International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Rank Based Secure M-WSN Network using Machine Learning for Efficient Routing

Kamalinder Kaur *[1], Dr. Sandeep Kang [2]

Submitted:01/05/2024 **Revised**: 10/06/2024 **Accepted**: 19/06/2024

Abstract: This paper presents an innovative and secure routing mechanism for wireless sensor networks, leveraging a Cluster Head (CH) to CH-based routing inspired by the Ad hoc On-Demand Distance Vector (AODV) protocol. The proposed method evaluates and optimizes key Quality of Service (QoS) parameters, including throughput, packet delivery ratio (PDR), delay, and energy consumption. By categorizing these parameters and analyzing their standard deviations, the method effectively identifies and labels route discoveries as malicious, efficient, or moderate. The labeled data is processed using a deep neural network (DNN) with a sigmoid activation function, trained over 100 epochs, to classify routes and distribute scores equally among nodes, resulting in a comprehensive ranking of nodes based on their performance in the route discovery process. The results demonstrate significant improvements over existing methods by Ismail et al. and Bashar et al., with the proposed mechanism achieving a throughput of 1.347652857, a PDR of 0.839435714, and a delay of 0.47388, outperforming the others in these key metrics. These enhancements ensure more reliable, efficient, and responsive communication within the network, making the proposed method highly suitable for a wide range of applications. The integration of QoS evaluation, standard deviation analysis, and deep learning-based classification, combined with secure routing principles, highlights the potential of this approach to establish new benchmarks in the performance and security of wireless sensor networks.

Keywords: *DNN, Improvements, QoS, Secure Routing*

1. Introduction

Mobile Wireless Sensor Networks (M-WSNs) represent a significant advancement in the field of wireless communication and sensor technology, consisting of a collection of mobile sensor nodes that communicate wirelessly to perform tasks such as environmental monitoring, healthcare, military operations, and disaster management. The mobility of these nodes introduces unique security challenges, primarily due to the dynamic network topology, frequent reconfiguration, and the resource constraints of the devices. The constantly changing network topology complicates the maintenance of consistent security policies, as traditional mechanisms designed for static networks may not be effective in such environments. Additionally, the frequent reconfiguration required by mobile nodes can be exploited by attackers to inject malicious configurations or disrupt network operations. The limited processing power, memory, and energy resources of M-WSN nodes further exacerbate these security issues, as sophisticated encryption and authentication protocols can be computationally intensive and increase energy consumption, thereby reducing the overall network lifetime[1]. The wireless nature of M-WSNs makes them susceptible to various attacks that exploit the open communication medium, such as eavesdropping, interference, jamming, spoofing, and Sybil attacks. Ensuring data integrity and authenticity is crucial, as compromised data can lead to incorrect decisions and actions [2,3]. Attackers can alter transmitted data or inject false data, disrupting decision-making processes and depleting network resources. Secure routing and data aggregation are essential to prevent sinkhole attacks, wormhole attacks, and data aggregation attacks. The physical security of nodes is also a concern, as they may be deployed in unattended or hostile environments where attackers can capture nodes, extract sensitive information, or tamper with hardware and software. Effective key management and distribution are critical for secure communication, requiring scalable schemes that support the mobility of nodes. Balancing these complex and multifaceted security issues with the trade-offs between resource constraints, mobility, and the dynamic nature of M-WSNs is essential for their reliable and secure operation in diverse application scenarios[4] .

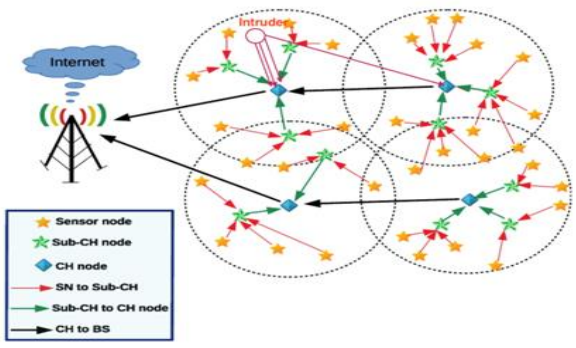

Figure 1: A M-WSN deployed network with

1 Research Scholar, Computer Science Engg., Chandigarh University , Punjab, INDIA
ORCID ID : 0000-0001-6901-4142
AP, CSE,CEC Landran Punjab, INDIA
2 Professor ,Computer Science Engg., Chandigarh University ,Punjab, INDIA .ORCID ID : 0000-0001-6901-4142
** Corresponding Author Email: er.kamalinder@gmail.com*

