Journal of Theoretical and Applied Information Technology
15th May 2026. Vol.104. No.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURE ENHANCED DUAL AUTHENTICATION IN MPSO FOR WSNS

Dr.M.SUPRIYA [1] , Dr.T. ADILAKSHMI [2]

[1] Associate Professor and HOD, Dept. of CSE(Data Science) , Swami Vivekananda Institute of Technology, JNTUH, Secundrabad, India

[2]Professor and Head, Dept of CSE, Vasavi College of Engineering, Osmania University,Hyderabad,India

E-mail: [1]supriyasamuel@svit.ac.in , [2]t_adilakshmi@staff.vce.ac.in

ABSTRACT

Wireless Sensor Networks (WSNs) are essential in fields like military surveillance, industrial monitoring, and environmental observation. However, they are particularly vulnerable to different security attacks during Cluster Head (CH) selection and data aggregation due to their distributed nature and limited computational capacity. This work offers an improved and secure method for CH selection combined with the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol in order to overcome these difficulties. The suggested framework includes sophisticated security features as well as an effective way to identify malicious network nodes. The enhanced scheme eliminates nodes that exhibit unusual or malevolent packet-dropping tendencies during the CH selection stage by combining the traditional LEACH protocol with two evaluation metrics: Dropped Packet Ratio (DPR) and Residual Energy (RE). Particle Swarm Optimization (PSO) is used to further optimize routing efficiency, allowing for dependable path formation and better energy utilization. An Enhanced Dual Authentication (EnDA) method with a strongkey management system adds an extra layer of security that ensures data integrity and guards against unauthorized access. Simulations show notable improvements in network performance, security, and dependability.. Consequently, the suggested system improves the general security and dependability of WSN operations.

Keywords: *Residual Energy. Dropped Packet Ratio (DPR), Enhanced dual authentication (EnDA) , K-LionER ,PSO,Energy Consumed*

1. INTRODUCTION

There has been a lot of interest in wireless sensor networks (WSNs) lately because they can be used in many areas, such as smart cities, healthcare [1], the military, and environmental monitoring. There are a lot of sensor nodes in these networks that gather, look at, and send information to central base stations [2]. This enables real-time monitoring and decision-making in a range of situations. However, WSNs' inherent characteristics—such as their distributed architecture, limited energy sources [3], and vulnerability to physical attacks—present unique challenges, particularly with regard to ensuring secure and efficient data transfer. Wireless Sensor Networks (WSNs) depend on the proper Cluster Heads (CHs) to maintain the base station connection and oversee data aggregation.

Through effective CH selection, the well-known Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol has contributed to lower energy usage and longer network lifetimes [4]. However, malevolent nodes might jeopardize the integrity of the data aggregation process by rejecting packets or initiating other kinds of assaults, and LEACH does not automatically resolve these security flaws. Additionally, the potential of security breaches has increased as WSNs continue to be employed in increasingly sensitive and critical applications.

Enhanced Dual Authentication (EnDA) mechanism with a double key management system, which protects against unwanted access and guarantees data integrity.

The Dropped Packet Ratio (DPR) is a metric that indicates no of packets lost during transmission in a wireless network. A higher DPR indicates poorer channel conditions As a result, it is essential to create CH selection strategies that give energy efficiency top priority while also bolstering the network's security posture against these kinds of internal attacks [5]. Optimizing the route selection mechanism is as crucial as safeguarding the CH selection process. Energy efficiency remains the top priority because the majority of sensor nodes are powered by batteries with a limited capacity. One potential solution to this problem is to use metaheuristic algorithms such as PSO. The best routing pathways that balance

energy consumption and network performance can be chosen thanks to PSO's efficient exploration and exploitation. PSO and other metaheuristic algorithms are one possible solution to this issue. PSO's effective exploration and exploitation of the search space enables the selection of optimal routing pathways that balance energy consumption and network performance. resulting in improved reliability and extended operational lifetime

