



## **Trust Aware Manta Ray Foraging Optimization based Secure Routing Protocol for Wireless Sensor Networks**

**Mohammed. I. Alghamdi<sup>1</sup>, Salwa. H. Alghamdi<sup>2</sup>, Abeer. Y. Salawi<sup>3</sup>**

<sup>1</sup> Department of Engineering and Computer Science

<sup>2</sup> College of Computer Science and Information Technology

<sup>3</sup> Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia

**Emails:** mialmushilah@bu.edu.sa, 442021118@stu.bu.sa, 442020222@stu.bu.edu.sa

### **Abstract**

In Wireless sensor network (WSN) is a different type of ad-hoc network has of battery powered minimum cost sensor node with restricted computation and communication abilities used densely from a target region. The routing in WSN roles is an essential part due to their inherent energy storing ability and is suitable to extremely scalable networks. The trust in WSN roles an essential play in creating the network and addition or deletion of sensor nodes in a network very smooth and translucent. The trust was formalized as a computational method. This study develops a novel Trust Aware Manta Ray Foraging Optimization based Secure Routing (TAMRFO-SR) protocol for WSN. The proposed TAMRFO-SR model accomplishes optimal and secure routes for WSN. In addition, the TAMRFO-SR model is mainly stimulated by the fascinating characteristics of manta rays. Besides, the TAMRFO-SR model derives a fitness function with multiple parameters for secure route selection process. Moreover, the inclusion of trust in the route selection process assists in accomplishing enhanced security. The design of TAMRFO-SR model for secure data transmission depicts the novelty of the study. The experimental validation of the TAMRFO-SR model demonstrates better performance over the other approaches.

**Keywords:** Wireless sensor network; Security; Route selection; Fitness function; Routing; Manta ray optimization

### **1. Introduction**

The fast improvement of Internet of things (IoT) advances distributed computing, informal organization, and the development of smart cities constantly [1]. Smart cities depend on various sorts of appropriated keen gadgets that can furnish metropolitan occupants with a wide scope of uses like ecological observing, traffic the board, and social diversion [2]. WSN with the quality of minimal expense, fast sending, and self-association assumes an essential part in working with the administrations of shrewd city. The omnipresent sensor nodes can both gather the actual data of metropolitan climate and control general society and private offices with regards to shrewd metropolitan climate. Notwithstanding, the multi-hop routing is helpless against different sorts of attacks because of the open, dispersed, and dynamic quality of WSN [3], which truly affects information and data security. As of now, the current secure routing calculations are normally coordinated against explicit malicious or egotistical conduct attacks, since they principally depend on encryption calculations and verification instruments, which are not appropriate for the multi-jump conveyed and energy-compelled WSN [4]. Fig. 1 depicts the structure of WSN.

The examination shows that trust is a compelling method for tackling the security issues of WSN, notwithstanding, the traditional routing convention in view of trust is hard to guarantee the security of

multi-jump data transmission, and the reasons can be summed up as follows. Right off the bat, albeit the plan in light of trust can deal with intrinsic attacks in WSN, they likewise brief a few new dangers. Also, trust is altogether not the same as other ordinary course pointers, like the quantity of jumps, delay, or other QoS prerequisites, however, the most dependable models don't consider the exceptional property of trust degree in the plan of routing conventions. Thirdly, the current routing convention in view of trust has specific impediments, for example, reliance on explicit course plans or stages. At the end of the day, the security component might be invalid assuming the network routing convention is changed [5].

