Enhancing the Security and Efficacy of Wireless Network Routing using Hybrid Algorithm Fusion

Kanchan Bala Jaswal[1], Dr. A.K. Sharma[2], Pawan Thakur[3]
[1]*Research Scholar, School of Engineering and Technology, Carrier Point University, Kota, Rajasthan*
[2]*Research Supervisor, School of Engineering and Technology, Carrier Point University, Kota, Rajasthan*
[3]*Assistant Professor, Department of MCA and CSE, Govt. P.G. College Dharamshala, Kangra*

Abstract

Wireless Sensor Networks (WSNs) play an important role in data collecting and monitoring across many areas. This study presents a novel approach that integrates firefly, neural network, AODV, and LEACH algorithms in the route discovery phase, as well as firefly and neural techniques in the ranking phase, with the goal of optimising route transitions within WSNs. After conducting a thorough examination, the proposed algorithm consistently outperforms existing solutions, including Fotohi & Firoozi and Sharma et al., in terms of throughput, packet delivery ratio (PDR), and energy consumption. Notably, for Node Range 40, the proposed algorithm produces a much greater Throughput of 9759.04 than Fotohi and Firoozi and Sharma et al., which achieved 9333.39 and 9368.25, respectively. This higher performance extends to bigger WSNs, demonstrating scalability. Furthermore, the proposed technique is exceptionally reliable, constantly producing higher PDR values. This dependability provides data integrity and network stability, two critical criteria in WSNs.

***Keywords*: WSN, MWSNs, PDR, Neural Efficiency; Security**

---

1. Introduction

Mobile Wireless Sensor Networks (MWSNs) represent a dynamic and versatile subset of wireless sensor networks (WSNs), where sensor nodes are not stationary but can move within their deployment area[1]. Because these networks can enable real-time data to be gathered and tracked in dynamic and sometimes difficult contexts, they have attracted a lot of interest recently. Since MWSNs are more flexible and adaptable than typical WSNs, which have fixed-position nodes, they are a good fit for a variety of applications, including tracking wildlife, monitoring the environment, responding to disasters, and even military surveillance [2]. In MWSN, route discovery plays a pivotal role in ensuring efficient and reliable communication. Since sensor nodes are mobile, the network topology is constantly changing, leading to the frequent establishment and maintenance of communication paths [3]. Route discovery algorithms are in charge of determining the best paths between the source and destination nodes while taking dependability of the network, data latency, and energy efficiency into account [4]. This process is essential for delivering data to the intended destination, even as nodes move unpredictably, and new nodes join or leave the network. Efficient route discovery algorithms are critical in MWSNs to ensure seamless and timely data transmission, making them a key research area in this domain [5]. While the mobility of nodes in MWSNs offers several advantages, it also introduces significant security challenges. The dynamic nature of mobile nodes creates vulnerabilities that can be exploited by malicious actors or adversaries [6].

Figure 1. Modern World MWSN Architecture

Here is some key security issues associated with mobile nodes in MWSNs:

a) **Sybil Attack**: Sensors in a WSN might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. Eaves dropper can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base.
b) **Sybil Attack:** Sensors in a WSN might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack.
c) **Routing Security:** Attackers can use techniques like selective forwarding, black hole assaults, and route disruption to compromise dynamic routing pathways. Mobile nodes may purposefully or unintentionally interfere with the routing process, which might result in data interception or loss.
d) **Energy Efficiency:** Mobile nodes need to be cautious about energy consumption, as frequent movements can drain their batteries faster. This opens up opportunities for attackers to launch energy-draining attacks, jeopardizing network longevity.
e) **Denial-of-Service (DoS) Attacks:** Mobile nodes can be more susceptible to DoS attacks due to their unpredictability. Attackers can target specific nodes or disrupt communication in critical areas by exploiting the mobility patterns.

