INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Robust AI Based Bio Inspired Protocol using GANs for Secure and Efficient Data Transmission in IoT to Minimize Data Loss

P Aruna Devi[1]*, D Megala[2], N Paviyasre[3], S Nithyanandh[4]

1 Assistant Professor, Department of Computer Technology, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India
2 Assistant Professor, Department of Information System Management, Gurunanak College, Chennai, Tamil Nadu, India
3 Assistant Professor, Department of Computer Science, Kongunadu Arts and Science College, Coimbatore, Tamil Nadu, India
4 Assistant Professor, Department of Computer Applications (MCA), PSG College of Arts & Science, Coimbatore, Tamil Nadu, India

OPEN ACCESS

Received: 20-07-2024
Accepted: 05-08-2024
Published: 28-08-2024

Citation: Devi PA, Megala D, Paviyasre N, Nithyanandh S (2024) 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 17(35): 3609-3622. https://doi.org/10.17485/IJST/v17i35.2342

* **Corresponding author**.

aruna7825@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 an AI-based protocol to enhance the reliability and security of IoT data transmission in a robust manner. Deep learning with bio-inspired methods is employed to address real-time challenges such as route optimization, data integrity, error recovery, and end-to-end delay in order to minimize data loss and maximize the transmission rate. **Methods:** Generative Adversarial Networks (GANs) are used to enhance the robustness of the protocol in combination with a bio-inspired Artificial Immune System (AIS) to detect IoT network anomalies and responds to malicious activities by using the adaptive learning capabilities of IS. Hybrid Automatic Repeat Request (HARQ), an error recovery method, is utilized to detect network errors in order to correct and retransmit data to the destination during error-prone network conditions. Queue learning action sets are used to discover the finest path for efficient data transmission. The OMNeT++ simulator is used to assess the performance of the proposed BIP-GANs protocol. The performance results are compared with the prevailing data transmission protocols, such as EAP-IFBA, DNN-CSO, and ALO-DHT. **Findings:** The suggested BIP-GANs data transmission protocol outperforms with promising results, with an energy consumption rate of 6%, 8 seconds data transmission speed, 6 second less delay rate, 98% robustness (security and confidentiality), 98.5% alive nodes, and 99% network life span, which is higher than the prevailing methods. **Novelty:** This research study provides a comprehensive solution to secure and efficient data transmission by integrating the AI-based bio-inspired BIP-GANs method to address the security and data transmission challenges of existing methods such as EAP-IFBA, DNN-CSO, and ALO-DHT in terms of energy consumption rate, transmission speed, delay rate, life span of the network, robustness, and number of alive nodes.

Keywords: Artificial Intelligence; Generative Adversarial Networks; Error Recovery; Secured Data Transmission; Deep Learning; BioInspired Algorithm

1 Introduction

The IoT and 5G network standards have grown remarkably and revolutionized the way sensor devices communicate each other for efficient data exchange from source to destination, which helps enhance real-time applications like healthcare, industrial automation, smart cities, environmental monitoring, etc. However, as the IoT network ecosystem expands, the prevailing IoT network protocols encounter significant drawbacks like data loss, data security, device failure, and susceptibility to malicious attacks. To address the above challenges, a new artificial intelligence-based bioinspired protocol is proposed in this research study to maximize end-to end data transmission and minimize data loss. Generative Adversarial Networks (GANs)in combination with Artificial Immune System (AIS) and Hybrid Automatic Repeat Request (HARQ) methods enhance the performance of IoT in terms of responding effectively to topology changes, malicious attacks, cyber threats, and network errors. By integrating AI and bioinspired strategies, BIP-GANs overcome all the challenges of prevailing protocols and provide a comprehensive solution to make the IoT ecosystem more reliable and secure. As the security features are embedded in BIP-GANs, it helps to safeguard the data packets transmitted from S→D with maximum speed and efficient energy.

The main goal is to develop a robust adaptive IoT network protocol using AIS and GANs to handle network congestion dynamically in order to address sensor device failures and security vulnerabilities. GAN[1] is applied to perform data augmentation through sensors to detect lung nodules in combination with machine and deep learning methods. XAI is introduced by the authors to extract knowledge from patterns, but it has a few drawbacks, including a lack of deep sense, which helps with data transformation. All the cluster data is dealt with by LLM to discrete the data space, which helps the new model use the data. GOM[2–4] is used to train the neural networks where classification of complex tasks is reduced. N-Minimize, the new concept introduced by the authors along with a radial basis in order to optimize large dimensions. A precise study has been carried out on anomaly detection, which paves a clear path towards the ADS CAD system. Two GAN architectures were trained and captured the network traffic anomaly features to make them more authentic in order to avoid fake data. Many optimization algorithms for data forwarding were proposed, like BIP-CHN, MPT-LNN, and LEACH-PN[5], to transmit the data in a robust way to minimize data loss and energy consumption. This helps in the data transmission process, where this will not deal with detection and responding to malicious attacks, which is considered to be the drawback of the optimization machine learning models. The authors proposed AI and ML-based models[6–8] specifically for brain and computer interaction to enable the system to identify intrinsic features in any data, thereby achieving the essential goal of enhancing security. The only drawback of conventional models is their static and restricted flexibility. ACO-based demand vector, GSO-CODLBS, SPM-UN and QOS-ARP protocols[9–12] work towards an intelligent routing method where the data is transferred intrinsically in the shortest path to destiny with minimal false rate due to poor interaction with bio-inspired algorithms. Imbalanced data prediction is done using SPM-UN to optimize the network data for a specific input. RSVRP, RABCRP, DDOS-SGA, and an AI-based network communication scheme[13–15] were proposed to solve the performance degradation in the dynamic network structure and optimization issues in a large-scale IoT environment. A few shortcomings are noted in terms of data loss, high latency, energy consumption, etc., which will burden the network and lead to security threats.