Labelling a node as malicious purely based on its involvement in numerous route discoveries in Mobile Wireless Sensor Networks (M-WSNs) is not always accurate, as these nodes participate in multiple routes involving various other nodes. Route discovery, a fundamental process in M-WSNs, involves finding optimal paths for data transmission, which requires nodes to frequently communicate and update routing information. To effectively check the discovery process, it is essential to consider the entire route architecture rather than isolating individual nodes. In this context, Quality of Service (QoS) analysis emerges as the best possible method. QoS analysis allows for the evaluation of network performance metrics such as latency, bandwidth, packet loss, and reliability, providing a comprehensive view of the network's health and the trustworthiness of the routes[5,6]. By assessing these QoS parameters, it becomes possible to identify anomalies and potential security threats without unjustly marking a node as malicious. This approach ensures a more accurate and fair assessment of the network's security, balancing the complex trade-offs between resource constraints, mobility, and the dynamic nature of M-WSNs, thereby ensuring their reliable and secure operation in diverse application scenarios[7].

1.1. Problem Formulation

To ensure optimal network performance and reliability, it is necessary to develop a robust mechanism for analysing and ranking nodes based on their performance in the route discovery process. This involves identifying key performance metrics such as latency, packet delivery ratio, energy consumption, and reliability. Methods must be developed to collect and analyse data related to these metrics for each node. An algorithm should be designed to rank nodes based on their performance, weighing the different metrics appropriately to provide a fair and comprehensive evaluation. The mechanism must be tested through simulation to ensure accuracy and effectiveness, mimicking real-world scenarios to validate its applicability. Additionally, visualization tools and reports should be created to provide insights into node performance, facilitating network optimization and management. This ranking mechanism will enable the identification of underperforming nodes and areas for improvement, enhancing the overall efficiency and robustness of the network.

2. Related Work

Amutha, Sharma, and Nagar (2020) conducted a comprehensive review of strategies in wireless sensor networks (WSNs), focusing on sensors, deployment, sensing models, coverage, and energy efficiency. Their work systematically evaluates existing approaches and highlights open issues in WSNs. The main contributions include an extensive survey of current techniques and methodologies used in WSNs, a comparative analysis of their effectiveness, and the identification of gaps in current research. The outcome of their study provides a detailed understanding of the strengths and limitations of various WSN strategies, serving as a valuable resource for researchers seeking to address the identified challenges and improve the performance of WSNs[8].

