International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 16 August 2023 **Revised:** 10 October 2023 **Accepted:** 19 October 2023*

Secure Clustering and Routing using Adaptive Decision and Levy Flight based Artificial Hummingbird Algorithm for Wireless Sensor Networks

Preethi Vennam[1], Mouleeswaran, S.K.[2]
[1]Department of Computer Science & Engineering,
Dayananda Sagar University, Bengaluru 560078, India.
E-mail: preethivennam.res-soe-cse@dsu.edu.in.
[2]Department of Computer Science & Engineering,
Dayananda Sagar University, Bengaluru 560078, India.
E-mail: mouleeswaran-cse@dsu.edu.in

Abstract: Wireless Sensor Network (WSN) receives huge attention from various remote monitoring applications because of its self configuration, ease of maintenance and scalability features. But, the sensors of the WSNs vulnerable to malicious attackers due to the energy constraint, open deployment and lack of centralized administration. Therefore, the secure routing is established for achieving the secure and reliable data broadcasting in the WSN. In this paper, an Adaptive Decision and Levy Flight based Artificial Hummingbird Algorithm (ADLFAHA) is proposed for performing an effective secure routing under the blackhole and Denial of Service (DoS) attacks. The ADLFAHA is developed to perform Secure Cluster Head (SCH) selection and secure path identification according to the trust, energy, load and communication cost. An adaptive decision strategy and levy flight incorporated in the ADLFAHA is used to enhance exploration and achieves global optimization capacity that helps to enhance the searching process. Moreover, the developed ADLFAHA helps to avoid the congestion among the nodes by balancing the load in network. The ADLFAHA is analyzed using End to End Delay (EED), throughput, Packet Delivery Ratio (PDR) and overhead. The existing researches such as Firebug Optimized Modified Bee Colony (FOMBC) and Lightweight Secure Routing (LSR) are used to compare the ADLFAHA. The PDR of the ADLFAHA for the simulation time of 100 s is 98.21 that is high than the FOMBC and LSR.

Keywords: Adaptive Decision and Levy Flight based Artificial Hummingbird Algorithm, Congestion, Secure Cluster Head (SCH) selection, secure routing, Trust, Wireless Sensor Networks.

1. Introduction

Wireless Sensor Network (WSN) is group of nodes that are linked as network for transferring and sharing the information gathered from the surrounding environment via the intermediate links [1]. The tiny sensors of the WSN uses the radio signals for data transferring with each other and it is installed for perceiving, tracking and observing the physical world by acquiring various parameters such as vibrations, temperature, air pressure, moisture, wind speed, humidity and so on [2] [3]. WSN performs key role in various applications such as gas detection, home automation, crop monitoring habitat surveillance, medical treatments, environmental monitoring, industrial monitoring, military applications and so on [4]. The sensor based devices used in WSN becomes intelligent and it has various functions such as inter-communication, calculation, sensing and decision making capacity which makes the WSN is powerful based on today's requirements [5]. The sensors are operated with the battery power, therefore the capacity of computation and data transferring is limited over the network [6]. The WSN is susceptible to the malicious attacks due to its energy constraint, lack of centralized administration and open deployment [7] [8].

The WSN is determined as insecure environment, when the malicious attacks are activated in sensor nodes [9]. This malicious attacks in the WSN causes the unauthorized access and affects the network integrity and confidentiality [10]. Cluster based routing is considered as a promising approach to achieve the energy efficiency, scalability of data delivery and energy efficiency [11]. In clustering process, the sensors are separated into small groups called clusters whereas each cluster has special node namely Cluster Head (CH). The CH has the responsibility of gathering the information from remaining nodes of the cluster [12] [13]. There are two different ways for the clusters of the WSN for broadcasting the data with another cluster such as intra-cluster and inter-cluster communications. In inter cluster communications, the CH transfers the data to BS by utilizing the multi hop by hop hierarchical clustering approach whereas the cluster member transfers the with its CH via single hop communication at intra-cluster communication [14]. A secure routing is required to be developed to avoid the malicious nodes for performing the reliable transmission [15].

The contributions are summarized as follows:

- An effective SCH and route selection is performed by optimizing the ADLFAHA using four distinct parameters such as trust, energy, load and communication cost. The trust value considered in the ADLFAHA avoids the attacks which helps to enhance the data broadcasting over the WSN.
- The congestion among the nodes is avoided by considering the load of the nodes which avoids the packet loss over the network.

The rest of paper is structured as follows: Section 2 provides the related works of secure routing in WSN. The detailed information about the ADLFAHA based SCH and path discovery are provided in the section 3. Section 4 provides the outcomes and section 5 concludes the overall research.

