Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

An Energy-Efficient and Secured Routing Protocol in Wireless Sensor Network Using Machine Learning Algorithm

Dr. F. Rahman[1], Omprakash Dewangan[2]

[1]Assistant Professor, Faculty of CS & IT, Kalinga University, Naya Raipur, Chhattisgarh, India, ku.frahman@kalingauniversity.ac.in
[2]Assistant Professor, Faculty of CS & IT, Kalinga University, Naya Raipur, Chhattisgarh, India, ku.omprakashdewangan@kalingauniversity.ac.in

Wireless Sensor Systems (WSNs) are employed for data collection and transmission to the Base Station (BS). This field designs and analyzes routing issues inside the WSN network. Maintaining the appropriate energy levels in WSN networks is critical to prevent packet loss or drop, minimize power consumption, and avoid deterioration in node efficiency, all while reducing packet delivery delays throughout the networks. To make routing decisions more effective, it is crucial to assess the power utilization of the nodes and optimize the network's total efficiency using machine learning algorithms. One of the main difficulties in clustering sensor nodes is balancing loads while improving the use of Cluster Heads (CH) and members. The research has suggested a hybrid C-means donkey-smuggler optimizing approach to enhance the routing efficiency of WSNs. The research has verified the effectiveness of the suggested approach by evaluating its performance using measures such as packet delivery ratio, network lifespan, energy use, and latency. The proposed solution surpasses others and produces a very effective network operation.

Keywords: Wireless Sensor Systems, Routing Protocol, Energy Efficiency, Security.

1. Introduction

A Wireless Sensor Network (WSN) consists of several sensor nodes and gateway nodes that gather and share data from the surrounding environment [1][18]. The network consists of inexpensive, compact sensor nodes that collect data using powerful computational capabilities and little bandwidth. WSN is used for landslide monitoring, military observation, medical care, subsurface water tracking, and mining activities [26]. In these applications, the WSN nodes are placed in the real-time environment to gather data and transmit it to the sink or central server. WSNs encounter a primary limitation in regularly replacing batteries. The routing protocol's architecture prioritizes energy efficiency and includes multicast capabilities to facilitate real-time applications [2][19][20]. Creating an energy-efficient routing system is one of the least attention-seeking research issues.

To ensure the efficient operation of the WSN network, it is necessary to solve critical issues such as coverage difficulties, scalability issues, challenges related to the surroundings, energy consumption, and localization [24]. Wireless networks use more energy when sending information than during processing and information reception [3] [2].

Energy consumption rises while data is transferred over greater distances. The central hub that receives data gathered by SNs is called the Base Station (BS) [4][21]. The central hub is a high-capacity machine with ample storage and processing capabilities, and it operates without any power limitations [5]. One of the most intellectually engaging occupations in WSN involves efficiently transferring data to a BS while conserving energy [28][30]. Distance has a significant role in energy attenuation during data transmission—long-distance transmission results in more substantial energy loss. Multi-hop communication in WSN reduces the transmission length since it facilitates short-range communication [6][23].

Several other multi-hop routing techniques have previously been suggested. The routing algorithms are classified as data-centric, geographically-based, and grouping or hierarchy-based systems [7]. This study effectively addresses vulnerability using fuzzy rules to optimize cluster formation and facilitate group-based routing. Analyzing the practical scenario of the donkey-smuggler method makes it simpler to prevent traffic congestion and choose the most efficient network route for quicker routing. The suggested approach should have reduced energy consumption and provided faster routing with lower time complexity via an improved hybrid c-means donkey-smuggler method.

2. Related Works

WSNs have gained significant recognition as a promising technology in recent decades. Scholars have implemented many routing protocols to extend the network's lifespan and reduce energy consumption. El Khediri et al. introduced a k-means method that divides the data identified by the nodes into distinct groups with participation values of either 0 or 1 [8][25]. This approach enhances the rate at which convergence occurs and improves the likelihood of obtaining the optimal solution. It exhibits reduced complexity and utilizes the directed graph inside the networks. This method's primary characteristic is its ability to offer soft-distributed grouping.