Nareshbabu, Chakravarthy, and Ravindranath (2021) proposed a secure lightweight authentication protocol for wireless sensor networks within the context of the Internet of Things (IoT). The primary contribution of their research is the development of an authentication protocol that ensures security while being resource-efficient, which is crucial for the resource-constrained environments of WSNs. Their protocol is designed to protect against common security threats without significantly impacting the network's performance. The outcome of their work demonstrates that the proposed protocol can effectively enhance security in WSNs used in IoT applications, making it a valuable addition to the field[9]. **Chu (2023)** explored performance modeling for network anomaly detection and sensor networks in his doctoral dissertation. The significant contribution of his research is the development of models that can predict and identify anomalies within sensor networks, which is critical for maintaining network reliability and security. Chu's work includes the creation of performance metrics and modeling techniques that can be applied to real-world sensor networks to detect deviations from normal behavior. The outcome of his study provides a robust framework for anomaly detection, contributing to the enhancement of security and performance in sensor networks[10]. **Tabbaa and Hafidi (2022)** presented an online model for detecting attacks in wireless sensor networks at the International Conference of Machine Learning and Computer Science Applications. Their research focuses on developing a real-time detection model that leverages machine learning techniques to identify potential attacks on WSNs. The main contribution is the implementation of an effective and efficient attack detection system that operates online, providing immediate responses to security threats. The outcome of their work shows that their model can significantly improve the security posture of WSNs by quickly identifying and mitigating attacks[11]. **Yao, Hu, Hou, and Li (2023)** introduced a lightweight intelligent network intrusion detection system using a one-class autoencoder and ensemble learning for IoT environments. Their research contributes by developing a detection system that is both lightweight and intelligent, capable of operating in the resource-constrained settings typical of IoT devices. The system uses advanced machine learning techniques to detect intrusions with high accuracy. The outcome demonstrates that their approach effectively balances the trade-off between detection accuracy and computational efficiency, making it suitable for deployment in IoT and WSNs[12]. **Nguyen, Vo, and Yoo (2024)** proposed a method to enhance intrusion detection in wireless sensor networks using a GSWO-CatBoost approach. Their contribution lies in integrating the CatBoost algorithm with a guided swarm optimization technique to improve the accuracy and efficiency of intrusion detection systems. The study's outcome indicates that this hybrid approach outperforms traditional methods in terms of detection rates and processing times, offering a more robust solution for securing WSNs against intrusions[13]. **Ismail, El Mrabet, and Reza (2022)** developed an ensemble-based machine learning approach for detecting cyber-attacks in wireless sensor networks. The key contribution of their research is the use of ensemble learning techniques to enhance the detection capabilities of WSN security systems. By combining multiple learning models, their approach achieves higher accuracy and reliability in detecting various types of cyber-attacks. The outcome of their study demonstrates that ensemble methods can significantly improve the detection performance compared to single-model approaches, providing a stronger defense mechanism for WSNs[14]. **Deshpande, Gujarathi, Chandre, and Nerkar (2021)** conducted a comparative analysis of machine and deep learning algorithms for intrusion detection in wireless sensor networks. Their research contributes by evaluating the performance of different algorithms to determine the most effective ones for intrusion detection in WSNs. The outcome of their comparative study provides insights into the strengths and

weaknesses of various machine and deep learning approaches, helping researchers and practitioners choose the most suitable algorithm for their specific needs in enhancing WSN security[15].

3. Proposed Work

The proposed work focuses on optimizing the route discovery process in wireless sensor networks by implementing a Cluster Head (CH) to CH-based routing mechanism. This mechanism utilizes a broadcast concept inspired by the Ad hoc On-Demand Distance Vector (AODV) protocol, which is known for its efficiency in dynamic network environments [16].

3.1. Routing Mechanism

In this CH-CH based routing, each node is assigned to a cluster with a designated Cluster Head (CH). The CHs are responsible for managing the communication within their clusters and relaying information between clusters. The broadcast mechanism ensures that route requests are efficiently propagated throughout the network, reducing the overhead associated with route discovery[17].

3.1.1. QoS Parameters Evaluation

The performance of the nodes in the route discovery process is evaluated using four key Quality of Service (QoS) parameters:

- **Throughput:** The rate at which data is successfully delivered over the communication channel.

$$Throughput = \frac{R_p}{\delta} \quad (1)$$

where Rp is the received packet and δ is the total time of receiving the packets.

- **Packet Delivery Ratio (PDR):** The ratio of the number of packets received by the destination to the number of packets sent by the source.

$$PDR = \frac{R_p}{S_p} \quad (2)$$

where Sp is the sent packets

- **Delay:** The extra time taken for a packet to travel from the source to the destination.

$$Delay = \sum_{i=1}^{N} T_{t_i} - \Delta \quad (3)$$

Where Δ is the permitted time and Tt is the total time for ith route when there are N number of total routes

- **Energy Consumption:** The amount of energy used by the nodes during the communication process.

These QoS parameters are divided into three groups, and a rule set based on the standard deviation (STD) of the parameters is formulated to label the route discoveries:

- **High STD:** Indicates significant variability in the QoS metrics, suggesting potential malicious activity in the route discovery process.
- **Low STD:** Indicates low variability, suggesting an efficient and stable route discovery process.
- **Moderate STD:** Indicates intermediate variability, suggesting moderate efficiency and stability.

