INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Energy Aware Adaptive Sleep Scheduling and Secured Data Transmission Protocol to enhance QoS in IoT Networks using Improvised Firefly Bio-Inspired Algorithm (EAP-IFBA)

S Nithyanandh[1]*, S Omprakash[2], D Megala[3], M P Karthikeyan[4]

1 Assistant Professor & HOD, PG Department of Computer Science, Sankara College of Science and Commerce, Coimbatore, Tamil Nadu, India
2 Assistant Professor, Department of Computer Science, KG College of Arts and Science, Coimbatore, Tamil Nadu, India
3 Assistant Professor, Department of Information System Management, Gurunanak College, Chennai, Tamil Nadu, India
4 Assistant Professor, School of CS & IT, Jain Deemed to be University, Bengaluru, Karnataka, India

OPEN ACCESS

Received: 09-07-2023

Accepted: 01-08-2023

Published: 15-09-2023

Citation: Nithyanandh S, Omprakash S, Megala D, Karthikeyan MP (2023) 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 16(34): 2753-2766. https://doi.org/10.17485/IJST/v16i34.1706

* **Corresponding author**.

nknithu@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To propose a suitable bio-inspired algorithm for energy-aware adaptive sleep scheduling and secured data transmission in IoT networks. Machine learning with bio-inspired technique is employed to schedule sleep periods for sensor nodes to maximize the lifetime of the IoT network, minimize energy consumption, and ensure robust data security during attacks. **Methods:** Improvised Firefly Bio-Inspired Algorithm (IFBA) is employed for adaptive sleep scheduling, and Dynamic Key Distribution Management (DKDM) with the elliptic curve method is used for secured and reliable data transmission between sensor nodes. Enhanced Recurrent Neural Networks (ERNN) with the N-Key method is deployed to identify the abnormal patterns associated with attacks and topology changes. Mean Square Error Data Recovery (MSEDR) is utilized to evaluate the error in data recovery, and Q-Learning Technique (QLT) with action sets is used to identify the finest path to ensure fast transmission of data. OMNETC++ simulator software is used to evaluate the performance of the proposed EAP-IFBA IoT network protocol with baseline protocols such as IWD-ARP, ECC-ILEACH, and RLSSA-CDGP. **Findings:** The proposed EAP-IBFA sleep scheduling and secured data transmission algorithm outperforms the prevailing methods IWD-ARP, ECC-ILEACH, and RLSSA-CDGP with an energy depletion rate of 8%, 97.5% alive nodes, 98% network life span in an IoT environment, 97.6% data transmission speed, 98% quick sleep scheduling, and 96.5% robustness to attacks. **Novelty:** The comprehensive solution of EAP-IFBA enhances QoS in IoT sensor networks. The proven results show that the proposed novel sleep scheduling and secured data transmission algorithm has the ability to address the challenges of prevailing methods IWD-ARP, ECC-ILEACH, and RLSSA-CDGP in terms of energy consumption, data security, and dynamic sensing of topology changes for efficient and reliable IoT deployments.

Keywords: Energy Efficiency; IoT Networks; Sleep Scheduling; Secured Data Transmission; Machine Learning; Bio-Inspired Algorithm; Quality of Service

1 Introduction

The rapid growth of the Internet of Things (IoT) has ushered in a multitude of smart devices, resulting in massive data generation and communication requirements. Efficient energy management, reliable data transmission, and enhanced Quality of Service (QoS) are critical considerations for IoT networks. To address these challenges, researchers have made significant advancements in developing sleep scheduling and data transmission protocols. However, existing protocols often fall short in achieving optimal energy consumption, ensuring secure data transmission, and maintaining QoS standards. One major gap lies in the lack of effective adaptation to dynamic network topologies and changing energy requirements. Additionally, ensuring robust security measures to protect sensitive IoT data remains a significant concern. To overcome the research gap, this research paper proposes an innovative approach called Energy Aware Adaptive Sleep Scheduling and Secured Data Transmission Protocol using the Improvised Firefly Bio-Inspired Algorithm (EAP-IFBA). By leveraging the bio-inspired behavior of fireflies and incorporating energy-awareness and security measures, EAP-IFBA aims to optimize energy consumption, enhance data transmission efficiency, and ensure QoS in IoT networks. EAP-IFBA addresses the limitations of existing models and provides a comprehensive solution for energy efficiency, secure communication, and improved QoS in IoT networks.