Hussien et al. suggested employing the Crow Search Algorithm (CSA) for the power-generating system in this study [9]. The CSA method is a meta-heuristic method. The primary inspiration for this method was derived from the foraging behavior of crows in their quest for food. The crow is a brilliant bird that observes other birds, conceals their food, and grabs it while they are away.

Sahoo et al. elucidated network transport design issues using the BAT algorithm in this method [10][27]. The BAT method is used to adjust the nodes' positions based on the fitness function produced by the process. The present position's fitness score is equivalent to the value of the prior location. The area is modified if the current fitness score exceeds the initial fitness value.

The Butterfly Optimization Algorithm (BOA) is implemented to efficiently pick the Cluster Head (CH) from many nodes [11]. The choice of the CH can be improved by considering the node centrality, node level, length to the BS, length to nearby nodes, and the nodes' residual

power. Ant Colony Optimization (ACO) determines the BS and CH path [12]. The ACO algorithm selects the most efficient route based on node level, residual power, and distance. By using this optimization methodology, the energy utilization is lowered while simultaneously reducing packet loss.

This research discusses the Hybrid Multihop Partition-Based Clustering (HMPBC) approach, which aims to improve the network's lifespan and distribute the network load more evenly [13][29]. The wireless network region is divided into many areas, and the formation of singular chain-like structures characterizes each group zone. CH choosing networks during data propagation time depends on the remaining energy of the nodes.

Keerthika et al. have proposed an improved routing-Gi protocol for a mobile sink in WSNs [14]. The introduction of routing-Gi has lowered packet loss rate, improved energy efficiency, and prolonged the lifespan of networks for mobile sinks in relevant conditions. The communication length is reduced to a minimum.

The research has studied a routing method for WSNs based on trust, energy-awareness, and security [15]. The goal of this method is to achieve efficient communication. The novel trust score computation technique effectively identified hostile participants in WSNs. Decision tree methods, including spatiotemporal restrictions, were employed to choose the most efficient path.

Al Aghbari et al. introduced a routing protocol with optimization techniques [16]. This protocol involves clustering, where the CH selection is done using an enhanced Artificial Bee Colony (ABC) algorithm. The authors use parameters such as location, density, and power of CHs to improve the conventional ABC algorithm.

El Alami et al. suggested an Enhanced Clustering Hierarchy (ECH) method to achieve energy efficiency in WSNs [17]. The ECH technique facilitates communication between surrounding and overlapping nodes utilizing alternating sleep and wakefulness periods. The duration of network operation is prolonged while the amount of duplicated data is reduced.

Although the routing methods mentioned above exist, the energy usage problem must be solved due to the grouping and routing strategies utilized. This research proposes a solution by introducing a machine learning-based root node choosing and an integrated searching algorithm-based routing method. The goal is to improve WSN's energy efficiency.

3. Proposed Secured and Energy-Efficient Routing in WSN

3.1 Donkey–Smuggler Method

The smuggler determines the donkey's target (optimal solution) and can modify the target or establish the most efficient route based on the optimal solution. Upon detecting signs of congestion or overloading, the smuggler establishes two channels to alleviate network traffic. The general model for the Donkey–Smuggler Method is shown in Figure 1.