LEACH protocol

The LEACH protocol is acknowledged as the first clustering-based routing protocol that achieves scalable solutions and extends network lifetime [8]. By uniformly distributing the network workload among multiple nodes at various intervals, the LEACH protocol makes it possible to reduce overall energy consumption. Sensor nodes are frequently arranged hierarchically within clusters, and each cluster has a CH. The CH is in charge of collecting data from the nodes in its group, creating data reports, and forwarding them to the sink node. Equation 1 states that if a randomly generated number between 0 and 1 is less than the predetermined threshold,

$TH(n)$, a node in the LEACH protocol becomes a CH.

$$TH(n) = \begin{cases} \frac{P}{1-P\left[\left(r \bmod \frac{1}{P}\right)\right]}, & if\ n \in G \\ 0, & otherwise \end{cases}$$

Eq(1)

The probability is represented by P, and the threshold value of n nodes is represented by $TH(n)$. A random integer between 0 and 1 is chosen by each network node.

This study offers a novel approach to guarantee the security of data aggregation and CH selection in WSNs.The suggested method uses a statistic called Dropped Packet Ratio (DPR) and Residual Energy (RE) to enhance the traditional LEACH process. By identifying malicious nodes, this statistic prevents them from turning into CHs.The PSObased routing algorithm also helps to improve the network's energy efficiency by identifying the best paths for data transfer. This improves the security and reliability of the data aggregation process in WSNs.

2. LITERATURE SURVEY

Aarti Sharma et al. [10] have developed a novel method by combining the Fire Fly algorithm, Artificial Neural Network, and an enhanced LEACH algorithm to overcome the challenges mentioned above. This strategy focuses on ensuring energy efficiency and security. A new threshold Value considering the distance of coverage, average energy, and residual energy of the nodes is used in choosing the CHs. This is contrary to the traditional LEACH technique that selects the cluster head only using a random integer determined by probability. Performance suffers and the risk of data loss increases when there are rogue nodes in the route network. As a result, a secure and energy-efficient routing protocol is required. The best node properties are produced using the firefly approach. After that, an artificial neural network (ANN) is used to identify any attacker nodes that may be present along the current route and to detect the existence of communicative and non-communicating nodes.R. Hajian et al [12] introduced the new continuous hybrid and energy-efficient secure data aggregation (CHESDA) method, which balances data integrity, privacy protection, latency, accuracy, and communication overload. The algorithm intelligently selects the most suitable scenario depending on the specific application and the relevance of the parameters involved. The slice-mixing approach is used to preserve privacy preservation. Fuzzy logic serves to the algorithm determines the optimal slicing for each subtree, while GNY logic is used to authenticate the key verification. methodology. Khushboo Jain et al. [13] proposed the Scalable Clustering Algorithm for Data Aggregation (SCADA), a clustering-based scheme specially designed for efficient data aggregation in WSNs. Each cluster in SCADA consists of a single Cluster Head (CH) and multiple Cluster Relays (CRs), where the number of CRs is changes according to distance between cluster and Base Station. The method minimizes energy consumption. it achieves multi-hop short-distance data transfer and optimizes control packet usage by rotating the CHs at at appropriate intervals. The approach features a mixed CH selection mechanism, a threshold-based CH rotation. system, along with an optimized CR distribution policy, renders it effective for both homogeneous and heterogeneous WSNs. The performance of the method is analyzed based on several varied parameters, such as the length of the sensing field and sensor node. density, cluster count, initial energy, and variability. Rekha et al

[14] presented the K-LionER scheme, a Hybrid approach for energy-efficient clustering-based routing in WSN enabled by the Internet of Things (IoT). It combines K-means clustering with ant Lion optimization. The major objectives of the K-LionER,The objectives of project are to increase energy efficiency and network lifetime. K-means method is applied to form a clusters in the WSN under study, and the ant lion optimization strategy