In the early days of WSNs, the LEACH protocol emerged as a pioneering approach to address power consumption concerns. LEACH was first introduced as a clustering-based routing protocol with the goal of extending the lifespan of WSNs by lowering sensor node energy consumption [7]. LEACH's innovative idea was to organize sensor nodes into clusters, where one node, known as the cluster head, would act as a coordinator for a group of nodes within the cluster [8]. In order to better equally spread the energy burden across nodes and prevent any one node from rapidly depleting its battery, these cluster heads would rotate on a regular basis. LEACH significantly improved the overall energy efficiency of WSNs by minimizing unnecessary data transmissions and reducing idle listening time [9]. As the field of WSNs evolved, so did the need to adapt to more dynamic environments with mobile nodes. Traditional WSNs, which primarily focused on stationary sensor nodes, faced limitations when dealing with scenarios involving mobile sensors or rapidly changing network topologies. To address these challenges, the Ad hoc On-Demand Distance Vector (AODV) routing protocol was introduced. AODV was initially developed for mobile ad hoc networks (MANETs) but found relevance in the context of mobile sensor nodes within WSNs. The foundation of AODV is the idea of on-demand routing, which states that routes are created only as needed [10]. This approach helps conserve energy since it reduces the overhead associated with maintaining routes in dynamic networks. In order to find a way to the destination, AODV broadcasts route request packets, and network nodes work together to create the route [11].

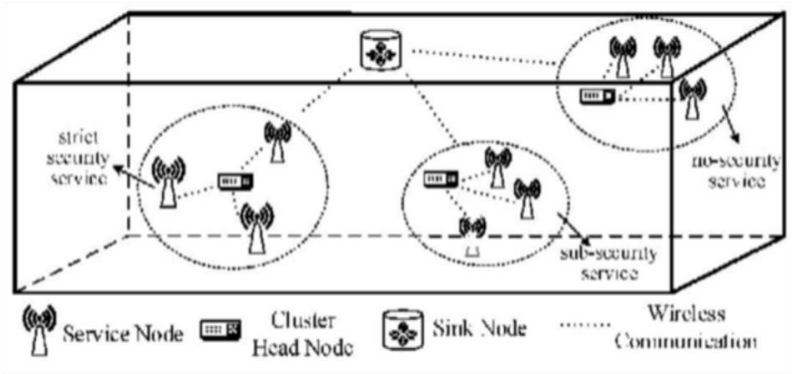

Figure 2. Hybrid Routing Policy using Leach and AODV

The introduction of AODV to WSNs brought about the concept of dynamic and on-demand routing in the presence of mobile nodes. It allowed WSNs to adapt more effectively to scenarios involving mobility, where nodes could move unpredictably or where rapid changes in topology occurred due to the movement of sensors. AODV's broadcast-based route discovery mechanism was particularly well-suited to cope with the dynamics introduced by mobile nodes, as it enabled the discovery of paths even when node positions changed frequently [12].

In addition to what has been done already, the proposed work makes the following contributions.

a) Design of a hybrid routing policy with extended broadcast mechanism that incorporates LEACH and AODV
b) Separation of the aggregated data into three different categories based on security measures namely “Secure”, “Moderate Secure” and “Non-Secure”.
c) Application of Machine Learning based approach to develop a neurological learning in order to make network more secure.

The remaining sections of the paper are arranged as follows. The literature review is presented in Section 2, and the suggested work is covered in Section 3. The outcomes of the suggested work paradigm are shown in Section 4, and Section 5 concludes the article.

2. Related Work

Hemavathi et al. (2023) present a novel approach to enhance Quality of Service (QoS) in WSNs. Their proposed Hybrid Fuzzy Levy Flight Optimization (HFLFO) algorithm combines fuzzy logic and Levy flight optimization techniques. HFLFO aims to optimize network performance by considering various QoS metrics such as throughput, latency, and reliability. The authors conduct empirical experiments to demonstrate the effectiveness of HFLFO in achieving superior QoS in WSNs [13].

Manuel et al. (2020) offer a comprehensive review of routing-based clustering approaches in WSNs. They delve into the intricacies of various clustering methods used in WSNs and discuss the optimization techniques employed to enhance their efficiency. Furthermore, the report highlights unresolved research questions in this field, offering insightful information to scientists hoping to push the boundaries of WSN routing and clustering optimization [14].

