Journal of Theoretical and Applied Information Technology
31st January 2025. Vol.103. No.2

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

JAGUAR-BASED ROUTING PROTOCOL (JRP) FOR IMPROVED RELIABILITY AND REDUCED PACKET LOSS IN DRONE AD-HOC NETWORKS (DANET)

Dr J RAMKUMAR[1], VARUN B[2], V. VALARMATHI[3], D R MEDHUNHASHINI[4], R. KARTHIKEYAN[5]

[1]Department of Computer Science, Apex Professional University, Arunachal Pradesh, India
[2]Department of Mechanical Engineering, Sri Ramakrishna Institute of Technology, Tamil Nadu, India
[3]Department of IT & Cognitive Systems, Sri Krishna Arts and Science College, Tamil Nadu, India
[4]Department of IT & Cognitive Systems, Sri Krishna Arts and Science College, Tamil Nadu, India
[5]Department of Computer Technology, Sri Krishna Adithya College of Arts and Science, Tamil Nadu, India

E-Mail : [1]drjramkumarphd@gmail.com, [2]bvarun.me@gmail.com, [3]valarmathiv@skasc.ac.in, [4]medhunhashinidr@skasc.ac.in

ABSTRACT

Drone Ad hoc Networks (DANETs) represent an innovative paradigm in wireless communications, utilizing the inherent mobility of drones to create dynamic, self-organizing networks without relying on pre-established infrastructure. Routing within these networks poses significant challenges due to the high mobility of drones, which often disrupts communication links, leading to considerable packet loss and impacting network reliability and performance. To effectively address these challenges, this paper proposes the Jaguar-based Routing Protocol (JRP). Inspired by the stealth and strategic agility of jaguars, JRP is engineered to enhance routing dynamics through several meticulously designed phases. It begins with a scanning phase, where drones assess the network topology and identify optimal communication paths. This is followed by a target selection phase, where the most stable and efficient routes are chosen based on real-time network conditions. The protocol also incorporates a secure data exchange mechanism to safeguard communications against potential security threats. The performance of JRP is rigorously tested through simulations that demonstrate its ability to significantly reduce packet loss and improve energy efficiency. These attributes make JRP a superior choice compared to existing state-of-the-art routing protocols, particularly in environments demanding high network resilience and operational efficiency.

Keywords: *Drone Ad Hoc Networks, Jaguar-Based Routing Protocol, Dynamic Routing, Packet Loss Mitigation, Network Reliability*

1. INTRODUCTION

Drone Ad hoc Networks (DANET) embody a transformative approach to wireless communication, leveraging the autonomous nature of drones to form dynamic, self-organizing networks. These networks eliminate the need for pre-existing infrastructure, enabling drones to communicate directly with one another, which is particularly advantageous in environments where conventional communication systems are infeasible [1]. DANETs offer unparalleled flexibility, allowing drones to adapt to changing conditions in real-time. This capability is essential for applications in search and rescue, environmental monitoring, and military operations, where rapid response and adaptability are crucial. Drones' inherent mobility and flexibility in DANETs open up new possibilities for efficient and resilient communication systems [2]. Routing protocols in DANET are specifically designed to manage the challenges associated with drone mobility. Traditional static networks often fall short, necessitating continuous adjustments in drone positions, leading to frequent route discoveries and modifications [3]. These protocols maintain efficient data transmission by dynamically establishing, maintaining, and terminating routes as drones move. Effective routing in DANET involves finding the optimal path for data packets, considering factors such as distance, signal strength, and energy efficiency. Balancing the need for current routing information with the overhead required to maintain it ensures that the network can scale and adapt without excessive resource consumption [4]. Protocols must also address security concerns, preserving data integrity and confidentiality despite

the open and decentralized nature of the network. Continuous development and refinement of these routing protocols are critical for successful deployment and operation in various real-world applications [5].

In disaster response operations, packet loss in DANETs emerges as a significant challenge. The constant movement of drones creates frequent disconnections, leading to high rates of data packet loss. This instability severely undermines network reliability and data integrity [6]. In critical scenarios requiring precise location data of survivors or structural damage assessments, packet loss can result in incomplete or delayed information, potentially causing critical delays. High mobility of drones and challenging environmental conditions, such as strong winds or obstacles in disaster areas, further exacerbate communication instability, increasing packet loss rates [7]. This issue can impede the effectiveness of disaster response operations by causing delays in transmitting crucial information. Ensuring that data packets reach their intended destinations without loss is essential for maintaining the reliability and integrity of the network [8].

Maintaining reliable data transmission despite high mobility and unstable conditions remains a significant concern. Addressing packet loss in DANETs is crucial for enhancing the reliability and effectiveness of disaster response efforts, ensuring that vital information is transmitted accurately and timely [9].

1.1. PROBLEM STATEMENT

A significant issue in DANETs is the high packet loss rate resulting from unstable communication links. The frequent disconnections caused by drone mobility lead to data packets being lost during transmission, severely impacting the reliability and integrity of the network. In critical applications such as military operations and emergency response, packet loss can result in incomplete or delayed information, adversely affecting decision-making processes. The challenge is further intensified by environmental factors like wind, which can cause drones to deviate from their intended paths, disrupting established communication links and increasing packet loss rates. Addressing this issue requires robust routing protocols capable of maintaining consistent and reliable data transmission despite the frequent changes in network topology.

1.2. MOTIVATION

The issue of unstable communication links in DANET is a primary cause of packet loss, significantly degrading network performance and reliability. Various factors contribute to link instability, including physical obstacles, interference from external sources, the inherent mobility of drones, and the varying distances between nodes. These factors can lead to frequent link breakages and fluctuating link quality, resulting in high packet loss rates. Such losses can compromise the integrity and timeliness of data transmission, which is critical for applications that rely on real-time data. To mitigate these challenges, developing robust routing protocols that effectively manage link instability is imperative. These protocols should incorporate mechanisms for continuous link quality assessment, rapid detection of link failures, and dynamic rerouting strategies. By enhancing the network's resilience to unstable links, these protocols can maintain high packet delivery ratios, ensuring consistent and reliable communication. Addressing packet loss due to unstable communication links is essential for improving the overall performance and dependability of DANETs, facilitating their use in various high-stakes applications.

1.3. OBJECTIVE

This paper aims to develop a bio-inspired optimization routing protocol to mitigate packet loss from unstable communication links in DANETs. Unstable links, caused by physical obstructions, signal interference, drone mobility, and varying distances between nodes, lead to significant packet loss and degraded network reliability. The proposed protocol will utilize principles from biological systems to assess and adapt to link quality in real-time continuously. The protocol aims to reduce packet loss and enhance overall communication reliability by dynamically rerouting data through more stable communication paths. Rigorous simulations and practical implementations will be conducted to validate the protocol's robustness in managing link instability and maintaining high packet delivery ratios under diverse conditions.

2. LITERATURE REVIEW

"Drone-Assisted V2X Routing" [10] enhances vehicle-to-everything (V2X) communication by using drones as mobile relay nodes. Drones dynamically position themselves to bridge communication gaps, ensuring robust connectivity. Advanced routing algorithms help

optimize their positions based on real-time data. This setup supports uninterrupted data exchange, which is crucial for autonomous driving and traffic management. Integrating drones into the V2X network improves the reliability and efficiency of vehicular communication systems. "Stocktaking Data Routing Optimization" [11] focuses on efficient data transmission from drones during warehouse stocktaking to central processing units. Drones collect inventory data and transmit it using optimized routing algorithms. These algorithms consider network topology, data packet sizes, and potential interference to ensure reliability. Multi-hop communication enhances coverage and reliability, accounting for drone battery levels and node availability. This approach ensures timely and accurate inventory management. "Swarm Sync Data Routing" [12] addresses synchronizing data transmission among drone swarms for efficient routing to a central destination. Drones collect data collaboratively, using synchronization protocols to manage transmission timing. Advanced algorithms optimize data routes based on network topology and link quality. Multi-hop communication and adaptive control mechanisms prevent congestion and optimize network throughput. This method ensures reliable and timely data delivery for complex missions.