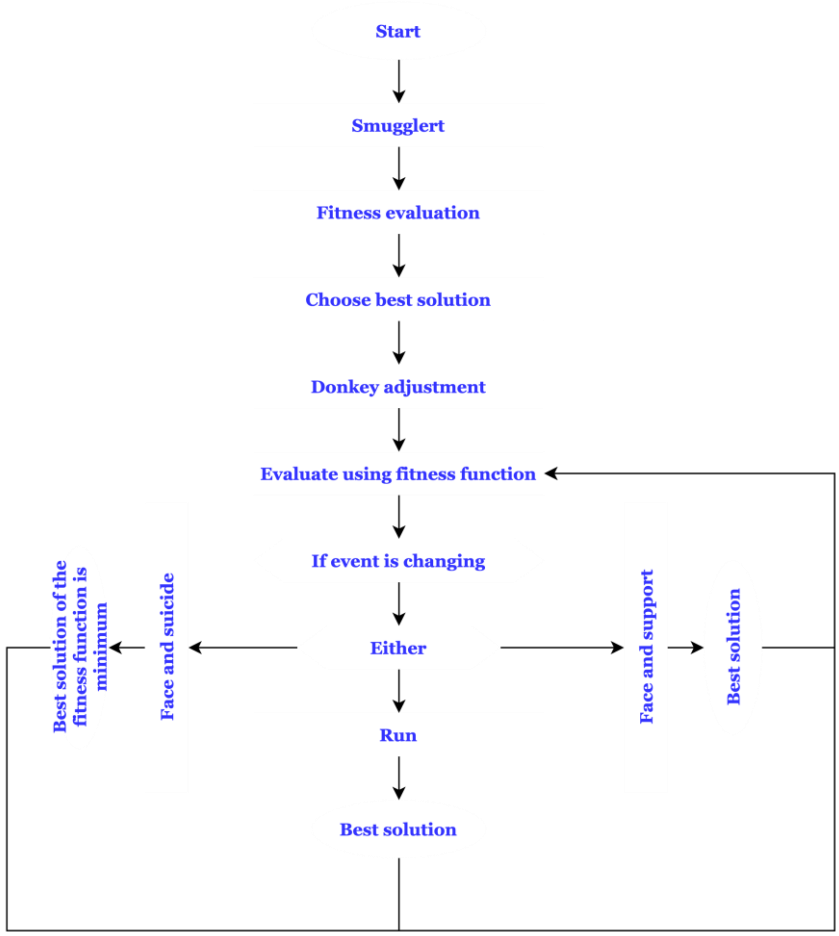

Figure 1. Donkey–Smuggler model

The similarity between two data points inside a single group is expected to be strong, whereas two points corresponding to separate clusters are expected to be dissimilar. The research suggests using this hybrid approach to minimize the distance, mitigate packet loss, and optimize energy consumption.

Step 1: Determine the desired number of clusters and establish the optimal degree of fuzziness for each cluster.

Step 2: Utilize data to determine the first cluster center.

Step 3: Identify the nth most severe samples from each cluster center.

Step 4: Calculate the average value for every group's most extreme samples.

Step 5: Invert the coordinates of each estimated mean and then determine the nearest data point to each group's center utilizing different pairwise lengths.

Step 6: Upon completing the iteration, determine the group's center and accompanying data for every group or modify the distance metric.

3.2 Routing Method

This study introduces a cluster-based routing method that leverages an improved hybrid c-means donkey-smuggler method for achieving energy-efficient routing. The process for calculating the planned steering is as follows:

Stage 1: Utilize sensor hubs' energy levels and coordinates.

Stage 2: Transmit "DATA" wallets to all neighboring hubs from the BS and determine the distances between the hubs and the BS and between the hubs.

Stage 3: Utilize the hybrid C-means algorithm to calculate the optimal grouping of data points into c clusters based on their distances.

Stage 4: Employing BS as the controlling system, carry out the CH selection for all groupings by considering nodes' distances and energy levels.

Stage 5: Perform course disclosure by determining the shortest route from each node to the BS via the CH.

Stage 6: Transmit information collected from hubs to CHs via the shortest route established in stage 5, then distribute it based on clustering principles.

Stage 7: Collect data at the BS.

Stage 8: If no less than half of the nodes' energy levels are exhausted, STOP.

Stage 9: Evaluate the significance of the CH pivot.

Stage 10: If the answer is affirmative, go to stage 4. Alternatively, go to step 6.

The sensor hubs collect data and transmit it to the BS periodically. The computation stops when the energy levels of half of the hubs are drained and have less than 10% of the initial energy phase.

3.3 Security Model

The study's objective is to monitor the functioning of the network and provide protection against various types of assaults on the WSN. The proposed method establishes network groups to preserve efficiency. The proposed method has excellent potential to enhance mobility management, network flexibility, and power efficiency. The research is inclined to employ this to construct network groups. The security mechanism is installed at the end of the BS.

3.4 Security model

The suggested security model or Intrusion Detection System (IDS) has two phases: initial training using sample sequences and subsequent categorization of hostile nodes. A standard network is first established with 100 nodes to produce learning samples. The same networking is utilized for launching assaults and monitoring the network traffic circumstances. A training database will be built using the specimens of produced traffic patterns. The database will include the following characteristics that follow:

1. The node ID is an additional learning variable eliminated during training. This attribute is

employed to establish the node's unique identification.