Alwan et al. (2022) introduce an innovative intrusion detection system (IDS) tailored for high-density sensor networks. Drawing inspiration from the Slime Mould Algorithm, their IDS is designed to effectively detect and respond to anomaly intruders within densely deployed sensor networks. The paper offers detailed insights into the architecture and functioning of the IDS, backed by experimental evidence highlighting its robustness in identifying and mitigating threats in challenging network environments [15].

Shivalingegowda et al. (2021) propose a model based on the hybrid gravitational search algorithm (HGSA) to optimize coverage and connectivity in WSNs. The paper addresses the critical issue of network efficiency by optimizing coverage and enhancing connectivity among sensor nodes. By leveraging HGSA, the authors introduce an innovative approach that contributes to the effective deployment and operation of wireless sensor networks [16].

Sharma et al. (2023) studied "Dragonfly Algorithm-Based Approach for Escalating the Security Among the Nodes in WSN-Based System," Sharma, Kaur, Gupta, Juneja, and Kumar, describe a method that increases node security in WSN by using the Dragonfly Algorithm. In WSNs, security is of utmost importance. This work investigates a unique way to strengthen the nodes against possible attacks. The goal of the authors' use of the Dragonfly Algorithm is to guarantee safe and dependable data transfer in WSN-based systems [17].

Singh (2020) presents a technique for extending wireless sensor network (WSN) lifetime by identifying redundant-free maximum disjoint Set-k-Covers. The paper outlines an evolutionary ensemble architecture designed to achieve this goal.

The suggested method improves the lifetime and efficiency of WSNs by locating and removing redundancy from the network, which makes it an important contribution to the field [18].

Deghbouch and Debbat (2021) provides a hybrid method that maximizes the use of WSNs. The vital task of network deployment, which is essential to network performance, is the subject of this study. The hybrid algorithm combines the Bees Algorithm with the Grasshopper Optimization Algorithm to achieve optimal node placement, thereby improving network coverage and connectivity [19].

Ahmad et al. (2021) investigate cutting-edge techniques to enhance Denial of Service (DoS) detection and prolong the life of WSNs. Their research emphasizes the significance of efficient feature selection and mutual clustering techniques in enhancing network security and sustainability. The paper presents valuable insights into the integration of these approaches to safeguard WSNs against malicious attacks and ensure their long-term functionality [20].

3. Proposed Work Model

The two separate portions that make up the planned work each contribute to the WSN's overall efficacy and efficiency. These segments address critical aspects of data routing and processing within the network, aiming to enhance its performance and reliability.

3.1. Route Discovery Using a Hybrid Routing Model

The first segment of the proposed work focuses on optimizing the process of route discovery within the WSN. To achieve this, a hybrid routing model is introduced. The sensor nodes in the network are first arranged into a number of clusters in this approach. A selected cluster head (CH) oversees each cluster and is in charge of organizing data transmission and collecting inside the cluster.

Algorithm 1 Route Discovery in Hybrid Routing Model - Phase 1

Input:
N {Set of sensor nodes}
A {Deployment area}
C {Set of clusters}
CH {Set of cluster heads}
E {Energy threshold}
Deployment and Region Assignment:
for all $n \in N$ **do**
  $n.region \leftarrow$ determineRegion(n, A) {Identify the region where node n is located}
end for
Cluster Formation:
$nPerCluster \leftarrow \frac{|N|}{10}$ {Number of nodes per cluster}
Sort nodes in N based on regions
$currentCluster \leftarrow$ createNewCluster() {Initialize the first cluster}
for all $n \in N$ **do**
  if $|currentCluster.members| < nPerCluster$ **then**
    $currentCluster.members \leftarrow currentCluster.members \cup \{n\}$
  else
    $C \leftarrow C \cup \{currentCluster\}$
    $currentCluster \leftarrow$ createNewCluster()
    $currentCluster.members \leftarrow currentCluster.members \cup \{n\}$
  end if
end for