"Weighted Cluster S-UAV" [13] leverages latency-oriented trust for efficient drone communication. Drones form clusters managed by a leader chosen based on a trust metric considering latency and reliability. Real-time data exchanges continuously assess trust levels, ensuring low-latency communication paths. Cluster leaders optimize data routing within and between clusters, enhancing network performance. This approach is crucial for time-sensitive applications. "Coordinated UAV-Rider Dispatching" [14] optimizes the collaboration between UAVs and human riders in delivery services. UAVs handle aerial routes, while riders manage ground deliveries. A coordination algorithm dynamically allocates tasks based on real-time data such as location and delivery urgency. Advanced routing algorithms optimize paths for both UAVs and riders, ensuring seamless transitions. Real-time communication maintains dynamic route adjustments, enhancing delivery efficiency. "Smart Clustering Routing" [15] utilizes Q-learning to enhance data transmission efficiency in UAV networks. Drones are organized into clusters, each with a selected cluster head for data relay. Q-learning optimizes cluster head selection and routing paths based on network performance metrics. The algorithm continuously adapts to changes in mobility and communication conditions. This intelligent approach extends the network's operational lifetime and improves data transmission reliability.

"Enhanced GPSR" [16] is an updated GPSR protocol optimized for dynamic environments. Greedy forwarding is used until a local minimum is reached, then perimeter routing is applied. The protocol adjusts routes based on real-time link quality and node stability. This minimizes packet loss and adapts to frequent topology changes. Enhanced GPSR ensures reliable and efficient data transmission in FANETs. "UAV Inspection Routing and Scheduling" [17] involves strategic planning of drone paths for efficient inspections. Data on inspection sites is gathered, and optimal routes are planned considering no-fly zones and battery life. Scheduling assigns specific time slots for UAVs, avoiding overlap. Real-time adjustments to routes and schedules are made based on UAV status and environmental conditions. This systematic approach minimizes downtime and operational costs. "Multi-Depot UAV Routing" [18] coordinates multiple UAVs from various depots for emergency tasks, minimizing total completion time. Tasks are allocated based on urgency, with UAVs stationed at strategic depots. Optimization algorithms determine efficient paths considering UAV range and battery life. Real-time adjustments are made based on evolving conditions, ensuring timely aid delivery. This approach enhances disaster response effectiveness.

"Distance and Connectivity-Based Traffic Density Routing" [19] ensures efficient data transmission by assessing vehicle distance and connectivity. The protocol dynamically selects stable routes based on real-time traffic density. Vehicles broadcast their status, allowing the protocol to evaluate potential routes. High connectivity and stable links are prioritized, reducing disconnections. Real-time adjustments maintain efficient data flow in dynamic environments, enhancing VANET performance. "HVNS-TDR" [20] tackles sustainable truck-drone routing using a hybrid variable neighborhood search heuristic. Trucks and drones are assigned routes with rendezvous points for drone dispatch. The method iteratively explores different route sequences to optimize for sustainability. It considers time-dependent factors like traffic and drone battery life. This process ensures efficient routing for truck-drone delivery systems. "MDVRP-Drones" [21] coordinates ground vehicles and drones for efficient deliveries. Vehicles with drones depart from multiple depots, with drones servicing

remote areas. A mixed-integer linear programming model defines constraints and objectives. A hybrid heuristic algorithm iteratively improves routes by balancing tasks between vehicles and drones. This approach addresses complex logistics challenges, enhancing delivery efficiency.

"Ad-hoc On-Demand Distance Vector (AODV)" [22] operates by discovering routes on-demand through the broadcast of RREQ packets. Intermediate nodes or the destination respond with RREP packets to establish the path. This mechanism avoids needing unnecessary routes and reduces overhead under stable conditions. The protocol's broadcast-based route discovery consumes significant bandwidth, as frequent control messages are broadcasted throughout the network. Battery drain occurs because drones expend energy processing these control messages. High control message traffic increases the risk of packet collisions, particularly in dense networks. The protocol does not consider link quality in routing decisions, leading to unreliable data transmission. Additionally, the lack of multicast support limits AODV's efficiency in group communication scenarios, as it cannot simultaneously send messages to multiple nodes. "Q-learning-based Secure and reliable Clustering Routing (QSCR)" [23] utilizes Q-learning to form clusters and make routing decisions, dynamically adjusting nodes' roles and parameters to enhance network reliability and security. Performance depends heavily on the initial setup of learning parameters, which can lead to scalability issues when managing many drones. The Q-learning algorithm may converge to local optima, resulting in suboptimal routing solutions. High mobility causes frequent changes in cluster formations, requiring constant recalculations. Dynamic changes in drone states lead to inconsistent cluster head elections, disrupting network operations and stability.

Several optimization algorithms are being utilized in different research for achieving better performance [24]-[52].

2.1. TECHNOLOGICAL GAPS

Current solutions like Drone-Assisted V2X Routing and Stocktaking Data Routing Optimization show promise, yet gaps persist in real-time data analysis and processing. These methods often face delays and increased packet loss. Techniques such as Swarm Sync Data Routing require precise synchronization, a challenging feat in dynamic environments, potentially leading to data collisions. Real-time trust assessment and cluster formation in protocols like Weighted Cluster S-UAV need improvements to minimize latency and enhance reliability. More effective methods are required to handle interference and maintain stable communication links amid environmental obstacles and high mobility. Optimization of existing algorithms is essential to ensure low-latency communication while managing high computational demands of continuous learning and adaptation.

3. JAGUAR-BASED ROUTING PROTOCOL

The Jaguar-based Routing Protocol (JRP) enhances drone ad hoc networks by minimizing packet loss through adaptive routing, energy efficiency, and robust security. Inspired by jaguars' stealth, precision, and efficiency, JRP integrates multiple phases, from scanning and target selection to stealth operations and secure data exchange. The protocol leverages the jaguar's characteristics of strategic planning, agility, and covert movement to ensure stable and efficient communication in dynamic environments. The following sections describe each mechanism involved in JRP in detail.

3.1. SCANNING PHASE

The Scanning Phase in JRP plays a crucial role in establishing efficient communication paths within a drone ad-hoc network, drawing inspiration from the meticulous scanning behaviour of jaguars in their hunting process. This phase involves systematically exploring the network environment by individual drones to detect nearby nodes and assess network topology, ultimately facilitating the selection of optimal communication targets. Mathematically, the Scanning Phase can be represented through various sub-processes and equations, each contributing to the overall effectiveness of the protocol. In the Scanning Phase, drones determine their sensing range. R_s Based on their sensory capabilities and environmental conditions. This range dictates the maximum distance within which a drone can detect neighbouring nodes, influencing the density of the network and the efficiency of communication links. Mathematically, sensing range R_s can be expressed as Eq.(1).

$$R_s = f(Sensors, Environment) \quad (1)$$

Sensors represent the drone's sensory parameters, and the environment encapsulates terrain, weather, and interference.

The probability of discovering a neighboring node within the sensing range R_s is a

critical metric in the Scanning Phase. It determines the likelihood of establishing communication links and influences the overall connectivity of the network. Mathematically, node discovery probability P_d can be defined as Eq.(2).

$$P_d = \frac{N_n}{N_t} \quad (2)$$

where N_n represents the number of neighbouring nodes within the sensing range R_s, and N_t denotes the total number of nodes in the network.

During the Scanning Phase, drones estimate the signal strength S of neighbouring nodes to assess the quality of potential communication links. This estimation is crucial for selecting reliable communication partners and optimizing data transmission efficiency. Mathematically, signal strength S can be calculated using the Friis transmission equation:

$$S = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 \quad (3)$$

P_t represents the transmitted power, G_t and G_r denote the antenna gains of the transmitter and receiver, λ denotes the signal's wavelength, and d denotes the distance between the two.

