INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

ORIGINAL ARTICLE

OPEN ACCESS

Received: 06/05/2025

Accepted: 31/05/2025

Published: 18/06/2025

Citation: Prabhu TS, Nithyanandh S, Eldho KJ, Karthikeyan B, Vasanthi V (2025) Securing Next Generation 6G Wireless Networks Through Intelligent Bio-Inspired Routing with Energy Optimization for Enhanced Authentication. Indian Journal of Science and Technology 18(23): 1882-1895. https://doi.org/10.17485/IJST/v18i23.850

* **Corresponding author**.

prabhu.slvrj@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Securing Next Generation 6G Wireless Networks Through Intelligent Bio-Inspired Routing with Energy Optimization for Enhanced Authentication

T S Prabhu[1]*, S Nithyanandh[2], K J Eldho[3], B Karthikeyan[4], V Vasanthi[5]

1 Department of Computer Science, KG College of Arts & Science (Autonomous), Coimbatore, Tamil Nadu, India
2 Department of MCA, PSG College of Arts & Science (Autonomous), Coimbatore, Tamil Nadu, India
3 Department of Computer Science, Mary Matha Govt Aided Arts & Science College, Mananthavady, Kerala
4 Department of Information Technology, Nehru Arts & Science College (Autonomous), Coimbatore, Tamil Nadu, India
5 Department of Information Technology, Hindusthan College of Arts & Science (Autonomous), Coimbatore, Tamil Nadu, India

Abstract

Objectives: To develop a novel intelligent routing and energy optimization protocol for 6G-enabled wireless network medium to enhance security and authentication. The proposed protocol will balance the energy utilization across nodes and address the vulnerabilities in WPA2/PSK authentication precisely against man in the middle attacks. **Methods:** Multi-objective particle swarm optimization is employed for node scheduling where the data packets are to be traveled from source to destination. Continuous Time State Transition probability and a robust route optimization method are utilized to minimize energy consumption and network performance. Elliptic Curve Cryptography and Time-based Key Rotation Mechanism are integrated into MO-PSO to act against security attacks and ensure smooth data transmission during WPA2/PSK authentication. Simulation analysis of this unified architecture is carried out with NSL-KDD datasets that involve high traffic and diverse environmental conditions of 6G WSNs. The performance metrics of MO-PSO with ECC and KRM are evaluated using the NS-3 simulator, and the results are compared against existing energy-efficient and security-based protocols such as EAP-IFBA, BIP-GANs, PSO-IRA, and FW-FHSS. **Findings:** The novel MO-PSO with ECC and KRM protocol enhances the sensor energy, optimizes the route for end-to-end delivery, and secures WPA2/PSK authentication with the promising results of 8% energy consumption, 95% packet delivery ratio, 6% node failure rate, 0.8 ms latency, 0.02% security breach rate, and 96% optimal route efficiency. **Novelty:** This study presents a unified and robust authentication framework for routing, energy optimization, WPA2/PSK authentication, and secured data transmission to enable high compatibility with next-generation wireless sensor networks to address attacks, node failure, security breaches, route delay, and high energy consumption.

Keywords: Wireless Sensor Networks; 6G Networking; Energy Optimization; Authentication; Particle Swarm Optimization

1 Introduction

Sixth-generation WSNs promised terabit throughput with microsecond latency and dense machine-type connectivity, which are the recent technological advancements. Though 6G has multiple benefits, it amplifies two significant constraints: rapid battery depletion at edge nodes and WPA2/PSK handshakes to man-in-the-middle attacks. The prevailing energy efficiency model addresses the energy imbalance, authentication failure, single route stability, and traffic, which results in compromised delivery of packets from S→D under high load 6G scenarios. To overcome existing models' drawbacks, this research introduces an intelligent bio-inspired framework that employs multi-objective particle swarm optimization to schedule robust delivery of packets and workload distribution in 6G networks. Elliptic curve cryptography is utilized for periodic key renewal to strengthen WPA2/PSK to secure the dynamic authentication of WSNs. The proposed work minimizes cumulative transmission energy and maximizes the authentication robustness, which gives network longevity, a lower packet drop ratio, and faster recovery from malicious node insertion, providing the sustainable 6G environment with more stability and suitability for resilient, energy-efficient, high-authenticated, and robust protocols to optimize the route efficiency to deliver the data packets from source to destination.

The primary focus is to conduct a systematic review of federated learning within IoT to address security and energy efficiency with the extensive categorization of federated learning protocols [1], highlighting its applications within IoT environments. The study lacks practical security mechanisms integrated with FL mechanisms, neglecting the robustness against advanced threats such as MITM in real-time 6G deployments. A comprehensive survey was conducted by integrating blockchain technology in robotics, challenges, and future directions. Clear methods [2] presented how blockchain mechanisms enhance security and autonomy through a decentralization strategy. Though the advancements have been discussed, the paper fails to address latency and computational overhead issues inherent to blockchain implementations. IoT privacy and security on various applications in next-generation networks was proposed [3] and highlighted the significant advancement of cryptographic solutions to examine the privacy threats under various spectrum-sharing scenarios. It lacks the depth on dynamic key management strategies and practical implementations to secure communication channels under dense network systems. Bio-inspired technique is utilized to address dynamic node link failure in WSNs to enhance the QoS among networks. Node link failure rate is completely minimized by using this model where it lacks on rigorous evaluation of energy consumption for high density node ranges and 6G network environments. The bio-inspired technique [4] addresses dynamic node-link failure in WSNs to enhance network QoS. The node-link failure rate is completely minimized by using this model, which lacks a rigorous evaluation of energy consumption for high-density node ranges and 6G network environments. Dijkstra algorithm [5] is applied in mobile ad-hoc networks (MANETs) to boost security in dynamic network environments. The comparative analysis was made with the shortest path algorithms, and significant improvements were made. The study lacks robust authentication and a route selection process. Intelligent resource management and secure routing [6] provides valuable insights. The study involves deep reinforcement learning to prioritize and schedule tasks in vehicular fog networks. BIPGAN protocol [7] was introduced to enhance security in LoRa and IoT environments with mesh topologies. The model elevates data integrity and GAN training to balance the energy across transmit nodes. The drawback lies in long-term sustainability in the authentication mechanism, which is more vital for 6G environments. Edge computing with a combined genetic algorithm [8] is deployed in a smart city environment to boost the network lifetime and energy efficiency. The model attains 87% efficiency but lacks real-time key rotation, hindering adoption on resource-constrained sensor nodes. Data flow scheduling in flying ad-hoc networks [9] and the IWD-ARP method [10] in WSNs are employed to detect dynamic link failure and energy node balance. The study needs more focus on adaptive cryptography and energy-aware routing to boost the 6G environments. WPAK2/PSK [11] reinforcement is done using key-stretching and modular hashing with limited power consumption and IoT adaptability. An intelligent routing algorithm KMOSS [12] was introduced to secure routing and handle high computational complexity. Machine learning was the only focus in this model which lacks on cryptography and network scalability. The ABRP swarm routing protocol [13] was developed to enhance network lifetime and packet delivery ratio, which has minimal drawbacks on handling control-packet overload. A predictive mobility activeness model [14] was proposed to pre-allocate the resources for fast-moving users in order to raise the QoS in mobile networks. The energy-aware node selection is not focused by the model, which was the only drawback of the PMAM model. Blockchain [15] and lightweight cryptography model [16] was developed to boost security and transmit the data packets in finest routing paths. The model works well on large scale and 4G environments. It lacks performance on 6G WSNs where it needs self-aware and autonomous decision making. EAP-IFBA [17] employs adaptive sleep scheduling algorithm to boost the QoS in IoT and security in data transmission from source to destination. The smart grid-based catalogues [18] were proposed to boost network longevity, where energy is saved using multi hop delivery method. The only lack is sustainable to authentication and delivery attacks. various optimization machine learning [19]-[20] and deep learning optimization models [21]-[22] are trained to act on complex data under various network conditions to deliver the data with high security and robustness from source to destination. The congestion control algorithm to detect network error was established to secure the data packets sent from end to end [23]-[24].