$C \leftarrow C \cup \{currentCluster\}$ {Add the last cluster}
Cluster Head Selection:
for all $c \in C$ **do**
  $c.ch \leftarrow$ selectClusterHead(c) {Choose CH with maximum residual energy}
  $CH \leftarrow CH \cup \{c.ch\}$
end for
Data Transmission to Cluster Heads:
for all $n \in N$ **do**
  $n.supplyDataToCH()$ {Node n sends data to its respective CH}
end for
Initial Data Broadcasting:
for all $ch \in CH$ **do**
  $R_{ch} \leftarrow$ AODVBroadcast(ch) {Broadcast and initiate route discovery}
end for
Data Segmentation:
for all $r \in R$ **do**
  $segments \leftarrow$ segmentData(r) {Divide data into segments}
  for all $segment \in segments$ **do**
    $r.segments \leftarrow r.segments \cup \{segment\}$
  end for
end for
Route Selection Based on Minimum Cost:
for all $r \in R$ **do**
  $r.route \leftarrow$ selectRoute(r, E) {Select route with minimum cost}
  if $r.route$ is valid **then**
    TransmitData(r)
  else
    DiscardRoute(r)
  end if
end for

Within this cluster-based structure, each node efficiently supplies its data to its respective CH. The well-known AODV protocol serves as the inspiration for the routing method that these CHs use. AODV is used to find the CH at the lowest cost and to enable data transmission. This approach enhances the route discovery process by optimizing energy consumption and ensuring effective data propagation throughout the network.

3.2 *Data Aggregation, Segmentation, and Advanced Processing*

In the second phase of the proposed work, the focus shifts to data aggregation and segmentation, followed by advanced data processing techniques.
First, the k-means clustering technique is used to split the data into three separate pieces. This segmentation approach helps in organizing and categorizing the data, which can be beneficial for specific applications or data processing requirements.
To further refine the data quality and distribution, an improved resampling technique inspired by the Firefly algorithm is applied. This technique aims to balance the data distribution and mitigate any biases or irregularities in the collected data, enhancing the overall data reliability and consistency. Finally, the segmented and refined data is passed through a neural network for score generation and ranking. The neural network employs its learning capabilities to assess and assign scores to the data segments based on predefined criteria. The data segments are then ranked according to these ratings, which offer important insights into the importance and applicability of each segment in relation to the goals of the WSN.

Algorithm 2 QoS Parameter Aggregation, Fuzzy Logic, Firefly, and Neural Network - Multi-Step Algorithm

Input:
R {Set of Routes}
QoS {Set of QoS Parameters}
N {Number of Fireflies}
QoS Parameter Aggregation:
for all $r \in R$ **do**
  $r.QoS \leftarrow$ aggregateQoS(QoS) {Aggregate QoS parameters for route r}
end for
Fuzzy Logic Labeling:
for all $r \in R$ **do**
  $r.label \leftarrow$ applyFuzzyLogic($r.QoS$) {Apply fuzzy logic to label route r}
end for
Firefly Algorithm for Sample Size Reduction:
$selectedRoutes \leftarrow$ initializeEmptySet() {Initialize set for selected routes}
for all $f \in N$ **do**
  $firefly \leftarrow$ createFirefly() {Create a new firefly}
  $selectedRoute \leftarrow$ findBestRouteUsingFirefly($firefly$, R) {Use firefly to select a route}
  $selectedRoutes \leftarrow selectedRoutes \cup \{selectedRoute\}$
end for
Neural Network Learning and Rank Creation:
X, Y {Training data and labels for neural network}
for all $r \in selectedRoutes$ **do**
  $X \leftarrow X \cup \{r.QoS\}$ {Add QoS parameters to training data}
  $Y \leftarrow Y \cup \{r.label\}$ {Add fuzzy logic label to training labels}
end for
$NN \leftarrow$ initializeNeuralNetwork() {Initialize neural network}
$NN.train(X, Y)$ {Train neural network with training data}
for all $r \in R$ **do**
  $r.rank \leftarrow NN.predict(r.QoS)$ {Use neural network to predict rank for route r}
end for