2. Related work

The related works of secure data transmission are provided in this section along with its merits and limitation.

Vinitha, A. and Rukmini, M.S.S [16] presented the Taylor based Cat Salp Swarm Algorithm (Taylor C-SSA) to perform a multi-hop routing in WSN. At first, the Low Energy Adaptive Clustering Hierarchy (LEACH) approach was used to discover the optimal CHs from the network. Next the optimum hop for performing the data transmission was chosen using the Taylor C-SSA whereas the secure multi hop routing was done by using the trust model during route discovery. However, the load balancing among the sensors was not considered in routing which affected the routing process.

Sudha, G. and Tharini, C [17] developed the clustering and routing solution for developing an energy efficient WSN with trust. At first, the nodes of the network were clustered using Dempster-Shafer Theory (DST) where it doesn't require any prior knowledge to perform the clustering. Next, the Lion Optimization Algorithm (LOA) was used to identify appropriate route by considering the trust metric for performing the secure data transmission. However, the developed LOA was not considered the distance which lead to discover the route with higher transmission distance.

Vijayalakshmi, S *et al.* [18] presented an Energy-Efficient Adaptive Cluster-Head Selection Algorithm (EEACHS) for selecting the CH according to the energy. This energy based CH selection was used to alter the role of integrated cluster which used to balance the energy usage of the cluster. On the other hand, trust value of the nodes was computed to perform the secure routing over the network. The EEACHS was adapted to the energy load and the rotating CH among all nodes in the cluster. An appropriate fitness value was required to be incorporated for further enhancing the WSN performances.

Alamelumangai, M. and Suresh, S [19] developed the Firebug Optimized Modified Bee Colony (FOMBC) for enhancing the network security. At first, the secure node from the network was chosen according to the trust, Quality of Services and delay. Further, an appropriate route over the network was discovered using the FOMBC. However, the FOMBC doesn't considered the clustering over the network, therefore the direct transmission of data packets was affected the data transmission.

Pathak, A *et al.* [20] presented the Lightweight Secure Routing (LSR) for enhancing the security and avoiding the energy hole issue. The developed LSR used the ant colony optimization an adaptive security approach according to the direct and indirect trust computations. The improvement over connectivity among the sensors was used to avoid the energy hole issue. The developed LSR was not avoided the congestion occurred during the data transmission.

3. ADLFAHA method

In this research work, the proposed ADLFAHA is used to discover optimum SCHs and secure route over the network. The developed ADLFAHA performs the secure data broadcasting the under the blackhole and DoS attacks which helps to avoid the packet drop. Next, the load in the network is considered in ADLFAHA for avoiding the congestion between the sensors that additionally enhances the data delivery. The secure clustering and routing using ADLFAHA is shown in the Figure 1.

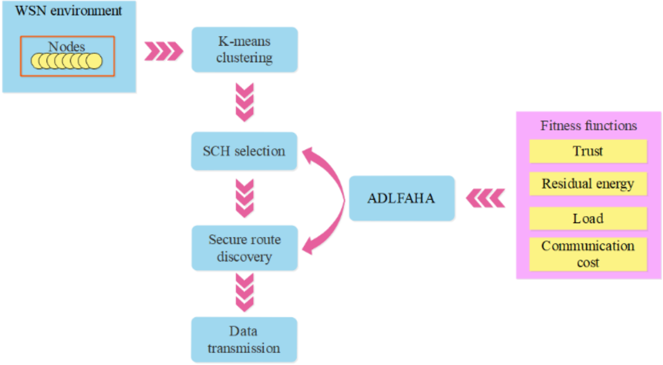

Figure 1. Secure clustering and routing using ADLFAHA

Article Received: *16 August 2023* ***Revised:*** *10 October 2023* ***Accepted:*** *19 October 2023*

3.1. Clustering process

At first, the K-means algorithm clusters the randomly located nodes in network based on the Euclidian distance. The ADLFAHA identifies optimum SCHs and route for broadcasting the data in the WSN.

3.2. SCH selection using ADLFAHA

The optimum SCHs from normal sensors are discovered by using ADLFAHA. The conventional AHA is inspired by the hummingbirds special flight skills during foraging and prey hunting process. The levy flight incorporated in the AHA is used to expand the search space that enhances the global optimization capacity. On the other hand, adaptive control strategy is incorporated for enhancing the exploration processes. Here, the ADLFAHA is used for discovering the optimum SCHs.

