SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Security Augmentation for Deep Reinforcement Learning - Drivenv Strategies in Energy-Efficient Wireless Sensor Networks

N. Karthick[1], Dr. K. Ranjith Singh[2]

[1]Ph.D. Research Scholar, Department of Computer Science,Karpagam Academy of Higher Education (Deemed to be University), Coimbatore, Tamil Nadu, India.
[2]Assistant Professor and Research Supervisor, Department of Information Technology, Karpagam Academy of Higher Education (Deemed to be University), Coimbatore, Tamil Nadu, India.

Abstract:
Owing to the inherent transmission nature of wireless communication and the partial battery capacity of sensor nodes, achieving both energy efficiency and secure communication remains a major challenge in Wireless Sensor Networks (WSNs). Consequently, considerable research attention has been directed toward developing intelligent solutions that can simultaneously enhance network security and reduce energy consumption. To overcome these challenges, this study introduces a novel Deep Reinforcement Learning (DRL) based framework, termed DeepNR, to enhance both security and energy efficiency in Wireless Sensor Networks (WSNs). The proposed DeepNR model utilizes a Deep Neural Network (DNN) to dynamically acquire network state data and effectively estimate the Q-value function. Through continuous monitoring and analysis of network conditions, the framework is capable of making intelligent and adaptive decisions for efficient network operation and management. Moreover, the proposed framework employs a DRL-based multi-tier decision-making approach to dynamically optimize data transmission routes in real time. This adaptive strategy enables accurate network state prediction and efficient routing decisions, resulting in improved communication performance and resource utilization. In addition, DeepNR integrates a real-time defense mechanism capable of responding to detected threats while maintaining normal network operations, thereby significantly strengthening overall network security.
The framework further integrates deep learning techniques to dynamically adjust to varying network conditions and emerging cyber threats. Experimental results indicate that the proposed DeepNR approach surpasses traditional methods, delivering nearly 25% higher network throughput, 20% better security efficiency and approximately 30% longer network lifetime.

Keywords: WSN-wireless sensor networks, Energy Efficiency, Network Security, Intelligent Routing, Adaptive Communication, Deep Reinforcement Learning

1. INTRODUCTION

1.1. Traditional Solutions

Conventional techniques for increasing WSN energy efficiency frequently entail using low-power operating modes and optimising communication protocols. For example, methods such as duty cycling, dynamic power modification, data aggregation extensively investigated. To increase energy efficiency, Perrig suggested data consolidation, dynamic broadcast power modification and low-power monitoring systems.
In terms of security, the majority of tactics meant to protect network communications are based on intrusion detection systems, authentication and encryption. Akoglu suggested techniques for intrusion detection, authentication and encrypted communication in security guidelines for network communications. Ioannou successfully identified malicious action in 88 - 100% rangea by classifying local sensor movement as caring or malicious using a binary logistic regression statistical method. These methods, however, only take into account a one side increase in performances benefits are frequently at the expense of additional performances.Network security is compromised when low power communications and the processing techniques are employed to increase energy efficient, leaving the networking model more open to outside threats. Thus, it is essential to make energy competence and security compatible in Wireless Sensor Networks.

1.2 Machine Learning Based Solution

Artificial Neural Networks (ANNs) are computing frameworks modeled after the information-processing behavior of biological neurons in the hominoid brain. These networks are composed of interconnected neuron layers that analyze input data using weighted links and activation mechanisms. Deep Neural Networks (DNNs), which include multiple hidden layers, have achieved remarkable success over conventional machine learning methods in areas such as speech recognition, image analysis and natural language processing. Owing to their advanced learning and decision-making capabilities, DNNs are increasingly being utilized for the enhancement and efficient management of Wireless Sensor Networks (WSNs).

Numerous studies have investigated the application of deep learning methods to enhance the efficiency of Wireless Sensor Networks (WSNs). An energy-efficient routing mechanism utilizing multi-objective cluster head selection was introduced to enable secure data aggregation within WSN environments. The developed method demonstrated better performance in terms of packet delivery rate, reduced communication latency, and extended network lifetime compared with conventional routing approaches.

Graph Neural Networks (GNNs) combined with deep learning techniques have also been introduced to optimize sensor energy consumption and prolong network lifetime in WSNs. In addition, DNN-based intrusion detection approaches have been applied in IoT-enabled WSN systems to identify cyber threats and abnormal activities in real time. Researchers have also employed DNN-based models to enhance communication reliability in Wireless Sensor Networks by evaluating network characteristics such as available bandwidth and transmission latency.

Reinforcement Learning (RL) has become a significant intelligent learning technique for adaptive network optimization. In this approach, an agent acquires optimal behavior through continuous interaction with the environment by monitoring system states, executing actions and obtaining reward feedback. The main goal of the agent is to maximize long-term cumulative rewards by determining the most suitable sequence of actions. Thus, reinforcement learning allows systems to develop effective decision-making policies through ongoing environmental interaction and learning.

The Markov Decision Process serves as the fundamental theoretical model for reinforcement learning. Based on the MDP principle, the future state of a system is determined solely by the present state and the action taken by the agents. Deep Reinforcement Learning (DRL) combines reinforcement learning techniques with Deep Neural Networks (DNNs), in which neural networks are utilized to estimate value functions or decision policies for enhanced prediction accuracy and intelligent control. Through continuous adaptive learning, DRL effectively optimizes network parameters and improves overall system performance.

