International Academic Institute for Science and Technology

International Academic Journal of Innovative Research
Vol.10, No.2, 2023, pp. 1-9.

ISSN 2454-390X

International Academic Journal of Innovative Research

www.iaiest.com

Cluster Head Selection and Secured Routing Using Glowworm Swarm Algorithm and Hybrid Security Algorithm for Over IoT-WSNs

M. Prakash [a*], Dr. A. Prakash [b]

[a] Research Scholar, Department of Computer Science, Hindusthan College of Arts &Science, Coimbatore. E-mail: guru8026@gmail.com*
[b] Professor, Department of Computer Applications (PG), Hindusthan College of Arts &Science, Coimbatore. E-mail: prakashankar75@gmail.com

Abstract

WSNs (Wireless Sensor Networks) have received a lot of attention in a number of industries due to its self-configurability, simplicity in maintenance, and scaling capacities. WSN is configured with extra nodes in order to transport data around the network. The usual characteristics of sensor networks are low bandwidth, low energy, constrained power supply, and little memory space, which makes security particularly difficult in these networks. CH (Cluster heads) in a cluster experience heavier traffic loads than other cluster nodes. This results in the hotspot problems. Therefore, in a cluster-oriented routing scheme, picking the right CH is crucial. The two-level security is recommended in this research to safeguard data transmission via the WSN. A novel CH selection methodology is presented in order to increase the network's lifespan and energy effectiveness. This work also combines the fruit fly algorithm (FGF) with the GSA (firefly swarm algorithm) based on fitness to choose the optimal CH. To defend the network from assaults, it employs a hybrid security method that combines the Diffie-Hellman key exchange mechanism and the ECC (elliptic curve cryptography) algorithm. The suggested GSA-HSA protocol consistently produces good performance results in terms of MSR (Message Success Rate), E2E (End-to-End) Latency, NT (Network Throughput), and network throughput. average AEE (energy efficiency). The suggested approach outperforms all prior research by giving the wireless sensor network combination security, optimised coverage, and energy savings.

Keywords: Wireless Sensor Network (WSN), Cluster Head (CH), Secured Routing (SR), Glow-Worm Swarm Algorithm (GSA), Fruit Fly Algorithm (FFA), Hybrid Security Algorithm (HSA), Diffie-Hellman Key, Elliptic- curve Cryptography (ECC).

DOI: 10.71086/IAJIR/V10I2/IAJIR1004
Received: 20 March 2023/Revised: 06 April 2023/Accepted: 15 May 2023/Published: 30 June 2023

Introduction

WSNs have received a lot of interest recently because to their potential and diverse range of applications, which include combat monitoring, security, carpet management, and physical and ecological observation. catastrophe [1]. The fundamental issue is that supporting nodes could or might not be trusted, which raises vulnerability to numerous attacks that have a big impact on data security [2].

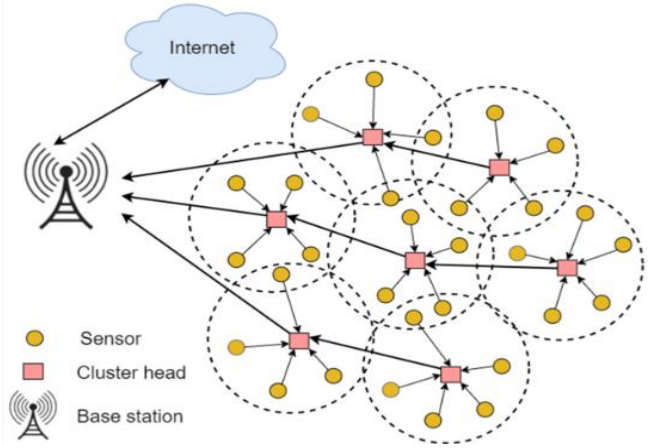


Fig. 1: Clustering Architecture in A WSN

Figure 1 depicts the WSN clustering architecture. For greater lifespan, dependability, and appropriate network path selection [3] as well as connection security, efficient routing protocol implementation is of utmost importance. Security concerns like espionage are greatly facilitated by wireless communications. Malicious communications can be sent out fast by a network attacker [4]. Implementations of security, firefly, PSO (bee colony optimisation), ABC (artificial bee colony), GA (genetic algorithm), PSO (bee colony optimisation), and PSO (bee colony optimisation) are similar to some of the most popular metadiagnostics in [5]–[7]. method employed to get the optimum response.