To optimize the energy, speedup the data transmission using finest route various protocols were identified by employing ML and DL methods. QoS enabled cluster based routing protocol[(1)] was introduced to enhance the lifetime of networks in hierarchal networking structures. It acts as a load balancing method where it transmits data from $S \rightarrow D$ by compressing data into an archive model and extracting the same at the destination. The network traffic is controlled by the QoS-CBR protocol, which helps to reduce node energy. But the shortcomings of QoS-CBR are that the percentage of dead nodes is high when large amounts of data are being transferred in WSNs, which leads to network shutdown or data loss. A detailed review has been made by the authors on IoT for smart home automation and applications[(2)] which give a clear picture of how IoT works on smart applications and how data is being captured, utilized, and monitored in an IoT background in a dynamic way. Also, the deployment of nodes in an IoT environment was portrayed. The authors also discussed the wired and wireless communication mediums and compared the existing protocols used in IoT environments using various performance evaluation metrics. The EESFS scheme[(3)] was introduced to minimize end-to-end delay and maintain QoS in data transmission. The hop-by-Hop security model was utilized for security and reliability. A ML data forwarding scheme is employed to forward the data from node to node in a robust manner without losing the data. The drawback of this EESFS is that data recovery and re-transmission are not possible when there is any corruption during topology changes or some external factors. CDGP-RLSSA[(4)] was introduced to minimize energy expenditure by using the RIL-SS sleep scheduling method. Residual energy of nodes is considered a reward function in CDG to validate the balance energy of sensor nodes that are deployed in an IoT environment. Random SSA is employed to balance the state between active and sleepy nodes. The drawback that is identified with this method is that it will not balance the load and transfer the data with more security. Vulnerability identification is limited in CDG-RLSSA, where the use of protocols in large environments may lead to data loss. ECC-ILEACH[5] method was specifically designed to protect communication between two nodes during the real-time process. The energy efficiency is achieved up to 89%. The shortcomings and limitations are adaptive to IoT, Security, Data forwarding, etc., where the QoS is not up to standards. IWD-ARP[6] was proposed to minimize energy, delay, and traffic and maximize the life span and packet delivery. The water drop method is employed to minimize energy in the nodes. This is one of the robust ML methods where the ECM is achieved at 92% and the life span is enhanced up to 94%. The only drawback of IWD-ARP is that it will not suit wide area and metropolitan networks, where everyone is now using WAN and MAN for data transmission. Optimizing energy, sleep scheduling, and node management schemes were introduced to manage scalable networks and surveillance applications. Data forwarding and RSA techniques are employed for reliable and secured data transmission from $S \rightarrow D$. The shortfalls are effective node deployment, deep sensing, usage of residual energy of sensor nodes, adaptive sleep scheduling, etc., which lead to a minimum lifespan of the IoT network[7–9]. The QoS-enabled MACP protocol[10] was identified to offer a cross-layer communication method in an IoT environment. Here, multi-hop routing is followed, where the cross-layer method looks after packet delivery and prioritizes the request from the base station, and based on the request, the data transmission happens. The node energy is minimized and packet delivery is maximized in the MACP protocol, with limitations such as security, adaptivity, and scalability during real-time data capture and transmission. Secured DT protocol and RVS-RP bio-inspired dynamic link failure monitoring protocol[11,12] weredeveloped to achieve promising results in delay, efficient packet delivery, finest route identification, enhancing lifespan, etc. The virus-based population technique is deployed to detect dynamic link failure in WSN and IoT network space. 93% detection accuracy is attained. The limitations of RVS-RP are that data cannot be recovered if it is corrupted, and re-transmission is not possible by using residual energy. A lightweight encryption model[13] was proposed to transfer the data with more security with the help of a dynamic key generation method. Classical cryptographic methods are employed to overcome the security drawbacks. The Raspberry Pi 3 is used for simulation, and promising results were achieved in terms of secured DT from $S \rightarrow D$. The limitations are that Q-LT and error detection are not achieved in this CCM model. QoS-enabled STM protocol for IoT and trust-based decision-making CSM protocol[14,15] was introduced to enhance the IoT network service in terms of security, data transmission, minimizing end to end delay, robust communication, maximizing LT of network etc. A monotype secured protocol was employed in STM and CSM to work in a specific type of environment to transmit the data from node to node in a dynamic way. The limitations of STM and CSM are that they work for a minimum distance, where the nodes cannot be deployed for more than 1000 m which is not sufficient for large scale networks. Intelligent energy-aware QoS protocol[16] was designed specifically for dynamic mobility and effective use in IoT environments, especially for secured data transmission. The protocol aims to take the edge off potential threats and ensure the integrity and confidentiality of the transmitted data in the IoT space. QoS routing mechanism[17] explores the utilization of trust models to make informed decisions about data routing and node selection. Through extensive experiments and evaluations, the effectiveness and efficiency of the proposed approach are demonstrated. EESRF[18] was introduced for hybrid environments and the results highlight its ability to enhance the overall security and reliability of streaming video in sensor networks, thereby contributing to the advancement of multimedia applications in various domains. The drawbacks are a lack of retransmission and data recovery. IOMT, RAB-CRP, and cluster-Based routing protocols[19–21] are deployed in large-scale networks where nature-inspired concepts are used to minimize delay and maximize the life of nodes. In the IoT environment, the nodes are deployed at a minimum distance for effective communication and successful packet delivery from source to destination. The energy is saved if the nodes are deployed at a distance of 20m in large-scale environments. The study mainly focuses on the utilization of spectral classification to improve the clustering process and enhance network security. A comprehensive evaluation of the proposed approach EEAS, SFTNP, AWFS and SEETA-IoT[22–25] was proposed, considering energy consumption as a key metric. The results demonstrate the effectiveness of the algorithm in achieving secure and energy-efficient WSNs, highlighting its potential for real-world applications with minimal drawbacks. All the existing methods have not shown the impressive results in terms of secured DT, adaptive sleep scheduling, data recovery, data re-transmission, minimizing energy consumption, maximizing lifespan etc. To overcome the drawbacks the energy aware adaptive sleep scheduling bio-inspired protocol (EAP-IFBA) is proposed in this paper to enhance QoS in IoT environment. Some of the unique methods of EAP-IFBA are,

- **Adaptive Sleep Scheduling with Energy Prediction:** The Improvised Firefly Bio-Inspired Algorithm (IFBA) is utilized to dynamically adjust sleep schedules of nodes based on their predicted energy levels.
- **Dynamic Key Management & N-Key Encryption :** Integrate a robust key management scheme using IFBA to dynamically distribute encryption keys among IoT devices.
- **Traffic-Aware Routing and Path Selection :** Integrating real-time IoT traffic monitoring and analysis to adaptively adjust routing decisions based on the current network conditions.

- **Data Fusion and Aggregation :** Implementing distributed data fusion algorithms that leverage the aggregated data from multiple devices to enhance data accuracy and reliability.
- **QoS Monitoring and Adaptation :** Designing QoS monitoring framework that continuously evaluates key performance indicators (KPIs) such as latency, reliability, and throughput.

2 Methodology

The proposed bio-inspired protocol mainly focuses on adaptive sleep scheduling for energy efficiency and secured data transmission from one end to the other without any noise. The bio-inspired machine learning technique, Improvised Firefly Algorithm (IFBA), is deployed along with DKDM-EC to identify an IoT protocol that effectively works for sleep scheduling and reliable data transmission in real time. In addition to SS and DT, topology changes, abnormal network patterns, and vulnerability entries are also monitored and recorded to enhance the quality of the IoT environment. Error handling, data recovery, and finest path calculation are also done by EAP-IFBA with the help of MSEDR and QLT techniques. ERNN with the N-Key technique is used to identify network changes during data transmission. The sleep periods and wake-up times are scheduled by the protocol itself without any external command when the sensor state is idle and no data transmissions happen. This approach helps to save sensor energy to the maximum level, which helps to avoid node link failure during real-time processing and implementation.

