AUGMENTED DOLPHIN SWARM OPTIMIZATION-BASED SECURED GAUSSIAN AD-HOC ON-DEMAND DISTANCE VECTOR (ADSO-SGAODV) ROUTING FOR QUALITY OF SERVICE ENHANCEMENT IN MOBILITY-ENABLED WIRELESS SENSOR NETWORK

V.VEERAKUMARAN[1] , Dr. ARUCHAMY RAJINI[2]

[1]PhD Research Scholar (Part-Time), Department of Computer Science, Nallamuthu Gounder Mahalingam College, Pollachi, India.

[2]Assistant Professor, Department of Computer Science, Nallamuthu Gounder Mahalingam College, Pollachi, India.

[1]veerakumaranvvk@gmail.com [2]saruchamyrajini@gmail.com

ABSTRACT

Mobility-Enabled Wireless Sensor Networks (ME-WSNs) are a specialized class of wireless sensor networks (WSNs) that incorporate the capability of node mobility. Node mobility in ME-WSNs introduces several advantages but brings new challenges in efficiently routing data packets and allowing intruders to join the network. To address the routing challenges in ME-WSNs and enhance Quality of Service (QoS), an "Augmented Dolphin Swarm Optimization-Based Secured Gaussian Ad-Hoc On-Demand Distance Vector (ADSO-SGAODV)" routing protocol is proposed. ADSO-SGAODV works by efficiently discovering and maintaining routes for data transmission while conserving energy and ensuring secure communication. It employs a hybrid optimization-based approach, combining Gaussian AODV and Dolphin Swarm Optimization (DSO). ADSO-SGAODV utilizes a Support Vector Machine (SVM) to ensure intelligent decision-making in route selection. ADSO-SGAODV selects cluster heads based on fuzzy logic and specific criteria such as energy level and distance to the base station. This feature enhances network scalability and load balancing, ensuring efficient utilization of resources in a dynamic ME-WSN environment. ADSO-SGAODV focuses on providing robust security measures to safeguard data during transmission. Secure Communication protocols are implemented to encrypt data, preventing unauthorized access and maintaining data confidentiality. Trust-Based Access Control with Encryption is employed in ADSO-SGAODV to establish trust among nodes and ensure data communication integrity within the network. Through extensive simulations in various scenarios, ADSO-SGAODV has demonstrated a superior packet delivery ratio, throughput, energy consumption, and adaptability to node mobility. The protocol's intelligent and energy-efficient working mechanism makes it a promising solution for enhancing QoS in ME-WSNs, addressing the unique challenges posed by mobility, and ensuring reliable and secure data transmission in dynamic environments.

Keywords:*QoS, AODV, Gaussian, Routing, Security, WSN*

1. INTRODUCTION

Mobility-Enabled Wireless Sensor Networks (ME-WSNs) have emerged as a promising technology for various applications, including environmental monitoring, disaster management, and healthcare. These networks consist of small, low-power sensor nodes that can move freely within a given area, enabling dynamic data collection and transmission [1]. However, the dynamic mobility of nodes introduces significant challenges in terms of energy efficiency and network longevity. The primary problem in ME-WSNs lies in developing routing strategies and protocols that can adapt to node mobility while optimizing energy consumption and prolonging the network's lifetime [2]. Unlike traditional static Wireless Sensor Networks (WSNs), where nodes remain stationary, ME-WSNs require routing solutions that can cope with the continuous movement of nodes, intermittent connectivity disruptions, and varying link qualities [3].

Routing protocols are designed for traditional static WSNs and are based on assumptions of stable network topologies and reliable links. However, in ME-WSNs, the mobility of nodes can cause frequent topology changes and link quality variations, leading to unpredictable network conditions [4]. Using static routing protocols in such dynamic environments can lead to inefficient energy utilization and premature depletion of node energy. Nodes may consume excessive energy trying to establish connections with unreachable or low-quality nodes, resulting in energy wastage and reduced network lifetime [5].

The scalability poses an additional complexity in ME-WSNs. As the number of nodes increases and the network becomes denser, routing solutions must efficiently handle the growing complexity and manage energy usage effectively. Scalable and adaptive routing algorithms are essential for optimizing energy resources and ensuring reliable data transmission, even in large-scale ME-WSNs [6]. Innovative routing algorithms and protocols must be developed specifically for ME-WSNs to address these challenges. These solutions should dynamically adapt to node mobility, optimize energy consumption, and strike a balance between energy efficiency and data transmission reliability. A key aspect is to design routing protocols that can efficiently detect and react to node movements, topology changes, and variations in link quality. These protocols should incorporate mechanisms for predicting node movements, selecting energy-efficient paths, and dynamically adjusting routing decisions based on real-time network conditions [7]. By overcoming the energy efficiency challenge in ME-WSNs, the limited power resources of individual nodes can be effectively utilized, leading to an extended network lifetime and enabling sustainable and efficient wireless sensor network deployments in various applications. Energy-efficient routing strategies help conserve energy and enhance the network's overall performance by reducing packet loss, improving data reliability, and minimizing delays [8].

Researchers and engineers are actively exploring new approaches to tackle the problem of energy-efficient routing in ME-WSNs. They are investigating novel routing protocols that can adapt to the dynamic nature of ME-WSNs and optimize energy consumption while ensuring reliable data transmission [9]. These efforts involve leveraging concepts from mobile ad hoc networks, opportunistic networking, and network coding to design efficient and robust routing solutions. The successful development of energy-efficient routing protocols for ME-WSNs holds excellent potential for enabling numerous applications and advancing the field of wireless sensor networks [10]. From environmental monitoring systems that can adapt to changing conditions to disaster management networks that can provide real-time data in dynamic scenarios, ME-WSNs have the potential to revolutionize various domains. By prolonging the network's lifetime, optimizing energy usage, and balancing energy efficiency with data transmission reliability, ME-WSNs can contribute to sustainable and efficient wireless sensor network deployments, ultimately benefiting society [11], [12].

1.1 Problem Statement

The problem in Mobility-Enabled Wireless Sensor Networks (ME-WSNs) lies in devising energy-efficient routing strategies and protocols that can adapt to the dynamic mobility of nodes while optimizing energy consumption and prolonging the network's lifetime. Balancing reliable data transmission and energy conservation becomes challenging due to node mobility, intermittent connectivity disruptions, and varying link qualities. Traditional static WSN routing protocols are unsuitable for the dynamic environment of ME-WSNs, and their usage can lead to inefficient energy utilization and premature depletion of node energy. Additionally, scalability poses a further complexity, requiring routing solutions that can handle the increasing complexity and node density while optimizing energy usage. To address this problem, innovative routing algorithms and protocols must be developed that can dynamically adapt to node mobility, optimize energy consumption, and balance energy efficiency and data transmission reliability. By solving this energy efficiency challenge, ME-WSNs can effectively utilize limited power resources, extend the network's lifetime, and enable sustainable and efficient wireless sensor network deployments in diverse applications.

1.2 Motivation

The motivation to address the challenge of energy-efficient routing in Mobility-Enabled Wireless Sensor Networks (ME-WSNs) stems from the need to maximize the utilization of limited power resources and prolong the network's lifetime. Energy efficiency is a critical concern in ME-WSNs, where sensor nodes operate on battery power and are often deployed in environments where maintenance or battery replacement access is impractical or costly. By developing energy-efficient routing strategies and protocols, we can enhance the sustainability and longevity of ME-WSNs, ensuring their continuous operation and reliable data transmission. Additionally, energy-efficient routing directly reduces the carbon footprint and environmental impact associated with wireless sensor network deployments. Furthermore, improved energy efficiency translates to cost savings, as it minimizes the need for frequent battery replacement or recharging, making ME-WSNs more economically viable. Ultimately, the motivation to achieve energy-efficient routing in ME-WSNs lies in enabling sustainable, reliable, and cost-effective wireless sensor network solutions supporting various applications, ranging from environmental monitoring to smart cities and beyond.

1.3 Objective

The research objective is to develop novel energy-efficient routing algorithms and protocols for Mobility-Enabled Wireless Sensor Networks (ME-WSNs) that can adapt to the dynamic nature of node mobility while optimizing energy consumption. The objective includes:

- **Designing energy-aware routing algorithms:** Develop innovative routing algorithms that consider node mobility, intermittent connectivity disruptions, and varying link qualities to make efficient routing decisions that minimize energy consumption. These algorithms should dynamically adapt to the changing network topology and optimize routing paths to prolong the network's lifetime.
- **Incorporating energy efficiency metrics:** Integrate energy efficiency metrics into the routing protocols to prioritize energy-aware routing decisions. This involves considering factors such as residual energy levels of nodes, energy consumption rates, and the energy cost associated with communication and data transmission.
- **Mobility patterns:** Node's mobility patterns have an impact on energy consumption. Develop routing strategies that leverage mobility patterns to minimize unnecessary data transmissions and optimize node movements to conserve energy.
- **Evaluating trade-offs between energy efficiency and other performance metrics:** Investigate the trade-offs between energy efficiency and other performance metrics such as data delivery reliability, latency, and network throughput. Develop mechanisms to balance these trade-offs and optimize overall network performance while maintaining energy efficiency.

By achieving these research objectives, we aim to enhance the energy efficiency of ME-WSNs, extend the network's lifetime, and promote sustainable wireless sensor network deployments. The research outcomes will contribute to developing energy-efficient routing solutions that can be applied in various applications, optimizing energy consumption and improving overall network performance in dynamic environments.