In WSN environments, DRL has demonstrated significant potential in routing optimization, resource management and security enhancement. Deep learning-assisted routing algorithms have been developed to monitor network conditions in real time and dynamically select optimal communication paths. Similarly, DRL-based energy management approaches have been proposed for WSNs with multiple local subnetworks, where the optimization problem is modeled using an MDP framework to determine efficient resource allocation strategies.

Reconfigurable Intelligent Surfaces (RISs) have also been investigated in WSN security applications to enhance secure communication. By jointly optimizing interference power, sensor scheduling strategies and RIS phase shifts, these techniques improve secrecy rates and strengthen network protection against attacks. Despite these advancements, achieving an effective trade-off between security and energy efficiency remains a major challenge in Wireless Sensor Networks. Therefore, intelligent frameworks that combine DRL with advanced optimization strategies are essential for developing secure, energy-efficient and sustainable WSN architectures.

1.3. Existing Challenges and Gaps

WSN dispositions and operations present many difficulties, particularly in striking a balance between strong security protocols and energy efficiency. Conventional methods frequently address these problems separately, which results in less-than-ideal network performance. The key among the difficulties are the following:

- Efficiency of Energy Use

Increasing network lifespan while preserving operational efficacy is still a top priority because sensor nodes have limited power resources.

- Safety

Because wireless communication is open, WSNs are vulnerable to a variety of security risks, such as node manipulation and data breaches, which calls for all-encompassing security solutions.

- **Flexibility and Adaptability:**

Wireless Sensor Networks (WSNs) operate in highly dynamic environments where network conditions and cyber threats continuously evolve. Traditional static optimization techniques are often unable to effectively respond to these rapid changes. To overcome this limitation, the proposed DeepNR framework utilizes Deep Reinforcement Learning (DRL) to provide an adaptive and intelligent network management solution.

In contrast to traditional techniques, DeepNR continuously acquires knowledge from the network environment and swiftly adapts its strategies in response to varying network conditions and evolving security threats. The framework intelligently balances energy efficiency and security performance in real time, thereby maintaining reliable and stable network functionality. Furthermore, the proposed method not only overcomes the shortcomings of existing approaches but also provides a scalable and adaptable solution for effective WSN management and sustainable long-term network operation.

2. LITERATURE REVIEW

Wireless Sensor Networks (WSNs) have emerged as a fundamental technology for enabling intelligent communication in Internet of Things (IoT) environments. The rapid growth of WSN applications has motivated extensive research in areas such as energy efficiency, secure communication, routing optimization, data aggregation and intelligent network management. Several researchers have proposed advanced methodologies to improve network lifetime, scalability and security in dynamic wireless environments.

An energy-efficient WSN configuration strategy based on clustering and location-awareness techniques. Their work focused on optimizing node placement and cluster formation to minimize energy consumption during communication. By utilizing geographical information, the proposed approach significantly improved network lifetime and reduced unnecessary data transmission among sensor nodes. The study demonstrated that intelligent clustering mechanisms can effectively balance energy utilization across the network [1]. A communication framework integrating Mobile Ad Hoc Networks (MANETs) and WSNs for IoT-enabled smart environments. Their framework enabled seamless communication between heterogeneous wireless systems to improve connectivity and data exchange. The proposed architecture enhanced flexibility and adaptability in smart environments while supporting reliable communication among distributed sensor devices. The study highlighted the importance of integrating WSNs with other wireless technologies to achieve scalable IoT infrastructures [2].

To address routing and energy conservation challenges, a comprehensive survey on the successors of the PEGASIS routing protocol. Their work analyzed various enhancements proposed for PEGASIS, focusing on energy-efficient chain-based communication approaches. The survey emphasized the advantages of hierarchical routing mechanisms in reducing communication overhead and extending sensor node lifetime. The authors concluded that optimized routing protocols remain essential for improving the overall efficiency of WSNs [3]. Security remains one of the major concerns in wireless sensor networks due to their distributed architecture and limited computational capabilities. To investigated the role of machine learning techniques in WSN security. Their study reviewed several machine learning algorithms used for intrusion detection, anomaly detection and attack mitigation in sensor networks. The authors identified key challenges such as limited training datasets, computational complexity and real-time implementation constraints. Their findings demonstrated that intelligent learning-based security mechanisms can significantly improve threat detection accuracy in WSNs [4].

A secrecy enhancement technique for Space Shift Keying (SSK)-based wireless sensing communications. Their work focused on improving communication confidentiality by utilizing secure modulation schemes in wireless sensing environments. Experimental analysis showed that the proposed method enhanced resistance against eavesdropping attacks while maintaining communication reliability [5]. In another study, an optimization framework based on SSK for secure Industrial Internet of Things (IIoT) communication systems. Their model improved data security and transmission performance by optimizing signal design and channel utilization. These studies indicate that physical-layer security techniques can effectively strengthen WSN communication against malicious attacks [6].

Wireless multimedia sensor networks have also gained significant attention in healthcare applications. The image transmission framework using decode-and-forward cooperative communication in medical IoT systems. Their research focused on improving image delivery reliability under Rayleigh fading channel conditions. The proposed model enhanced communication quality and reduced transmission errors during remote healthcare monitoring. This work demonstrated the growing importance of WSNs in real-time medical communication systems [7].