In the Scanning Phase, drones analyze their energy consumption to ensure sustainable operation throughout the network exploration. This analysis estimates the energy expended in sensing, processing, and communication tasks, considering factors such as battery capacity and power efficiency. Mathematically, energy consumption E can be modeled as Eq.(4).

$$E = \sum_{i=1}^{N_s} \left(E_s + E_p + E_c\right) \quad (4)$$

where N_s is the total number of scanned nodes, E_s is the energy consumed for sensing, E_p is the energy expended for processing and E_c is the energy consumed for communication.

Determining the density of neighbouring nodes within the sensing range R_s is essential for evaluating network connectivity and optimizing routing decisions. Mathematically, network density D can be calculated using Eq.(5).

$$D = \frac{N_n}{\pi R_s^2} \quad (5)$$

Based on the information gathered during the Scanning Phase, drones employ a neighbour selection strategy to prioritize communication links with optimal partners. This strategy aims to maximize signal strength, minimize energy consumption, and ensure robust network connectivity. Mathematically, neighbour selection involves a combination of criteria such as signal-to-noise ratio, distance, and available bandwidth, and it is represented as Eq.(6).

$$Neighbor_i = argmax_j\left(S_j - \alpha E_j\right) \quad (6)$$

where $Neighbor_i$ is the selected neighbour node, S_j is the signal strength of node j, E_j is the energy consumption of node j, and α is a weighting factor balancing signal strength and energy efficiency.

3.2. TARGET SELECTION

Target selection in JRP is a pivotal phase where drones within a drone ad-hoc network strategically choose optimal communication targets based on various parameters and criteria. Drawing inspiration from the precision and discernment of jaguars in selecting their prey, the target selection process in JRP involves mathematical formulations and decision-making algorithms to ensure efficient and reliable communication links. One of the primary considerations in target selection is the distance between drones, which directly impacts signal strength, latency, and energy consumption. Drones calculate the distance metric. D_{ij} between potential communication partners i and j using geometric formulas such as the Euclidean distance.

$$D_{ij} = \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \quad (7)$$

where (x_i, y_i) and (x_j, y_j) represent the coordinates of drones i and j, respectively.

Another critical factor in target selection is estimating signal strength between drones. This estimation is crucial for determining the reliability and quality of communication links. Signal strength S_{ij} between drones i and j can be calculated using propagation models such as the Friis transmission equation expressed in Eq.(8).

$$S_{ij} = P_t G_t G_r \left(\frac{\lambda}{4\pi D_{ij}}\right)^2 \quad (8)$$

In this context, P_t denotes the transmitted power, G_t and G_r denote the transmitter's and receiver's antenna gains, λ denotes the signal's wavelength, and D_{ij} denotes the distance between drones i and j.

Target selection also involves analyzing the energy consumption of establishing and maintaining

communication links. Drones evaluate energy expenditure. E_{ij} required for data transmission between nodes i and j, considering factors such as signal strength and data packet size. Energy consumption can be modeled as Eq.(9).

$$E_{ij} = \frac{S_{ij}.T_{ij}}{R} \quad (9)$$

where T_{ij} is the time required for data transmission between drones i and j, and R is the data transmission rate.

In addition to distance, signal strength, and energy consumption, drones consider various Quality of Service (QoS) metrics during target selection to meet application-specific requirements. Eq.(10) and Eq.(11) include Throughput, delay, jitter, and packet loss, which are crucial for ensuring reliable and efficient communication. QoS metrics are typically a multi-objective optimization problem, aiming to maximize utility while satisfying constraints.

$$max_{Targets} \sum_{k=1}^{K} U_k \quad (10)$$

$$subject\ to\ C_k \leq T_k \leq \bar{C}_k \quad (11)$$

where U_k represents the utility of QoS metric k, C_k and $\bar{C}_k$ denote the lower and upper bounds of QoS metric k, and T_k represents the actual value of QoS metric k.

JRP incorporates dynamic neighbour selection strategies to adapt to changing network conditions and optimize communication links in real-time. Drones continuously monitor the performance of neighbouring nodes and adjust their target selection based on evolving criteria such as signal strength fluctuations, node mobility, and network congestion. Eq.(12) plays a major role in selecting the dynamic neighbour.

$$Neighbor_i = argmax_j(S_{ij} - \alpha E_{ij}) \quad (12)$$

where $Neighbor_i$ represents the selected neighbour node for drone i, S_{ij} is the estimated signal strength between drones i and j, E_{ij} is the energy consumption for data transmission between drones i and j, and α is a weighting factor balancing signal strength and energy efficiency.

To enhance target selection performance and adaptability, JRP may leverage reinforcement learning techniques to enable drones to learn and optimize their decision-making processes over time. Drones may use data from their surroundings and experiences to make educated target selection judgments with the help of Eq.(13).

$$Q(s,a) = Q(s,a) + \alpha[R(s,a) + \gamma max_{\alpha'} Q(s',a') - Q(s,a)] \quad (13)$$

where $Q(s,a)$ denotes the anticipated total benefit from action a in-state s, α stands for the learning rate, $R(s,a)$ denotes the immediate benefit from the action of an in-state s, γ is the discount factor, and s' represents the subsequent state after action a.

3.3. STEALTHY APPROACH

The stealth and precision jaguars inspire the Stealthy Approach phase in JRP exhibited in their hunting behaviour. This phase involves drones maneuvering the network environment with discretion and agility to minimize detection and optimize communication efficiency. Mathematically, the Stealthy Approach phase incorporates various strategies and algorithms to ensure covert navigation and effective data transmission. Path planning is a fundamental aspect of the Stealthy Approach phase, where drones calculate optimal routes to their destination while avoiding obstacles and minimizing exposure. Mathematically, path planning involves finding the shortest path. P_{ij} between nodes i and j in the network graph, considering factors such as distance, terrain, and potential interference. This can be formulated as a graph traversal problem, as explored in Eq.(14).

$$P_{ij} = argmin_P \sum_{k=1}^{K} d_k \quad (14)$$

where d_k represents the distance or cost associated with traversing edge k in path P.

In the Stealthy Approach phase, drones employ dynamic routing techniques to adapt to changing network conditions and optimize their path selection in real-time. This involves continuously monitoring network topology and adjusting routing decisions based on signal strength, congestion, and node mobility. Mathematically, dynamic routing algorithms aim to minimize a cost function J representing the overall path quality, and it is expressed as Eq.(15).

$$J = \sum_{k=1}^{K} Cost_k \quad (15)$$

where $Cost_k$ represents the cost associated with traversing edge k in the network graph.

Drones implement obstacle avoidance strategies during the Stealthy Approach phase to maintain stealth and avoid detection. This involves detecting and circumventing physical obstacles such as buildings, terrain features, and other drones to ensure smooth and uninterrupted navigation. The obstacle avoidance algorithms utilize sensor data and environmental maps to compute collision-free trajectories which is mathematically expressed as Eq.(16).

$$Avoidance_i = argmin_P \sum_{k=1}^{K} Distance_k \quad (16)$$

where $Avoidance_i$ represents the optimal avoidance trajectory for drone i, and $Distance_k$ represents the distance to obstacle k along trajectory P.

Stealthy movement in the network requires drones to conserve energy while navigating the environment. Energy-efficient movement strategies aim to minimize the energy expended during traversal by optimizing flight paths, velocity profiles, and acceleration patterns. Energy-efficient movement can be formulated as Eq.(17).

$$Minimize\ E = \int_{t_0}^{t_f} P(v(t))\, dt \quad (17)$$

where E represents the total energy consumption, $v(t)$ represents the velocity profile over time, and $P(v)$represents the power consumption as a velocity function.

In some scenarios, coordinated movement among multiple drones enhances stealth and improves overall network performance. Coordinated movement strategies involve synchronizing the actions of various drones to achieve common objectives such as coverage, surveillance, or data relay. The coordinated movement algorithms optimize trajectories and control inputs to maintain formation and achieve desired spatial configurations, which are mathematically expressed as Eq.(18).

$$Minimize\ J = \sum_{i=1}^{N} Error_i \quad (18)$$

where J represents the overall coordination error and $Error_i$ represents the deviation from the desired position or trajectory for drone i.