is used to choose each CH. Cluster.In such a clustering, the leader in every cluster collects information from each member individually and forwards the aggregated information.to the base station. Shiv Dutta Mishra et al. [15] proposed a technique known as "Reliable Clustering with Optimized Scheduling and Routing for Wireless Sensor Networks, to improve energy efficiency and the reliability of clustering, this method presents the GridCosins chain Clustering technique, organizing sensor nodes are based on GridCosins distance and form a distance tree structure within clusters, thereby increasing network life and decreasing transmission range. The methodology includes a novel dual Cluster Head Selection strategy using Turtle Search Technique-Desert Cat Swarm Optimization (TSA-DCSO) to improve CH selection to minimize idleness and passive listening. In addition, the Robust Node Switching algorithm can State Algorithm controls energy consumption to avoid CH overload and decreases excessive consumption of energy during data transmission to the CH,p18[16]Their scheme can resist node captured attacks, but the low efficiency in communication and high energy consumption makes it impractical. After that, Jiang et al.

3. PROPOSED MPSOENDA

The suggested approach for choosing CHs and the strategy for stabilizing the random number generation process are described in this section. The method is to multiply a random integer by the sensor nodes' DPR and RE measurements. By ensuring that dynamic network circumstances have an impact on the CH selection process, this integration produces results that are more dependable.

Remaining energy: The remaining energy Re isinitial energy ei minus total energy consumed eec by the node. Here, Re is measured because to avoid the weaker nodes in CH candidate participation.

The remaining energy of node "n" is

$$R_e^T(n) = e_i^T(n) - e_{ec}^T(n)$$

Where, Eec of node n can be evaluated as

$$e_{ec}(n) = e_{i,n} + e_{n2s} + e_{el} + e_{ae}$$

Here, ei,n & $en2s$ are the energy transmitted for "l" bits from node "i" to "n" and "n" to base station s or sink, respectively, and eae is aggregating energy of a data, eel is energy consumed by the receiver circuit per bit.Dropped packet rate: The Dropped Packet Ratio (DPR) is a metric that indicates no of packets lost during transmission in a wireless network. A higher DPR indicates poorer channel conditions. Malicious nodes can significantly increase the DPR by using various attack strategies, such as packet dropping, jamming, black hole attacks, and selective forwarding. This can lead to reduced network performance, inaccurate channel assessment, and compromised cluster head selection in protocols like LEACH. Higher DPR can result in decreased throughput, increased latency, and lower network reliability. Malicious nodes can also manipulate channel quality assessment metric and influence the selection process by artificially increasing or decreasing their own DPR. This can be calculated using the below formula

$$DPR = \frac{\sum_{i=1}^{N}\left(\frac{P_{d,i} + \alpha \times P_{r,i}}{P_{t,i} + \beta \times P_{re,i}}\right)}{N}$$

N is the total number of nodes. $P_{d,i}$ is the number of packets dropped by the node i. $P_{t,i}$ is the total number of packets sent by the node i. $P_{r,i}$ is the number of packets retransmitted by the node i. $P_{re,i}$ are the number of retransmissions attempts for the node i. where N indicates the total number of nodes.$P_{d,i}$ represents the quantity of packets that the node drops. The total number of packets transmitted by node i is denoted by $P_{t,i}$. $P_{r,i}$ is the number of packets that node i retransmits. $P_{re,i}$ represents the node i's retransmission attempt count.α & $\beta$are the weight factors.Each node is assigned with a weight-coefficient by estimating the selection parameters. A Weighted Sum Approach (WSA) is used to manage the trade-off between the parameters. On every value the weight value is multiplied to this objective value. Finally, all of the multiplied values are added to combine the various objectives into a single scalar objective function.

This can be represented as:

$$w = (\alpha 1 \times RE) + (\alpha 2 \times DPR)$$

Journal of Theoretical and Applied Information Technology
15th May 2026. Vol.104. No.9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$w_n = \left(\alpha 1 \times e_i^T(n) - e_{ec}^T(n)\right) + \left(\alpha 2 \times \left(\frac{\sum_{i=1}^{N}\left(\frac{P_{d,i} + \alpha \times P_{r,i}}{P_{t,i} + \beta \times P_{re,i}}\right)}{N}\right)\right)$$

Here $\alpha 1 + \alpha 2 = 1$.