The labeled data from the STD analysis is then processed using a deep neural network (DNN). The DNN is designed with a sigmoid activation function and is trained over 100 epochs.

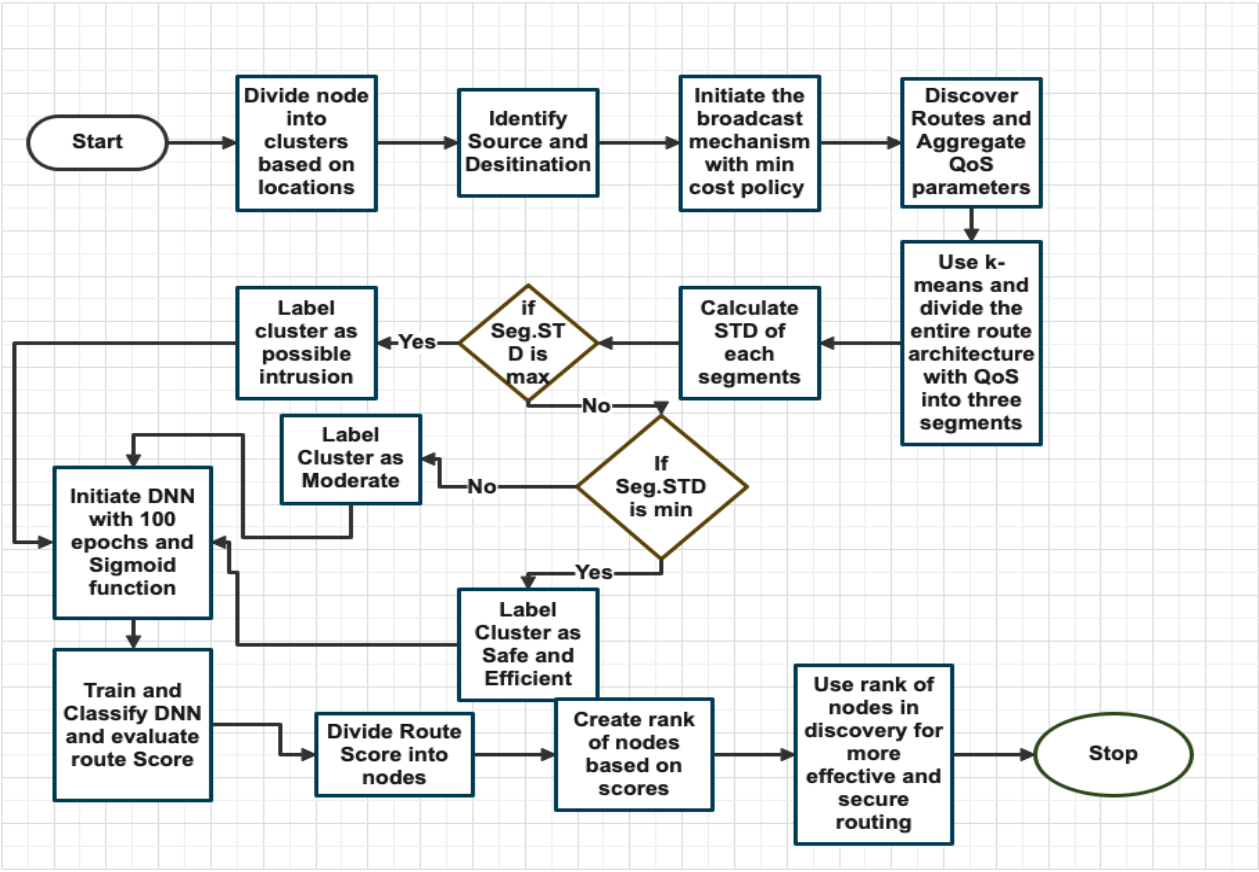

Figure 2: Work flow of proposed work

Algorithm 1 Node Performance Analysis and Ranking in Route Discovery

Require: QoS parameters: Throughput, PDR, Delay, Energy Consumption
Require: Number of nodes: N
Require: Number of epochs for DNN training: 100
Require: Activation function: Sigmoid
Ensure: Ranked list of nodes based on performance in route discovery