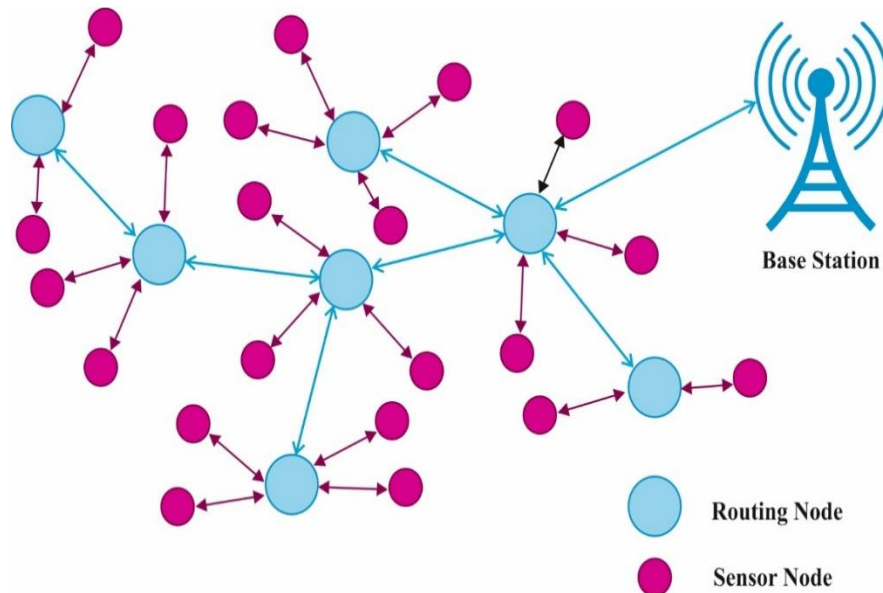


Figure 1: WSN structure

The current routing conventions for WSNs can't really adjust security and energy utilization [6]. A large portion of these conventions depends on encryption and trust systems to ensure security. Despite the fact that encryption can assist WSNs with opposing explicit kinds of network attacks, the routing conventions implanted with encryption are helpless against different sorts of network interruptions, which will bring about more energy utilization [7]. Trust-based routing conventions can oppose different sorts of attacks, yet the computation of trust esteems generally utilizes extremely high memory and consumes significant energy [8]. The current routing conventions are ordinarily streamlined for energy utilization; consequently, a total course for a couple of nodes is typically produced by enlarging the current way each jump in turn [9]. Notwithstanding, the produced courses are not internationally ideal and may neglect to work within the sight of malicious attacks. Accordingly, it is exceptionally hard for existing routing conventions to observe a solid course that can adjust security and the imperatives on the registering and battery limits of WSNs [10]. Fig. 2 illustrates the routing in WSN.

In [11], a novel fuzzy temporal rule-based cluster based routing technique with trust modelling and outlier recognition to monitor the node contributing from the transmission was presented. Also, the fuzzy temporal rule- and distance-based outlier recognition technique was presented. In [12], an effectual and optimum secured routing technique called as Particle-Water Wave Optimization (P-WWO) was established to routing the data packet from secured way. The presented P-WWO technique was planned by combining the PSO with WWO techniques. The secured route required for broadcasting the data packet was defined with the chosen CH utilizing the PSO based cellular automata with fitness measures. Lazrag et al. [13] present a routing protocol which utilizes Blockchain system for offering a shared memory amongst the network nodes. Alotaibi [14] establishes a novel secured routing method by applying a better way chosen and encrypted. Primarily, an optimum link-state multi-path routing occurs, whereas optimum directions or nodes were selected to secure broadcast. In order to optimum path selective source and target, the Crossover Mutated Marriage in Honey Bee (CM-MH) technique was established and presented under this work.

This study develops a novel Trust Aware Manta Ray Foraging Optimization based Secure Routing (TAMRFO-SR) protocol for WSN. The proposed TAMRFO-SR model accomplishes optimal and

secure routes for WSN. In addition, the TAMRFO-SR model is mainly stimulated by the fascinating characteristics of manta rays. Besides, the TAMRFO-SR model derives a fitness function with multiple parameters for secure route selection process. Moreover, the inclusion of trust in the route selection process assists in accomplishing enhanced security. The design of TAMRFO-SR model for secure data transmission depicts the novelty of the study. The experimental validation of the TAMRFO-SR model demonstrates better performance over the other approaches.