3.2.1. Initialization

The initial population of AHA is set with the candidate nodes to be selected as SCH. The random sensor ID between 1 and M is taken to initialize the hummingbird solution, where M is total sensors in WSN. Let, i th hummingbird is $X_i = (X_{i,1}, X_{i,2}, \dots, X_{i,d})$, where dimension of AHA is represented as d that identical to amount of SCHs.

3.2.2. Iterative process

The initial solutions of the AHA is given as input to discover the optimum SCHs. The food source's visit table is created by using equation (1).

$$VT_{ij} = \begin{cases} 0 & if\ \ i \neq j \\ null & i = j \end{cases}, \quad i = 1, 2, \dots, N, j = 1, 2, \dots, N \tag{1}$$

Where, $VT_{ij} = null$ for $i = j$ represents the food consumed by hummingbird at significant food source and N represents the amount of hummingbirds. Moreover, a $VT_{ij} = 0, i \neq j$ represents the hummingbird i visits the food source j.

3.2.2.1. Guided Foraging

In guided searching phase, a different flight skills such as axial, diagonal and omnidirectional flight are applied as shown in equations (2), (3) and (4) respectively. In this phase, the levy flight is incorporated for further increasing the search space.

$$D_i = \begin{cases} 1 & if\ \ i = randi([1, d]) \\ 0 & else \end{cases}, \quad i = 1, 2, \dots, d \tag{2}$$

$$D_i = \begin{cases} 1 & if\ \ i = P(i), j \in\ [1, k], P = randperm(k), k \in [2, r_1(d-1)+1] \\ 0 & else \end{cases}, \quad i = 1, 2, \dots, d \tag{3}$$

$$D_i = 1 \quad i = 1, 2, \dots, d \tag{4}$$

Where, $randi([1, d])$ denotes the random integer among the $[1, d]$; d denotes the dimension; $randperm(k)$ denotes the random permutation of integers among $[1, k]$ and r_1 is the random value among $[0, 1]$. The guided foraging behavior is shown in equation (5).

$$V_i(t+1) = X_{i,t}(t) + a \times D \times \left(X_i(t) - X_{i,t}(t)\right), \ \ a \in N(0,1) \tag{5}$$

Where, $X_{i,t}(t)$ denotes the ith food source of tth iteration that is the target food source visited by ith hummingbird. Equation (6) shows the update of X_i.

$$X_i(t+1) = \begin{cases} X_i(t) + \alpha \oplus Levy\ (\lambda) & if\ f\left(X_i(t)\right) \leq f(V_i(t+1)) \\ V_i(t+1) & otherwise \end{cases} \tag{6}$$

Where, fitness value is denoted as f; dot multiplication is denoted using $\oplus$; step size control parameter is denoted as α; random search path is denoted as $Levy\ (\lambda)$ that required to satisfies the equation (7).

$$Levy \sim u = t^{-\lambda}, \ \ 1 < \lambda \leq 3 \tag{7}$$

The step size follows the distribution of Levy and its step size s is computed using equation (8).

$$s = \frac{\mu}{|v|^{1/\beta}} \tag{8}$$

Where, μ and v are Gaussian distribution values that are expressed in equations (9) and (10).

$$\mu \sim N(0, \sigma_\mu^2) \tag{9}$$

$$v \sim N(0, \sigma_v^2) \tag{10}$$

The σ_μ and σ_v are expressed in equations (11) and (12) respectively.

$$\sigma_\mu = \frac{(1+\beta)\left(sin\frac{\pi\beta}{2}\right)}{\left(\frac{1+\beta}{2}\right)\beta^2\left(\frac{\beta-1}{2}\right)} \tag{11}$$

$$\sigma_v = 1 \tag{12}$$

Where, β is constant value equals to 1.5.

3.2.2.2. Territorial Foraging

The hummingbird searches for new food source instead of checking the other food sources, when the flower nectar is empty. Hence, the hummingbird explores the adjacent area within the range where a new food source is identified when compared to the precious solution. Equation (13) expresses the territorial foraging of AHA.

$$V_i(t+1) = X_{i,t}(t) + b \times D \times X_i(t), \quad b \in N(0,1) \tag{13}$$

3.2.2.3. Migration foraging

The hummingbird goes for huge distance, when the desired feeding location has no food. The migration coefficient is developed for this AHA. Consequently, the old food source is abandoned, new source is utilized and visit table is modified in AHA. Equation (14) shows the travelling of hummingbird from the source with smaller nectar-refilling rate to modem randomly created source.

$$X_w(t+1) = L + r \times (U - L) \tag{14}$$

Where, X_w is the food source with worst fitness, and lower and upper limits are denoted as L and U.

