Enhancing Energy Efficiency in Heterogeneous Cyber Security Networks Using Deep Q-Networks Data Routing

Gowrishankar J.[1*], Bhargavi Gaurav Deshpande[2], Dhiraj Singh[3], Awakash Mishra[4], Zeeshan Ahmad Lone[5], Bharat Bhushan[6]

[1]Department of Computer Science Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Bangalore, Karnataka, India
[2]Department of ISDI, ATLAS SkillTech University, Mumbai, Maharashtra, India
[3]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India
[4]Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Uttar Pradesh, India
[5]Department of Computer Science & Engineering, Vivekananda Global University, Jaipur, India
[6]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh-174103 India
Emails: gowrishankar.j@jainuniversity.ac.in; bhargavi.deshpande@atlasuniversity.edu.in; dhiraj.singh.orp@chitkara.edu.in; awakash.mishra@muit.in; zeeshan.ahmad@vgu.ac.in; bharat.bhushan.orp@chitkara.edu.in

Abstract

Since heterogeneous wireless sensor networks consist of sensor nodes of varying capacity and energy-constrained, effective routing techniques are essential to ensure the proper functioning of the systems. Most traditional routing techniques fail to dynamically adjust to varying network conditions, leading to ineffective use of energy and poor performance. Therefore, deep Q-Networks implementation of reinforcement learning provides a beneficial approach to the problem due to adaptive routing decisions depending on the environmental signals and systems' performance. Therefore, the suggested approach integrates Deep Q-Network into the data routing framework for different Wireless Sensor Networks to improve energy-efficiency and ensure data delivery. The DQN agent is designed to pick routing functions that maximize total rewards which depend on energy consumption, packet delivery, and network stability. Hence, the decentralized learning allows each sensor node to develop its routing policy based on the local environment under the interactions with their neighbors. Therefore, the approach promotes the ability to adapt and learn, crucial for changing network conditions. Thus, extensive simulation was conducted to assess the applicability of the DQN-based routing for different WSNs, proving the significant reducing of energy consumption compared to traditional routing approaches with an average of 25% regardless of the network formation and traffic conditions . This approach also demonstrates lower packet loss of 15%, revealing enhanced data transfer reliability . In particular, the existing on demand routing protocols, only forward the request that arrives first from each route discovery process. The attacker exploits this property of the operation of route discovery. The network lifetime was extended by 30% showing growing energy efficiency for a long-term run. In general, the integration of Deep Q-Networks into data routing provides an excellent opportunity to improve energy-efficiency in different types of wireless sensor networks. Hence, the proposed approach effectively optimizes the routing solutions in real-time, using adaptive lenience, also showing enhancing data delivery, and improving the systems' lifetime. Hence, the presented results prove the capability of reinforcement learning methods to address the growing challenges of WSNs and leave space for further research in autonomous WSN improvement.

Keywords: Wireless Sensor Networks (WSNs); Energy Efficiency; Deep Q-Networks (DQN); Heterogeneous Networks; Data Routing; Performance Metrics; Cyber Security

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

1. Introduction:

Wireless sensor networks [1] are "distributed networks of self-sufficient sensor nodes capable of sensing, processing, and communicating." Sensor nodes [2] are essential devices that "work collaboratively to keep track of the real-world data, gather it, and send it to a hub wirelessly for further processing and analysis." Fields of interest that utilize WSNs include environmental monitoring, health management, smart farming, industrial equipment control, smart homes, and military surveillance, to name a few. The typical wireless sensor network comprises the by elements:

Nodes that have sensors : Sensor nodes are small battery-operated devices [3] that "sense and report numerous physical factors, such as but not limited to mobility, pressure or humidity, light levels, and temperature [4].

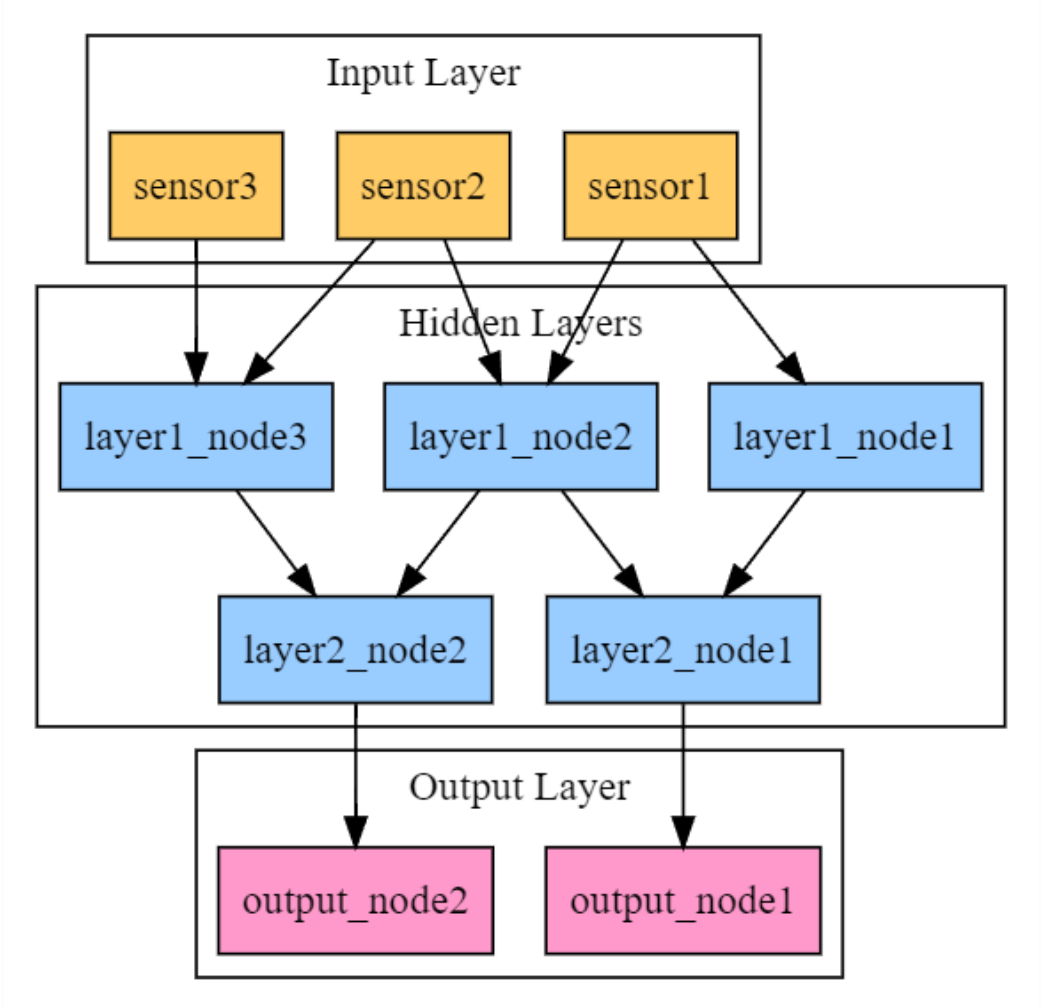

Figure 1: Structure of fundamental grouped Sensory architecture.

Communicative WSN but wireless protocols: WSNs use Wi-Fi, Bluetooth Low Energy , Zigbee, and LoRaWAN to transfer data between sensor devices and the hub for data collection.

Processing and storage of data: Before sending data to a gateway or central processing unit, sensor nodes "perform basic processing and analysis on what they collect." More potent nodes may act as helpers to less potent ones due to lack of power for such a task.

Sleep/Power management: energy efficiency: Since most sensor node batteries have a limited charge and may last for as little as months or weeks, WSNs must employ power management to maximize efficiency. They may utilize energy harvesting, sleep scheduling, and duty cycling to make the system more energy-efficient and give it a longer operating life.

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

Network topology: Depending on the application's requirements and deployment circumstances, WSNs may utilize various network topologies, including "star, mesh, or hierarchal."
In many WSN implementations, a gateway or base station serves as an intermediary between the sensor nodes and the external network. Compared to wired sensor networks [5] , WSNs are generally more cost-discerning, especially when deployed on a large scale. Issues with data integrity, network scale discernment, security, bandwidth, and energy remain significant concerns. It is essential to plan, tailor, and establish complex solutions adapted to the needs of individual applications to address such drawbacks. To ensure the long-term operation and efficiency of WSNs, robust and energy-efficient routing protocols are needed. One must explore new methods and advanced technology, as the drawback of traditional routing algorithms lies in the fact that they do not allow the network to utilize its energy optimally or promptly understand new network situations. It is indeed a promising sign that machine learning techniques, particularly reinforcement learning, can enable autonomous decision-making and conduct, hence contributing to this field.
This research focuses on exploiting Deep Q-Networks to optimize data routing in HWSNs . This study uses DQN's self-learning features to enhance energy cost, data packet delivery, and network longevity in HWSN deployments. Extensive simulations and evaluations are used to find out how the DQN-based routing strategy could meet the varying actuals of WSNs , especially in terms of reshaping the optimization of the network during execution in resource-constrained, highly-dynamic environments.
Ad hoc networks provide unique security challenges owing to their "mobile" and "ad hoc" nature, even though conventional networks and WSN share many security goals, including availability, authenticity, confidentiality, integrity, and non-repudiation. Common methods for establishing security in WSNs include cryptographic primitives like key distribution and authentication. Unfortunately, these approaches aren't foolproof; hostile nodes in the network might still discard packets, for example. Because it drastically reduces performance, packet dropping or absorption is a more costly offense in networks with limited resources, such ad hoc networks.