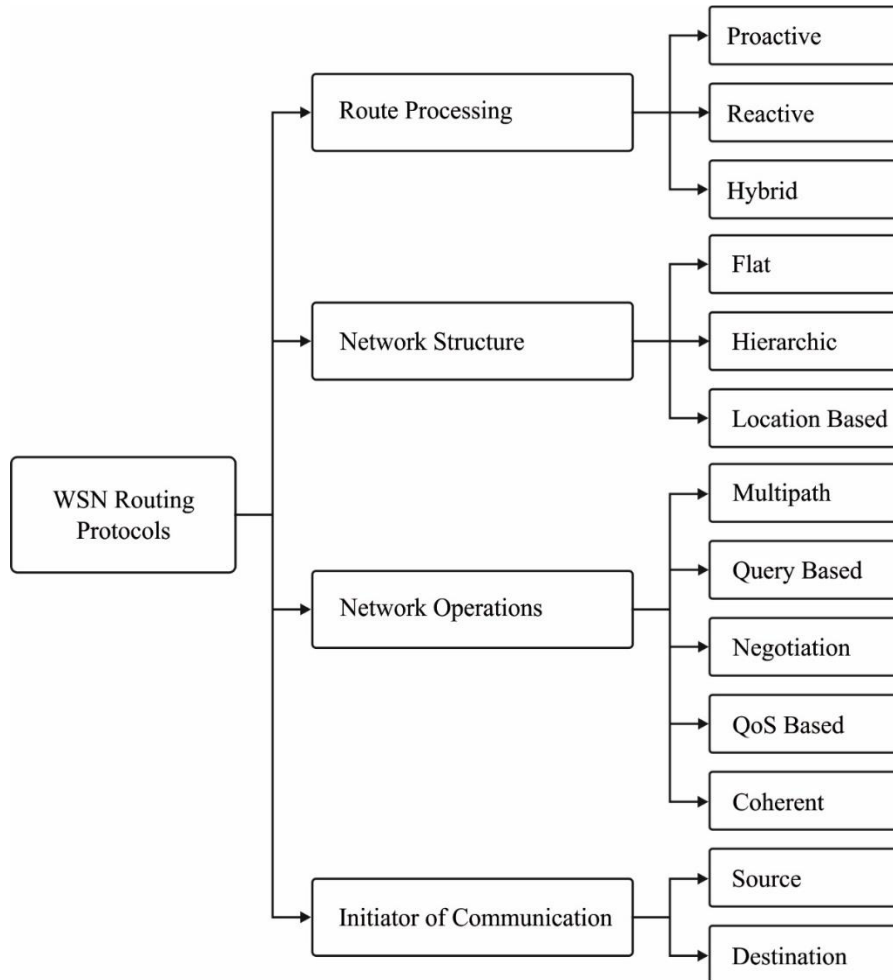


Figure 2: Routing in WSN

**2. The Proposed TAMRFO-SR Model**

In this study, a new TAMRFO-SR model has been developed to accomplish optimal and secure routes for WSN. In addition, the TAMRFO-SR model is mainly stimulated by the fascinating characteristics of manta rays. Besides, the TAMRFO-SR model derives a fitness function with multiple parameters for secure route selection process.

**2.1 Overview of MRFO Algorithm**

The MRFO has functioned with 3 foraging behaviors as Somersault foraging, Chain foraging, and Cyclone foraging. Arithmetical approaches are shown in the following [15].

***Chain Foraging***

In MRFO, the MR monitor the position of plankton and moves concern them. Once plankton concentration is greater, then the position is finest, each position is upgraded by extraordinary solution. It can be arithmetically expressed in the following:

$$C_x^{dim}(n+1) = C_x^{dim}(n) + rand.C_{best}^{dim}(n) + \varphi C_{best}^{dim}(n) - C_x^{dim}(n) \quad (1)$$

$$C_x^{dim}(n+1) = C_x^{dim}(n) + rand.C_{x-1}^{dim}(n) - C_x^{dim}(n) + \varphi C_{best}^{dim}(n) - C_x^{dim}(n) \quad (2)$$

Whereas denotes the position of  $x$ th individual at time  $n$  in  $dim$  is a dimension,  $rand$  indicates a subjective value within  $[0, 1]$ ,  $\varphi$  indicates weight coefficient, indicates the plankton with highest concentration.