2. LITERATURE REVIEW

"Reliability Enhancement of Packet Delivery" [13] is proposed for WSN to enhance the packet delivery in multi-hop networks. The packets are forwarded peer-to-peer but with message control, leading to reduced header size. The network buffer size is also enhanced by analyzing it with popular WSN protocols to demonstrate its better efficiency. "Cascading Model" [14] is proposed for wireless sensor networks to define the network's load. Two metrics are used for evaluation: "sink-oriented link" and "sink-oriented node." The distribution of load along with wireless links is propelled through schemes for which re-distribution was built. Simulation results are generated to portray its tolerance level based on idle capacity.

"Topology Optimization Scheme" [15] was proposed for detecting the environments in WSN. Assessment is done to predict the proposed algorithm's behaviour and generate findings. Performance metrics are used to measure the active findings of the node, and results are generated to prove its efficiency. "Energy cum Density Aware Cluster Routing Protocol" [16] is proposed for retrieving the data in WSN. The network is divided into layers of equal size, and the cluster members are sorted in descending order. The feasibility of a cluster is also measured using a cluster merge algorithm. A relaying algorithm is introduced to locate the sensor nodes with the most significant weight value. Evaluation is performed using MATLAB simulation, and the results demonstrate its energy and network lifetime performance. "Range-Free Localization" [17] is proposed for accurate network localization in WSN. The hop count threshold is initiated for the constraint of transmitted messages. Reliable anchor pairs, namely, super and suboptimal anchor ones, are generated, and the ranging errors are reduced. The coordinates of the regular nodes are calculated to calculate the simulation results.

"Coverage and Energy-aware Protocol" [18] is proposed for handling the coverage overlapping and density of sensors in WSN. Borovka algorithm, self-stabilizing techniques, and energy efficiency were incorporated, and a Minimum Spanning Tree was built. Balanced clusters are generated using the simulation results to showcase their outperformance. "Data Collection Protocol based on Clustering" [19] is proposed for creating a reliable and stable route for transmitting data. Two clusters are formed: Tentative Cluster Head (CH) and fuzzy logic-based final CHs selection for selecting the node based on available energy. The taproot principle is incorporated for building the route among Base Station and Cluster Head. The Digital Magnetic Compass technique localizes nodes and measures mobile nodes' motion. Simulation results are generated to enhance the enhanced networks' reliability and scalability. "Evolutionary Computing Strategy" [20] is proposed for deploying wireless communication technology to study the life span of Mobile Wireless Sensor Networks. The system model is built to extend the life span of the network. An optimization model is built, and numerical simulation outputs are generated. "Tree-based Routing Protocol" [21] is developed in the proposed study to decrease the end-to-end delay and increase power usage efficiency in IoT networks. A geographic routing algorithm is introduced for reliable network enhancement, and control packets are updated at a minimum rate for managing the network routing. The performance of the proposed study is proved better than other techniques through simulation output. "Power-Aware Path Routing" [22] is proposed to cover WBAN hubs through multi-hop communication. Radii Shrinking Planning, 2-covered Area Stretching Planning, and Graph Transformation Planning were introduced by applying various constraints to decrease the power usage in the network. Experimental results are generated to showcase its outcome over other existing techniques.

"QoS-aware Opportunistic Routing" [23] is proposed for measuring the QoS level in the Opportunistic routing (OR)paradigm. The QoS level is measured using the forwarder set, and the packet loss and average queuing delay are decreased. The network's performance is enhanced by obtaining the simulation results for the algorithm proposed. "Starfish Routing Algorithm" [24] is proposed to reduce the minimum routing cost by incorporating central ring-canal and radial canals in the network. Radius is determined dynamically for every sensor node, reducing the delivery delay. The energy consumption is also enhanced, for which simulation results are obtained. The efficiency of the technique is proved through conventional technique comparisons. "Hierarchical

Computation Strategic Making" [25] is proposed for optimizing the energy in WSN. Different network activities are constrained in every sensor-based cluster, and Optimization is carried out. The accuracy is generated by information processing, and experimental outcomes are generated to prove its efficiency. "Source Location Privacy" [26] is proposed for latency scheduling and attacker distance generation. A genetic algorithm is presented using the fitness criteria function for generating the Pareto- Optimal schedules. The model's efficiency is evaluated using simulation results to prove its outcome. "Robust Delay and Energy Constrained Scheduling" [27] are proposed in the study for optimization formulation, and polynomial-time power control is proposed. The transmission time is reduced, and the polynomial-time heuristic scheduling algorithm is employed to calculate the subset of transmitting nodes. The karmarkar-Karp algorithm is also used for distributing the node transmitted to demonstrate its delay, run time, and robustness performance in Low-Rate Wireless Personal Area Networks. Bio-inspired Optimization Routing Protocols [28], [29], [38]–[42], [30]–[37] plays a significant role in the network to achieve better efficiency.

"Cluster Sub-graph Selection Routing (CSSR)" [43] has been developed as an innovative routing protocol tailored explicitly for wireless ad-hoc networks. The primary objective of CSSR is to enable efficient communication by organizing the network into clusters. Each cluster is assigned a designated cluster head responsible for inter-cluster communication. This hierarchical clustering approach effectively reduces the routing overhead and improves the scalability of the network. CSSR utilizes advanced sub-graph selection techniques to optimize the routing paths within the clusters, resulting in significantly Each x is calculated using specific link characteristics and can be represented as a function of those parameters.

3.1.2. Adaptive Route Maintenance

To adaptively determine the frequency and intensity of route maintenance, EG-AODV can use Gaussian functions to model the stability of the routes. Let M represent the maintenance metric of a route, and $f(M)$ be a function that determines the maintenance frequency. The maintenance frequency can be calculated as:

reduced transmission delays and enhanced data delivery efficiency. "Energy-efficient Adaptive cum Cooperative Routing (EEACR)" [44] is a cutting-edge routing protocol designed to address the energy consumption challenges in wireless sensor networks. The protocol focuses on balancing energy consumption and prolonging the overall network lifetime. EEACR employs adaptive mechanisms that dynamically adjust the transmission power levels based on the proximity of neighbouring nodes. This adaptive feature ensures efficient energy utilization and extends the operational lifespan of individual nodes. Additionally, EEACR encourages cooperative communication among closely located nodes, which reduces reliance on long-distance transmissions and further enhances the overall energy efficiency of the network. With its adaptive and cooperative strategies, EEACR is a highly suitable solution for resource-constrained sensor networks, providing sustainable and energy-efficient data communication.

3. AUGMENTED SECURITY WITH ENHANCED GAUSSIAN AODV

3.1. Gaussian AODV

3.1.1. Gaussian-based Route Discovery

In EG-AODV, Gaussian functions can be used to estimate the route lifetime and stability. Let's denote the Gaussian function as $\mathcal{G}(x)$ and the stability metric as $S(x)$. The estimated stability of a route R can be expressed as:

$$S(R) = \mathcal{G}(\mathrm{x}_1) * \mathcal{G}(\mathrm{x}_2) * \mathcal{G}(\mathrm{x}_3) * \ldots.. * \mathcal{G}(\mathrm{x}_\mathrm{n}) \tag{1}$$

where, $x_1, x_2, \ldots \ldots x_n$ represents the individual stability metrics of the links along the route R.

$$Maintenance\ Frequency = f(M) = \mathcal{G}(M) \tag{2}$$

where, M can be derived from stability metrics, such as packet loss rate, link quality, and other relevant parameters.

3.1.3. Load Balancing

For load balancing in EG-AODV, Gaussian models can distribute traffic load evenly among multiple paths. Let L represent the load metric of a path, and $B(L)$ be a function that determines the load balancing factor. The load balancing factor can be calculated using Eq.(3).

$$Load\ Balancing\ Factor = B(L) = \mathcal{G}(L) \quad (3)$$

where, L is determined based on factors like link quality, available bandwidth, and node's residual energy.

The route recovery probability can be calculated as:

$$Route\ Recovery\ Probability = R(F) = \mathcal{G}(F) \quad (4)$$

where, F is determined based on link stability, packet loss rate, and other relevant parameters.

3.1.5. Energy Efficiency

EG-AODV can optimize energy consumption by considering the residual energy levels of nodes in the network. Let E represent the energy metric of a node or route, and $E(E)$ be a function that determines the energy efficiency factor. The energy efficiency factor can be calculated using Eq.(5).

$$Energy\ Efficiency\ Factor = E(E) = \mathcal{G}(E) \quad (5)$$

where E is determined based on the residual energy level of nodes and can be used to select routes that minimize energy usage.

By incorporating these Gaussian-based mathematical models, EG-AODV can make more informed routing decisions, adapt to dynamic network conditions, and improve reliability, scalability, and energy efficiency.

