Salud, Ciencia y Tecnología - Serie de Conferencias. 2024; 3:946
doi: 10.56294/sctconf2024946

Category: STEM (Science, Technology, Engineering and Mathematics)

ORIGINAL

An Energy-Efficient improved Grey Wolf Optimization Algorithm-Based Cluster Head and Shamir Secrets Sharing-Based WSNs with Secure Data Transfer

Un cabezal de clúster basado en el algoritmo de optimización Grey Wolf mejorado y energéticamente eficiente y WSN basadas en el intercambio de secretos de Shamir con transferencia segura de datos

Yuvaraja M[1], Sureshkumar S[2], Joseph James S[3], Teresa V V[4]

[1]Department of ECE, P. A. College of engineering and technology. Pollachi-642001.
[2]Department of Computer Science and Engineering, P. A. College of Engineering and Technology. Pollachi-642001.
[3]Department of Computational Intelligence, SRM Institute of Science and Technology. Chennai, Tamil Nadu.
[4]Department of ECE, Sri Eshwar College of Engineering. Coimbatore-641202.

Cite as: M Y, S S, S JJ, V TV. An Energy-Efficient improved Grey Wolf Optimization Algorithm-Based Cluster Head and Shamir Secrets Sharing-Based WSNs with Secure Data Transfer. Salud, Ciencia y Tecnología - Serie de Conferencias. 2024; 3:946. https://doi.org/10.56294/sctconf2024946

Submitted: 12-02-2024 **Revised:** 03-05-2024 **Accepted:** 28-06-2024 **Published:** 29-06-2024

Editor: Dr. William Castillo-González

ABSTRACT

Introduction: due to its self-configurability, ease of maintenance, and scalability capabilities, WSNs (Wireless Sensor Networks) have intrigued plenty of interest in a variety of fields. To move data within the network, WSNs are set up with more nodes. The security of SNs (sensing nodes), which are vulnerable to malevolent attackers since they are network nodes, is a crucial element of an IoT (Internet of Things)-based WSN. This study's primary objective is to provide safe routing and mutual authentication with IoT-based WSNs.
Method: the basic GWO algorithm's imbalances between explorations and mining, lack of population heterogeneity, and early convergences are all issues that this paper addresses by selecting energy-efficient CHs (cluster Heads) using EECIGWO algorithm, an upgraded version of the GWO, is used. Mean distances within clusters, well-spaced residual energies, and equilibrium of CHs are all factors that influence the choices of CHs. The average intra-cluster distances, sink distances, residual energies, and CHs balances are some of the criteria used to choose CHs.
Results and Discussion: the proposed EECHIGWO-based clustering protocol's average throughput, dead node counts, energy consumption, and operation round counts have all been evaluated. Additionally, mutual authentication between the nodes is provided through SSS (Shamir Secret Sharing) mechanism. PDR (Packet Delivery Ratio) analysis is used to assess how well the EECHIGWO-IOT-WSNs are performing.
Conclusions: the suggested proposed approach is assessed against existing methods like HHH-SS (Hybrid Harris Hawk and Salp Swarm), ESR (Energy-efficient and Secure Routing) protocol, and LWTS (Light Weight Trust Sensing) approaches in terms of AEED (Average End-to-End Delay), network overheads, and PLR (Packet Loss Ratio).

Keywords: Wireless Sensor Network (WSNs); Energy Efficient Cluster Head Improved Grey Wolf Optimization; Shamir Secret Sharing (SSS); Hybrid Harris Hawk and Salp Swarm (HHH-SS); Energy-efficient and Secure Routing (ESR) protocol; Light Weight Trust Sensing (LWTS).

RESUMEN

Introducción: debido a su capacidad de autoconfiguración, facilidad de mantenimiento y capacidades de escalabilidad, las WSN (redes de sensores inalámbricos) han despertado mucho interés en una variedad de campos.