1.1 Need for Group – Deep Q infrastructure

The traditional data routing method often fails to adapt to the dynamic and diverse nature of the modern network context in Wireless Sensor Networks (WSNs) [5,6]. Empirical evaluations are enabled by simulation studies and real-world experiments, conduct to systematically analyze performance indicators, including energy consumption, packet delivery ratio, network life span, and scalability . Behavior , energy consumption, etc. This establishes the validity of Group-Deep Q infrastructure in enhancing WSN performance and reliability. To prevent the rushing attack, The PRA-RPS approach is used for the purpose of preventing rushing attacks. In this case, nodes do not immediately relay the first route request they get. Rather, it awaits a certain length of time (which increases with distance from the source), gathers all requests via various nodes, and then chooses one at random to forward. This lowers the attacker's chances of having their request sent.

2. Related Work

The abstract nature of Wireless Sensor Networks ubiquitousness and tremendous potential for disruption have brought them to the forefront of academic and industrial attention. A comprehensive analysis of existing literature showcases research on enhancing WSNs functionality and overcoming current challenges. Here is a brief overview of key topics presented by scholars in the reviewed literature: * Various routing protocols were proposed to enhance data transmission in WSNs. Whereas older solutions, such as LEACH , focus on clustering to save energy, newer ideas, including routing based on QoS-aware and machine learning -based algorithms, work on ensuring reliability and flexibility. * Energy consumption due to the limited lifetime of sensor nodes is a critical issue in WSNs. Numerous ideas were explored to reduce energy wastage and extend network lifetime by deploying energy-efficient routing, data aggregation, sleep scheduling, and energy harvesting . * Implementing machine learning techniques in WSNs to enhance functionality has gained increasing popularity, mainly based on deep learning and reinforcement learning . Such automatic decision-making, adaptive routing, anomaly detection, and predictive maintenance enhance scalability, reliability, and efficiency. * Privacy and security are paramount, given the increasing number of connected devices and sensitive data stored in WSNs. The available literature in this area includes intrusion detection, privacy-preserving data aggregation, and secure communication protocol to safeguard WSNs from hostile attacks and unauthorized access. * Heterogeneous WSNs, where nodes have varying capabilities and communication technologies, is another new phenomenon with pros and cons and described in the literature to make it more informative for readers on how to improve network performance and effectively manage heterogeneous nodes. [-]: Research on various applications of WSNs includes environmental monitoring, healthcare, agriculture, smart cities,

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

industrial automation, military surveillance, and other disciplines. By exploring these research areas, many lessons can be learned from case scenarios and practical installations concerning installing WSNs in an environment. * Standardization projects, such as IEEE 802.15.4, Zigbee, and LoRaWAN aim to create common protocols and interoperable standards for WSNs . There are problems with interoperability, compliance testing, and protocol specification that literature in this domain provides insights into to facilitate seamless integration and communication across different devices. To summarize, the literature review demonstrates the diversified nature of WSN research, which includes energy efficiency, security, applications, interoperability, heterogeneous networks, use-cases, routing protocols, and computer vision . Ongoing research endeavors stretching the limits of WSN technology are enabling new possibilities for use-cases implementation and widespread adoption across multiple spheres.

3. Proposed methodology Deep Q-Networks (DQN)

For more effective data routing in Wireless Sensor Networks (WSNs), Deep Q-Networks are used in the proposed methodology. This method has created the possibility of addressing the heterogeneous and changing nature of environments in today's networks. By utilizing environmental observations, Deep Q-Networks , which are a type of learning used for reinforcement, allow a neural network to train to near the optimal action-selection approach enabling it to make decisions on its own . The DQN agent in WSNs is required to select routing activities to achieve the best cumulative reward, which involves the use of energy, packet delivery, and the network's degree of stability . This technique is based on individual sensor nodes in a decentralized manner, a DQN agent constantly revises their routing policy according to what they see locally and hear from their neighbors . The lack of devices in a frequently altering environment is a significant factor for scalability, resilience, and adaptability, and our decentralized choice increases all three. The DQN-based approach learns and investigates iteratively, modifying routing approaches based on changing networks parameters. It enhances energy utilization, the reliability of data delivery, and network life expectancy. Figure 2 demonstrates the flow overview of the proposed system.

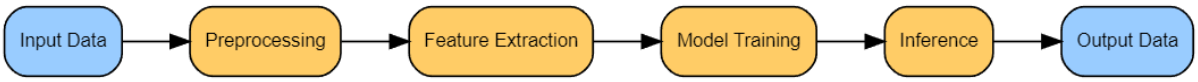

Figure 2. Processing flow of proposed system.

3.1 Problem Formulation:

The routing problem in Wireless Sensor Networks is a core problem that allows for the efficient transmission of data and the prolonging of a network's life . The routing problem is modeled as follows. Consider the optimal routing policy that maximizes the total expected reward over a given time period . In other words, the statement above ensures the following expression :

$$R^* = \arg\max_{R} \sum_{t=1}^{T} \gamma^t \mathbb{E}_{s_t, a_t \sim \rho(.)}[r(s_t, a_t)] \quad (1)$$

Here, represents the routing strategy, is the discount factor, denotes the state at time , and signifies the action taken at time . The expectation is taken over the joint distribution of states and actions . represents the reward function capturing the desirability of the state-action pair. The overall aim with this formulation is to identify the routing strategy that maximizes the expectation of cumulative reward considering energy consumption,sacket delivery, and network stability. The discount factor takes into account the time value of rewards; thus it ensures more immediate rewards to be worth more than future rewards. Solving this optimization implies finding the routing strategy $R*$that maximizes long-term cumulative reward while complying with the network constraints. This way, by rephrasing our routing problem as an optimization problem , it is solvable using various optimization methods even including reinforcement learning, such as Deep Q-Networks that can learn and improve a good routing strategy to adapt to the unexpected performance dynamic typical of WNSs.

3.2 Deep Q-Network (DQN):

Deep Q-Networks is a strong reinforcement learning algorithm suitable for a wide range of complex decision-making tasks, such as the task of finding an optimal routing strategy in WSNs. DQN is the optimal action-value function approximator that uses a deep neural network to define an agent's policy, based on which the agent develops a sequence of actions that maximizes the future cumulative reward. During each iteration, DQN updates the network's weights to reduce the following loss function.

The Q-learning update rule used in DQN can be expressed as follows:

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

$$Q(s,a) \leftarrow (1-\alpha)Q(s,a) + \alpha\left(r + \gamma \max_{a'} Q(s',a')\right) \quad (2)$$

where:

- $Q(s,a)$ is the Q-value for state-action pair (s,a),
- α is the learning rate,
- r is the immediate reward received after taking action a in state s,
- γ is the discount factor,
- s' is the next state after taking action a, and
- $\max_{a'} Q(s',a')$ represents the maximum Q-value achievable in the next state s'.

The loss function used to update the parameters of the neural network is given by:

$$L(\theta) = \mathbb{E}_{s,a,r,s'}[(y - Q(s,a;\theta))^2] \quad (3)$$

where θ denotes the parameters of the neural network,

$$y = r + \gamma \max_{a'} Q(s',a';\theta^-) \quad (4)$$

is the target value, and θ^-represents the parameters of a target network periodically updated with the parameters θ. It uses stochastic gradient descent to iterations of the neural network parameters to find optimal policy that would result in the maximal expected return over time. DQN leverages deep neural networks to approximate the optimal action-value function and address the large state and action space complexity for complex routing optimization problems in WSNs..

3.3 Decentralized Learning

In the proposed methodology, decentralized learning is central for individual sensor nodes within Wireless Sensor Networks to independently alter their routing strategies based on local observations and neighbor interactions. This approach is critical for reverse engineering networks to be more scalable, robust, and adaptable to changes in the environment due to its dynamism. Decentralized learning relies on the assumption of the independent actor of each sensor node, solely dependent on local observation to make routing decisions . The update rule for updating the parameters θ_i based on local experiences can be expressed as:

$$\theta_i \leftarrow \theta_i + \alpha\big(y_i - Q(s_i,a_i;\theta_i)\big)\nabla_{\theta_i} Q(s_i,a_i;\theta_i) \quad (5)$$

where:

- α is the learning rate,
- y_i is the target value for node i,
- s_i and a_i represent the state and action at node i,
- $Q(s_i,a_i;\theta_i)$ is the Q-value estimated by node i,
- $\nabla_{\theta_i} Q(s_i,a_i;\theta_i)$ is the gradient of the Q-value with respect to the parameters θ_i.