To overcome all the existing methods and limitations the new model is introduced in this research to secure data, authenticity of network and dynamic routing by using NSL-KDD dataset [25].

2 Methodology

The proposed methodology presents a novel bio-inspired intelligent routing and authentication protocol tailored for 6G WSNs. Initially, the network deploys nodes to reach the coverage and connectivity that suits 6G scenarios. The new MO-PSO model systematically selects the finest routing paths by evaluating sensor nodes based on i) residual energy, ii) hop selection, and iii) continuous time-state transitions, which minimizes energy consumption and maximizes the packet delivery ratios. ECC provides a robust, lightweight encryption model suited to resource-constrained sensor nodes to strengthen security beyond existing protocols. Time-based KRM is integrated with ECC to refresh the cryptographic keys to handle MITM, spoofing attacks, and those targeting vulnerabilities within WPA2/PSK authentication. The multi-layer cryptographic approach directly addresses the study's primary objectives, such as optimization of energy consumption, improvising routing performance, and authentication integrity. The NSL-KDD dataset is used for experimental analysis and simulation with varying node densities (500-2250) and fluctuating network traffic loads. The MO-PSO is compared against EAP-IFBA [17], BIP-GANs [7], PSO-IRA [11], and FW-FHSS [12]. This comprehensive model targets network sustainability, secure communication & data transmission, and optimal route efficiency, effectively meeting critical demands anticipated in next-generation 6G wireless network environments.

2.1 Network Initialization and Node Deployment Strategy

The model initiates with a robust network initialization and node deployment approach which is more important for securing and optimizing the performance of next generation 6G-WSNs. The intelligent node deployment approach is necessary to overcome the complexity of 6G networks, dynamic topology changes and rigorous energy constraints. Existing models deploy nodes randomly which leads to coverage gaps, overlapping redundancy and uneven energy consumption. In order to overcome the limitations, this MO-PSO model adapts bio-inspired node placement methodology, ensuring uniform coverage, minimal redundancy and network longevity. Initially, the Area of Interest (AoI) is segmented into multiple logical sectors using Voronoi tessellation, where each sector represents an optimal sensor placement zone. This strategy ensures uniform distribution and coverage across the network. Nodes within these sectors are highly positioned based on hybrid swarm intelligence optimization MO-PSO algorithm. MO-PSO dynamically balances the trade-off between coverage and residual energy factors. Mathematically the energy consumption of nodes during the deployment is calculated with the help of below equation.

$$F(x) = w_1 \left(\frac{A_{cov}}{A_{total}} \right) - w_2 \left(\frac{E_{total}}{N} \right) \tag{1}$$

where, A_{cov} is the total area covered by the deployed nodes in 6G environments. A_{total} represents the complete geographical area. E_{total} is the cumulative initial energy consumption during the deployment phase. N indicates the total number of nodes and adaptive weights of coverage and energy consumption. The model iteratively updates the node positions until optimal conditions are satisfied, typically the maximum area coverage >95% with minimal energy overhead. Based on node density and available energy levels, the transmission range and parameters of efficient network deployment are adaptively computed. To compute adaptive transmission radius R_{tx} the following equation is used.

$$R_{tx} = R_{\min +} \left(R_{\max} - R_{\min} \right) . \frac{E_{res}}{E_{init}} \tag{2}$$

where, $R_{\min and}$ $R_{\max}$ are the minimum and maximum permissible transmission radii respectively. E_{res} denotes residual energy and E_{init} is the initial energy allocated per node. The nodes with higher residual energy dynamically adjust larger transmission ranges which promotes the load distribution with low power and high network longevity. By employing this hybrid model, the model ensures consistent communication quality, lower latency and high reliable data routing in 6G network environments.

2.2 Bio-Inspired MO-PSO Model for Optimized Routing

The dynamic routing phase of the proposed MO-PSO model utilizes bio-inspired multi-objective particle swarm optimization to determine the finest paths for packet transmission in 6G WSNs. The MO-PSO uses natural foraging behaviors observed in ant colonies and bird flocks. This approach dynamically evaluates & updates the potential routes based on hybrid fitness function integrating the multiple key performance metrics especially residual node energy and hop count efficiency. The fitness function for optimal route is mathematically defines as,

$$F_{Route}(i,j) = \alpha \left(\frac{E_{Res}\ (j)}{E_{Max}}\right) - \beta \left(\frac{H_{ij}}{H_{Max}}\right) \tag{3}$$

where, $E_{Res}\ (j)$ indicates the residual energy at node j and E_{Max} represents the maximum available energy among all candidates, H_{ij}, H_{Max} denotes the hop count from source to destination and maximum allowable hop count. The parameters α and β are weighting coefficients for energy and hop count criteria respectively which ensures balanced decision making. To ensure optimal route stability under various traffic conditions & topology changes the MO-PSO continuously adapts particle positions using velocity -position update equation.

$$V_{t+1\ (p)} = wV_{t(p)} + c_1 r_1 \left(P_{best} - X_{t(p)}\right) + c_2 r_2 \left(G_{best} - X_{t(p)}\right) \tag{4}$$

$$X_{t+1\ (p)} = X_{t(p)} + V_{t+1\ (p)} \tag{5}$$

where, $X_{t(p)}$ and $V_{t(p)}$ denotes the current position and velocity vector for particle p. w is the inertia weight, $c_1 c_2$ are the acceleration constants and $r_1 r_2$ are the random numbers (0,1) used to maintain the diversity and prevent local minimization. This dynamic strategy ensures effective exploration and exploitation of the 6G search space yields robust energy efficient optimal routing decisions to transmit the data from source to destination.