3.2.2.4. Adaptive decision strategy

The adaptive decision is used to enhance the exploration (i.e., guided foaging) via the opposition-based learning during the searching process. Further, the location update by utilizing adaptive decision of AHA is expressed in equation (15).

$$X_i = \begin{cases} X_i(t+1) & f\big(X_i(t+1)\big) \le f(X_i(t)) \\ X_i(t) & f\big(X_i(t+1)\big) > f(X_i(t)) \end{cases} \quad (15)$$

3.3. Fitness function computation

The different finesses considered in the AHA for selecting the CH are trust (FF_1), energy ratio (FF_2), load (FF_3) and communication cost (FF_4). The fitness value mentioned in equation (6) is computed by using equation (16).

$$F = \sigma_1 \times FF_1 + \sigma_2 \times FF_2 + \sigma_3 \times FF_3 + \sigma_4 \times FF_4 \quad (16)$$

Where, the weight parameters assigned to fitness value is denoted as σ_1 to σ_4. The fitness values are detailed below:

- Equation (17) is primary fitness value considered while choosing the SCH. A mutual trust among the sensors are essential to broadcast the data packets, because this trust is utilized for mitigating the attacks. The trust is computed based on the data broadcasting among the sensors that is the proportion of received packets and broadcasted packets between the sensors a and b

$$FF_1 = \frac{Received\ packets_{a,b}}{Sent\ packets_{a,b}} \quad (17)$$

- Energy is important parameter during the SCH selection, hence the ratio of energy is considered in this AHA. The energy ratio is defined as the ratio among initial energy and residual energy as shown in equation (18).

$$FF_2 = \sum_{i=1}^{M} \frac{Initial\ energy}{Remaining\ energy} \quad (18)$$

- Load expressed in the network is considered for balancing the load while transmitting the data packets. This load balancing among the sensors used to avoid the congestion over the network. Equation (19) and (20) denotes the load value among the network

$$FF_3 = \frac{\sum_{i=1}^{d} Clustering\ (SCH_i)}{M} \quad (19)$$

$$Clustering\ (SCH_i) = K \times |Load(SCH_i) - dist(BS, SCH_i) \times \frac{\sum_{i=1}^{d} Load(SCH_i)}{M}| \quad (20)$$

Where, $Load(SCH_i)$ is the received packets at SCH; K is Proportionality constant and $dist(BS, SCH_i)$ denotes the distance among SCH and BS.

- A communication cost used for broadcasting the information with neighbor sensor is shown in equation (21).

$$FF_4 = \frac{d_{avg}^2}{d_0^2} \quad (21)$$

Where, average distance among sensor and adjacent sensor is denoted as d_{avg}^2 and radius of sensor is d_0^2.

The above-mentioned fitness value is employed to identify optimum set of SCHs. The trust value considered in the AHA is used to avoid the blackhole and DoS attacks which helps to avoid the packet loss over the WSN. The sensor with enough energy is chosen as SCH by considering the ratio of energy which helps to eliminate the failure node. The load value considered in the AHA is used to balance the load among the SCHs which helps to reduce the energy usage. The communication cost is employed to reduce the delay while broadcasting the information over the WSN.

3.4. Route discovery using AHA

After identifying the SCH from clusters, the AHA based route discovery is used to identify the route. The control messages are utilized in AHA to identify the path via the SCHs. The route identification using AHA also considers the same fitness values such as trust, energy ratio, load and communication cost. At first, the route request is transmitted by source SCH for all the nearby SCHs. The SCH with optimum fitness replies with route reply while the same procedure is done until the BS receives the route request. The data packets are broadcasted once the secure path is identified using AHA. Moreover, the route error and hello messages are utilized by AHA to maintain the route.

4. Results and discussion

The Network Simulator version 2.34 is used to design and simulate the proposed ADLFAHA based secure routing approach. The system configuration used to analyze this research are 6GB RAM, i5 processor and Windows 7 OS. In this simulation, a network of 100 nodes considered to be deployed in the area of $1500m \times 1500m$. The simulation specifications are shown in the Table 1.

Table 1. Simulation parameters

Parameter	Value
Number of nodes	100
Area	$1500m \times 1500m$
Initial energy	5J
Propagation model	Two-ray ground reflection
Traffic source	CBR
Mac	IEEE 802.11 DCP
Antenna pattern	OmniAntenna
Network interface type	WirlessPhy

4.1. Performance analysis

The ADLFAHA is evaluated by using the throughput, EED, PDR and overhead. The proposed ADLFAHA is compared with the classical approach namely Ad-hoc On-demand Distance Vector (AODV) with the blackhole and DoS attacks.

