9395–9412, 2025, doi: 10.1109/TMC.2025.3562209.

[9] N. Pacharla and K. S. Reddy, "Vehicle Authentication-Based Resilient Routing Algorithm With Dynamic Task Allocation for VANETs," *IEEE Access*, vol. 12, pp. 195344–195357, 2024, doi: 10.1109/ACCESS.2024.3520999.

[10] K. Wang, J. Wu, X. Zheng, J. Li, W. Yang, and A. V Vasilakos, "Cloud-Edge Orchestrated Power Dispatching for Smart Grid With Distributed Energy Resources," *IEEE Trans. Cloud Comput.*, vol. 11, no. 2, pp. 1194–1203, 2023, doi: 10.1109/TCC.2022.3185170.

[11] M. K. Somesula, S. K. Mothku, and S. C. Annadanam, "Cooperative Service Placement and Request Routing in Mobile Edge Networks for Latency-Sensitive Applications," *IEEE Syst. J.*, vol. 17, no. 3, pp. 4050–4061, 2023, doi: 10.1109/JSYST.2023.3260028.

[12] Y. Chang and X. Wang, "Robust Predictive Routing for Internet of Vehicles With Context-Aware Link Estimation and Multipath Verification," *IEEE Internet Things J.*, vol. 12, no. 20, pp. 43345–43358, 2025, doi: 10.1109/JIOT.2025.3596073.

[13] V. K. Quy, A. Chehri, N. M. Quy, V.-H. Nguyen, and N. T. Ban, "An Efficient Routing Algorithm for Self-Organizing Networks in 5G-Based Intelligent Transportation Systems," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1757–1765, 2024, doi: 10.1109/TCE.2023.3329390.

[14] Q. Gao, F. GU, L. Li, and J. Guo, "A framework of cloud-edge collaborated digital twin for flexible job shop scheduling with conflict-free routing," *Robot. Comput. Integr. Manuf.*, vol. 86, p. 102672, 2024, doi: https://doi.org/10.1016/j.rcim.2023.102672.

[15] S. Zhang, R. Xu, Z. Xu, C. Yu, Y. Jiang, and Y. Zhao, "Dynamic Routing of Multiple QoS-Required Flows in Cloud-Edge Autonomous Multi-Domain Data Center Networks," *Comput. Mater. Contin.*, vol. 78, no. 2, pp. 2287–2308, 2024, doi: https://doi.org/10.32604/cmc.2023.046550.

[16] C. Fan, X. Zhang, Y. Zhao, Y. He, and Y. Yang, "Dynamic relay node selection and routing for cloud-native Software Defined WANs," *Comput. Networks*, vol. 241, p. 110219, 2024, doi: https://doi.org/10.1016/j.comnet.2024.110219.

[17] Z. Liu, L. Wang, X. Wang, X. Shen, and L. Li, "Secure Remote Sensing Image Registration Based on Compressed Sensing in Cloud Setting," *IEEE Access*, vol. 7, pp. 36516–36526, 2019, doi: 10.1109/ACCESS.2019.2903826.

[18] R. Kumar and R. Goyal, "Modeling continuous security: A conceptual model for automated DevSecOps using open-source

software over cloud (ADOC)," *Comput. Secur.*, vol. 97, p. 101967, 2020, doi: 10.1016/j.cose.2020.101967.

[19] R. Jaganathan, S. Mehta, and R. Krishan, "Preface," *Bio-Inspired Intell. Smart Decis.*, pp. xix–xx, 2024, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85195725049&partnerID=40&md5=7a2aa7adc005662eebc12ef82e3bd19f

[20] R. Jaganathan, S. Mehta, and R. Krishan, "Preface," *Intell. Decis. Mak. Through Bio-Inspired Optim.*, pp. xiii–xvi, 2024, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85192858710&partnerID=40&md5=f8f1079e8772bd424d2cdd979e5f2710

[21] B. Suchitra, R. Karthikeyan, J. Ramkumar, and V. Valarmathi, "Enhancing Recurrent Neural Network Performance for Latent Autoimmune Diabetes Detection (Lada) Using Exocoetidae Optimization," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 5, pp. 1645–1667, 2025, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-105000948603&partnerID=40&md5=66c8f111b153fed68b3d0ea9c88c411e

[22] R. Jaganathan, K. Rajendran, and P. S. Ponnukumar, "Peregrine Falcon Optimization Routing Protocol (PFORP) for Achieving Ultra-Low Latency and Boosted Efficiency in 6G Drone Ad-Hoc Networks (DANET)," *Int. J. Comput. Digit. Syst.*, vol. 17, no. 1, pp. 1–18, 2025, doi: 10.12785/ijcds/1571111848.