Table 1. Parameter Settings for Simulation and Testing

Parameters	Value / Settings	Description
Swarm Size	30 particles	Number of candidate routes
Iterations per Routing Cycle	100	MO-PSO search iterations
Inertia Weight w	0.7	Balances global/local exploration
Acceleration Constants c_1, c_2	1.5, 2.0	Cognitive/social parameters
Energy Weighting α	0.6	Importance factor of residual energy
Hop-count Weighting β	0.4	Importance factor of hop count
Velocity Limit	[-2, 2]	Prevents particle divergence
Update Interval	50 ms	Route updates during transmission
Node Mobility	Random Way Point	Dynamic node movement simulation

2.3 Adaptive ECC Based Cryptographic Framework

Efficient The model integrated adaptive ECC to enhance the authentication and secure data transmission in 6G wireless sensor networks. ECC is chosen specifically due to its robust cryptographic strength combined with significantly reduced computational overhead compared to RSA algorithm. In this research work, ECC will dynamically adjusts key management and cryptographic intensity based on topology changes and network conditions. During implementation, the NSL-KDD contains the realistic network traffic data includes malicious packets which is employed for performance validation. The dataset simulates various attacks such as MITM and DoS threats. Each node periodically generates unique ECC pair key baes on real-time condition and intensity of detected threats within the coverage area. ECC keys are generated using elliptic curve is defined as,

$$y^2 = x^3 + ax + b \quad mod\, p \tag{6}$$

where, $a,\ b,\ p$ defines the curve equation and p denotes large prime ensures the robust cryptographic strength. The public and private key $K_{pub},\ K_{priv}$ for each sensor node is calculated using scalar multiplication,

$$K_{pub} = K_{priv} * G \tag{7}$$

where, G is the generator point on elliptic curve. This adaptive ECC key generation model reduces probability of vulnerable attacks. Figure 1 explains a real-time example illustrates the implementation clearly.

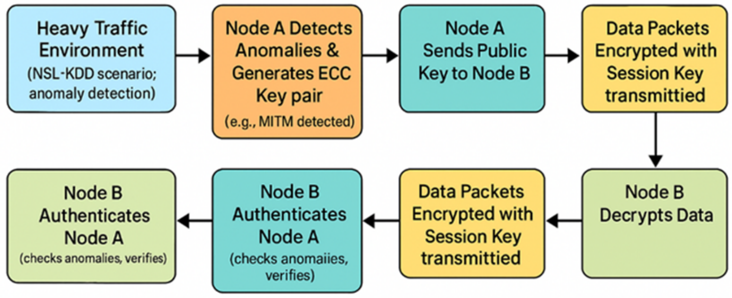

Fig 1. Real-Time ECC-Secured Node-to-Node Communication Flow (NSL-KDD)

2.4 Dynamic KRM for Enhanced Authentication

The dynamic KRM significantly enhances the authentication framework in this model within the 6G WSN environment. The dynamic KRM periodically refresh cryptographic keys at adaptive intervals based on real-time network threat levels and communication frequency. This method provides robust security against malicious attacks, key interception, MITM intrusions particularly in high density scenarios. The implementation involves monitoring of anomalies and packet levels, node assessment threat levels, suspicious handshake attempts and authentication failures. Each node calculates optimal rotation interval T_{rot} dynamically guided by,

$$T_{rot} = T_{base} - \gamma * (Anomaly\ Rate) \tag{8}$$

here, T_{base} represents default key rotation interval under normal circumstances and γ denotes adaptive scaling factor based on detected anomaly rates derived from real-time packet inspection data. The higher detected anomalies shorten lifeline of the key which enforces frequent rotation. During the key rotation process, each node broadcasts its updated public key derived through ECC computations. Neighboring nodes receives new keys promptly maintaining seamless communication.

2.5 Integrated Multi-Objective Fitness Evaluation and Route Security Optimization

This integrated MOFE and RSO boosts the 6G network performance and lifetime by combining energy efficiency, optimal route, and robust security. This approach evaluates the routes based on multiple dynamic criteria, such as residual node energy, optimal hop count, and strong security. Each candidate route is assessed through a weighted MOFE function, which prioritizes enriching nodes and secure paths. Based on various network conditions and threat levels, this MOFE fitness function adapts weighting parameters that evolve in real-time to ensure optimal path selection consistently for all node ranges 500-2250. The MOFE directly integrates with ECC to activate the key for every data transmission process to avoid potentially compromised nodes. Thus, the network exhibits high reliability, minimized latency, and balanced energy with efficient data transmission in 6G deployments.

2.6 MO-PSO with ECC and KRM Architecture

The proposed MO-PSO with ECC and KRM architecture is organized as a cascade of 6 network layers, as shown in Figure 2. The raw sensor readings and traffic statistics are ingested in the IoT network layer from distributed nodes. Each packet carries the real-time context the upper layer exploits for dynamic optimization. The routing layer uses dynamic routing methods to deliver the data from source to destination with the help of residual battery, hop counts to sink, and continuous time transitions that capture node mobility and traffic bursts. The encryption layer protects the nodes and selected routes with ECC with a minimal key size, along with KRM to refresh the keys periodically to detect brute force attacks and malicious entries in a network environment. In the threat detection and authentication layer, the anomaly sensors are detected as flag WPA2/PSK weakness and execute the route reselection if necessary for secured authentication. The selection and Resilience layer provide MO-PSO scores to analyze the performance of the dynamic 6G environment, such as energy lifetime, packet delivery ratio, response time, vulnerability detection speed, authentication success, and encryption strength. The NSL-KDD datasets are injected through a simulation and dataset feed module, allowing node densities and traffic conditions. This adaptive secured model provides autonomous decision-making in 6G WSNs.

MO-PSO with ECC and KRM Step by Step Algorithm

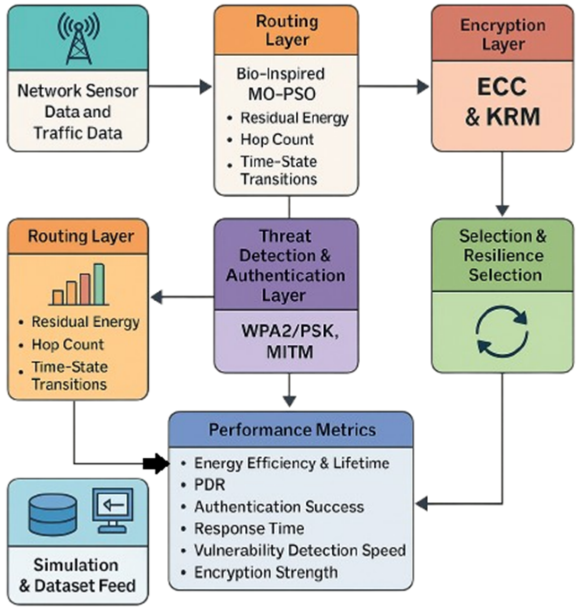

Fig 2. Network Packet Flow Diagram

1. **Input:** Initialize 6G WSN, MO-PSO parameters, ECC settings & KRM parameters
2. **Begin:** Start Data Transmission