2.1 Proposed Methodology

The new bio-inspired adaptive sleep scheduling and secured data transfer protocol specifically works on all IoT-based data sense and delivery environments to reduce energy consumption and boost the lifespan of the network in a robust manner. Here, the sensor nodes are deployed in an IoT environment for real-time data capture and delivery. The number of nodes tested in this study is 2500–3000 in the testbed. After the deployment of nodes, communication channels are established for effective data transfer from one end to the other. As a new method, the nodes are deployed and scheduled to alternate between the active and sleep states to perform a duty cycle for effective data sensing, processing, and delivery in an IoT environment. Adaptive sleep scheduling works on reducing dynamic link failure and adjusts the DC of each sensor node deployed based on topology, traffic, data availability, and real-time application prerequisites. Local node compression takes place during data transfer from one end to the other when using the EAP-IFBA protocol. Assume that n_node is the number of sensor nodes deployed in the IoT environment. The IDn & IDs denotes the source and destination node and n_loc is the location of the node. Initially the protocol measures the distance between the $node\_i$ and $node\_n$. Once the distance is measured, $initial\_energy$ of the node is calculated to begin the ready state to sense and capture the data in real time. Each node has individual access points where it stores the data as a volatile memory and then transfers it to the destination node. All the deployed nodes have equal communication points for accurate packet transfer from source to destination. The packet transfer and initial energy are calculated by using the below equation,

$$Node_{Energy} = \left(\frac{Node\ (i)\ (With\ IDs)}{Total\ Energy\ Consumed} \right]^{*} (node\,(i))\ |\, node_n\ X\ \ no.of i\_nodes \tag{1}$$

where, $Total\ Energy\ Consumed$ is the final consumed energy value of all the deployed nodes in the IoT environment. Here the $node\_active$ denotes the number of active nodes and i_nodes denotes the number of initialized nodes in the specified location for DC and DT.

$$Total\ Node\ Energy = \frac{(\ individual\ node\,(e)\}}{(Total\ node\,(e)\}}\ x\ 100\ \ (Range\ can\ be\ any) \tag{2}$$

where, $node(e)$ is to calculate the range of sensor node and total node energy of the active nodes in the deployed IoT environment.

2.2 Dynamic Key Distribution Management with EC

DKDM with DC is a new proposed technique used in EAP-IFBA for secure transmission of encrypted keys among sensor nodes in an IoT environment during the real-time transmission process with the help of the elliptic curve crypto method. To minimize energy-intensive operations in the centralized management, the key is generated by the system and distributed dynamically to ensure that the packets are transferred more securely and reliably. ECC offers strong security with short key lengths compared to baseline asymmetric algorithms. The ECC results in lower computational requirements and reduces energy consumption during dynamic key generation, encryption, and decryption operations during data transmission in an IoT environment. DKDM with

ECC reduces the node communication overhead associated with key management in an IoT network. By using the elliptic curve-based key exchange method, nodes are securely establishing shared secret keys without transmitting large amounts of data, which reduces the energy consumed in transmitting and processing key-related messages, resulting in improved energy efficiency. Table 1 shows the parameter settings to measure the speed of data transfer, sleep scheduling, and energy consumption.

Table 1. Parameter Setting for Simulation & Distribution Values

Parameters	**Values**
Monitoring Value	5000m x 3000m
Nodes Count	500 - 2500
IoT network range	600 x 600 m^2
Size of data packet	800-bit
Mobility Model	Random Way Point
Natre of Traffic	Constant Bit Rate
Nature of IoTMedium	Wireless medium
Initial transmission of deployed nodes	75 m
Initial energy of each node	20 J
Sensing Range	10 m
Threshold Distance	80 m
Simulator Name and Version	OMNET C++
Learning Rate	0.5 (alpha)
Total Number of Sample Nodes	T=50
No.of sample nodes in each round	M=500
Length of data packet	88 m
Circuit energy comsumption	E_{elec}= 50 J
Key Distribution Value (KDV)	K_i to K_n times (DKDM)

EAP-IFBA follows five steps for dynamic key distribution, such as:

- Randomly Generate keys and distribute them among nodes.
- Dynamic Key Update, such as time-based or event-based triggers
- Exchange the key using ECC between two nodes.
- Employ Key Derivation by using a shared secret key obtained from the key exchange process to derive the session keys.
- Secure Communication: Employ integrated ECC for DC and DT to minimize energy

2.3 EAP-IFBA for Adaptive Sleep Scheduling

The Energy Aware Protocol is introduced here with the help of the Improvised Firefly Bio-Inspired Algorithm for Adaptive Sleep Scheduling. Initialize the network parameters, which include the number of nodes, location, and communication range in an IoT environment. Initialize the population (firefly) by assigning the random positions to each firefly, which represents the number of nodes in real-time. Calculate the fitness value of each FF, which reflects the energy level of nodes, which was already calculated during key distribution management. The fitness value is calculated based on residual energy, distance to the base station, and quality of data transmitted. Now calculate the attractiveness between fireflies based on Nodes with maximum fitness emit brighter light in fireflies. Here, FF uses their brightness to communicate with neighboring fireflies and attract them. But the communication range is minimum, and in real-time, nodes should be deployed with the minimum communication range. Movements and adjustment values are recorded in the search space. FF with superior attractiveness tends to stay active for data transmission, while those with inferior attractiveness enter a sleep mode to conserve energy. The adaptive sleep scheduling process with Improvised Firefly follows the steps below for the implementation process.

