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

Energy Efficient Clustering with Secured Aggregation (EECSA) for Improving Energy Efficiency in Wireless Sensor Networks through Clustering and Data Aggregation

B. Mekala[1], Dr. Nagarajan Munusamy[2]

[1]Research Scholar, Department of Computer Science, K.S.G College of Arts & Science, India, mekalaksg@gmail.com
[2]Associate Professor & Principal, Department of Computer Science K.S.G College of Arts & Science, India, mnaagarajan@gmail.com

Energy efficiency in Wireless Sensor Networks (WSNs) is crucial to prolonging the network's lifespan and reliability. Sensor nodes are often battery-powered, with limited energy resources, so effective energy usage is critical for long-term operation. Transmitting and receiving data take a considerable percentage of a sensor node's power. Reducing the quantity of data exchanged and improving the connection protocol can help save energy. Instead of delivering raw data, nodes might aggregate data to reduce the number of transmissions. Aggregation merges several data packets into a single one, reducing transmission overhead. In this paper, we suggest a novel methodology called "Energy Efficient Clustering with Secured Aggregation (EECSA)" that will improve node clustering by separating the entire deployment area into equal portions, allowing nodes to be placed throughout the network for better network coverage. The cluster heads use the average weight function to aggregate data, and Energy-Efficient Secure Aggregation with Weights (ESAW) is used for data security because it is lightweight and can help reduce energy usage. The simulated results suggest that the proposed method outperforms a few other methods in terms of network coverage, energy usage, and security.

1. Introduction

Wireless Sensor Networks (WSNs) are distributed networks made up of autonomous sensors that are connected and geographically dispersed to monitor and record environmental variables. The data from these sensors is received by a central hub or gateway, which then processes it before sending it to other systems for further inspection or action. WSNs are widely used in applications including healthcare, smart cities, industrial automation, environmental monitoring, and military operations. The sensors operate together to convey the collected data via a network to a central location. The primary characteristics of nodes in a Wireless Sensor Network are low power consumption and limited computing capability. It is

crucial to optimize energy consumption in WSN applications. Clustering in Wireless Sensor Networks (WSNs) is a strategy for optimizing resource utilization, improving scalability, and increasing energy efficiency. It entails grouping sensor nodes into clusters, each with a chosen leader known as the Cluster Head (CH). The CH manages the cluster's activity and sends aggregated data to the base station. Data aggregation in Wireless Sensor Networks (WSNs) is the act of gathering and merging data from various sensor nodes in order to eliminate redundancy and save energy. This method is crucial in WSNs, where limited resources require energy efficiency and bandwidth optimization. This study focuses on using clustering and data aggregation to increase energy efficiency and security in wireless sensor networks. This study offers a novel protocol, EECSA (Energy Efficient Clustering with Secured Aggregation), which will help reduce energy consumption in WSN.

2. Review of Literature

[1] Hassan et.al proposes an energy-efficient clustering protocol (IEECP) to extend the lifetime of WSN-based IoT. The proposed IEECP has three successive components. The overlapping balanced clusters are first divided into an ideal number of clusters. The balanced-static clusters are generated by combining a modified fuzzy C-means algorithm with an energy-saving strategy for sensor nodes. The cluster heads (CHs) are rotated in ideal places using a new algorithm that includes a back-off timer for CH selection and a rotation mechanism for CH rotation. The proposed methodology minimizes and balances energy. [2] Khan et.al suggests a new system, "A Content-based Adaptive and Dynamic Scheduling (CADS) using a two-way communication paradigm in WSNs", to improve WSN longevity and energy efficiency. CADS dynamically adjusts node states during data aggregation based on observed data packets. The Analyzer module at the Base-Station analyses data packets and governs node activities through backward control messages. CADS reduces energy usage by decreasing superfluous network traffic and eliminating redundant message forwarding. [3] Bhushan et.al proposes the FAJIT algorithm, which uses fuzzy logic to create trees and choose parent nodes in heterogeneous networks. FAJIT aims to enhance energy efficiency by tackling the challenge of selecting parent nodes in heterogeneous networks and aggregating various data packet types. Parent nodes are chosen based on those with the fewest dynamic neighbours. Fuzzy logic is used when there are equal numbers of dynamic neighbours. The suggested technique applies fuzzy logic to WSN and then uses min-max normalization to extract normalized weights (membership values) for given edges in the graph. This membership value represents the degree to which an element belongs to a set. The node with the lowest sum of all weights is designated the parent node. FAJIT is compared to DICA on several parameters, including average schedule length, energy consumption data interval, total number of transmission slots, control overhead, and energy consumption during the control phase. The results show that the proposed algorithm is more energy efficient. [4] Sert et.al proposes a modified clonal selection method (CLONALG-M) to enhance energy efficiency in rule-based fuzzy clustering algorithms. While there are studies on fuzzy optimization in general, there is currently no focus on improving the performance of rule-based fuzzy clustering methods. The CLONALG-M method, based on the Clonal Selection Principle, helps understand the fundamental principles of adaptive immune systems. This study demonstrates how output-based membership functions can improve the performance of rule-based fuzzy clustering