During the Stealthy Approach phase, drones continuously monitor their surroundings for anomalies and potential threats. Anomaly detection algorithms analyze sensor data and network metrics to identify abnormal behaviour or malicious activity, triggering appropriate responses such as rerouting, encryption, or alerting. Anomaly detection involves detecting deviations from expected patterns or norms, which are expressed as Eq.(19).

$$Anomaly_i = argmax_P \sum_{k=1}^{K} Deviation_k \quad (19)$$

where $Anomaly_i$represents the detected anomaly for drone i, and $Deviation_k$ represents the deviation from the expected behaviour along path P.

3.3. CAMOUFLAGE MECHANISM

The Camouflage Mechanism in JRP draws inspiration from the natural camouflage abilities of jaguars, allowing drones within a drone ad-hoc network to conceal their presence and protect sensitive data transmissions from detection or interception. This phase encompasses cryptographic techniques, secure communication protocols, and stealth strategies to ensure covert operation and robust data security. Encryption plays a fundamental role in the Camouflage Mechanism phase, enabling drones to encrypt transmitted data to prevent unauthorized access or interception. JRP utilizes Rivest-Shamir-Adleman (RSA) to secure data payloads against eavesdropping or tampering. Eq.(20) transforms plaintext M into ciphertext C using a cryptographic key K.

$$C = E_K(M) \quad (20)$$

where E_K represents the encryption function with key K.

Secure key exchange protocols are essential for establishing encrypted communication channels between drones while preventing key compromise or interception. JRP implements protocols such as Diffie-Hellman key exchange or Elliptic Curve Cryptography (ECC) for secure key negotiation. Eq.(21) shows how the key exchange protocols enable drones to derive a shared secret S without revealing it to potential adversaries.

$$S = DH(G, a, b) \quad (21)$$

where DH represents the Diffie-Hellman essential exchange function, G is the generator point, and a and b are private keys chosen by the communicating drones.

Drones may use digital signatures to check the legitimacy of sent data, ensuring it came from a genuine source and hasn't been altered en route. JRP uses the Elliptic Curve Digital Signature Algorithm (ECDSA) to authenticate and sign data payloads. To

sign a message M mathematically using a private key is to create a digital signature. Key private K_{priv} and checking the signature with its matching public key K_{pub} is expressed in Eq.(22) and Eq.(23).

$$Signature = Sign_{K_{priv}}(M) \quad (22)$$

$$Verify_{K_{pub}}(Signature, M) \quad (23)$$

Steganography techniques enable drones to conceal secret information within seemingly innocuous data payloads, adding camouflage to covert communication. JRP may utilize steganography algorithms such as LSB (Least Significant Bit) embedding or spread spectrum modulation to hide data within images, audio, or other media files. The steganography involves embedding secret information S within a cover medium C, and Eq.(24) expresses the same.

$$C_{stego} = Embed(C, S) \quad (24)$$

Protocol hiding mechanisms disguise the communication protocols drones use to prevent network fingerprinting and reconnaissance by potential adversaries. JRP may employ protocol obfuscation or traffic normalization to mask communication protocols' distinctive patterns and signatures. Eq.(25) mathematically provides how protocol involves transforming protocol headers or payloads to obscure their true nature.

$$Transofrmed_{Packet} = Obfuscate(Original\_Packet) \quad (25)$$

To adapt to evolving threats and environmental conditions, JRP incorporates dynamic stealth strategies that adjust camouflage mechanisms in real-time. These strategies may involve changing encryption keys, rotating cryptographic algorithms, or altering steganography parameters to maintain covert operations. The dynamic stealth strategies optimize camouflage mechanisms based on feedback and environmental cues, as expressed in Eq.(26).

$$Stealth_t = f(Feedback_t, Environment_t) \quad (26)$$

where $Stealth_t$ represents the level of stealthiness at time t, $Feedback_t$ represents feedback received from the network or sensors and $Environment_t$ represents environmental conditions at time t.

3.4. WAITING FOR OPPORTUNITY

This phase in JRP mirrors the patient observation and strategic timing of jaguars' hunting behaviour. In this phase, drones within the ad-hoc network patiently monitor network dynamics, environmental conditions, and communication opportunities before initiating or optimizing communication links. This phase involves various algorithms and strategies to maximize data transmission's success rate and efficiency. During the Wait for Opportunity phase, drones analyze network congestion levels to identify periods of low traffic and optimal communication windows. By monitoring packet arrival rates, queue lengths, and transmission delays, drones can determine the best time to initiate or prioritize data transmission. Network congestion can be mathematically quantified using Eq.(27) and Eq.(28) where P_l and average queue length Q_{avg} plays a significant role.

$$P_l = \frac{Total\ Packets\ Lost}{Total\ Packets\ Sent} \quad (27)$$

$$Q_{avg} = \frac{\sum_{i=1}^{N} Q_i}{N} \quad (28)$$

where N is the total number of nodes in the network and Q_i represents the queue length at node i.

Assessing the quality of communication channels is crucial for determining the suitability of initiating data transmission. Drones measure channel conditions such as signal-to-noise ratio (SNR), signal strength, and error rates to evaluate the reliability and performance of communication links. The channel quality Q can be quantified using metrics such as SNR, where Eq.(29) will be used to assess the quality.

$$Q = \frac{P_s}{P_n} \quad (29)$$

where P_s represents the signal power and P_n represents the noise power.

$$Opportunityi=argmaxjQj-\beta Cj \quad (30)$$

where $Opportunity_i$ represents the selected communication opportunity for drone i, Q_j is the channel quality at opportunity j, C_j is the congestion level at opportunity j, and β is a weighting factor.

Waiting for opportune moments to initiate data transmission also involves conserving energy resources to prolong drone operation and maximize network lifetime. Drones optimize energy consumption by employing sleep modes, dynamic power management, and duty-cycling techniques during idle periods. Eq.(31) is applied to minimize the energy expended for communication tasks.

$$Minimize\ E = \sum_{i=1}^{N} E_i \quad (31)$$

where E_i represents the energy consumption of the drone i.

JRP utilizes traffic prediction models to forecast network activity patterns and trends and anticipate future communication opportunities. By analyzing historical traffic data and network statistics, drones can predict upcoming peaks and valleys in traffic volume, enabling proactive scheduling and resource allocation. The traffic prediction models leverage time series analysis, machine learning algorithms, and statistical methods to forecast future traffic patterns where Eq.(32) is applied for the same.

$$\hat{T}_{t+1} = f(T_t, T_{t-1}, \dots, T_{t-n}) \quad (32)$$

where $\hat{T}_{t+1}$ represents the predicted traffic volume at time $t+1$, T_t represents the observed traffic volume at time t, and n is the number of previous time steps considered in the prediction.

The wait-for-opportunity phase in JRP is characterized by dynamic adaptation to changing network conditions and communication opportunities. Drones continuously monitor network metrics, environmental factors, and application requirements to adjust their behaviour and decision-making in real-time. Eq.(33) involves updating algorithms, parameters, and strategies based on feedback and observations from the network environment.

$$Opportunity_f = f(Metrics_t, Environment_t) \quad (33)$$

where $Opportunity_f$ represents the selected communication opportunity at time t, $Metrics_t$ represents network metrics observed at time t, and $Environment_t$ represents environmental conditions at time t.

3.5. SWIFT CONNECTION ESTABLISHMENT

The Swift Connection Establishment phase in JRP emulates jaguars' rapid and decisive actions when seizing opportunities during hunting. In this phase, drones within the ad-hoc network swiftly establish communication links with selected targets to facilitate efficient data transmission. Mathematically, this phase involves algorithms and protocols to minimize connection setup latency and optimize link establishment. Neighbour discovery is the initial step in the Swift Connection Establishment phase, where drones identify nearby nodes within their communication range. This process involves broadcasting discovery messages and listening for responses from potential neighbours. Eq.(34) is applied to model a distributed algorithm where drones exchange hello messages and update their neighbour tables.

$$Neighbor_i = argmax_j(S_j - \alpha E_j) \quad (34)$$

where $Neighbor_i$represents the selected neighbour node for drone i, $S_j$is the signal strength of node j, E_j is the energy consumption of node j, and α is a weighting factor balancing signal strength and energy efficiency.