- Random Initialization of Improvised Firefly population
- Calculate the fitness value based on firefly attraction
- Measure the location & communication range by using light propagation
- Allow multiple iterations where the fireflies adjusts their positions and attract each other
- For each firefly (source): Measure the distance to neighboring fireflies (destination)

- If the destination firefly is out of the IoT communication range, adjust the brightness of the destination firefly towards the source firefly's brightness.
- Adaptive Sleep Scheduling takes place based on the final position of FF
- Secured data transmission is done with DKDM by considering the attractiveness of each node and adjusting the sleep schedule accordingly

Let us assume $i\_fireflies$ is the number of population initialized in the IoT environment. The distance between $S \rightarrow D$ is calculated using $calculate\_distance$ and $adjust\_brightness$ is used to measure the light value and $get\_best\_neighbour$ is the neighbour attracted firefly to transfer the message and $adjust\_position$ stores the adjustments and movements of fireflies. The new position is stored in $new\_position$ and the updated position is stored in$updated_position$.

$$\text{Firefly } y_{\text{Position}} = FF_{-}\text{Distance}\ \frac{\text{new}_{\text{ position}}\, xi_{\text{fireflies}}}{\text{updated}_{\text{ position}}} \times \text{number of iterations} \tag{3}$$

where, $FF_{Distance}$ is the calculated distance of each fireflies in the deployed environment or search space and $time$ refers the time duration of data transmission process between each nodes. As the iterations progress, fireflies gradually converge towards an optimal configuration that minimizes energy consumption. During the active periods, nodes transmit data to the base station or to neighboring nodes as required. Based on the final positions of the fireflies, determine the optimal sleep schedule for each sensor node. The adaptive sleep schedule ensures that energy consumption is minimized, as only necessary nodes are active. Effective data transmission is achieved by considering the attractiveness of each node and adjusting the sleep schedule accordingly. The sleep schedule can be adjusted dynamically based on topology changes and the energy level of the IoT sensor nodes.

Improvised Firefly Algorithm (IFA) for Adaptive Sleep Scheduling

```
Input: OMNET Simulation settings with Parameter Values
Begin
Initialize the parameters and set num_nodes = 50
Set Communication Ranze = 100
Fitness Function = $Node_{Energy}Level$
max(n)_iterations = 100|$sleep\ (s)\_duration|\ activre\ (a)\_duration\ =\ 5$
Initialize firefly positions
fireflies = [(random.randint(0, 100), random.randint(0, 100)) for _ in range(num_nodes)]
Initialize adaptive-sleep-schedule (all nodes are to begin with active)
Sleep Schedule = [False] * num_nodes
Calculate attractiveness = [$Fitness_{\ function(node)}$ for node in fireflies]
Perform iterations in EAP-IFBA
for _ in range(max_iterations):
For i in range(num_nodes):
source_i-firefly = fireflies[i]
source_brightness = brightness[i]
For j in range(num_nodes):
If i != j:
destination_i-firefly = fireflies[j]
destination_brightness = brightness[j]
distance = calculate_distance(source_i-firefly, destination_i-firefly)
If distance <= communication_range and source_brightness > destination_brightness:
brightness[j] = adjust_brightness(destination_brightness, source_brightness)
for i in range(num_nodes):
current_firefly = fireflies[i] (Improvised Firefly Method)
best_neighboring_firefly = get_best_neighboring_firefly(current_firefly, fireflies, brightness)
```

```
27. new_position = adjust_position(current_firefly, best_neighboring_firefly)
28. fireflies[i] = new_position
29. If brightness[i] > threshold: (Calculate Brightness)
30. sleep_schedule[i] = False
31. Else
32. sleep_schedule[i] = True
33. Repeat the iterations
34. Calculate the number of active nodes and sleep nodes
35. Compute $FF\_distance$
36. Calculate $Node_{Energy}$ based on active nodes in the IoT environment
37. Measure $DT\_speed$ to get the data transmission speed and time
38. Get the $Optimal\ Value$
39. End
```

Here, the fitness function, distance calculation, brightness adjustment, position adjustment, and other IFBA functions will produce the optimal value based on the parameter settings in the OMNET C++ simulator. The placeholder function in EAB-IFBA is used to compute the distance and brightness of fireflies and adjust the position of fireflies in the search space.

2.4 ERNN with N-Key to identify topology changes

ERNN with the N-Key method is used to track the topology changes in an IoT environment. In this method, each node is assigned a unique N-Key based on the identifier or position where it is deployed. It captures the patterns in the data, which include N-Key and topology structure changes. Also, it records the addition and removal of nodes and updates to the N-Key. ERNN is trained to understand the characteristics of topology changes in IoT. The N-Key serves as the identifier or unique value for the sensor node location or the connectivity of nodes within the deployed area or network. Key encoding and decoding take place during the data transmission process. Train the ERNN model using historical data from the IoT network, including node positions, connectivity information, and associated N-Keys. Deploy the trained ERNN model in the IoT network for real-time topology monitoring. Continuously collect and feed input data to the ERNN model, including current node positions, connectivity information, and associated N-Keys.

For efficient monitoring of topology changes by ERNN, the below-mentioned steps were used.

- Capture the data and assign an N-Key for each node.
- Encode the N-Key for reliable communication.
- Monitor the network changes in the ring-round method.
- Identify the learned patterns to capture the topology changes.
- Establish communication with BS-Base Station.
- Detect the topology changes.

Detect 0 or 1 (No change or Change in topology).The change value is stored in $Topology\_Change$ and this value is used to identify the active nodes and proceed for sleep scheduling with the help of below equation,

$$Topology\_Changes = \ (N - Key\ (Node))\ |\ (Pattern_i\ x\ Pattern_n) \tag{4}$$

where, $(Pattern_i and\ Pattern_n)$ denotes the value of captured patterns in IoT environment during topology changes.

2.5 MSEDR & Q-LT Data Recovery & Finest Route discovery Method in IoT Environment

When the data is transmitted, it might be subject to noise or, due to some other external factors, data corruption might occur. MSEDR measures the mean square error between the original data and the recovered data from the loss in an IoT environment. The recovery process involves error corrections, re-transmission, or data reconstruction. During the data re-transmission, the Q-LT method is deployed to transfer the data on the best path to reach its destiny. In the context of data transmission, the environment consists of different network paths, each with varying characteristics like latency, bandwidth, or reliability. The Q-LT maintains a Q-table that stores the expected utility (Q-values) for taking specific actions (choosing a particular path) in a given state (current network conditions). By using the optimal path identified by QLT, the data transmission process of

EAP-IFBA minimizes delays, reduces errors, and ensures fast and reliable data transmission. In equation 5, the improved Q-LT performance is presented.

$$Q-LT\ \ (DT)=\ Data\frac{Recovery\ Nodes}{No.of\ Nodes}\ x\ Captured\ Datas\rightarrow\ Best_{Route} \tag{5}$$

where, the term $Best_{Route}$ denotes the finest route identified by Q-LT for efficient data transmission.

