











ORIGINAL

Hybrid Elephant Herding Optimization Approach for Cluster Head Selection and Secure Data Transmission in WSN Using Hybrid Approach Cryptography Techniques

Enfoque Híbrido de Optimización del Manejo de Elefantes para la Selección de Cabezas de Cluster y la Transmisión Segura de Datos en WSN Utilizando Técnicas de Criptografía de Enfoque Híbrido

M. Yuvaraja¹  , D. Sumathi²  , M. Rajeshkumar³  , Mohamed Uvaze Ahamed Ayoobkhan⁴  

¹Associate Professor, P. A. College of Engineering and Technology. Pollachi-642001.

²Associate Professor, Alliance College of Engineering and Design. Bangalore.

³Assistant Professor, KPR College of Arts Science and Research. Coimbatore.

⁴Assistant Professor, New Uzbekistan University. Tashkent, Uzbekistan-100007.

Cite as: M. Y, D. S, Rajeshkumar M, Ahamed Ayoobkhan MU. Hybrid Elephant Herding Optimization Approach for Cluster Head Selection and Secure Data Transmission in WSN Using Hybrid Approach Cryptography Techniques. Data and Metadata. 2024; 3:.366. <https://doi.org/10.56294/dm2024.366>

Submitted: 25-01-2024

Revised: 21-04-2024

Accepted: 02-09-2024

Published: 03-09-2024

Editor: Adrián Alejandro Vitón Castillo 

Corresponding Author: M. Yuvaraja 

ABSTRACT

Introduction: the wireless nature of sensor networks makes safe transfer of data from one node to another a major challenge in communications. Sensing tasks connect these sensor nodes which have limitations of memories and energies. Cryptography techniques are utilised to handle critical issues of security in these networks. The performance of large-scale networks is enhanced in this case by optimisation algorithm mimicking natural behaviours.

Method: this work uses H-EHO (Hybrid Elephant Herding Optimisation technique based on Individual strategies to enhance cluster head selections in WSNs (Wireless Sensor Networks) and thus extend networks' lifetime. WSNs complete cluster head selection processes, and proposed optimisation approach which selects cluster heads based on tracking of sensor nodes for enhancements. The clan operators of optimisation algorithms are adjusted to handle random walk scale factors of elephants. Clusters of WSNs elect updated sensor nodes in principle. Hybrid algorithm HSR19, a novel security symmetric technique offers greater security during data transfers. It offers integrity, confidentiality, and authentication for cryptographic primary keys.

Results: the output of the simulation demonstrates the energy consumption, network longevity, end to end delay, and secure data transfer metrics. The results for choosing an effective and time-efficient cluster head selection process for WSNs are improved by contrasting the two approaches.

Conclusion: this comparison also shows the efficiency of communication devices in terms of calculation times for encoding, decoding and energies consumed for various file sizes.

Keywords: Wireless Sensor Network (WSNs); Hybrid-Elephant Herding Optimization (H-EHO); Hybrid Algorithm HSR 19; Cryptography.

RESUMEN

Introducción: la naturaleza inalámbrica de las redes de sensores hace que la transferencia segura de datos de un nodo a otro sea un desafío importante en las comunicaciones. Las tareas de detección conectan estos nodos sensores que tienen limitaciones de memoria y energía. Se utilizan técnicas de criptografía para manejar problemas críticos de seguridad en estas redes. En este caso, el rendimiento de las redes a gran escala se mejora mediante un algoritmo de optimización que imita los comportamientos naturales.

Método: este trabajo utiliza H-EHO (técnica de optimización híbrida de pastoreo de elefantes basada en estrategias individuales para mejorar las selecciones de cabezas de grupo en WSN (redes de sensores inalámbricos) y así extender la vida útil de las redes. Las WSN completan los procesos de selección de cabezas de grupo y proponen un enfoque de optimización que selecciona cabezas de grupo basadas en el seguimiento de nodos de sensores para mejoras. Los operadores de clan de algoritmos de optimización se ajustan para manejar factores de escala de caminata aleatoria de elefantes. Los grupos de WSN eligen nodos de sensores actualizados en principio. El algoritmo híbrido HSR19, una novedosa técnica de seguridad simétrica, ofrece mayor seguridad durante las transferencias de datos. Ofrece integridad, confidencialidad y autenticación para claves primarias criptográficas.

Resultados: el resultado de la simulación demuestra el consumo de energía, la longevidad de la red, el retraso de un extremo a otro y las métricas de transferencia segura de datos. Los resultados para elegir un proceso de selección de jefes de grupo eficaz y eficiente en el tiempo para las WSN mejoran al contrastar los dos enfoques.

Conclusión: esta comparación también muestra la eficiencia de los dispositivos de comunicación en términos de tiempos de cálculo para codificación, decodificación y energías consumidas para varios tamaños de archivos.