### Cyclone Foraging

Here, the MR was spirally moved towards the place of food source; the MR swims from the plankton [16]. Also, follow the one in front of them and swim toward food. It can be arithmetically expressed in the following equations

$$C_x(n+1) = C_{best} + rand.(C_{x-1}(n) - C_x(n) + r^{at} \cdot \cos(2\pi t) \cdot (C_{best} - C_x(n))) \quad (3)$$

$$D_x(n+1) = D_{best} + rand.(D_{x-1}(n) - D_x(n) + r^{at} \cdot \cos(2\pi t) \cdot (D_{best} - D_x(n))) \quad (4)$$

It upgrades to  $d$  space. The numerical model can be expressed in the following equations

$$C_x^{dim}(n+1) = C_{best}^{dim} + rand.(C_{best}^d(n) - C_x^d(n) + \alpha C_{best}^{dim}(n) - C_x^{dim}(n)). \quad (5)$$

$$C_x^{dim}(n+1) = C_{best}^{dim} + rand.(C_{best}^d(n) - C_x^d(n) + \alpha C_{best}^{dim}(n) - C_x^{dim}(n)) \quad (6)$$

$$A = 2E^{rand1 \frac{T-t+1}{T}} \cdot \sin(2\pi rand1) \quad (7)$$

Whereas  $\alpha$  denotes the weight coefficient,  $T$  demonstrates the higher volume of iterations, and  $rand1$  illustrates the random number within  $[0, 1]$ . Each individual explores the novel position from existing optimal one by allocating a new position from the searching area. This method has been very focused on MRFO for finishing broader global searching; it can be expressed as follows:

$$C_r^{dim} = LB^{dim} + rand(UB^{dim} - LB^{dim}) \quad (8)$$

Now  $LB$  and  $UB$  denote the lower and upper limits.

### Somersault Foraging

Each MR proposes to move and somersault to novel position. Thus, it exploits the position and generates good locations. The arithmetical expression can be given in the following:

$$C_x^{dim}(n+1) = C_x^{dim}(n) + som.rand2.(C_{best}^{dim}(n) - rand3C_x^{dim}(n)) \quad (9)$$

Whereas  $som$  denotes the somersault factor which chooses a somersault threshold of MR and  $Som = rand2$  and  $rand3$  define 2 random numbers within  $[0, 1]$ . Thus, the time difficulty of MRFO is given by:

$$O(MRFO) = O(T (Ochainforaging + Ocycloneforaging + OSomersaultforaging)) \quad (10)$$

Here  $T$  denotes the greater volume of iterations.

## 2.2 Process involved in TAMRFO-SR Model

To determine an optimum group of routes, the dimensional of MRFO is initiated that is equivalent to CH, and more place was located from the BS. Let,  $\theta^i = (\theta_1^i, \theta_2^i | \theta_{p+1}^i)$  is a  $i^{th}$  MR,  $\theta_{n_i}^i$  represents the real value lies from the interval of zero and one. Afterward, the provided function was utilized for determining the succeeding hop to target and is determined as [17]:

$$f(x) = \{i, for\ which\ \left| \left( \frac{i}{k} - X_{i,j} \right) \right| \text{ is minimum}, \forall_i 1 \leq i \leq k \quad (11)$$

The intention is for determining an optimum group of routes in CHs to target consuming a FF having 2 parameters such as energy as well as distance. In the beginning, the trust level is used and the node with highest trust was preserved as relay node. The primary sub-objective  $f1$  was offered as:

$$f1 = \sum_{i=1}^m TL_{CHi} \quad (12)$$

Moreover, Euclidean distance was executed for resolving the distance in CHs to target. The minimized energy dissipation was mostly depended on the broadcast distance. Therefore, the next sub-objective by mean of distance is  $f_2$  that is signified as [18]:

$$f_2 = \frac{1}{\sum_{i=1}^m dis(CH_i, NH) + dis(NH, BS)} \tag{13}$$

The aforementioned sub-objectives were summarizing as to a FF as provided under in which  $\alpha_1$  and  $\alpha_2$  indicates the weighted allocated to all the sub-objectives.