Once neighbouring nodes are discovered, drones initiate a handshake process to establish communication links. This involves exchanging synchronization messages, negotiating communication parameters, and verifying mutual authentication. The connection setup handshake can be represented as a series of message exchanges and cryptographic operations as it is expressed from Eq.(35) to Eq.(37).

$$Drone_i \xrightarrow{Sunc} Drone_j \quad (35)$$

$$Drone_j \xrightarrow{Authenticate} Drone_i \quad (36)$$

$$Drone_i \xrightarrow{Acknowledge} Drone_j \quad (37)$$

Efficient channel access mechanisms are essential for minimizing contention and collision during connection establishment. JRP utilizes carrier sensing, random backoff, and contention resolution techniques to coordinate access to the shared wireless medium. Eq.(38) optimizes the probability of successful transmission while avoiding collisions.

$$Probability_{Success} = \frac{G_{Transmission}}{G_{Transmission} + G_{Interference} + G_{Noise}} \quad (38)$$

where $G_{Transmission}$represents the gain of the transmitted signal, $G_{Interference}$represents the gain of interfering signals and G_{Noise} represents the gain of background noise.

Drones dynamically configure communication parameters such as data rate, modulation scheme, and transmission power during connection establishment to adapt to channel conditions and network requirements. This ensures optimal link performance and reliability. Eq.(39) involves selecting parameters that maximize the achievable data rate while satisfying constraints.

$$Data\ Rate_{Optimal} = argmax_{Date\ Rate}\left(\begin{matrix}Throughput - \\ \alpha Energy\ Consumption\end{matrix}\right) \quad (39)$$

Throughput represents the achievable data rate, and α is a weighting factor balancing Throughput and energy consumption.

During connection setup, drones negotiate Quality of Service (QoS) parameters such as latency, jitter, and reliability to meet application-specific requirements. This involves exchanging QoS negotiation messages and agreeing on service-level agreements (SLAs) to ensure desired performance levels. Eq.(40) aims to maximize utility while satisfying constraints.

$$max_{QoS} Parameters \sum_{k=1}^{K} U_k \quad (40)$$

Eq.(40) is subject to Eq.(41).

$$C_k \leq T_k \leq \bar{C}_k \quad (41)$$

where $U_k$represents the utility of QoS metric k,C_k and $\bar{C}_k$ denote the lower and upper bounds of QoS metric k, and T_k represents the actual value of QoS metric k.

In scenarios where drones are mobile, or the network topology is dynamic, fast handover techniques ensure seamless connections and continuity of communication during node movement. JRP employs handover algorithms such as predictive handover, proactive scanning, and parallel handover to minimize handover latency and packet loss. Eq.(42) fast optimizes the handover decision based on predicted mobility patterns and network conditions.

$$Handover_i = argmin_j\left(Latency_{ij} - \beta PacketLoss_{ij}\right) \quad (42)$$

where $Handover_i$ represents the selected handover target for drone i, $Latency_{ij}$ is the handover latency between drones i and j, $PacketLoss_{ij}$ is the packet loss rate during handover, and β is a weighting factor.

3.6. SECURE DATA EXCHANGE

Secure data exchange in JRP ensures the confidentiality, integrity, and authenticity of transmitted data within the drone ad-hoc network. This phase employs cryptographic techniques, authentication mechanisms, and data integrity checks to safeguard sensitive information during transmission. Mathematically, secure data exchange encompasses various protocols and algorithms to mitigate security threats and protect communication channels. End-to-end encryption is a fundamental aspect of secure data exchange, where data payloads are encrypted at the source and decrypted at the destination to prevent eavesdropping or tampering by unauthorized entities. The Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) are two examples of symmetric and asymmetric encryption algorithms used by JRP. Eq.(43) and Eq.(44) restrict end-to-end encryption access to the plaintext data to authorized parties only.

$$C = E_K(M) \quad (43)$$

$$M = D_K(C) \quad (44)$$

where C represents the ciphertext, M represents the plaintext, $E_K$represents the encryption function with key K, and D_K represents the decryption function with key K.

Message Authentication Codes (MACs) check the data's validity and integrity to ensure that messages haven't been altered en route. The JRP uses cryptographic hash functions like CMAC or Hash-based Message Authentication Code to create MACs for data packages. MACs are calculated using Eq.(45), which is a cryptographic key K and the message M.

$$MAC = HMAC_K(M) \quad (45)$$

where $HMAC_K$ represents the HMAC function with key K.

Receiver authentication of the sender and detection of any unauthorized changes are made possible by digital signatures, validating the origin and integrity of sent data. JRP employs asymmetric cryptographic techniques like RSA and ECDSA when creating and checking digital signatures. Eq.(46) involves signing a message M with a private key. K_{priv} and verifying the signature using the corresponding public key K_{pub}.

$$Verify_{K_{pub}}(Signature, M) \quad (46)$$

Secure hashing functions are crucial in data integrity checks and fingerprinting, enabling drones to verify the integrity of received data payloads and detect any unauthorized modifications. JRP employs cryptographic hash functions such as SHA-256 (Secure Hash Algorithm 256-bit) to compute hash values for data payloads. Secure hashing functions produce fixed-size hash values $H(M)$ for input messages M using Eq.(47).

$$H(M) = SHA - 256(M) \quad (47)$$

Ensuring the secrecy of cryptographic keys and keeping encrypted communication routes secure requires effective key management. JRP employs key distribution protocols such as Diffie-Hellman key exchange or vital pre-distribution schemes to establish shared keys securely between communicating drones. The key management protocols enable drones to negotiate and exchange cryptographic keys without revealing them to potential adversaries using Eq.(48).

$$S = DH(G, a, b) \quad (48)$$

where S represents the shared secret key, G is the generator point, and a and b are private keys chosen by the communicating drones.

By preventing a compromise of previous session keys that may be caused by a breach of the long-term private key, forward secrecy methods improve the security of encrypted communication channels. JRP employs forward secrecy methods like session key derivation or ephemeral key exchange to ensure every communication session uses a unique key. The forward secrecy ensures that session keys are derived from temporary or ephemeral secrets, expressed in Eq.(49).

$$K_{Session} = f(K_{Ephemeral}) \quad (49)$$

where $K_{Session}$ represents the session key and$K_{Ephemeral}$ represents the temporary key.

3.7. OVERALL STRUCTURE AND FRAMEWORK OF JRP

The JRP enhances drone ad hoc networks by minimizing packet loss due to unstable communication links. This protocol integrates adaptive routing, energy efficiency, and robust security across various phases, ensuring stable and efficient communication in dynamic environments. Algorithm 1 outlines the key steps of JRP.

Algorithm 1: JRP

Input:
- Source Drone
- Destination Drone
- Intermediate Drones
- Spatial coordinates
- Neighbor table
- Number of neighboring Drones

Output:
- Filtered candidate set (i.e., Best Route)

Procedure:

Step 1 : Scanning Phase:
- Determine sensing range, node discovery probability, and signal strength
- Adjust parameters, analyze energy consumption, calculate network density
- Apply neighbor selection strategy

Step 2 : Target Selection:
- Calculate distance, signal strength, and energy consumption
- Evaluate QoS, select optimal neighbor

Step 3 : Stealthy Approach:
- If stealth required: plan path, apply dynamic routing, avoid obstacles, optimize movement

Step 4 : Camouflage Mechanism:
- Apply encryption, secure key exchange, digital signatures, steganography

Step 5 : Waiting for Opportunity:
- Analyze network congestion, assess channel quality, apply opportunistic transmission, conserve energy

Step 6 : Swift Connection Establishment:
- Discover neighbors, setup connection, apply channel access, configure links

Step 7 : Secure Data Exchange:
- Apply end-to-end encryption, message authentication, digital signatures, manage keys

Step 8 : Data Relay and Forwarding:
- Discover routes, forward packets, apply QoS routing, balance load

Step 9 : Data Processing and Analysis:
- Apply dynamic routing, allocate resources, adjust link metrics, apply energy-aware routing

Step 10: Decision: Further Processing Needed?
- If yes, go to Scanning Phase
- Else, end JRP

4. RESULTS AND DISCUSSION

4.1. SIMULATION SETTING

In this study on DANET, the NS-3 simulation tool is employed. The simulation duration is 900 seconds, and data is collected every second. Random seeds ensure robustness. The network includes 50 to 500 nodes in a 1000m x 1000m area, using grid and random topologies and the Random Waypoint mobility model. Communication parameters follow IEEE 802.11 standards.