CH selection: Rand (n) is a representation of the normal random number. The enhanced random number process in the suggested method may be expressed as follows:

$$rand(n)' = rand(n) * (w_n)$$

A key component of the CH selection process, which chooses the CH based on node probabilities, is the threshold function. The threshold function effectively modifies the network's performance by utilizing the nodes' average node energy. To ensure consistent energy consumption, the CH duty is shared across all network nodes. From the start to the finish of the network, the energy, dropped rate, and threshold function of the suggested LEACH algorithm determine which node is chosen for CH.

According to equation 1 r stands for the round number and P_n for the probability that n will become CH.The threshold function is now matched to the value of the modified random number.

$$rand(n)' \leq TH(n)$$

The node becomes CH if the random value is less than the threshold; else, the procedure will restart for the next node.

Particle swarm optimization (PSO)

Particle Swarm Optimization (PSO) draws inspiration from natural phenomena, such as fish schools and flocks of birds. In quest of food or refuge, these birds frequently move in groups without clashing. Each bird or member of a group modifies its location and speed in accordance with the group information. Because group members share knowledge, each bird's or member's own effort to find food and shelter decreases. PSO is made up of a predetermined number of particles (S_n), each of which provides a solution to a particular issue instance. A fitness function will be used to assess each particle. Every particle has the same dimension. In the dth dimension of the hyperspace, each particle possesses a location (P_{id}) and velocity (Vel_{id}). Therefore, particle is represented at any given moment as $P_i = P_{i1}, P_{i2}, P_{i3}, \ldots . P_{id}$

Each particle P_i repeatedly updates its location and velocity by following its own best ($pbest$) and global best ($Gbest$) to arrive at the global best position. Until the $Gbest$ is discovered or the maximum number of iterations is reached, this updating procedure is repeated. Each particle i is first given a location X_{id} and a velocity $V_{id}(i = 1,2, \ldots S)$ at random, where S$= 1.2 \ldots D$. Every particle records the global best position $gbest_i$ and its own best position $pbest_i$.

The original PSO algorithm is shown below:

Particle Swarm Optimization (PSO) Loop
1. Initialize particles
2. While goal not reached:
   - Evaluate each particle's fitness
   - Update personal best (pbest)
   - Set global best (gbest)
   - Update velocity & position of each particle

The position and velocity of the particles are updated as follows

$$V_{id}(t+1) = w * V_{id}(t) + L_1 * R_1 * \left(pbest_i(t) - X_{id}(t)\right) + L_2 * R_2 * \left(Gbest_i(t) - X_{id}(t)\right)$$

$$X_{id}(t+1) = X_{id}(t) + V_{id}(t+1)$$

r1 and r2 are random variables between [0,1]. L_1 & L_2 are the learning factors. W It is a weight factor that controls the velocity of the particle.

4. PROPOSED RELAY SELECTION SCHEME

The proposed approach uses the PSO technique to choose efficient relay nodes for data transfer between sensor nodes and CHs. The nodes are considered particles, and their fitness value is evaluated using a Fitness function that takes into account residual energy and transmission latency. The fitness value will then be computed for each sensor node in the relay node selection procedure. This method saves network energy while ensuring efficient data transfer between sensor nodes and CHs.

The PSO approach is used in conjunction with transmission delay and node residual energy to choose the relay nodes. The selection criteria of the relay, which determines the most effective CH node, is quite important. To save on the battery life, the relay node transmits the data of the member nodes to the CH.The PSO approach uses the relay selection parameters to provide fitness values for the CH nodes taking part in the relay selection process. The following are the parameters used for selecting the relay:

Residual Energy: Through relay nodes, each member node sends data to its corresponding CH. Energy is regarded as the most crucial factor in relay selection as a node with high energy can carry out relay functions well and endure for a longer amount of time. Insufficient energy can cause the minimal energy node to expire or cease operating during data transmission. It can be formulated as follows

$$f_1 = \frac{1}{M} * \sum_{i=1}^{N} E_{res}(N)$$

Transmission delay: This refers to the delay in transmission that occurs between the sensor nodes. The network's energy usage rises in tandem with the delay. For effective data transmission, the relay nodes should have the least amount of latency. The node's anticipated transmission count (ETC), propagation delay (PD), and network transmission delay (TD) all directly affect the node's latency. This can be formulated as follows:

$$Delay\ D(t) = \sum_{i=1}^{m} ETC_i(t)(TD + PD_i)$$

$$f_2 = \sum_{i=1}^{m} \min\left(Dt_{Si}\right)$$

A fitness value is produced for each node involved in the relay selection process using the suggested

$$e(j, i+k) == e(i+k, j)\ \&\&$$
$$e(i+k, j) == e(i, j) * e(k, j)$$

PSO approach.The nodes broadcast a message with their node ID and fitness value to the nodes within their range when the fitness values are generated.The relay election nodes compare their fitness results with those of the cluster's other sensor nodes.In order to convey the data to CH, the node with the best fitness value will be chosen as the ideal relay. The relay selection process's fitness function is provided as:

$$pbest_i = \omega_1 \times f_1 + \omega_2 \times f_2$$
$$f_1 = max\{residual_{energy}(n)\}, \quad 1 \le n \le N,$$
$$where\ N = tot\ no\ of\ nodes$$
$$pbest_i = \omega_1 * \frac{1}{M} \times \sum_{i=1}^{N} E_{res}(N) + \omega_2 \times \sum_{i=1}^{m} \min\left(Dt_{Si}\right)$$

$$Gbest_i = max[pbest_i]$$

Where the weight coefficient for the fi tness functions, denoted by, ranges from 0 to 1. $(0 < \omega < 1)$

The relay task is awarded to the node with the greatest fitness value in the relay competition. The sensor nodes send their collected data to the closest relay node which then forwards it to the next relay, and so on, until the data reaches the CHs.

5. Proposed dual authentication (EnDA) key management scheme

This section describes a method for improving communication security utilizing the Diffie-Hellman key exchange protocol with a bilinear map mechanism and elliptical curve cryptography (ECC). es security & data integrity.
A central authority in WSN is responsible for managing certificate requests from every node. Mutual authentication, session key management, privacy protection, reduced transmission overhead, and quick verification are all possible with ECC.

Using the ECC technique, the batch request may be divided and processed independently. Assume that a central authority is used to link every node. Every node in the area is referred to as the domain. Region is presumed to be defined as a component of communication. Communication and information sharing between domains are contingent upon central authority consent

The proposed protocol is operated in phases: setup phase, and phase, authentication phase. The setup phase algorithm is presented below:

The central authority creates a bilinear map during system setup by implementing the following restrictions.

e is a mapping function employing simple distribution, and i, j, and k are natural integers.

The following bilinear map restrictions are used to manage mapping distribution for group communication.

$$e(a*i,b*i)=e(i,b*i)\wedge a \;\&\&\; e(i,b*i)\wedge a == e(a*i,i)\wedge b \;\&\&\; e(a*i,i)\wedge b == e(i,i)\wedge(ab)$$

Using a chosen random integer as input, a second - level hash function is used to construct the central authority's trust parameter.

$$S_{TA}=H2(r,id)$$

where r is a random integer chosen from a bilinear map, id is the central authority's ID, T's security parameter, and H2 is a second-level hash function that uses a cryptographic key function.

In conclusion, a mapping distribution with bilinear constraint is used during the setup phase.

Additionally, a random value related to the bilinear map is used to construct the trust parameter.

Communication takes place during the communication phase once the setup has been created with the central authority.

-The central authority communicates with mobile nodes by sending an announcement message.
-The receiver stores the communication ID of the central authority.
-Upon receiving the central authority announcement message, the node requests the secret key and security parameters.
-To commence this procedure, submit a key request message to the central authority, including the node ID.
-The central authority receives key request messages from nodes and creates a hash key using the following method.

$$INP = CT_{ID}\ XOR\ NODE_{ID}$$
$$KEY = sha1\big(ECC(INP)\big)$$

where, ECC elliptic curve key generation function,- Sha1 -Sha algorithm to apply hash function.

-The central authority sends a unicast message with the produced key to the node.

-The node keeps the key and expiration time for key updates.

-After obtaining the key from the central authority, nodes send announcement messages to other nodes, including their position coordinates.