Para mover datos dentro de la red, las WSN se configuran con más nodos. La seguridad de los SN (nodos sensores), que son vulnerables a ataques malévolos ya que son nodos de red, es un elemento crucial de una WSN basada en IoT (Internet de las cosas). El objetivo principal de este estudio es proporcionar enrutamiento seguro y autenticación mutua con WSN basadas en IoT.
Método: los desequilibrios del algoritmo básico GWO entre exploraciones y minería, la falta de heterogeneidad de la población y las convergencias tempranas son cuestiones que este documento aborda mediante la selección de CH (Cabezas de Clúster) energéticamente eficientes utilizando el algoritmo EECIGWO, una versión mejorada del GWO. Las distancias medias dentro de los grupos, las energías residuales bien espaciadas y el equilibrio de los CH son factores que influyen en las elecciones de los CH. Las distancias promedio dentro del grupo, las distancias de sumidero, las energías residuales y los equilibrios de CH son algunos de los criterios utilizados para elegir los CH.
Resultados y Discusión: se han evaluado el rendimiento promedio, el recuento de nodos muertos, el consumo de energía y el recuento de rondas de operación del protocolo de agrupamiento basado en EECHIGWO propuesto. Además, la autenticación mutua entre los nodos se proporciona a través del mecanismo SSS (Shamir Secret Sharing). El análisis PDR (índice de entrega de paquetes) se utiliza para evaluar qué tan bien se están desempeñando los EECHIGWO-IOT-WSN.
Conclusiones: el enfoque propuesto sugerido se evalúa en comparación con métodos existentes como HHH-SS (Hybrid Harris Hawk y Salp Swarm), el protocolo ESR (enrutamiento seguro y eficiente en energía) y los enfoques LWTS (Light Weight Trust Sensing) en términos de AEED (promedio de enrutamiento).Retraso de extremo a extremo), gastos generales de red y PLR (índice de pérdida de paquetes).

Palabras clave: Red de Sensores Inalámbricos (WSN); Optimización del Lobo Gris Mejorada del Cabezal de Clúster con Eficiencia Energética; Shamir Secret Sharing (SSS); Híbrido Harris Hawk y Salp Swarm (HHH-SS); Protocolo de Enrutamiento Seguro y Energéticamente Eficiente (ESR) y Luz; Sensor de Confianza en el Peso (LWTS).

INTRODUCTION

WSNs are a rapidly expanding area of computer science research because they combine sensor, processing, and communication technology.[1] One of the technologies that will develop the fastest in the future is the IoT. IoT enables it for various physical objects to be connected, fundamentally altering how we live.[2] As a result, communication is constantly and urgently required, especially in industries with significant activity. According to connectivity and coverage, each node in the IoT paradigm achieves sensing, monitoring, and processing activities.[3] For instance, sensors put in a home could alert a resident to any security or health threats via their mobile phone.

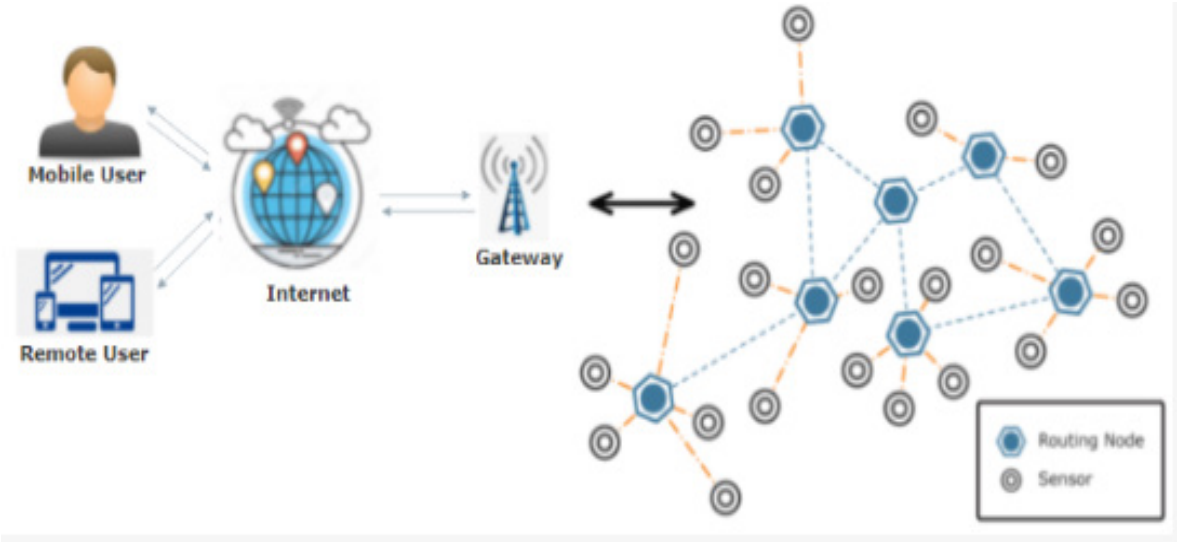

Figure 1. Architecture of WSNs

WSNs are key elements of IoT-enabled smart city applications[4] and are networks made up of several wireless networks connected for creating distributed networks of independent devices.[5] One of the fundamental criteria for WSNs is their security.[6] Confidentiality, integrity, authentication, and data availability are four key

components of WSNs security.[7,8] RSA is an open key calculation that is typically utilised in a variety of corporate and personal communication settings.[9] To partially encrypt secured data, Jang et al.[10] suggested a method. The proposed method addresses the problem of unused memory space by encrypting secured data without increasing the data size. Additionally, a specific segment of encrypted data is identified and decrypted before the entire segment is decrypted, which addresses the issue of circumventing privacy-masking techniques and data encryption.