Palabras clave: Red de Sensores Inalámbricos (WSN); Híbrido-Optimización de Pastoreo de Elefantes (H-EHO); Algoritmo Híbrido HSR 19; Criptografía.

INTRODUCTION

Recent research uses bio-inspired optimisation methods to carry out diverse applications of WSNs and enhance performance. The wireless sensor nodes are selected for clustering in order to carry out communications in WSNs.⁽¹⁾ The uses of WSNs are widespread in the modern society, including in military, large-scale data network transmissions, etc. In order to create energy-efficient WSNs, acoustic localizations are used and performances are enhanced in terms of network longevity, energy efficiencies, transmission rates, and choices of sensor nodes.⁽²⁾

Optimal node points are used to choose the cluster head probability, and optimisation algorithms like PSO, genetic algorithms, and other naturally inspired algorithms are used. Localization challenges in WSNs are solved using a swarm intelligence algorithm based on a metaheuristic method.⁽³⁾ Due to the nodes' limited resources, complicated algorithms cannot be executed on them and consequently security becomes a major concern in WSNs.

The use of cryptographic techniques in WSNs is crucial for securing these networks.⁽⁴⁾ Numerous cryptography methods, including symmetric, asymmetric, and hybrid ones, have been presented thus far. Every network node needs to incorporate security in order for the network to be cryptographically secure.⁽⁵⁾ Therefore, security must be implemented at every network node.⁽⁶⁾ Cryptography algorithms in WSNs should be active while not consuming excessive amounts of memory, power, or energy for prolonging networks' lives.⁽⁷⁾ However, in other circumstances, the security will depend on the various application kinds, and the method may be unique to the application.⁽⁸⁾

This work suggests a new approach for cluster head selections and secure data transmissions to address these problems. H-EHO is used in cluster selections in order to raise thresholds and prolong lives of applications in WSNs. Cluster heads are selected using the clan and separation operators from the WSNs, and the updating approach makes use of the greatest number of sensor nodes with the greatest potential based on weight factor. To discover the intra-cluster communication, the cumulative distance between each cluster head is calculated. The main goal of the presented study is to compare AES, DES, 3DES, RC5 and IDEA encryption methods. Further, Symmetric key and asymmetric key cryptographies are also evaluated. High security is promised via a brand-new symmetric security algorithm. It offers main key integrity, confidentiality, and authentication in cryptography, and it also lengthens the network's lifetime and lowers E2E (end-to-end) latency, among other benefits.

Literature review

Wang et al.⁽⁹⁾ suggested the EDO-CS method, which stands for evolutionary diversity optimisation with clustering-based selection. After dividing policies into many groups based on their behaviours, high-quality policies are chosen in clusters which are then duplicated in iterations. The EDO-CS adaptively strikes a balance between quality and variety in the breeding process. Experiments on a variety of continuous control tasks, including deceptive and multi-modal tasks, demonstrate EDO-CS's superior performance over earlier approaches. Specifically, EDO-CS provided highly diverse and qualitative policy sets when compared to earlier approaches.

Shankar et al.⁽¹⁰⁾ combined two optimisation algorithms namely HAS (Harmony Search Algorithm) and SSA (Squirrel Search Algorithm), to obtain optimality in in terms of distance and energy during selections of cluster heads for WSNs. Their proposed schema, HSHSA (Harmony Search Algorithm hybrid squirrel) was more energy efficient when compared to prevailing CHS (Cluster Head Selection) procedures in identifying FND (first node removal) and LND (last node removal). Additionally, their proposed HSHSA showed enhancements in overall throughputs and remaining energies for WSNs.

Govardanagiri et al.⁽¹¹⁾ suggested selection of cluster heads using HGIBOA (hybrid grasshopper and improved bat optimisation algorithm) to maintain stable energy and extend the lifespan of WSNs. To increase the exploration potentials of GOA, their HGIBOA used variable coefficient-based Levy flights. To strike a balance between exploitation and exploration, the schema adopted the bat algorithm's local searching function. In order to increase its ability to be exploited, it also contained a random technique for applying it to high quality populations. The study's simulated results demonstrated the superiority of the proposed HGIBOA over QoS dependent multipath routing protocol based on CSPSO (Cuckoo search and PSO), FMABCCS (clustering scheme using Firefly and ABC already revised) and an integrated clustering strategy based on GWO and WOA (GWWOA). The proposed HGIBOA maintained excess energy, improved throughputs, extended network lifetime, and maintained stability with different counts of sensor nodes.

Bhandari et al.⁽¹²⁾ designed an improved cryptography approach combining Public Key Servers, symmetric and asymmetric encryption methods, and other factors. Elliptic Curve Cryptography was used to create each endpoint's unique MAC address and register key pairs between endpoints (user and IoT devices) and associated public keys in the public key server. Subsequently, parties decided on singular shared private secret keys that could be used as the base for all future AES-based encryptions. This concept can be referred to as multiphase protection systems as it can safeguard data transfers without any tampering from middlemen.