The Glow-worm Swarm method is used in this work to build a combined security mechanism in the cluster head and safe routing. The following are the main findings of our study. In order to increase the network's QoS (quality of service), the proposed system i) suggests a model that is energy-efficient; ii) uses hybrid security, which combines the Diffie-Hellman key exchange mechanism and the elliptic curve cryptographic algorithm, in our proposed model to address attack problems; and iii) incorporates the GSA's cluster lead selection. iv) To increase network service quality, the suggested solution has better network security routing, and v) the proposed work is carried out using NS2 software. To assess our protocol's effectiveness in terms of safety and optimisation, we constructed this simulated scenario.

Related Works

Clustering is one of the WSNs' most debated fields. This work aims to effectively maintain power dissipation of sensor nodes which influence their communication within clusters using cluster-based routing and implementing data collections and fusions to reduce the amount of information forwarded to base stations and transmission ranges of nodes.

The author discussed the cluster-based protocols LEACH [8] and LEACH-C [9], where the sink randomly chooses CHs. The LEACH algorithm's selection of CH is random, and the cluster's sensor nodes alternately perform the CH's duties. Therefore, selecting a sensor as a CH with insufficient power can cause the network's lifetime to shorten quickly while in LEACH-C, the sink uses a simulated annealing technique to find the best solution with fewer spots where energy is lost from the cluster heads.

Though multiple authentication techniques have been offered, they do not solve all known security flaws. If the broadcaster intends to keep the predicted lifetime with a guaranteed level of service, the nodes' energy must be utilised effectively [10]. Here, the HABC-MBOA (Hybrid Artificial Bee and Monarch Butterfly Colony Optimisation Algorithm) is suggested to choose the majority of CH [11] [12]. Other effective path selection techniques include PSO [13], Adaptive QOBOA (Nearly Opposite Butterfly Optimisation Algorithm) [14], ACO [15], BOA (Butterfly Optimisation Algorithm) [16], and GWO (Grey Wolf Optimisation) [17]. have been applied in earlier research. Several assessment studies examine security services such as availability, availability, secrecy, and authentication.

Proposed Methodology

In this work, GSA-HS algorithm is proposed to improve the CH node selection and safe IoT-based WSN routing. The system model, CH node selection using the GSA method, routing, and safe data transmission using the hybrid security algorithm are the primary contributions of this work. The suggested system's overall block diagram is displayed in Figure 2.