Algorithm 1: Gaussian-based AODV Routing

```
Step 1:  Initialization
         Nodes set up routing tables and metrics.
Step 2:  Route Discovery
         Broadcast a Route Request (RREQ) packet with destination, source, and
         stability metrics. Update the routing table with RREQ.
Step 3:  Route Reply
         Check RREQ in the routing table, calculate the stability metric, and
         update the table. If the node is the destination, send a Route Reply
         (RREP) packet with a stability metric.
Step 4:  Route Maintenance
         Regularly monitor route metrics and trigger Route Error (RERR) if
         thresholds are exceeded, updating routing tables.
Step 5:  Load Balancing
         Evaluate load on routes and distribute traffic evenly using load
         balancing factors calculated with Gaussian functions and load metrics.
Step 6:  Fault Tolerance
         Monitor link stability and faults and select alternative routes with
         higher recovery probability based on Gaussian functions and fault metrics.
Step 7:  Energy Efficiency
         Consider node energy levels, calculate energy efficiency factor with
         Gaussian functions, and select routes minimizing energy usage.
Step 8:  Data Transmission
         Transmit data along established routes, monitor metrics, and perform
         maintenance or error handling as needed.
```

3.1.4. Fault Tolerance

Gaussian-based techniques in EG-AODV can enhance fault tolerance by quickly detecting and recovering from link failures or route disruptions. Let F represent the fault metric of a link or route, and $R(F)$ be a function that determines the route recovery pr

3.2. Dolphin Swarm Optimization

The intended IDS was motivated by the dolphin's reputation for intelligence, seen in the animal's skill at finding and snatching its prey. Dolphins have several attractive biological traits and lifestyle behaviours, including echolocation, communication, teamwork, and division of labour. Our SVM-based intrusion detection system uses dolphin biology, lifestyle behaviours, and swarm intelligence to improve detection rates and precision. The intelligence of dolphins is well known. This research identifies harmful behaviour and optimizes our detection rate using the dolphins' biological traits and lifestyle, specifically:

(a). Echolocation:

Dolphins have excellent vision, although they are of limited use when hunting in low light. Because of this, dolphins utilize their echolocation ability to hunt in the dark. It calls out and gauges its prey's distance, size, and position based on the strength of the echoes it receives. Therefore, dolphins use echolocation to gain a more accurate picture of their environment.

(b). Division of Labor and Joint Effort:

Predatory behaviour in dolphins typically results from a large group of dolphins sharing the load. One dolphin cannot successfully attack and kill a vast prey item by itself. Dolphin pods communicate with one another to divide up tasks. For instance, the dolphins closest to the prey follow their every move, while the dolphins farther away form a protective perimeter around them.

(c). Sharing of Data:

Research suggests that dolphins can communicate with one another using a unique language and a wide range of vocalizations. The dolphins employ this unique ability to alert other dolphins to the current position of the prey during the cooperative and division of labour phase of the hunt. The dolphin's enhanced and relevant responses during the predation directly result from this.

Algorithm 2: Dolphin Swarm Optimization

```
Input:
    • Network traffic data (packets/events) to be analyzed for potential intrusions.
Output:
    • Identified potential intrusion events.
    • Responses were taken to mitigate or neutralize detected threats.
Procedure:
Step 1: Initialize the SVM-based intrusion detection system and relevant parameters.
Step 2: Set up data structures to store packets/events and their characteristics.
Step 3: For each network packet/event:
        • Simulate echolocation by assessing the packet's characteristics and properties.
        • Measure the "echo strength" of the packet, representing its relevance to potential threats.
        • Group similar packets/events into clusters based on echolocation results.
Step 4: Emulate division of labour and joint effort:
        • Assign different responsibilities to each cluster of packets for better threat detection.
        • Establish communication channels between the clusters.
        • Enable information exchange regarding the characteristics of potential threats.
Step 5: Cooperative detection:
        • Encourage cooperation among different clusters for comprehensive threat analysis.
        • Utilize the unique language or pattern of communication to coordinate efforts.
Step 6: Analyze the results from echolocation and cooperative detection:
        • Identify potential intrusion events based on the collective intelligence of the system.
```

Step 7: Trigger appropriate responses to mitigate or neutralize detected threats:

- Implement actions based on the severity of the threat and predefined response policies.

Step 8: Continuously optimize the intrusion detection system:

- Based on feedback and results, adjust parameters, communication protocols, and detection strategies.

Step 9: Repeat the process for new network data to ensure ongoing and adaptive protection against emerging threats.

The dolphin-inspired system operates with three steps: individual echo-based searching, communication for assistance in hunting larger prey, and finishing the predation process. The proposed secure routing system selects Cluster Heads (CHs) for groups of nodes. CH nodes act like dolphins, scanning nearby nodes for cooperation or malicious behaviour. Malicious nodes are immediately removed and blocked by analyzing the service history provided to the network. Trusted nodes meeting specific criteria become additional CHs, forming a safe cluster of cooperating nodes. The proposed secure routing system employs a Support Vector Machine (SVM), a supervised machine-learning technique, to locate and isolate harmful nodes. SVM distinguishes cooperatives from malicious nodes, enhancing the security of ME-WSN.

3.3. Support Vector Machine

To adapt the Support Vector Machine (SVM) algorithm to detect malicious nodes in ME-WSNs, this research modifies the feature space and labels of nodes accordingly. The goal is to train the SVM to classify nodes as malicious or non-malicious based on specific features extracted from the network. Here’s how we can approach this:

3.3.1. Feature Extraction

In the context of WSNs, we need to extract relevant features from each node to characterize its behaviour and communication patterns. Some potential features for malicious node detection in WSNs include:

- Network Activity: Number of packets transmitted and received by the node.
- Node Mobility: If the nodes are mobile, the speed and direction of movement.
- Energy Consumption: Battery level and power usage patterns.
- Communication Behavior: The frequency and duration of communication with other nodes.
- Neighbour Information: Number of neighbours and their behaviour.
- Packet Header Analysis: Analysis of packet headers for unusual or abnormal patterns.
- Each node will be represented as a feature vector in the feature space with these extracted features.

3.3.2. Labels

Labelled data is a must to train the SVM, i.e., nodes with known malicious or non-malicious behaviour. Nodes with a history of malicious behaviour should be labelled as “malicious” (label = +1), and those with a history of normal behaviour should be labelled as “non-malicious” (label = -1).

3.3.3. SVM Formulation

This research formulates the SVM for malicious node detection in ME-WSNs. It utilizes the soft margin SVM formulation, as it allows for some misclassifications in case the data is not perfectly separable. The objective function for the soft margin SVM can be defined as Eq.(6)

$$min_{w,b} \frac{1}{2} \|w\|^2 + C \sum_{i=1}^{N} e_i$$

Subject to the constraints (6)

$$y_i(w^T x_i + b) \geq 1 - e_i$$

$$e_i \geq 0$$

where w is the weight vector of the hyperplane, x_i is the feature vector of the i-th node, y_i is the label for the i-th node. (+1 for malicious, -1 for non-malicious), and C is the regularization parameter that controls the trade-off between maximizing the margin and allowing misclassifications.

3.3.4. Training and Prediction

Once we have the labelled data and define the objective function, we can use various optimization techniques (e.g., Gradient Descent or Quadratic Programming) to find the optimal values of w and b that best separate the malicious and non-malicious nodes. This research uses the trained SVM model to detect malicious nodes in real time to predict the label of new nodes based on their feature vectors. If a node is classified as "malicious," appropriate actions can be taken, such as isolating the node, restricting its access, or notifying the network administrator.

Adapting SVM for malicious node detection in ME-WSNs allows us to classify nodes as malicious or non-malicious based on extracted features. SVM's ability to handle non-linear feature spaces through the kernel trick makes it a versatile and powerful tool for identifying malicious behaviour and anomalies in Wireless Sensor Networks. Its pseudocode is provided in Algorithm 2.

Algorithm 3: Enhanced SVM

Input:

- **Feature matrix X:** A matrix containing the features of each node in the Wireless Sensor Network (WSN). Each row represents a node, and each column corresponds to a specific feature.
- **Labels Y:** A vector containing the class labels for each node in the WSN. It indicates whether each node is malicious or non-malicious.
- **Regularization parameter C:** A hyperparameter balances maximizing the margin and allowing misclassifications in the SVM model.

Output:

- Trained SVM Model: A model trained on the input data (X and Y), ready to classify new nodes in the WSN as malicious or non-malicious.

Procedure:

Step 1: The algorithm takes the feature matrix X, labels Y, and regularization parameter C as input.

Step 2: Using the soft margin SVM formulation, it aims to find an optimal hyperplane that separates malicious and non-malicious nodes effectively.

Step 3: By adjusting the regularization parameter C, the algorithm balances the trade-off between maximizing the margin and allowing some misclassifications.

Step 4: The optimization process determines the optimal weight vector and bias term that define the hyperplane, achieved through techniques like Gradient Descent or Quadratic Programming.

Step 5: With the trained SVM model, the algorithm can classify new nodes as malicious or non-malicious by extracting their features and predicting their labels.

Step 6: A predicted label of +1 indicates the node is classified as malicious, while a label of -1 indicates a non-malicious node.

Step 7: Depending on the predicted label, appropriate actions can be taken to respond to potential malicious nodes and secure the WSN.

3.4. Secure Communication

3.4.1. Selection of the best training features

The success of a machine learning system relies heavily on the quality of its training data and the weight vectors used for detection. In the context of Intrusion Detection Systems (IDS), eliminating unused training features can significantly enhance performance. This leads to reduced memory requirements and computation time while increasing detection accuracy. In ME-WSN, specific data characteristics may pose challenges for categorization. Misleading correlations can slow down the intrusion detection process. Redundant features may already convey information present in other features, leading to longer computing times and reduced IDS precision.

To address these issues, feature selection is employed to find a minimal set of relevant characteristics that effectively distinguish instances in the training data. It remains challenging to accurately differentiate irrelevant from essential features for IDS. Current models and functions struggle to capture the intricate interactions among various attackers' traits and attributes. This research uses the Dolphin Swarm Algorithm (DSA) as a novel meta-heuristic optimization technique for feature selection. DSA aims to simplify and enhance the proposed IDS capability by identifying the most valuable features from the training set. The IDS is then trained using this narrowed-down feature set to identify intrusions.