2. Overall send data bytes: the whole quantity of data sent.

3. Overall forwarded bytes: the aggregate count of bytes sent via the node for routing purposes.

4. Overall route request submerged: the number of route requests or HELLO messages disseminated within a specified sample period.

5. Round Trip Time: the node's round trip time refers to the time it takes for a packet of data to go from the source node to the destination node and back again.

6. Packet loss rate: the proportion of lost packets throughout various communication conditions.

7. Energy level rate of shifts: the difference in battery level over a specific sample period.

8. Buffer length refers to the difference in buffer size during a certain sample period.

9. Class labeling: The label options are standard, Blackhole, wormhole, Selective transmission, HELLO flood assault Jamming, and Exhaustion assault.

The training database includes six significant features or qualities and seven additional categories. Therefore, it is necessary to use a multi-class classification based on the literature. The research has discovered multi-class issues. The BS's IDS modeling has been created using these two machine-learning approaches. One significant benefit is that this centralized approach does not impose any additional burden on the sensor nodes. Figure 2 showcases the suggested IDS concept designed to enhance WSN security.

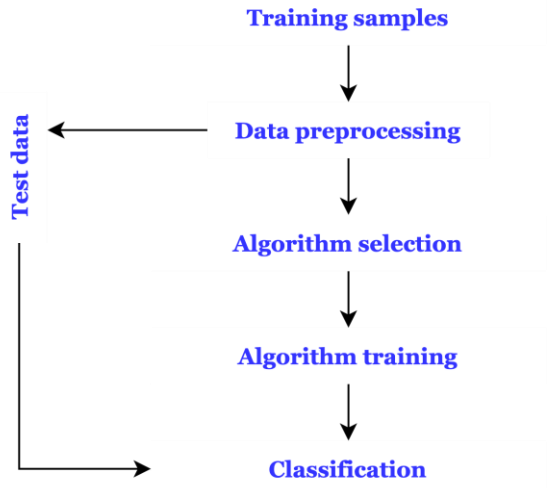

Figure 2. IDS model in WSN

The training sample has six characteristics and a category label. The qualities are quantified using distinct scales. The research uses a min-max normalization approach to transform the data into a range of 0 to 1. Before transmitting information for learning, the research chose a random subset of 30% of the specimens as test information. The dataset is currently being used to validate the trained system. Once the information has been normalized during the

preprocessing step, the consumer chooses a classification for the reason for conducting experiments. The remaining training data are used to train the specified classification. Once an approach has been taught, it will accurately categorize each specimen given for testing.

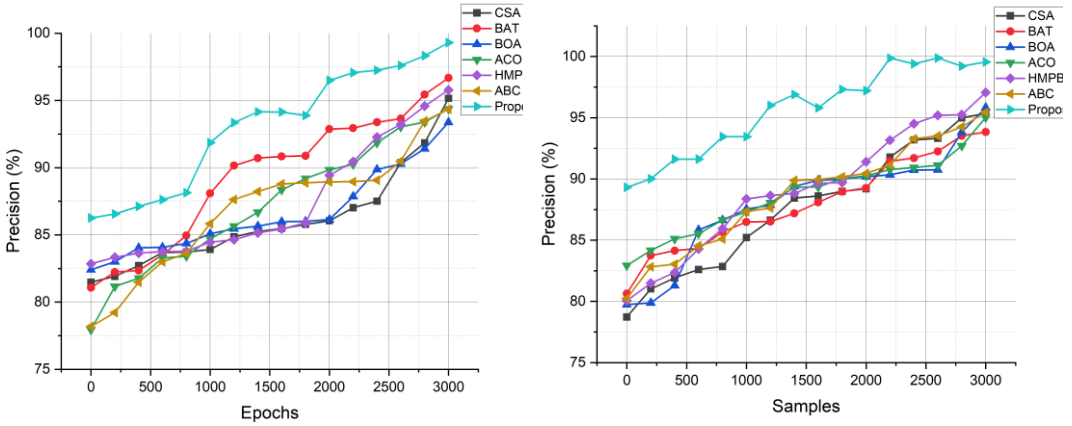

Figure 3. Precision analysis for (a). Different epochs and (b). Different samples