algorithms that already have known membership functions. The proposed approach has been tested and evaluated using several fuzzy clustering approaches. [5] The proposed approach by Khedri et.al is referred to as the Distance Energy Evaluated (DEE) Approach. The DEE technique has a lower message complexity. The proposed approach is tested using MATLAB simulations. Our proposed protocol outperforms current alternatives in terms of network longevity and energy usage. [6] Sharada et.al introduces the AACDIC approach, which enhances energy efficiency by identifying optimal cluster counts through connectivity and distributed cluster-based sensing.

This study considers a system with an unknown number of primary and secondary users. The proposed AACDIC approach uses multi-user clustered communication to accelerate solution convergence, outperforming previous optimization algorithms. Experiments reveal that the AACDIC approach significantly reduces node power usage by 9.646 percent when compared to other algorithms. [7] Blockchain technology will be implemented to address security issues. Rehman et.al focuses on the security of wireless sensor networks using blockchain, unlike previous studies on homogeneous systems. This research focuses on identifying privacy and security vulnerabilities in IoT systems. Additionally, blockchain technology can address security concerns. We will examine the wireless sensor network to understand how data functions in distributed or decentralized network architectures. Researchers proposed the wireless sensor network clustering technique to improve network efficiency by spreading workload. This allows for faster and more efficient system performance. [8] This research paper by Khera et.al proposes a novel technology called Hibernated Clustering Wireless Sensor Networks (HC-WSN). The proposed methodology improves the operating time of individual sensor nodes, which leads to an increase in overall network lifetime. The simulation results reveal that our suggested scheme outperforms other schemes in terms of individual node lifespan, average energy, and throughput. Furthermore, the proposed methodology increases the lifespan of both WSNs and individual nodes. [9] This paper by Nedham et.al presents an Energy-Saving Clustering Algorithm (ESCA) that reduces energy usage and increases network longevity. The clustering phase involves both centralized cluster formation and dispersed cluster heads. The clustering is done using a centralized K means approach, resulting in static clusters throughout the process. The system selects and rotates cluster heads (CHs) based on energy levels in nodes to reduce energy consumption before transmitting data to the base station (BS). The proposed ESCA is compared to the current two MOFCA and IGHND clustering algorithms using a Python-based custom simulator. As a result, the proposed ESCA efficiently addresses the energy utilization issue while also significantly expanding the network lifetime. [10] Dogra et.al provides an improved smart-energy-efficient routing protocol (ESEERP) technique that extends the network's lifetime and enhances its connectivity to address the aforementioned inadequacies. It picks the Cluster Head (CH) using an effective optimization mechanism drawn from multiple uses. It reduces sleepy sensor nodes and saves power. Following CH selection, a Sail Fish Optimizer (SFO) is utilized to determine the best route to the sink node for data transfer. The proposed methodology has been mathematically studied and compared to existing approaches like Genetic Algorithm (GA), Ant Lion Optimization (ALO), and Particle Swarm Optimization (PSO) in terms of energy utilization, bandwidth, packet delivery ratio, and network longevity. [11] This research proposed by Dattatraya et.al presents a new cluster head selection approach that maximizes network longevity and energy efficiency. Furthermore, this work offers a new Fitness-based

Glowworm Swarm with Fruitfly Algorithm (FGF), which is a hybrid of Glowworm Swarm Optimization (GSO) and Fruitfly Optimization Algorithm (FFOA) for selecting the optimal CH in WSN. The performance of the developed FGF is compared to other existing methods such as Particle Swarm Optimization (PSO), Genetic Algorithm (GA), Artificial Bee Colony (ABC), GSO, Ant Lion Optimization (ALO) and Cuckoo Search (CS), Group Search Ant Lion with Levy Flight (GAL-LF), Fruitfly Optimization algorithm (FFOA), and Grasshopper Optimization algorithm (GOA) in terms of alive node analysis, energy analysis, and cost function, and the proposed work is also proven to be superior. [12] Ahmed et.al proposes Energy-Efficient Data Aggregation Mechanism (EEDAM) utilizes blockchain technology to aggregate data at the cluster level, resulting in energy savings. Edge computing provides on-demand trustworthy services to IoT with minimal delay. Integrating blockchain into a cloud server validates the edge and ensures secure services for IoT. We simulated the performance of the suggested mechanism and compared it to standard energy-efficient techniques. Simulation findings indicate that the suggested structural design effectively reduces data, enhances IoT security, and expands the wireless sensor network. [13] Ramasamy et.al addresses energy consumption and security limits in reconfigurable WSNs, with the goal of increasing network lifetime and ensuring data privacy. The network consists of scattered nodes that reconfigure to meet user requirements. Our proposed solutions enhance network lifetime by reducing traffic and enabling effective reconfigurable routing. Our proposal involves employing hashing distance computation (HDC) to reduce duplicate packets at the node level within the network. [14] This study proposed by Said et.al introduces a lightweight Secure Aggregation and Transmission Scheme (SATS) for safe and efficient data computation and transmission. SATS uses a lightweight XOR operation to obtain batch keys, instead of the costly multiplication operation. The AN Receiving Message Algorithm (ARMA) aggregates data from sensor nodes. The Receiving Message Extractor (RME) technique is used to decrypt messages and verify batches at the Fog-Server. SATS defends against several security risks, including denial of service, man-in-the-middle, and reply attacks. The suggested SATS is simulated with the simulation tool NS 2.35. Results indicate that SATS reduces processing and communication costs, resulting in lightweight data transmission.