Deep data augmentation [16–18] for the physical layer is carried out in the LORA network environment to forward the data between sensors dynamically without any loss, which increases network performance. EAP-IFBA [19] enhances the QoS of the IoT network, which optimizes the energy to speed up the data forwarding process using the bio-inspired firefly method. Adaptive sleep scheduling is the method deployed to reduce energy during data forwarding from S→D. The major drawback of this system is that the protocol may adapt only for small-scale networks, which complicates LORA-WSN during the real-time data capture and forwarding process. In order to solve the optimization and security issues in IoT devices, the AI-based security-enabled DNN-CSO [20] protocol was introduced for secured data forwarding, which concentrates multiple route attacks and defends the networks in a robust way. The sole drawback of DNN-CSO is constant traffic learning and the adaptation of IoT, which leads to high computing needs and heavy resources. A hybrid mechanism ALO-DHT [21] is designed specifically for data transfer in IoT edge-based networks and integrates RSA and cryptographic methods to ensure data is forwarded to the destination without any breach or loss. The system performance is affected while deploying in a real-time environment, which is the only issue with using ALO-DHT. MANET, LFSTN, and S-Paradigm [22–25] add performance to networks in terms of load balancing, minimizing energy depletion rate, etc., where these protocols slowdown the data forwarding and increases latency time. A detailed survey was conducted on deep learning GANs, and meta-analysis was done for remote sensing the data for an efficient data capture system, which helps the research work to take forward on GAN implementation [26,27]. To overcome the drawbacks of the prevailing approaches, a robust AI-based data forwarding protocol called BIP-GANs is proposed for secured data transmission processes and efficient anomaly detection in a dynamic manner in an IoT network environment to maximize the energy consumption rate and security.

2 Methodology

The proposed BIP-GANs AI-based nature-inspired network protocol helps to boost the data transmission process with high security in an IoT environment. GANs have multiple interconnected networks that deal with IoT traffic, intruder activities, and fake paths, which potentially help the system to identify and capture new threats to minimize data loss. The Bio-Inspired Artificial Immune System detects malicious activities and network anomalies and responds immediately to secure the data during transmission. It creates an artificial path to deliver the sensed data to the destination. Errors are handled by a hybrid auto-request model where data loss is minimized during the transmission process. The energy is reduced by cutting down the bandwidth to its maximum level, which makes the data transmission process reliable. The queue learning method discovers the finest route between sensor nodes in the IoT search space and makes the data travel from base station to destination without any loss. Real-time Example: For instance, in a healthcare IoT environment, the sensor devices capture patient data and transmit it to the main central server. The proposed BIP-GANs protocol detects anomalies, reports them to the network, is corrected by a HARQ error detector, and transmits data in the finest route from S→D using queue action sets. This method of integration ensures an efficient data-transmitting framework that will address the challenges of security and reliability.

2.1 Proposed Data Transmission Approach

In this research work, an AI-based bio-inspired protocol is proposed that aims to boost security, efficient data transmission, anomaly detection, and error handling in a large-scale IOT network environment by integrating the GAN and AIS models. GAN creates realistic discriminator network traffic patterns, including normal and anomalous, to differentiate between legitimate and malicious data. Malicious attacks such as unauthorized access, intruder attempts, and data manipulations will be monitored by GANs. Once the abnormal activities are monitored, AIS analyzes the incoming threats using its bio-learning and immune memory methods, responds continuously, and sends information to the base station. Let's assume $G\ and\ D$ are generator and discriminator with the objective to produce discrimination created network data from real data. $G_{Loss} and\ D_{Loss}$ is calculated to maximize $Log\ D$.

$$G_{Loss} = E_z \sim P_z(z)\left[Log\ D(G(z))\right] \tag{1}$$

where, $z = noise\ input$ to the GAN generator, G_z is the data generated by GAN from P-distribution P_z.

$$D_{Loss} = -E_X \sim P_{data}(x)\left[Log\ D(x)\right] - E_z \sim P_z(z)[Log\ D(G(z))] \tag{2}$$

where, $x = real\ data\ input$ sampled from GAN data distribution to maximize $[Log\ D(x)]$ for real and $1 - D(G(z)$ for GAN generated network traffic data. Once the data is recorded, AIS starts detecting the anomalies in the generated samples by GAN. The matching rule and anomaly scores are updated by AIS using its learning and memory methods. The matching rule is to identify the similarity between GAN samples and anomaly scores and point out how the patterns are differentiated between

current and collected traffic IoT data. $m(x,y)$ is the matching rule, where $x\ and\ y$ are the IoT network feature sets. The anomaly score is derived using,

$$Score_{anomaly(x)} = 1 - max(y€m)\,[m\,(x,y)] \tag{3}$$

where, m is the known patterns (memory cells of AIS). The high score points the higher anomaly, and the system responds to it time to time and records in the log.

Hybrid auto request method collects the network errors and retransmits the data by correcting it after recording into log to make sure the timely data delivery is happened from source to destination. The QL process discovers the optimal route in IoT network environment to improve data delivery though the network in congested settings which will ensure secured and robust delivery. The data transfer from S→D is calculated using the below equation,

$$E_{tx}\,(k,d) = E_{elec} * k + E_{amp} * k\,x\,d(square) \tag{4}$$

where, $E_{tx}\,(k,d)$ the is the energy consumed by sensor devices to transmit a data of size k over a distance d. E_{elec} is the energy consumed per bit to run the IoT process. E_{amp} is the energy consumed per bit per square meter by the transmitter. $k\ \&\ d$ denotes the size of data packet and distance.