The validation findings obtained during the test information categorization are shown in Figures 3(a) and 3(b). The studies were conducted using two experimental settings, first using a predetermined dataset. In this scenario, a set of 1000 samples is employed to train both the CSA, BAT, BOA, ACO, HMPBC, ABC, and proposed models. The models are trained using varying numbers of epoch cycles. All methods exhibit an increase in accuracy as the number of optimizing cycles increases. The proposed method shows superior growth compared to the other classifiers. The quantity of samples is augmented in each experiment using both techniques. Both methods in this experiment provided strong performance, but the research highly suggests using the proposed approach for this prediction issue. Optimizing the learning variables enhances the accuracy.

4. Simulation Analysis and Outcomes

The objective of this research is to enhance the real-time efficiency of the offered algorithms to ensure network security in real-time scenarios. A Network Simulator (NS-2.35) has been established. The system is equipped with random mobility to showcase the mobile sensor nodes. The simulation region is set at 1000 X 1000 meters. The network has a predetermined number of nodes, namely 100. A distinct group of malicious nodes is introduced into the networks.

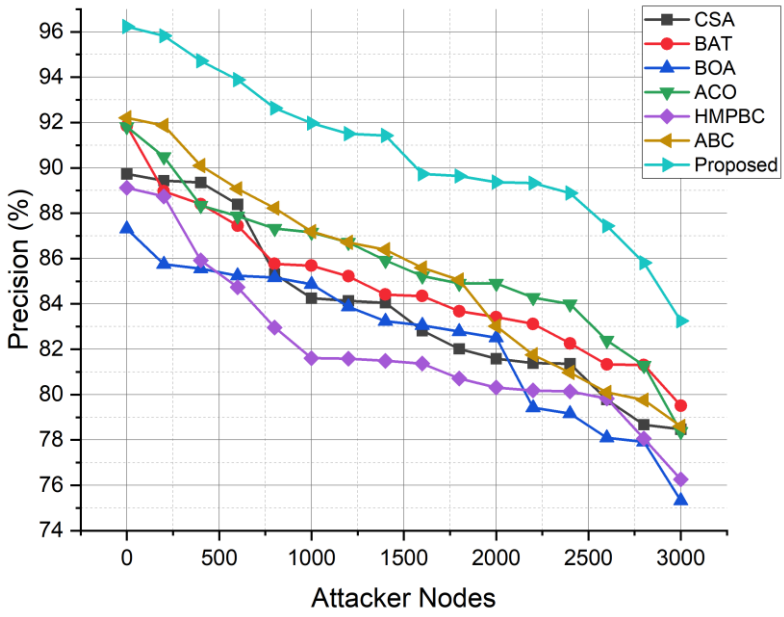

Figure 4. Precision analysis of different attacker nodes

The precision of real-time identification is shown in Figure 4. Figure 4 illustrates the correlation between the number of epoch cycles and the various experiments while keeping the number of attackers constant at 15 for all kinds. Based on the findings, the detection efficiency of the proposed method exhibits a significant increase as the number of epoch cycles increases. The effectiveness of both strategies in terms of attack size has risen consistently, although it could be better compared to earlier instances. This model offers efficient detection capabilities and comprehensive information on the suggested IDS system.

The proposed method has robust security measures to counter various forms of assault. This section analyzes the network performance of the suggested IDS model. Packet Delivery Ratio (PDR) is analyzed and compared using different methods. This denotes the quantity of data packets that have been correctly sent. The suggested model's PDR is quantified as a percentage. Figure 5(a) illustrates the effectiveness of the proposed method. The X-axis of this line graph represents the frequency of assaults.