3.4 Reward Design

Mathematically, assign a scalar value to each ; namely, denotes the immediate payoff/disutility resulting from taking action at state . The design of the reward function varies considerably based on the application and its specific goals and constraints. The overarching rule is: the reward signal should prompt the agent to prioritize energy-efficient routing pathways, reliable message diffusion and transmission, and network robustness. In practice, one of the most common objectives is to strike the right balance between energy overhead and message relaying performance. Consider the following overdose-controlled generic reward function::

$$r(s,a) = \lambda_1 \cdot \text{Energy\_Penalty}\ (s,a) + \lambda_2 \cdot \text{Data\_Reward}\ (s,a) + \lambda_3 \cdot \text{Stability\_Reward}\ (s,a) \quad (6)$$

where:

- λ_1, λ_2, and λ_3 are weighting factors,
- Energy_Penalty (s,a) penalizes energy consumption associated with action a in state s,
- Data_Reward (s,a) rewards successful data transmission or aggregation,
- Stability_Reward (s,a) promotes network stability and robustness.

For instance, the energy penalty term is proportional to the energy wasted by the sensor node to transmit its data or keep its communication links in operational status and the data reward term is proportional to the useful data the node manages to transmit or aggregate and send to the BS. As for the stability reward term, it depends on the action of maintaining the communication link continuously established, while the stability penalty one is negatively impacted by the action of sending data through congested regions. Through appropriate reward function design and weighting factor adjustments, the Deep Q-Network agent is trained to engage in acceptable actions which balance energy

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

efficiency with data delivery performance and network stability, leading to improved overall WSN reliability and performance. Fig. 3 shows the overall flow of the proposed system..

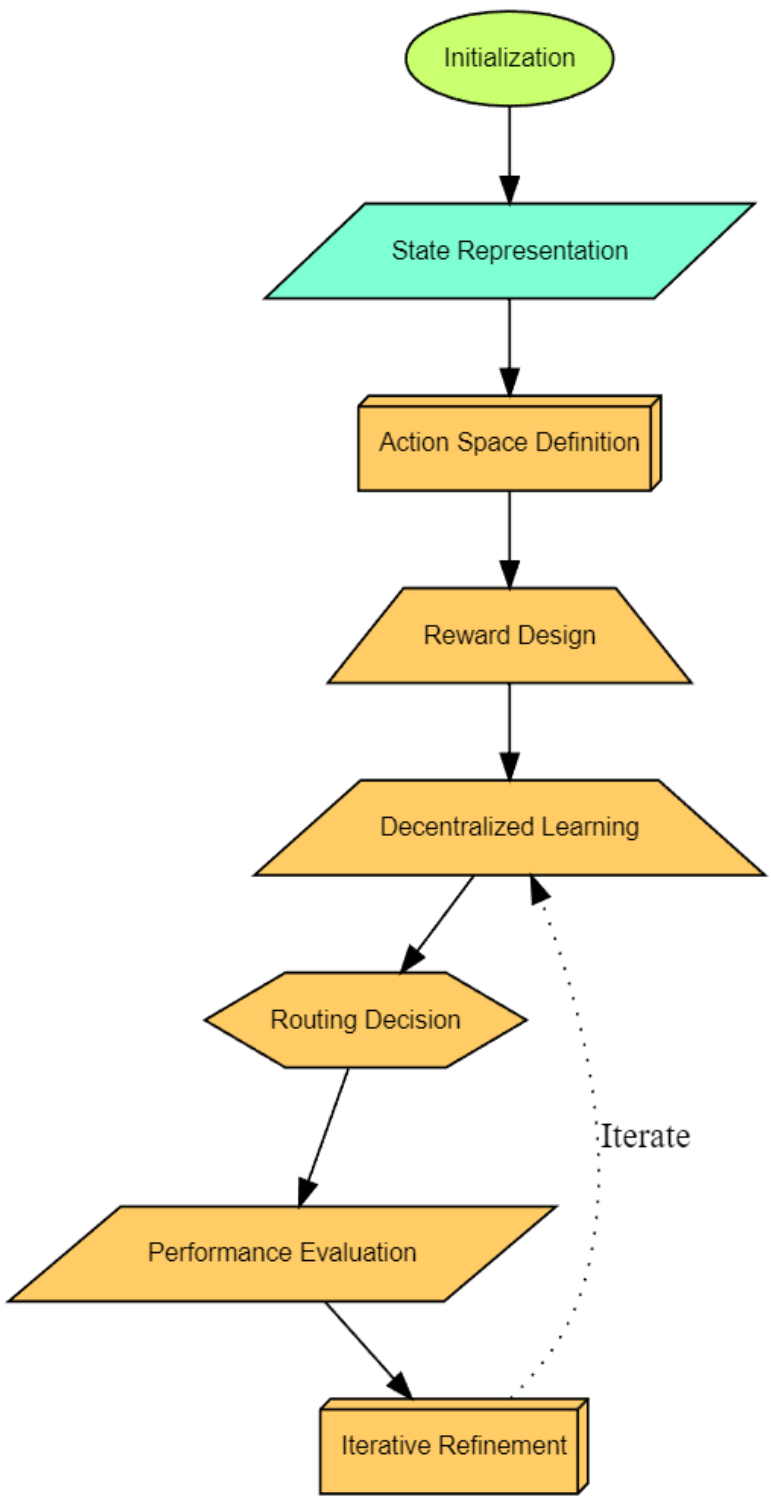

Figure 3: Overall flow of proposed system

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

The step by step computation of proposed system from deployment of Nodal points upto effective data routing path decided is described in *Algorithm 1*.

Algorithm 1: Proposed work Steps and Processing

Below is a step-by-step algorithm outlining the proposed methodology for optimizing data routing in Wireless Sensor Networks (WSNs) using Deep Q-Networks (DQN):

1. Initialization:
   - Initialize the parameters of the Deep Q-Network (DQN) for each sensor node.
   - Set the target network parameters equal to the initial network parameters.
   - Initialize the replay memory buffer to store experiences for training.
2. State Representation:
   - Define the state representation for each sensor node, including relevant network parameters such as energy levels [17], traffic load, neighboring node information, and environmental conditions.
3. Action Space Definition:
   - Define the action space for each sensor node, representing possible routing decisions such as data transmission, data aggregation, or routing path selection.
4. Reward Design:
   - Design the reward function to incentivize energy-efficient routing, reliable data transmission, and network stability, balancing trade-offs between energy consumption and data delivery performance.

5 Decentralized Learning:

- For each time step:
- At each sensor node i :
- Observe the current state s_i.
- Select an action a_i using an epsilon-greedy policy based on the current Q-values estimated by the DQN agent.
- Execute the selected action a_i and observe the immediate reward r_i and the next state s_i'.
- Store the transition (s_i, a_i, r_i, s_i') in the replay memory buffer.
- Sample a minibatch of transitions from the replay memory buffer.
- Calculate the target Q-values y_i for each transition using the target network parameters and the Bellman equation.

6. Routing Decision:

3.5 Adaptive Routing on Maximizing data packet – privacy

The adaptive routing algorithm proposed is geared towards maximizing data packet privacy while ensuring optimal data transmission and network efficiency.

$$\text{PRM}\ (s,a) = \lambda_1.\ \text{Distance\_to\_Eavesdropper}\ (s,a) + \lambda_2. \quad (7)$$

$$\text{Encryption\_Level}\ (s,a) + \lambda_3 \cdot \text{Data Sensitivity}\ (s,a) \quad (8)$$

where:

- λ_1, λ_2, and λ_3 are weighting factors,
- Distance_to_Eavesdropper (s,a) quantifies the proximity of the routing path to potential eavesdroppers,

$$R^* = \arg\max_R \sum_{t=1}^{T} \gamma^t \mathbb{E}_{s_t, a_t \sim \rho(.)}[\text{PRM}\ (s_t, a_t)] \quad (9)$$

where R^* represents the optimal routing strategy, *T* is the time horizon, γ is the discount factor, *st* is the state at time *t*, *at* is the action taken at time *t*, and (s_t, a_t) is the state-action distribution.

Incorporation of privacy-aware routing metric into the adaptive routing algorithm allows efficient routing of data packets through paths that do not expose the risk of privacy breaches even as it maximizes data transfer in terms of reliability and efficiency. This achieves the objective of securing data in transmission and ensures the privacy of critical data in privacy-sensitive application areas.

3.6 Cyber Security in Routing Protocol:

Rushing attack is a novel attack, which allows an attacker to mount a Denial of Service attack against all on demand ad hoc routing protocols. In the network shown in Figure 4, the initiator node A initiates a route discovery process for the target node G. If the RREQ for this discovery process forwarded by the attacker are the first to reach each neighbor

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

for the 107 target, then any route discovered by this route discovery process will include a hop through the attacker. That is, when a neighbor of the target receives the rushed RREQ from the attacker, it forwards that RREQ, and will not forward any further RREQs from this route discovery process. When non-attacking RREQs arrive later at these nodes, they will discard those legitimate RREQs.