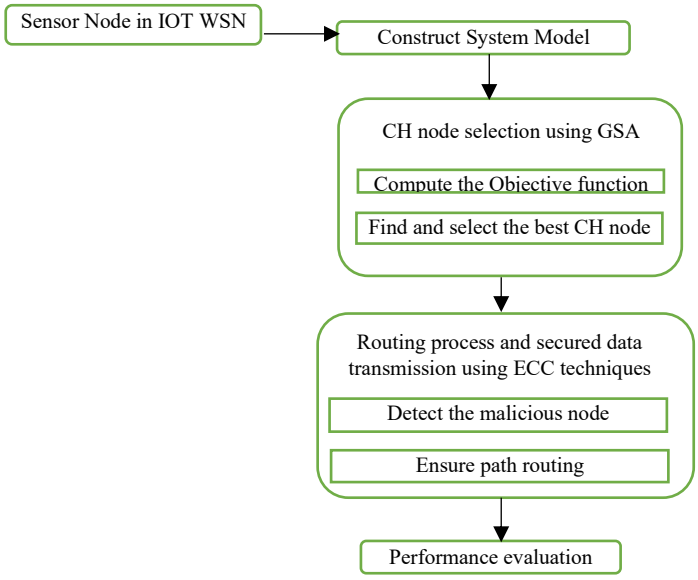


Fig. 2: Overall Block Diagram of the Proposed System

Optimal Selection of CH in WSNs

Assuming WSNs have n^c clusters, where cl_i, $(i = 1, \dots \dots \dots \dots n^c)$ is used to denote clusters. B_{ij} stands for the cluster's nodes, where $i = 1,2, \dots . . M \; and \; j = 1,2, \dots \dots . L$.. The head node, designated as CH_1, is chosen from among the cluster's nodes and serves as the group's coordinator. CH and BS D_s have direct communication. Additionally, a unique hybrid method is applied to select the best CH while accounting for restrictions like energy, distance, and latency.

Evaluation of Appropriate Functions

Constraints like energy, distance, and hysteresis must be taken into account for the best CH selection. Furthermore, a significant component of network performance in this work is QoS limitation. The goal of this effort is illustrated by equation (1), where is a constant with the value 0.3. In Eq. (2),$\gamma^1\gamma^2\gamma^3$ refers to distance constraints, energies and delays respectively and $||Br - Ds||$ in Eq. (3) stands for distances amongst nodes and BS.

$$OF = \beta \times f^2 + (1-\beta)f^1; 0 < \beta < 1 \quad (1)$$

$$f^1 = \gamma^1 * f_i^{dist} + \gamma^2 * f_i^{energy} + \gamma^3 * f_i^{delay} \quad (2)$$

$$f^2 = \frac{1}{n^C}\sum_{r=1}^{n^C} \|B_r - D_s\| \quad (3)$$

Parameters Considered for Selecting Optimal CHs

The following parameters are quantitatively modelled for the purposes of this work:

Energy: The required energies can be determined using Eq. (4), where $E(B_i)$ and $E(CH_j)$ refer to the energy of i^{th} normal nodes and energies of j^{th} CH, in that order.

$$f^{energy} = \frac{f^{energy}(q)}{f^{energy}(p)} \quad (4)$$

$$f^{energy}(q) = \sum_{j=1}^{M} uE(j) \quad (5)$$

$$uE(j) = \sum_{\substack{i=1 \\ i \epsilon j}}^{M} \left(1 - E(B_i) * E\left(CH_j\right)\right); 1 \leq j < L \quad (6)$$

$$f^{energy}(u) = L * MAX_{i=1}^{M}\left(E(B_i)\right) * MAx_{j=1}^{L}\left(E\left(CH_j\right)\right) \quad (7)$$

Distances : Distances are calculated using Eq. (8), where $f^{dist}(q)$ stands for distances amongst nodes and CHs and between CHs and BSs based on Eq. (9) and$f^{dist}(p)$ represents distances between normal nodes as per Eq. (10) with values if $f^{distance}(q)$in the range [0,1].

$$f^{dist} = \frac{f^{dist}(q)}{f^{dist}(p)} \quad (8)$$

$$f^{dist}(q) = \sum_{i=1}^{M}\sum_{j=1}^{L}\left\|B_i - CH_j\right\| + \left\|CH_j - D_s\right\| \quad (9)$$

$$f^{dist}(p) = \sum_{i=1}^{M}\sum_{j=1}^{L}\left\|B_i - B_j\right\| \quad (10)$$

Delay: Equation (11) depicts the latency between the nodes, which is between [0, 1], reducing node density in cluster results i. In equation (11), "CH_j" stands for the WSN's CH, and "M" stands for all nodes combined.

$$f^{delay} = \frac{Max_{j=1}^{L}\left(CH_j\right)}{M} \quad (11)$$

QoS: This parameter encompasses constraints which need to be compulsorily satisfied.