[23] J. Ramkumar, V. Valarmathi, and R. Karthikeyan, "Optimizing Quality of Service and Energy Efficiency in Hazardous Drone Ad-Hoc Networks (DANET) Using Kingfisher Routing Protocol (KRP)," *Int. J. Eng. Trends Technol.*, vol. 73, no. 1, pp. 410–430, 2025, doi: 10.14445/22315381/IJETT-V73I1P135.

[24] J. Ramkumar, B. Varun, V. Valarmathi, D. R. Medhunhashini, and R. Karthikeyan, "Jaguar-Based Routing Protocol (JRP) For Improved Reliability and Reduced Packet Loss in Drone Ad-Hoc Networks (DANET)," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 2, pp. 696–713, 2025, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85217213044&partnerID=40&md5=e38a375e46cf43c95d6702a3585a7073

[25] B. Suchitra, J. Ramkumar, and R. Karthikeyan, "Frog Leap Inspired Optimization-Based Extreme Learning Machine for Accurate Classification of Latent Autoimmune Diabetes in Adults (LADA)," *J. Theor. Appl. Inf. Technol.*, vol. 103, no. 2, pp. 472–494, 2025, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85217140979&partnerID=40&md5=9540433c16d5ff0f6c2de4b8c43a4812

[26] J. Ramkumar and R. Vadivel, "CSIP—cuckoo search inspired protocol for routing in cognitive radio ad hoc networks," in *Advances in Intelligent Systems and Computing*, Springer Verlag, 2017, pp. 145–153. doi: 10.1007/978-981-10-3874-7_14.

[27] R. Jaganathan and R. Vadivel, "Intelligent Fish Swarm Inspired Protocol (IFSIP) for Dynamic Ideal Routing in Cognitive Radio Ad-Hoc Networks," *Int. J. Comput. Digit. Syst.*, vol. 10, no. 1, pp. 1063–1074, 2021, doi: 10.12785/ijcds/100196.

[28] J. Ramkumar, A. Senthilkumar, M. Lingaraj, R. Karthikeyan, and L. Santhi, "Optimal Approach for Minimizing Delays in IoT-Based Quantum Wireless Sensor Networks Using NM-Leach Routing Protocol," *J. Theor. Appl. Inf. Technol.*, vol. 102, no. 3, pp. 1099–1111, 2024, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85185481011&partnerID=40&md5=bf0ff974ceabc0ad58e589b28797c684

[29] J. Ramkumar and R. Vadivel, "Improved frog leap inspired protocol (IFLIP) – for routing in cognitive radio ad hoc networks (CRAHN)," *World J. Eng.*, vol. 15, no. 2, pp. 306–311, 2018, doi: 10.1108/WJE-08-2017-0260.

[30] J. Ramkumar, S. S. Dinakaran, M. Lingaraj, S. Boopalan, and B. Narasimhan, "IoT-Based Kalman Filtering and Particle Swarm Optimization for Detecting Skin Lesion," in *Lecture Notes in Electrical Engineering*, K. Murari, S. Kamalasadan, and N. P. Padhy, Eds., Springer Science and Business Media Deutschland GmbH, 2023, pp. 17–27. doi: 10.1007/978-981-19-8353-5_2.

[31] R. Jaganathan, S. Mehta, and R. Krishan, *Intelligent Decision Making Through Bio-Inspired Optimization*. IGI Global, 2024.

doi: 10.4018/979-8-3693-2073-0.

[32] R. Jaganathan and V. Ramasamy, "Performance modeling of bio-inspired routing protocols in Cognitive Radio Ad Hoc Network to reduce end-to-end delay," *Int. J. Intell. Eng. Syst.*, vol. 12, no. 1, pp. 221–231, 2019, doi: 10.22266/IJIES2019.0228.22.

[33] M. P. Swapna, J. Ramkumar, and R. Karthikeyan, "Energy-Aware Reliable Routing with Blockchain Security for Heterogeneous Wireless Sensor Networks," in *Lecture Notes in Networks and Systems*, V. Goar, M. Kuri, R. Kumar, and T. Senjyu, Eds., Springer Science and Business Media Deutschland GmbH, 2025, pp. 713–723. doi: 10.1007/978-981-97-6106-7_43.

[34] P. Menakadevi and J. Ramkumar, "Robust Optimization Based Extreme Learning Machine for Sentiment Analysis in Big Data," in *2022 International Conference on Advanced Computing Technologies and Applications, ICACTA 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICACTA54488.2022.9753203.

[35] J. Ramkumar, R. Vadivel, and B. Narasimhan, "Constrained Cuckoo Search Optimization Based Protocol for Routing in Cloud Network," *Int. J. Comput. Networks Appl.*, vol. 8, no. 6, pp. 795–803, 2021, doi: 10.22247/ijcna/2021/210727.

[36] D. Jayaraj, J. Ramkumar, M. Lingaraj, and B. Sureshkumar, "AFSORP: Adaptive Fish Swarm Optimization-Based Routing Protocol for Mobility Enabled Wireless Sensor Network," *Int. J. Comput. Networks Appl.*, vol. 10, no. 1, pp. 119–129, 2023, doi: 10.22247/ijcna/2023/218516.