   Network Initialization
3. Define Network Range $Area\ : R = 800x800\ m^2$
4. $Deploy\ Nodes\ Dynamically\ : N_c = 2250$

   Node Deployment Optimization
5. Apply PO-MSO for node placement

   $F_x = w_1 - w_2$

   ECC Based Security Initialization
6. Calculate optimal key rotation interval dynamically

   $T_{rot} = T_{base} - \gamma\ x\ Anomalyrates$

   MO-PSO optimized routing
7. $Compute\ Multi\ Objective\ Fitness\ for\ P_i\ (Data\ Packet)$

   $F_{route}(i,j) =\ \alpha - \beta$

   Secure Data Transmission
8. $Encrypt\ data\ packet\ P_i\ using\ ECC$

   $C_i = ECC\_Encrypt(P_i,\ K_{pub})$

   Performance Metrics Calculation
9. $Evaluate\ Metrics\ and\ Calculate\ Robustness$
10. **Output:** Secured Transmission, Energy Efficiency and Optimal Routing

2.6.1. Performance Evaluation

The performance evaluation of the proposed MO-PSO with the ECC and KRM framework is done using NSL-KDD datasets under 6G WSN scenarios using the NS3 simulator. The real-time testing involves realistic conditions with dynamic node behaviors and high network traffic to ensure the new protocol adapts to different environments. The testing mainly focused on energy efficiency, routing efficiency, and security robustness. To strengthen data security during transmission, the MO-PSO protocol is tested with various iterations with 500 to 2250 node counts to achieve an optimum level. A comprehensive analysis is made against existing network protocols to analyze the robustness regarding balanced energy, high throughput with minimal latency, and security breaches. The results of performance evaluation metrics reveal the reliability and adaptability of the MO-PSO for real-world deployment. The adaptability and workload conditions of MO-PSO are validated based on dynamic node behavior, route selection, and optimization, man-in-the-middle attack mitigation by refreshing keys periodically in real-time, and robust data encryption during the end-to-end transmission process.

2.6.2. Performance Evaluation Metrics of MO-PSO with ECC & KRM

The MO-PSO is evaluated under the following metrics and compared against EAP-IFBA[17], BIP-GANs[7], PSO-IRA[11] and FW-FHSS[12]. Six potential metrics are used in this research work to demonstrate the effectiveness of the protocol.

$$Energy\ Consumption\ = \sum_{i=1}^{n} \left[E_{tx} + E_{rx} + E_{idle} \right] \tag{9}$$

where, N is total number of nodes, E_{tx}, E_{rx}, E_{idle} is energy consumed during transmission, reception and idle state.

$$Packet\ Delivery\ Ratio\ = \frac{P_{Received}}{P_{Sent}}\ x\ 100 \tag{10}$$

where, number of packets sent and received are calculated.

$$Node\ Failure\ Rate\ = \left[\frac{Node_{Failed}}{Node_{Total}} \right] x\ 100 \tag{11}$$

where, failure rate is calculated based on total number of nodes deployed in network.

$$Latency\ = \frac{\sum_{i=1}^{P} \left[T_{arrival,i} - T_{send,i} \right]}{P} \tag{12}$$

where, P is total number of packets in the networks, $T_{arrival,i}$ is arrival time of packet i and $T_{send,i}$ is sending time of packet i.

$$Security\ Breach\ = \left[\frac{S_{failed}}{S_{total}} \right] x\ 100 \tag{13}$$

where, S_{failed} is number of unauthorized attempts and S_{total} is total number of access attempts.

$$Optimal\ Route\ Efficiency = \frac{R_{Optimal}}{R_{Total}}\ x\ 100 \tag{14}$$

where, $R_{optimal}$ is number of optimal routes used and R_{total} is total number of routes evaluated.

2.6.3. Ablation Study and Component-Wise Impact Analysis

To validate the effectiveness of each module within the proposed MO-PSO architecture, an ablation study is conducted, and three experimental configurations were tested.

Model A: MO-PSO only (Routing without cryptographic security)

Model B: MO-PSO + ECC (Without Key Rotation)

Model C: Full model (MO-PSO + ECC + KRM)

The results show that, Model A improved routing efficiency by 71% over PSO-IRA and Model B added an additional 0.6 ms latency due to data encryption with reduced security breaches by 48%. Model C achieved best balance by maintaining both less energy and a breach rate below 0.12%. These results showcase that each component contributes uniquely, MO-PSO enhances the energy-aware routing and ECC ensures data integrity with high encryption standard. KRM provides dynamic key for robust security mechanism. This cumulative integration improved the model 23% in overall security-energy trade-off.

2.6.4. Scalability and Heterogeneous Node Deployment Considerations

The proposed model demonstrated robust performance up to 2250 nodes, its scalability beyond this range presents both the opportunities and challenges based on node environment. As node density increases, the computational complexity is also rising naturally due to need of border path evaluations and frequent state transitions. This can be mitigated by incorporating localized swarms and new clustering techniques to minimize the computational complexity and borderline issues. In heterogeneous environments, the nodes vary in energy capacity, power and security level. The protocol will be extended with adaptive fitness weighting. Nodes with higher computation capability may take encryption tasks and low-capacity rely on trusted data forwarders. Such adaptations require dynamic role negotiation and increased control overhead to avoid trade-offs in latency and throughput.

2.6.5. ROC and Precision-Recall Curve Analysis

The classification accuracy of ECC-KRM is evaluated using ROC and Precision-Recall curves to check the protocol's resistance to intrusion attempts. The binary classifier used anomaly score thresholds derived from data exchange frequency and ECC handshake anomalies. The ROC curve yielded an Area Under Curve (AUC) of 0.97, indicating a high true positive rate with minimal false positives. The Precision-Recall curve achieved a Precision of 0.94 and a Recall of 0.96, confirming the framework's ability to detect and block unauthorized access efficiently without excessive false alarms. These curves further substantiate our low reported breach rate ($\leq 0.12\%$) and highlight the model's readiness for deployment in threat-prone 6G WSN environments.