Solution Encodes

This work uses FGF algorithm for selecting optimal CHs (Refer Fig 1), where CH_n imply counts of CHs represented in Figure 3.

Fig. 3: Solution Encoding

Algorithm FGF

The FFOA and GSO algorithms are combined to create the FGF algorithm. In actuality, search issues may be resolved via associative optimisation [20]. The relevance evaluation is carried out initially, then the relevance is ranked, in accordance with the FGF algorithm [21]. Pick the top five items after sorting (using metrics). If the index is below 5, the GSO update will be run. The luminous chemical "luciferin" is expressed in minute levels by fireflies in GSO. They also decide on their own what to do in the choice area. in $G_e^g\left(0 < G_e^g \leq G_u\right)$ with g glow-worms, and with w neighbours.

Initializations: The distribution of the firefly throughout the search area is random. Therefore, the glowworm was made up of similar luciferin intensities and G0 decision domains.

Luciferin-update

Generally, physical states directly impact luciferin intensities. Best positions can be attained if intensity values are higher. $Z_g(t)$ stands for glow-worm positions at t times and $J\left(Z_g(t)\right)$ implies related objective values of gthglow-worm positions at t. Further, converting $J\left(Z_g(t)\right)$ to $U_g(t)$, represents luciferin levels associated to g glow-worms at times t and depicted in Eq. (12), wherein υ refers to luciferin decay constants, η implies constant variables.

$$U_g(t) = (1 - \upsilon)U_g(t-1) + \eta\left(J\left(Z_g(t)\right)\right) \quad (12)$$

Movements: g glow-worm move towards w neighbors in this phase, initiated from $H_g(t)$ with committed probabilities $P_{gj}(t)$, and modelled in Eq. (13).

$$P_{gj}(t) = \frac{U_w(t) - U_g(t)}{\sum_{l \epsilon Y_{g(ti)}} U_l(t) - U_g(t)} \quad (13)$$

As glowing worms g move, their positions are updated and evaluations of positional updates occur as per equation. (14), where sizes represent step sizes.

$$Z_g(t+1) = Z_i(t) + size * \left[\frac{Z_w(t) - Z_g(t)}{\|Z_w(t) - Z_g(t)\|}\right] \quad (14)$$

If the index is greater than 5 then the update of FFOA is performed as indicated in the equation. (15) and (16). Fruit flies are randomly distributed according to the FFOA model where Z_{axis} and W_{axis} and index ^{best} point out higher components with their respective indices.

$$Z_{axis} = Z(index^{best}) \quad (15)$$
$$W_{axis} = W(index^{best}) \quad (16)$$

Hybrid Security Algorithm for Transfer Data in Node

Encryption

The input data will be changed into codes during the encryption process for increased security. The Diffie-Hellman Key Exchange Algorithm and ECC may now be used for encryption and is described in the following manner: In order to create public keys, non-ECC cryptographic keys that are at least as safe as ECC cryptographic keys are added to finite field-oriented algebraic expressions. The encrypted versions of the private and public keys are therefore available. The following is the general equation for the ellipse curve. It is a method for limiting unauthorised access that transforms data into code. Currently, data encryption is possible by combining the Diffie-Hellman and ECC key exchange methods. The step-by-step method of this hybrid system is the next in the equation. (17):

$$Y^2 = X^3 + AX + B(mod\ C) \quad (17)$$

where, A, B, and C indicate random integers in the interval [0,-1]. By lowering numbers specified, values of Y become convertible, allowing identification of odd points. As indicated in the equation (18), private and public keys can be selected from unequal points

$$Pub(key) = Pri(key) \times c \quad (18)$$

In this case, the public key note is denoted by Pub(key), while the private key is denoted by Pri(key). These keys are used to perform encryption and decryption. After selecting the sender's key value, the key agreement step is performed according to our recommended protocol. The suggested key exchange approach employs the Diffie-Hellman key exchange mechanism. A cryptographic key exchange technique is the Diffie-Hellman method. This is a method of transferring a master key in the field of cryptography when two individuals who have never met before create a public key during an unsafe discussion. The system's communications will then be protected with this key using the symmetric cypher Cs(key).