4.1.1. Throughput

Throughput is the ratio among total packets received by the BS and total simulation time. Figures 2 and 3 shows the throughput analysis of ADLFAHA for blackhole and DoS attacks respectively. This analysis indicates that the ADLFAHA obtains higher throughput than the AODV. The trust consideration of ADLFAHA leads to avoid the attacker nodes that helps to achieve the successful data reception by the BS. On the other hand, the load balancing among the nodes is used to avoid the collision that further helps to enhance the throughput.

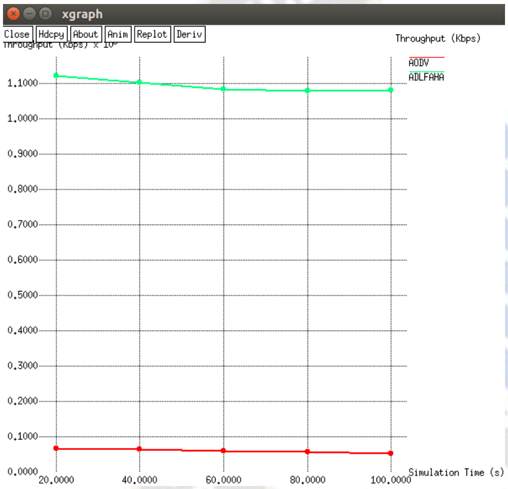

Figure 2. Throughput analysis of ADLFAHA for blackhole attacks

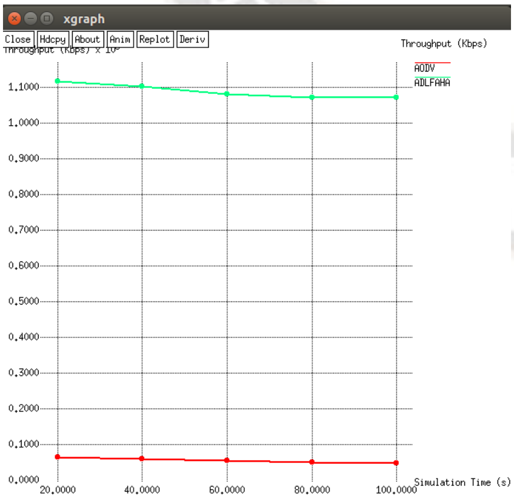

Figure 3. Throughput analysis of ADLFAHA for DoS attacks

4.1.2. Delay

Delay is the time used to broadcast the information from the source to destination. The delay evaluation of ADLFAHA for blackhole and DoS attacks are shown in the Figures 4 and 5 respectively. From the analysis, it is cleared that the ADLFAHA achieves less delay when compared to the AODV. The shortest path identification using ADLFAHA and less control packet usage during route discovery are helps to reduce the delay taken during the transmission.