$$Fitness = \alpha_1(f_1) + \alpha_2(f_2), \text{ where } \sum_{i=1}^2 \alpha_i = 1, \alpha_i \in (0,1); \tag{14}$$

### 3. Result Analysis

Table 1 and Fig. 3 offer a detailed average residual energy (ARE) examination of the TAMRFO-SR model with recent models [19]. The experimental outcome showcased that the TAMRFO-SR model has gained increased ARE under all rounds. For instance, with 25 rounds, the TAMRFO-SR model has given higher ARE of 0.993J whereas the Leach, TCBMA, and BTWSN models have obtained lower ARE of 0.897J, 0.924J, and 0.966J respectively. Also, with 150 rounds, the TAMRFO-SR model has given higher ARE of 0.799J whereas the Leach, TCBMA, and BTWSN models have obtained lower ARE of 0.526J, 0.642J, and 0.755J respectively. Concurrently, with 250 rounds, the TAMRFO-SR model has given higher ARE of 0.642J whereas the Leach, TCBMA, and BTWSN models have obtained lower ARE of 0.337J, 0.472J, and 0.551J correspondingly.

Table 1: Average residual energy analysis of TAMRFO-SR technique with distinct count of rounds

Average Residual Energy				
No. of Rounds	Leach	TCBMA	BTWSN	TAMRFO-SR
0	1.000	1.000	1.000	1.000
25	0.897	0.924	0.966	0.993
50	0.848	0.878	0.924	0.956
75	0.762	0.819	0.851	0.910
100	0.661	0.760	0.826	0.833
125	0.561	0.693	0.755	0.819
150	0.526	0.642	0.755	0.799
175	0.499	0.625	0.718	0.784
200	0.448	0.553	0.647	0.750
225	0.398	0.504	0.585	0.701
250	0.337	0.472	0.551	0.642

Table 2 and Fig. 4 offer a detailed maximum communication over head (MCOH) examination of the TAMRFO-SR model with recent models. The experimental outcome showcased that the TAMRFO-SR model has gained increased MCOH under all nodes. For instance, with 50 nodes, the TAMRFO-SR model has given higher MCOH of 1665899 packets whereas the Leach, TCBMA, and BTWSN models have obtained lower MCOH of 1078341, 13887097, and 7541475 packets correspondingly. Followed by, with 1500 nodes, the TAMRFO-SR model has given higher MCOH of 1195853 packets whereas the Leach, TCBMA, and BTWSN models have obtained lower MCOH of 4721198, 6248848, and 2958525 packets respectively. Eventually, with 2500 nodes, the TAMRFO-SR model has given higher MCOH of 2841014 packets whereas the Leach, TCBMA, and BTWSN models have obtained lower MCOH of 13182028, 14357143, and 6718894 packets correspondingly.