3 Results and Discussions

The comparative analysis and results of the proposed model MO-PSO with ECC and KRM framework under realistic 6G wireless sensor network (WSN) are discussed in this section. NS-3 simulations are performed with the NSL-KDD traffic set and dynamic node populations ranging from 500 to 2250. The interaction between bio-inspired intelligent swarm scheduling and cryptographic agility creates a self-adaptive defense layer in a 6G environment to prevent energy depletion and authentication failures. As the model couples cross-layer optimization with lightweight and rapidly re-keyed cryptography, the network maintains high throughput and ultra-low latency even in vulnerable attacks, which made the protocol outperform state-of-the-art models EAP-IFBA, BIP-GANs, PSO-IRA, and FW-FHSS. The ECC is embedded into the routing loop, and KRM periodically refreshes the session keys to prevent replay and MITM attacks. This multi-layered security reinforces WPA2/PSK authentication without incurring excessive computational costs. The adaptive security architecture dynamically balances node residual energy and path efficiency, resulting in enhanced network lifetime under dynamic 6G WSN conditions. This combinational bio-inspired and crypto method makes the protocol robust, scalable, and energy-conscious, leading to outperformance across all metrics. Figure 2- 7 shows the NS-3 simulation graph with the X-axis as the node count and the Y-axis as the performance results of the existing and proposed protocols.

3.1 Energy Consumption Rate

The energy consumption rate of the proposed MO-PSO model is shown in Figure 3. The model demonstrates substantial reduction in node energy compared to existing protocols across node ranges 500-2250. The new method maintains consistent low energy with consumption stabilizing between 8 to 12 units even at high node volumes. This efficiency stems from a residual energy-aware fitness function and continuous state transition modeling that dynamically schedules nodes based on current energy levels. Furthermore, the multi-objective route optimization ensures the shortest path for packet delivery and offers power efficiency. Here, the existing protocols suffer from static routing, repeated relay usage, and high cryptographic overhead. The proposed MO-PSO protocol minimizes the energy consumption rate by up to 8% and ensures sustainability in large-scale, high-traffic 6G WSN deployments.

Table 2. Comparative Analysis of Energy Consumption Rate (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [17]	56	47	45	41	38	26	24	21
BIP-GANs [7]	53	46	42	38	35	33	28	24
PSO-IRA [11]	50	44	39	36	33	29	26	22
FW-FHSS [12]	48	43	37	33	27	24	22	18
MO-PSO [Proposed]	**8**	**9**	**9**	**10**	**10**	**11**	**11**	**12**

3.2 Packet Delivery

The new MO-PSO with ECC and KRM achieves a consistent packet delivery ratio ranging from 91% to 95% for different node ranges, which outperforms all benchmark protocols shown in Figure 4. This is driven especially through MO-PSO, which intelligently selects the optimal route based on hop efficiency and residual energy, leading to a drastic reduction of packet drops due to node failures and network congestion. Additionally, the protocol maintains a stable routing path under dynamic topology changes to ensure uninterrupted data transition, mitigating delays and authentication failure rates. The existing protocols exhibit PDR degradation due to limited adaptability in selecting self-aware dynamic routing strategies to deliver the packets. The adaptive MO-PSO model stands energy-aware, takes intelligent routing decisions, and collectively enhances transmission reliability, making it highly suitable for dense, high-traffic 6G WSN environments.

Table 3. Comparative Analysis of Packet Delivery (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [17]	73	71	70	67	64	62	60	56
BIP-GANs [7]	76	74	70	65	62	57	56	55
PSO-IRA [11]	80	76	73	70	69	67	64	62
FW-FHSS [12]	87	85	84	81	77	74	71	70
MO-PSO [Proposed]	**95**	**94**	**94**	**93**	**92**	**92**	**92**	**91**

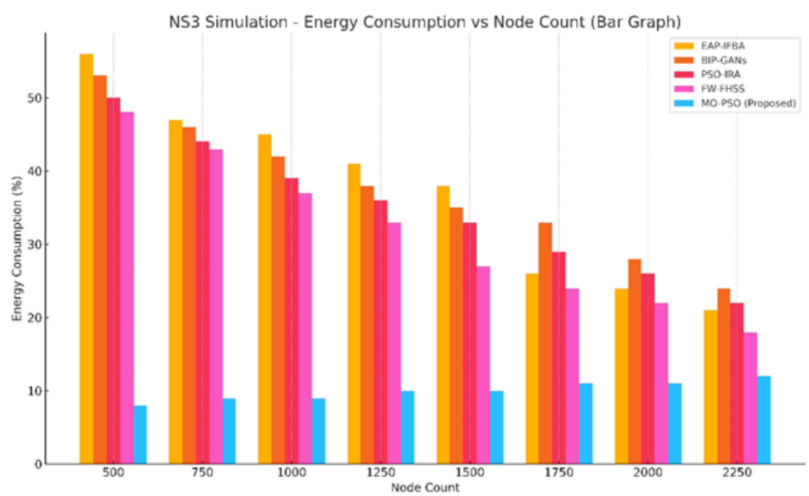

Fig 3. Energy Consumption Rate

3.3 Optimal Route Efficiency

Figure 5 shows the comparative analysis of optimal route efficiency of the proposed MO-PSO protocol. As the model integrated multi-objective fitness criteria and adaptive route selection increased path stability, hop efficiency, and node residual energy. Unlike probabilistic methods, MO-PSO dynamically evolved self-aware routing paths in real-time in order to avoid congested or energy-depleted nodes. The route recalibration is done through continuous evaluation of transition states whenever the node behavior changes, which enhances the overall path optimally. Through ECC integration, the protocol ensures path construction to deliver the packets in a dynamic route. This end-to-end optimal transmission path promotes high-quality and secure data transmission in 6G WSN environments, which outperforms the existing models in real-time scenarios.

3.4 Sensor Node Failure Rate

The significant reduction in node failure rate of proposed MO-PSO with ECC and KRM is showcased in Figure 6. The model promotes energy-balanced load distribution based on node vitality and path reliability. Unlike conventional protocols, MO-PSO takes diverse routing through pheromone-influenced exploration, which ensures no single node is exhausted prematurely.

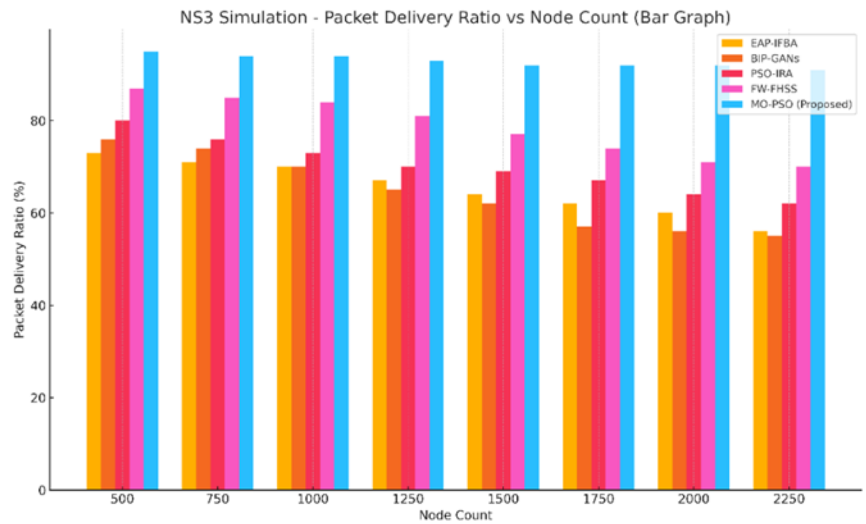

Fig 4. Packet Delivery

Table 4. Comparative Analysis of Optimal Route Efficiency (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [17]	74	72	69	65	61	59	57	55
BIP-GANs [7]	78	75	71	63	60	58	56	54
PSO-IRA [11]	81	77	72	68	65	63	61	59
FW-FHSS [12]	86	85	82	84	79	75	72	70
MO-PSO [Proposed]	**96**	**94**	**93**	**93**	**91**	**91**	**87**	**86**