Environmental factors like wind speed and obstacles are included. Table 1 provides the simulation settings for evaluating the proposed routing protocol against the stzsxate-of-the-art literature.

Table 1: Simulation Setting

Parameter Category	Parameter	Value/Range
General	Simulation Tool	NS-3
	Simulation Duration	900 seconds
	Data Collection Frequency	1 second
	Simulation Seed	Random
Network and Environment Parameters	Nodes	50 - 500
	Environment Dimensions	1000m x 1000m
	Network Topology	Grid, Random
	Model of Mobility	Random Waypoint
	Speed of Drone Movement	5 - 18 m/s
	Standby Time	20 - 180 seconds
	Environmental Factors	Wind Speed, Obstacles
Communication Parameters	MAC and PHY Layers	IEEE 802.11
	Transmission Range	80m - 240m
	Channel Bandwidth	20 MHz
	Interference Model	Basic, Detailed
	Propagation Model	Two-Ray Ground Reflection
	Path Loss Model	Free Space, Two-Ray Ground
	Collision Avoidance Mechanism	RTS/CTS
Traffic and Protocol Parameters	Protocol	AODV, DSR, OLSR, etc.
	Traffic Pattern	CBR (Constant Bit Rate)
	Packet Size	256 bytes
	Transmission Rate	2 Mbps - 12 Mbps
	Packet Interval	0.2 - 1 second
	Queue	FIFO, DropTail
	Control Packet Interval	0.5 - 5 seconds
	Congestion Control Mechanism	TCP, UDP
Energy Parameters	Initial Energy	1000 Joules
	Energy Model	Linear Battery Model
	Sleep Mode Energy Consumption	0.1 Joules/second
	Packet Transmission Energy	0.5 Joules/packet
	Packet Reception Energy	0.3 Joules/packet

4.2. PACKET DELIVERY RATIO AND PACKET LOSS RATIO ANALYSIS

Figure 1 offers a detailed comparative evaluation of Packet Delivery Ratio (PDR) and Packet Loss Ratio (PLR) across three routing protocols specifically applied within DANETs: AODV, QSCR, and JRP. The PDR is a crucial metric in DANETs, reflecting the percentage of packets successfully delivered across the network, which indicates the network's operational reliability. On the other hand, PLR measures the percentage of packets that fail to reach their destinations, providing insights into potential issues affecting network robustness and efficiency. Analyzing the data from Figure 1, a clear trend emerges across varying scales of drone deployments, ranging from 50 to 500 units. AODV exhibits a continuous decrease in PDR from 44.492% at 50 drones to 21.541% at 500 drones, with a corresponding increase in PLR from 55.508% to 78.459%.

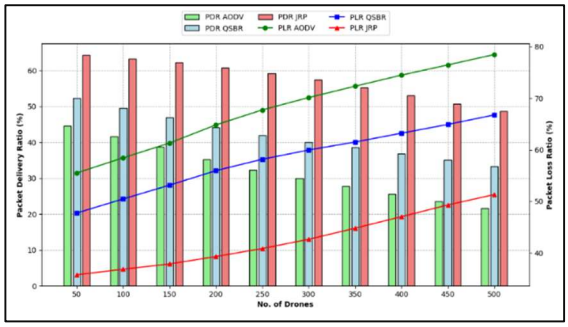

Figure 1. Packet Delivery Ratio and Packet Loss Ratio Results

This pattern underscores significant challenges related to bandwidth consumption due to the frequent broadcasting of control messages. This reduces available bandwidth and increases collision risks, which are detrimental in dense DANET environments. JRP shows a more robust performance with the highest PDR, initiating at 64.245%, reducing to 48.692%, and maintaining the lowest PLR, starting at 35.755% and increasing to 51.308%. JRP's architecture prioritizes critical data packets and ensures enhanced packet management, leading to reduced delays and lower loss rates even as network density escalates. This analysis highlights JRP's superior capability in managing high reliability and efficient packet delivery in densely populated DANET scenarios, proving its effectiveness in environments demanding high network performance and stability. The comparative metrics significantly advocate for JRP's adoption in DANET applications where reliable and timely data transmission is crucial.

4.3. LATENCY ANALYSIS

Figure 2 displays the results of a latency analysis for three routing protocols—AODV, QSCR, and JRP—employed within DANETs. Latency, measured in milliseconds, is a critical performance metric that reflects the time a data packet travels from the source to the destination across the network. Lower latency values indicate more efficient data handling and faster communication response times, which are vital in time-sensitive drone operations. AODV exhibits the highest latency throughout the experiment, starting at 3623 milliseconds for 50 drones and increasing to 4105 milliseconds for 500 drones. This rise in latency can be linked to AODV's reliance on frequent route discoveries and updates, which prolong the data transmission time, especially as the network density increases.

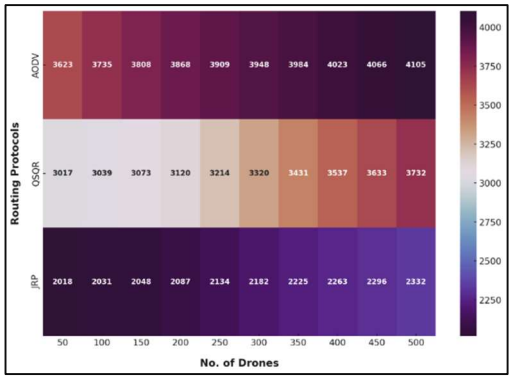

Figure 2. Latency Analysis Results

JRP demonstrates the most efficient latency performance, beginning at 2018 milliseconds for 50 drones and only moderately rising to 2332 milliseconds for 500 drones. This efficient latency management stems from JRP's protocol design, which intelligently prioritizes routing critical data packets. By expediting the transmission of high-priority packets and optimizing routing decisions based on current network conditions, JRP substantially reduces the time delays in packet delivery. This comparative analysis underscores JRP's superior capability to manage communication delays effectively within densely populated drone networks. By maintaining lower latency levels, JRP enhances real-time data transmission capabilities, which are crucial for applications that rely on swift and reliable communication to perform critical tasks. This makes JRP an advantageous choice for deployment in DANET environments where reducing communication delays is imperative for operational success.

4.4. ENERGY CONSUMPTION ANALYSIS

Figure 3 compares energy usage across three routing protocols—AODV, QSCR, and JRP—utilized in DANETs, with drone counts ranging from 50 to 500. Evaluating energy usage is crucial for assessing routing protocols' sustainability and operational effectiveness in environments where drone longevity and energy management are pivotal. Figure 3 indicates that AODV records the highest energy usage throughout the range of drone operations, starting at 58.567 for 50 drones and escalating to 77.762 for 500 drones.

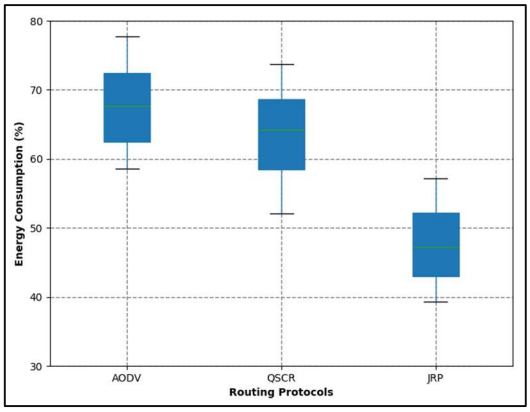

Figure 3. Energy Consumption Results

This trend can be attributed to the operational characteristics of AODV, which include extensive control message broadcasts that increase bandwidth utilization and elevate energy demands.