-The node uses Euclidean distance estimates to establish contact with the nearest node within its communication range after receiving announcements from all accessible nodes.

-Nodes transmit registration requests to the central authority after receiving the announcement message.

-The central authority receives messages and produces pseudonyms for nodes using the following method.

$$INP = CT_{ID}\ XOR\ NODE_{ID}$$
$$\text{pseudonym} = \text{hash(INP)}$$
$$KEY = sha1\big(ECC(INP)\big)$$

In conclusion, to provide secure communication, the communication phase generates a hash key and a pseudonym.Every communication node's session is updated.Nodes can use a one-way hash function to update session keys throughout time slots in a group session. Following a key update message, each node may create a new session key.

Algorithm

For every node $'n'$

Compute w

Compute $TH(n)$

Estimate $rand(n)$

$rand\ (n)' = rand(n) + w$

If $rand\ (n) \leq TH(n)$

CH = n;

End if

End for

Data transmission phase

Calculate $pbest$

If $pbest_j > pbest_i$

$pbest = pbest_j$

End if

If $pbest_j > Gbest$

$Gbest = pbest_j$

End if

Compute relay nodes using $Gbest$

End for

6. SIMULATION RESULTS ANALYSIS

We assessed the efficacy of the suggested techniques using simulations conducted using NS2 and compared them with the K-LionER [14] and TSA-DCSO [15] approaches. The sensor nodes are distributed in a field with dimensions of 1000m X 500m in a random manner, and each sensor node is initially assigned an energy level of 100j. There are between 50 and 200 nodes in the network. The experimental parameters are shown in Table 1 below

Table 1 End to End delay

NODES	K-LionER	TSA-DCSO[15]	PROPOSED
50	0.39	0.23	0.16
100	0.38	0.24	0.17
150	0.42	0.25	0.16
200	0.45	0.24	0.18
250	0.48	0.25	0.17

Fig 2. End to End Delay

The overall time needed for data transmission, also known as end-to-end latency, is shown in Figure 2 . The network had a minimum average delay of 0.17 ms and a maximum delay of 0.18 ms when the number of nodes was increased to 250.In contrast, the KLionER approach experienced a maximum delay of 0.48 ms, while the TSA-DCSO method had a maximum delay of 0.25 ms.

Table2 : Energy Consumption

NODES	K-LionER	TSA-DCSO	PROPOSED
50	4.54	4.01	3.81
100	4.9	4.28	4.05
150	5.34	4.61	4.24
200	5.88	4.99	4.48
250	6.4	5.4	4.85

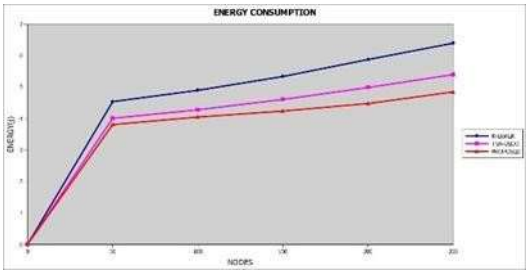

Fig 3. Energy consumption

The simulation findings in Figure 3 above show how quickly both the current and novel methods utilize energy. The energy levels of each sensor node were the same at first. Generally speaking, any network action uses energy. Based on the results of the trial, the recommended method required an average of 4.1 joules of energy. The average energy usage was 5.40 joules in the TSA-DCSO model and 6.4 joules in the K-LionER model, which were both very low. Incorporating variables like packet loss rate and residual energy into the cluster head selection process, in addition to using Particle Swarm Optimization (PSO) for the

best relay selection, allowed for this decrease in energy use

Table 4: Network Overhead

NODES	K-LionER	TSA-DCSO	PROPOSED
50	0.29	0.28	0.27
100	0.59	0.55	0.54
150	0.65	0.63	0.59
200	0.89	0.88	0.67
250	0.96	0.91	0.76