In existing methods, the authors discussed, the Misra[11] talked on how the Internet of Things is crucial for bridging the gap between the physical and digital worlds. They talked on technological advancements, obstacles, upcoming trends, and Internet of Things (IoT) applications. The method developed by Liu et al.[12] used both "K-means and perceptron" techniques to evaluate the trust values of IoT nodes and to identify distinct malicious nodes. Through the use of the PDE model, the routing network was optimised to increase detection accuracy. In the end, the achieved results showed how effective the developed strategy was at finding the malicious node and getting rid of it. As an outcome, extending the life of the network and ensuring its security requires a secure and energy-efficient routing protocol. Integrity, backward secrecy, forward secrecy, non-repudiation, freshness, and availability must all be taken into account when building a protocol to achieve protected communication via WSNs.

So, utilising the EECHIGWO approach, this research provided a safe clustering and routing with encrypted data transmission. In order to increase energy efficiencies, network stability, average throughputs, and network lives of WSNs, this work suggests using energy-saving EECHIGWO algorithm to choose the most effective CHs. Sink distances, residual energies, equilibrium of CHs, and mean cluster distances are amongst the criteria used to choose CHs. Network packet losses are reduced by selecting CHs and routing paths avoid hostile nodes. SSS approach further ensures mutual authentications of IoT-WSN nodes where simulated findings show that this lowers packet losses, boosts packet delivery speeds, decreases end-to-end latencies, and lowers networks' expenses.

METHOD

The suggested EECHIGWO method is described fully in this part with the goal of extending network lifetime through the use of an ideal selection procedures for CHs.[13] The following assumptions underlie this network architecture, which is primarily intended for industrial applications when a plant's various manufacturing units are dispersed across multiple geographic locations:

1. The SNs are dispersed at random over a two-dimensional geographic area.
2. Communication from CHs to the BS occurs via multiple hops, and BSs are based at network's geographic centers.
3. The SNs are allocated at arbitrary within each group after being separated into roughly equal groups.
4. The SNs in the group are homogeneous and have a 0,2 m/s top speed.
5. The BS will have a constant power supply, as will the nodes involved in multi-path communication only.
6. BS runs the method for choosing a CH and gathers the combined data from all CHs.

The free-space path losses (d2) for single-hop transmissions and multipath propagation faded (d2) channel models are used to illustrate radio power models of SNs in Figure 1 where (d4) used dor multi-hop communications [14]. The energy needed to transport an n-bit packet across a distance "d" is computed using equation 1:

$$E_{TX}(n,d) = \{nE_{elec} + n\, e_{fs} d^2 \quad d < d_0\; nE_{elec} + \; n\, e_{mp}\, d^4 \quad d \geq d_0 \qquad (1)$$

Where:
e_{fs} = coefficient of energy dissipations in free-space attenuation models.
n = Packet Lengths
$e_{mp=}$ coefficient of energy dissipations in multi-path attenuation models.
d = distances between sending and receiving nodes
$d_0 = \sqrt{(ef_s / em_p)}$ = threshold distances
E_{elect} = energies consumed in transmissions/ receipt of 1-bit data.

https://doi.org/10.56294/sctconf2024946

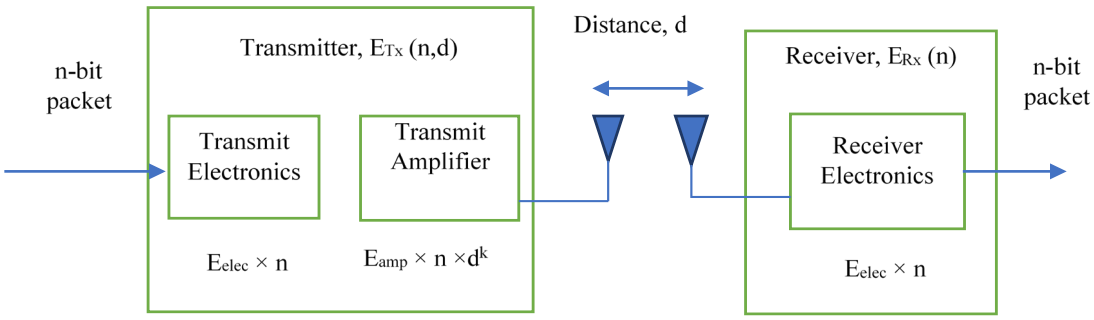

Figure 2. Radio Energy Model of a Sensor Node

At R_x, energies consumed during receipt of n-bit data packets can be calculated using equation 2:

$$E_{RX}(n) = n \times E_{elec} \quad (2)$$

Three factors affect how much energy is used by CHs: the quantity of data packets broadcast from the CH to the BS in aggregate form, the quantity of data aggregation carried out by CHs, and the quantity of data packets received from SNs that make up specific bursts[15]. Equation 3 just illustrates energy usage.