This mechanism proves less efficient when conserving energy is essential for extending drone operational life. JRP shows significantly more efficient energy management, beginning at 39.359 for 50 drones and peaking at 57.125 for 500 drones. This efficiency is achieved by prioritizing essential data transmissions, which reduces extra network chatter and conserves energy. By streamlining communications to prioritize crucial data, JRP minimizes the power spent on non-essential processes, which is beneficial for maintaining longer drone operation times and enhancing the overall sustainability of the network. This detailed comparison highlights the effectiveness of JRP in optimizing energy usage within dense drone networks. Its minimal energy consumption supports extended deployments and promotes a more robust and enduring network infrastructure, making it a favorable choice for DANET applications where efficient energy utilization is a critical requirement.

4.5. LINK STABILITY

Figure 4 explores link stability within Drone Ad hoc Networks (DANETs) employing three routing protocols: AODV, QSCR, and JRP. Link stability, quantified here through a stability index, crucially impacts the robustness and reliability of the network connections. This index reflects the ability of a routing protocol to maintain consistent and reliable links between nodes under varying network conditions and drone densities, from 50 up to 500.

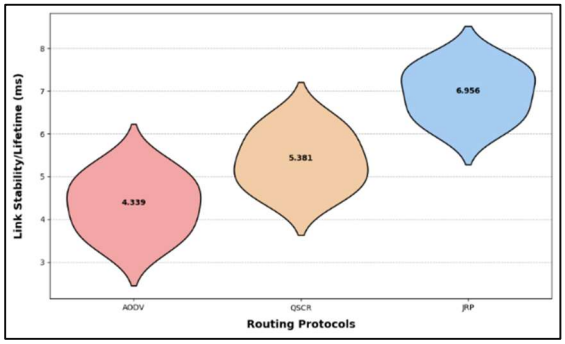

Figure 4. Link Stability Results

According to Figure 4, AODV shows the lowest stability scores, starting at 5.368 and decreasing to 3.310 as the number of drones increases. This trend suggests that AODV struggles with maintaining stable connections in larger and more dynamic networks, likely due to its reactive nature, which requires frequent route discoveries that disrupt ongoing transmissions. JRP records the highest link stability values, initiating at 7.760 and gradually decreasing to 6.040. The design of JRP, which includes prioritizing routes based on link quality and network conditions, significantly enhances its ability to maintain stable and reliable connections. This protocol minimizes the impact of changing network dynamics, leading to more onsistent performance even as network size and complexity increase. This analysis highlights JRP's effectiveness in sustaining higher levels of link stability across a wide range of network densities, underscoring its suitability for critical applications within DANETs where maintaining reliable network connections is essential. By ensuring more stable links, JRP supports enhanced communication continuity and reduces the likelihood of data loss or delays caused by frequent link failures, thereby improving overall network performance and reliability.

4.6. HOP COUNT ANALYSIS

Figure 5 presents a detailed examination of the hop count metric within Drone Ad hoc Networks (DANETs) using three routing protocols: AODV, QSCR, and JRP. The hop count, which measures the number of intermediate nodes a packet passes through from source to destination, is an essential indicator of the routing efficiency and network topology complexity. Lower hop counts typically signify more direct routing paths, which can lead to reduced latency and lower communication overhead.

The data from Table 7 shows that AODV consistently exhibits higher hop counts, starting at 9.969 for 50 drones and slightly increasing to 10.141 for 500 drones. This increase reflects AODV's characteristic of establishing routes based on first-available paths rather than optimizing for the shortest or most stable path, which can result in less efficient routing in larger, more complex networks. JRP demonstrates significantly lower hop counts, beginning at 6.441 for 50 drones and marginally rising to 6.949 for 500 drones. This efficiency is attributed to JRP's advanced routing algorithms prioritizing route stability and path length optimization. By efficiently selecting the most direct and stable routes, JRP minimizes the number of intermediate nodes involved, which enhances overall network efficiency by reducing potential points of failure and delays.

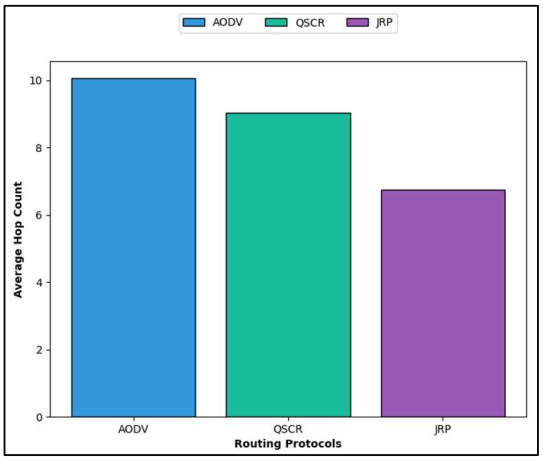

Figure 5. Hop Count Analysis

This comparative analysis emphasizes JRP's superior performance in minimizing hop counts, thus enhancing routing efficiency within densely populated drone networks. By optimizing path selection, JRP contributes to more streamlined network operations, supporting faster and more reliable data transmission essential for the operational success of applications reliant on timely and effective communication within DANETs.

5. CONCLUSION

The development and validation of the Jaguar-based Routing Protocol (JRP) signify a transformative enhancement in the field of Drone Ad hoc Networks (DANETs). This research tackles the prevalent issues of high mobility and unstable communication links within DANETs, which frequently lead to considerable packet loss, thereby impacting network integrity and performance. By leveraging strategies inspired by the natural behaviors of jaguars, JRP excels in stabilizing communication links and minimizing energy consumption, thus significantly improving the reliability and efficiency of network operations. The application of JRP can be pivotal in sectors like disaster response and environmental monitoring, where robust and dependable communication is critical. Furthermore, the principles underlying JRP could extend to other types of mobile ad hoc networks, suggesting a broad potential for future adaptations and research. Authors are reminded to adhere strictly to submission guidelines to ensure the coherence and quality of presentation, facilitating a smooth review and publication process. This adherence underscores the professionalism and attention to detail necessary for dissemination within the academic community.

REFERENCES

[1] N. Bartolini, A. Coletta, F. Giorgi, G. Maselli, M. Prata, and D. Silvestri, "Stop & Route: Periodic Data Offloading in UAV Networks," *2023 18th Wirel. On-Demand Netw. Syst. Serv. Conf. WONS 2023*, vol. 212, pp. 92–99, 2023, doi: 10.23919/WONS57325.2023.10062043.

[2] A. V. Savkin and H. Huang, "Multi-UAV Navigation for Optimized Video Surveillance of Ground Vehicles on Uneven Terrains," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 9, pp. 10238–10242, 2023, doi: 10.1109/TITS.2023.3270969.

[3] K. Wu, K. W. Chin, and S. Soh, "UAVs Deployment Algorithms for Maximizing Backhaul Flow," *IEEE Syst. J.*, vol. 17, no. 4, pp. 5592–5603, 2023, doi: 10.1109/JSYST.2023.3267447.

[4] S. Punia, H. Krishna, B. Vishwas Navada, and A. Sajjad, "Agrosquad - An IoT based precision agriculture using UAV and low-power soil multi-sensor," in *Proceedings of CONECCT 2021: 7th IEEE International Conference on Electronics, Computing and Communication Technologies*, 2021. doi: 10.1109/CONECCT52877.2021.9622639.

[5] R. G. Ribeiro, L. P. Cota, T. A. M. Euzebio, J. A. Ramirez, and F. G. Guimaraes, "Unmanned-Aerial-Vehicle Routing Problem With Mobile Charging Stations for Assisting Search and Rescue Missions in Postdisaster Scenarios," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 52, no. 11, pp. 6682–6696, 2022, doi: 10.1109/TSMC.2021.3088776.

[6] Y. Li, S. Wang, S. Zhou, and Z. Wang, "A mathematical formulation and a tabu search heuristic for the joint vessel-UAV routing problem," *Comput. Oper. Res.*, vol. 169, p. 106723, 2024, doi: 10.1016/j.cor.2024.106723.