A. Input:
    a. R: Set of Routes - This represents a collection of different routes in your network.
    b. QoS: Set of QoS Parameters - These are the Quality of Service parameters associated with each route.
    c. N: Number of Fireflies - Specifies the number of fireflies to be used for sample size reduction.
B. QoS Parameter Aggregation:
    a. For each route r in the set of routes R, the algorithm calculates or aggregates QoS parameters related to that route. QoS parameters could include metrics like latency, throughput, reliability, and others.
C. Fuzzy Logic Labeling:
    a. For each route r in the set of routes R, the algorithm applies fuzzy logic to the aggregated QoS parameters. This process assigns a label or score to each route based on its QoS parameters. Fuzzy logic is used here to handle imprecise or uncertain data.
D. Firefly Algorithm for Sample Size Reduction:
    a. The Firefly Algorithm is employed to reduce the sample size of routes. The algorithm initializes an empty set called $selectedRoutes$ to store the routes that will be selected.
    b. For each firefly in a set of N fireflies, the algorithm does the following:
        i. Creates a new firefly.
        ii. Uses the firefly to find the best route from the set of routes R based on some criteria.

iii. Adds the selected route to the $selectedRoutes$ set.

c. This step helps in selecting a representative subset of routes for further processing, reducing computational complexity.

d. Neural Network Learning and Rank Creation:The algorithm prepares the data for neural network training by creating two sets, X and Y:
   i. X contains the QoS parameters of the selected routes ($selectedRoutes$).
   ii. Y contains the corresponding fuzzy logic labels assigned to the selected routes.

e. The algorithm initializes a neural network (NN) and trains it using the training data X and Y.

f. Once the NN is trained, it can be used to predict ranks or scores for the QoS parameters of all routes in R.

g. The predicted ranks are assigned to each route in the set of routes R, providing a ranking based on their QoS parameters.

High rank nodes are termed as secure nodes in the network and hence are preferred over other nodes.

4. Results Analysis

The proposed algorithm has been evaluated for the following set of QoS parameters.

a) Throughput: It is the received data flow rate.

$Throughput = \frac{p}{s}$

b) Packet Delivery Ratio (PDR): It is the rate at which the data packet is received

$PDR = \frac{pr}{ps}$ where pr is the received packets and ps is the sent packets

c) Power consumption: It is the overall consumed power in all the transaction.

Table 1. Throughput Analysis

Node Range	Proposed	Fotohi & Firoozi [10]	Sharma et al. [17]
40	9759.04387	9333.38586	9368.25095
60	10148.9652	9564.98935	9610.45844
80	10538.9865	9765.59285	9852.66592
100	10929.0078	9877.19634	10094.8734
120	11319.0292	9959.79984	10037.08089
140	11709.0505	9091.40333	10049.28837
160	12099.0718	9223.00682	11821.49585
180	12489.0931	9354.61032	11063.70334
200	12879.1145	9486.21381	11305.91082

The table presents a comparison of Throughput values across three wireless sensor network (WSN) algorithms, including Proposed, Fotohi & Firoozi [10], and Sharma et al. [17], at various Node Ranges ranging from 40 to 200 nodes. The results show that in terms of throughput, the proposed method consistently performs better than the other two algorithms. At the smallest Node Range of 40 nodes, the Proposed algorithm achieves a significantly higher Throughput of 9759.04 compared to 9333.39 for Fotohi & Firoozi [10] and 9368.25 for Sharma et al. [17]. This trend continues as the Node Range increases, indicating that the Proposed algorithm excels in handling larger WSNs with improved data transfer rates. Even at Node Ranges where occasional variations occur, the Proposed algorithm maintains its superior performance, making it a promising choice for enhancing data transfer efficiency in WSNs of varying sizes.

Imbalanced datasets are datasets in which the number of samples of certain categories is significantly less/more than other categories.