METHOD

More energy is used for sensor network communication in the WSNs application. For efficient optimisation in WSNs, the Elephant Herding Optimisation (EHO) imitates elephant behaviour. In this case, a multi-hop transmission network is collecting different send data on sensor node members.⁽¹³⁾ The proposed method intends to minimize shortcomings of current methods in terms of energy transmissions, PDRs (packet delivery ratios), and throughputs. Clusters are collections of sensor nodes that carry out specific tasks for specific applications. Exploitation and exploration of the hybridization strategy is used in local and global optimisation.⁽¹⁴⁾ In WSNs, the sensor node is compared to an elephant, and the clusters to the clan, each of which is associated with a matriarchal cluster leader. Each cluster contains identical and fixed sensor nodes, which alter their positions based on the optimisation approach's clan operator. Every sensor node's fitness value is calculated using a separation node. The cluster head is constructed using sensor nodes with the largest potential value.

Clan operator is represented by the equation (1) and (2).

$$X_{new,c,e} = X_{c,e} + \alpha (X_{best_{clan}} - X_{c,e}) O_{fit} \quad (1)$$

$$X_{new,c,e} = \beta (X_{center,clan}) \quad (2)$$

Where, the center of clan operator is obtained by below equation (3). In this, the dimension is measured to get the search process effectiveness.

$$X_{center_{clan},dim,c} = \frac{1}{nc} \sum_{e=1}^{n_{clan}} X_{c,e,dim} \quad (3)$$

The elephant clan is denoted as 'c' and elephant of sensor node is represented as 'e'. Both its updates the position of matriarch x(c,e).The scale factor of matriarch is used to obtain the fitness value of updated elephant.⁽¹⁵⁾ The separation operation helps to recognize the clan position for finding the individual nodes for getting optimal value. In clan operator, the best possible value is updated and the separation operator measures the worst clan value based on minimum and maximum instance. The optimizer initializes the upper and lower bound that is Xmin and Xmax.

Separation operator

$$X_{worst,clan} = Xmin + (Xmax - Xmin) * R \quad (4)$$

The equation (4) describes the Exploitation and exploration of H-EHO is achieved by updating the position of

elephant. Here the maximum fitness value is generated the clan 'c' and matriarch 'M(x)' at the time function 't'. Fitness of \max_{clan} is given by:

$$M(x) = \operatorname{argmax}_{x \in c} F(X) \quad (5)$$

The equation (5) represents the updating process of clan operator in EHO is updating the position. Based on the scale factor $\alpha \in [0,1]$, the position $\beta \in [0,1]$ is updated and it determines the factor ρ .

Matrix form of updated clan is given in equation (6).

$$X_{c,e}(t+1) = X_{c,e}(t) + \alpha \left(M(x+t) - X_{c,e}(t) \right) + \beta \left(c(t) - X_{c,e}(t) \right) + \rho R \quad (6)$$

Where, the clan operator with center position $c(t)$ is given by the equation (7).

$$c(t) = \frac{1}{n} \sum_e X_{c,e}(t) \quad (7)$$

The stochastic behavior of distributed function frames the uniform matriarch for making cluster from the sensor node of WSNs. Skewed distribution function is initializing with the separation operator based on the position of elephant. Random walk of elephant clan is determined lower and upper bound based on uniform distribution function and the individuals are generated with random vector.

Proposed hybrid-elephant herding optimization (h-eho)

The proposed hybrid EHO uses elitism strategy for updating best position of sensor nodes based on clan and separation operator. Initially, the best position is updated though finding the weight function of uniform distribution on the overall area.⁽¹⁶⁾ The best position is updated and the worst value in separation operator is replaced to update the best position of clan on exploration process. It searches every iteration for updating the value of cluster (elephant clan). Cluster head selection process updates matriarchs on fitness values and find optimal values involuminous data. The convergence rate is reduced to obtain better time consumption for getting energy efficient network model. The position of each sensor node is determined by the equation (8).

$$p_i(t+1) = aQ_i(t+1) + bP_i(t) \quad (8)$$

Here the 'a' and 'b' of weight factor is determined y maximum iteration. The fitness vector is randomly analyzed on the clusters based on time 't'.

$$a = Vrand(t) \quad (9)$$

$$b = 1 - Vrand(t) \quad (10)$$

In equation (9,10) the position of sensor node $p_i(t+1)$ is updated with iteration of fitness value and it has the weight factor of $(a+b+1)$. The random walk is updated to find the location and it measures the maximum population for getting better optimal value. The cluster head is updated with given equation (11).