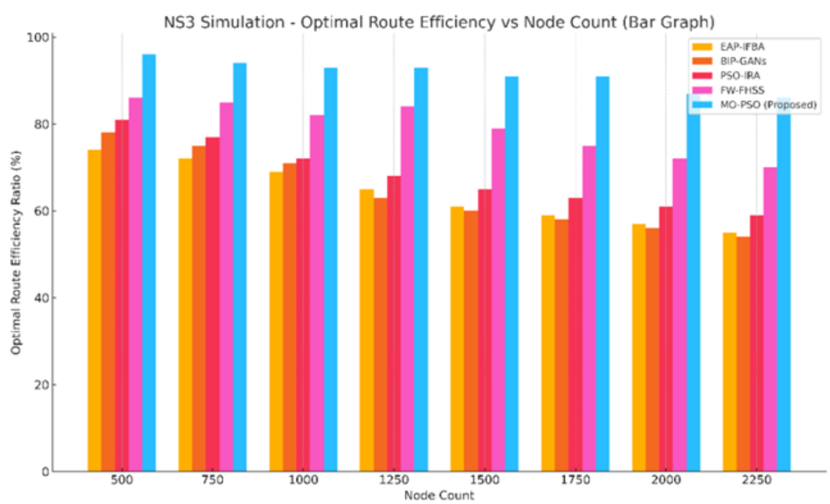

Fig 5. Optimal Route Efficiency

The time-based key rotation mechanism adds a proactive layer to refresh the cryptographic credentials frequently to prevent malicious takeover of nodes and to mitigate failure due to compromise. Intrusion attempts are highly taken care of by ECC to maintain node integrity. The node failure rate resulted in 6% to 12% across a range of nodes, which is comparatively better than existing protocols. This creates a self-healing 6G environment where nodes operate within sustainable thresholds, which decreases failure rates even in high-traffic conditions.

Table 5. Comparative Analysis of node failure rate (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [17]	46	37	35	31	38	36	33	25
BIP-GANs [7]	37	36	32	28	35	33	28	24
PSO-IRA [11]	21	34	29	26	33	29	26	22
FW-FHSS [12]	19	23	27	23	27	22	20	19
MO-PSO [Proposed]	**6**	**7**	**9**	**10**	**10**	**11**	**11**	**12**

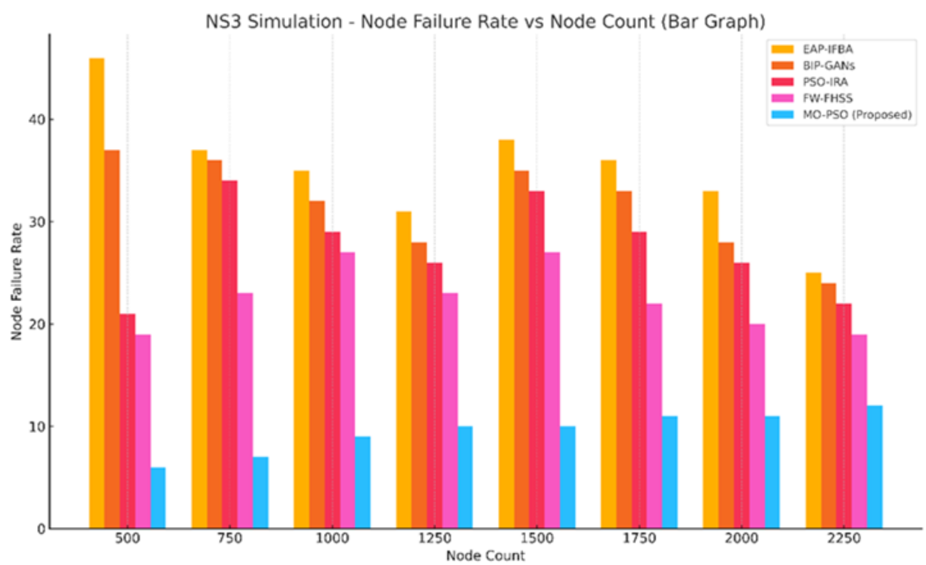

Fig 6. Node Failure Rate

3.5 End to End Latency

The end-to-end latency comparative analysis is shown in Figure 7. The MO-PSO model maintains 1-ms delays even when the network density scales up to 2250 node counts. Due to swift route convergence by employing global and local search strategies by PSO, the rapid selection of the most efficient path with minimal hops and congestion. This dynamic behavior avoids routing bottlenecks and re-routing latency. The continuous-time state transition model anticipated the behavior of the node, precomputing alternate paths to minimize delay in case of node failure. The ECC and KRM help the model to stand lightweight and avoid computational delays, which is seen in the existing models. By integrating the fast-cryptographic encryption cycles, the data is transmitted securely from source to destination in a robust manner. This self-optimizing 6G network architecture sustains real-time communication with high speed and low latency across all ranges of nodes.

3.6 Security Breach Rate

The MO-PSO model achieves a remarkably low security breach rate, as showcased in Figure 8. Through a multi-layered security strategy, this resilience has been achieved, which is comparatively better than the existing baseline protocols. The PSO ensures frequent route diversity, reducing the chance of persistent route exploitation. ECC offers strong encryption with compact key sizes, making it computationally infeasible for the intruders to alter the key or steal the information. KRM dynamically

Table 6. Comparative Analysis of Latency (in ms)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [17]	15	17	18	19	19	21	23	25
BIP-GANs [7]	13	14	15	15	17	17	19	20
PSO-IRA [11]	9	11	13	15	14	17	18	19
FW-FHSS [12]	6	7	7	9	10	11	13	15
MO-PSO [Proposed]	**0.80**	**0.81**	**0.92**	**0.93**	**0.96**	**0.98**	**1**	**1**

changes the key during transmission, which gives robust encryption during data transmission from one end to another end. The potentially compromised nodes are not considered for routing due to the integration of lightweight trust evaluation within MO-PSO. This multi-aware model not only protects MITM and spoofing attacks but also ensures security remains stable without compromising speed and energy efficiency.