2.5.1 Implementation using OMNETC++ Simulator

Implementing the EAP-IFBA IoT network protocol using the OMNETC++ simulator provides a authoritative platform for energy-efficient and robust IoT network design, performance evaluation, scalability analysis, and protocol evaluation. It aids in optimizing the protocol parameters and enhancing the overall efficiency, reliability, and security of IoT networks. Also, it provides a versatile simulation environment to assess various performance metrics of the EAP-IFBA protocol and to measure factors such as data transmission speed, latency, throughput, and network efficiency, which enables fine-tuning and optimization of the protocol parameters and design to achieve better overall performance. OMNET aids in identifying potential bottlenecks, load balancing issues, and resource management strategies to ensure efficient operations in large-scale IoT deployments, also it is one of the top-end simulators to measure various types of PEM in bio-inspired-based network protocols.

2.5.2 PEM of EAP-IFBA

The PEM of the proposed model EAP-IFBA is measured against the baseline algorithms chosen in the previous section, IWD-ARP[6], ECC-ILEACH[5], and RLSSA-CDGP[4]. The PEM equations used to derive the solution.

$$EDR=\frac{(\text{ Initial Energy }-\text{ Remaining Energy })}{(\text{ Time }(\text{ Duration }))} \tag{6}$$

$$\text{Network } LT=\frac{\text{Total Energy}}{(\text{ Energy Depletion Rate })} \tag{7}$$

$$\text{No.of Active Nodes }=\frac{\text{Total Nodes }-\text{ Failed Nodes}}{(\text{ Data Transmission Time })} \tag{8}$$

$$\text{Data Transmission Speed }=\frac{\text{Data Size}}{(\text{ Transmission Time })} \tag{9}$$

$$\text{Sleep Scheduling Time }=\text{ Total Time }-\text{ Active Time} \tag{10}$$

$$RTA(\text{ Robustness })=\frac{\text{Node Disjoint Path}}{(\text{ Network Diameter })} \tag{11}$$

where, IE denotes Initial energy, RE denotes Remaining energy and LT denotes latency time.

- **(EDR) Energy Depletion Rate:** The total amount of energy spent by the recommended bio-inspired technique EAP-IFBA in the IoT network environment throughout the data sensing, capture, and transmission processes.
- **(LN) Lifespan of Network:** Identifies the network lifetime required for efficient data transmission processes by measuring the lifespan of the deployed IoT sensor nodes.
- **(NAC) Number of alive or active nodes:** To assess network traffic and determine the proportion of active nodes after successful data transmission.
- **(DTS) Data Transmission Speed:** Analyze the speed of data transfer between S and D to see if the protocol is taking the best possible path for successful packet delivery.
- **(SST) Sleep Scheduling Time:** measures the proposed EAP-IFBA's sleep scheduling time in an IoT network environment while the system is idle.
- **(RTA) Robustness to attacks:** To evaluate the proposed EAP-IFBA protocol's robustness against attacks and topological changes.

3 Results and Discussion

This chapter shows the comparative analysis and findings of the proposed novel bio-inspired Energy Aware-Improvised Firefly Bio-Inspired Algorithm (EAP-IFBA)-based protocol for secured data transmission and effective sleep scheduling. EAP-IFBA is compared with the prevailing data transmission and energy-aware models such as IWD-ARP [(6)], ECC-ILEACH [(5)], and RLSSA-CDGP [(4)]. The new protocol shows remarkable results, works well in an IoT distributed environment, and overcomes the drawbacks of the existing methods. Queuing Theory a measuring technique is used to monitor the sleep scheduling process when the system is in an idle state. The unique feature of EAP-IFBA is that it sends the data from source to destination by removing noise and duplicates. Figs. 1-6 represent the comparative analysis of the proposed protocol against current models. The plotted graph with the X axis shows the node counts, and the Y axis shows the percentage analysis of comparative models.

3.1 Energy Depletion Rate - Comparative Analysis

The energy depletion rate of the proposed novel EAP-IFBA is presented in Figure 1. The comparative analysis of EAP-IFBA is done against the existing methods: IWD-ARP [(6)], ECC-ILEACH [(5)], and RLSSA-CDGP [(4)]. It is observed that due to sleep scheduling at the time of idle state, the system will save more energy and take very little time during data transmission from $S \to D$. The tested node count in the test-bed is 2500. The proposed protocol outperforms at an 8% energy consumption rate for 500 NC and 15% for 2500 NC. As the model uses IDKM, the sensor nodes activate only on request during data transmission, which saves more energy.

Table 2. Energy Depletion Rate Analysis (%)

Node Counts / Protocols	500	1000	1500	2000	2500
IWD-ARP [(6)]	46	51	57	61	68
EEE-LEACH [(5)]	38	43	49	53	56
RLSSA-CDGP [(4)]	33	40	43	48	50
EAP-IFBA (Proposed)	**8**	**11**	**13**	**14**	**15**

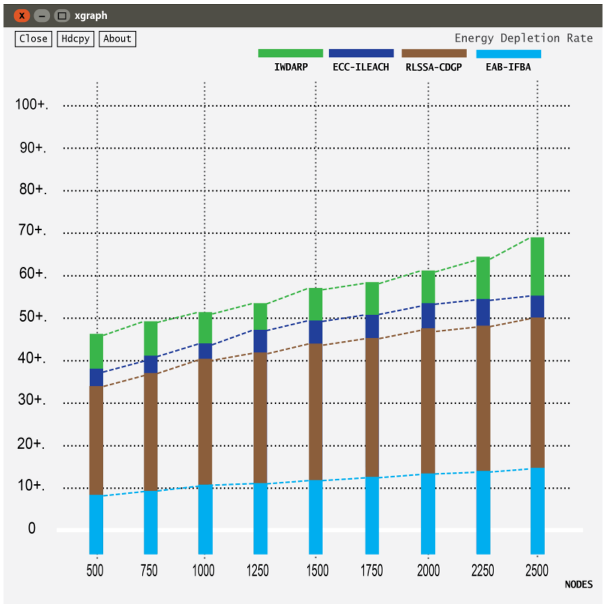

Fig 1. Comparative Analysis of Energy Depletion

3.2 Network Lifespan - Comparative Analysis

The performance of EAP-IFBA in terms of network lifespan is presented in Figure 2 . The proposed bio-inspired model is measured against baseline methods such as IWD-ARP [(6)], ECC-ILEACH [(5)], and RLSSA-CDGP [(4)]. As the abnormal patterns are identified using the N-Key method in an IoT environment for effective data transmission, all the duplicate data is removed with robust data optimization. The sleep scheduling process takes place when the system state is idle. The sensor nodes will consume less energy, which leads to an increase in lifespan. The network lifetime is enhanced by up to 98% during the test-bed process in EAB-IFBA.