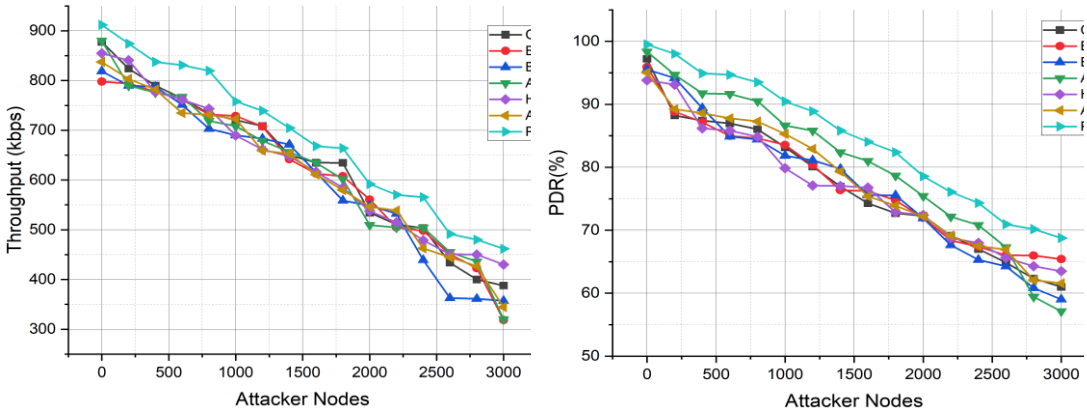

Figure 5(a). Throughput analysis and 5(b). PDR analysis of different attacker nodes

The Y-axis represents the proportion of packets that have been successfully delivered. During the trials, varying numbers of attacker nodes are inserted into a fixed set of 100 nodes. During this process, the effectiveness is documented. Based on the experiments, it has been determined that the efficacy of the proposed model is more effective than the proposed model when subjected to assault situations. The proposed method can identify and minimize the effects of assaults.

Figure 5(b) illustrates the efficiency of the network using both techniques, specifically in terms of throughput. The network settings and the number of nodes stay unchanged from the previous test. The throughput is a crucial metric for quantifying the efficiency of a network. The result varies based on the channel capacity. The amount of data sent during a specific period from the total available is called throughput. The network's throughput is quantified in kbps. Based on the experimental findings, the effectiveness of the suggested method is deemed more satisfactory. The proposed methodology is the most superior of the three deployed ways.

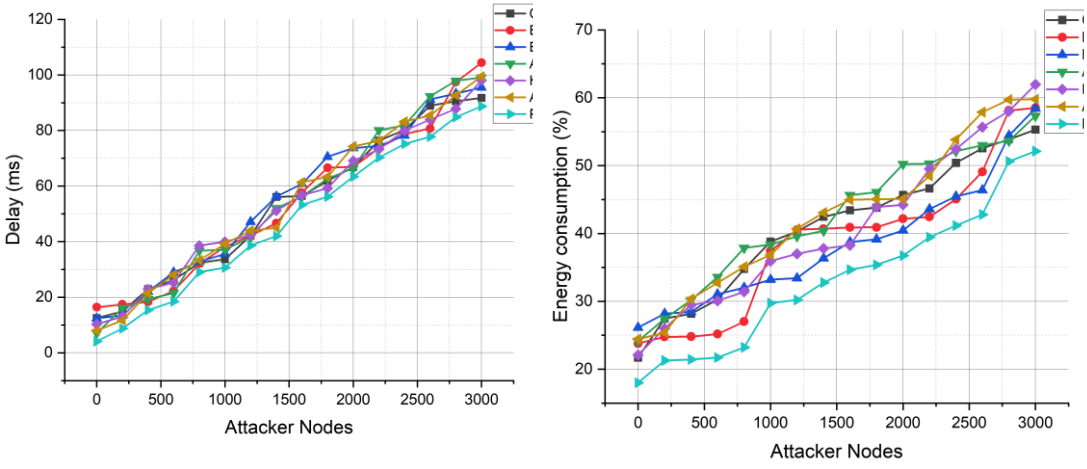

Figure 6(a). Delay analysis and 6(b). Energy consumption analysis of different attacker nodes

Figures 6(a) and 6(b) provide information on the end-to-end latency and the network's energy usage during the assault scenarios. The network and simulation settings remain unchanged from the prior experimental findings. Figure 6(a) illustrates the end-to-end latency of a network. The delay refers to the time it takes for a packet to be sent over a network. The delay is quantified in milliseconds. Based on the findings, the delay of the proposed method at times registers as 0 due to the absence of packet delivery during an attack. The proposed method demonstrates efficient performance and a high success rate in delivering packets. The suggested versions of the proposed method effectively protect the network from various types of threats. Figure 6(b) illustrates the energy consumption efficiency of the WSN. Energy consumption refers to the set quantity of energy consumed for various network processes. The energy consumption of the proposed method procedures is quantified in joules. The real-world effects of nodes' energy usage have shown that the proposed method is more reliable and energy-efficient than the earlier accessible proposed method.