Final Encryption

Having stated that, encryption is the phenomena of sharing data in the form of a code with increased security through the process of producing ciphertext, as shown in the equation. (19) and (20).

$$CT1 = CA * C \quad (19)$$
$$CT2 = message + CA * C_s(key) \quad (20)$$

where 'CA' indicates the coverage area from $1\ to\ n-1$, $CT1$ and $CT2$ are the cipher text keys.

Decryption

Decryptions are exchanges of encrypted communications for regular messages and can be carried out manually or technically using keys. Relevant message can be decrypted using Equ. (21),

$$Message = CT2 - C_s(key) \times CT1 \quad (21)$$

The secret key is used to locate the distinct message, which is then optimally transmitted to the access point. Analysis was done on the GSA-HAS method's findings and analysis.

Results and Discussion

This explanation of the suggested strategy, which produces efficient results, uses the NS2 programme. The following statement anticipates that the method's efficacy will be demonstrated throughout the simulation results.

Simulation Parameters

Our HSA-GSA-provided assessment's main goal is to raise network performance as a whole. Our procedure is compared to earlier research like AOMDV and TC-SSA in order to assess how much better it is. The outcomes were attained using the Network Simulator-2 (NS-2) simulator. With a transmission range of 250 metres, a two-beam model, 100 nodes with 1000*1000 m, and a speed of 5 m/s, the AOMDV protocol is used. MDR (Message Delivery Rate), E2E Latency (End-to-End Latency), NT (Network Throughput), and AEE (Average Energy Efficiency) are important performance-improving indicators. By deriving the following metrics from the equation, our routing protocol assessed the performance. (22) & (23):

MDR

MDRs are defined as ratios of packets received by nodes to packets sent. MDR units are percentages whose mathematical expressions are:

$$MDR = \frac{\sum_{x=0}^{n} Node_x^{receiver}}{\sum_{y=0}^{m} Node_y^{sender}} \quad (22)$$

E2E-Delays

The network terminal delay calculation measures the amount of time it takes for the sending node to transfer every packet to the recipient. Ms is measures of E2E delays and expressed mathematically:

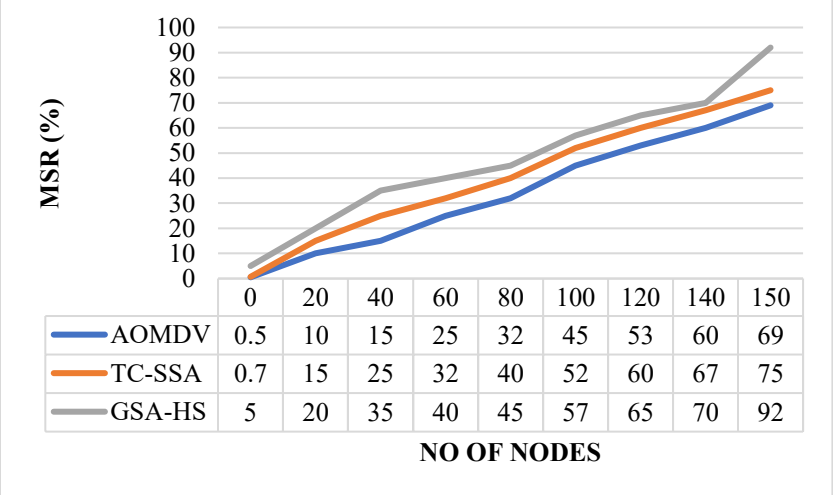
$$E2E_{delay} = \frac{\sum_{x=0}^{n}(time_x^{received} - time_x^{transmitted})}{n} \quad (23)$$

Network Throughputs

The complete network's data transmission during communications between senders and receivers are computed in Kbps.