Table 3. Network Lifespan Analysis (%)

Node Counts / Protocols	500	1000	1500	2000	2500
IWD-ARP [6]	59	55	48	39	26
EEE-LEACH [5]	78	75	68	56	35
RLSSA-CDGP [4]	86	82	77	70	65
EAP-IFBA (Proposed)	**98**	**95**	**94**	**93**	**93**

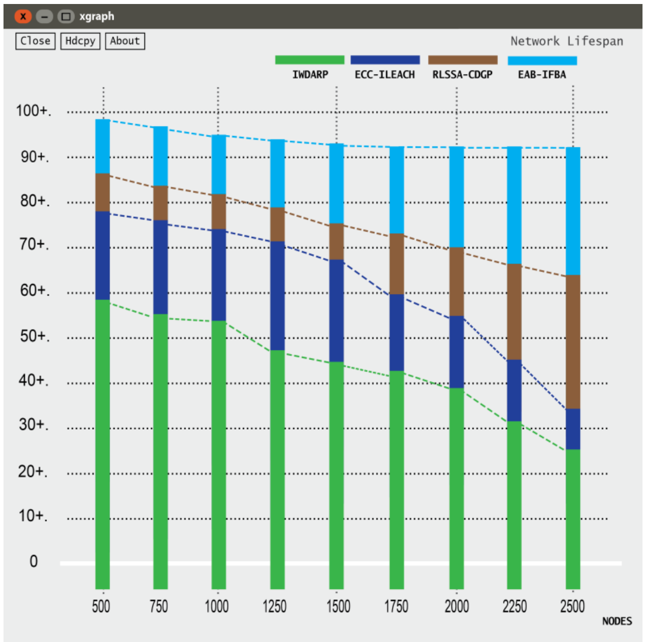

Fig 2. Comparative Analysis of Network Lifespan

3.3 Percentage of Alive Nodes - Comparative Analysis

Figure 3 shows the percentage of active nodes in an IoT network when a large number of data transmissions happen and also in real-time. It is noted that the proposed novel bio-inspired method EAP-IFBA outperforms well when compared to the existing protocols IWD-ARP [6], ECC-ILEACH [5], and RLSSA-CDGP [4]. EAP-IFBA is tested with a minimum of 500 NC and a maximum of 2500 NC. As the Q-Learning method is used to identify the finest path for data transmission, the load and data transmission time are minimized. 97.5% of alive nodes are marked during the iteration process, which is comparatively higher than any other IoT network protocol. The protocol effectively works in real-time sensing, capturing live data and transferring it immediately.

Table 4. Alive/Active Nodes Analysis (%)

Node Counts / Protocols	500	1000	1500	2000	2500
IWD-ARP [6]	61	58	48	42	28
EEE-LEACH [5]	82	78	71	58	38
RLSSA-CDGP [4]	91	88	80	74	69
EAP-IFBA (Proposed)	**97.5**	**95**	**93**	**92**	**92**

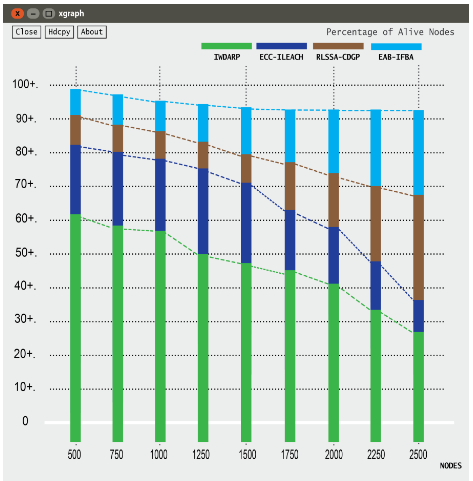

Fig 3. Comparative Analysis of Alive Nodes

3.4 Data Transmission Speed - Comparative Analysis

Figure 4 show cases the data transmission speed analysis of the proposed bio-inspired novel algorithm EAB-IFBA. Comparative analysis is done against the prevailing IoT DT protocols such as IWD-ARP [6], ECC-ILEACH [5], and RLSSA-CDGP [4]. The proposed method shows promising results with high-speed data transmission from $S \rightarrow D$. As the EAP-IFBA uses the ECM method for secured data transmission and QLT is employed to identify the finest path in an IoT network environment, the data transmission happens very fast. 97.6% was achieved when using EAB-IFBA, which is comparatively higher than the existing protocols during the OMNETC++ test-bed process.

Table 5. Data Transmission Speed Analysis (%)

Node Counts / Protocols	500	1000	1500	2000	2500
IWD-ARP [6]	76	71	59	52	35
EEE-LEACH [5]	82	78	71	59	35
RLSSA-CDGP [4]	89	85	78	72	68
EAP-IFBA (Proposed)	**97.6**	**94**	**92**	**90**	**88**

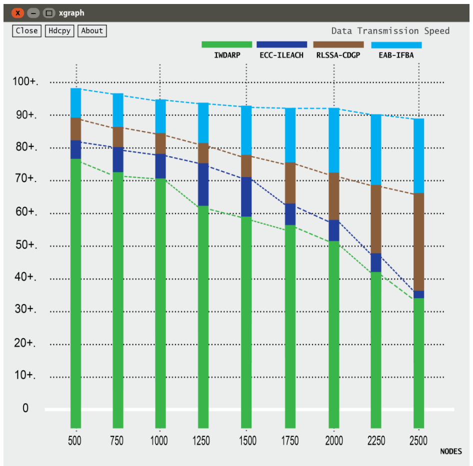

Fig 4. Comparative Analysis of Data Transmission Speed

3.5 Robustness to Attacks (RTA) - Comparative Analysis

Figure 5 portrays the robustness to attacks analysis of the proposed ML bio-inspired IoT protocol EAP-IFBA and compares it with the baseline protocols such as IWD-ARP [(6)], ECC-ILEACH [(5)], and RLSSA-CDGP [(4)]. In EAB-IFBA, the DKDM with ECM method is employed for data security, where the captured data is encrypted with N-Key and sent to the destination. During this process, if any error occurs, mean square error data is used to recover the error data and transmit the same to destiny. 96.5% of the time, the protocol withstands attacks in a network environment such as topology changes, hacking, etc.