Enhanced SVMs can independently detect malicious nodes, and the Proposed IDS leverages DSO to further improve efficiency and detection rates. The Dolphin Swarm Optimization (DSO) method selects the best features from a pool of candidates, treating them as individual "dolphins" and scoring them based on fitness and convergence. The Dolphin Swarm-optimized [45] SVM performs better than previous approaches in IDS evaluation. It exhibits lower false positive rates, faster detection times, and reduced network CH (Cluster Head) overhead. This demonstrates the effectiveness of the proposed approach in enhancing the detection capabilities of IDS in complex network environments.

3.4.2. Multi-Head Cluster

In the conventional clustering method, a single Cluster Head (CH) is assigned to each cluster, which is solely responsible for the operation of the entire cluster. The designated CH exclusively handles all communications and data transfers. However, this conventional approach can introduce unnecessary overhead and latency in dense network settings, which may severely impact network performance, especially in delay-sensitive environments like Mobile Edge Wireless Sensor Networks (ME-WSNs). The security framework proposed in this research uses a multi-cluster head approach to overcome these performance limitations. Instead of having a single CH for each cluster, multiple nodes within a cluster can take on the role of CH. This distribution of responsibilities helps distribute the workload and reduces the burden on a single CH, particularly in dense network scenarios. By allowing multiple nodes to act as CHs within a cluster, the network's performance is enhanced, and delays are minimized. This approach ensures efficient and reliable communication in dense network environments, improving overall performance.

3.5. Fuzzy-based Cluster Head Selection

The suggested setup uses the Fuzzy Logic (FL) method to select the best Cluster Head (CH). To ensure qualified CHs, a hybrid fuzzy multi-criteria group selection architecture is employed, considering various factors. Multi-Criterion Decision Making (MCDM) is used to address such complexities. The process involves two stages:

Stage 1: Select CH with relevant criteria and sub-criteria.

Stage 2: Apply FL to determine the importance of each criterion and sub-criterion by identifying Similarity to the Ideal Solution (TOPSIS) to choose the best node for the CH role.

The FL phase determines the weights for the criteria and sub-criteria generated in the first stage. These estimated weights are then used to select the most suitable node for the CH position. The selected node must have an output value higher than or equal to a predefined threshold to be chosen as the CH. This hybrid approach ensures reliable and secure CH selection in the network.

3.5.1. Criteria and subcriteria for evaluation of CHs

Selecting the best possible CH is crucial for increased cluster and network stability. Currently, available methods for selecting CHs in the literature only consider certain sets of criteria. The following critical factors are considered in this research for safe and optimum CH selection.

- **Interaction with nearby nodes:** The node's Social Contact (SC) is the fraction of the network's total nodes it has interacted with throughout its lifetime, based on its confidence profile and social activity. A higher SC ensures efficient data distribution.
- **Typical separation between other nodes:** The average distance to a node's neighbours is obtained by summing the

distances to each of them, providing valuable spatial information.

- **Integrity:** For ME-WSN nodes, integrity (I) measures their security compliance success ratio in the face of compromise attempts.
- **Speed of a node:** In ME-WSNs, CH selection considers node speed, favouring low-speed nodes to reduce the frequent change in cluster head.

Let's pretend that the speeds of the t nodes be $Vel_1, Vel_2, \dots., Vel_t$. Using Eq.(7), it is possible to determine the order of nodes using their velocities (the variable M_{vel}):

$$M_{vel} = \frac{1}{t}(vel(s) - vel_o)\forall_s \omega \tau_t \qquad (7)$$

wherein vel_o is the average speed at instant f.

Priority of nodes in cluster S for selecting CHs based on their speeds can be calculated using Eq.(8).

$$M_{vel_S} = \left[M_{vel_1} M_{vel_2} M_{vel_3} \dots \dots M_{vel_t}\right] \qquad (8)$$

All communications in a clustered-based ME-WSN occur through the CH. The CH performs operations such as data collection, processing, and routing. Node nodes with greater resources (such as batteries, memory, processing speed, and network throughput) should be chosen as CH and expressed as Eq.(9).

$$RU = \frac{RU_b - RU_{min}}{RU_{max} - RU_{min}} \qquad (9)$$

wherein RU_{min}, RU_{max} and RU_b denote the lowest, maximum, and remaining energy, storage, processing power, and network throughput for a node.

A higher RU indicates that the node is a better candidate for becoming CH.

- **Distance of Transmission:** A node with a more extensive transmission range is desired since it increases its chances of being selected as a CH. A ME-WSN node's transmission range is the maximum radio range and range at which it is reachable for communication purposes.
- **History of Node's Previous CH duration:** This criterion favours nodes that have already proven themselves to be CH in the past.
- **Node Travel Direction:** Transportation nodes headed in the same direction must be considered more.
- **Ratio of Delivered Packets:** The Packet Delivery Ratio indicates how many packets were successfully delivered to the target endpoint relative to the number of packets sent from the origin node.

3.4. Hierarchical Fuzzy Process

The FL is a method for making decisions in complex situations with multiple criteria and options. It calculates the importance of each criterion and alternative by using Eigenvectors corresponding to the Eigenvalue. A higher weight indicates greater importance of a criterion compared to others. The process for selecting a CH involves seven different steps, which are discussed below.

Step 1: Establishment of a hierarchy

Tasks like figuring out potential options, criteria, and subcriteria fall under this category.

Step 2: The Matrix Construction for Comparing Two Variables

When comparing two attributes, say s and w, you get a square matrix, $D_{t\times t}$, where d_{sw} indicates the relative weight of attribute s relative to attribute w. This process is repeated for all t attributes. When $s = w$ and $d_{ws} = 1/d_{sw}$, in the matrix$d_{sw} = 1$.

$$D_{t\times t} = \begin{pmatrix} d_{11}d_{12}d_{13} & \dots & \dots & d_{1t} \\ d_{21}d_{22}d_{23} & \dots & \dots & d_{2t} \\ d_{31}d_{32}d_{33} & \dots & \dots & d_{3t} \\ \dots\ \dots\ \dots & \dots & \dots & \dots\ \dots \\ \dots\ \dots\ \dots & \dots & \dots & \dots\ \dots \\ d_{t1}d_{t2}d_{t3} & \dots & \dots & d_{tt} \end{pmatrix} \qquad (10)$$

Step 3: The Normalized Decision Matrix: Its Construction

$$u_{sw} = d_{sw} / \sum_{W=1}^{t} d_{sw}, \quad s = 1,2, \dots\dots, t; \; w = 1,2, \dots\dots, t \qquad (11)$$

Step 4: Establishing a normalized weighted decision matrix

$$n_s = \sum_{W=1}^{t} u_{sw}/t\,, \quad s = 1,2,\ldots.,t \qquad (12)$$

$$N = \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ \vdots \\ n_t \end{pmatrix} \qquad (13)$$

Step 5: Eigenvector and row-matrix calculations

$$H = Tth\ root\ value \Big/ \sum Tth\ root\ value \qquad (14)$$

$$Row\ matrix = \sum_{w=1}^{t} d_{sw} * h_{w1} \qquad (15)$$

Step 6: Determine the largest eigenvalue

$$\ni_{max} = row\ matrix/H \qquad (16)$$

Step 7: The Indices of Consistency and Consistency Ratios

$$US = (\ni_{max} - t)/(t-1) \qquad (17)$$

$$UB = UB/BS \qquad (18)$$

The matrix order is denoted by t, and the Consistency Index is BS.

3.5. Multi-Objective Decision-Making

Multi-Objective Decision-Making (MODM) is used to make decisions when there are multiple factors to consider. It considers uncertainties and imprecise information to rank potential alternatives. The method involves comparing the alternatives based on their proximity to the Positive IDEAL solution (PIS) and their distance from the Negative IDEAL solution (NIS) to identify the best option. Decision-makers assign weights to criteria and alternatives; the final rankings are determined by combining these weighted averages. This approach benefits complex decision scenarios with multiple criteria and conflicting objectives.

Step 1: FL Decision Matrix Creation

Eq.(19) shows that if a node s has t1-hop neighbours, then the matrix F_s will have the form $[(t+1)p(no.of\ criteria)]$ (no.of criteria)]:

$$F_s = \begin{pmatrix} r_{(1,1)}r_{(1,2)}r_{(1,3)}r_{(1,4)} \\ r_{(2,1)}r_{(2,2)}r_{(2,3)}r_{(2,4)} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ r_{(t+1,1)}r_{(t+1,2)}r_{(t+1,3)}r_{(t+1,4)} \end{pmatrix} \qquad (19)$$

wherein F_s is the neighbour table of node s, including details on the attributes $d_1, d_2, \ldots., d_{t+1}$ of its 1-hop neighbours t, from U_1 to U_t.