2.2 Security Enhancement using GANs

By The main aim of this BIP-GANs protocol is to enhance security in the IoT environment. Two main processes happen during the GAN implementation:

- Anomaly detection
- Data generation for testing the robustness

The normal and anomaly traffic patterns are recorded initially to check the energy consumed by the sensor devices in IoT, transmission speed, lifetime, security, confidentiality, etc. The network is trained for both normal and anomaly packets generated by GANs. If malicious attacks and anomalies are detected during the training phase, the encryption levels are tightened by the administrators by blocking suspicious IPs, which triggers warning messages to the base station. The loss function is applied to train the GAN and classify the real and generated data. Through this security implementation, data tampering and DDoS attacks can be eliminated. As GANS generates diverse traffic scenarios, the network can be trained in any condition with both real and generated data. The protocol uses an adaptive learning method to log real-time security breaches and responds immediately to the sensor devices that transmit data to the destination, which helps ensure the IoT environment is under full protection. Table 1 shows the OMNET++ parameter settings to measure the performance metrics and to perform comparative analysis.

Table 1. Parameter Settings for OMNET Simulation & Values

Parameters	Values
$N/W\ Monitoring\ Value$	5000m x 3000m
$No.\ of\ Nodes\ (Count)$	500 - 2500
$IoT\ Network\ Range$	600 x 600 m^2
$Packet\ Size-Constant$	800 bits
$Mobility\ MM\ Model$	Random Way Point
$Traffic\ Nature\ (TN)$	Constant Bit Rate
$Nature\ of\ IOT$	Wireless Medium
$AIS\ Learning\ Rate\ in\ Bits$	75 m
$Initial\ Energy\ (IE)$	20 J
$Sensor\ Range\ \ (SR)$	10 m
$Total\ Constant\ Distance$	80 m
$Name\ of\ Simulator$	OMNET++
$Learning\ Rate\ (LR)$	0.5 (alpha)
$Sample\ Nodes-Total$	T = 50
$Num\ of\ Samples\ in\ Epocs$	M = 500
$Data\ Packet\ Width$	88 m
$Circuit\ Energy\ Consumtion$	E_{elec} = 50 nJ/bit

Continued on next page

Table 1 continued

$KDV\ Value\ Bifurcation$	$K_i to\ K_n$ times (AIS)
$Architecture$	GAN
$Training\ Iterations$	N (Max 200)
$AIS\ Bio\ L-Rate$	0.1
$HARQ\ Mechanism$	FEC + ARQ
$RLA\ Notation$	Q-learning
$Reward\ Fucniton\ Set$	D-Latency, D-Packet Loss, D-Throughput

2.3 Efficient Data Transmission using AIS

Efficient AIS holds the human potential of LRA (Learn, Remember, and Adapt) to detect new threats in IoT environments. In order to manage an efficient data transmission process, AIS enhances the optimal selection of sensor devices to transmit data in a robust manner. The following are the steps to transmit the data from source to destination. The protocol itself recognizes low-traffic routes and transmits the data dynamically from source to destination in a robust way, which increases the performance and life span.

- **Step 1:** Setup the network parameters by defining topology, bandwidth, and latency where N, L_{ij}, B, L represents node, link between node i and j, bandwidth and latency time.
- **Step 2:** Packet Size and transmission frequency is defined where, P, $F\ and\ E$ denotes packet size, transmission time and energy consumed.
- **Step 3:** Mutation and node selection using BIO-AIS to improve performance of IoT, where AIS generates mutations to select the node and deliver the data. Once the AIS generate the mutations, the updates are carried out to measure the fitness value $max(p)$.
- **Step 4:** Identify the finest path to measure the data loss, number of death nodes, and delay using AF (Affinity Function) as the metrics are measured in weight factors.
- **Step 5:** Select the path with the highest affinity factor, which is mutated for node selection.
- **Step 6:** Transmit the data to the IoT and monitor its performance. Calculate energy, transmission time, and life span.

The optimal path for data transmission is calculated using the below equation,

$$Path_{Optiml} = argmax\,(p)\,\frac{N\,(i=1)\,R_i}{l_i + T_i + C_i} \tag{5}$$

where, $P_{Optimal}$ is the optimal path, P represents all the possible search paths in the IoT search space, R_i, L_i, T_i, C_i represents reward, latency, throughput, and cost associated with path i. Even if there is a change in a change in network topology, the protocol itself will identify and detect anomalies in all situations to ensure robust end-to-end data delivery. This method adapts the LRA technique to learn all the intrinsic patterns from all types of networks to transmit the data. The protocol identifies real and fake network traffic to ensure that the data is transferred in high order with more security and confidentiality. A new block is generated by AIS called a crypto block, in which all the raw data is encoded, transmitted to the sensor devices, and decoded by the destiny node with a key called D-Key. The simulation is performed in a network testbed with an IoT network environment with the necessary parameter values. All the malicious data is removed, and perfect data is passed in the testbed, which increases the performance of IoT in large-scale environments.

2.4 Error Detection and Recovery using HARQ

To enhance fault tolerance, the BIP-GANs protocol uses a hybrid auto-repeat request method to detect and correct the error at the initial stage before the data is transmitted from source to destination. This helps administrators minimize the retransmission cost and save sensor energy to the maximum. The errors are identified using FEC codes, which allow the receiver to detect them. The data is captured and transmitted to the destination through a central monitoring system where each data point is associated with FEC codes. The HARQ model initiates data retransmission only for the corrected data rather than transmitting the whole. Once the corrected data is retransmitted, the original data is reconstructed and delivered to the destiny by the BIP-GANs protocol in the finest route. This selective retransmission technique saves energy for sensor nodes and boosts network performance in large-scale IoT environments. The following are the steps breakdown for ERC process:

- Bytes of data transmitted by the sensors

- HARQ model detects the error (5% of size)
- Correct the detected errors and ready for retransmission
- Retransmit only the corrected data in a finest route
- Activate HARQ in terms of reconstructing the data
- Reconstruction of data for transmission
- Deliver the data to destination
- Wait for next data transmission
- HARQ process repeats for all transmissions

2.5 BIP-GANs Architecture

The new AI-based BIP-GANs architecture shows the clear process of data transmission from source to destination, anomaly detection, error detection, and finest route selection in 4 different phases, which combine GANs, AIS, HARQ, and QL methods to enhance the robustness of the IoT long-range networks.