AEE (Average Energy Efficiency)

The quantity of residual energy computed at the simulation's conclusion is known as AEE.



	0	20	40	60	80	100	120	140	150
AOMDV	0.5	10	15	25	32	45	53	60	69
TC-SSA	0.7	15	25	32	40	52	60	67	75
GSA-HS	5	20	35	40	45	57	65	70	92

Fig. 4: Message Success Rate Calculation

Figure 4 displays MSR performances for proposed work together with comparative findings from earlier models like AOMDV and TC-SSA. The suggested GSA-HS MSR is comparatively greater than that of earlier approaches, as can be shown in the figure. The earlier works were 69%, 75%, and 92%, whereas the suggested HSA-ISSA MSR is around 94%. The suggested solution uses both a hybrid security and an advanced SSA optimisation model to arrive at this conclusion.

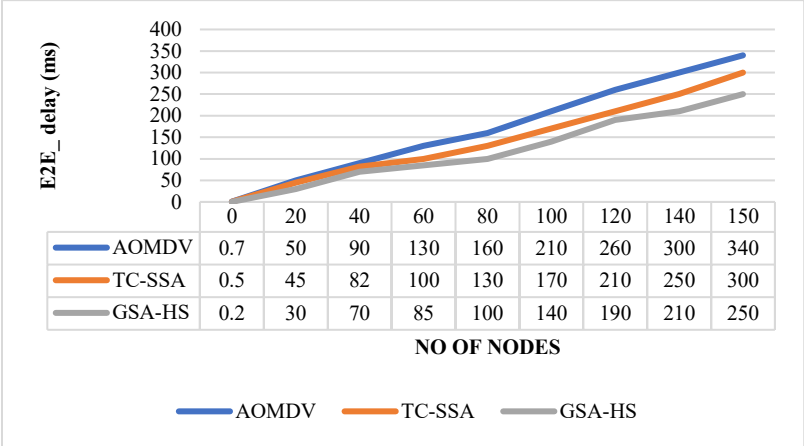


Fig. 5: End to End Delay Calculations

Figure 5 displays E2E_delay's performance. The proposed job's E2E_delay delay is 250ms, compared to the tasks that came before it that were 340ms and 300ms.

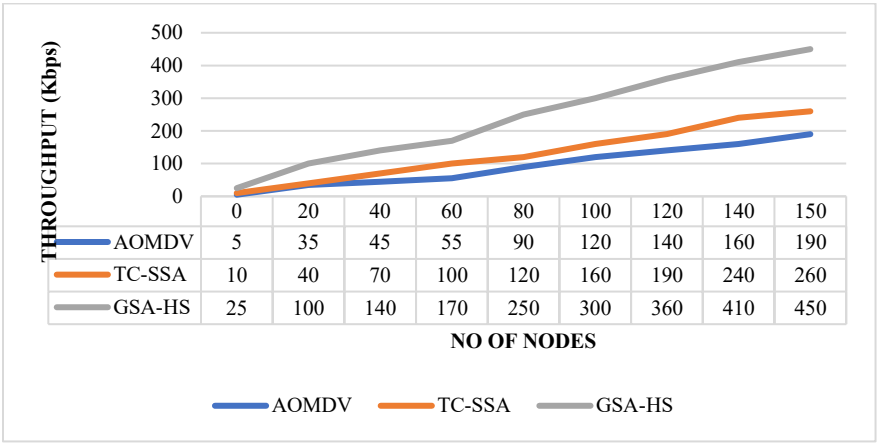


Fig. 6: Network Throughput Calculations

The network throughput calculation is shown in Figure 6. When compared to prior efforts, the suggested model generates extremely high throughput. While other protocols are 190 kbps and 260 kbps, the recommended task rate is 450 kbps.