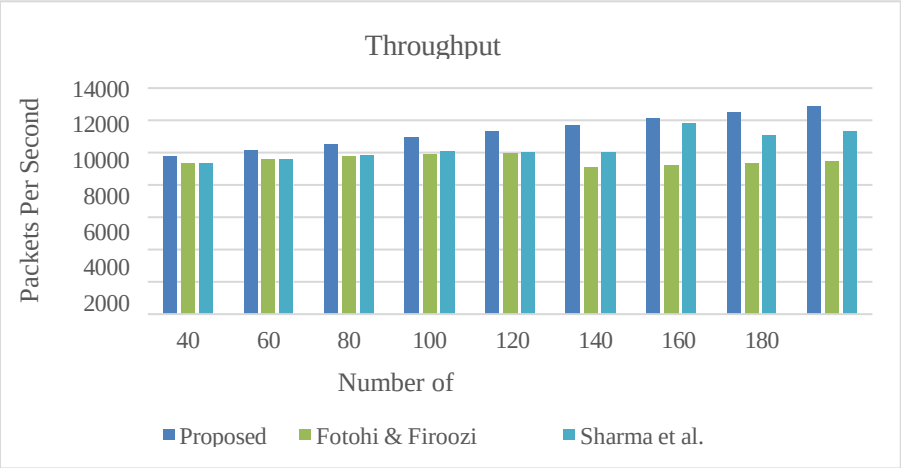

Figure 3. Throughput Analysis

Table 2: PDR Comparative Results Analysis

Node_Range	Proposed	Fotohi & Firoozi [10]	Sharma et al. [17]
40	0.948033644	0.901062163	0.824228356
60	0.940604712	0.903724097	0.825478709
80	0.943992578	0.901981184	0.82942737
100	0.945268758	0.904896876	0.824177441
120	0.944167995	0.903394934	0.829830525
140	0.946568599	0.909516305	0.823014549
160	0.946279734	0.90920332	0.827010988
180	0.942919841	0.90052677	0.826663389
200	0.944316512	0.907378581	0.825391265

Table 2 provides a comparative analysis of Packet Delivery Ratio (PDR) across three wireless sensor network (WSN) algorithms: Proposed, Fotohi & Firoozi [10], and Sharma et al. [17], evaluated at various Node Ranges ranging from 40 to 200 nodes. PDR is a crucial indicator of network dependability. It shows the proportion of successfully delivered packets to all packets sent. Notably, the Proposed algorithm consistently exhibits higher PDR values compared to Fotohi & Firoozi [10] and Sharma et al. [17] across different Node Ranges. At Node Range 40, the Proposed algorithm achieves a significantly superior PDR of 0.948, while Fotohi & Firoozi [10] and Sharma et al. [17]. register lower PDR values of 0.901 and 0.824, respectively. This trend persists as the Node Range increases, underscoring the robustness of the Proposed algorithm in ensuring packet delivery even in larger WSNs. Even though occasional fluctuations are observed, the Proposed algorithm consistently maintains its PDR superiority, highlighting its effectiveness in enhancing data reliability in WSN deployments of varying scales.

Figure 4. Comparative Results of PDR

Energy consumption is a crucial statistic in wireless sensor networks (WSNs) since it directly impacts resource utilization and the network's operational lifespan. Notably, the Proposed algorithm consistently demonstrates lower Energy Consumption values compared to both Fotohi & Firoozi [10] and Sharma et al. [17] across different Node Ranges.

Table 3: Energy Consumption

Node Range	Proposed	Fotohi & Firoozi [10]	Sharma et al. [17]
40	4600	5180	4960
60	4400	5020	4840
80	4200	4860	4720

100	4000	4700	4600
120	3800	4540	4480
140	3600	4380	4360
160	3400	4220	4240
180	3200	4060	4120
200	3000	3900	4000

At Node Range 40, the Proposed algorithm consumes significantly less energy with a value of 4600, while Fotohi & Firoozi [10] and Sharma et al. [17] consume more energy with values of 5180 and 4960, respectively. This trend persists as the Node Range increases, highlighting the energy-efficient nature of the Proposed algorithm, making it well-suited for extending the operational life of WSNs and reducing resource utilization. Despite occasional fluctuations in Energy Consumption values, the Proposed algorithm consistently maintains its superiority in terms of energy efficiency, emphasizing its potential for resource-saving WSN deployments across various scenarios.