$$p_i(t+1) = aQ_i(t+1) + b1P_i(t) + b2P_i(t) \quad (11)$$

Number of sensor node is generating the cluster head on WSNs and it identifies the maximum population diversity vector. Here the weight factor is considered as $a+b1+b2=1$, which updates the random vector for getting best population value. In this the weight factor is updated with random walk of elephant and the iteration is finding the fitness value 'Iteration (It $\in [1,2,\dots,n]$)'. The first to third weight factor is given by the equation (12,13 and 14).

$$a = Vrand(It) \quad (12)$$

$$b1 = (1 - Vrand(It)) \frac{Fi(t-1)}{Fi(t-1)+Fi(t)} \quad (13)$$

$$b2 = (1 - Vrand(It)) \frac{Fi(t)}{Fi(t-1)+Fi(t)} \quad (14)$$

Here the random selection process of cluster head is optimized through updating every sensor node with its iteration. The threshold value is analysed for selecting cluster head and randomly analysed position is updated for iteration basis function.

Cluster head selection process in wsns

Cluster heads are identified based on node functions and their position for updating weights which are used to obtain fitness values in cluster head selection processes.⁽¹⁷⁾ Network routers are used to gather information about sensor nodes and their counts in clusters, which perform communications of the network model. The router is setup for selection process of cluster head, which is shown in figure 1.

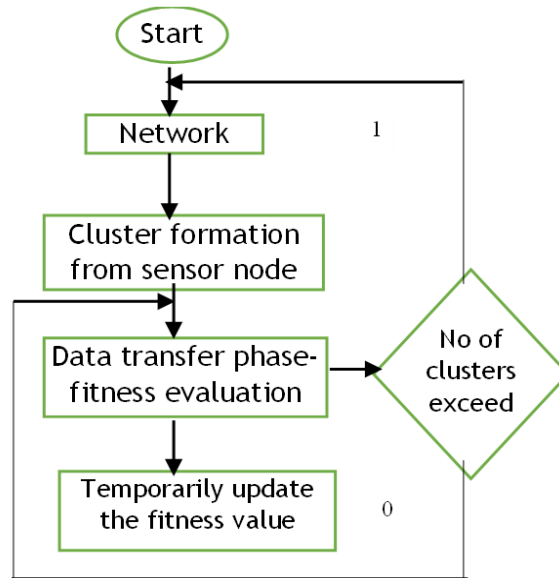


Figure 1. Routing process of cluster in WSNS

In this, the network model is setup with application of WSNs and it forms the clusters based on availability of sensor nodes. Data transformation is performed with active sensor nodes and it selects the cluster randomly for optimization. The fitness value is evaluated by updating position of individual nodes. If it exceeds the cluster counts, the process will be continued and for searching missing nodes and performs the operation.

Extending the network lifetime

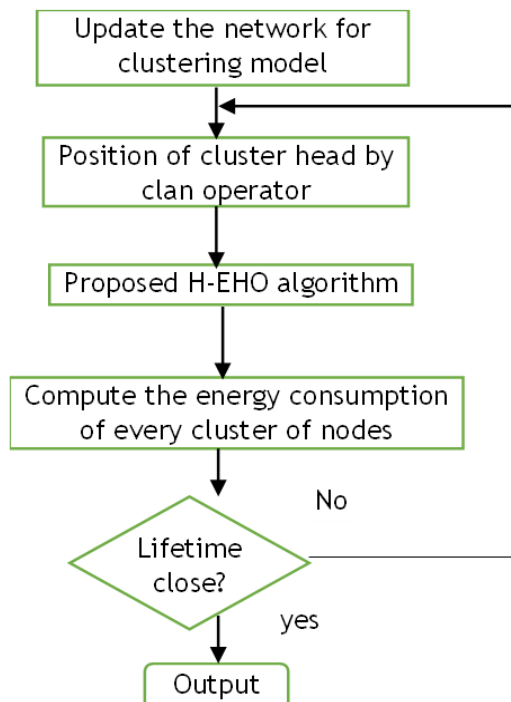


Figure 2. Process flow of network lifetime extension

The main objective of this proposed H-EHO for WSNs are extending network life time and energy efficiency. The objective is achieved by time consumption reduction and effective communication in network model, which improves the overall performance of WSNs communication.⁽¹⁸⁾ Here the threshold based random selection of cluster head selection process improves the result than existing approach. The process flow of network lifetime achievement is given in figure 2. In this, the updating strategy is employed only for updating position of elephant-clan (cluster node) and every time it gives the recent position for getting effective fitness value.

Based on the iteration level and fitness vector, the random value of cluster head is selected. Number of sensor node with its selected iteration is identified to find the maximum population cluster. Therefore, the routing process in WSNs communication using hybrid model of threshold-based elephant herding optimization approach. In this, the network lifetime extension and energy efficient model is designed and obtain the best result than recent related literatures.