Efficient data aggregation techniques are essential for reducing communication overhead and conserving sensor energy. Their method improved network performance by organizing sensor nodes into optimized clusters for efficient data forwarding. Simulation results showed considerable improvements in packet delivery and communication delay reduction. The study confirmed that cluster-based aggregation strategies are highly effective in enhancing WSN reliability [8]. Duty cycling is another important approach for energy conservation in sensor networks. A Q-learning-based delay-aware data for fusion mechanism for duty-cycled WSNs. Their approach utilized reinforcement learning to optimize data fusion and transmission scheduling based on network conditions. The proposed system achieved lower communication delays while maintaining energy efficiency. The integration of reinforcement learning into WSN management demonstrated the potential of intelligent decision-making techniques in adaptive wireless environments [9]. Clustering-based routing protocols continue to play a significant role in WSN optimization. A detailed study on LEACH-based clustering protocols for WSNs. Their study reviewed various modifications of the LEACH protocol designed to improve scalability, energy balancing, and communication efficiency. The authors concluded that adaptive clustering strategies are highly effective for extending network lifetime in large-scale sensor deployments [10].

The broad applications of WSNs across multiple domains, including industrial automation, healthcare monitoring, military operations and environmental sensing. Their work highlighted the versatility and growing importance of WSN technology in modern communication systems. However, the authors also identified challenges related to energy limitations, communication reliability and network security [11].

Recent advancements in deep learning have further transformed communication network management. A survey on graph-based deep learning techniques for communication networks. The study explored the application of graph neural networks and deep learning models in routing optimization, traffic prediction and network security. The author emphasized that deep learning approaches can effectively model complex network relationships and improve communication efficiency [12]. Reinforcement learning has also been extensively investigated for intelligent resource management in wireless networks. A multi-agent reinforcement learning framework for cooperative edge caching in Internet of Vehicles (IoV) environments. Their approach enabled multiple agents to collaboratively optimize caching decisions and reduce communication latency. The study demonstrated the effectiveness of reinforcement learning in dynamic and distributed wireless systems [13]. One of the earliest and most influential studies on WSNs, who provided a comprehensive survey of wireless sensor network architectures, communication protocols and applications. Their work established the foundation for subsequent WSN research by identifying major challenges such as energy constraints, routing complexity, scalability and fault tolerance. The survey remains a key reference in WSN research literature [14]. A joint user scheduling and trajectory planning strategy for Unmanned Aerial Vehicle (UAV) assisted WSN data collection. Their model optimized UAV movement and sensor communication scheduling to improve data gathering efficiency. Experimental results showed reduced communication delay and enhanced energy utilization. This study highlighted the integration of UAV technologies with WSNs to support advanced data collection applications [15].

Overall, the existing literature demonstrates that energy efficiency, secure communication, intelligent routing, and adaptive learning remain the primary research directions in wireless sensor networks. Although several techniques have been proposed to improve WSN performance, challenges related to network lifetime, scalability and cyber security still persist. Therefore, integrating advanced deep reinforcement learning techniques with intelligent security frameworks offers significant potential for developing sustainable, secure and energy-efficient WSN architectures.

The network's resilience is increased by the suggested DeepNR strategy, which incorporates state-of-the-art security improvements directly into the DRL model and provides strong defence against a variety of cyberthreats. The experiments confirm the suggested DeepNR's advantages and efficacy. While maintaining security, DeepNR can greatly increase WSN energy efficiency when compared to other traditional techniques. The balance of the documents structure are as follows: Current research on WSN security and energy efficiency is presented in Section 1. Section 3 provides a description of the suggested techniques. Section 4 displays the outcomes of the experiment. This paper is finally concluded in Section 5.

3. PROPOSED METHODOLOGY

Around here the outlines are suggested DeepNR approach, which optimises network strategy using DRL and represents the Q-value function using DNN.

3.1. Network Design

To implement the suggested network optimization framework, a Deep Q-Network (DQN) - based model was adopted as the core learning mechanism. DQN, a widely recognized approach within Deep Reinforcement Learning (DRL), is highly effective in managing complex and high-dimensional environments. This characteristic makes it well suited for Wireless Sensor Networks (WSNs), where network conditions continuously change and efficient decision-making is essential.

The proposed DQN framework integrates the decision-making capability of Q-learning with the powerful feature mining ability of deep neural networks. The developed model consists of an input layer that received the current state information of the Wireless Sensor Network, multiple hidden layers responsible for learning and processing network patterns, and an output layer that determines the most appropriate action for improving both energy efficiency and network security. Through unceasing interaction with the network environment, the model learns optimal strategies that enhance communication performance while reducing energy consumption and security risks.

Real-time responses to shifting circumstances and dangers are made easier by this model's ability to provide a detailed understanding of and interaction with the network settings. The neural network architecture of the suggested DeepNR approach is shown in Figure 1. The neural network's purpose is to develop the network's current states and produce a probability distribution of possible courses of action. In particular, the states is a neural network input that represents the WSN's current state.