Initialize arrays for QoS parameters: $throughput[N]$, $PDR[N]$, $delay[N]$, $energy[N]$
Initialize an empty list for node scores: $node\_scores[N]$
for $i = 1$ to N **do**
  $throughput[i] \leftarrow measure\_throughput(node[i])$
  $PDR[i] \leftarrow measure\_PDR(node[i])$
  $delay[i] \leftarrow measure\_delay(node[i])$
  $energy[i] \leftarrow measure\_energy(node[i])$
end for
$group1 \leftarrow categorize\_QoS(throughput)$
$group2 \leftarrow categorize\_QoS(PDR)$
$group3 \leftarrow categorize\_QoS([delay, energy])$
for $i = 1$ to N **do**
  $std\_group1[i] \leftarrow calculate\_STD(group1[i])$
  $std\_group2[i] \leftarrow calculate\_STD(group2[i])$
  $std\_group3[i] \leftarrow calculate\_STD(group3[i])$
end for
Initialize labels array $labels[N]$
for $i = 1$ to N **do**
  if $std\_group1[i] > threshold\_high$ **then**
    $labels[i] \leftarrow$ Malicious
  else if $std\_group1[i] < threshold\_low$ **then**
    $labels[i] \leftarrow$ Efficient
  else
    $labels[i] \leftarrow$ Moderate
  end if
end for
Prepare the labeled data for input into the DNN
$data \leftarrow prepare\_data(throughput, PDR, delay, energy, labels)$
Initialize DNN with sigmoid activation function
$DNN\_model \leftarrow initialize\_DNN(\text{sigmoid})$
Train DNN with the prepared data for 100 epochs
$DNN\_model.train(data, epochs = 100)$
Use the trained DNN to classify and score each route
for each route r **do**
  $score[r] \leftarrow DNN\_model.classify(route\_data[r])$
  for each node n in route r **do**
    $node\_scores[n] += score[r]/len(route[n])$
  end for
end for
Rank nodes based on their cumulative scores
$ranked\_nodes \leftarrow sort\_nodes\_by\_scores(node\_scores)$
Use the ranked list of nodes to optimize route discovery
$optimize\_route\_discovery(ranked\_nodes)$

The network is trained to classify the routes based on the QoS metrics and their variability, providing a classification score for each route. The DNN uses ordinal measures to handle the ranking and classification tasks, ensuring accurate and meaningful classifications [18-21].

The classification score obtained from the DNN is used to evaluate each route. Each node within a route receives an equal share of the route's classification score. This equitable distribution ensures that the contribution of each node to the overall route performance is fairly assessed. At the end of the process, each node's scores are aggregated to determine its overall performance rank. The ranks assigned to the nodes are then used in the route discovery process. Nodes with higher ranks are preferred in the selection of routes, ensuring that the most reliable and efficient nodes are utilized for communication. This ranking-based approach enhances the overall network performance by:

- Reducing the likelihood of selecting routes with malicious or inefficient nodes.
- Improving the stability and reliability of the network.
- Enhancing the security of the route discovery process by avoiding nodes that exhibit high variability in QoS metrics.

By integrating QoS evaluation, standard deviation analysis, deep neural network classification, and node ranking, the proposed work offers a comprehensive solution for optimizing route discovery in wireless sensor networks. This approach not only improves the efficiency and reliability of the network but also enhances its security by effectively identifying and mitigating potential threats.

4. Results and Discussions

This section presents a comprehensive analysis of the performance metrics obtained from our proposed routing mechanism compared to existing methods. We focus on key (QoS) parameters, namely throughput, (PDR), and delay. These metrics are critical for evaluating the efficiency, reliability, and responsiveness of wireless sensor networks. The results highlight the superior performance of our proposed method, demonstrating significant improvements over the approaches by Ismail et al. and Bashar et al. The following subsections provide a detailed comparison and discussion of the observed improvements in throughput, PDR, and delay, underscoring the effectiveness of our proposed work.