Secure data transmission using hybrid secure transmission 19 (hsr 19)

The hybrid secure data transmission 19 with a clustering architecture is presented to secure data transmissions and lengthen the lifespan of WSNs.⁽¹⁹⁾ Sensor nodes are deployed in simulated region during network model’s training processes, and cluster heads are selected based on super ring and residual energies within inter and intra-cluster communication groups. The suggested approach’s main goal is to protect data transmitted between cluster heads and clusters.⁽²⁰⁾

Algorithm 1: hybrid secure data transmission (hsr 19)

- Initialization: Sensor node counts, present remaining energies, distances, and hyperloops
- Step 1: Node (n) deployments
- Step 2: Based on remaining energies (e), choose the cluster heads (ch).
- Step 3: Use a genetic algorithm to link nodes and determine paths between them
- Step 4: Using networks to exchange data
- Step 5: if data transfers occur between cluster heads (ch) then
 - a. Generate shared key values (ki) based on cluster heads (chi, chi+1) where chi+1 equal to routing tables ri, go to step 6.
- Else go to step 8
- Step 6: for each data process execute the functions below until data is encrypted
 - Select data (di) to be transferred for data transmissions
 - Encrypt data using $(E_i)=(k_i * d_i)$ before transfers
 - Send encrypted data to cluster heads (chi+1)
- Step 7: for each encrypted data process execute the function below until complete data is received
 - For each data Received, decrypt using $(D_i)= (E_i * \text{multiplicative inverse of } (k_i))$, goto step 9
- Step 8: Data transmissions within cluster leaf nodes (clfi), generate shared key values (ki) based on cluster heads (clfi, clfi+1) where Clfi+1 equals routing tables ri and neighbour nodes, go to step 6
- Step 9: End

RESULT AND DISCUSSION

The design model of proposed H-EHO is performed the cluster head selection approach. Here the routing process of cluster formation and selection is performed on WSNs.⁽²¹⁾

Table 1. System Parameters for Implementation	
Simulation Parameters	Value used in simulations
Simulation Areas	400*400 Meter
Sensor node Counts	1000
Initial energies of sensor nodes	1joules
Speeds	1-15 meters per second
control packet lengths	50 bytes
Data Packet Lengths	512 bytes
Mobility Model	threshold- random way
Interface queue Types	Drop Tail
Sizes of packets	100 bits
Distances from base stations	50 meters
Locations of base stations	(200,200)
Communicational Model	bidirectional

Benchmark design simulation is compared with other existing approaches like Artificial Bee colony optimization for cluster selection approaches in WSNs and KHA optimized cluster selection approach.

The setup parameter of simulation is implemented with 400*400 meters of area, in this, 2000 sensor node is used and it searches for random selection process. Setup parameter of simulation experiment is tabled for implementation, which is given in table 1. The communication overhead is changed under the network size and the network lifetime extension is the major thing to enhance the performance of WSNs, which utilizes network overhead, size and throughput. E2E delay and network size improve the performance of energy efficient system.⁽²²⁾

The simulation process investigates the benchmark model of existing EEST-OCHS, KHA-OCHS and H-EHO-HSR19 scheme. Here the evaluation process of Proposed H-EHO algorithm is modelled for improving the performance of WSNs communication. Active and inactive sensor node is analysed for getting effective cluster scheme in WSNs.

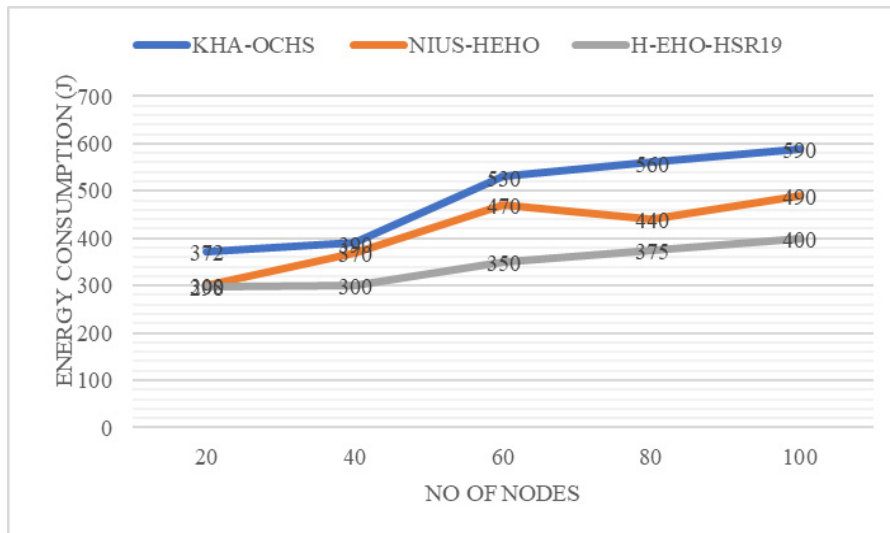


Figure 3. Energy Consumption Results

The energy efficient system is created with proposed approach and it measures the unit of energy (Joules). The energy analysis is given in the energy graph is given in figure 3.