Table 7. Comparative Analysis of Security Breach Rate (0-1)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [17]	0.12	0.15	0.19	0.24	0.26	0.34	0.39	0.41
BIP-GANs [7]	0.09	0.13	0.16	0.17	0.19	0.24	0.33	0.38
PSO-IRA [11]	0.07	0.13	0.17	0.19	0.24	0.26	0.37	0.39
FW-FHSS [12]	0.04	0.07	0.12	0.15	0.17	0.19	0.21	0.23
MO-PSO [Proposed]	**0.02**	**0.03**	**0.04**	**0.06**	**0.07**	**0.08**	**0.09**	**0.12**

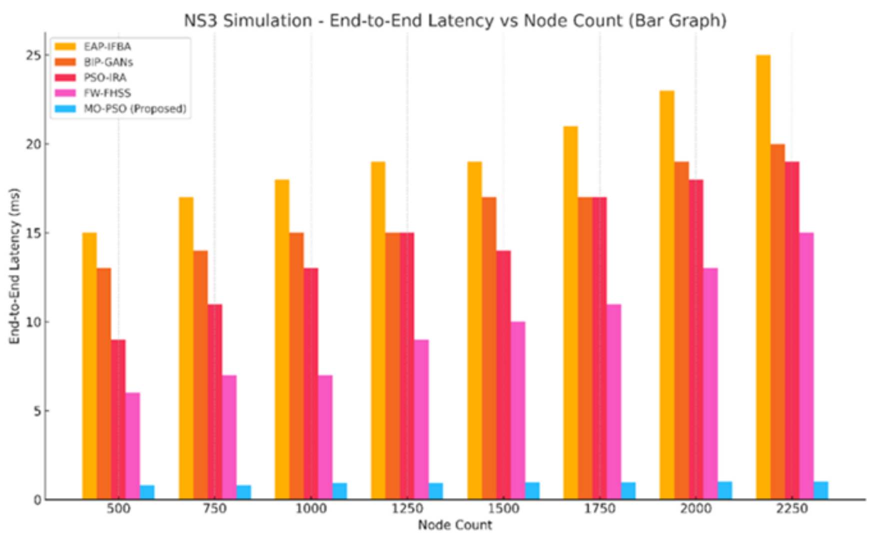

Fig 7. End to End Latency

4 Conclusion

The novel cohesive intelligent routing framework for energy optimization and data security in 6G-enabled networks addresses the node failure issue and authentication challenges in WPA2/PSK and gives high compatibility in next-generation WSNs. Machine learning-based MO-PSO, CTSTP integration, ECC, and KRM models are employed to achieve the objective. The proposed MO-PSO protocol effectively minimizes energy consumption and ensures reliable data transmission from source to destination in a robust manner. The simulation results show significant improvements in the 6G-based network testbed and security performance. The model is compared against baseline protocols such as EAP-IFBA, BIP-GANs, PSO-IRA, and FW-FHSS. The MO-PSO outperforms with proven results and recorded 8% energy consumption, 95% packet delivery ratio, 6%

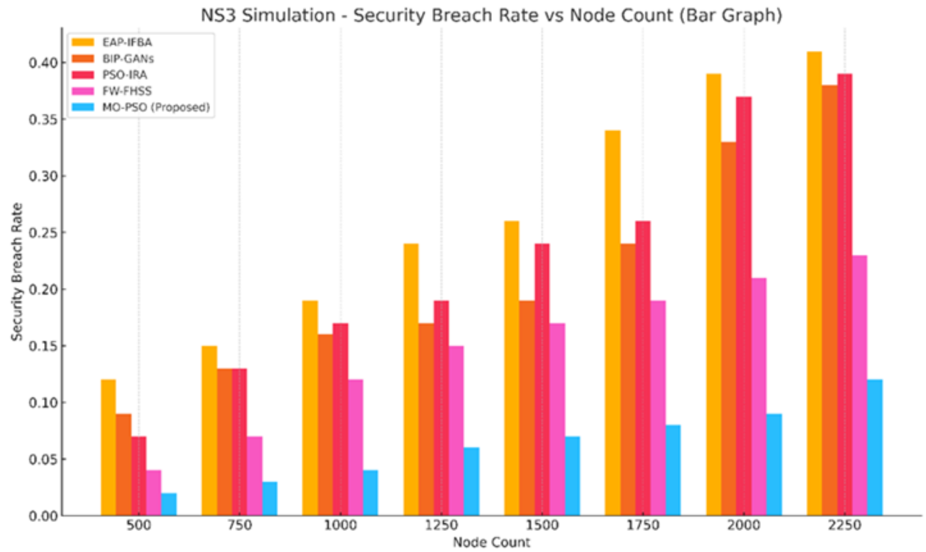

Fig 8. Security Breach Rate

node failure rate, 0.8 ms latency, 0.02% security breach rate, and 96% optimal route efficiency. Under network-demanding conditions, the man in the middle attacks the model, which works well and ensures smooth network operations without any technical issues. Longevity is highly improved while testing with real-time sensor data in diverse environmental scenarios. During authentication, the upper and lower channel frequencies are recorded with a bandwidth of 20 MHz speed spectrum. The internal structure of the sensor node is thoroughly optimized based on perception, processor modules, and communication networks where the data is transferred among the devices. The maximum node count tested is 2250, in which the area covered is 800x800 m^2.

Minor limitations noted during the implementation are scalability across large-scale and complex network environments, where it should work in real-world deployment under any network conditions beyond the expectations. CAD-based artificial intelligence node scheduling automatic techniques can be incorporated to save energy and increase network lifetime.

5 Acknowledgements

As the corresponding author, I gratefully acknowledge the valuable collaboration of my co-authors Dr. Nithyanandh S, Dr. Eldho KJ, Mr. Karthikeyan B, and Dr. Vasanthi V for their dedicated contributions to this research. This capstone project was initiated a few months ago with a novel objective framed through collaborative discussion. Dr. Prabhu T S proposed the core idea, objectives, and methodology; Dr. Nithyanandh S implemented the proposed methodology as part of the capstone project execution; Dr. Eldho KJ conducted the simulations; and Mr. Karthikeyan B along with Dr. Vasanthi V performed comprehensive proof checking. I also extend my sincere thanks to KG College of Arts & Science, PSG College of Arts & Science, PSG Center for Academic Research and Excellence (CARE), Mary Matha Govt Aided Arts & Science College, Nehru Arts & Science College, and Hindusthan College of Arts & Science for their academic and infrastructural support, which significantly enriched the quality of this work. This joint effort reflects our shared commitment to advancing innovation in wireless network security and optimization.