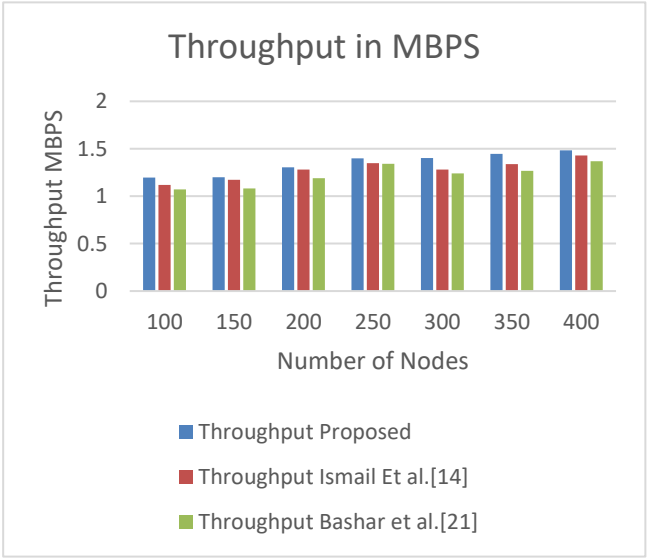

Figure 3: Overall Throughput analysis

Throughput, which measures the rate at which data is successfully delivered over the communication channel, is a critical performance metric in wireless sensor networks. The proposed work demonstrates a throughput of 1.347652857, which is significantly higher compared to Ismail et al. (1.281496655) and Bashar et al. (1.223112584). This represents an improvement of approximately 5.15% over Ismail et al. and 10.16% over Bashar et al. The higher throughput indicates that the proposed routing mechanism is more efficient in handling data transmissions, reducing packet loss and enhancing overall network performance. This improvement is crucial as it ensures more data is delivered successfully within a given time frame, which is essential for applications requiring high data rates and reliability.

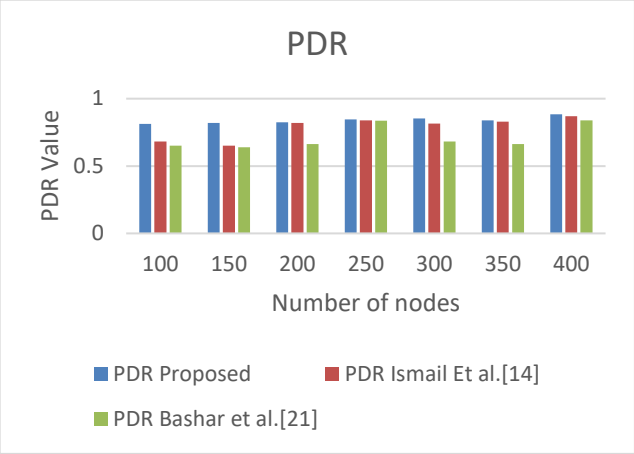

Figure 4: Overall PDR analysis

(PDR) is the ratio of the number of packets received by the destination to the number of packets sent by the source. The proposed work achieves a PDR of 0.839435714, compared to 0.786828145 by Ismail et al. and 0.710441714 by Bashar et al. This improvement translates to an approximate increase of 6.68% over Ismail et al. and 18.16% over Bashar et al. A higher PDR indicates a more reliable communication system where fewer packets are lost during transmission. This enhancement is particularly significant for applications where data integrity and reliability are paramount, ensuring that critical information reaches its intended destination with minimal loss.