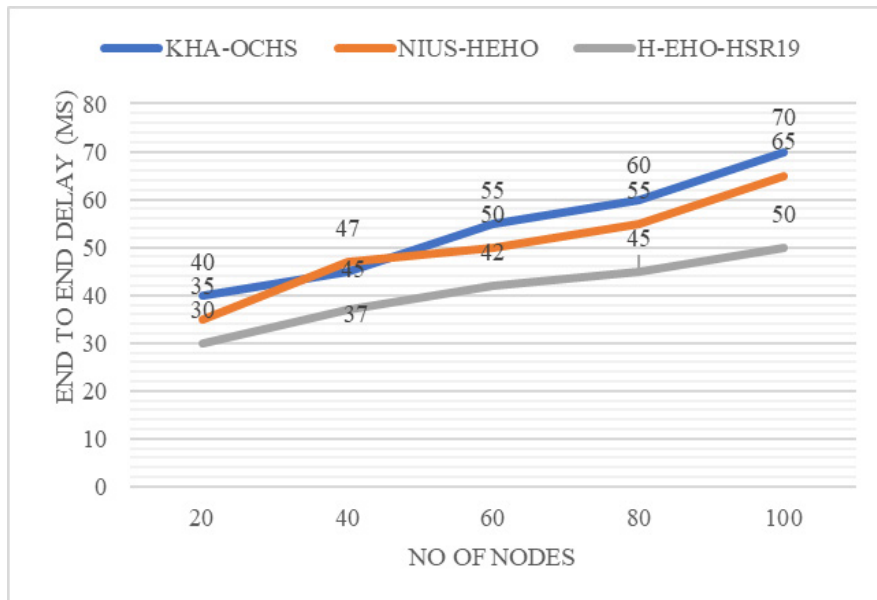


Figure 4. End to End Delay Results

Figure 4 displays E2E latency comparisons for ground routing for KHA-OCHS, NIUS-HEHO, and H-EHO-HSR19 methods. The counts of nodes rise from 20 to 100, and their E2E delay is expressed in milliseconds (ms). The graph shows that routing H-EHO-HSR19 works better than other copies with E2E delay because it is grounded owing to the delay factor when matching the ideal path. the very last. The suggested ways accomplish less than 50 (ms), whereas other approaches achieve, respectively, more than 70 (ms) and 65 (ms).

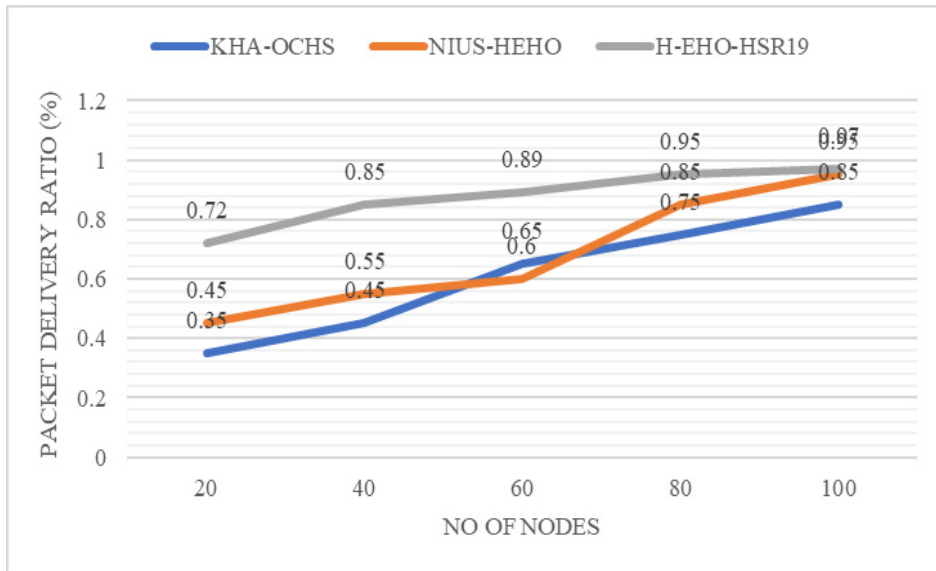


Figure 5. Packet Delivery Ratio Results

Figure 5, compares PDR when KHA-OCHS, NIUS-HEHO, and H-EHO-HSR19 ground routing are taken into account. PDR was intended for a specific number of nodes per second and the number of nodes rose from 20 to 100. The graph makes it evident that the H-EHO-HSR19 ground routing performs better than other clones with outstanding PDRs owing to optimum path categorization. In comparison to the current approach, which achieves 0,85 and 0,95 respectively, the suggested technique obtains 0,97 (%).