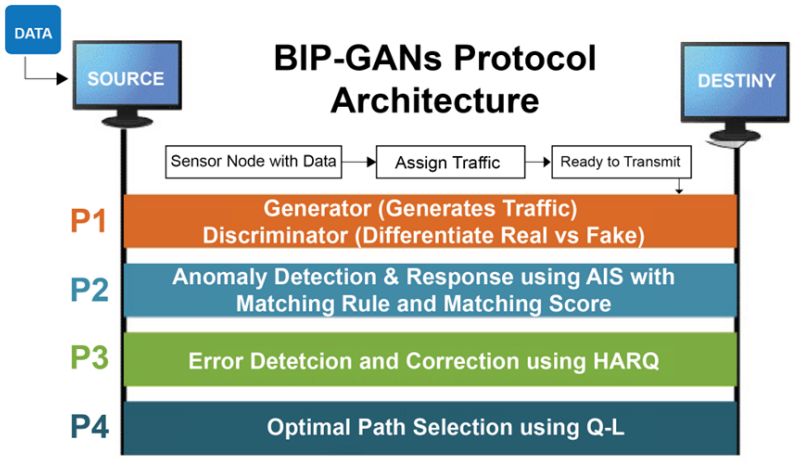

Fig 1. BIP-GANs Protocol Architecture

BIP-GANs for End to End Data Transmission Process

1. **Input:** Initialize IoT network with nodes and data traffic patterns
2. **Begin:** Start Network Monitoring using BIP-GANs

Anomaly Detection using BIP-GANs

3. Initialize GANs with G and D networks
$initialize\_IOTnetwork(nodes,\ traffic\_patterns)$
4. $start\_monitoring()$
5. $initialize\_GAN(G,\ D)$
6. $while\ !\,D\ is\_high\_accuracy()$:
7. $synt\_traffic\ =\ generator.generate()$ (Synthetic/Abnormal Traffic)
8. $D.train(real\_traffic,\ synt\_traffic)$
9. $G.update(D.feedback)$

AIS based security feature

10. Initialize Bio-AIS with memory and learning components $initialize\_BIOAIS(memory,\ learning)$
11. $while\ monitoring$
12. $if\ GANNetwork.detect_{anomaly(traffic)}$,
13. $BIOAIS.respond()$
14. $BIOAIS.update\_memory(threat\_info)$
15. Adapt AIS learning mechanisms to new threats, $BIOAIS.adapt()$

HARQ - Error Detection and Correction

Transmit data with FEC (Error Correction) codes

16. $transmit\_networkdata(FEC\_codes)$
17. $if\ receiver.detect\_networkerrors()$
18. $if\ networkerrors <= correction\_capability$
19. $receiver.correct\_networkerrors()$
20. $else$
21. $request\_retransmission()$
22. $retransmit_{networkerrors()}$
23. Retransmit only error datas segments

Q-Learning to discover Optimal Path Selection

24. Initialize QL-Queue learning for path selection
$initialize\_Q\_learning()$
25. $define\_QLaction\_sets()$
26. $while\ transmittin,\ performance\_metrics = measure\_network()$
27. $rewards = assign\_rewards(performance\_metrics)$
28. $update\_QLaction\_sets(rewards)$
29. $optimal\_path = select\_optimal\_path()$
30. $transmit\_data(optimal\_path)$
31. Assign rewards based on path performance
32. Update QLAS based on GANs generated real-time network conditions
33. Select finest path for data transmission from S→D
34. Transmit data in the finest path and calculate metrics
35. End

2.6 Performance Evaluation using OMNeT++

The AI-based bio-inspired secured data transmission BIP-GANs protocol is assessed in the OMNETC++ network simulation tool. OMNeT++ provides a dynamic environment to test network protocols to test the efficiency, reliability, and data integrity of the IoT networks, where flexibility and extensibility are high. A new IoT network test model is created, which includes node devices, communication protocols, and network topology. Various thresholds are introduced, such as node mobility, traffic, topology changes, network failure, etc., to test the performance and robustness of the proposed protocol and to check LoRa networks in all scenarios. Various thresholds are introduced, such as node mobility, traffic, topology changes, network failure, etc., to test the performance and robustness of the proposed protocol. To make sure the protocol detects real-time anomalies and withstands malicious attacks, synthetic network conditions are tested. A detailed comparative analysis is done with prevailing methods, which helps to highlight the performance of protocols.

2.7 Evaluation Metrics of BIP-GANs Framework

The evaluation metrics of the proposed IoT network protocol BIP-GANs is compared against the existing network data transmission protocols such as, EAP-IFBA [19], DNN-CSO [20], and ALO-DHT [21]. The following are the PEM equations used to derive the results.

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

$$Network\ Lifespan = \frac{Total\ Energy}{(Energy\ Consumption\ Rate)} \tag{7}$$

$$\%\ of\ Active\ Nodes = \frac{Total\ Nodes - Failed\ Nodes}{(Data\ Transmission\ Time)} \tag{8}$$

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

$$Delay_{End\ to\ End} = D_{Propogation} + D_{Transmission} + D_{Queueing} + D_{Processing} \tag{10}$$

$$Robustnes = \frac{Node\ Disjoint\ Path}{(Network\ Diameter)} \tag{11}$$

where, IE denotes network initial energy, TE denotes Total energy and DT denotes delay time.