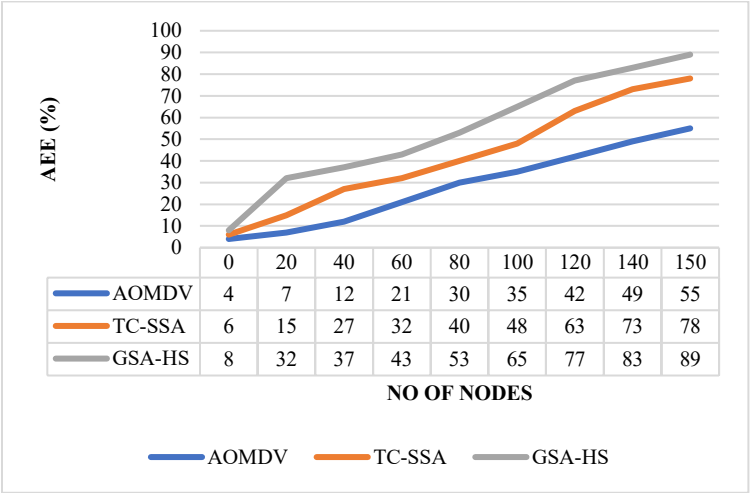


Fig. 7: Average Energy Efficient Calculations

The comparative analysis of the AEE computation is shown in Figure 7. The HSA-ISSA protocol obtained an AEE score of 89.2%, with the remaining values being 56%, 79%, and 85%. One of the criteria needed to improve the network's quality of service is AEE. This computation shows that our suggested model performs far better than earlier approaches.

Conclusion

In this study, it increased the security and breadth of the Cluster Head (CH) protocol. It concentrated on the CH selection approach for extending the EE and network life. This paper used the FGF algorithm, which was a combination of the FFOA and GSO models, for the best CH selection. Finally, analysis was carried out to verify the improvement of the model that was presented by altering the number of neighbours and sensor ranges. Hybrid security is used to facilitate trustworthy and secure communication. It combines the ECC method and the Diffie-Hellman key exchange algorithm. The results show that the proposed GSA-HSA gives better results in terms of MSR, E2E_delay, NT, AEE and average power consumptions. It may draw the conclusion that the network's overall performance improved and became more reliable after the introduction of hybrid security and GSA into the Cluster head protocol as compared to the earlier work. However, due to high packet retransmission rates during simulations, significant routing overheads lead to additional latencies and power consumptions. Therefore, this study can be continued in the future by focusing on efficiencies and latencies during emergencies in WSNs.

Reference

Ahmad, H., & Kohli, N. (2021). LBCM: Energy-efficient clustering method in wireless sensor networks. *Engineering and Applied Science Research*, *48*(5), 529-536.

Ahmad, S.A., Krishnahari, E., Khan, M.Y., & Rao, S.P. (2020). Withdrawn: Neighbor node intimacy (N2i) for trust management in WSN.

Tita, E.D., Nwadiugwu, W.P., Lee, J.M., & Kim, D.S. (2021). Real-time optimizations in energy profiles and end-to-end delay in WSN using two-hop information. *Computer Communications*, *172*, 169-182.

Roslin, S. E. (2021). Data validation and integrity verification for trust based data aggregation protocol in WSN. *Microprocessors and Microsystems, 80,* 103354.

Rao, A.N., Naik, B.R., & Devi, L.N. (2020). Withdrawn: On the relay node placement in WSNs for lifetime maximization through metaheuristics.

Nikouei, R., Rasouli, N., Tahmasebi, S., Zolfi, S., Faragardi, H., & Fotouhi, H. (2019). A quantum-annealing-based approach to optimize the deployment cost of a multi-sink multi-controller wsn. *Procedia Computer Science*, *155*, 250-257.