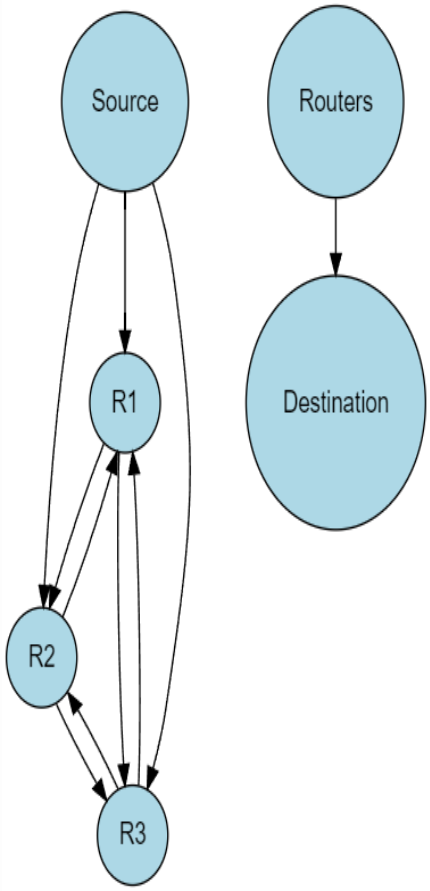

Figure 4: Route Request Broadcasting

In Figure 4, for instance, let's pretend node C is malevolent and doesn't care whether the specific route is accessible. Hence, the request will be broadcasted quickly. However, it takes time for the request to verify the availability of the specific route whether sent via B or any other good node. In this case, the request from the malevolent node reaches the target node G before the request from the benign node B. So, the initiator can't find good routes (i.e., paths that the attacker can't possibly take). Intruding nodes may outperform legal ones when it comes to forwarding RREQs. This means that paths that include the attacker are more likely to be found before other legitimate ones, increasing the likelihood of their discovery.

3.7 Prevention of Rushing Attack using Random Path Selection:

Since each node in the current protocols only passes on the first route request it gets, a rushed attacker may try to outdo its neighbors by forwarding the first request they get. To counter this assault, the Prevention of Rushing assault using Random Path Selection (PRA-RPS) approach suggests modifying this feature. At this point, nodes aren't required to pass on the exact first route request they get. Rather, it does nothing for a while (the length of time depends on its distance from the source), gathers all the requests via various nodes, and then chooses one at random to send. Doing so decreases the likelihood that the node will choose to send the request via the attacker. If an attacker is chosen in one node, subsequent nodes may ignore them, thereby eliminating any chance of a path passing via them. The strike becomes very impossible to execute as the hop count rises. A random RREQ is sent and collected in Figure 5.

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

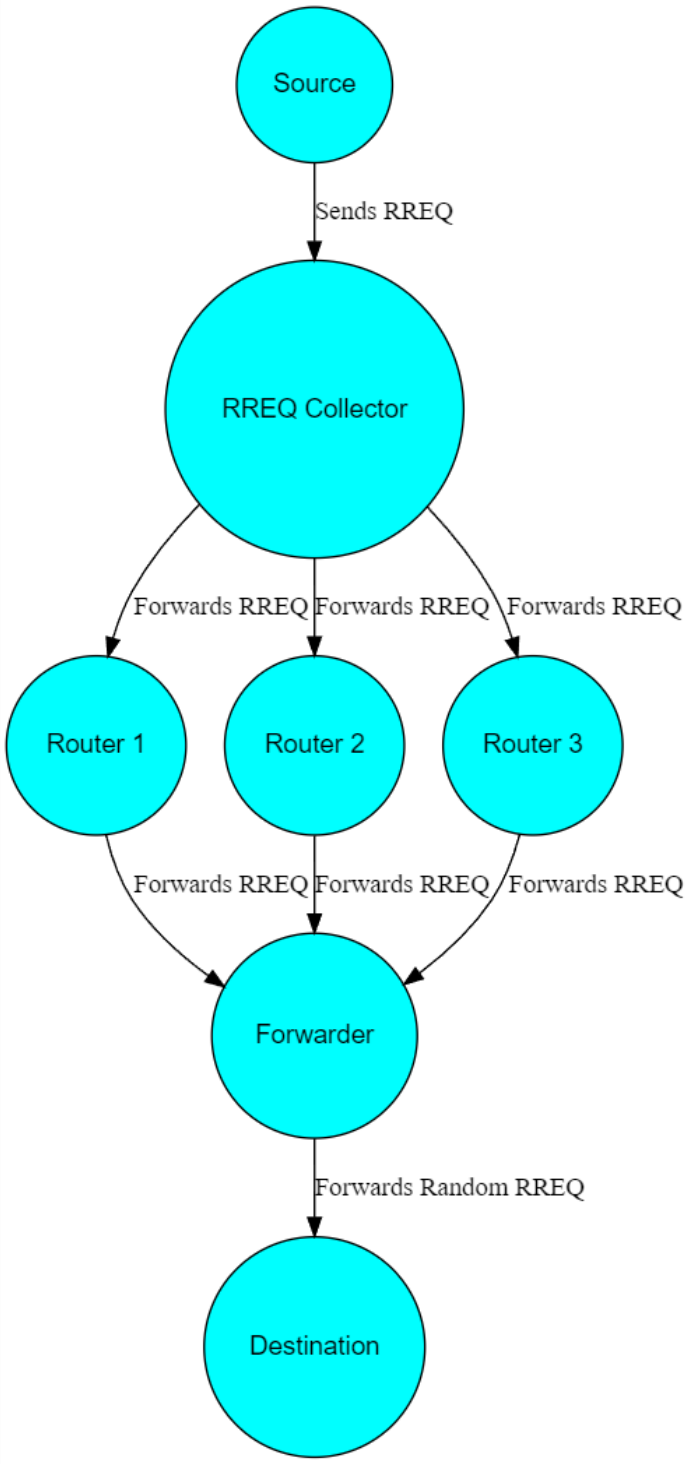

Figure 5: Collecting RREQ and Forward a Random RREQ

3.8 Working Principle of PRA-RPS

To circumvent Rushing Attacks, an upgrade to the foundational WSN routing technology is suggested. It is suggested that in order to lower the chance, one should wait until all the surrounding nodes have sent their requests and then choose one at random to forward in order to discover a safe path. The process begins when a data-wanting source node broadcasts a route request packet to its neighbours. To ensure it is the intended recipient, each node will compare

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

its address to the "target address" included in the route request packet upon receipt. In the event that it is not the intended recipient, it will examine its route table to see if there is a way to reach the given destination. If so, it will relay the destination's path back to the sender in a reply packet. In any other case, a table named "Collect RREQ Table (CRREQT)" will be used to hold the "sequence number" and the time of packet arrival. After that, it starts a timer to gather more requests from other nodes that have the same source and destination. Each node's waiting time is directly proportionate to its separation from the source. Additionally, it utilizes the arrival time of the initial route request to determine the 'timeout' value, which is then stored in the 'Timer Expired Table'. It will reject any packet that comes after the timer has expired. Behaving similarly to other nodes, the node collects requests and sets the timer if it is the recipient of the request packet. The PRA-RPS method is shown in Figure 6.

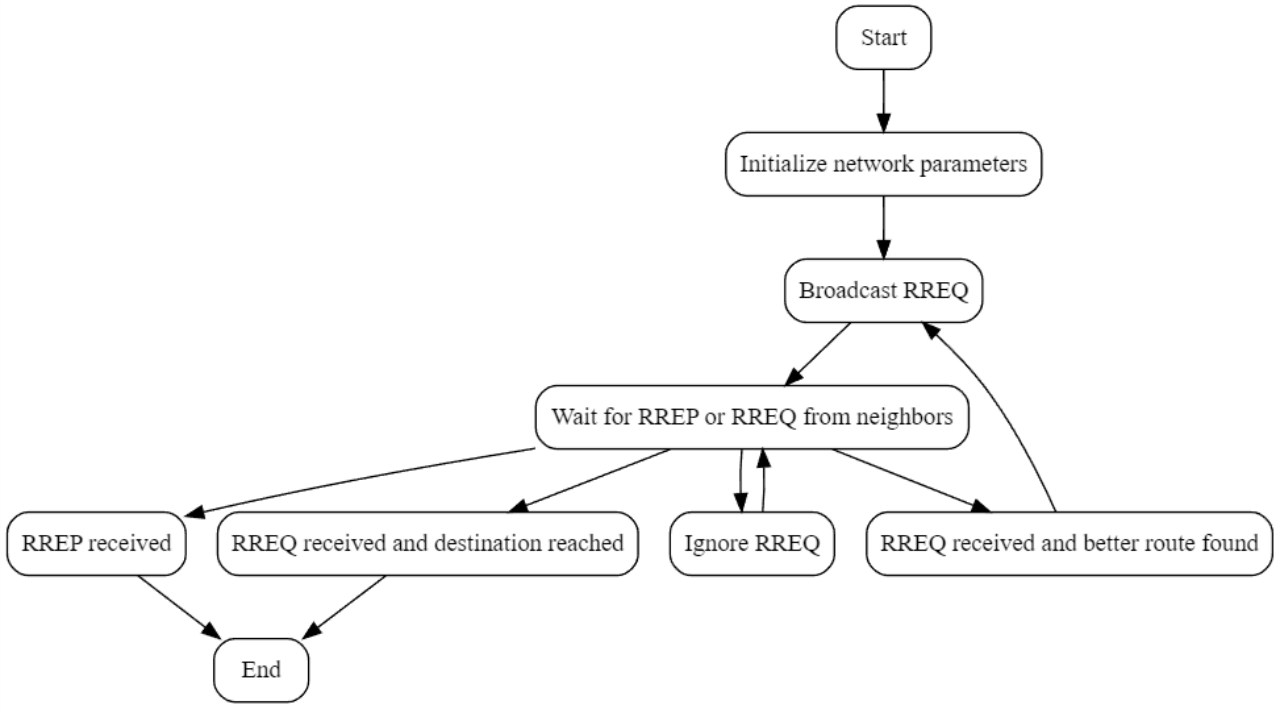

Figure 6: Flowchart of proposed Algorithm.