- (E**DR) Energy Depletion R ate: Th**e EDR helps to calculate the energy depletion rate in the IoT network environment for an efficient data transmission process from S→D using BIP-GANs protocol.
- **(LNW) Lifespan of Network:** Calculates the entire data transmission duration of the network, which remains stable for efficient data transmission from S→D.
- **(PAC) Percentage of active nodes:** Measures the number of active nodes in the IoT environment after successful data transmission from one end to another end.
- **(DTS) Data Transmission Speed:** Calculates the data transmission speed (in seconds) to check whether the protocol is taking the finest route for efficient transmission.
- **(DR) Delay Rate :** Measures the latency time of the proposed BIP-GANs during data transmission in an IoT network environment.
- **(RT) Robustness:** To evaluate the security and confidentiality of the BIP-GANs protocol against malicious attacks and rapid network changes.

3 Results and Discussions

This chapter portrays the detailed findings and comparative analysis of the newly suggested AI-based bio-inspired framework BIP-GANs for secured data transmission in an IoT network environment. AIS and HARQ are unique methods to detect network anomalies, malicious attacks, and errors and retransmit the failure data to the destination at the right time. The scalability is tested to measure the performance of the network protocol to ensure whether it maintains reliability in a real-time scenario. The BIP-GANs protocol compares prevailing energy models such as EAP-IFBA [19], DNN-CSO [20], and ALO-DHT [21]. The new model shows promising results in terms of data transmission with high security in the network testbed and overcomes the drawbacks of the prevailing methods. Figures 2, 3, 4, 5, 6 and 7 show the OMNeT++ simulation graphs of the BIP-GANs protocol against prevailing methods. The X-axis shows the node counts, and the Y-axis shows the performance of all network protocols.

3.1 Energy Consumption Rate

The energy consumption rate of the proposed BIP-GANs is showcased in Figure 2. The new model optimizes the energy levels during data transmission in the IoT by discovering the best route and neutralizing malicious activities. In order to maximize energy, the GANs network is trained in diverse network scenarios that allow proactive adjustments. HARQ reduces multiple transmissions where it retransmits by detecting errors simultaneously. Dynamic power adjustments help to save node energy, which increases the sustainability and cost effectiveness of the IoT network. 6% energy loss is recorded for 500 NC, and 14% is recorded for 2250 NC, which is very low and effective in terms of energy consumption rate compared to existing methods.

Table 2. Energy Consumption Rate (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [19]	41	42	43	44	44	45	45	46
DNN-CSO [20]	37	37	38	38	39	39	40	40
ALO-DHT [21]	23	25	27	31	33	35	36	37
BIP-GANs (Proposed)	**6**	**7**	**9**	**11**	**12**	**13**	**14**	**14**

3.2 Lifespan of Network

The comparative analysis of the lifespan of the network of newly proposed BIP-GANs is portrayed in Figure 3. The network's sustainability is widely extended with the use of the bi-inspired GAN protocol. It continuously monitors and responds to threats

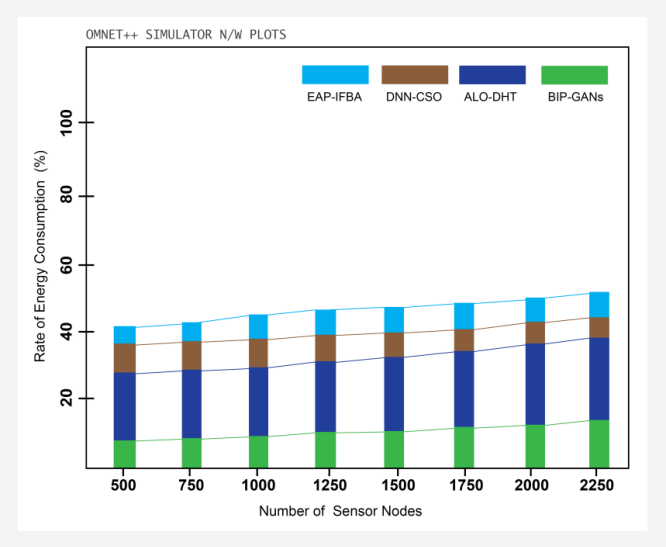

Fig 2. Comparative Analysis of Energy Consumption

and malicious attacks to ensure the IoT networks operate smoothly, which extends their longevity. BIP-GANs are tested under various scenarios, which help to increase data integrity, reliability, and sustainability. The operation time of individual nodes gets extended due to HARQ error detection and the retransmitting method. The network lifetime is boosted up to 99% and the proposed protocol withstands up to 83% for NC 2250.

Table 3. Lifespan of Network (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [19]	30	28	26	24	23	22	21	20
DNN-CSO [20]	75	73	72	70	68	66	64	60
ALO-DHT [21]	85	82	80	79	79	77	77	76
BIP-GANs (Proposed)	**99**	**11**	**11**	**11**	**13**	**11**	**14**	**83**