Nivedhitha, V., Saminathan, A. G., & Thirumurugan, P. (2020). DMEERP: A dynamic multi-hop energy efficient routing protocol for WSN. *Microprocessors and Microsystems, 79*, 103291.

Daanoune, I., Baghdad, A., & Ballouk, A. (2020). An enhanced energy-efficient routing protocol for wireless sensor network. *International Journal of Electrical & Computer Engineering (2088-8708)*, *10*(5), 5462-5469.

Esmaeili, H., Hakami, V., Bidgoli, B. M., & Shokouhifar, M. (2022). Application-specific clustering in wireless sensor networks using combined fuzzy firefly algorithm and random forest. *Expert Systems with Applications, 210,* 118365.

Ding, Q., Zhu, R., Liu, H., & Ma, M. (2021). An overview of machine learning-based energy-efficient routing algorithms in wireless sensor networks. *Electronics, 10(13)*, 1539.

Nashwan, S. (2021). AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment. *Egyptian Informatics Journal*, *22*(1), 15-26.

Ding, Q., Zhu, R., Liu, H., & Ma, M. (2021). An overview of machine learning-based energy-efficient routing algorithms in wireless sensor networks. *Electronics, 10(13),* 1539.

Ramteke, R., Singh, S., & Malik, A. (2022). Optimized routing technique for IoT enabled software-defined heterogeneous WSNs using genetic mutation based PSO. *Computer Standards & Interfaces, 79*, 103548.

Malisetti, N.R., & Pamula, V.K. (2020). Performance of quasi oppositional butterfly optimization algorithm for cluster head selection in WSNs. *Procedia Computer Science*, *171*, 1953-1960.

Karpagam, M., Vinesha, P., Devi, D., & Karthika, S. (2020). Withdrawn: Reduction in information loss due to isolated and dumb nodes using ant colony optimization for WSN.

Maheshwari, P., Sharma, A. K., & Verma, K. (2021). Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization. *Ad Hoc Networks, 110*, 102317.

Lipare, A., Edla, D. R., & Kuppili, V. (2019). Energy efficient load balancing approach for avoiding energy hole problem in WSN using Grey Wolf Optimizer with novel fitness function. *Applied Soft Computing, 84*, 105706.

Hamdi, M.M., Audah, L., Rashid, S.A., & Alani, S. (2021). VANET-based traffic monitoring and incident detection system: A review. *International Journal of Electrical & Computer Engineering (2088-8708)*, *11*(4).

Hamdi, M.M., Audah, L., Abood, M.S., Rashid, S.A., Mustafa, A.S., Mahdi, H., & Al-Hiti, A.S. (2021). A review on various security attacks in vehicular ad hoc networks. *Bulletin of Electrical Engineering and Informatics*, *10*(5), 2627-2635.

Remmiya, R., & Brajula, W. (2019). Available Transfer Capability Enhancement using Fruitfly Optimization. *Journal of Computational Mechanics, Power System, and Control*, *2*(1), 1-8.

Kulkarni, Y.R., & Murugan, T.S. (2019). Hybrid weed-particle swarm optimization algorithm and C-mixture for data publishing. *Multimedia Research*, *2*(3), 33-42.

Vasundhara, S. (2017). Elliptic curve cryptography and Diffie-hellman key exchange. *IOSR Journal of Mathematics (IOSR-JM)*, *13*(1), 56-61.

Li, B. (2015). Human nature, the means-ends relationship, and alienation: Themes for potential East–West collaboration. *Technology in Society*, *43*, 60-64.

Vinitha, A., & Rukmini, M.S.S. (2022). Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm. *Journal of King Saud University-Computer and Information Sciences*, *34*(5), 1857-1868.

Chen, Z., Zhou, W., Wu, S., & Cheng, L. (2021). An on-demand load balancing multi-path routing protocol for differentiated services in MWSN. *Computer Communications*, *179*, 296-306.