3. Proposed Work

Clustering methods in Wireless Sensor Networks (WSNs) frequently try to organize sensor nodes into clusters, each managed by a cluster head (CH), in order to improve communication and energy efficiency. Interpolation-based clustering algorithms use mathematical interpolation techniques to improve cluster formation or analyse sensing data. The sensors are deployed randomly in a 2D region and their positions are fixed throughout their lifespan. The energy level for all the sensors is same initially. Each sensor is associated with a GPS device and the energy consumption for GPS is ignored. The coordinates of the sensors are transmitted to the mobile sink. The deployment area is divided into sections of $50m^2$ intervals and clusters are formed in each section using interpolation.

Let the nodes be represented as $\{n_1,n_2,\ldots\ldots\ldots n_N\}$ and let their location be (x_i,y_i), E_i be their residual energy and D_i be its density. For node i, the interpolated density D_i is calculated as

$$D_i = \frac{\sum_{j=1}^{N} \frac{1}{d_{i,j}^{p}}}{\sum_{j=1}^{N} \frac{1}{d_{i,j}^{p}}} \quad (1)$$

Where $d_{i,j}$ is the distance between the nodes i and j.

The CHs are selected based on the metric $CH = \arg_i^{max}(E_i \times D_i)$ (2)

Assign each node to the nearest CH and the distance between the nodes and CH is calculated using the equation $d_{i,j} = \sqrt{(x_i - y_i)^2 + (x_j - y_j)^2}$ (3)

Node i joins the cluster managed by CH j using the equation $C_j = \arg_i^{max} d_{i,j}$ (4)

Energy threshold is fixed for the CHs and once the energy is depleted below the threshold the node next CH is selected based on the residual energy and interpolation density.

Data aggregation is performed at the cluster heads using the equation given below

$$D_{agg} = f(D_1, D_2, \ldots \ldots . . D_n) \quad (5)$$

Where D_{agg} is the aggregated data and $D_1, D_2, \ldots \ldots . . D_n$ are data inputs from the sensor nodes.

The average function is considered to reduce the size of data and it is calculated using the equation

$$D_{agg} = \frac{1}{n} \sum_{i=1}^{n} D_i \quad (6)$$

Where D_i is the data input and n denote the number of sensor nodes. To ensure that data is transmitted securely we incorporate Energy-Efficient Secure Aggregation with Weights (ESAW) with our proposed work to enhance the security and efficiency of Wireless Sensor Networks (WSNs). It emphasizes secure data collection and processing while minimizing energy consumption—a critical concern in resource-constrained WSN environments. Each sensor node assigns a weight to its data before aggregation, based on predefined metrics like sensor trustworthiness, data quality, or environmental conditions. The network is divided into clusters, and data aggregation occurs within clusters. Cluster heads aggregate data from member nodes and forward it to the base station or higher layers in the hierarchy. The cryptographic methods, such as lightweight encryption or Message Authentication Codes (MACs), are implemented to ensure data integrity and prevent eavesdropping. It detects and handles malicious or faulty nodes through redundancy or anomaly detection mechanisms. The weights can be adjusted dynamically to reduce the impact of compromised nodes. It minimizes energy consumption through optimized routing and aggregation schemes and balances energy usage across the network to extend the lifetime of the WSN. The aggregated data is encrypted to maintain privacy and security.

The aggregated value is computed using weighted sums. Suppose there are n sensor nodes in a cluster, and each node i produces a data value d_i with a weight w_i. The weighted aggregate W_{agg} can be computed as:

$$W_{agg} = \frac{\sum_{i=1}^{n} w_i . d_i}{\sum_{i=1}^{n} w_i} \quad (7)$$

Here w_i represents the importance or reliability of the data from node i.