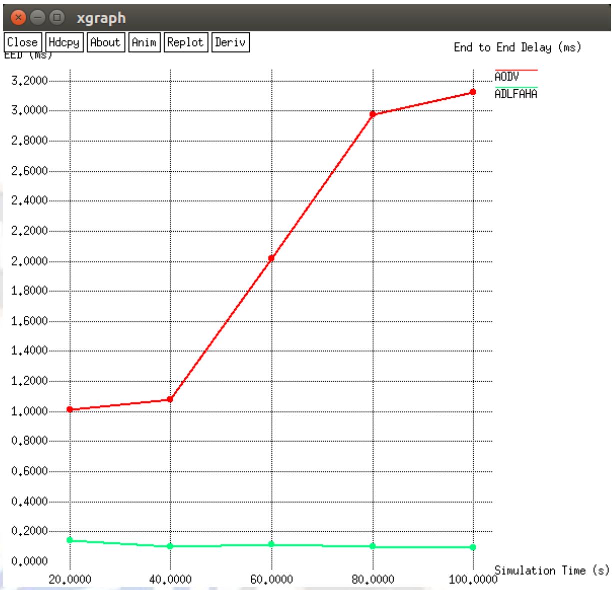

Figure 4. Delay analysis of ADLFAHA for blackhole attacks

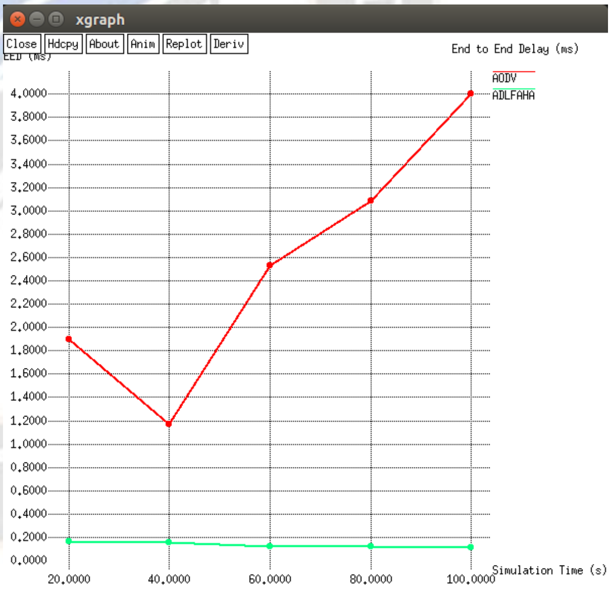

Figure 5. Delay analysis of ADLFAHA for DoS attacks

4.1.3. PDR

PDR is the proportion among a packets received and amount of packets broadcasted over the network. Figures 6 and 7 shows the PDR analysis of ADLFAHA for blackhole and DoS attacks respectively. This evaluation depicts that the ADLFAHA achieves higher PDR when compared to the AODV. The PDR of ADLFAHA is improved based on the following ways: 1) The trust value of ADLFAHA is used to avoid the blackhole and DoS attacks. 2) Moreover, the data

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 16 August 2023 **Revised:** 10 October 2023 **Accepted:** 19 October 2023*

collision is avoided by performing the load balancing among the nodes.

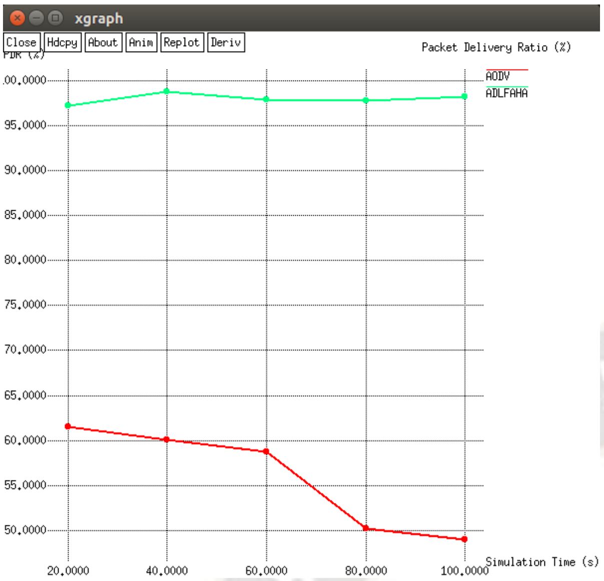

Figure 6. PDR analysis of ADLFAHA for blackhole attacks

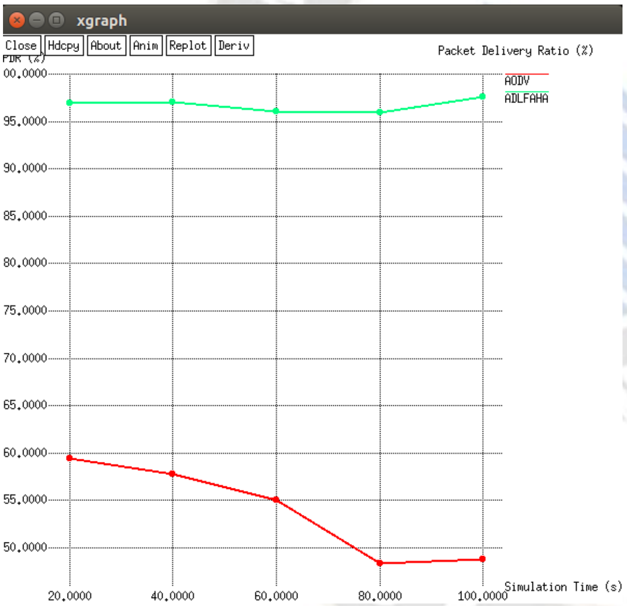

Figure 7. PDR analysis of ADLFAHA for DoS attacks

4.1.4. Overhead

The overhead defines the total amount of control packets transmitted during the route discovery. The overhead comparison of ADLFAHA for blackhole and DoS attacks are shown in the Figures 8 and 9 respectively. From the analysis, it is cleared that the ADLFAHA achieves less overhead when compared to the AODV. The ADLFAHA requires only less amount of control packets while searching optimum route. Therefore, the ADLFAHA achieves the less overhead than the AODV.