Within the suggested DeepNR framework, the state representation can incorporate a wide variety of sensor data, network performance metrics, and environmental factors that influence the decision-making process. The neural network's output is the collection of the actions that are represented by the distribution of probabilities. Every activity relates to a potential choice or action that the WSN may take, like changing the routing, deciding how to manage power, or starting security procedures. Given the network's present state, the probability distributions are shows that the possibility that every action is the best option. There are $3N + T \times (3N + 2N)$ neurones in the input layer. 256 neurones are present in hidden layers 1 & 2 and 128 neurones with the ReLU stimulation function, respectively. The action vector's Q-value is represented by 2N neurones in the output layer. Additionally, we use a DNN to represent the policy π.

The network's input $x=[s, h1, h2, \ldots hT]$ here, s is the present states, which includes each node's energy data, communication quality, and most recent security incidents. h is the node's historical status, which includes each node's state and actions throughout the prior time step.

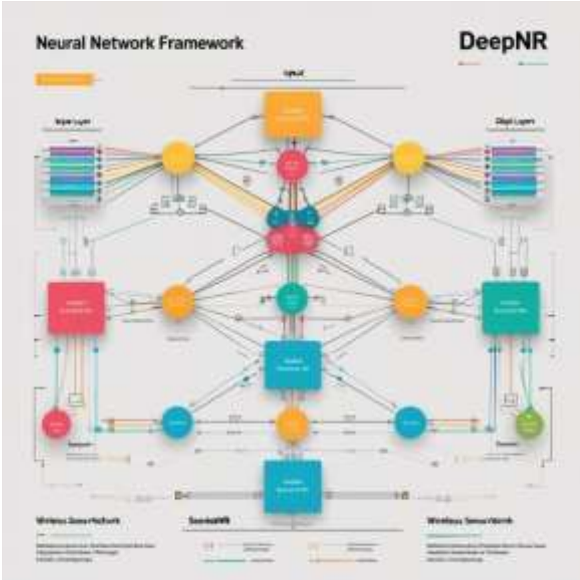

Figure 1: Framework of Neural Network Vs DeepNR

In this research, the proposed Deep Neural Network (DNN) is trained using target network mechanisms and experience replay to enhance learning stability and overall system performance. Experience replay enables the model to learn from previously stored interactions by randomly selecting past experiences during the training phase, thereby minimizing the correlation between training samples and improving learning effectiveness. At the same time, the target network helps stabilize the optimization process by providing consistent target values during Q-value updates.

Instead of relying on the traditional Q-learning table-based approach, the proposed DeepNR framework employs a DNN to estimate the Q-value function. Within this framework, Q-learning is utilized as an iterative decision-making strategy to identify optimal actions based on the current network state. The integration of neural networks with Q-learning enables the model to efficiently manage large and critical state spaces, making it highly suitable for dynamic Wireless Sensor Network (WSN) environments,

In a complicated WSN context, the DeepNR approach can maximise network performance. Our approach's novel features are emphasised in a number of crucial areas as associated to DNN:

• **WSN-Oriented DNN Customization:** Conventional deep neural network (DNN) models are generally not designed to manage the complex and high-dimensional state spaces commonly found in Wireless Sensor Networks (WSNs). To address this limitation, the proposed framework introduces a specially designed DNN architecture tailored to the unique characteristics and operational requirements of WSN environments.

• **Real-Time Adaptive Learning:** The integration of Deep Reinforcement Learning (DRL) with DNNs enables the proposed approach to continuously learn from the network environment and dynamically adapt to changing network conditions as well as evolving attack behaviors. This adaptive capability is particularly important in WSNs, where network topology and communication patterns frequently vary over time. Unlike traditional DNN-based approaches, the proposed method supports intelligent real-time decision-making to maintain stable and efficient network operation.

• **Multi-Level Decision-Making Mechanism:** The proposed framework incorporates a hierarchical decision-making strategy driven by a DNN-based policy model. By dynamically adjusting network operations at multiple levels, the system effectively balances energy conservation and security enhancement, thereby improving overall WSN performance and reliability.

• **Hybrid Reward Function Design:** To guide the training process within the DRL framework, a composite reward function is developed that simultaneously considers both security performance and energy efficiency. This reward mechanism enables the learning model to identify optimal actions that enhance secure communication while minimizing unnecessary energy consumption in the network.

3.2. Strategy Optimization

WSNs are essential to many applications, from allowing smart cities to monitoring the environment. They must contend with the twin problems of partial energy supplies and the security concerns. Conventional approaches frequently tackle these issues in isolation, which may result in compromises that impair network functionality.

The proposed DeepNR framework is designed with the objective of attaining the balanced enhancement in both energy efficiency and network security through the intelligent application of Deep Reinforcement Learning (DRL). Unlike conventional approaches that optimize a single performance metric, the proposed method dynamically manages network operations to enhance security and energy utilization simultaneously without compromising either aspect.

A key component of the proposed framework is the accurate modeling of communication interactions between sensor nodes. This communication model forms the basis for optimizing overall network performance, including secure data transmission, energy-aware routing, and adaptive network management. Considering the Wireless Communications features of Wireless Sensor Networks (WSNs), the communication relationship between node (i) and node (j) can be mathematically represented as follows:

$$Q_{ij} = \frac{P_{tx} \times G_{tx} \times G_{rx}}{L(d_{ij}) \times V}$$

where G_{tx} and G_{rx} are trans receiving the antenna gains and respectively and Ptx is the transmission power. V is the noise power, and L (d_{ij}) is the route loss function.