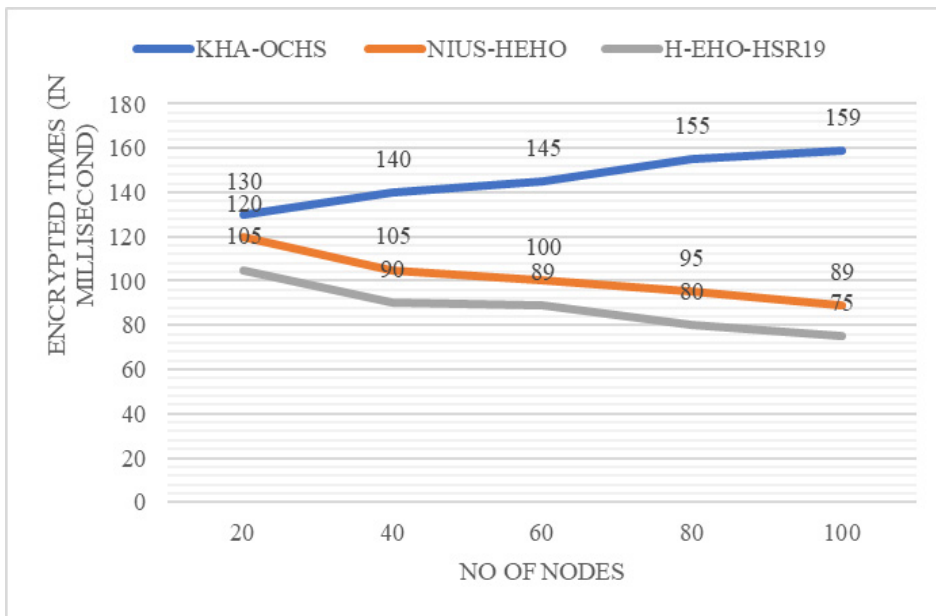


Figure 6. Encrypted Times Result

Figure 6, shows the differences in time utilisation for the ground routing KHA-OCHS, NIUS-HEHO, AND H-EHO-HSR19. For some nodes, this update converts the encoded timing scheme to milliseconds (Ms). The graph shows that ground routing H-EHO-HSR19 performs better than other clones with reduced encoding time consumption owing to remaining time considerations. Compared to the 159 (Ms) and 89 (Ms), respectively, that are achieved by the known techniques and the suggested approach, the latter has a low time consumption of 75 (Ms).

CONCLUSIONS

This study technique integrates meta-heuristic algorithms and proposes H-EHO algorithm for energy efficient cluster head selection in WSNs. Data transmission between intra nodes and the cluster head internodes is handled to transfer data securely, and performance is assessed. It offered a new proposed algorithm to handle the issue, modelling the selection of the cluster head in a WSNs application using a proposed threshold-based Hybrid-Elephant Herding Optimisation algorithm. The cluster head is selected using the clan and separation

operators from the WSNs, and the updating approach makes use of the greatest counts of sensor nodes with the greatest potential based on weight factor. To discover the intra-cluster communication, the cumulative distance between each cluster head is calculated. The optimizer's iterations determine how quickly the best fitness value can be produced. HSR19 is more secure than other methods in securely transmitting data between sensor nodes and consumes less energy. Because the sender and receiver must share the same key for each operation when utilising symmetric keys, creating a safe key is a difficulty. According to experimental findings, this configuration enhances safe data transfer, raises PDRs, lengthens network lifetime, and decreases E2E latency.