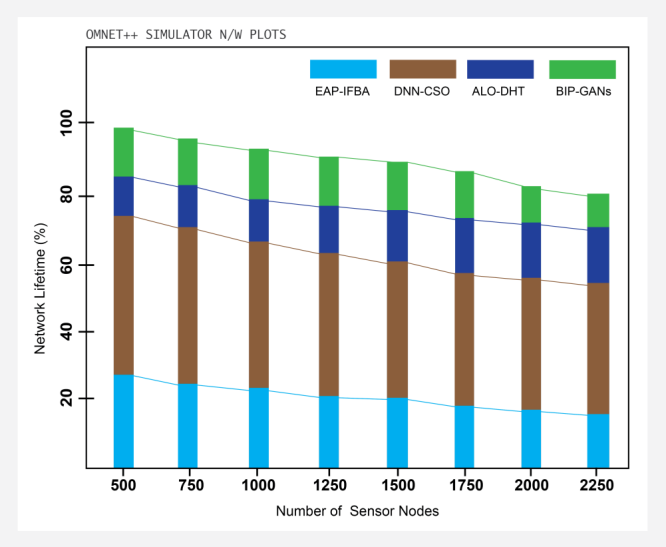

Fig 3. Comparative Analysis of Network Lifetime

3.3 Number of Active/Alive Nodes

Figure 4 portrays the node analysis of the proposed BIP-GANs protocol in terms of the number of active nodes after data transmission in the IoT network environment. As the protocol learns efficient data paths with optimal routing, the sensor nodes transmit data by handling traffic volumes under various topology changes. BIP-GANs dynamically allocate resources, detect malicious attacks and anomalies, and save data. It is observed that the proposed bio-inspired BIP-GANs method, EAP-IFBA, outperforms the existing computational models in terms of the percentage of active nodes. 98% of active nodes for NC 500 and goes up to 84% when NC is 2250 after successful data transmission from S→D in IoT, which is higher than other models.

Table 4. Percentage of Alive/Active Nodes (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [19]	30	27	25	23	21	19	18	17
DNN-CSO [20]	71	70	68	66	64	62	60	58
ALO-DHT [21]	83	82	81	80	79	78	77	76
BIP-GANs (Proposed)	**98**	**96**	**94**	**92**	**91**	**87**	**87**	**84**

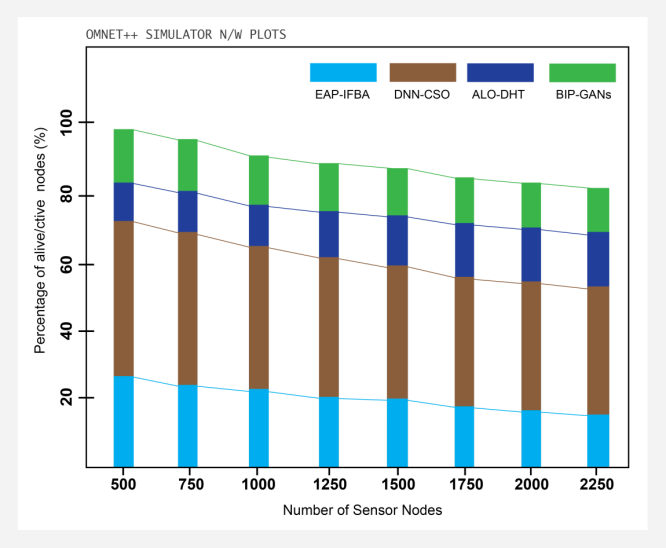

Fig 4. Comparative Analysis of Active Nodes

3.4 Data Transmission Speed

Figure 5 portrays the data transmission speed rate of the bio-inspired protocol BIP-GANs in IoT networks. The dynamic employment of bio inspired AIS, HARQ, and GANs dynamically boosts the speed rate by identifying the finest route, optimizing the shortest network paths, and reducing network congestion, which helps overall transmission time. The new protocol handles complex networks such as LoRA and transmits data with minimal errors in real-time, which increases the integrity and sustainability of IoT networks. The data transmission speed is reduced to 8 seconds when the NC is 500 and 10 seconds when the NC is 2250, which is high compared to the prevailing models.

Table 5. Data Transmission Speed (in seconds)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [19]	30	31	32	32	33	33	34	35
DNN-CSO [20]	27	27	27	27	28	28	28	29
ALO-DHT [21]	20	21	21	22	22	23	24	25
BIP-GANs (Proposed)	**8**	**8**	**8**	**8**	**9**	**9**	**9**	**10**

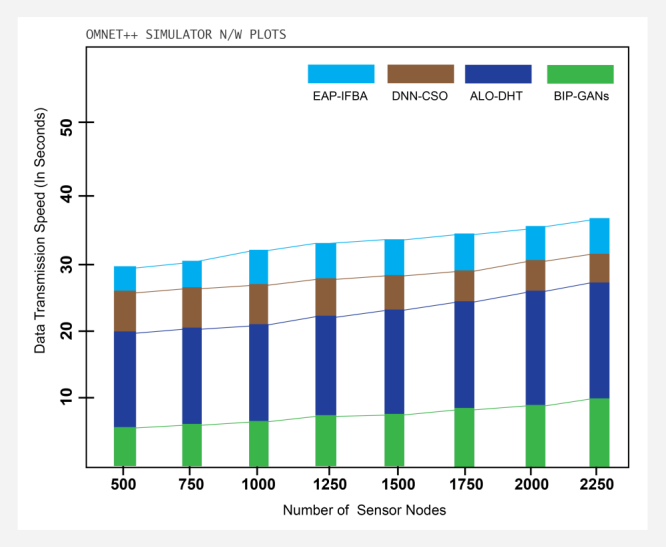

Fig 5. Comparative Analysis of Data Transmission Speed

3.5 Robustness (Security & Confidentiality) Analysis

The robustness comparative analysis is examined and portrayed in Figure 6. Responding to anomalies after detection is one of the unique methods of the BIP-GANs protocol, which helps security enhancement and data integrity. GANs simulate attacks under various network conditions, which enable the system to stand against failures, which potentially increase the data security and decrease the loss. 98% of the protocol secures the data and maintains robustness against malicious attacks, which is relatively high compared to the existing network models. BIP-GANs help IoT build a secured environment with high data transmission efficiency.

Table 6. Robustness (%)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [19]	30	27	25	24	22	19	18	19
DNN-CSO [20]	72	70	68	66	64	62	60	56
ALO-DHT [21]	83	82	81	80	79	78	77	75
BIP-GANs (Proposed)	**98**	**96**	**94**	**92**	**91**	**87**	**87**	**85**

3.6 End to End Delay Rate

Minimizing end-to-end data transmission delay is the key objective of any IoT environment. Here, the comparative analysis of protocols in terms of latency is projected in Figure 7. The combination of AIS, GANs, and HARQ potentially addresses the data transmission challenges where the packets are delivered in the optimal route. The new method decreases the retransmission time, waiting time, energy, and network traffic, which helps the packets travel from source to destination in a robust manner. The overall end-to-end delay time is reduced to 6 seconds when NC is 500 and 10 seconds when NC is 2250, which is more effective than other network models.