It should be noted that, in contrast to deep Q-learning and our suggested method seeks to develop to more reliable and efficient strategy optimisation procedure for WSNs, guaranteeing that DeepNR and it can manage the complexities and difficulties unique to these networks. The dynamic and varied character of network analysis situs, the fluctuating energy outlines of the sensor nodes and the changing threat landscape with regard to network security are a few examples of this. In particular, our optimisation procedure possesses the following traits:

• Better representation of the state space. DeepNR's state space is intended to contain a more extensive collection of network parameters that have been especially selected to capture the intricate changing aspects of WSNs.

• A personalised recompence system. We using a specially designed reward function that is intended to fulfil the two goals of optimising energy efficiency, guaranteeing network security, which are not typically the main emphasis of conventional Deep Q-learning systems.

• WSN strategy optimisation. Our method modifies the procedure optimisation procedure to accommodate the unique operational limitations and performance objectives of WSNs, including the requirement for quick reaction to security risks and node energy limitations.

• A sophisticated technique for replaying experiences. Beyond the conventional Deep Q-learning method, we have improved the learning process by implementing an enhanced skill repetition mechanism that are better fits the temporal and spatial variability in WSNs.

• Integration with protocols unique to WSNs. In a real-world network setting, DeepNR's integration with WSN specific protocols allows for a smooth conversion from learnt policies to implementable rules.

4. RESULTS AND DISCUSSION

This testing environment was created to mimic the standard WSN placement using 500 MICAz sensor lumps with CC2420 communication modules, in which dispersed at random in order to confirm the true performance of the suggested DeepNR technique. An area of 500m by 500m. Every node has an preliminary energy of 100 J and a communication range of 50m. The TinyOS operating system was used by every node. The nodes were set up to function within a network that adheres to IEEE 802.15.4 standards. There were several PANs on the network, and the PAN coordinator was a specific Full-Function Device (FFD). The remaining nodes served as the end nodes with particular sensing and the communication responsibilities and are identifying as Reduced Function Devices (RFDs).

For effective data routing and aggregation, the nodes were arranged into hierarchical tiers. Constructed on the network's size and density where the number of hierarchy levels were decided, paying particular emphasis to maximising the trading off between energy usage and inactivity. We were ran 100 tests in total for every situation to guarantee statistical consequence in our findings and a thorough assessment of the suggested DeepNR approach. Each experiment was conducted over a continuous 24-hour operational period to simulate realistic network conditions and long-term system behavior. This evaluation approach enabled us to thoroughly analyze the recital, stability and robustness of the suggested method under continued and dynamic operating environments.

Remember that the duration of the test should be sufficient to see how the network behaves under pressure, but not so long as to unreasonably drain its energy resources. Furthermore, our experimental configuration meticulously adjusted to provide accurate representation of the WSN activities, accounting for the usual energy limitations and security needs of these networks.

Three WSN strategies DEEC is an energy based clustering algorithm, PEGASIS is a link-based data fusion strategy and LEACH is a traditional clustering routing method, were chosen as baseline algorithms in order to objectively assess the DeepNR strategy's performance.

4.1. Network Life Cycle

We could compare the life cycles of WSNs with different node counts based on the network's overall energy usage. One hundred, two hundred, three hundred, four hundred, and five hundred nodes were established.

The network size is represented by the vertical axis in the Figure 2(b), while the entire network energy feeding (J) is represented by its horizontal axis. The aggregate of all the energy expenditure made by the wireless sensor network's nodes during simulation's lifetime is known as the total energy consumption. Transmission energy, reception energy, processing energy and idle energy.

Figure 2(a): Wireless Network Framework of DeepNR

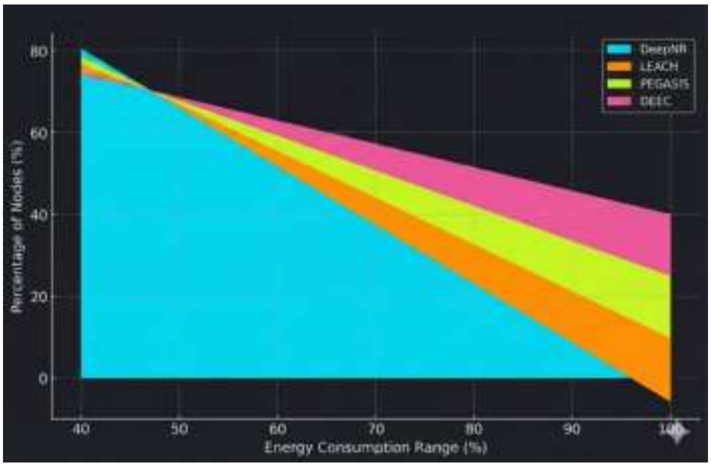

Figure 2(b): Comparison between nodes and energy Consumptions Range

It goes without saying that the network's energy usage rises with its size. Additionally, our suggested DeepNR approach prolongs the network life cycle and efficiently lowers energy consumption in wireless sensing when compared to alternative tactics, which can be explained by the fact that it minimises the energy used per node by improving node communication and data handing out.

The proposed DeepNR framework optimizes communication among sensor nodes by choosing the most energy-efficient data communication routes according to the current network conditions learned dynamically through the DRL model. By continuously adapting routing decisions based on real-time network states, the approach minimizes unnecessary energy consumption during data communication. This optimization strategy enables sensor nodes to conserve energy more effectively, thereby extending the overall operational lifetime and efficiency of the wireless sensor network.