$$E_{CH} = E_{RX}(n,d) \times SN_{num} + E_{DF} \times n \times (SN_{num} + 1) + E_{TX}(n,d) \quad (3)$$

SNnum = SN's number in clusters, E_{DF} = data fusion energy/bit.
Energies consumed by SNs except CHs can be represented as $E_{TX}(n,d)$.
Remaining energies during kth rounds are computed using equation 4:

$$E_R(K) = E_R(k-1) - \left(\sum_{l=1}^{CH_{num}(l)} E_{CH}(l) + \sum_{m=1}^{SN_{alive}(k)-CH_{num}(k)} E_{SN}(m)\right) \quad (4)$$

E_R(K-1) =Total balance energies at (k-1) th rounds
CH_{num}(k) = counts of CHs in Kth rounds
SN_{alive}(k) = counts of alive nodes in Kth rounds
E_{CH}(l)= energies consumed by Ith CHs
E_{CH}(m)= energy consumed by mth SNs

Cluster selections using the proposed EECHIGWO algorithm

The suggested EECHIGWO algorithm is used by BS to perform CH selection to avoid randomness. Using the multi-hop communication nodes, the selected CHs' data is disseminated to all SNs. According to the fitness value, the entire counts of SNs is separated into four subsets, sixteen of which are designated as fixed in order to allow multi-hop pathways. Grey wolves are thought of as the SNs, while CHs are preys. The rounds of EECHIGWO includes stages for generation of CHs and data transmissions. Fitness values of SNs are computed from residual energies and distances from BS.

$$F = \{0.8 \times \left(\frac{E_{residual}}{E_{initial}}\right) + 0.2 \times \left(\frac{d_{max}-d}{d_{max}-d_{min}}\right), E_{residual} < 0\ 0.2 \times \left(\frac{E_{residual}}{E_{initial}}\right) + 0.8 \times \left(\frac{d_{max}-d}{d_{max}-d_{min}}\right), E_{residual} \geq d_0 \quad (5)$$

Where:
$E_{initial}$ = initial energies of SNs
$E_{residual}$= residual energies of SNs during rounds
d= distances between SNs and BS
d_{max}= max. distances between SNs and BS,
d_{min} = min. distances between SNs and BS.

Fitness functions represented by equation 5 includes residual energies of SN (80 % weights) and distances between SNs and BS (20 % weights). Equation 6 is used for calculating BS's initial position.

$$X_{CH} \rightarrow = \left|\omega_\alpha X_\alpha \rightarrow + \omega_\beta X_\beta \rightarrow + \omega_\delta X_\alpha \rightarrow\right| \quad (6)$$

https://doi.org/10.56294/sctconf2024946

Where ω_α, ω_β, ω_δ are initial weights as per equation 7:

$$\omega_\alpha = \frac{F_\alpha}{F_\alpha+F_\beta+F_\delta}, \omega_\beta = \frac{F_\beta}{F_\alpha+F_\beta+F_\delta}, \omega_\delta = \frac{F_\delta}{F_\alpha+F_\beta+F_\delta} \quad (7)$$

F_α, F_β, F_δ are top three optimal fitness of SNs.

The weights ω_α, ω_β, ω_δ are dynamically changed utilizing the vectors $D\rightarrow$, $A\rightarrow$ to improve the capabilities of global search utilizing the GWO methodand at ith iterations, weights are estimated using equations 8-10:

$$\omega_\alpha^{i+1} = \frac{D_\alpha^{i+1\rightarrow} \times A_\alpha^{i+1\rightarrow}}{D_\alpha^{i+1\rightarrow} \times A_\alpha^{i+1\rightarrow} + D_\beta^{i+1\rightarrow} \times A_\beta^{i+1\rightarrow} + D_\delta^{i+1\rightarrow} \times A_\delta^{i+1\rightarrow}} \quad (8)$$

$$\omega_\beta^{i+1} = \frac{D_\beta^{i+1\rightarrow} \times A_\beta^{i+1\rightarrow}}{D_\alpha^{i+1\rightarrow} \times A_\alpha^{i+1\rightarrow} + D_\beta^{i+1\rightarrow} \times A_\beta^{i+1\rightarrow} + D_\delta^{i+1\rightarrow} \times A_\delta^{i+1\rightarrow}} \quad (9)$$

$$\omega_\delta^{i+1} = \frac{D_\delta^{i+1\rightarrow} \times A_\delta^{i+1\rightarrow}}{D_\alpha^{i+1\rightarrow} \times A_\alpha^{i+1\rightarrow} + D_\beta^{i+1\rightarrow} \times A_\beta^{i+1\rightarrow} + D_\delta^{i+1\rightarrow} \times A_\delta^{i+1\rightarrow}} \quad (10)$$