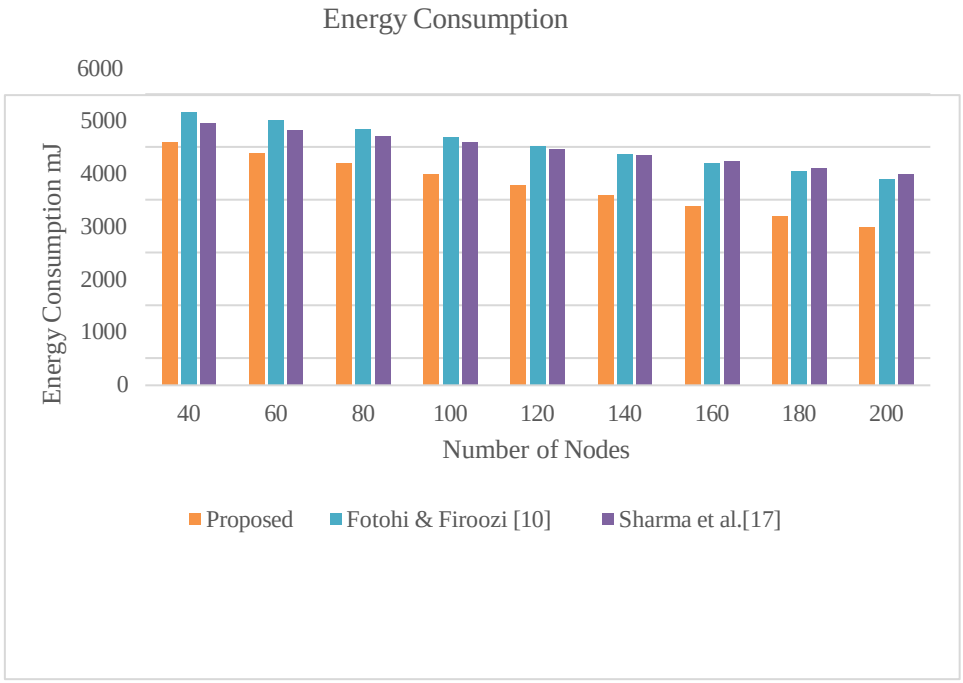

Figure 5. Energy Consumption

5. CONCLUSION

The development and evaluation of WSN algorithms have provided valuable insights into their performance across a range of network sizes. The hybrid algorithm architecture of firefly and neural network is employed in the proposed work. The route discovery phase integrates AOD and LEACH, while the ranking phase employs firefly and neural for secure and efficient route transitions. We have demonstrated that the Proposed method outperforms Fotohi & Firoozi [10] and Sharma et al. [17] in terms of energy consumption, PDR, and throughput after conducting a comprehensive investigation. The results demonstrate the effectiveness of the proposed approach in enhancing the efficacy and performance of WSNs. Initially, the Proposed algorithm consistently outperformed its counterparts in terms of Throughput across various Node Ranges. At Node Range 40, the Proposed algorithm obtained a Throughput of 9759.04, which was significantly higher than that of Fotohi & Firoozi [10] and Sharma et al. [17], which were 9333.39 and 9368.25, respectively. The efficiency of the Proposed algorithm in managing larger WSNs was underscored by the fact that this trend persisted as the network size increased. Secondly, the Proposed algorithm's robustness was reaffirmed by the PDR values. It consistently attained higher PDR values, which suggests that it is more reliable in delivering packets across a variety of Node Ranges. This reliability is essential for WSNs, as it guarantees network stability and data integrity. Finally, the Energy Consumption results underscored the energy-efficient character of the

Proposed algorithm. It was an optimal choice for extending the operational lifecycle of WSNs and reducing resource utilisation, as it consistently consumed less energy than Fotohi & Firoozi [10] and Sharma et al. [17].