Additionally, by using clever data accumulation techniques that reduce dispensation overhead and prolong the battery life of the nodes, the DeepNR policy improves data processing effectiveness. The DRL model's adaptive learning component consistently ensures that the network maintains its energy efficiency even when circumstances change by continuously improving these procedures. By using a multi-level decision-making process, the DeepNR approach strategically distributes network resources, such power and bandwidth, to the areas that require them the most. This prolongs the useful life of the network by improving its energy efficiency and guaranteeing that crucial components continue to operate for longer periods of time.

4.2. Data Throughput

The latency standards for wireless sensing communications are also getting better as a result of the communication environment's ongoing innovation and development. As the need for immediate response and real-time data grows, wireless sensing communiqué systems can be to process and send the data are more quickly. We replicated the average communication interruptions for 4 techniques under varied network loads to account for the requirements of diverse communication settings.

We look at the average announcement delay under different network conditions in Figure 3. It is evident that each strategy's communication delay rises in proportion to the network load. Interestingly, DeepNR continuously shows low communication inactivity across all network loads, which are explained by its sophisticated packet processing processes and effective data routing algorithms. By cutting down on the amount of time packets apply in the queue, during transmission, these features help it handle heavy data traffic more effectively and minimise total communication inactivity.

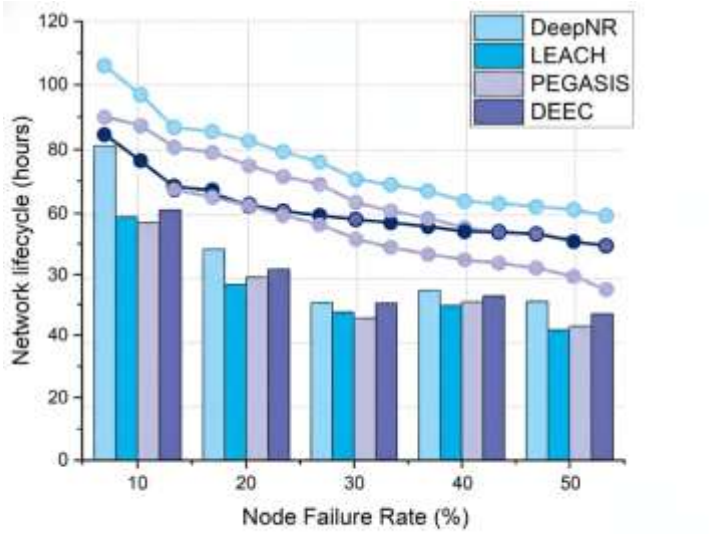

Figure 3: The Middling Communication Delay

Through the use of sophisticated packet processing mechanisms and effective data routing algorithms, the suggested DeepNR technique increases data throughput. By making sure that data packets travel the least crowded and most energy-efficient routes throughout the network, these methods are intended to lower communication delay. This not only increases the broadcast time but also reduces the likelihood of packet loss and retransmissions, which can significantly degrade network throughput.

Additionally, our approach uses smart packet processing methods that rank data packets according to its time sensitivity and significance. DeepNR makes sure that important data is sent quickly by processing and forwarding packets according to their urgency, which raises the network's throughput overall. The DRL typical model in DeepNR in which acquires from the network environment and adjusts the serves as the foundation for these techniques. the real-time processing and routing techniques. This enables an adaptable and responsive network that can be sustain very-high throughput even in the face of fluctuating load.

4.3. Security Assessment

We replicated 3 popular attacks models – a) Single Node b) Distributed Denial of Service (DDoS) c) Deception – so as to assess the security presentation of the suggested DeepNR approach. Next, we contrasted the networks' transmission performance. employing various tactics and evaluated the resilience according to the network lifespan under varied rates of node failure. Our DeepNR approach uses sophisticated detection techniques that make use of DRL's predictive capability to find possible security risks before they have a chance to affect the network. This proactive approach enables prompt and efficient response actions, lowering the probability of the successful attacks and as a result the number of nodes that are impacted. Using a mixture of anomaly detection algorithms and pattern recognition are trained using DRL, DeepNR's improved detection capabilities are intended to detect threats in real time. When DeepNR detects a danger, it starts a pre-planned reaction mechanism that may involve changing transmission patterns, isolating impacted nodes, or rerouting data to lessen the impact of the attack.

The network can dynamically modify its security mechanisms thanks to DeepNR's DRL paradigm. It gets better at anticipating and stopping assaults by uninterruptedly learning from network interactions and threats that are discovered. Because of this continuous learning process, the network's security features adapt to the shifting strategies of the attackers, guaranteeing that the systems is resilient to both well-known and unknown attacks. Figure 4 displays the number of nodes is impacted by each attacks model. The following are the ranking of the effectiveness of several tactics against different types of harmful attacks: DEEC, PEGASIS, LEACH, and DeepNR. This outcome demonstrates the superiority of the security performance of our suggested DeepNR approach. Across a variety of attack types, DeepNR consistently displays fewer impacted nodes, proving both its resilience and its sophisticated security measures. This is because, in contrast to previous approaches, DeepNR has stronger methods to identify and eliminate a variety of network risks, guaranteeing improved network security and integrity.