Normalizing by $\sum_{i=1}^{n} w_i$ ensures that the aggregate value is proportional to the weights.The total energy consumption E_{agg} in a cluster during aggregation can be modeled as:

$$E_{agg} = E_s + E_c + E_{tx} \quad (8)$$

Where E_s is the Energy spent on sensing by all nodes, E_c Energy spent on computation (weight assignments, encryption, aggregation) and E_{tx} Energy spent on transmission to the cluster head or base station. The aggregated data is transmitted to the base station. The energy for transmitting 'l' bit data is calculated using the following equations:

$$E_{tx} = l.E_{elec} + l.E_{amp}.d^2 \quad (9)$$

$$E_{rx} = l.E_{elec} \quad (10)$$

Where E_{tx} Energy spent to tansmit 'l' bit of data and E_{rx} is the energy spent to receive 'l' bit of data. The cryptographic overhead is computed as follows:

$$O = E_{crypto} + T_{crypto} \quad (11)$$

E_{crypto} is the energy spent on encryption and MAC generation and T_{crypto} is the time delay caused by cryptographic operations. To minimize the overhead light weight cryptography is used.

Algorithm

Input

Number of nodes, N

Size of the sensing field, field_size

Initial energy of nodes, E_i

Base station location, (x_i,x_j)

Communication range, R_c

Deploy nodes at random positions

nodes = np.random.rand(N, 2) * field_size

Calculate the residual energy of the nodes

$E_{r(n)}$ = np.ones(N) * E_i

Calculate the distance between the nodes

distance(a, b): return np.sqrt((a[0] - b[0])**2 + (a[1] - b[1])**2)

Define interpolation function to calculate node density

interpolate_density(nodes, R_c):

densities = []

for i, node in enumerate(nodes):

distances = np.array([distance(node, neighbor) for neighbor in nodes])

weights = 1 /(distances + 1e-6)**2

[distances > R_c] = 0

density = np.sum(weights)

densities.append(density)

return np.array(densities)

Calculate node densities

densities = interpolate_density(nodes, R_c)

Select cluster heads

ch_threshold = np.percentile(densities, 90)

cluster_heads = np.where(densities >= ch_threshold)[0]

Form clusters in the respective sections

clusters = {ch: [] for ch in cluster_heads} for i, node in enumerate(nodes):

if i not in cluster_heads:

nearest_ch = min(cluster_heads, key=lambda

ch: distance(nodes[i], nodes[ch]))

clusters[nearest_ch].append(i)

Aggregate data at the cluster heads using average function.

Implement secure aggregation by assigning weights to data.

Transmit data to base station.

4. Results and Discussion

The proposed algorithm "EECSA (Energy Efficient Clustering with Secured Aggregation)" creates clusters to reduce energy usage and increase network longevity. The metrics such as cluster size, energy consumption during clustering and data aggregation, packet delivery ratio, security and transmission latency are studied and discussed in the results to demonstrate the effectiveness of the proposed algorithm. The proposed algorithm's performance is compared to two existing clustering algorithms: the Energy-Saving Clustering Algorithm (ESCA) (Nedham et al. 2022) and the Improved energy-efficient clustering protocol (IEECP) (Hassan et al. 2020).

Simulation Parameters		
1	Simulation area	100 m x 100 m
2	Number of nodes	100
3	Deployment	Random

4	Node Mobility	Fixed
5	Optimal number of CH	10%
6	Initial energy	1000 J
7	Energy threshold for CH	Below 70%
8	E_{fs}	$10 * 10^{-2}$ J
9	E_{tx}	$50 * 10^{-9}$ J
10	E_{rx}	$50 * 10^{-9}$ J
11	E_{agg}	$50 * 10^{-9}$ J
12	Radio propagation range	300 m
13	Channel capacity	2 M bits/s
14	Data packets	3200 bits
15	Distance threshold	35 m
16	Simulation time	180 s

Table 4.1. Simulation Parameters

The entire area of deployment is divided into four sections in EESA are the number of nodes in each cluster are given below in Figure 4.1:

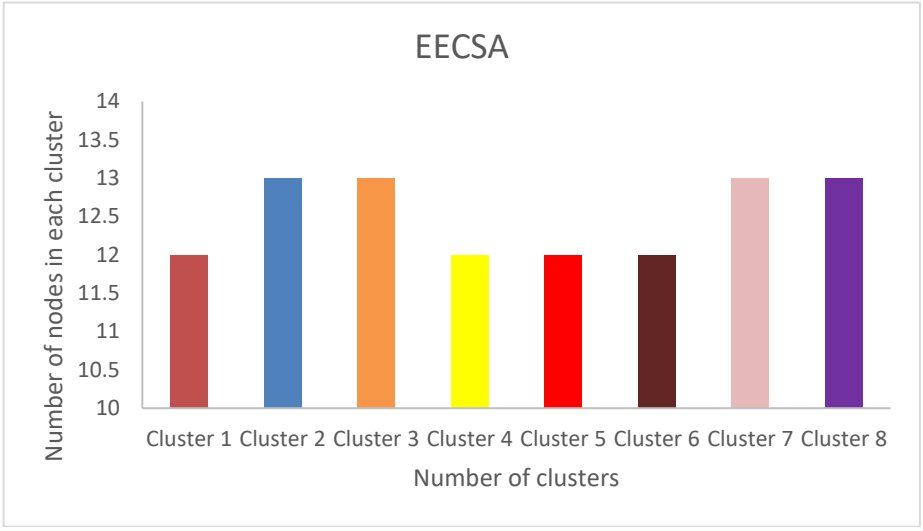

Fig 4.1. Number of nodes Vs Number of Clusters (EECSA)

ESCA and IEECP are the existing methodologies which aim in generating balanced clusters which do not change throughout the network lifetime and their comparisons on the number of clusters towards number of nodes in each cluster are shown in Fig 4.2 and 4.3.