Utilizing α, ß, ω wolves, the CH's location is calculated during selections of CHs. As seen in figure 2, the other SNs determine their separation from the BS. The adjusted location of the SN in the titration (i + 1) is determined using equation 11.

$$X^{1+1\rightarrow} = X_{CH}^{i\rightarrow} - \square\rightarrow \times \square\rightarrow \quad (11)$$

Where stands for convergence vectors and given by $A\rightarrow=2\ \alpha\rightarrow \times r1\rightarrow - \alpha\rightarrow$, $X_{CH}^{(i\rightarrow)}$ is the CH position in the previous iteration, i.e., ith iteration.

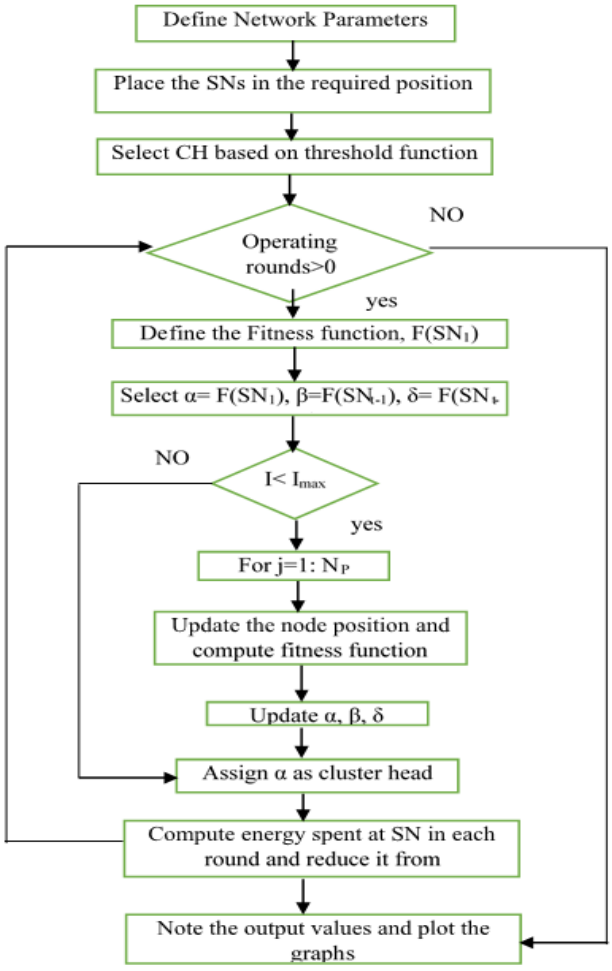

Figure 3. Flow diagram of the proposed eechigwo algorithm

https://doi.org/10.56294/sctconf2024946

Shamir's secret sharing method (sss)

Utilizing a (t,n) threshold depending on SSS method, BSs produce secret keys S for distributions amongst n CHs, where subsets of CHs are sufficient to regenerate secret keys S. To qualify for the SSS technique, the following two conditions need be provided.[16]

The secret key S recreate utilizing any collection of t or more subkeys $S0$, $S1$, …, $St-1$.

It is impossible to recreate the secret key S with t or less subkeys.

Polynomials of t-1 degrees are formed in SSS for t subkeys. T-1 random values (b1, b2,.bt-1) > 0 are selected to generate (t,n) threshold schemes. When b0=S, coefficients of polynomials are (b1, b2, bt-1) and depicted in equation 12.

$$f(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \ldots\ldots + b_tx^{t-1} \qquad (12)$$

LaGrange bases polynomiale[17] need to be computed for recreating secret keyss S as per equation 13.

$$l_j(X) = \prod_{0\le m\le t\ m\ne j} \frac{x-x_m}{x_j-x_m} \qquad (13)$$

Once t − 1 LaGrange values are computed calculated, secret keys S are calculated using equation 14.

$$f(X) = \sum_{j=0}^{t-1} y_i l_j(x) \quad (14)$$

A portion of the key S_i which is distributed to each CHs, is then flooded to a single cluster node.