5. Conclusion and Discussions

This research proposes a new routing method for effective cluster-based sensor networks. The program optimizes the group formation approach using a hybrid c-means donkey-smuggler method. This strategy aims to enhance the network performance by enhancing cluster-based routing. This approach utilizes an integrated clustering system with the donkey-smugger method to efficiently guide packages in WSNs. The vitality-exhibiting technique adjusts the weights, resulting in an extended system lifespan.

The research has taken into account four specific aspects that significantly impact the durability of the CH: the enduring vitality of the CH, the gap between the CH and the sinking hub, the gap between the sensing hub and the CH, and the condition of the CH. These factors are crucial in determining the efficiency and lifespan of the system. The research evaluated the suggested computation using network simulations, using the components above as an improved hybrid C-means don-key-smuggler method. The yield calculation of the proposed method was used to determine the CH for the hub to join as a member. Based on the results obtained in this study, it has been observed that the suggested approach outperformed the channel, grouping, and notice methods regarding energy consumption and system lifespan. This is attributed to the usage of clustering rules derived through learning and the application of cluster-based routing. A limitation of this approach is the assumption that all hubs are trustworthy, which is only sometimes feasible.

References

1. Verma, S., Zeadally, S., Kaur, S., & Sharma, A. K. (2021). Intelligent and secure clustering in wireless sensor network (WSN)-based intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems, 23(8), 13473-13481.
2. Jelena, T., & Srđan, K. (2023). Smart Mining: Joint Model for Parametrization of Coal Excavation Process Based on Artificial Neural Networks. Archives for Technical Sciences, 2(29), 11-22.
3. Zagrouba, R., & Kardi, A. (2021). Comparative study of energy efficient routing techniques in wireless sensor networks. Information, 12(1), 42.

4. Praveenchandar, J., Venkatesh, K., Mohanraj, B., Prasad, M., Udayakumar, R. (2024). Prediction of Air Pollution Utilizing an Adaptive Network Fuzzy Inference System with the Aid of Genetic Algorithm. Natural and Engineering Sciences, 9(1), 46-56.
5. Bhadouria, A. S., Bhadouria, I. S., Patel, V., & Upasani, A. (2024). Performance Analysis of Internet of Things Enabled WSN for Agriculture. Smart Engineering Technology and Management, 382.
6. Khamayseh, Y.M., Mardini, W., Aldwairi, M., & Mouftah, H.T. (2020). On the Optimality of Route Selection in Grid Wireless Sensor Networks: Theory and Applications. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 11(2), 87-105.
7. Ding, Q., Zhu, R., Liu, H., & Ma, M. (2021). An overview of machine learning-based energy-efficient routing algorithms in wireless sensor networks. Electronics, 10(13), 1539.
8. Cabra, J. L., Parra, C., & Trujillo, L. (2022). Earprint touchscreen sensoring comparison between hand-crafted features and transfer learning for smartphone authentication. Journal of Internet Services and Information Security JISIS, 12(3), 16-29.
9. Hussien, A. G., Amin, M., Wang, M., Liang, G., Alsanad, A., Gumaei, A., & Chen, H. (2020). Crow search algorithm: theory, recent advances, and applications. IEEE Access, 8, 173548-173565.
10. Giji Kiruba, D., Benita, J., & Rajesh, D. (2023). A Proficient Obtrusion Recognition Clustered Mechanism for Malicious Sensor Nodes in a Mobile Wireless Sensor Network. Indian Journal of Information Sources and Services, 13(2), 53–63.
11. Maheshwari, P., Sharma, A. K., & Verma, K. (2021). Energy-efficient cluster-based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization. Ad Hoc Networks, 110, 102317.
12. Xiao, X., & Huang, H. (2020). A clustering routing algorithm based on improved ant colony optimization algorithms for underwater wireless sensor networks. Algorithms, 13(10), 250.
13. Jonnerby, J., Brezger, A., & Wang, H. (2023). Machine learning based novel architecture implementation for image processing mechanism. International Journal of Communication and Computer Technologies (IJCCTS), 11(1), 1-9.
14. Keerthika, A., & Berlin Hency, V. (2022). Reinforcement-Learning-based energy efficient optimized routing protocol for WSN. Peer-to-Peer Networking and Applications, 15(3), 1685-1704.
15. Han, Y., Hu, H., & Guo, Y. (2022). Energy-aware and trust-based secure wireless sensor network routing protocols using adaptive genetic algorithms. IEEE Access, 10, 11538-11550.
16. Al Aghbari, Z., Khedr, A. M., Osamy, W., Arif, I., & Agrawal, D. P. (2020). Routing in wireless sensor networks using optimization techniques: A survey. Wireless Personal Communications, 111, 2407-2434.
17. Vidhya, G. (2021). Energy-efficient enhanced hierarchical routing chain-based clustering for wireless sensor networks. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 5509-5514.
18. Trivedi, J., Devi, M. S., & Solanki, B. (2023). Step Towards Intelligent Transportation System with Vehicle Classification and Recognition Using Speeded-up Robust Features. Archives for Technical Sciences, 1(28), 39-56.
19. Ghawy, M. Z., Amran, G. A., AlSalman, H., Ghaleb, E., Khan, J., Al-Bakhrani, A. A., ... & Ullah, S. S. (2022). An effective wireless sensor network routing protocol based on particle swarm optimization algorithm. Wireless Communications and Mobile Computing, 2022(1), 8455065.
20. Camgözlü, Y., & Kutlu, Y. (2023). Leaf Image Classification Based on Pre-trained Convolutional Neural Network Models. Natural and Engineering Sciences, 8(3), 214-232.