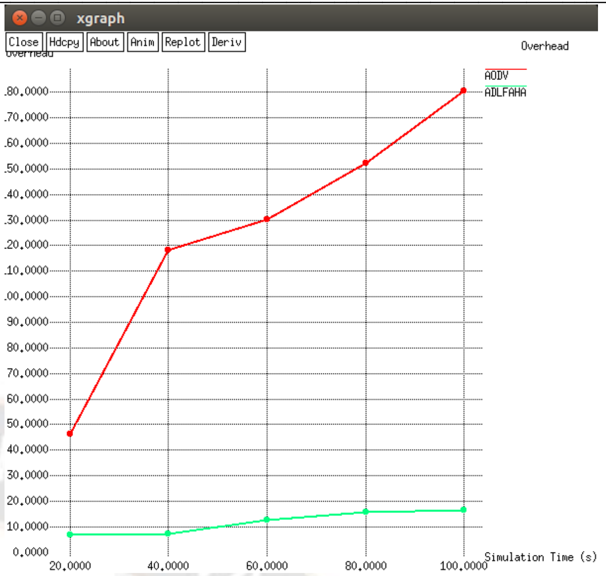

Figure 8. Overhead analysis of ADLFAHA for blackhole attacks

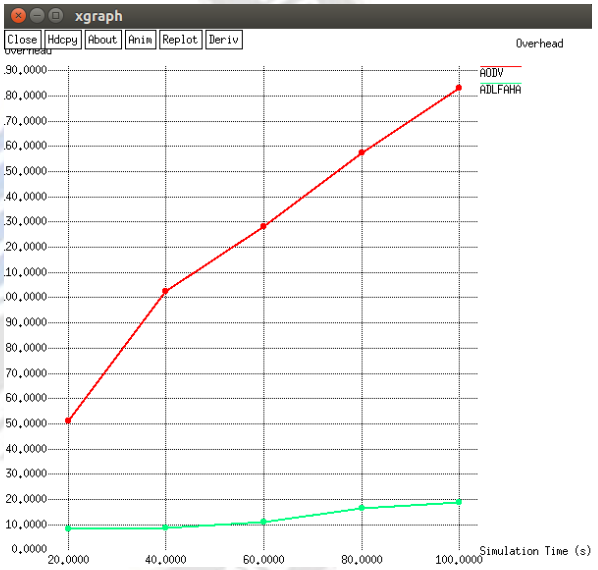

Figure 9. Overhead analysis of ADLFAHA for DoS attacks

4.2. Comparative analysis

The existing researches such as FOMBC [19] and LSR [20] are utilized to estimate the proposed ADLFAHA. Table 2 indicates the comparison of ADLFAHA with FOMBC [19] and LSR [20], where NA denotes the values which are not available in the respective research. This comparison shows that the ADLFAHA achieves the better performance than the FOMBC [19] and LSR [20]. The secure routing based on the trust value of ADLFAHA is used to enhance the data delivery. Further, the congestion over the network is avoided in ADLFAHA by considering the load occurred over the network that additionally used to enhance the data delivery.

Table 2. Comparative analysis

Performances	**Methods**	**Simulation time (s)**				
		20	**40**	**60**	**80**	**100**
Throughput (Kbps)	**FOMBC [19]**	89	79	76.3	72.7	65.2
	ADLFAHA	1121.58	1104.26	1084.76	1078.92	1081.11
EED (ms)	**FOMBC [19]**	1	4	9	11	13
	LSR [20]	NA	NA	NA	NA	0.200
	ADLFAHA	0.138	0.103	0.111	0.103	0.097
PDR (%)	**FOMBC [19]**	84.7	76.7	62.2	54.1	50.7
	LSR [20]	NA	NA	NA	NA	96.9
	ADLFAHA	97.22	98.68	97.84	97.76	98.21
Overhead	**FOMBC [19]**	45.1	71.2	126.5	142.7	172.7
	ADLFAHA	6.95	7.13	12.76	15.79	16.66

5. Conclusion

This paper proposes the secure clustering and routing using ADLFAHA for enhancing the security over the WSN. At first, the nodes in the network is clustered using K-means followed by SCH from an each clusters is discovered by using the ADLFAHA according to the trust, energy, load and communication cost. This SCH discovery avoids the malicious attackers (Blackhole and DoS attacks) for enhancing the security. Next, the secure multi path routing is obtained by ADLFAHA to achieve the reliable data transmission. The malicious attacks avoidance is used to avoid the packet loss caused in the WSN. Moreover, the load value considered in the ADLFAHA used to avoid the congestion occurred in the nodes that helps to improve the data transmission. From the simulation, it is cleared that the ADLFAHA outperforms well when compared to the FOMBC and LSR. The PDR of the ADLFAHA for the simulation time of 100 s is 98.21 which is high when compared to the FOMBC and LSR.