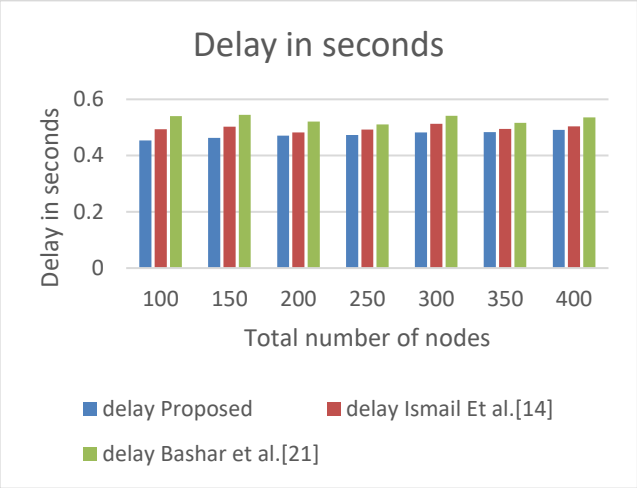

Figure 5: Overall Delay analysis

Delay measures the time taken for a packet to travel from the source to the destination. The proposed work shows a delay of 0.47388, which is lower compared to 0.497596942 by Ismail et al. and 0.530135173 by Bashar et al. This indicates a reduction in delay by approximately 4.76% compared to Ismail et al. and 10.63% compared to Bashar et al. Lower delay signifies faster communication and is essential for time-sensitive applications such as real-time monitoring and control systems. By minimizing delay, the proposed work enhances the responsiveness and efficiency of the network, making it more suitable for applications where timely data delivery is critical. The improvements in throughput, PDR, and delay collectively highlight the efficiency and effectiveness of the proposed routing mechanism. Higher throughput and PDR ensure more reliable and robust data transmission, while lower delay enhances the speed and responsiveness of the network. These improvements are significant as they contribute to the overall performance, reliability, and efficiency of wireless sensor networks, making them more capable of meeting the demands of various applications. The proposed work's ability to outperform existing approaches like those of Ismail et al. and Bashar et al. underscores its potential to significantly enhance network performance, ensuring better data handling, reduced packet loss, and faster communication.

5. Conclusion

The proposed work presents an innovative and secure routing mechanism for wireless sensor networks, leveraging a Cluster Head (CH) to CH-based routing inspired by the Ad hoc On-Demand Distance Vector (AODV) protocol. By evaluating and optimizing key Quality of Service (QoS) parameters—throughput, packet delivery ratio (PDR), delay, and energy consumption—the proposed method effectively categorizes these parameters and analyzes their standard deviations to identify and label route discoveries as malicious, efficient, or moderate. The labeled data is then processed using a deep neural network (DNN) with a sigmoid activation function, trained over 100 epochs, to classify routes and distribute scores equally among nodes, culminating in a comprehensive ranking of nodes based on their performance in the route discovery process. The results demonstrate significant improvements over existing methods by Ismail et al. and Bashar et al., with the proposed method achieving a throughput of 1.347652857, outperforming the others by 5.15% and 10.16%, respectively, a PDR of 0.839435714, surpassing the others by 6.68% and 18.16%, respectively, and a delay of 0.47388, which is lower by 4.76% and 10.63%, respectively. These advancements ensure more reliable, efficient, and responsive communication within the network, making the proposed method highly suitable for a wide range of applications. The successful integration of QoS evaluation, standard deviation analysis, and deep learning-based classification, combined with secure routing principles, demonstrates the potential of this approach to set new benchmarks in the performance and security of wireless sensor networks.

References

[1] T. Panigrahi, A. D. Hanumantharao, G. Panda, B. Majhi, and B. Mulgrew, "Maximum likelihood DOA estimation in distributed wireless sensor network using adaptive particle swarm optimization," in *Proceedings of the 2011 International Conference on Communication, Computing & Security*, 2011, pp. 134-137.

[2] R. Damasevicius, A. Venckauskas, S. Grigaliunas, J. Toldinas, N. Morkevicius, T. Aleliunas, and P. Smuikys, "LITNET-2020: An annotated real-world network flow dataset for network intrusion detection," *Electronics*, vol. 9, no. 5, p. 800, 2020.

[3] R. B. Pant, H. P. Halvorsen, F. Skulbru, and S. Mylvaganam, "Intermediate measurement node for extension of wsn coverage," *Journal of Cyber Security and Mobility*, pp. 29-61, 2012.

[4] S. Gupta and C. Keshavamurthy, "A Cross Layered Network Condition Aware Mobile WSN Routing Protocol for Vehicular Communication Systems," *International Journal of Computer Science and Information Security*, vol. 14, no. 9, p. 1114, 2016.