[7] G. O. Tiniç, O. E. Karasan, B. Y. Kara, J. F. Campbell, and A. Ozel, "Exact solution approaches for the minimum total cost traveling salesman problem with multiple drones," *Transp. Res. Part B Methodol.*, vol. 168, pp. 81–123, 2023, doi: 10.1016/j.trb.2022.12.007.

[8] Z. Jin, K. K. H. Ng, C. Zhang, W. Liu, F. Zhang, and G. Xu, "A risk-averse distributionally robust optimisation approach for drone-supported relief facility location problem," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 186, p. 103538,

2024, doi: 10.1016/j.tre.2024.103538.

[9] J. Escorcia-Gutierrez *et al.*, "Sea turtle foraging algorithm with hybrid deep learning-based intrusion detection for the internet of drones environment," *Comput. Electr. Eng.*, vol. 108, p. 108704, 2023, doi: 10.1016/j.compeleceng.2023.108704.

[10] O. Chughtai, N. N. Qadri, Z. Kaleem, and C. Yuen, "Drone-Assisted Cooperative Routing Scheme for Seamless Connectivity in V2X Communication," *IEEE Access*, vol. 12, pp. 17369–17381, 2024, doi: 10.1109/ACCESS.2024.3359273.

[11] X. Ren, A. Froger, O. Jabali, and G. Liang, "A competitive heuristic algorithm for vehicle routing problems with drones," *Eur. J. Oper. Res.*, 2024, doi: 10.1016/j.ejor.2024.05.031.

[12] H. Li, F. Wang, and Z. Zhan, "Drone routing problem with swarm synchronization," *Eur. J. Oper. Res.*, vol. 314, no. 2, pp. 477–495, 2024, doi: 10.1016/j.ejor.2023.10.015.

[13] G. Khayat, C. X. Mavromoustakis, A. Pitsillides, J. M. Batalla, E. K. Markakis, and G. Mastorakis, "On the Weighted Cluster S-UAV Scheme Using Latency-Oriented Trust," *IEEE Access*, vol. 11, pp. 56310–56323, 2023, doi: 10.1109/ACCESS.2023.3282441.

[14] X. Sun, M. Fang, S. Guo, and Y. Hu, "UAV-rider coordinated dispatching for the on-demand delivery service provider," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 186, p. 103571, 2024, doi: 10.1016/j.tre.2024.103571.

[15] M. Hosseinzadeh *et al.*, "A Q-learning-based smart clustering routing method in flying Ad Hoc networks," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 36, no. 1, p. 101894, 2024, doi: 10.1016/j.jksuci.2023.101894.

[16] M. Hosseinzadeh, M. S. Yousefpoor, E. Yousefpoor, J. Lansky, and H. Min, "A new version of the greedy perimeter stateless routing scheme in flying ad hoc networks," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 36, no. 5, p. 102066, 2024, doi: 10.1016/j.jksuci.2024.102066.

[17] L. Zhen, Z. Yang, G. Laporte, W. Yi, and T. Fan, "Unmanned Aerial Vehicle Inspection Routing and Scheduling for Engineering Management," *Engineering*, 2024, doi: 10.1016/j.eng.2023.10.014.

[18] T. Calamoneri, F. Corò, and S. Mancini, "Management of a post-disaster emergency scenario through unmanned aerial vehicles: Multi-Depot Multi-Trip Vehicle Routing with Total Completion Time Minimization," *Expert Syst. Appl.*, vol. 251, p. 123766, 2024, doi: 10.1016/j.eswa.2024.123766.

[19] S. Dhanasekaran, S. Ramalingam, K. Baskaran, and P. Vivek Karthick, "Efficient Distance and Connectivity Based Traffic Density Stable Routing Protocol for Vehicular Ad Hoc Networks," *IETE J. Res.*, vol. 70, no. 2, pp. 1150–1166, Feb. 2024, doi: 10.1080/03772063.2023.2252385.

[20] E. Teimoury and R. Rashid, "A hybrid variable neighborhood search heuristic for the sustainable time-dependent truck-drone routing problem with rendezvous locations," *J. Heuristics*, vol. 30, no. 1–2, pp. 1–41, Apr. 2024, doi: 10.1007/s10732-023-09520-z.

[21] P. Stodola and L. Kutěj, "Multi-Depot Vehicle Routing Problem with Drones: Mathematical formulation, solution algorithm and experiments," *Expert Syst. Appl.*, vol. 241, p. 122483, 2024, doi: 10.1016/j.eswa.2023.122483.

[22] C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, USA: IEEE, 1999, pp. 90–100.

[23] M. Hosseinzadeh *et al.*, "A Q-learning-based smart clustering routing method in flying Ad Hoc networks," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 36, no. 1, p. 101894, 2024, doi: 10.1016/j.jksuci.2023.101894.

[24] 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.

[25] 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.

[26] K. S. J. Marseline, J. Ramkumar, and D. R. Medhunhashini, "Sophisticated Kalman Filtering-Based Neural Network for Analyzing Sentiments in Online Courses," in *Smart Innovation, Systems and*

Technologies, A. K. Somani, A. Mundra, R. K. Gupta, S. Bhattacharya, and A. P. Mazumdar, Eds., Springer Science and Business Media Deutschland GmbH, 2024, pp. 345–358. doi: 10.1007/978-981-97-3690-4_26.

[27] 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.

[28] 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.

[29] 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.

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

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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, Jan. 2023, doi: 10.22247/ijcna/2023/218516.

[36] 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.

[37] M. P. Swapna and J. Ramkumar, "Multiple Memory Image Instances Stratagem to Detect Fileless Malware," in *Communications in Computer and Information Science*, S. Rajagopal, K. Popat, D. Meva, and S. Bajeja, Eds., Cham: Springer Nature Switzerland, 2024, pp. 131–140. doi: 10.1007/978-3-031-59100-6_11.

[38] 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.

[39] R. Jaganathan, S. Mehta, and R. Krishan, *Intelligent Decision Making Through Bio-Inspired Optimization*. Sri Krishna Arts and Science College, India: IGI Global, 2024. doi: 10.4018/979-8-3693-2073-0.

[40] 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.

[41] 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.

[42] R. Karthikeyan and R. Vadivel, "Boosted Mutated Corona Virus Optimization

Routing Protocol (BMCVORP) for Reliable Data Transmission with Efficient Energy Utilization," *Wirel. Pers. Commun.*, vol. 135, no. 4, pp. 2281–2301, 2024, doi: 10.1007/s11277-024-11155-7.

[43] 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.

[44] 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

[45] N. K. Ojha, A. Pandita, and J. Ramkumar, "Cyber security challenges and dark side of AI: Review and current status," in *Demystifying the Dark Side of AI in Business*, 2024, pp. 117–137. doi: 10.4018/979-8-3693-0724-3.ch007.

[46] R. Vadivel and J. Ramkumar, "QoS-enabled improved cuckoo search-inspired protocol (ICSIP) for IoT-based healthcare applications," *Inc. Internet Things Healthc. Appl. Wearable Devices*, pp. 109–121, 2019, doi: 10.4018/978-1-7998-1090-2.ch006.

[47] R. Karthikeyan and R. Vadivel, "Proficient Dazzling Crow Optimization Routing Protocol (PDCORP) for Effective Energy Administration in Wireless Sensor Networks," in *IEEE International Conference on Electrical, Electronics, Communication and Computers, ELEXCOM 2023*, 2023, pp. 1–6. doi: 10.1109/ELEXCOM58812.2023.10370559.

[48] 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.

[49] 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.

[50] 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.

[51] 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, N. Prasad Padhy, and S. Kamalasadan, Eds., Singapore: Springer Nature Singapore, 2023, pp. 17–27. doi: 10.1007/978-981-19-8353-5_2.

[52] P. Menakadevi and J. Ramkumar, "Robust Optimization Based Extreme Learning Machine for Sentiment Analysis in Big Data," *2022 Int. Conf. Adv. Comput. Technol. Appl. ICACTA 2022*, pp. 1–5, Mar. 2022, doi: 10.1109/ICACTA54488.2022.9753203.