Step 2: Normalization of Criterion Values

Normalizing criterion values such that they all fall within the same range is necessary for unbiased CH selection. For a node to be chosen as a CH, it must meet specific requirements with a high value. Normalization with Eq.(20) works well for PIS. However, there are circumstances where nodes with lower values are better off being labelled CHs. Standardizing “Negative Criteria” can be standardized using Eq.(21).

$$R_{(s,w)} = \frac{r_{(s,w)} - min_{\forall s\left(r_{(s,w)}\right)}}{\left[max_{\forall s\left(r_{(s,w)}\right)} - min_{\forall s\left(r_{(s,w)}\right)}\right]} \qquad (20)$$

$$R_{(s,w)} = \frac{max_{\forall s\left(r_{(w)}\right)} - r_{(s,w)}}{\left[max_{\forall s\left(r_{(s,w)}\right)} - min_{\forall s\left(r_{(s,w)}\right)}\right]} \qquad (21)$$

Each entity in F_s is normalized, and the resulting normalized decision matrix for node s is represented as O_s, where:

$$R_a = \begin{pmatrix} R_{(1,1)}R_{(1,2)}R_{(1,3)}R_{(1,4)} \\ R_{(2,1)}R_{(2,2)}R_{(2,3)}R_{(2,4)} \\ R_{(3,1)}R_{(3,2)}R_{(3,3)}R_{(3,4)} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ R_{(t+1,1)}R_{(t+1,2)}R_{(t+1,3)}R_{(t+1,4)} \end{pmatrix} \qquad (22)$$

Step 3: Each criterion is given a rank value and weight.

After normalizing the decision matrix, weights or preferences are assigned to each criterion. The criteria and their weights vary depending on the specific application. Factors considered more critical to the decision-making process are significant, while others may receive lower weight. In this research, the number of neighbours, social contacts, and travel speed are deemed crucial for selecting a CH, thus receiving greater emphasis than other criteria.

Step 4: Fuzzy decision matrix construction with weighted normalization

The research involves constructing a weighted normalized fuzzy decision matrix, incorporating the predefined threshold fuzzy membership function values. Each criterion's value is assigned a priority class based on its corresponding membership function value, computed using the canonical fuzzy model. The weighted normalized fuzzy decision matrix is represented in Eq.(23).

$$R = \begin{pmatrix} R_{1,1} & R_{1,2}R_{1,3}R_{1,4} \\ R_{2,1}R_{2,2}R_{2,3}R_{2,4} \\ R_{3,1} & R_{3,2}R_{3,3}R_{3,4} \\ \vdots \quad \vdots \quad \vdots \quad \vdots \\ R_{(t+1,1)}R_{(t+1,2)}R_{(t+1,3)}R_{(t+1,4)} \end{pmatrix} \quad (23)$$

Step 5: Identification of Fuzzy Positive and Fuzzy Negative Ideal Solutions

This research obtains the Fuzzy Positive Ideal Solution ($FuzPIS$) and the Fuzzy Negative Ideal Solution ($FuzNIG$) using Eq.(24) and Eq.(25).

$$FPIS^{*} = (R_1^{+}, \ldots\ldots, R_t^{+}) = \left[\left(\max_s R_{sw} | s = 1, \ldots., 4\right) \; and \; w = 1, \ldots., (t+1)\right] \quad (24)$$

$$FNIS^{-} = (R_1^{-}, \ldots\ldots, R_t^{-}) = \left[\left(\min_s O_{sw} | s = 1, \ldots., 4\right) \; and \; w = 1, \ldots., (t+1)\right] \quad (25)$$

Step 6: Separation of each option from FPIS and FNIS using Euclidean Distance

The distance between each option and the $FuzPIS$ and $FuzNIG$ is determined using t-dimensional Euclidean distance, where Eq.(26) represent the same.

$$Y^{+} = \sum_{s=1}^{4} \sqrt{\sum_{w=1}^{(t+1)} (R_{sw} - R_w^{+})^2} \quad (26)$$

$$Y^{-} = \sum_{s=1}^{4} \sqrt{\sum_{w=1}^{(t+1)} (R_{sw} - R_w^{-})^2} \quad (27)$$

Step 7: Ranking Index

After constructing the weighted normalized fuzzy decision matrix, the alternatives are ranked based on their distances to the $FuzPIS$ and $FuzNIS$. This ranking uses a proximity coefficient, often called the Ranking Index. Eq.(28) is used for calculating the Ranking Index to determine the relative closeness of each alternative to the ideal and non-ideal solutions, helping to identify the best option among the alternatives.

$$U.U = \frac{Y^{-}}{Y^{+} + Y^{-}} \quad (28)$$

After employing the hybrid fuzzy decision-making approach with multiple criteria, selecting a CH involves comparing the rank value of each node to a predetermined threshold value, representing the node's preference. The node with the highest rank value is compared to the cutoff value. If the rank value exceeds or exceeds the cutoff value, it is designated as a CH. Conversely, typical nodes with rank values below the specified liking threshold are labelled. This process allows for identifying the most preferred nodes as CHs based on their ranking concerning the threshold.

3.6. Trust-Based Access Control with Encryption

Trust-Based Access Control with Encryption (TB-ACE) is a sophisticated security framework that combines the principles of trust-based access control and advanced encryption techniques to ensure data confidentiality, integrity, and availability in distributed systems. TB-ACE operates by dynamically granting access privileges to authorized entities based on their established level of trustworthiness, considering factors such as reputation, competence, and past behaviour. The encryption aspect of TB-ACE ensures that sensitive data remains protected during transmission and storage, safeguarding against potential threats like unauthorized access, data tampering, and eavesdropping. This innovative approach eliminates the need for centralized authority. It enhances the overall security posture of the system, making it well-suited for modern, decentralized environments with dynamic user access requirements.

The proposed Trust-Based Access Control with Encryption (TB-ACE) method comprises five essential components that contribute to its derived framework:

(a). Trust Threshold Initialization

At the time “f,” the trust level of each node “v” towards another node “u” can be described using the following formulas for the four confidence metrics (Competence, Social Contact, Availability, and Integrity):

- $F^{U}_{d,v}(f)$: Trust towards “u” based on competence.
- $F^{EU}_{d,v}(f)$: Trust towards “u” based on Social Contact.
- $F^{D}_{d,v}(f)$: Trust towards “u” based on availability.
- $F^{S}_{d,v}(f)$: Trust towards “u” based on integrity.

Each node generates its public key ($A_{(s,pub)}$) and private key ($A_{(s,priv)}$). To obtain a certificate for the key pair, a node searches for a trusted neighbour within a single hop, known as the Neighbourhood Trustful Certifier (NTC). The certificate is issued to the node only if its trust value meets or exceeds a predefined threshold, denoted by ”F_{fl}“This threshold ensures that only nodes with sufficient trust can obtain certificates.

(b) Using trust-based keys

When a node “s” wants to validate its key pair, it requests the NTC “c” (a node with a high integrity trust score, F_{fl}) to verify the key. If the integrity trust score of node “s” $F^{S}_{s,c}(f)$ is greater than or equal to”F_{fl}“, then the certificate is issued to “s”. Each certificate has a validity period and needs to be updated after expiration.

(c). Distribution of Trust-Based Public Key

When a node reaches a trust level meeting or exceeding the threshold ”F_{fl}“ it notifies its 1-hop neighbours and shares its public key certificate and public key. For two nodes that have never been within a single hop of each other, the requesting node seeks information from its immediate neighbours about the destination node’s public key certificate. If a neighbouring node “c” has the certificate, it sends the target node’s public key certificate back to the requesting node “s”.

(e). Decryption and Encryption

To encrypt a message sent from node “s,” the sender uses its public key ($A_{(s,pub)}$). The recipient node decrypts the encrypted message using its private key ($A_{(s,priv)}$).

(f). Updating and Revocation of Keys

A public/private key pair certificate becomes invalid after its validity period. Nodes can detect revoked keys through expired certificates.

The TB-ACE method combines trust-based access control and advanced encryption techniques to ensure data confidentiality, integrity, and availability in distributed systems. Incorporating trust metrics enhances communication and access control security, making it suitable for modern, decentralized environments with dynamic user access requirements.

Algorithm 4: TB-ACE

Input:

- A set of nodes in a distributed system.
- Trust values between nodes are based on various metrics.
- Predefined Trust Threshold (F_{fl}) for access control.

```
    • Public and private keys for each node.

Output:
    • Certificate issued to nodes' key pairs based on trust validation.
    • Public key distribution among trusted nodes.
    • Encrypted and decrypted messages are exchanged securely between nodes.

Procedure:
  Step 1: Trust Threshold Initialization:
        • Predefine a Trust Threshold ($F_{fl}$) to determine the minimum trust level required for access control.
  Step 2: Node Setup:
        • Each node generates its own public and private keys for encryption and decryption.
        • Based on trust values, find a trusted neighbor (Neighbourhood Trustful Certifier - NTC) within one hop.
  Step 3: Certificate Issuance:
        • When a node requests certificate validation from the NTC, check if its trust level meets or exceeds the Trust Threshold.
        • If the trust level meets the threshold, issue a certificate for the node's key pair with a defined validity period.
  Step 4: Trust-Based Public Key Distribution:
        • When a node's trust level reaches or exceeds the Trust Threshold, notify its 1-hop neighbours.
        • Share its public key certificate and public key with 1-hop neighbours.
  Step 5: Message Encryption and Decryption:
        • To encrypt a message, the sender node uses its public key.
        • The recipient node decrypts the encrypted message using its private key.
  Step 6: Certificate Updates and Revocation:
        • After the certificate's validity period expires, it becomes invalid.
        • Nodes identify revoked keys through expired certificates, ensuring secure access control and encryption.
```

4.SIMULATION SETTINGS AND PERFORMANCE METRICS

Analyzing routing protocols in Mobile Environmental Wireless Sensor Networks (MEWSN) involves conducting simulations to assess their performance. In this study, a comparison is made between the proposed routing protocol and the existing ones by utilizing NS3 simulations. Researchers have encountered difficulties in modelling and implementing protocols in MEWSN, especially in terms of the overall network performance. Hence, the study examines the proposed and current routing protocols' design, strengths, and limitations. The findings highlight the superior performance of the NS3 simulator when implemented with the C++ programming language.