BIBLIOGRAPHIC REFERENCES

1. Ismaeel AA, Elshaarawy IA, Houssein EH, Ismail FH, Hassanien AE. Enhanced elephant herding optimization for global optimization. *IEEE Access*. 7, pp. 34738-52. <https://doi.org/10.1109/ACCESS.2019.2904679>
2. Alghamdi TA. Energy efficient protocol in wireless sensor network: optimized cluster head selection model. *Telecommunication Systems*. 74(3), pp. 331-45. <https://doi.org/10.1007/s11235-020-00659-9>
3. Mann PS, Singh S. Artificial bee colony metaheuristic for energy-efficient clustering and routing in wireless sensor networks. *Soft Computing*. 21, pp. 6699-712. <https://doi.org/10.1007/s00500-016-2220-0>
4. Liu Y, Wu Y. Employ DBSCAN and neighbor voting to screen selective forwarding attack under variable environment in event-driven wireless sensor networks, 9, pp. 77090-105. <https://doi.org/10.1109/ACCESS.2021.3083105>
5. Bhat S, Kapoor V. Secure and efficient data privacy, authentication and integrity schemes using hybrid cryptography. In *International Conference on Advanced Computing Networking and Informatics: ICANI-2018*, pp. 279-285. https://doi.org/10.1007/978-981-13-2673-8_30
6. Al-Hyari A, Al-Taharwa I, Al-Ahmad B, Alqadi Z. CASDC: a cryptographically secure data system based on two private key images. *IEEE Access*. 10, pp. 126304-14. <https://doi.org/10.1109/ACCESS.2022.3226319>
7. Thakor VA, Razzaque MA, Khandaker MR. Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. *IEEE Access*. 9, pp. 28177-93. <https://doi.org/10.1109/ACCESS.2021.3052867>
8. Fu X, Fortino G, Pace P, Aloï G, Li W. Environment-fusion multipath routing protocol for wireless sensor networks. *Information Fusion*, 53, pp. 4-19. <https://doi.org/10.1016/j.inffus.2019.06.001>
9. Wang Y, Xue K, Qian C. Evolutionary diversity optimization with clustering-based selection for reinforcement learning. In *International Conference on Learning Representations*. <https://doi.org/10.1016/j.inffus.2019.06.001>
10. Lavanya N, Shankar T. Energy efficient cluster head selection using hybrid squirrel harmony search algorithm in WSN. *International Journal of Advanced Computer Science and Applications*, 10(12), pp. 1-11. <https://doi.org/10.14569/ijacsa.2019.0101265>
11. Govardanagiri R, Sanjeevulu V. Hybrid Grasshopper and Improved Bat Optimization Algorithms-based clustering scheme for maximizing lifetime of Wireless Sensor Networks (WSNs). *International Journal of Intelligent Engineering & Systems*. 15(3), pp. 536-546. <https://doi.org/10.1007/s10586-024-04619-9>
12. Bhandari R, Kirubanand VB. Enhanced encryption technique for secure iot data transmission. *International Journal of Electrical and Computer Engineering*. 9(5), pp. 3732. <https://doi.org/10.11591/ijece.v9i5.pp3732-3738>
13. Alekya Rani Y, Sreenivasa Reddy E. Stability-aware energy efficient clustering protocol in WSN using opposition-based elephant herding optimisation. *Journal of Control and Decision*. 9(2), pp. 202-17. <https://doi.org/10.1080/23307706.2021.1941337>
14. Rami Reddy M, Ravi Chandra ML, Venkatramana P, Dilli R. Energy-efficient cluster head selection in wireless sensor networks using an improved grey wolf optimization algorithm. *Computers*. 12(2), pp. 35. <https://doi.org/10.3390/computers12020035>

15. Veerapaulraj S, Karthikeyan M, Sasipriya S, Shanthi AS. An Optimized Novel Trust-Based Security Mechanism Using Elephant Herd Optimization. *Computer Systems Science & Engineering*. 44(3), pp. 2489-2500. <https://doi.org/10.1109/ACCESS.2024.3374691>
16. Niranjana G, Poongodai A, Soujanya KL. Biological inspired self-organized secure autonomous routing protocol and secured data assured routing in WSN: Hybrid EHO and MBO approach. *International Journal of Communication Systems*. 35(4), pp. 5044. <https://doi.org/10.1002/dac.5044>
17. Arulmurugan A, Waris SF, Bhagyalakshmi N. Analysis of cluster head selection methods in WSN. In 2021 6th International Conference on Inventive Computation Technologies (ICICT), pp. 114-119. <https://doi.org/10.1109/ICICT50816.2021.9358532>
18. Sinda R, Begum F, Njau K, Kaijage S. Refining network lifetime of wireless sensor network using energy-efficient clustering and DRL-based sleep scheduling, 20(5), pp. 1540. <https://doi.org/10.3390/s20051540>
19. Vimala D, Manikandan K. PIRAP: Intelligent Hybrid Approach for Secure Data Transmission in Wireless Sensor Networks. *International Journal of Cooperative Information Systems*, 32(01n02), pp. 2350002. <https://doi.org/10.1142/S0218843023500028>
20. Anita EM, Geetha R, Kannan E. A novel hybrid key management scheme for establishing secure communication in wireless sensor networks. *Wireless Personal Communications*. 82, pp. 1419-33. <https://doi.org/10.1007/s11277-015-2290-9>
21. Paulraj D, Lavanya R, Jayasudha T, Niranjana MI, Daniya T, Shadrach FD. Blockchain-based wireless sensor network security through authentication and cluster head selection. In 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), pp. 1-5. <https://doi.org/10.1109/ICICACS57338.2023.10099593>
22. Vidhya N, Seethalakshmi V, Monisha R, Dhanasekar J, Gurunathan V, Rajanandhini C. Coherent Data Transmission Using Multiplexing for a DWDM Communication System. In 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), pp. 1-4. IEEE. <https://doi.org/10.1109/MysuruCon55714.2022.9972482>

FINANCING

The authors did not receive financing for the development of this research.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Dr. Yuvaraja M.

Data curation: Dr. Rajeshkumar M.

Formal analysis: Dr. Sumathi D.

Research: Dr. Rajeshkumar M.

Methodology: Mohamed Uvaze Ahamed Ayoobkhan.

Drafting - original draft: Dr. Yuvaraja M.

Writing - proofreading and editing: Mohamed Uvaze Ahamed Ayoobkhan.