Table 7. Delay Time Rate (in seconds)

Node Counts / Protocols	500	750	1000	1250	1500	1750	2000	2250
EAP-IFBA [19]	28	29	30	30	31	32	32	33
DNN-CSO [20]	25	25	26	26	27	27	27	28
ALO-DHT [21]	18	18	19	20	21	22	23	24
BIP-GANs (Proposed)	**6**	**6**	**7**	**8**	**8**	**9**	**9**	**10**

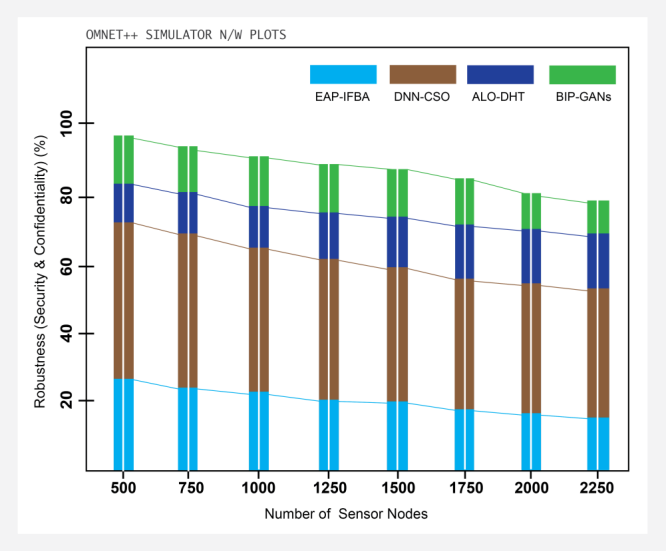

Fig 6. Comparative Analysis of Robustness

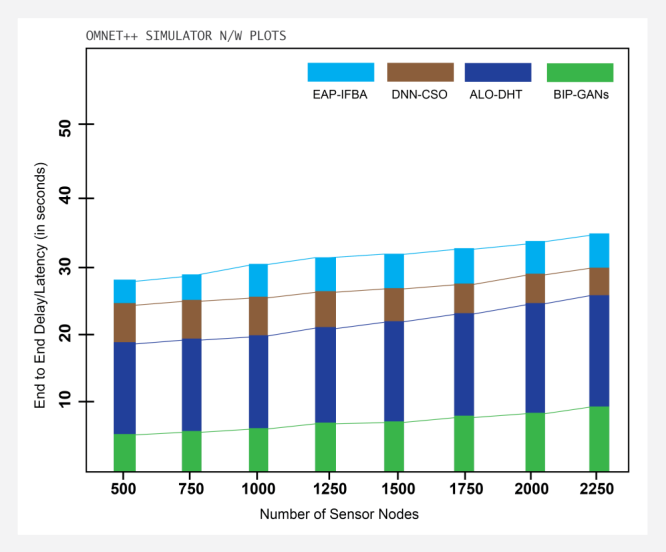

Fig 7. Comparative Analysis of Delay Rate

4 Conclusion

The BIP-GANs capture the data and transport it to the destination in a secured manner. GANs and AIS are the main components of the IoT model to transmit data efficiently. It carefully analyzes the collected observations for anomalies. Upon detecting anomalies, the self-learning system swiftly responds to secure data transmission and maintain performance. The HARQ error recovery method identifies data transmission and network errors during topology changes and retransmits the data to the destination address without any data loss. Queue learning action sets help the protocol identify the finest route where the data travels and reaches the end point, which increases data transmission speed. The proposed BIP-GANs IoT protocol was evaluated using a custom testbed equipped with IoT devices for real-time data collection. BIP-GANs effectively capture network errors, data transmission rates, optimal routing paths, the number of active sensor nodes post-transmission, sensor energy levels, and the overall lifetime of the IoT network. To address data forwarding and security issues, the protocol is tested in all conditions to record results up to 2500 node counts. The proven results are recorded with an energy consumption rate of 6%, 8 seconds data transmission speed, 6 seconds less delay rate, 98% robustness, 98.5% alive nodes, and 99% network life span. The results

highlight that the proposed model outperforms the baseline versions such as EAP-IFBA, DNN-CSO, and ALO-DHT.

The new BIP-GANs model performs better than existing models such as EAP-IFBA, DNN-CSO, and ALO-DHT. The limitations are that it's not very scalable, and optimizing parameters and adapting to rapidly changing environments can be difficult. In the future, we could enhance this model by incorporating compressive AI techniques to reduce computational complexity and minimize error rates, making it more efficient in dynamic network conditions.