21. Rahman, G. M., & Wahid, K. A. (2021). LDCA: Lightweight dynamic clustering algorithm for IoT-connected wide-area WSN and mobile data sink using LoRa. IEEE Internet of Things Journal, 9(2), 1313-1325.
22. Park, M., You, G., Cho, S.J., Park, M., & Han, S. (2019). A Framework for Identifying Obfuscation Techniques applied to Android Apps using Machine Learning. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 10(4), 22-30.
23. Haque, K. F., Kabir, K. H., & Abdelgawad, A. (2020). Advancement of routing protocols and applications of underwater wireless sensor network (UWSN)—A survey. Journal of Sensor and Actuator Networks, 9(2), 19.
24. Kang, J., Kim, J., & Sohn, M. M. (2019). Supervised learning-based Lifetime Extension of Wireless Sensor Network Nodes. Journal of Internet Services and Information Security, 9(4), 59-67.
25. El Khediri, S., Fakhet, W., Moulahi, T., Khan, R., Thaljaoui, A., & Kachouri, A. (2020). Improved node localization using K-means clustering for Wireless Sensor Networks. Computer Science Review, 37, 100284.
26. Cabra, J. L., Parra, C., & Trujillo, L. (2022). Earprint touchscreen sensoring comparison between hand-crafted features and transfer learning for smartphone authentication. Journal of Internet Services and Information Security JISIS, 12(3), 16-29.
27. Sahoo, B. M., & Amgoth, T. (2021). An improved bat algorithm for unequal clustering in heterogeneous wireless sensor networks. SN Computer Science, 2(4), 290.
28. Juma, J., Mdodo, R.M., & Gichoya, D. (2023). Multiplier Design using Machine Learning Alogorithms for Energy Efficiency. Journal of VLSI Circuits and Systems, 5(1), 28-34.
29. Rezaeipanah, A., Amiri, P., Nazari, H., Mojarad, M., & Parvin, H. (2021). An energy-aware hybrid approach for wireless sensor networks using re-clustering-based multi-hop routing. Wireless Personal Communications, 120(4), 3293-3314.
30. Alnumay, W. S. (2024). The Past and Future Trends in IoT Research. National Journal of Antennas and Propagation, 6(1), 13-22.