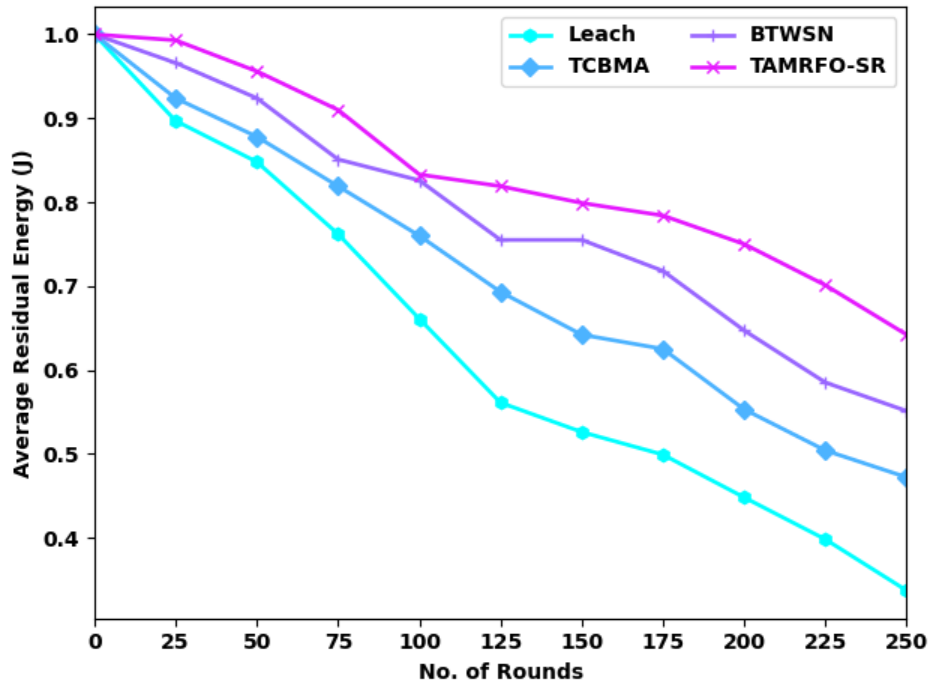


Figure 3: ARE analysis of TAMRFO-SR technique with distinct count of rounds

Table 2 :Maximum communication over head analysis of TAMRFO-SR technique with distinct count of nodes

Maximum Communication Over Head (Packets)				
No. of Nodes	LEACH	TBCMA	BTWSN	TAMRFO-SR
50	1078341	13887097	7541475	1665899
250	960829	11771889	5896313	1313364
500	1078341	8246544	3663594	725806
750	960829	6131336	2253456	725806
1000	2605991	3311060	1900922	960829
1250	3193548	5073733	2488479	725806
1500	4721198	6248848	2958525	1195853
1750	6601382	7894009	3781106	1313364
2000	8599078	9539171	4133641	1665899
2250	10596774	11654378	4956221	2253456
2500	13182028	14357143	6718894	2841014

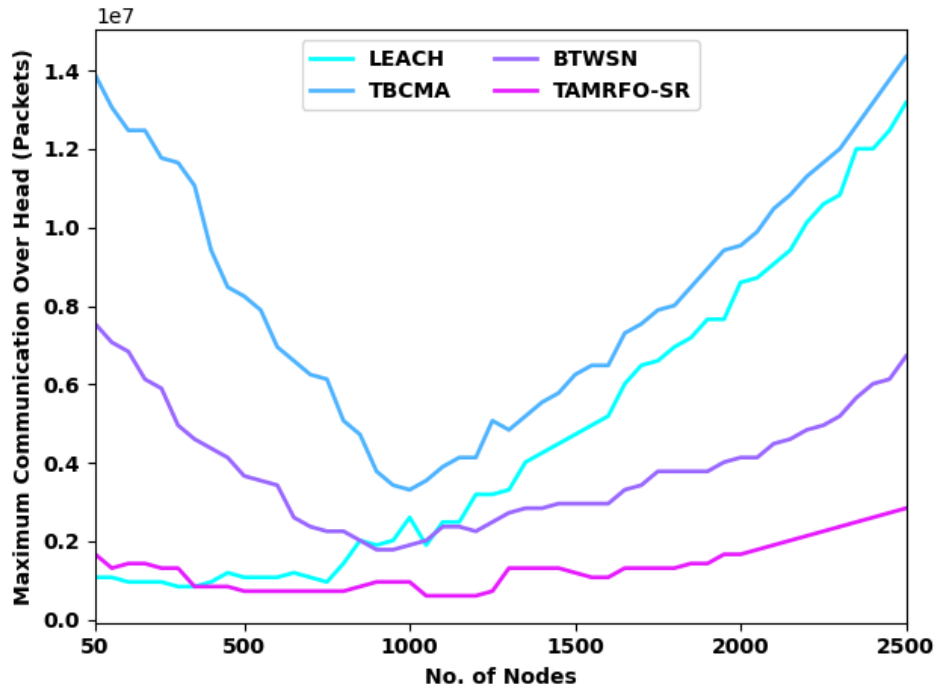


Figure 4: MCOH analysis of TAMRFO-SR technique with distinct count of nodes

Table 4: Number of alive nodes analysis of TAMRFO-SR technique with distinct count of rounds