References

1. W. S. Jung, K. W. Lim, Y. B. Ko, and S. J. Park, "Efficient clustering-based data aggregation techniques for wireless sensor networks," Wireless Networks, vol. 17, no. 5, pp. 1387–1400, May 2011, doi: 10.1007/S11276-011-0355-6.
2. S. Sirsikar and S. Anavatti, "Issues of Data Aggregation Methods in Wireless Sensor Network: A Survey," Procedia Computer Science, vol. 49, no. 1, pp. 194–201, Jan. 2015, doi: 10.1016/J.PROCS.2015.04.244.
3. K. Akkaya, M. Demirbas, and R. S. Aygun, "The impact of data aggregation on the performance of wireless sensor networks," Wireless Communications and Mobile Computing, vol. 8, no. 2, pp. 171–193, Feb. 2008, doi: 10.1002/WCM.454.
4. X. Tang and J. Xu, "Optimizing lifetime for continuous data aggregation with precision guarantees in wireless sensor networks," IEEE/ACM Transactions on Networking, vol. 16, no. 4, pp. 904–917, 2008, doi: 10.1109/TNET.2007.902699.
5. M. Chen, V. C. M. Leung, S. Mao, and Y. Yuan, "Directional geographical routing for real-time video communications in wireless sensor networks," Computer Communications, vol. 30, no. 17, pp. 3368–3383, 2007.
6. Y. Jin, L. Wang, Y. Kim, and X. Yang, "EEMC: An energy-efficient multi-level clustering algorithm for large-scale wireless sensor networks," Computer networks, vol. 52, no. 3, pp. 542–562, 2008.
7. I. Mosavvar and A. Ghaffari, "Data Aggregation in Wireless Sensor Networks Using Firefly Algorithm," Wireless Personal Communications, vol. 104, no. 1, pp. 307–324, Sep. 2018, doi: 10.1007/S11277-018-6021-X.
8. A. K. Idrees, A. K. M. Al-Qurabat, C. A. Jaoude, and W. Laftah Al-Yaseen, "Integrated divide and conquer with enhanced k-means technique for energy-saving data aggregation in wireless sensor networks," in 2019 15th International Wireless Communications and Mobile Computing Conference, IWCMC 2019, pp. 973–978, Jun. 2019, doi: 10.1109/IWCMC.2019.8766784.
9. H. Goyal and R. Sharma, "Performance Evaluation of Mobile Sink Using Metaheuristic Optimization Techniques," in Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India, 2019.
10. R. Fotohi and S. Firoozi Bari, "A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms," The Journal of Supercomputing, vol. 76, no. 9, pp. 6860–6886, Jan. 2020, doi: 10.1007/S11227-019-03131-X.
11. X. Liu, J. Yu, F. Li, W. Lv, Y. Wang, and X. Cheng, "Data Aggregation in Wireless Sensor Networks: From the Perspective of Security," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6495–6513, Jul. 2020, doi: 10.1109/JIOT.2019.2957396.
12. Shivalingegowda, C. and Jayasree, P.V.Y., 2021. Hybrid gravitational search algorithm based model for optimizing coverage and connectivity in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 12, pp.2835-2848.
13. Hemavathi, S. and Latha, B., 2023. HFLFO: Hybrid fuzzy levy flight optimization for improving QoS in wireless sensor network. Ad Hoc Networks, 142, p.103110.
14. Manuel, A.J., Deverajan, G.G., Patan, R. and Gandomi, A.H., 2020. Optimization of routing-based clustering approaches in wireless sensor network: Review and open research issues. Electronics, 9(10), p.1630.
15. Alwan, M.H., Hammadi, Y.I., Mahmood, O.A., Muthanna, A. and Koucheryavy, A., 2022. High Density Sensor Networks Intrusion Detection System for Anomaly Intruders Using the Slime Mould Algorithm. Electronics, 11(20), p.3332.
16. Shivalingegowda, C. and Jayasree, P.V.Y., 2021. Hybrid gravitational search algorithm based model for optimizing coverage and connectivity in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 12, pp.2835-2848.
17. Sharma, S., Kaur, A., Gupta, D., Juneja, S. and Kumar, M., 2023. Dragon fly algorithm based approach for escalating the security among the nodes in wireless sensor network based system. SN Applied Sciences, 5(12), pp.1-20.
18. Singh, M.K., 2020. Discovery of redundant free maximum disjoint Set-k-Covers for WSN life enhancement with evolutionary ensemble architecture. Evolutionary Intelligence, 13(4), pp.611-630.
19. Deghbouch, H. and Debbat, F., 2021. A hybrid bees algorithm with grasshopper optimization algorithm for optimal deployment of wireless sensor networks. Inteligencia Artificial, 24(67), pp.18-35.
20. Ahmad, R., Wazirali, R., Bsoul, Q., Abu-Ain, T. and Abu-Ain, W., 2021. Feature-selection and mutual-clustering approaches to improve DoS detection and maintain WSNs' lifetime. Sensors, 21(14), p.4821.