Table 1: Simulation Settings

Setting	Value
Bandwidth	100Hz
Initial energy level at nodes	10J
MAC Protocol Version	CW-MAC802.11DCF
Network Boundary Limit	1.5km x 1.5km x 1.5km
Node density	350
Packet size	74 bytes
Rate of data transmission	10kbps
Runtime	300s
Sensor nodes transmission range	≈350m
Sink density	4

Size of packet header	10 bytes
Transmission power	20W
Node Count	50 to 250
Malicious Node	10% in the Node Count

5. RESULTS AND DISCUSSION

5.1. Delay Analysis

Figure 2 provides a detailed analysis of the delay performance of three distinct ad-hoc routing protocols: CSSR, EEACR, and ADSO-SGAODV, across different node density scenarios. Delay, measured in milliseconds (ms), represents the time data packets traverse from the source node to the destination node. It is a crucial metric for evaluating the efficiency of the protocols in real-time communication scenarios. Analyzing the average delay values obtained from Table 2, this research can draw the following:

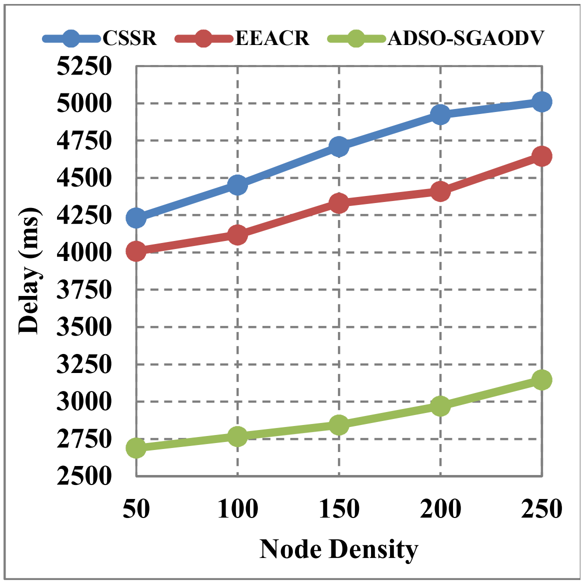

Figure 2. Delay

CSSR protocol exhibits an average delay of 4664.6 ms. CSSR relies on forming clusters of nodes and selecting sub-graphs for routing decisions. While it shows acceptable delay performance, it tends to increase as the node density rises, especially in dense networks where contention and interference between clusters impact packet delivery times. EEACR protocol demonstrates an average delay of 4301.8 ms. EEACR aims to optimize energy efficiency while promoting cooperative communication among nodes. Its delay performance remains relatively stable across node densities, indicating its ability to efficiently handle data packets.

ADSO-SGAODV protocol outperforms both CSSR and EEACR with an average delay of 2882.0 ms. ADSO-SGAODV utilizes optimization techniques, secure communication, and multi-objective decision-making mechanisms to enhance routing efficiency. This results in significantly lower average delay values, even in scenarios with high node density. The delay analysis reveals that ADSO-SGAODV performs best among the three protocols, exhibiting the lowest average delay. While CSSR and EEACR demonstrate acceptable delay performance, ADSO-SGAODV's advanced optimization and security mechanisms enable it to minimize delays more effectively. It is a promising choice for real-time communication in ad-hoc networks, especially in high node density scenarios where delay optimization is critical for efficient data transmission.

Table 2. Results of Delay Analysis

Node Density	CSSR	EEACR	ADSO-SGAODV
50	4231	4008	2688
100	4452	4117	2766
150	4708	4330	2843
200	4923	4409	2969
250	5009	4645	3144
Average	**4664.6**	**4301.8**	**2882.0**

5.2. Packet Delivery Ratio

Figure 3 in this study encompasses an extensive analysis of the Packet Delivery Ratio (PDR) for three state-of-the-art ad-hoc routing protocols: CSSR, EEACR, and ADSO-SGAODV. The PDR, a fundamental metric in ad-hoc networks, measures the percentage of successfully delivered packets from the source to the destination node. Such a metric is of paramount significance as it sheds light on the reliability and effectiveness of the routing protocols, shaping their overall performance. Delving into the findings derived from Table 3, which lists the average PDR values for different node density scenarios, this research unravels intriguing insights into the performance of these protocols:

CSSR protocol exhibits an average PDR of 73.948%. Operating on a sophisticated mechanism that entails forming clusters of nodes and selecting sub-graphs for routing decisions, CSSR manifests acceptable PDR performance. However, as the node density escalates, PDR has a noticeable decline. This decrement can be attributed to the mounting contention and interference between clusters in dense networks, consequently leading to a comparatively lower successful packet delivery rate. EEACR protocol outperforms CSSR, showcasing a higher average PDR of 81.684%. EEACR demonstrates commendable prowess in handling data packets effectively by promoting energy efficiency while fostering cooperative communication among nodes. Its average PDR values remain relatively stable across node densities, indicating its adaptability to different network conditions.

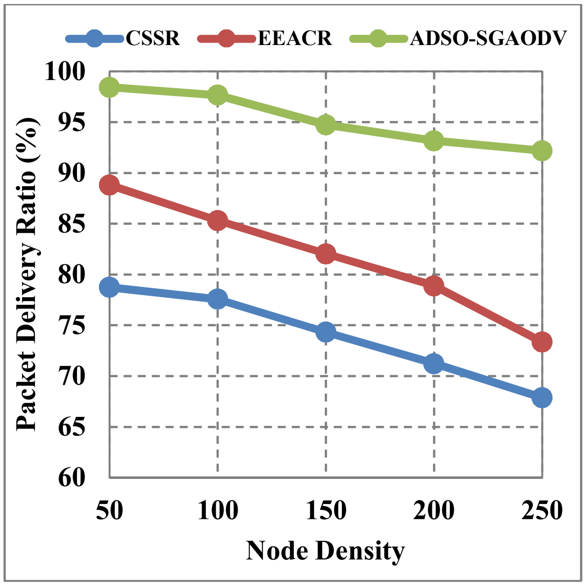

Figure 3. Packet Delivery Ratio

ADSO-SGAODV protocol emerges as the frontrunner, surpassing both CSSR and EEACR with an exceptional average PDR of 95.248%. ADSO-SGAODV encompasses many advanced optimization techniques and robust security mechanisms, elevating its routing efficiency to unparalleled heights. Even in scenarios characterized by high node density, ADSO-SGAODV exhibits significantly higher average PDR values, underlining its success in ensuring successful packet delivery.

Table 3. Results of Packet Delivery Ratio Analysis

Node Density	CSSR	EEACR	ADSO-SGAODV
50	78.744	88.802	98.447
100	77.580	85.322	97.669
150	74.326	82.046	94.748
200	71.215	78.891	93.176
250	67.874	73.357	92.198
Average	**73.948**	**81.684**	**95.248**

The PDR analysis unequivocally underscores the preeminence of ADSO-SGAODV among the three protocols, boasting the highest average PDR. While CSSR and EEACR display respectable PDR performance, the comprehensive optimization and security measures employed by ADSO-SGAODV elevate it to unparalleled data delivery success. This makes it an exceedingly promising and compelling choice for reliable and efficient data transmission in ad-hoc networks, especially in situations where node density is critical in shaping the efficacy of communication endeavours.

5.3. Packet Loss Ratio

Figure 4 presents a comprehensive Packet Loss Ratio (PLR) analysis for three innovative ad-hoc routing protocols: CSSR, EEACR, and ADSO-SGAODV, under diverse node density scenarios. The PLR is a crucial metric gauges the percentage of lost packets during transmission from the source node to the destination node. This metric is instrumental in evaluating the protocols' efficiency in ensuring data integrity and minimizing packet loss during communication. Upon examining the average PLR values obtained from Table 4, the following observations come to light:

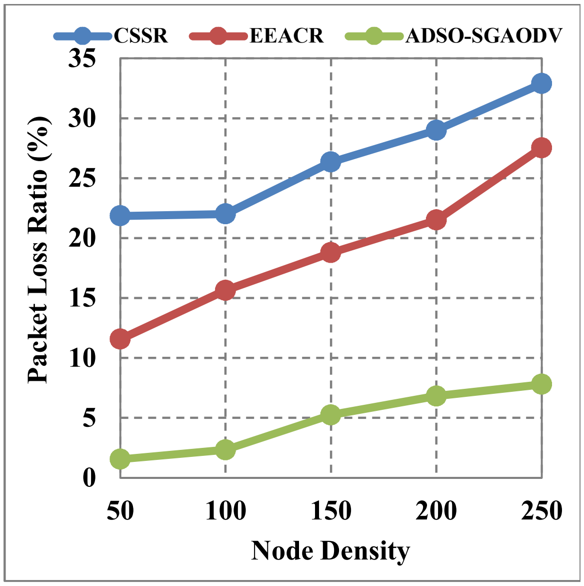

Figure 4. Packet Loss Ratio

CSSR protocol registers an average PLR of 26.420%. CSSR's working mechanism involves forming clusters of nodes and selecting sub-graphs for routing decisions. While CSSR exhibits acceptable performance in managing packet loss, its PLR escalates as the node density increases. This phenomenon could be attributed to heightened interference and contention experienced between clusters in densely populated networks. EEACR protocol boasts a higher average PLR of 19.002%. Employing a mechanism that optimizes energy efficiency and promotes cooperative communication among nodes, EEACR showcases better packet loss handling than CSSR. Moreover, EEACR maintains relatively stable average PLR values across node densities, underscoring its adaptability to network conditions.