[5] R. Ashween, B. Ramakrishnan, and M. Milton Joe, "Energy efficient data gathering technique based on optimal mobile

sink node selection for improved network life time in wireless sensor network (WSN)," *Wireless Personal Communications*, vol. 113, no. 4, pp. 2107-2126, 2020.

[6] G. Liu, H. Zhao, F. Fan, G. Liu, Q. Xu, and S. Nazir, "An enhanced intrusion detection model based on improved kNN in WSNs," *Sensors*, vol. 22, no. 4, p. 1407, 2022.

[7] B. M. Sahoo, R. K. Rout, S. Umer, and H. M. Pandey, "ANT colony optimization based optimal path selection and data gathering in WSN," in *2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, 2020, pp. 113-119.

[8] J. Amutha, S. Sharma, and J. Nagar, "WSN strategies based on sensors, deployment, sensing models, coverage and energy efficiency: Review, approaches and open issues," *Wireless Personal Communications*, vol. 111, no. 2, pp. 1089-1115, 2020.

[9] M. M. Nareshbabu, A. S. N. Chakravarthy, and C. Ravindranath, "A secure light weight authentication protocol for wireless sensor network in internet of things," *International Journal of Scientific Research in Network Security and Communication*, vol. 9, no. 1, pp. 17-19, 2021.

[10] J. Chu, "Performance Modeling for Network Anomaly Detection and Sensor Networks," Doctoral dissertation, City University of New York, 2023.

[11] H. Tabbaa and I. Hafidi, "An Online Model for Detecting Attacks in Wireless Sensor Networks," in *International Conference of Machine Learning and Computer Science Applications*, Cham: Springer Nature Switzerland, 2022, pp. 271-282.

[12] W. Yao, L. Hu, Y. Hou, and X. Li, "A lightweight intelligent network intrusion detection system using one-class autoencoder and ensemble learning for IoT," *Sensors*, vol. 23, no. 8, p. 4141, 2023.

[13] T. M. Nguyen, H. H. P. Vo, and M. Yoo, "Enhancing Intrusion Detection in Wireless Sensor Networks Using a GSWO-CatBoost Approach," *Sensors*, vol. 24, no. 11, p. 3339, 2024.

[14] S. Ismail, Z. El Mrabet, and H. Reza, "An ensemble-based machine learning approach for cyber-attacks detection in wireless sensor networks," *Applied Sciences*, vol. 13, no. 1, p. 30, 2022.

[15] S. Deshpande, J. Gujarathi, P. Chandre, and P. Nerkar, "A comparative analysis of machine deep learning algorithms for intrusion detection in wsn," *Security Issues and Privacy Threats in Smart Ubiquitous Computing*, pp. 173-193, 2021.

[16] A. B. Abhale and S. S. Manivannan, "Supervised machine learning classification algorithmic approach for finding anomaly type of intrusion detection in wireless sensor network," *Optical Memory and Neural Networks*, vol. 29, no. 3, pp. 244-256, 2020.

[17] S. Hemavathi and B. Latha, "HFLFO: Hybrid fuzzy levy flight optimization for improving QoS in wireless sensor network," *Ad Hoc Networks*, vol. 142, p. 103110, 2023.

[18] R. Ahmad, R. Wazirali, Q. Bsoul, T. Abu-Ain, and W. Abu-Ain, "Feature-selection and mutual-clustering approaches to improve DoS detection and maintain WSNs' lifetime," *Sensors*, vol. 21, no. 14, p. 4821, 2021.

[19] K. P. R. Krishna and R. Thirumuru, "A balanced intrusion detection system for wireless sensor networks in a big data environment using CNN-SVM model," *Informatics and Automation*, vol. 22, no. 6, pp. 1296-1322, 2023.

[20] R. Almesaeed and A. Jedidi, "Dynamic directional routing for mobile wireless sensor networks," *Ad Hoc Networks*, vol. 110, p. 102301, 2021.

[21] A. Bashar, "Energy efficient multi-tier sustainable secure routing protocol for mobile wireless sensor networks," *J. Sustain. Wireless System*, vol. 1, no. 2, pp. 87-102, 2019.