References

1) Vaccari I, Orani V, Paglialonga A, Cambiaso E, Mongelli M. A Generative Adversarial Network (GAN) Technique for Internet of Medical Things Data. *Sensors*. 2021;21(11):1–14. Available from: https://doi.org/10.3390/s21113726.
2) Tsoulos IG, Tzallas A. Training Artificial Neural Networks Using a Global Optimization Method That Utilizes Neural Networks. *Artificial Intelligence (AI)*. 2023;4(3):1–18. Available from: https://doi.org/10.3390/ai4030027.
3) Lim W, Yong KSC, Lau BT, Tan CCL. Future of generative adversarial networks (GAN) for anomaly detection in network security: A review. *Computers & Security*. 2024;139:1–22. Available from: https://doi.org/10.1016/j.cose.2024.103733.
4) Anande TJ, Al-Saadi S, Leeson MS. Generative adversarial networks for network traffic feature generation. *International Journal of Computers and Applications*. 2023;45(4):297–305. Available from: https://doi.org/10.1080/1206212X.2023.2191072.
5) Abdulkadirov R, Lyakhov P, Nagornov N. Survey of Optimization Algorithms in Modern Neural Networks. *Mathematics* . 2023;11(11):1–37. Available from: https://doi.org/10.3390/math11112466.
6) Barnova K, Mikolasova M, Kahankova RV, Jaros R, Kawala-Sterniuk A, Snasel V, et al. Implementation of artificial intelligence and machine learning-based methods in brain–computer interaction. *Computers in Biology and Medicine*. 2023;163:1–24. Available from: https://doi.org/10.1016/j.compbiomed.2023.107135.
7) Nithyanandh S. Interrogation of Dynamic Node Link Failure by Utilizing Bio Inspired Techniques to Enhance Quality of Service in Wireless Sensor Networks. 2020. Available from: http://hdl.handle.net/10603/400513.
8) Madasamy N, Eldho KJ, Senthilnathan T, Deny J. A Novel Back-Propagation Neural Network for Intelligent Cyber-Physical Systems for Wireless Communications. *IETE Journal of Research*. 2024;70(2):1361–1373. Available from: https://doi.org/10.1080/03772063.2023.2173669.
9) Devi PA, Karthikeyan K. Bio Inspired Ant Colony Optimization Based Neighbor Node Selection and Enhanced Ad Hoc on Demand Distance Vector to Defending Against Black Hole Attack by Malicious Nodes in Mobile AD HOC Networks. *Journal of Computational and Theoretical Nanoscience*. 2018;15(9-10):3004–3011. Available from: https://doi.org/10.1166/jctn.2018.7581.
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. Available from: https://doi.org/10.17485/IJST/v13i16.19.
11) Devi PA, Karthikeyan K. Glowworm Swarm Optimization based Clustered on - Demand Load Balancing Scheme (GSO-COD-LBS) for Heterogeneous Mobile Ad hoc Networks. *International Journal of Computer Sciences and Engineering*. 2019;7(8):130–136. Available from: https://doi.org/10.26438/ijcse/v7i8.130136.
12) Eldho KJ. Impact of Unbalanced Classification on the Performance of Software Defect Prediction Models. *Indian Journal of Science and Technology*. 2022;15(6):237–242. Available from: https://doi.org/10.17485/IJST/v15i6.2193.
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):1574–1579. Available from: https://www.ijrte.org/wp-content/uploads/papers/v8i2/B2271078219.pdf.
14) Garg N, Petwal R, Wazid M, Singh DP, Das AK, Rodrigues JJPC. On the design of an AI-driven secure communication scheme for internet of medical things environment. *Digital Communications and Networks*. 2023;9(5):1080–1089. Available from: https://doi.org/10.1016/j.dcan.2022.04.009.
15) Mazhar T, Talpur DB, Shloul TA, Ghadi YY, Haq I, Ullah I, et al. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. *Brain Sciences*. 2023;13(4):1–30. Available from: https://doi.org/10.3390/brainsci13040683.
16) 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://doi.org/10.35940/ijstr.b2271.0986231.
17) Hasan MK, Habib AKMA, Islam S, Safie N, Abdullah SNHS, Pandey B. Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. *Energy Reports*. 2023;9(Supplement 10):1318–1326. Available from: https://doi.org/10.1016/j.egyr.2023.05.184.
18) Alhoraibi L, Alghazzawi D, Alhebshi R. Generative Adversarial Network-Based Data Augmentation for Enhancing Wireless Physical Layer Authentication. *Sensors*. 2024;24(2):1–22. Available from: https://doi.org/10.3390/s24020641.
19) 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. Available from: https://doi.org/10.17485/IJST/v16i34.1706.
20) Khilar R, Mariyappan K, Christo MS, Amutharaj J, Anitha T, Rajendran T, et al. Artificial Intelligence-Based Security Protocols to Resist Attacks in Internet of Things. *Wireless Communications and Mobile Computing*. 2022;2022:1–10. Available from: https://dx.doi.org/10.1155/2022/1440538.
21) Almalawi A, Hassan S, Fahad A, Khan AI. A Hybrid Cryptographic Mechanism for Secure Data Transmission in Edge AI Networks. *International Journal of Computational Intelligence Systems*. 2024;17(1):1–15. Available from: https://dx.doi.org/10.1007/s44196-024-00417-8.
22) 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. Available from: https://doi.org/10.17485/IJST/v17i10.3085.
23) Song J, Yuan Y, Pang W. SAIS: A Novel Bio-Inspired Artificial Immune System Based on Symbiotic Paradigm. 2024. Available from: https://doi.org/10.48550/arXiv.2402.07244.
24) Tumula S, Devi NR, Ramadevi Y, Padmalatha E, Uyyala R, Abualigah L, et al. An enhanced bio-inspired energy-efficient localization routing for mobile wireless sensor network. *International Journal of Communication Systems*. 2024;37(12). Available from: https://dx.doi.org/10.1002/dac.5803.
25) Jim LE, Islam N, Gregory MA. Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes. *Computers & Security*. 2022;113. Available from: https://dx.doi.org/10.1016/j.cose.2021.102538.

26) Pradhyumna P, Mohana. A Survey of Modern Deep Learning based Generative Adversarial Networks (GANs). In: 2022 6th International Conference on Computing Methodologies and Communication (ICCMC). IEEE. 2022;p. 1146–1152. Available from: https://doi.org/10.1109/ICCMC53470.2022.9753782.
27) Jozdani S, Chen D, Pouliot D, Johnson BA. A review and meta-analysis of Generative Adversarial Networks and their applications in remote sensing. *International Journal of Applied Earth Observation and Geoinformation*. 2022;108:1–22. Available from: https://dx.doi.org/10.1016/j.jag.2022.102734.