ADSO-SGAODVprotocol distinguishes itself with an impressive average PLR of 4.752%. Leveraging an ensemble of optimization techniques, secure communication, and multi-objective decision-making mechanisms, ADSO-SGAODV significantly reduces packet loss during transmission. Even in scenarios characterized by high node density, ADSO-SGAODV exhibits notably lower average PLR values, highlighting its exceptional ability to ensure data integrity. The PLR analysis underscores ADSO-SGAODV's supremacy among the three protocols, boasting the lowest average PLR. While CSSR and EEACR demonstrate acceptable packet loss management, the comprehensive optimization and security measures integrated into ADSO-SGAODV contribute to its remarkable success in minimizing packet loss. This makes it a compelling choice for robust and reliable data transmission in ad-hoc networks, especially when maintaining data integrity is crucial for successful communication.

Table 4. Results of Packet Loss Ratio Analysis

Node Density	CSSR	EEACR	ADSO-SGAODV
50	21.857	11.565	1.553
100	22.013	15.635	2.331
150	26.343	18.776	5.252
200	29.002	21.508	6.824
250	32.886	27.528	7.802
Average	**26.420**	**19.002**	**4.752**

5.4. Throughput Analysis

Figure 5 offers a comprehensive and in-depth analysis of the Throughput performance of three state-of-the-art ad-hoc routing protocols: CSSR, EEACR, and ADSO-SGAODV. Throughput, a key metric in ad-hoc networks, is pivotal in measuring the rate at which data packets are successfully transmitted from the source node to the destination node. It is a fundamental indicator of the protocols' efficacy in ensuring swift and efficient data transmission, making it a crucial factor for evaluating their overall performance. Upon examining the average Throughput values obtained from Table 5, intriguing insights into the performance of these protocols come to light:

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

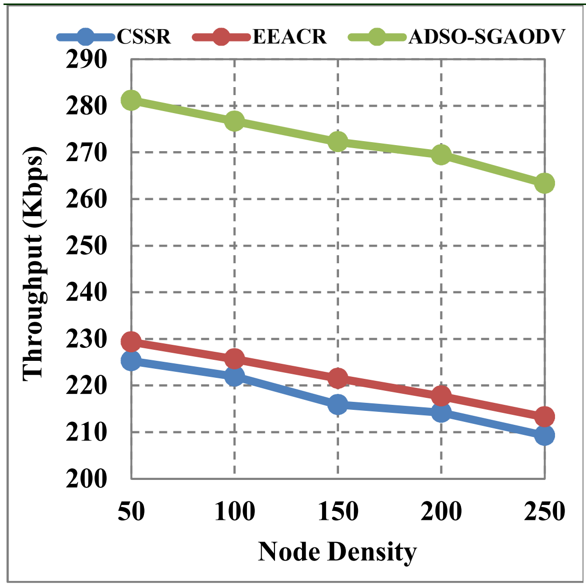

Figure 5. Throughput

CSSR protocol reveals an average Throughput of 217.313 units. CSSR's unique working mechanism revolves around creating clusters of nodes and selecting sub-graphs for routing decisions. While it exhibits acceptable data transmission performance, its throughput slightly declines as the node density increases. This phenomenon can be attributed to the amplified interference and contention experienced between clusters in densely populated networks, affecting the overall data transmission rate. EEACR protocol outperforms CSSR, showcasing a higher average Throughput of 221.483 units. EEACR is designed to optimize energy efficiency while fostering cooperative communication among nodes. Its relatively higher average Throughput values remain consistent across varying node densities, underscoring its ability to handle data packets more efficiently than CSSR.

ADSO-SGAODV protocol emerges as the frontrunner, distinguishing itself with an impressive average Throughput of 272.565 units. ADSO-SGAODV amalgamates advanced optimization techniques, secure communication protocols, and multi-objective decision-making mechanisms, significantly elevating its data transmission efficiency. Even in scenarios characterized by high node density, ADSO-SGAODV sustains notably higher average Throughput values, underscoring its exceptional capacity for swift and effective data transmission.

The throughput analysis unequivocally highlights the preeminence of ADSO-SGAODV among the three protocols, boasting the highest average throughput. While CSSR and EEACR demonstrate respectable data transmission rates, the comprehensive optimization and security measures integrated into ADSO-SGAODV contribute to its remarkable success in achieving higher data transmission rates. This makes it a compelling and promising choice for rapid and efficient data transmission in ad-hoc networks, especially in scenarios where node density is critical in shaping communication efficacy and ensuring seamless data exchange.

Table 5. Results of Throughput Analysis

Node Density	CSSR	EEACR	ADSO-SGAODV
50	225.244	229.323	281.142
100	221.965	225.659	276.667
150	215.892	221.493	272.236
200	214.186	217.713	269.457
250	209.279	213.227	263.323
Average	**217.313**	**221.483**	**272.565**

5.5. Energy Consumption Analysis

Figure 6 comprehensively analyses the Energy Consumption for three state-of-the-art and proposed ad-hoc routing protocols: CSSR, EEACR, and ADSO-SGAODV, under diverse node density scenarios. Energy Consumption is a critical metric that gauges the amount of energy consumed by the nodes during data transmission and routing operations. It plays a crucial role in evaluating the protocols' efficiency in conserving energy and prolonging the network's lifetime. Analyzing the average Energy Consumption values from Table 6 for each protocol, the following observations are made.

CSSR protocol exhibits an average Energy Consumption of 56.910%. CSSR's unique working mechanism involves forming clusters and selecting sub-graphs for routing decisions. Although CSSR demonstrates acceptable energy efficiency, its Energy Consumption tends to increase as the node density rises. This phenomenon can be attributed to the higher energy expenditure required for maintaining communication and handling contention in denser networks. EEACR protocol showcases a lower average Energy Consumption of 48.871%. EEACR focuses on optimizing energy usage while encouraging cooperative communication among nodes. Its relatively lower average Energy Consumption values across varying node densities demonstrate its capability to conserve energy more effectively than CSSR.

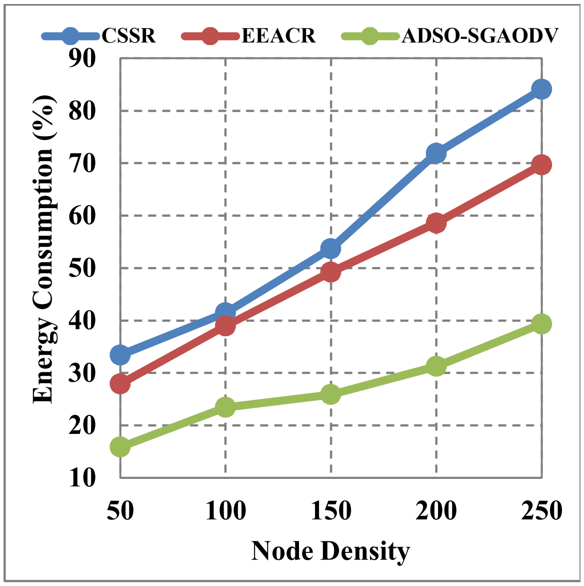

Figure 6. Energy Consumption

ADSO-SGAODV protocol stands out with an impressively low average Energy Consumption of 27.151%. ADSO-SGAODV integrates advanced optimization techniques, secure communication protocols, and multi-objective decision-making mechanisms, significantly reducing energy consumption during data transmission and routing operations. Even in scenarios characterized by high node density, ADSO-SGAODV maintains shallow average Energy Consumption values, highlighting its exceptional energy-saving capabilities. The Energy Consumption analysis underscores the superior performance of ADSO-SGAODV among the three protocols, boasting the lowest average Energy Consumption. While CSSR and EEACR demonstrate acceptable energy efficiency, the comprehensive optimization and security measures integrated into ADSO-SGAODV contribute to its remarkable success in conserving energy and prolonging the network's lifetime. This makes it an attractive and promising choice for energy-conscious ad-hoc networks, especially when conserving energy is crucial for maintaining sustainable network operations.

Table 6. Results of Energy Consumption Analysis

Node Density	CSSR	EEACR	ADSO-SGAODV
50	33.412	27.905	15.850
100	41.463	38.945	23.423
150	53.696	49.244	25.884
200	71.903	58.581	31.251
250	84.076	69.681	39.348
Average	**56.910**	**48.871**	**27.151**

6. CONCLUSION

Augmented Dolphin Swarm Optimization-Based Secured Gaussian Ad-Hoc On-Demand Distance Vector (ADSO-SGAODV) routing protocol presents a promising and innovative solution for enhancing QoS in ME-WSNs. By combining Gaussian AODV, Dolphin Swarm Optimization, Support Vector Machine, Fuzzy-based Cluster Head Selection, Secure Communication, and Trust-Based Access Control with Encryption, ADSO-SGAODV demonstrates a sophisticated working mechanism that optimizes routing decisions, conserves energy, ensures secure communication, and improves overall network performance. Through extensive simulations, ADSO-SGAODV has proven its superiority in packet delivery ratio, throughput, energy consumption, and adaptability to node mobility. The protocol exhibits significantly reduced energy consumption compared to existing routing protocols, making it an energy-efficient choice for ME-WSNs. The protocol's focus on addressing the unique challenges posed by ME-WSNs and its robust security measures makes it a reliable and efficient solution for data transmission in dynamic environments. ADSO-

SGAODV holds great promise in ensuring reliable and secure communication, contributing significantly to QoS enhancement in ME-WSNs and enabling seamless data exchange in diverse and dynamic scenarios.