RESULTS AND DISCUSSION

The EECHIGWO-IoT-WSNs technique's performance is evaluated using the NS2 simulation tool. Only authenticated nodes are permitted to transmit data using the EECHIGWO-IoT-WSNs technique. There, counts of SNs are changed from 100 to 400 in sitmulations. The network's nodes are dispersed at arbitrary between 100m × 100m, and they all adhere to the EECHIGWO-based routing system. Table 1 lists the simulation parameters assessed for this EECHIGWO-IoT-WSNs technique.

Table 1. Simulation parameters

Parameters	Values
Counts of nodes	100,200,300&400
Areas	100 ×100 m2
Initial energies	5J
Packet sizes	512 bytes
Antenna models	Omnidirectional
Network interface types	Phy /wireless Phy
Propagating Models	two ray ground
traffic types	CBR/UDP
MAC Protocols	IEEE 802,11
Routing Protocols	EECHIGWO
Simulation times	2000s

The PDR, PLR, AEED, and network overhead measures are used to evaluate the efficiency of the EECHIGWO - IoT-WSNs approach. Here, the ESR protocol,[18] HHH-SS[19] and LWTS[20,21,22] are utilized to assess the suggested EECHIGWO -IoT-WSNs technique and demonstrate its effectiveness. In that, the parameters accessible for the evaluation itself are used to compare the current techniques, such as ESR, HHH-SS, and LWTS.

PDR

PDRs are ratios amongst created packet volumes and those received at sources shown in table 2 and expressed as equation 15.

https://doi.org/10.56294/sctconf2024946

$$PDR = \frac{Amount\ of\ received\ packets}{Amount\ of\ generated\ packets} \times 100 \quad (15)$$

PLR

PLR determines the amount of packets lost during the communication phase, as illustrated in table 3. Equation 16 illustrates how PLR is defined as the ratio of the number of packets discarded to the number of created packets.

$$PLR = \frac{Amount\ of\ dropped\ packets}{Ampunt\ of\ generated\ packets} \times 100 \qquad (16)$$

AEED

AEED needed for packets to be transferred from source to endpoint is given by equation 17. The processing time, transmission delay, and transmission time are all included in the AEED that is displayed in table 4.

$$AEED = \frac{sum\ of\ all\ packets\ delay}{total\ amount\ of\ received\ packets} \quad (17)$$

Network overhead

The average counts of control packets generated by each node during communication is referred to as network overhead.

Table 2. Performance analysis of PDR

No. of Nodes	ESR	HHH-SS	LWTS	EECHIGWO
100	93	80	92	97,82
200	90	75	89	97,62
300	85	73	75	97,78
400	83	69	73	97,45

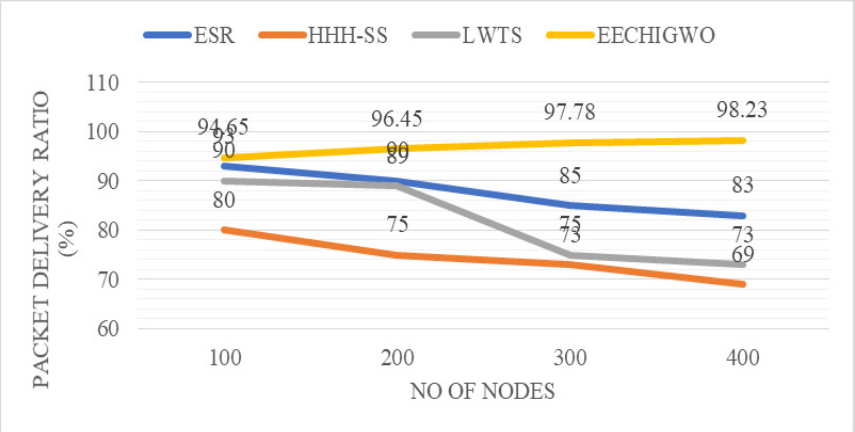

Figure 4. Comparison of PDR

Table 3. Comparison of PLR

No of Nodes	ESR	HHH-SS	LWTS	EECHIGWO
100	5	7	8	0,1519
200	10	19	15	0,3558
300	15	27	29	0,3817
400	17	35	40	2,6018