Table 6. RTA Analysis (%)

Node Counts / Protocols	500	1000	1500	2000	2500
IWD-ARP [(6)]	77	70	58	51	39
EEE-LEACH [(5)]	82	77	71	58	51
RLSSA-CDGP [(4)]	88	85	78	72	67
EAP-IFBA (Proposed)	**96.5**	**93**	**91**	**90**	**89**

3.6 Sleep Scheduling – Comparative Analysis

Quick sleep scheduling analysis is shown in Figure 6 of the proposed novel bio-inspired ML technique, EAB-IFBA. The method is compared against existing sleep scheduling IoT protocols, IWD-ARP [(6)], ECC-ILEACH [(5)], and RLSSA-CDGP [(4)]. Though the algorithm works on social behaviors, fast communication is done between sensors if the system is in an idle state. When there is no data transmission between $S \rightarrow D$, the sleep scheduling process activates, and the particular IoT environment hibernates until the next transmission starts. 98% of speed sleep scheduling takes place during the test process when employing the EAP-IFBA approach, which is comparatively higher than the existing protocols.

Table 7. Sleep Scheduling Analysis (%)

Node Counts / Protocols	500	1000	1500	2000	2500
IWD-ARP [(6)]	78	71	59.6	53	41
EEE-LEACH [(5)]	83	78	72	59	52
RLSSA-CDGP [(4)]	89.8	85	78	73	68
EAP-IFBA (Proposed)	**98**	**94**	**92**	**91**	**90**

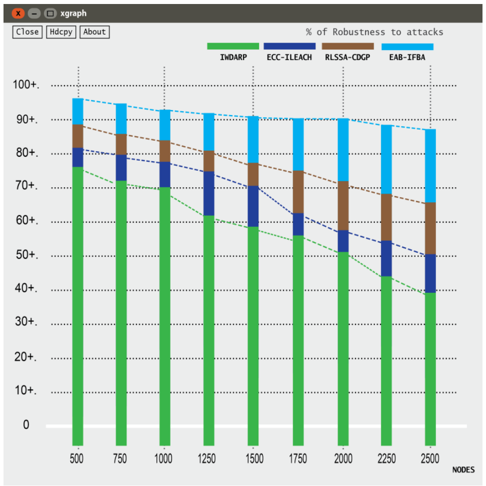

Fig 5. Comparative Analysis of RTA

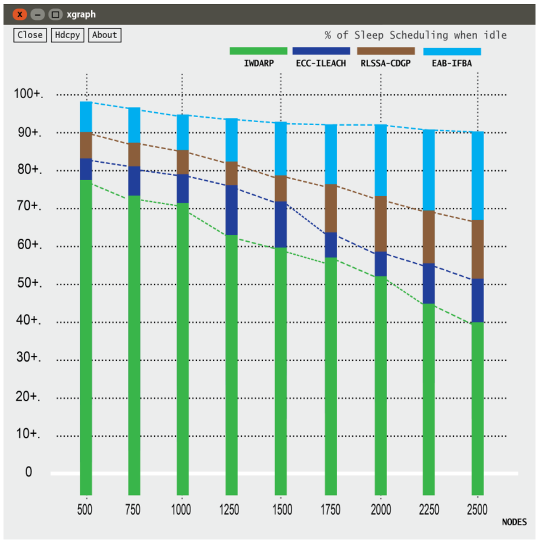

Fig 6. Comparative Analysis of Sleep Scheduling

4 Conclusion

The proposed sleep scheduling and secured data transmission protocol EAP-IFBA (Energy Aware Bio-Inspired Improvised Firefly Bio-Inspired Algorithm-Based Protocol) is used for adaptive sleep scheduling, boosting the energy in sensor nodes, reliable and secured data transmission, and sensing dynamic topology changes. Dynamic key generation with ECM is employed to overcome security issues and data loss in real-time data capture and delivery. Topology changes and abnormal patterns associated with network attacks are identified by ERNN, and data recovery errors are evaluated by MSEDR. A finite path for data transmission is created by utilizing QLT with action sets to minimize data loss and maximize sensor node energy. The EAP-IFBA is tested in a custom Testbed where physical IoT devices are deployed and sensors are installed to collect real-time data. EAB-IFBS captures network topology changes, traffic patterns, reliable data transmission, the lifespan of the IoT network, the number of active nodes, and energy consumption. The evident results clearly show that the new protocol works against network attacks, saves energy, and delivers data more securely. The OMNETC++ simulator is used to evaluate the performance metrics. The energy consumption rate is completely reduced to 8%, and the lifespan of the IoT network is increased to 98%. Though the proposed method gives promising results, it has a few limitations in that the placement of sensor nodes should be done properly for effectiveness. If it is deployed in an uneven area, the system will slow down in sensing the data, resulting in an increasing delay time. Also, EAB-IFBS will work in heterogeneous and distributed environments, and it will have property limitations when implemented in homogeneous models. In the future, this model can be enhanced to work in complex IoT homogeneous systems, large-scale WSNs, and be robust to all types of attacks.