Fig 4.2. Number of nodes Vs Number of Clusters (ESCA)

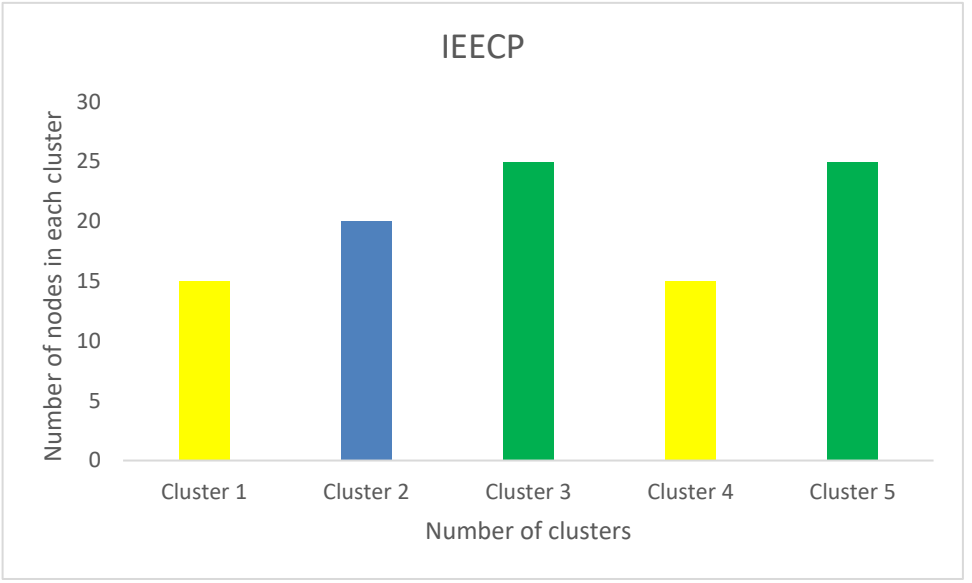

Fig 4.3. Number of nodes Vs Number of Clusters (IEECP)

The comparison of the existing and the proposed work on the number of clusters formed and average number of nodes in each cluster is depicted in Table 4.2. The total number of nodes deployed is 100.

Methodology	Number of Clusters	Average Number of nodes in each cluster
IEECP	5	15 -25
ESCA	10	10

EECSA	8	12-13

Table 4.2. Comparison on number of nodes Vs number of Clusters (IEECP)

In Wireless Sensor Networks (WSNs), network coverage refers to the spatial area over which sensor nodes can efficiently interact with one another. The coverage is governed by each node's communication range (radius) as well as the network topology. Providing adequate coverage is critical to the network's ability to monitor and gather data from all desired places. Fig 4.4 shows the comparison of network coverage among the proposed and existing algorithms. In the proposed EECSA with 100 nodes and a radius of 28.2 meters, the total coverage is approximately 249,730 m², which is much greater than the available area of 10,000 m² which depicts the network will easily cover the entire 10,000 m² area.

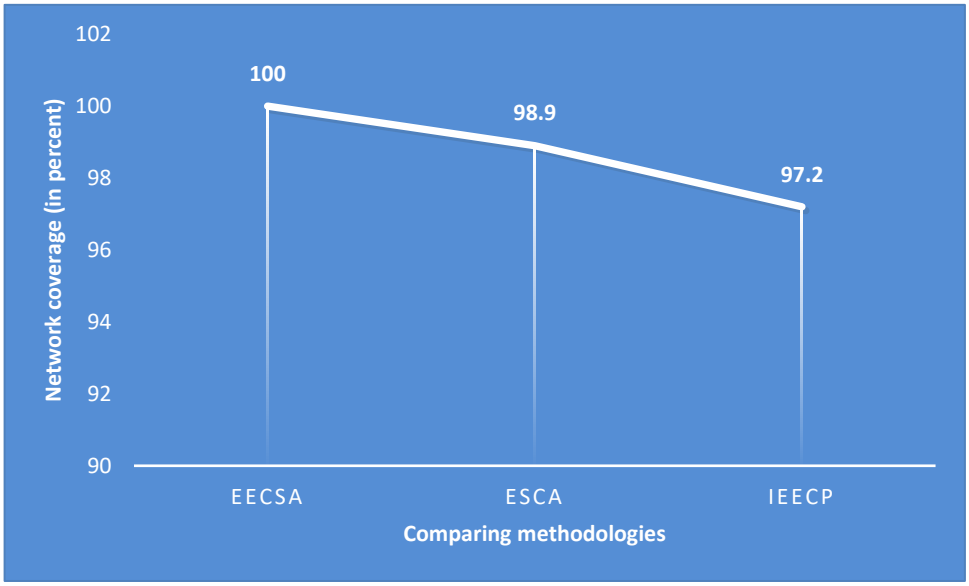

Fig 4.4. Comparison on network coverage among various methods with the proposed method