References

[1] Dinesh Kumar, P. and Valarmathi, K., 2023. Fuzzy based hybrid BAT and firefly algorithm for optimal path selection and security in wireless sensor network. Automatika, 64(2), pp.199-210.

[2] Bangotra, D.K., Singh, Y., Selwal, A., Kumar, N. and Singh, P.K., 2022. A trust based secure intelligent opportunistic routing protocol for wireless sensor networks. Wireless Personal Communications, 127(2), pp.1045-1066.

[3] Renuga Devi, R. and Sethukarasi, T., 2022. Develop Trust-Based Energy Routing Protocol for Energy Efficient with Secure Transmission. Wireless Personal Communications, pp.1-28.

[4] Kalburgi, S.S. and Manimozhi, M., 2022. Taylor-spotted hyena optimization algorithm for reliable and energy-efficient cluster head selection based secure data routing and failure tolerance in WSN. Multimedia Tools and Applications, 81(11), pp.15815-15839.

[5] Agarwal, V., Tapaswi, S. and Chanak, P., 2022. Energy-efficient mobile sink-based intelligent data routing scheme for wireless sensor networks. IEEE Sensors Journal, 22(10), pp.9881-9891.

[6] N., Sasikala & Sangaiah, Pavalarajan. (2022). Energy-aware redundancy-aware clustering in wireless sensor networks using Spined Loach Searching Optimization. International Journal of Communication Systems. 36. 10.1002/dac.5385.

[7] Thahniyath, G. and Jayaprasad, M., 2022. Secure and load balanced routing model for wireless sensor networks. Journal of King Saud University-Computer and Information Sciences, 34(7), pp.4209-4218.

[8] Yu, X., Li, F., Li, T., Wu, N., Wang, H. and Zhou, H., 2022. Trust-based secure directed diffusion routing protocol in WSN. Journal of Ambient Intelligence and Humanized Computing, pp.1-13.

[9] SureshKumar, K. and Vimala, P., 2021. Energy efficient routing protocol using exponentially-ant lion whale optimization algorithm in wireless sensor networks. Computer Networks, 197, p.108250.

[10] Haseeb, K., Almustafa, K.M., Jan, Z., Saba, T. and Tariq, U., 2020. Secure and energy-aware heuristic routing protocol for wireless sensor network. IEEE Access, 8, pp.163962-163974.

[11] Barnwal, S.K., Prakash, A. and Yadav, D.K., 2023. Improved African Buffalo Optimization-Based Energy Efficient Clustering Wireless Sensor Networks using Metaheuristic Routing Technique. Wireless Personal Communications, 130(3), pp.1575-1596.

[12] Mohanadevi, C. and Selvakumar, S., 2022. A qos-aware, hybrid particle swarm optimization-cuckoo search clustering based multipath routing in wireless sensor networks. Wireless Personal Communications, 127(3), pp.1985-2001.

[13] Khot, P.S. and Naik, U.L., 2022. Cellular automata-based optimised routing for secure data transmission in wireless sensor networks. Journal of Experimental & Theoretical Artificial Intelligence, 34(3), pp.431-449.

[14] Kranthikumar, B. and Leela Velusamy, R., 2023. Trust aware secured energy efficient fuzzy clustering-based protocol in wireless sensor networks. Soft Computing, pp.1-12.

[15] Bhanu, D. and Santhosh, R., 2023. Fuzzy enhanced location aware secure multicast routing protocol for balancing energy and security in wireless sensor network. Wireless Networks, pp.1-20.

[16] Vinitha, A. and 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), pp.1857-1868.

[17] Sudha, G. and Tharini, C., 2023. Trust-based clustering and best route selection strategy for energy efficient wireless sensor networks. Automatika, 64(3), pp.634-641.

[18] Vijayalakshmi, S., Kavithaa, G. and Kousik, N.V., 2023. Improving Data Communication of Wireless Sensor Network Using Energy Efficient Adaptive Cluster-Head Selection Algorithm for Secure Routing. Wireless Personal Communications, 128(1), pp.25-42.

[19] Alamelumangai, M. and Suresh, S., 2023. Firebug Optimized Modified Bee Colony Algorithm for Trusted WSN Routing. IETE Journal of Research, pp.1-14.

[20] Pathak, A., Al-Anbagi, I. and Hamilton, H.J., 2022. An adaptive QoS and trust-based lightweight secure routing algorithm for WSNs. IEEE Internet of Things Journal, 9(23), pp.23826-23840.