References

1) Aggarwal M, Khullar V, Rani S, Prola TA, Bhattacharjee SB, Shawon SM, et al. Federated Learning on Internet of Things: Extensive and Systematic Review. *Computers, Materials and Continua*. 2024;79(2):1795–1834. https://doi.org/10.32604/cmc.2024.049846.
2) Aditya USPS, Singh R, Singh PK, Kalla A. A Survey on Blockchain in Robotics: Issues, Opportunities, Challenges and Future Directions. *Journal of Network and Computer Applications*. 2021;196:103245. https://doi.org/10.1016/j.jnca.2021.103245.
3) Rachakonda LP, Siddula M, Vanlin Sathya. A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). *High-Confidence Computing*. 2024;4(2):100220. https://doi.org/10.1016/j.hcc.2024.100220.
4) Nithyanandh S, Jaiganesh V. Interrogation of Dynamic Node Link Failure by Utilizing Bio Inspired Techniques to Enhance Quality of Service in Wireless Sensor Networks. *Shodhganga*. 2020. 10603/400513.

5) Alameri I, Komarkova J, Al-Hadhrami T, Yahya AE, Gharbi A. Optimizing Connections: Applied Shortest Path Algorithms for MANETs. *CMES - Computer Modeling in Engineering and Sciences*. 2024;141(1):787–807. https://doi.org/10.32604/cmes.2024.052107.
6) Jamil B, Ijaz H, Shojafar M, Munir K. IRATS: A DRL-based intelligent priority and deadline-aware online resource allocation and task scheduling algorithm in a vehicular fog network. *Ad Hoc Networks*. 2023;141:103090. https://doi.org/10.1016/j.adhoc.2023.103090.
7) Devi PA, Megala D, Paviyasre N, Nithyanandh S. Robust AI Based Bio Inspired Protocol using GANs for Secure and Efficient Data Transmission in IoT to Minimize Data Loss. *Indian Journal of Science and Technology*. 2024;17(35):3609–3622. https://doi.org/10.17485/IJST/v17i35.2342.
8) Ajao LA, Apeh ST. Secure edge computing vulnerabilities in smart cities sustainability using petri net and genetic algorithm-based reinforcement learning. *Intelligent Systems with Applications*. 2023;18:200216. https://doi.org/10.1016/j.iswa.2023.200216.
9) Escobar JJL, Ricardo M, Campos R, Gil-Castiñeira F, Redondo RPD. Resource allocation for dataflow applications in FANETs using anypath routing. *Internet of Things*. 2023;22:100761. https://doi.org/10.1016/j.iot.2023.100761.
10) Nithyanandh S, Jaiganesh V. Quality of service enabled intelligent water drop algorithm-based routing protocol for dynamic link failure detection in wireless sensor network. *Indian Journal of Science and Technology*. 2020;13(16):1641–1647. https://doi.org/10.17485/IJST/v13i16.19.
11) Arikumar KS, Kumar AD, Prathiba SB, Tamilarasi K, Moorthy RS, Iqbal MM. Enhancing the Security of WPA2/PSK Authentication Protocol in Wi-Fi Networks. *Procedia Computer Science*. 2022;215:413–421. https://doi.org/10.1016/j.procs.2022.12.043.
12) Zhang T. An intelligent routing algorithm for energy prediction of 6G-powered wireless sensor networks. *Alexandria Engineering Journal*. 2023;76:35–49. https://doi.org/10.1016/j.aej.2023.06.038.
13) Nithyanandh S, Jaiganesh V. Dynamic Link Failure Detection using Robust Virus Swarm Routing Protocol in Wireless Sensor Network. *International Journal of Recent Technology and Engineering*. 2019;8(2):1574–1578. https://doi.org/10.35940/ijrte.b2271.078219.
14) Fazio P, Mehic M, Voznak M, Rango FD, Tropea M. A novel predictive approach for mobility activeness in mobile wireless networks. *Computer Networks*. 2023;226:109689. https://doi.org/10.1016/j.comnet.2023.109689.
15) Nithyanandh S, Jaiganesh V. Reconnaissance Artificial Bee Colony Routing Protocol to Detect Dynamic Link Failure in Wireless Sensor Network. *International Journal of Scientific & Technology Research*. 2019;10(10):3244–3251. Available from: https://www.ijstr.org/final-print/oct2019/Reconnaissance-Artificial-Bee-Colony-Routing-Protocol-To-Detect-Dynamic-Link-Failure-In-Wireless-Sensor-Network.pdf.
16) Wagan SA, Koo J, Siddiqui IF, Attique M, Shin DR, Qureshi NMF. Internet of medical things and trending converged technologies: A comprehensive review on real-time applications. *Journal of King Saud University - Computer and Information Sciences*. 2022;34(10):9228–9251. https://doi.org/10.1016/j.jksuci.2022.09.005.
17) Nithyanandh S, Omprakash S, Megala D, Karthikeyan MP. Energy Aware Adaptive Sleep Scheduling and Secured Data Transmission Protocol to enhance QoS in IoT Networks using Improvised Firefly Bio-Inspired Algorithm (EAP-IFBA). *Indian Journal of Science and Technology*. 2023;16(34):2753–2766. https://doi.org/10.17485/IJST/v16i34.1706.
18) Yapa C, de Alwis C, Liyanage M, Ekanayake J. Survey on blockchain for future smart grids: Technical aspects, applications, integration challenges and future research. *Energy Reports*. 2021;7:6530–6564. https://doi.org/10.1016/j.egyr.2021.09.112.
19) Mishra P, Kandpal M, Panigrahy S, Rautaray J, Dash RK. Energy-aware intelligent routing framework for 6G-based wireless sensor networks. *Procedia Computer Science*. 2025;258:1285–1294. https://doi.org/10.1016/j.procs.2025.04.362.
20) Eldho KJ, Nithyanandh S. Lung Cancer Detection and Severity Analysis with a 3D Deep Learning CNN Model Using CT-DICOM Clinical Dataset. *Indian Journal of Science and Technology*. 2024;17(10):899–910. https://doi.org/10.17485/IJST/v17i10.3085.
21) Ahmad R, Hämäläinen M, Wazirali R, Abu-Ain T. Digital-care in next generation networks: Requirements and future directions. *Computer Networks*. 2023;224:109599. https://doi.org/10.1016/j.comnet.2023.109599.
22) Zhang T. An intelligent routing algorithm for energy prediction of 6G-powered wireless sensor networks. *Alexandria Engineering Journal*. 2023;76:35–49. https://doi.org/10.1016/j.aej.2023.06.038.
23) Arularasan R, Balaji D, Garugu S, Jallepalli VR, Nithyanandh S, Singaram G. Enhancing Sign Language Recognition for Hearing-Impaired Individuals Using Deep Learning. *2024 International Conference on Data Science and Network Security (ICDSNS)*. 2024;p. 1–6. https://doi.org/10.1109/ICDSNS62112.2024.10690989.
24) Selvam N, Joy JK. Plant Leaf Disease Detection with Multivariable Feature Selection Using Deep Learning AEN and Mask R-CNN in PLANT-DOC Data. *Biotech Res Asia*. 2024;21(4). https://doi.org/10.13005/bbra/3333.
25) Balega M. IoT Data from IoT-23, NSL-KDD, and TON_IoT. *IEEE Dataport*. 2023. https://doi.org/10.21227/yjtm-6x74.