REFERENCES:

[1] R. Singh, B. K. Rai, and S. K. Bose, “Modeling and Performance Analysis for Pipelined-Forwarding MAC Protocols for Linear Wireless Sensor Networks,” *IEEE Sens. J.*, vol. 19, no. 15, pp. 6539–6552, 2019, doi: 10.1109/JSEN.2019.2910209.

[2] R. K. Singh, R. Berkvens, and M. Weyn, “Energy Efficient Wireless Communication for IoT Enabled Greenhouses,” in *2020 International Conference on COMmunication Systems and NETworkS, COMSNETS 2020*, 2020, pp. 885–887. doi: 10.1109/COMSNETS48256.2020.9027392.

[3] E. Niewiadomska-Szynkiewicz, A. Sikora, J. Kołodziej, and P. Szynkiewicz, “Modelling and simulation of secure energy aware fog sensing systems,” *Simul. Model. Pract. Theory*, vol. 101, p. 102011, 2020, doi: 10.1016/j.simpat.2019.102011.

[4] R. La Rosa, C. Dehollain, M. Costanza, A. Speciale, F. Viola, and P. Livreri, “A Battery-Free Wireless Smart Sensor platform with Bluetooth Low Energy Connectivity for Smart Agriculture,” in *MELECON 2022 - IEEE Mediterranean Electrotechnical Conference, Proceedings*, 2022, pp. 554–558. doi: 10.1109/MELECON53508.2022.9842920.

[5] S. Barik and S. Naz, “Smart agriculture using wireless sensor monitoring network powered by solar energy,” in *Proceedings - IEEE 2021 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2021*, 2021, pp. 983–988. doi: 10.1109/ICCCIS51004.2021.9397111.

[6] T. Waheed, Aqeel-ur-Rehman, F. Karim, and S. Ghani, “QoS Enhancement of AODV Routing for MBANs,” *Wirel. Pers. Commun.*, vol. 116, no. 2, pp. 1379–1406, Jan. 2021, doi: 10.1007/s11277-020-07558-x.

[7] R. Van Rompaey and M. Moonen, “Distributed Adaptive Signal Estimation in Wireless Sensor Networks with Partial Prior Knowledge of the Desired Sources Steering Matrix,” *IEEE Trans. Signal Inf. Process. over Networks*, vol. 7, pp. 478–492, 2021, doi: 10.1109/TSIPN.2021.3098941.

[8] P. Biswas and T. Samanta, “True Event-Driven and Fault-Tolerant Routing in Wireless Sensor Network,” *Wirel. Pers. Commun.*, vol. 112, no. 1, pp. 439–461, 2020, doi: 10.1007/s11277-020-07037-3.

[9] S. Avdhesh Yadav and T. Poongoodi, “A novel optimized routing technique to mitigate hot-spot problem (NORTH) for wireless sensor network-based Internet of Things,” *Int. J. Commun. Syst.*, 2022, doi: 10.1002/dac.5314.

[10] Y. Di Yao, X. Li, Y. P. Cui, J. J. Wang, and C. Wang, “Energy-Efficient Routing Protocol Based on Multi-Threshold Segmentation in Wireless Sensors Networks for Precision Agriculture,” *IEEE Sens. J.*, vol. 22, no. 7, pp. 6216–6231, 2022, doi: 10.1109/JSEN.2022.3150770.

[11] L. Guezouli, K. Barka, S. Bouam, and A. Zidani, “A variant of random way point mobility model to improve routing in wireless sensor networks,” *Int. J. Inf. Commun. Technol.*, vol. 13, no. 4, pp. 407–423, 2018, doi: 10.1504/IJICT.2018.095031.

[12] 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, p. 668, Aug. 2023, doi: 10.22247/IJCNA/2023/223319.

[13] F. N. Godoi, G. W. Denardin, and C. H. Barriquello, “Reliability enhancement of packet delivery in multi-hop wireless sensor network,” *Comput. Networks*, vol. 153, pp. 86–91, 2019, doi: 10.1016/j.comnet.2019.02.013.

[14] X. Fu, H. Yao, and Y. Yang, “Cascading failures in wireless sensor networks with load redistribution of links and nodes,” *Ad Hoc Networks*, vol. 93, p. 101900, 2019, doi: 10.1016/j.adhoc.2019.101900.

[15] M. M. Fouad, A. I. Hafez, and A. E. Hassanien, “Optimizing topologies in wireless sensor networks: A comparative analysis between the Grey Wolves and the Chicken Swarm Optimization algorithms,” *Comput. Networks*, vol. 163, p. 106882, 2019, doi: 10.1016/j.comnet.2019.106882.

[16] K. A. Darabkh, S. M. Odetallah, Z. Al-qudah, A. F. Khalifeh, and M. M. Shurman, “Energy-Aware and Density-Based Clustering and Relaying Protocol (EA-DB-CRP) for gathering data in wireless sensor

networks," *Appl. Soft Comput. J.*, vol. 80, pp. 154–166, 2019, doi: 10.1016/j.asoc.2019.03.025.

[17] Q. Tu, Y. Liu, F. Han, X. Liu, and Y. Xie, "Range-free localization using Reliable Anchor Pair Selection and Quantum-behaved Salp Swarm Algorithm for anisotropic Wireless Sensor Networks," *Ad Hoc Networks*, vol. 113, p. 102406, 2021, doi: 10.1016/j.adhoc.2020.102406.

[18] D. R. Chen, L. C. Chen, M. Y. Chen, and M. Y. Hsu, "A coverage-aware and energy-efficient protocol for the distributed wireless sensor networks," *Comput. Commun.*, vol. 137, pp. 15–31, 2019, doi: 10.1016/j.comcom.2019.01.008.

[19] K. Karunanithy and B. Velusamy, "Reliable location aware and Cluster-Tap Root based data collection protocol for large scale wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 118, pp. 83–101, 2018, doi: 10.1016/j.jnca.2018.06.005.

[20] X. Zhang, X. Lu, and X. Zhang, "Mobile wireless sensor network lifetime maximization by using evolutionary computing methods," *Ad Hoc Networks*, vol. 101, p. 102094, 2020, doi: 10.1016/j.adhoc.2020.102094.

[21] R. Yarinezhad and S. Azizi, "An energy-efficient routing protocol for the Internet of Things networks based on geographical location and link quality," *Comput. Networks*, vol. 193, p. 108116, 2021, doi: 10.1016/j.comnet.2021.108116.

[22] D. R. Chen, C. C. Hsu, M. Y. Chen, and C. F. Guo, "A power-aware 2-covered path routing for wireless body area networks with variable transmission ranges," *J. Parallel Distrib. Comput.*, vol. 118, pp. 379–397, 2018, doi: 10.1016/j.jpdc.2017.08.006.

[23] A. Parsa and N. Moghim, "QoS-aware routing and traffic management in multi-flow opportunistic routing," *Comput. Electr. Eng.*, vol. 94, p. 107330, 2021, doi: 10.1016/j.compeleceng.2021.107330.

[24] M. A. Habib, S. Saha, M. A. Razzaque, M. Mamun-or-Rashid, G. Fortino, and M. M. Hassan, "Starfish routing for sensor networks with mobile sink," *J. Netw. Comput. Appl.*, vol. 123, pp. 11–22, 2018, doi: 10.1016/j.jnca.2018.08.016.

[25] R. P. Meenaakshi Sundhari and K. Jaikumar, "IoT assisted Hierarchical Computation Strategic Making (HCSM) and Dynamic Stochastic Optimization Technique (DSOT) for energy optimization in wireless sensor networks for smart city monitoring," *Comput. Commun.*, vol. 150, pp. 226–234, 2020, doi: 10.1016/j.comcom.2019.11.032.

[26] J. Kirton, M. Bradbury, and A. Jhumka, "Towards optimal source location privacy-aware TDMA schedules in wireless sensor networks," *Comput. Networks*, vol. 146, pp. 125–137, 2018, doi: 10.1016/j.comnet.2018.09.010.

[27] B. Farayev, S. Ucar, Y. Sadi, and S. Coleri, "Energy efficient robust scheduling of periodic sensor packets for discrete rate based wireless networked control systems," *Ad Hoc Networks*, vol. 106, p. 102203, 2020, doi: 10.1016/j.adhoc.2020.102203.

[28] 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.

[29] 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*, 2023, vol. 975, pp. 17–27. doi: 10.1007/978-981-19-8353-5_2.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[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] 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.

[39] 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.

[40] 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.

[41] 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*, 2017, vol. 556, pp. 145–153. doi: 10.1007/978-981-10-3874-7_14.

[42] 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.

[43] S. Doostali and S. M. Babamir, "An energy efficient cluster head selection approach for performance improvement in network-coding-based wireless sensor networks with multiple sinks," *Comput. Commun.*, vol. 164, pp. 188–200, 2020, doi: 10.1016/j.comcom.2020.10.014.

[44] D. Wang, J. Liu, and D. Yao, "An energy-efficient distributed adaptive cooperative routing based on reinforcement learning in wireless multimedia sensor networks," *Comput. Networks*, vol. 178, p. 107313, 2020, doi: 10.1016/j.comnet.2020.107313.

[45] Aruchamy Rajini, Dr. (Mrs) Vasantha Kalayani David,"Constructing Models or MicroArray Data with Swarm Algorithms", International Journal of Computer Science and Information Security, Vol 8 No.9, Dec 2010,(pp.237-242).