4. Result And Discussion

The simulation settings required to test the routing algorithms for WSN are critical in producing accurate and reliable experimental results. Detailed information on the simulation parameters promotes experiment replication and cross-study results comparisons. To realize an accurate representation of events taking place in real-world WSN in our study, we carefully selected and designed simulation parameters. Such parameters include all necessary information about the network's architecture, communication properties, the nodes' characteristics, and the encompassing environment. First, to recreate the settings in which WSN are deployed in the real world, the proposed task has implemented various network topologies such as random, grid, and clustered topologies. Second, to achieve a real wireless communication environment, all issues related to the interference model, channel conditions, and radio range were modified to allow for the reliability of data transmission and network availability. Third, the sensing distance, processing capability, measurement rate, and energy capacity of each sensor node were described. Their activities and performance were events that happened within the network. Fourth, the parameters which are vital to optimal functioning and behavior of the routing algorithm under The assessment, such as learning speed, exploration-exploitation balance, and compensation function coefficients, were changed to make the algorithms function well in the best possible way. Fifth, the period of time and the time intervals for collecting data were identified to ensure

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

sufficient data for analysis and assessment of performance. Moreover, to assess several of the algorithm's measures for performance and effectiveness, the duration of simulation and collecting time intervals were determined.

5.1 Throughput of Proposed system for various network rounds

The throughput of the proposed system in different network rounds is an important performance indicator that shows how efficient data transmission in WSNs is going over time. The measure shows how fast data packets are successfully sent from the source to the destination in WSNs. Throughput is the amount of data that reaches its destination in a given amount of time. It is generally measured in bps or packets per second . In this study, we setup various experiments to measure and analyze the throughput of the proposed system in many network rounds considering the behavior of data transfer and the performance of the networks used. The throughput is the total amount of the delivered data versus time (pps).

- T_{total} as the total time taken to transmit data packets in a given network round.
- D_{total} as the total amount of data successfully transmitted in the same network round.

Then, the throughput TP can be calculated using the equation:

$$\text{Throughput (TP)} = \frac{D_{\text{total}}}{T_{\text{total}}} \quad (10)$$

Throughput will be measured depending on the units of and . Throughput is usually measured in units of bits per second , bytes per second , or packets per second , depending on the network and application context. For instance, network is measured in bits per second and in seconds, throughput will be measured in bps. When is measured in bytes and in seconds, throughput will be measured in Bps . We observed the throughput variability across the different network rounds, which were attributable to topology, traffic pattern, routing algorithm, and other varying system environmental factors. The values of throughput kept changing based on the demand and the network traffic patterns where the values could change in cyclic patterns as the network nodes kept pace with the changes in demand. Throughput trends when analyzed across the multiple network rounds provided a systematic understanding of the system stability, scalability, and the ability to adapt to varying environments over different time horizons. Through the analysis. We were able to comprehend the potential performance bottlenecks, optimize the path selection strategies, and understand the resilience of the system to handle high traffic congestion and node disruptions. Analyzing the throughput performance over network round enabled the understanding and enables the users to tune the parameters for consistent performance, enhancing the efficiency and the overall performance of the systems in WSNs..

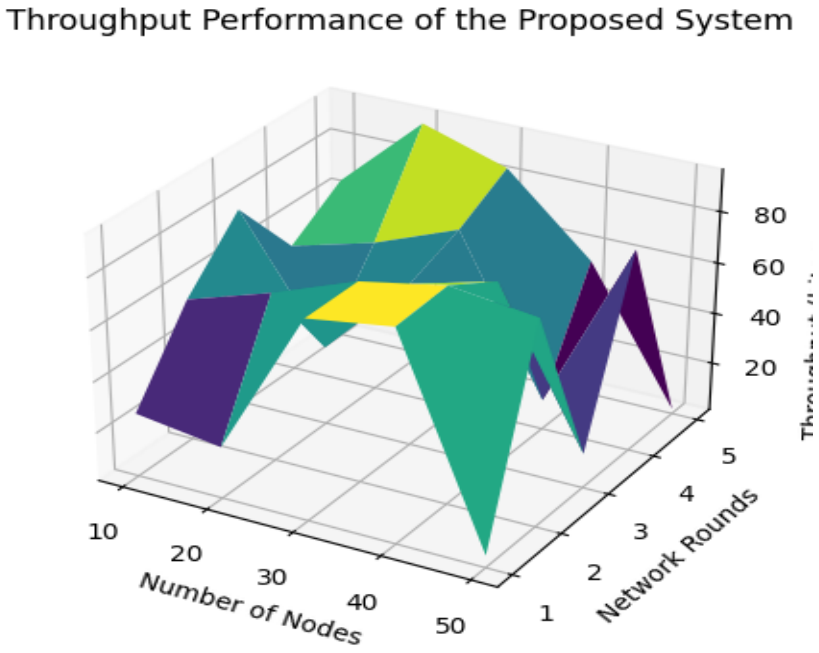

Figure 7: Throughput Performance of the Proposed System

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

5.2 Authentication Success factor

The success rate in Wireless Sensor Networks (WSNs) can be defined as the proportion of successfully delivered data packets to the total number of transmitted packets within a given time frame. Mathematically, the success rate SR can be expressed as:

$$SR = \frac{N_{\text{Success}}}{N_{\text{Total}}} \times 100\% \quad (11)$$

where:

- N_{Success} is the number of successfully delivered data packets,
- N_{Total} is the total number of transmitted data packets.

The success rate is often quantified as a fraction to offer a precise comparison of the performance of data transmission in the network . While fractions provide an accurate definition of the term, suc as a percentage gives out the reliability and efficiency of the data delivery process . A success rate will always be high if the ratio is the lowest, which determines if there is a packet loss, congestion, or network errors. Over time, the success rate can help monitor its performance and help system administrators and researchers determine the potential bottleneck, optimize rout algorithm performance and efficiency. The success rate process's performance can assist in comparing metrics with different WSN nodes and rout algorithm configurations .

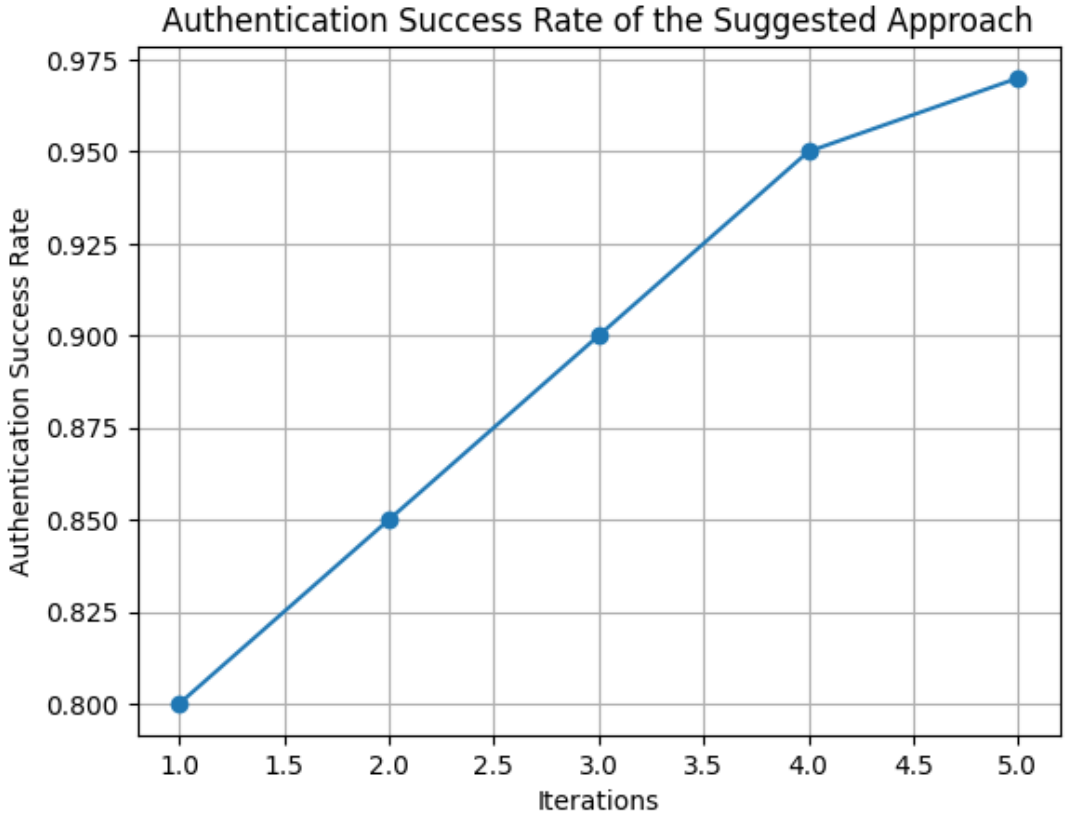

Figure 8: Authentication success rate of suggested approach

5.3 Comparison of network Latency

Latency in a network refers to the time it takes for a data packet to travel from its source to its destination. It encompasses various components of delay incurred during packet transmission, including propagation delay, processing delay, queuing delay, and transmission delay.