References

1) Sharma N, Singh BM, Singh KM. QoS-based energy-efficient protocols for wireless sensor network. *Sustainable Computing: Informatics and Systems*. 2021;30:100425. Available from: https://doi.org/10.1016/j.suscom.2020.100425.
2) Orfanos VA, Kaminaris SD, Papageorgas P, Piromalis D, Kandris D. A Comprehensive Review of IoT Networking Technologies for Smart Home Automation Applications. *Journal of Sensor and Actuator Networks*. 2023;12(2):30. Available from: https://doi.org/10.3390/jsan12020030.
3) Kim D, Yun J, Kim D. An Energy-Efficient Secure Forwarding Scheme for QoS Guarantee in Wireless Sensor Networks. *Electronics*. 1418;9(9):1418. Available from: https://doi.org/10.3390/electronics9091418.
4) Wang X, Chen H, Li S. A reinforcement learning-based sleep scheduling algorithm for compressive data gathering in wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*. 2023;(1):28. Available from: https://doi.org/10.1186/s13638-023-02237-4.
5) Hussein SM, Ramos JAL, Ashir AM. A Secure and Efficient Method to Protect Communications and Energy Consumption in IoT Wireless Sensor Networks. *Electronics*. 2022;11(17):2721. Available from: https://doi.org/10.3390/electronics11172721.
6) S N, V J. 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. Available from: https://doi.org/10.17485/IJST/v13i16.19.
7) Rishiwal V, Yadav P, Singh O, Prasad BG. Optimizing Energy Consumption in IoT-Based Scalable Wireless Sensor Networks. *International Journal of System Dynamics Applications*. 2021;10(4):1–20. Available from: http://doi.org/10.4018/IJSDA.20211001.oa21.
8) Wan R, Xiong N, Loc NT. An energy-efficient sleep scheduling mechanism with similarity measure for wireless sensor networks. *Human-centric Computing and Information Sciences*. 2018;8(1). Available from: https://doi.org/10.1186/s13673-018-0141-x.

9) Thomas D, Shankaran R, Sheng QZ, Orgun MA, Hitchens M, Masud M, et al. QoS-Aware Energy Management and Node Scheduling Schemes for Sensor Network-Based Surveillance Applications. *IEEE Access*. 2021;9:3065–3096. Available from: https://doi.org/10.1109/ACCESS.2020.3046619.

10) Sakib AN, Drieberg M, Sarang S, Aziz AA, Hang NTT, Stojanović GM. Energy-Aware QoS MAC Protocol Based on Prioritized-Data and Multi-Hop Routing for Wireless Sensor Networks. *Sensors*. 2023;22(7):2598. Available from: https://doi.org/10.3390/s22072598.

11) Panahi U, Bayılmış C. Enabling secure data transmission for wireless sensor networks based IoT applications. *Ain Shams Engineering Journal*. 2023;14(2):101866. Available from: https:/doi.org/10.1016/j.asej.2022.101866.

12) 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*. 2020;(2):1574–1578. Available from: https://doi.org/10.35940/ijrte.b2271.078219.

13) Panahi P, Bayılmış C, Çavuşoğlu U, Kaçar S. Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications. *Arabian Journal for Science and Engineering*. 2021;46(4):4015–4037. Available from: https://doi.org/10.1007/s13369-021-05358-4.

14) Velmurugadass P, Dhanasekaran S, Anand SS, Vasudevan V. Quality of Service aware secure data transmission model for Internet of Things assisted wireless sensor networks. *Transactions on Emerging Telecommunications Technologies*. 2023;34(1). Available from: https://doi.org/10.1002/ett.4664.

15) Ramesh S, Yaashuwanth C. Enhanced approach using trust based decision making for secured wireless streaming video sensor networks. *Multimedia Tools and Applications*. 2020;79(15-16):10157–10176. Available from: https://doi.org/10.1007/s11042-019-7585-5.

16) Baskaran D, Sairamesh L, Kamalanathan S. Intelligent energy-aware and secured QoS routing protocol with dynamic mobility estimation for wireless sensor networks. 2021. Available from: https://doi.org/10.1007/s11276-020-02532-8.

17) Diratie ED, Sharma DP, Agha KA. Energy Aware and Quality of Service Routing Mechanism for Hybrid Internet of Things Network. *Computers*. 2021;10(8):93. Available from: https://doi.org/10.3390/computers10080093.

18) Kalpana D, Ajitha P. An Implementation of Energy Efficient Secured Routing Framework in WSN by Honey Badger Algorithm. *2022 International Conference on Industry 40 Technology (I4Tech)*. 2022;2022:1–6. Available from: https://doi.org/10.1109/I4Tech55392.2022.9952953.

19) Singh S, Nandan AS, Sikka G, Malik A, Vidyarthi A. A secure energy-efficient routing protocol for disease data transmission using IoMT. *Computers and Electrical Engineering*. 2022;101:108113. Available from: https://doi.org/10.1016/j.compeleceng.2022.108113.

20) 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*. 2020;(10):3244–3251. Available from: https://doi.org/10.35940/ijstr.b2271.0986231.

21) Djene YFE, Idrissi MS, Tardif PM, Jorio A, Bhiri E, Fakhri B. A Formal Energy Consumption Analysis to Secure Cluster-Based WSN: A Case Study of Multi-Hop Clustering Algorithm Based on Spectral Classification Using Lightweight Blockchain. *Sensors*;2022(20):22. Available from: https://doi.org/10.3390/s22207730.

22) Nagaraja GS, Vanishree K, Azam F. Novel Framework for Secure Data Aggregation in Precision Agriculture with Extensive Energy Efficiency. *Journal of Computer Networks and Communications*. 2023;2023:1–11. Available from: https://doi.org/10.1155/2023/5926294.

23) Sharmila, Kumar P, Bhushan S, Kumar M, Alazab M. Secure Key Management and Mutual Authentication Protocol for Wireless Sensor Network by Linking Edge Devices using Hybrid Approach. *Wireless Personal Communications*. 2023;130(4):2935–2957. Available from: https://doi.org/10.1007/s11277-023-10410-7.

24) Shahraki A, Taherkordi A, Haugen O, Eliassen F. A Survey and Future Directions on Clustering: From WSNs to IoT and Modern Networking Paradigms. *IEEE Transactions on Network and Service Management*. 2021;18(2):2242–2274. Available from: https://doi.org/10.1109/TNSM.2020.3035315.

25) Dhaliwal BK, Rattan K, Datta. Secure and Energy Efficient Trust Aware Routing Protocol in IoT using the Optimized Artificial Neural Network: SEETA-IoT. *International Journal of Engineering and Advanced Technology (IJEAT)*. 2019;8(6):4341–4353. Available from: http://www.doi.org/10.35940/ijeat.F8928.088619.