https://doi.org/10.56294/sctconf2024946

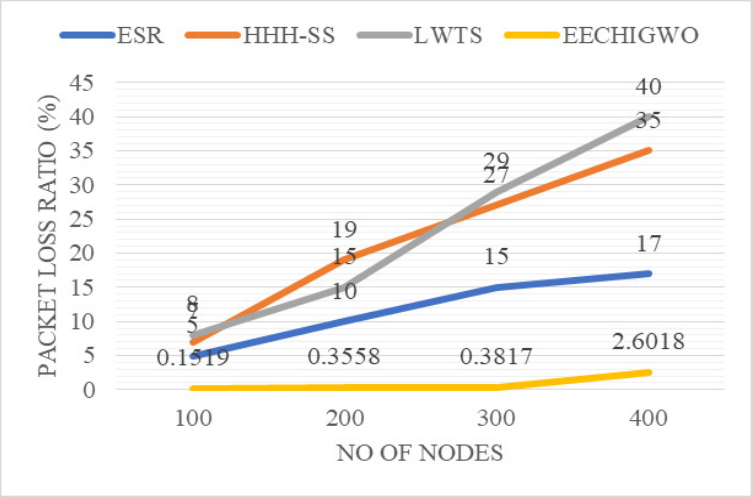

Figure 5. Comparison of PLR

Table 4. Comparison of AEER

No of Nodes	ESR	EECHIGWO
100	0,0175	0,000417088
200	0,02	0,00484892
300	0,024	0,000483543
400	0,0275	0,00217974

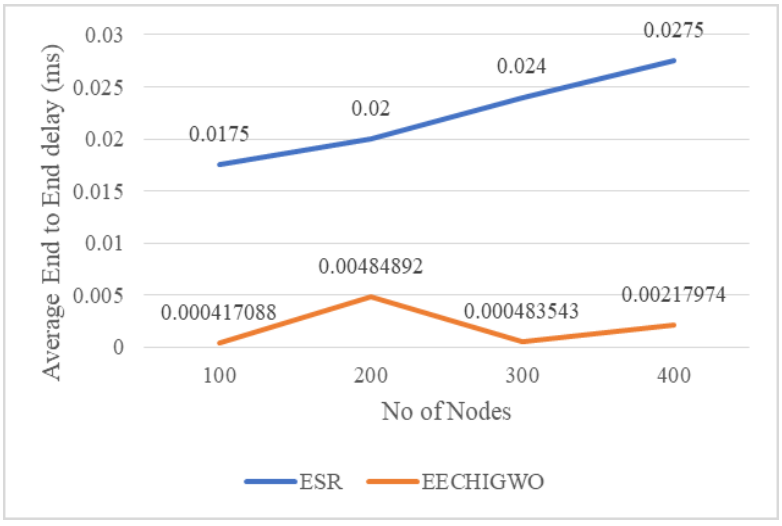

Figure 6. Comparison of Average End to End Delay

CONCLUSIONS

In this study, secure CHs and data transmission paths in IoT-based WSNs are selected using IGWO approach. Selections of CHs and generation of routing paths by IGWO avoids hostile nodes by taking into account the trust value. The CH choices are utilised to boost the IoT-based WSNs's performance. The suggested method additionally specifies a secure channel for data packet transmission from the source CH to the BS. In an IoT-based WSN, mutual authentication between nodes is accomplished via the SSS approach. Therefore, by employing this IGWO-IoT-WSNs approach, secure data transmission is achieved. The outcomes demonstrate that the IGW-SSS we've suggested offers superior PDR, PLR, and AEER results. We can draw the conclusion that by introducing both SSS approaches and the IGWO algorithm, the network's overall performance improved and remained stable when compared to the earlier study. However, the simulation's high rate of retransmitted packets causes a high level of routing overhead, which causes extra delay and loss. Therefore, by focusing on efficiency and delay during the emergency condition in WSNs, this research can be continued in the future.

https://doi.org/10.56294/sctconf2024946

BIBLIOGRAPHIC REFERENCES

1. Zhou W. Research on wireless sensor network access control and load balancing in the industrial digital twin scenario. Journal of Sensors, pp. 1-12. https://doi.org/10.1155/2022/3929958.

2. Gulati K, Boddu RSK, Kapila D, Bangare SL, Chandnani N, and Saravanan G. A review paper on wireless sensor network techniques in Internet of Things (IoT). Materials Today: Proceedings, 51, pp. 161-165. https://doi.org/10.1016/j.matpr.2021.05.067.

3. Lin JW, Chelliah PR, Hsu MC, and Hou JX. Efficient fault-tolerant routing in IoT wireless sensor networks based on bipartite-flow graph modeling. IEEE access, 7, pp. 14022-14034. https://doi.org/10.1007/s11277-022-09580-7.

4. Preeth SSL, Dhanalakshmi R, Kumar R, and Shakeel PM. An adaptive fuzzy rule based energy efficient clustering and immune-inspired routing protocol for WSN-assisted IoT system. Journal of Ambient Intelligence and Humanized Computing, pp. 1-13. https://doi.org/10.1007/s12652-018-1154-z.

5. Lyu C, Zhang X, Liu Z, and Chi CH. Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks. IEEE Access, 7, pp. 31068-31082. https://doi.org/10.1109/ACCESS.2019.2902843.