The Packet Delivery Ratio (PDR) is the ratio of packets delivered to the destination to packets sent from the source. The proposed technique calculates packet delivery using data packets sent from sensor nodes to cluster heads.

Total number of packets sent	ESCA	IEECP	EECSA
20	18	17	20
40	39	37	40
60	58	58	59
80	77	74	78
100	97	93	98

Table 4.3. Number of packets delivered to the total number of packets

Table 4.3 and Fig 4.5 shows the comparison in packet delivery ratio where it is seen all the

three approaches minimize loss of data packets. The proposed method shows that the packet loss is negligible compared to the other two methods.

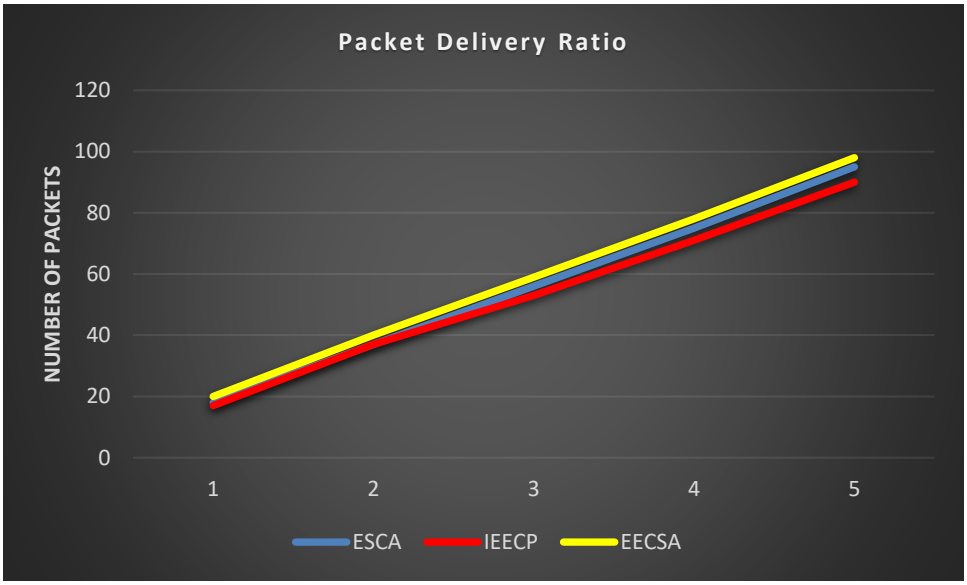

Fig 4.5. Comparison on packet delivery ratio among various methods with the proposed method

Data security in Wireless Sensor Networks (WSNs) is critical due to the very sensitive nature of the data transferred (for example, environmental monitoring, medical data, military surveillance, etc.). WSNs are frequently deployed in open, untrusted environments, leaving them vulnerable to a variety of assaults. As a result, protecting the data transmitted across the network is critical to maintaining confidentiality, integrity, authenticity, and availability. Implementing security mechanisms in WSNs can be computationally expensive and may necessitate more energy, which is a valuable resource in sensor networks. As a result, lightweight cryptographic approaches and energy-efficient security protocols must be utilized. Delay is defined as the time it takes to transmit and aggregate data which is one of the metric to analyse data security. The suggested technique calculates delay based on the time taken to generate clusters and aggregate data. The average latency is measured after deploying 100 nodes in the sensing field.

	ICEEP	ESCA	EECSA
Clustering	5.07 sec	5.93 sec	4.78 sec
Data aggregation	8.67 sec	7.32 sec	4.59 sec

Table 4.4. Delay during clustering and data aggregation of the various approaches

Table 4.4 shows the delay taken by the existing and proposed algorithms during clustering and data aggregation. Fig 4.6 compares the average delay between the proposed and existing algorithms. It is observed that the proposed algorithm causes minimum delay compared to the existing algorithms.