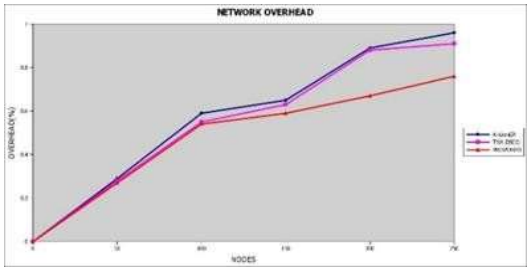

Fig. 4. Network overhead

The simulation results for the overhead of the network are shown below figure 4. The quantity of control packets that are sent across the network to support its operations causes the overhead to rise proportionately. The overhead for the recommended methodology was around 0.76%, whereas the overhead for the K-LionER and TSA-DCSO techniques was approximately 0.96% and 0.91%, respectively. By considering factors like transmission delay while choosing relays, the chance of a route failure is reduced, which reduces the need for control packets to be broadcast on a frequent basis. Thus, the recommended course of action successfully reduces the overhead.

Table 5: Packet Delivery Ratio

NODES	K-LionER	TSA-DCSO	PROPOSED
50	0.75	0.86	0.90
100	0.74	0.86	0.91
150	0.74	0.85	0.90
200	0.75	0.87	0.92
250	0.74	0.86	0.91

Figure 5 above displays the simulation results of the proposed and current methods in terms of packet de

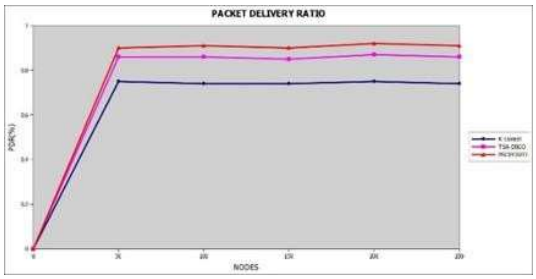

Fig. 5. Packet delivery ratio

livery ratio. Packet Delivery Ratio, or PDR, is a statistic used to measure how well a network transmits data. The prior approaches maintained average Packet Delivery Ratios (PDR) of 0.74% and 0.86%, respectively, whereas the new strategy achieved a maximum PDR of 0.92%. The proposed method outperforms the existing systems in terms of performance by selecting an efficient communication channel by using features such as transmission delay and CH selection based on lost packet rate.

Table 6 Network Performance

NODES	K-LionER	TSA-DCSO	PROPOSED
50	109	140	187
100	108	141	188
150	108	139	190
200	109	142	189
250	111	144	189

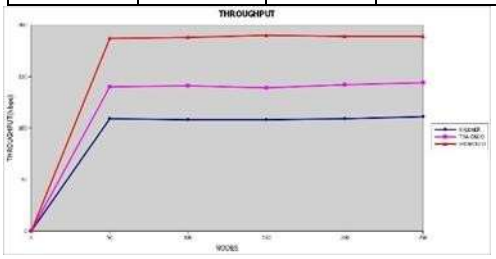

Fig 6. Network performance

The simulation results for the Throughput of the present and suggested ways are shown in the graph above figure 6. The amount of data that may be sent between sensor nodes is referred to as throughput. A high throughput ensures that a lot of data is sent quickly and efficiently. When compared to existing approaches, the data above shows that the recommended strategy delivers a substantially greater throughput rate. The suggested method continuously has maintained an average throughput rate of up to 189 kbps throughout the testing.

5. CONCLUSION

The suggested approach aims to solve the security

and efficiency issues in WSNs by putting in place a secure CH selection and data aggregation technique.. By adding a Dropped Packet Ratio (DPR) statistic, it improves on the conventional LEACH protocol by excluding hostile nodes and choosing only trustworthy nodes to be CHs. The routing technique based on Particle Swarm Optimization (PSO) balances energy consumption and network performance while optimizing data transmission channels. Longer operating lifespans and more effective utilization of network resources are the outcomes of this. An additional layer of security is added by an Enhanced Dual Authentication (EnDA) mechanism with a strongkey management system, which protects against unwanted access and guarantees data integrity. Simulations demonstrate significant gains in network security, dependability, and performance, which makes this method a beneficial addition to WSNs and a viable choice for applications needing high security and effectiveness

REFERENCES:

[1] Rao, P.M. and Deebak, B.D., 2023. Security and privacy issues in smart cities/industries: technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing, 14(8), pp.10517-10553.