6. Nayyar A, and Singh R. IEEMARP-a novel energy efficient multipath routing protocol based on ant Colony optimization (ACO) for dynamic sensor networks. Multimedia Tools and Applications, 79(47), pp. 35221-35252. https://doi.org/10.1007/s11042-019-7627-z.

7. Babaeer HA, and Al-Ahmadi SA. Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking. IEEE Access, 8, pp. 92098-92109. https://doi.org/10.1109/ACCESS.2020.2994587.

8. Biradar DN, and Vishanath TS. Secured Data Transmission and Malicious Node Detection in Wireless Sensor Network. International Journal of Engineering and Advanced Technology, 8(6), pp. 1062-1069.

9. Kang MS. Design of AES-based encryption chip for IoT security. The Journal of the Institute of Internet, Broadcasting and Communication, 21(1), pp. 1-6. https://doi.org/10.7236/JIIBC.2021.21.1.1.

10. Jang W, and Lee SY. Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment. International Journal of Distributed Sensor Networks, 16(3), pp. 1-17. https://doi.org/10.1177/1550147720914779.

11. Misra G, Kumar V, Agarwal A, and Agarwal K. Internet of things (iot)–a technological analysis and survey on vision, concepts, challenges, innovation directions, technologies, and applications (an upcoming or future generation computer communication system technology). American Journal of Electrical and Electronic Engineering, 4(1), pp. 23-32. https://pubs.sciepub.com/ajeee/4/1/4/index.html#:~:text=doi%3A%2010.12691/ajeee%2D4%2D1%2D4.

12. Liu L, Ma Z, and Meng W. Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks. Future generation computer systems, 101, pp. 865-879. https://doi.org/10.1016/j.future.2019.07.021.

13. Rami Reddy M, Ravi Chandra ML, Venkatramana P, and Dilli R. Energy-efficient cluster head selection in wireless sensor networks using an improved grey wolf optimization algorithm. Computers, 12(2), pp. 1-17. https://doi.org/10.3390/computers12020035.

14. Das I, Shaw RN, and Das S. Analysis of energy consumption of energy models in wireless sensor networks. In Innovations in Electrical and Electronic Engineering: Proceedings of ICEEE 2020, pp. 755-764. https://doi.org/10.1007/978-981-15-4692-1_57.

15. Ali H, Tariq UU, Hussain M, Lu L, Panneerselvam J, and Zhai X. ARSH-FATI: A novel metaheuristic for cluster head selection in wireless sensor networks. IEEE Systems Journal, 15(2), pp. 2386-2397. https://doi.org/10.1109/JSYST.2020.2986811.

16. VenkataRao S, and Ananth V. A Hybrid Optimization Algorithm and Shamir Secret Sharing Based Secure Data Transmission for IoT based WSN. International Journal of Intelligent Engineering & Systems, 14(6), pp. 498-506. http://dx.doi.org/10.22266/ijies2023.1231.44.

17. Essanhaji A, and Errachid M. Lagrange multivariate polynomial interpolation: a random algorithmic approach. Journal of Applied Mathematics, pp. 1-8. https://doi.org/10.1155/2022/8227086.

18. Haseeb K, Almogren A, Islam N, Ud Din I, and Jan Z. An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN. Energies, 12(21), pp. 1-18. https://doi.org/10.3390/en12214174.

19. Srinivas M, and Amgoth T. EE-hHHSS: Energy-efficient wireless sensor network with mobile sink strategy using hybrid Harris hawk-salp swarm optimization algorithm. International Journal of Communication Systems, 33(16), pp. e4569. https://doi.org/10.1002/dac.4569.

20. Rajendra Prasad M, and Krishna Reddy D. LWTSM-IoT: Light Weight Trust Sensing Mechanism for Internet of Things. International Journal of Intelligent Engineering & Systems, 14(1), pp. 82-92. https://inass.org/wp-content/uploads/2022/09/2023022809-2.pdf.

21. Paulraj D, Lavanya R, Jayasudha T, Niranjana MI, Daniya T, and Shadrach FD. Blockchain-based Wireless Sensor Network Security Through Authentication and Cluster Head Selection. In 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, and Rajanandhini C. Coherent Data Transmission Using Multiplexing for a DWDM Communication System. In IEEE 2nd Mysore Sub Section International Conference (MysuruCon), pp. 1-4. 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: Yuvaraja M.
Data curation: Sureshkumar S.
Formal analysis: Joseph James S.
Research: Teresa V V.
Methodology: Sureshkumar S.
Drafting - original draft: Teresa V V.
Writing - proofreading and editing: Yuvaraja M.