The Integrity Violation Rate (IVR) in Wireless Sensor Networks (WSNs) is the frequency with

which data is found to be altered, corrupted, or tampered with during transmission. Measuring this rate is critical for determining how well the network maintains data integrity and whether malicious acts or errors occur during data transfer. The Integrity Violation Rate is derived using the number of integrity violations discovered over a specified time period or number of data transactions. It is usually stated as a ratio or percentage.

$$\text{IVR} = \frac{\text{Number of Integrity Violations}}{\text{Total Number of Packets Sent}} \times 100 \qquad (12)$$

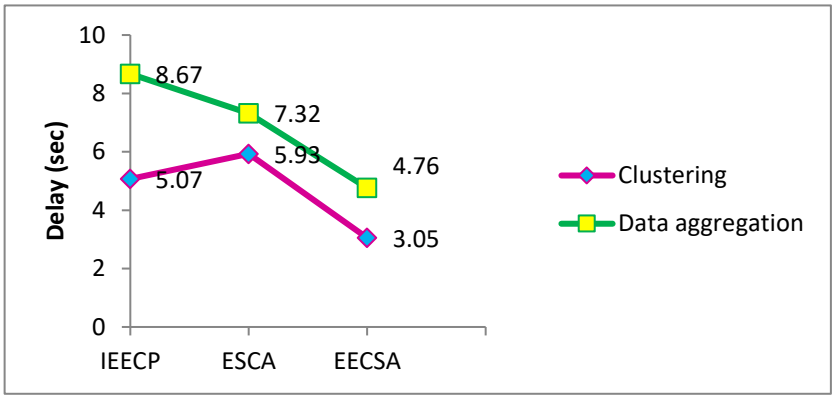

Fig 4.6. Comparison on delay among various methods with the proposed method

Total number of packets sent	ESCA	IEECP	EECSA
20	6	8	0
40	4	9	0
60	10	13	2
80	13	19	5
100	14	22	8

Table 4.5. Comparison on the number of packets affected by integrity violations

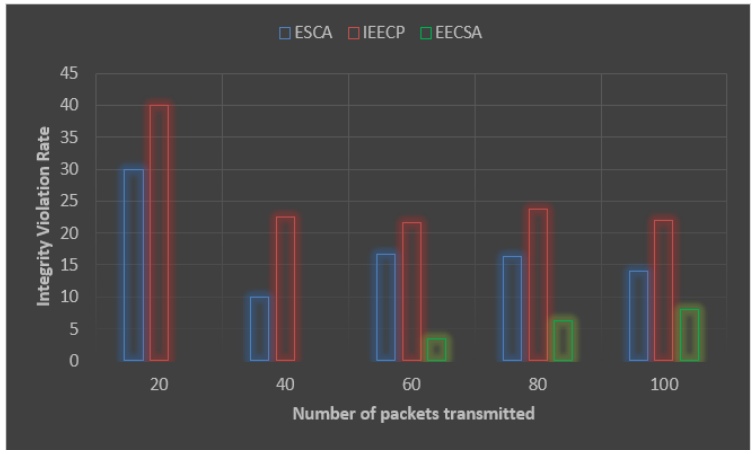

Fig 4.7. Comparison on IVR among various methods with the proposed method

Fig 4.7 shows that the proposed method displays very minimum IVR compared to the existing methodologies because both ESCA and IEECP have not incorporated any security during data transmission whereas the proposed method has incorporated security during data aggregation.

Due to the resource constraints of sensor nodes, energy consumption is an important consideration in the design, operation, and maintenance of Wireless Sensor Networks (WSNs). These nodes frequently rely on battery power or restricted energy sources, therefore reducing energy usage is critical to guaranteeing the network's longevity and efficiency. Energy consumption is especially essential in data security since many security techniques (such as encryption and authentication) need additional processing power, which might deplete sensor nodes' limited energy resources. Energy consumption in a wireless sensor network can occur during a variety of activities, including data sensing, transmission, processing, and security operations. The energy consumed during data aggregation and encryption is given below in table 4.6 and the comparison of energy usage during clustering and data aggregation is displayed in Fig 4.8.

	ESCA	ICEEP	EECSA
Data aggregation	123 J	214 J	103 J
Encryption	Not done	Not done	143 J