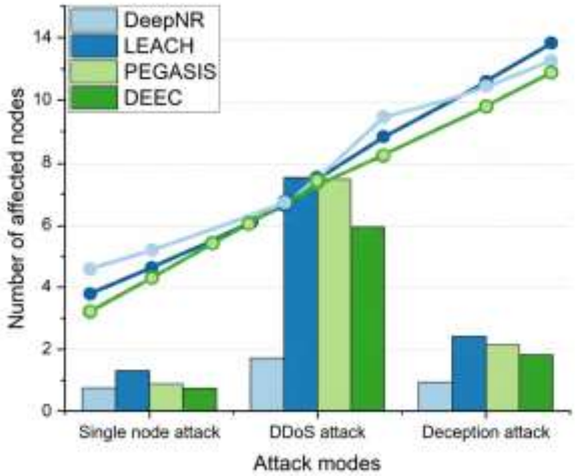

Figure 4: The Number of Nodes Impacted by Each Attack Model

Figure 5 illustrates the consistency of the network lifecycle under different node failure rates. In order to guarantee continuous service and save maintenance costs, a network strategy must be able to withstand an increase in node failures and preserve its operational lifetime. As node failures increase, the resilience of the network strategy becomes more evident. The suggested DeepNR beats alternative approaches in terms of network lifetime and maintains its robustness across a range of node failure rates. DEEC and PEGASIS are in close pursuit, but LEACH performs the poorest. However, the difference between the four techniques becomes less pronounced as, the node failure rate increases, highlighting the need for continuous research and development to further enhance the capability of networks to manage various types of failures.

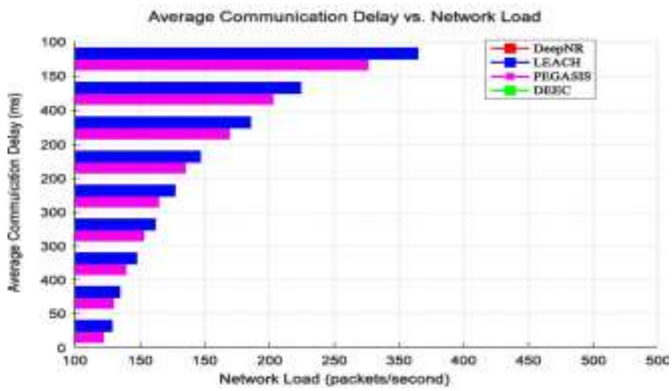

Figure 5: Network Life Cycle Corresponding to Different Node Failures Rates

4.4. Energy Spreading and Balance

DeepNR employs a sophisticated energy organization structure that keeps track of each node's energy levels and reassigns duties throughout the network to keep nodes from using up all of their energy too quickly. The DRL is the foundation of this system. models which are forecasts upcoming energy needs, modifies networks behaviour to preserve energy equilibrium. Figure 6 examines the energy distributions of every network bump to further illustrate effectiveness of the suggested DeepNR technique. It is evident that, in comparison to the other strategies, a larger proportion of nodes (90%) use energy in the 40–50 J range while using the DeepNR approach. Furthermore, just 2% of the nodes expend over 50 J of energy with the DeepNR technique, which is substantially less than that of the other options.

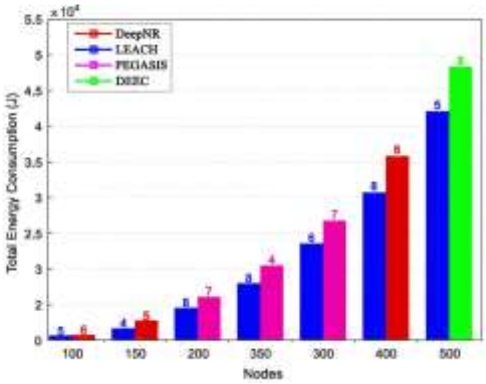

Figure 6: The Energy Spreading of Every Network Node

The research results indicate that the suggested DeepNR framework provides highly effective energy management by ensuring that energy consumption among sensor nodes remains within an optimized and balanced range. The method demonstrates improved control over node energy utilization, thereby enhancing the overall stability and efficiency of the wireless sensor network.

Based on the observed experimental outcomes, the DeepNR approach effectively achieves a balance between network security and energy efficiency. The framework incorporates intelligent algorithmic optimization techniques that dynamically regulate node energy consumption according to current network conditions, communication weights and the residual energy planes of individual sensor nodes. This adaptive strategy avoids excessive energy depletion in critical nodes responsible for maintaining network connectivity and encourages a balanced distribution of energy consumption throughout the network

By ensuring balanced energy utilization among sensor nodes, the proposed DeepNR framework considerably prolongs the operational lifespan of the network. In addition, the approach reduces the frequency of maintenance operations and minimizes the need for node replacement, thereby improving the long-term reliability and sustainability of wireless sensor network deployments.

The experimental evaluation confirms that security-augmented DRL strategies provide a multi-objective improvement in wireless sensor network performance. Unlike traditional protocols that treat energy efficiency and security as separate challenges, the proposed framework integrates both within a unified intelligent learning model.

Key consolidated outcomes:

- Extended network longevity through adaptive energy-aware routing.
- Stable and high data throughput under dynamic and adversarial conditions.
- Robust security resilience via real-time anomaly detection and response.
- Balanced energy consumption, preventing early node failures.

These findings highlight the practical feasibility of DRL-based secure routing for next-generation IoT and large-scale sensing environments. Future work may explore federated learning integration, lightweight model compression, and real-world deployment validation to further enhance scalability and applicability.