[37] J. Ramkumar and R. Vadivel, "Improved Wolf prey inspired protocol for routing in cognitive radio Ad Hoc networks," *Int. J. Comput. Networks Appl.*, vol. 7, no. 5, pp. 126–136, 2020, doi: 10.22247/ijcna/2020/202977.

[38] S. P. Geetha, N. M. S. Sundari, J. Ramkumar, and R. Karthikeyan, "Energy Efficient Routing In Quantum Flying Ad Hoc Network (Q-FANET) Using Mamdani Fuzzy Inference Enhanced Dijkstra's Algorithm (MFI-EDA)," *J. Theor. Appl. Inf. Technol.*, vol. 102, no. 9, pp. 3708–3724, 2024, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85197297302&partnerID=40&md5=72d51668bee6239f09a59d2694df67d6

[39] R. Vadivel and J. Ramkumar, "QoS-enabled improved cuckoo search-inspired protocol (ICSIP) for IoT-based healthcare applications," in *Incorporating the Internet of Things in Healthcare Applications and Wearable Devices*, IGI Global, 2019, pp. 109–121. doi: 10.4018/978-1-7998-1090-2.ch006.

[40] J. Ramkumar, R. Karthikeyan, and V. Valarmathi, "Alpine Swift Routing Protocol (ASRP) for Strategic Adaptive Connectivity Enhancement and Boosted Quality of Service in Drone Ad Hoc Network (DANET)," *Int. J. Comput. Networks Appl.*, vol. 11, no. 5, pp. 726–748, 2024, doi: 10.22247/ijcna/2024/45.

[41] J. Ramkumar, R. Karthikeyan, and M. Lingaraj, "Optimizing IoT-Based Quantum Wireless Sensor Networks Using NM-TEEN Fusion of Energy Efficiency and Systematic Governance," in *Lecture Notes in Electrical Engineering*, V. Shrivastava, J. C. Bansal, and B. K. Panigrahi, Eds., Springer Science and Business Media Deutschland GmbH, 2025, pp. 141–153. doi: 10.1007/978-981-97-6710-6_12.

[42] J. Ramkumar and R. Vadivel, "Multi-Adaptive Routing Protocol for Internet of Things based Ad-hoc Networks," *Wirel. Pers. Commun.*, vol. 120, no. 2, pp. 887–909, Apr. 2021, doi: 10.1007/s11277-021-08495-z.

[43] R. Jaganathan, S. Mehta, and R. Krishan, *Bio-Inspired intelligence for smart decision-making*, vol. i. 2024. doi: 10.4018/9798369352762.

[44] J. Ramkumar, K. S. Jeen Marseline, and D. R. Medhunhashini, "Relentless Firefly Optimization-Based Routing Protocol (RFORP) for Securing Fintech Data in IoT-Based Ad-Hoc Networks," *Int. J. Comput. Networks Appl.*, vol. 10, no. 4, pp. 668–687, 2023, doi: 10.22247/ijcna/2023/223319.

[45] M. Lingaraj, T. N. Sugumar, C. S. Felix, and J. Ramkumar, "Query aware routing protocol for mobility enabled wireless sensor network," *Int. J. Comput. Networks Appl.*, vol. 8, no. 3, pp. 258–267, 2021, doi: 10.22247/ijcna/2021/209192.

[46] J. Ramkumar, C. Kumuthini, B. Narasimhan, and S. Boopalan, "Energy Consumption Minimization in Cognitive Radio Mobile Ad-Hoc Networks using

Enriched Ad-hoc On-demand Distance Vector Protocol," *2022 Int. Conf. Adv. Comput. Technol. Appl. ICACTA 2022*, pp. 1–6, Mar. 2022, doi: 10.1109/ICACTA54488.2022.9752899.

[47] A. Senthilkumar, J. Ramkumar, M. Lingaraj, D. Jayaraj, and B. Sureshkumar, "Minimizing Energy Consumption in Vehicular Sensor Networks Using Relentless Particle Swarm Optimization Routing," *Int. J. Comput. Networks Appl.*, vol. 10, no. 2, pp. 217–230, 2023, doi: 10.22247/ijcna/2023/220737.

[48] L. Mani, S. Arumugam, and R. Jaganathan, "Performance Enhancement of Wireless Sensor Network Using Feisty Particle Swarm Optimization Protocol," *ACM Int. Conf. Proceeding Ser.*, pp. 1–5, Dec. 2022, doi: 10.1145/3590837.3590907.

[49] J. Ramkumar and R. Vadivel, "Whale optimization routing protocol for minimizing energy consumption in cognitive radio wireless sensor network," *Int. J. Comput. Networks Appl.*, vol. 8, no. 4, pp. 455–464, 2021, doi: 10.22247/ijcna/2021/209711.