Table 4.6. Comparison on energy usage in the various approaches

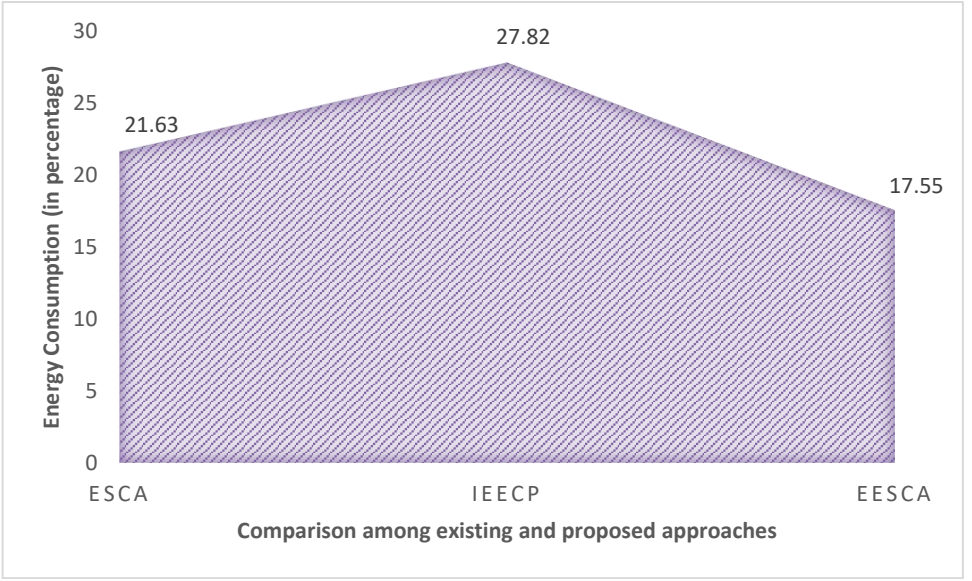

Fig 4.8. Comparison on IVR among various methods with the proposed method

Fig 4.8 shows that the energy consumed by the proposed methodology to perform clustering and data aggregation is minimal compared to existing approaches.

5. Conclusion

The proposed approach "Energy Efficient Clustering with Secured Aggregation" for clustering

and data aggregation with security appears to perform better than previous research. The research on this project would continue to calculate the energy consumed when data is sensed and sent to its destination. In the current phase, the proposed work provides good network coverage while minimizing packet loss and latency. It is evident that data may be pooled safely and energy is used efficiently.

References

[1] Hassan, A. A. H., Shah, W. M., Habeb, A. H. H., Othman, M. F. I., & Al-Mhiqani, M. N. (2020). An improved energy-efficient clustering protocol to prolong the lifetime of the WSN-based IoT. Ieee Access, 8, 200500-200517.

[2] Khan, M. N., Rahman, H. U., Almaiah, M. A., Khan, M. Z., Khan, A., Raza, M., ... & Khan, R. (2020). Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. Ieee Access, 8, 176495-176520.

[3] Bhushan, S., Kumar, M., Kumar, P., Stephan, T., Shankar, A., & Liu, P. (2021). FAJIT: a fuzzy-based data aggregation technique for energy efficiency in wireless sensor network. Complex & Intelligent Systems, 7, 997-1007.

[4] Sert, S. A., & Yazici, A. (2021). Increasing energy efficiency of rule-based fuzzy clustering algorithms using CLONALG-M for wireless sensor networks. Applied Soft Computing, 109, 107510.

[5] Khediri, S. E., Nasri, N., Khan, R. U., & Kachouri, A. (2021). An improved energy efficient clustering protocol for increasing the life time of wireless sensor networks. Wireless Personal Communications, 116, 539-558.

[6] Sharada, K. A., Mahesh, T. R., Chandrasekaran, S., Shashikumar, R., Kumar, V. V., & Annand, J. R. (2024). Improved energy efficiency using adaptive ant colony distributed intelligent based clustering in wireless sensor networks. Scientific Reports, 14(1), 4391.

[7] Rehman, A., Abdullah, S., Fatima, M., Iqbal, M. W., Almarhabi, K. A., Ashraf, M. U., & Ali, S. (2022). Ensuring security and energy efficiency of wireless sensor network by using blockchain. Applied Sciences, 12(21), 10794.

[8] Khera, S., Turk, N., & Kaur, N. (2023). HC-WSN: a Hibernated Clustering based framework for improving energy efficiency of wireless sensor networks. Multimedia Tools and Applications, 82(3), 3879-3894.

[9] Nedham, W. B., & Al-Qurabat, A. K. M. (2022, May). An improved energy efficient clustering protocol for wireless sensor networks. In 2022 International Conference for Natural and Applied Sciences (ICNAS) (pp. 23-28). IEEE.

[10] Dogra, R., Rani, S., Kavita, Shafi, J., Kim, S., & Ijaz, M. F. (2022). ESEERP: Enhanced smart energy efficient routing protocol for internet of things in wireless sensor nodes. Sensors, 22(16), 6109.

[11] Dattatraya, K. N., & Rao, K. R. (2022). Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN. Journal of King Saud University-Computer and Information Sciences, 34(3), 716-726.

[12] Ahmed, A., Abdullah, S., Bukhsh, M., Ahmad, I., & Mushtaq, Z. (2022). An energy-efficient data aggregation mechanism for IoT secured by blockchain. IEEE Access, 10, 11404-11419.

[13] Ramasamy, K., Anisi, M. H., & Jindal, A. (2021). E2DA: Energy efficient data aggregation and end-to-end security in 3D reconfigurable WSN. IEEE Transactions on Green Communications and Networking, 6(2), 787-798.

[14] Said, G., Ghani, A., Ullah, A., Azeem, M., Bilal, M., & Kwak, K. S. (2022). Light-weight secure aggregated data sharing in IoT-enabled wireless sensor networks. IEEE Access, 10, 33571-33585.