5. Conclusions

This study introduces a novel DeepNR framework aimed at overcoming the major challenges of security and energy efficiency in Wireless Sensor Networks. The proposed method employs Deep Reinforcement Learning (DRL) to create an intelligent decision-making system capable of dynamically optimizing network performance. Specifically, a Deep Neural Network architecture is developed to effectively estimate the Q - value function, while the training process is strengthened through the incorporation of experience replay and target network mechanisms. These techniques enhance learning stability and support efficient adaptation to dynamic network environments.

To ensure balanced optimization between network energy efficiency and security, the proposed DeepNR framework integrates a multi-tire decision-making mechanism together with a novel compound reward function. This reward strategy directs the learning process by jointly evaluating security performance and energy consumption. Using the knowledge acquired through the Deep Neural Network (DNN), the framework is capable of intelligently selecting optimal actions that enhance transmission reliability while reducing energy usage among sensor nodes.

Investigational results demonstrate that the planned DeepNR method suggestively improves throughput, network lifetime and communication security when compared with existing approaches. The findings confirm that the integration of DRL with intelligent network optimization techniques can effectively enhance the overall performance and sustainability of WSN environments.

In future work, the DeepNR framework will be extended to support multimodal wireless sensor networks

that include diverse sensor types such as temperature, humidity, audio and image sensors. Furthermore, the applicability of DeepNR against advanced AI-driven cyberattacks, including zero-day attacks, will be explored to strengthen WSN security under highly dynamic threat environments. As the number of Internet of Things (IoT) devices continues to increase, future research will also focus on adapting the DeepNR framework to support heterogeneous communication protocols and large-scale IoT ecosystems.
Additionally, cross-layer optimization techniques involving interactions among the physical, MAC, network and application layers that will be investigated to further enhance network efficiency. Beyond DRL, other advanced artificial intelligence approaches, including Generative Adversarial Networks (GANs) and neural-symbolic learning models, it may also be combined with the proposed framework to improve adaptability, intelligence and overall network performance.

References

1. Kim, J.; Lee, D.; Hwang, J.; Hong, S.; Shin, D.; Shin, D. Wireless sensor network (WSN) configuration method to increase node energy efficiency through clustering and location information. Symmetry 2021, 13, 390.
2. Tripathy, B.K.; Jena, S.K.; Reddy, V.; Das, S.; Panda, S.K. A novel communication framework between MANET and WSN in IoT based smart environment. Int. J. Inf. Technol. 2021, 13, 921–931.
3. Khedr, A.M.; Aziz, A.; Osamy, W. Successors of PEGASIS protocol: A comprehensive survey. Comput. Sci. Rev. 2021, 39, 100368.
4. Ahmad, R.;Wazirali, R.; Abu-Ain, T. Machine learning for wireless sensor networks security: An overview of challenges and issues. Sensors 2022, 22, 4730.
5. Zhu, H.; Peng, Y.; Xu, H.; Tong, F.; Jiang, X.Q.; Mirza, M.M. Secrecy enhancement for SSK-based communications in wireless sensing systems. IEEE Sens. J. 2022, 22, 18192–18201.
6. Zhu, H.; Huang, Z.; Lam, C.T.; Wu, Q.; Yang, B.; Ng, B.K. A Space Shift Keying-Based Optimization Scheme for Secure Communication in IIoT. IEEE Syst. J. 2023, 17, 5261–5271.
7. Al Hayani, B.; Ilhan, H. Image transmission over decode and forward based cooperative wireless multimedia sensor networks for Rayleigh fading channels in medical internet of things (MIoT) for remote health-care and health communication monitoring. J. Med. Imaging Health Inform. 2020, 10, 160–168.
8. Devi, V.S.; Ravi, T.; Priya, S.B. Cluster based data aggregation scheme for latency and packet loss reduction in WSN. Comput. Commun. 2020, 149, 36–43.
9. Donta, P.K.; Amgoth, T.; Annavarapu, C.S.R. Delay-aware data fusion in duty-cycled wireless sensor networks: A Q-learning approach. Sustain. Comput. Inform. Syst. 2022, 33, 100642.
10. Daanoune, I.; Abdennaceur, B.; Ballouk, A. A comprehensive survey on LEACH-based clustering routing protocols inWireless Sensor Networks. Ad Hoc Netw. 2021, 114, 102409.
11. Dalal, B.; Kukarni, S. Wireless sensor networks: Applications. In Wireless Sensor Networks: Design, Deployment and Applications; BoD–Books on Demand: Norderstedt, Germany, 2021; p. 3.
12. Jiang, W. Graph-based deep learning for communication networks: A survey. Comput. Commun. 2022, 185, 40–54.
13. Jiang, K.; Zhou, H.; Zeng, D.; Wu, J. Multi-agent reinforcement learning for cooperative edge caching in internet of vehicles. In Proceedings of the 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Delhi, India, 10–13 December 2020; pp. 455–463.
14. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: A survey. Comput. Netw. 2002, 38, 393–422.
15. Wang, X.; Liu, X.; Cheng, C.T.; Deng, L.; Chen, X.; Xiao, F. A joint user scheduling and trajectory planning data collection strategy for the UAV-assisted WSN. IEEE Commun. Lett. 2021, 25, 2333–2337.