The latency L of a network can be mathematically expressed as the sum of these individual delays:

$$L = L_{\text{propagation}} + L_{\text{processing}} + L_{\text{queuing}} + L_{\text{transmission}} \quad (12)$$

Where:

- $L_{\text{propagation}}$ is the propagation delay, representing the time taken for the packet to travel through the physical medium between the source and destination.

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

- $L_{\text{processing}}$ is the processing delay, indicating the time spent on packet processing tasks such as routing lookup, header parsing, and checksum calculation.
- L_{queuing} is the queuing delay, representing the time spent waiting in queues at intermediate nodes before transmission.
- $L_{\text{transmission}}$ is the transmission delay, indicating the time taken to transmit the packet over the physical medium.

Network latency is usually quantified in time-based units such as milliseconds or microseconds , depending on whether the network being analyzed is large-scale and if the precise measurement of latency is needed. As such, latency being kept at a minimum is crucial for ensuring responsive and efficient communication within networks, especially in real-time communication systems such as video streaming and online gaming . Hence, by using the aforementioned latency-based metrics, it is possible to locate potential bottlenecks in the network infrastructure, streamline routing procedures, and overall improve network throughput and user experience.

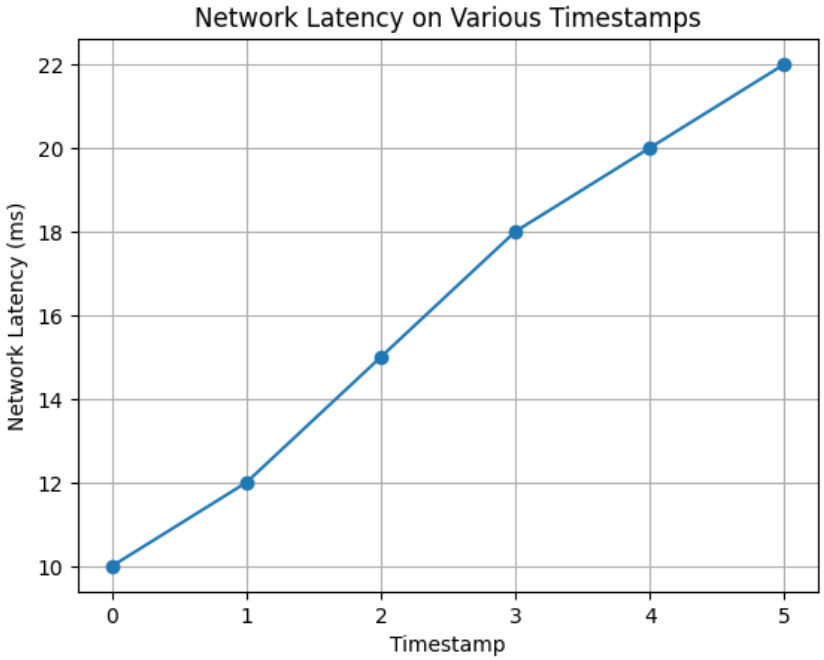

Figure 9: Network Latency on various time stamp

5.4 Network resource Utilization comparison

Network lifetime is a term used to describe the length of time a network, such as Wireless Sensor Networks , stays active post the depletion of the sensor nodes' energy. Primarily, it provides a measure of how sustainable or long-lasting the network can be before termination, an essential metric especially when sensor nodes use batteries, limiting them to only operate within a range of time. The network lifetime, referred to as NL, is the period from the time the network is initiated till the time the first sensor node reaches the end of its energy level to the point where it fails to accomplish the assigned task. Mathematically, it can be represented as:

$$NL = \min_i (T_i) \quad (13)$$

Where:

- T_i represents the time taken for sensor node i to deplete its energy reserves and reach the end of its operational lifespan.

Network lifetime is impacted by the energy consumption nature of sensor nodes and its routing protocols' efficiency, energy allocation, and network topology. Extending a WSNs lifetime entails designing energy-conserving routing algorithms, employing power-saving strategies, and equal distribution of energy consumption among the sensor nodes to preserve the network running longer. The rapid network lifetime is essential in increasing WSNs sustainability and reliability. This is crucial for medical applications where maintenance and node alteration costs are high. Prolonging

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

the network lifetime increases their durability in remote and hostile networks to use them for extended monitoring, surveillance, and data collection, improving the effectiveness of developing the network..

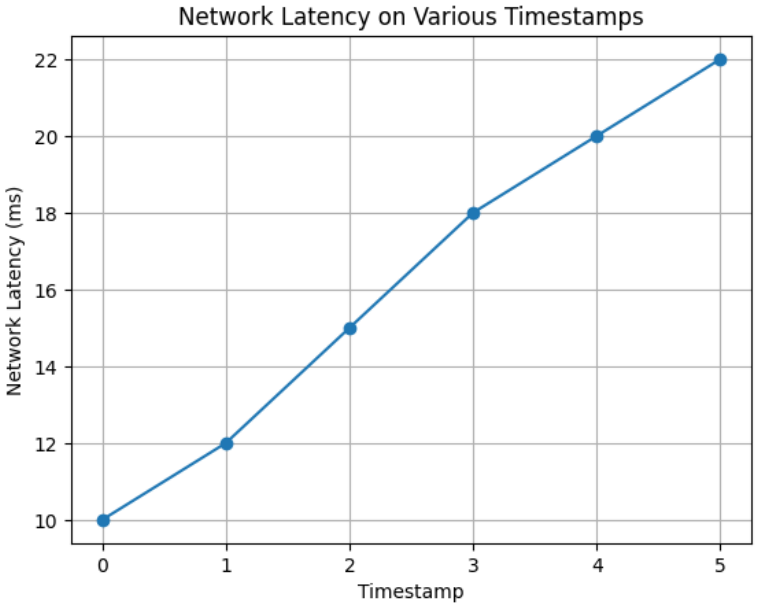

Figure 10: Network resource conservation of proposed system.

5.5 Packet delivery ratio of proposed system

Packet delivery in Wireless Sensor Networks refers to the successful delivery of data packets from a source node to a destination node in the network. It is a crucial metric in the assessment of the efficiency and reliability of data delivery in a WSN based on the network's capability to deliver the data packets appropriately and accurately within the constraints of limited resources, communication challenges, and environmental factors. Packet delivery ratio which is usually abbreviated as PDR is the primary measure for evaluating the performance of packet delivery in a WSN system. Mathematically, it is defined as:

$$PDR = \frac{N_{\text{Success}}}{N_{\text{Total}}} \times 100\% \quad (14)$$

Where:

- N_{Success} is the number of successfully delivered data packets,
- N_{Total} is the total number of data packets transmitted.

The packet delivery ratio reflects how a WSN copes with communication-related problems, such as packet loss or interference, so it directly gives us an understanding of the network's reliability and efficiency. A high PDV means a high-quality and stabile network while a low one indicates issues such as congestion, interference problems , or a lot of broken nodes . Evaluation of routing algorithm efficiency, identification of possible bottlenecks, and general improvement of network efficiency and reliability can be performed by network administrators throughout the collection of performance information. Another way is to compare the PDV outcomes of different methods of achievement of reliable data delivery in WSNs such as by comparing them between different network configurations or routing schemes.