[2] Gantassi, R., Messous, S., Masood, Z., Sias, Q.A. and Choi, Y., 2024. Enhanced Network QoS in Large Scale and High Sensor Node Density Wireless Sensor Networks Using (IR-DV-Hop) localization algorithm and mobile data collector (MDC). IEEE Access.

[3] Alamu, O., Olwal, T.O. and Djouani, K., 2023. Energy harvesting techniques for sustainable underwater wireless communication networks: A review. e-Prime- Advances in Electrical Engineering, Electronics and Energy, p.100265.

[4] Alghamdi, Turki Ali. "Energy efficient protocol in wireless sensor network: optimized cluster head selection model." Telecommunication Systems 74, no. 3 (2020):

331-345. Sharma, Aarti, and Ankush Kansal. "Enhanced CH selection and energy efficient routing algorithm for WSN." Microsystem Technologies (2024): 1-13.

[5] Sharma, Aarti, and Ankush Kansal. "Enhanced CH selection and energy efficient routing algorithm for WSN." Microsystem Technologies (2024): 1-13.

[6] Del-Valle-Soto, C., Rodríguez, A. and Ascencio-Piña, C.R., 2023. A survey of energy-efficient clustering routing protocols for wireless sensor networks based on metaheuristic approaches. Artificial Intelligence Review, 56(9), pp.9699-9770.

[7] Meenakshi, N., Ahmad, S., Prabu, A.V., Rao, J.N., Othman, N.A., Abdeljaber, H.A., Sekar, R. and Nazeer, J., 2024. Efficient communication in wireless sensor networks using optimized energy efficient engroove leach clustering protocol. Tsinghua Science and Technology, 29(4), pp.985-1001.

[8] Ramya, R., and Thomas Brindha. "A comprehensive review on optimal cluster head selection in WSN-IOT." Advances in Engineering Software 171 (2022): 103170.

[9] Guhan, T., N. Revathy, K. Anuradha, and B. Sathyabama. "EEDCHS-PSO: energy-efficient dynamic cluster head selection with differential evolution and particle swarm optimization for wireless sensor networks (WSNS)."In Evolution in Computational Intelligence: Frontiers in Intelligent Computing: Theory and Applications (FICTA 2020), Volume 1, pp. 715-726. Springer Singapore, 2021.

[10] Daanoune, Ikram, Baghdad Abdennaceur, and Abdelhakim Ballouk. "A comprehensive survey on LEACH-based clustering routing protocols in Wireless Sensor Networks." Ad Hoc Networks 114 (2021): 102409.

11] Sharma, Richa, Vasudha Vashisht, and Umang Singh. "eeTMFO/GA: a secure and energy efficient cluster head selection in wireless sensor networks." Telecommunication Systems 74, no. 3 (2020): 253-268.

[12] Hajian, Rahman, and Seyed Hossein Erfani. "CHESDA: continuous hybrid and energyefficient secure data aggregation for WSN." The Journal of Supercomputing 77, no. 5 (2021): 5045- 5075.

[13] Jain, Khushboo, Pawan Singh Mehra, Anshu Kumar Dwivedi, and Arun Agarwal. "SCADA: scalable cluster- based data aggregation technique for improving network lifetime of wireless sensor networks." The Journal of Supercomputing 78, no. 11 (2022): 13624-13652.

[14] Rekha, and Ritu Garg. "K-LionER: meta-heuristic approach for energy efficient cluster based routing for WSN-assisted IoT networks." Cluster Computing (2024): 1-15.

[15] Mishra, Shiv Dutta, and Dipti Verma. "Energy-Efficient and Reliable Clustering with Optimized Scheduling and Routing for Wireless Sensor Networks." Multimedia Tools and Applications (2024):

[16] Hu, B., Tang, W., & Xie, Q. (2022). A two-factor security authentication scheme for wireless sensor networks in IoT environments. *Neurocomputing*, *500*, 741-749.