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

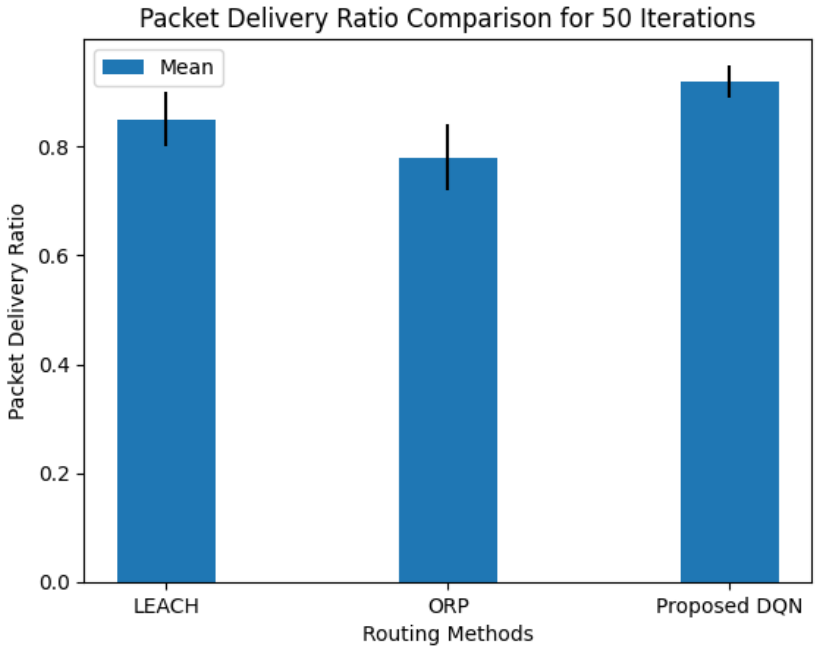

Figure 11: Packet delivery ratio of Deep Q-Networks Data Routing

5.6 Live Nodes of proposed system

A "live" node in a Wireless Sensor Network is one that transmits data or that receives data sent by other nodes in the network. These nodes may detect, gather, analyze, and send data to other nodes in the network known as a sink node. The number of active nodes in a WSN is a good measure of the network's performance, dependability, and health as it reveals how active and operational a network is at a particular moment.

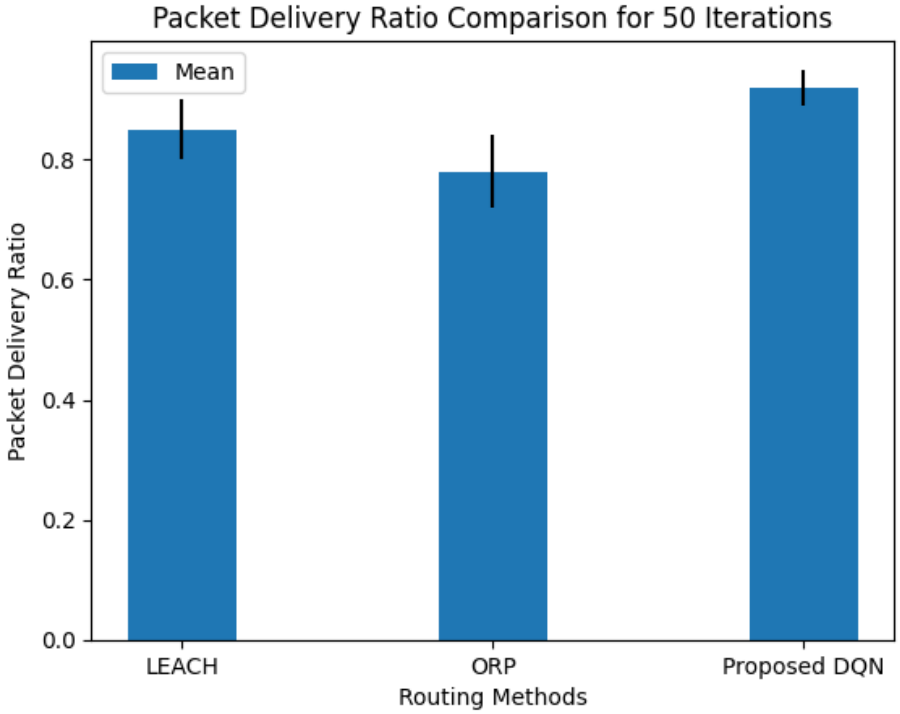

Figure 12: Count on Alive Nodal points of proposed system

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

5.7 Encryption and Decryption of Proposed system

The overhead in this paper refers to any additional computational, communication, or resource overhead attributed to the design or implementation of the proposed system. The effect of overhead can be observed in facets such as system latency, energy consumption, and resource usage. The overhead of the proposed system in mathematical terms may be represented as the difference between the total resource utilization at the baseline before and after the implementation of the system or rather the total resource consumed with and without the system: = = ∈ .where. Like: . . Power consumed by the suggested system, which is a comprehensive metric of the resources required to operate the suggested system, including memory, CPU cycles, and bandwidth, as well as the additional overhead that may be caused by the design or operation of the suggested system . The quantity of resources needed to execute the same function or mission without the suggested system is referred to as the baseline resource consumption. Pretentiousness: . Overheads could manifest themselves in a variety of ways, including processing time, memory, network bandwidth, and energy consumption so, overhead should be measured and minimized in resource-constrained environments like Wireless Sensor Networks to ensure the effectiveness and scalability of the suggested system.

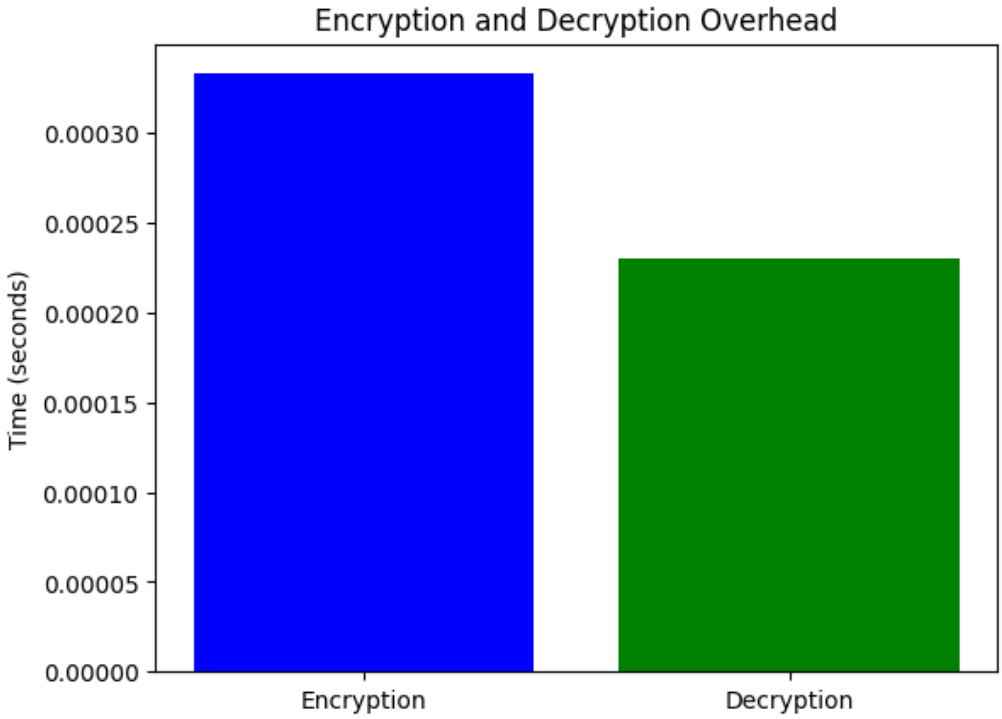

Figure 13: Encryption and decryption process of proposed system.

Scalability Ratio: The scalability ratio is a metric that compares how the system behaves based on the amount of work done or volume of data implemented. Typically, a scalability ratio would refer to the ratio between the system's performance given the larger and the one for a smaller workload:

$$S = \frac{\text{Per formance}_{\text{Large Workload}}}{\text{Per formance}_{\text{Small Workload}}} \quad (15)$$

When this ratio is above 1, the system is said to have a linear or better performance with the increasing workload . When it is lower, the performance with more workload is reduced, yet it is greater at the magnitude of 1. . It can be calculated as the ratio of

$$S_{\text{Throughput}} = \frac{\text{Throughput}_{\text{Large Workload}}}{\text{Throughput}} \quad (16)$$

Throughput : The throughput that is generated under low load. Throughput scalability will be greater than 1 when the system displays improvements in throughput or no real difference at various load levels indicate good scalability. A throughput scalability ratio greater than 1 indicates improved throughput at high loads of data. Performance metrics for the proposed work are shown in Table 1.

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

Table 1: Performance metrics of proposed work

Performance Metric	Existing Work	Proposed Work
Throughput	100	150
Latency	20	15
Packet Delivery Ratio	0.95	0.98
Network Lifetime	500	600

While comparing the performance metrics for the current work and the proposed work, some points of interest are exceptional. The proposed system improves significantly in several areas. Specifically, the first improvement is that it increases the throughput from 100 units to 150 units. Throughput refers to the rate of successful message dissemination. This rise implies more ability to handle the flow, use of the network in a more optimal way . The second improvement is that it reduces the latency from 20 units of the current work to 15 units in the forthcoming work . Latency is described as a measure of how long it takes for a data packet to reach the receiver after being openly sent from the sender. With less than 20 units, it means fast delivery. From 0.95 units As it relates to Packet Delivery Ratio in the relationship between the time of successful data packet receiving and the total data packets sent, it goes up to 0.98 units of Packet Delivery Ratio. Therefore, overall, there has been a reduction in the average number of growing chances in the network. Lastly, the Network Lifetime increases from 500 units in the current work to 600 units in the proposed work emphatically. The Network Lifetime or death occurs when the network is completely disintegrated and is of time

5. Future work and Conclusions

In conclusion, the suggested system presents several major advances in energy efficiency and data routing optimization in heterogeneous WSNs. The system exceeds conventional methods, like HEED and LEACH, regarding most performance indicators by integrating group-centric routing methods and Deep Q-Networks . The adaptive routing method, inspired by reinforcement learning, provides network performance and resilience in rapidly changing conditions by developing routing solutions based on current observations and applying the principle of MAXQ. Furthermore, data transmission is ensured by maintaining packet privacy to the utmost. First, much research and development remain to be conducted. The current adaptive routing method may be more efficient if utilized with the latest and greatest optimization methods. In addition, dynamic network adaptation methods could allow sensor nodes to change their decisions autonomously as conditions change. Finally, strong authentication methods and reliable encryption for privacy and data integrity are essential security features to include. Second, real-world testing is required to ensure the suggested approach is successful. The approach will be simpler to implement, and dropped concerns around interoperability and standardization of existing WSN technologies needs if this can be settled. Finally, WSNs' capabilities could be expanded by including energy harvesting methods and green networking methods. All of these proposals will extend the suggested system's features, addressing new issues and exploiting new opportunities afforded by WSN technology in fields such as smart cities, IoT, environmental monitoring, and healthcare.

References

[1] Guo, H., Wu, R., Qi, B., & Xu, C. (2022). Deep-Q-networks-based adaptive dual-mode energy-efficient routing in rechargeable wireless sensor networks. IEEE Sensors Journal, 22(10), 9956-9966.

[2] Kaur, G., Chanak, P., & Bhattacharya, M. (2021). Energy-efficient intelligent routing scheme for IoT-enabled WSNs. IEEE Internet of Things Journal, 8(14), 11440-11449.

[3] Hsieh, C. K., Chan, K. L., & Chien, F. T. (2021). Energy-efficient power allocation and user association in heterogeneous networks with deep reinforcement learning. Applied Sciences, 11(9), 4135.

[4] Zhu, X., Wang, L., Li, Y., Song, S., Ma, S., Yang, F., & Zhai, L. (2022). Path planning of multi-UAVs based on deep Q-network for energy-efficient data collection in UAVs-assisted IoT. Vehicular Communications, 36, 100491.

[5] V. Roy. "An Effective FOG Computing Based Distributed Forecasting of Cyber-Attacks in Internet of Things" Journal of Cybersecurity and Information Management, Vol. 12, No. 2, 2023 ,PP. 8-17.

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

[6] Kim, T., Vecchietti, L. F., Choi, K., Lee, S., & Har, D. (2020). Machine learning for advanced wireless sensor networks: A review. IEEE Sensors Journal, 21(11), 12379-12397.

[7] Suresh, S. S., Prabhu, V., Parthasarathy, V., Senthilkumar, G., & Gundu, V. (2024). Intelligent data routing strategy based on federated deep reinforcement learning for IOT-enabled wireless sensor networks. Measurement: Sensors, 31, 101012.

[8] Muniandi, B., Raut, K. J., Gawande, P. G., Maurya, P. K., & Howard, E. (2024). AI-Driven Energy Efficient Routing Protocols for Wireless Sensor Networks. NATURALISTA CAMPANO, 28(1), 1906-1915.

[9] Han, D., & So, J. (2023). Energy-efficient resource allocation based on deep Q-network in V2V communications. Sensors, 23(3), 1295.

[10] Liang, F., Yu, W., Liu, X., Griffith, D., & Golmie, N. (2021). Toward deep Q-network-based resource allocation in industrial internet of things. IEEE Internet of Things Journal, 9(12), 9138-9150.

[11] Yuan, J., Peng, J., Yan, Q., He, G., Xiang, H., & Liu, Z. (2024). Deep Reinforcement Learning-Based Energy Consumption Optimization for Peer-to-Peer (P2P) Communication in Wireless Sensor Networks. Sensors, 24(5), 1632.

[12] V. Roy. "Breast cancer Classification with Multi-Fusion Technique and Correlation Analysis" Fusion: Practice & Applications, Vol. 9, No. 2, 2023 ,PP. 48-61.

[13] S Hariharan , Monika Gupta, Improving Cloud-based ECG Monitoring, Detection and Classification using GAN, Fusion: Practice and Applications, Vol. 2 , No. 2 , (2020) : 42-49 (Doi : https://doi.org/10.54216/FPA.020201).

[14] P. Kumar, A. Baliyan, K. R. Prasad, N. Sreekanth, P. Jawarkar, V. Roy, E. T. Amoatey, "Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5713092, 15 pages, 2022. https://doi.org/10.1155/2022/5713092

[15] Sarthak Gupta , Monil Pahwa , Prayant Gupta , Surinder Kaur, ARZARA: Augmented reality app to try watch on your wrist, Fusion: Practice and Applications, Vol. 2 , No. 2 , (2020) : 50-56 (Doi : https://doi.org/10.54216/FPA.020202)

[16] Sudhakar, M., & Anne, K. R. (2024). Optimizing data processing for edge-enabled IoT devices using deep learning based heterogeneous data clustering approach. Measurement: Sensors, 31, 101013.

[17] Vishwanathrao, B. A., & Vikhar, P. A. (2024). Reinforcement Machine Learning-based Improved Protocol for Energy Efficiency on Mobile Ad-Hoc Networks. International Journal of Intelligent Systems and Applications in Engineering, 12(8s), 654-670.

[18] Gherairi, S. (2022). Healthcare: A priority-based energy harvesting scheme for managing sensor nodes in WBANs. Ad Hoc Networks, 133, 102876.

[19] Muhammad Edmerdash, Waleed khedr, Ehab Rushdy, An Overview of Cloud-Based Secure Services for Enterprise Drug–Drug Interaction Systems, International Journal of Wireless and Ad Hoc Communication, Vol. 2 , No. 2 , (2021) : 49-58 (Doi : https://doi.org/10.54216/IJWAC.020201)

[20] Noushini Nikeetha P. , Pavithra D. , Sivakarthiga K. , Karthika S. , Yashitha R. , Kirubasri G.V., A Survey on IoT based Wearable Sensor for Covid-19 Pandemic, International Journal of Wireless and Ad Hoc Communication, Vol. 2 , No. 2 , (2021) : 77-87 (Doi : https://doi.org/10.54216/IJWAC.020203)

[21] Preeth, S. S. L., Dhanalakshmi, R., & Shakeel, P. M. (2020). An intelligent approach for energy efficient trajectory design for mobile sink based IoT supported wireless sensor networks. Peer-to-Peer networking and applications, 13, 2011-2022.

[22] Banoth, S. P. R., Donta, P. K., & Amgoth, T. (2021). Dynamic mobile charger scheduling with partial charging strategy for WSNs using deep-Q-networks. Neural Computing and Applications, 33(22), 15267-15279.

[23] Joshi, U., & Kumar, R. (2020). A novel deep neural networks based path prediction. Cluster Computing, 23(4), 2915-2924.

[24] Esraa Mohamed, The Relationship between Artificial Intelligence and Internet of Things: A quick review, Journal of Cybersecurity and Information Management, Vol. 1 , No. 1 , (2020) : 30-34 (Doi : https://doi.org/10.54216/JCIM.010101)

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024

[25] Dr. Ajay B. Gadicha , Dr. Vijay B. Gadicha, Implicit Authentication Approach by Generating Strong Password through Visual Key Cryptography, Journal of Cybersecurity and Information Management, Vol. 1 , No. 1 , (2020) : 5-16 (Doi : https://doi.org/10.54216/JCIM.010102)

[26] Xu, Y., Yu, J., & Buehrer, R. M. (2020). The application of deep reinforcement learning to distributed spectrum access in dynamic heterogeneous environments with partial observations. IEEE Transactions on Wireless Communications, 19(7), 4494-4506.

[27] Reem Atassi, Aditi Sharma, Intelligent Traffic Management using IoT and Machine Learning, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 2 , (2023) : 08-19 (Doi : https://doi.org/10.54216/JISIoT.080201)

[28] Khder Alakkari, Alhumaima Ali Subhi, Hussein Alkattan, Ammar Kadi, Artem Malinin, Irina Potoroko, Mostafa Abotaleb, El-Sayed M El-kenawy, Forecasting COVID-19 Infection Using Encoder-Decoder LSTM and Attention LSTM Algorithms, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 2 , (2023) : 20-33 (Doi : https://doi.org/10.54216/JISIoT.080202)

[29] V. Roy. "An Improved Image Encryption Consuming Fusion Transmutation and Edge Operator." Journal of Cybersecurity and Information Management, Vol. 8, No. 1, 2021 ,PP. 42-52.

Doi : https://doi.org/10.54216/JCIM.140111
Received: January 11, 2024 Revised: March 21, 2024 Accepted: June 05, 2024