No. of Alive Nodes (%)				
No. of Rounds	Leach	TCBMA	BTWSN	TAMRFO-SR
0	100.00	100.00	100.00	100.00
25	100.00	100.00	100.00	100.00
50	100.00	100.00	100.00	100.00
75	100.00	100.00	100.00	100.00
100	83.78	96.35	99.80	100.00
125	79.10	86.74	95.86	98.32
150	71.95	77.62	87.72	98.08
175	61.11	65.54	77.62	91.67
200	42.63	47.55	54.70	79.59
225	29.32	34.99	38.93	62.09
250	17.73	22.66	32.77	48.54

Table 3 and Fig. 5 offer a detailed number of alive nodes (NOAN) examination of the TAMRFO-SR model with recent models. The experimental outcome showcased that the TAMRFO-SR model has gained increased NOAN under all rounds. For instance, with 100 rounds, the TAMRFO-SR model has given higher NOAN of 100% whereas the Leach, TCBMA, and BTWSN models have obtained lower NOAN of 83.78%, 96.35%, and 99.80% respectively. Likewise, with 150 rounds, the TAMRFO-SR model has given higher NOAN of 98.08% whereas the Leach, TCBMA, and BTWSN models have obtained lower NOAN of 71.95%, 77.62%, and 87.72% correspondingly. At last, with 250 rounds, the

TAMRFO-SR model has given higher NOAN of 48.54% whereas the Leach, TCBMA, and BTWSN models have obtained lower NOAN of 17.73%, 22.66%, and 32.77% respectively.

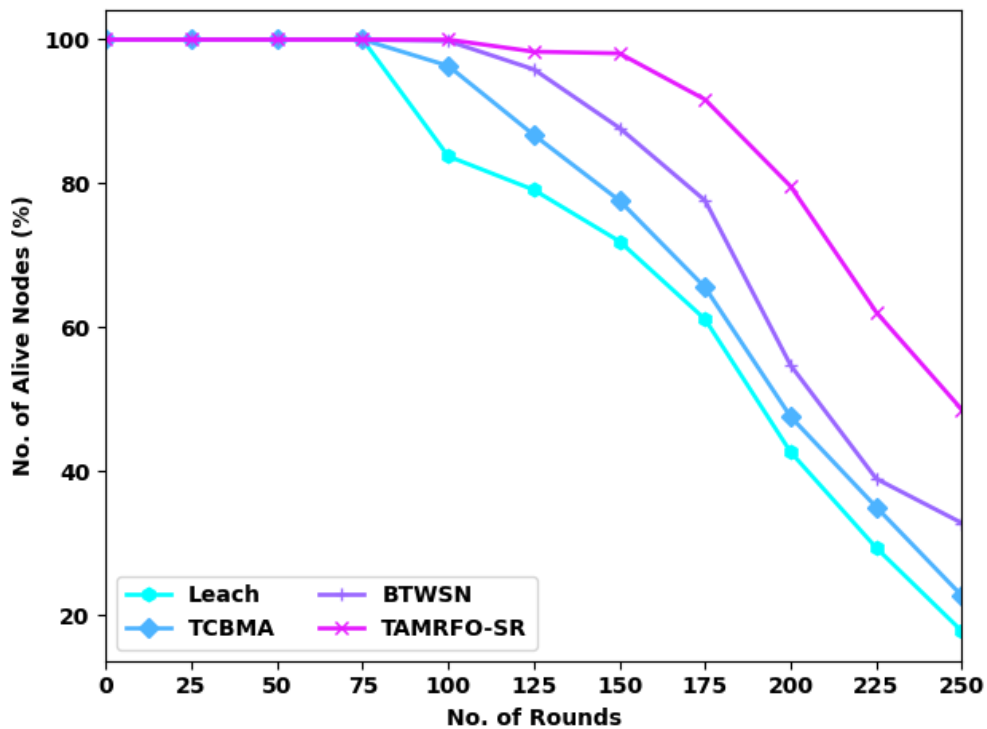


Figure 5: NOAN analysis of TAMRFO-SR technique with distinct count of rounds

A detailed number of dead nodes (NODN) investigation of the TAMRFO-SR model with recent models is given in Table 4 and Fig. 6. The experimental outcome implied that the TAMRFO-SR model has provided lower NODN over the other ones. For instance, with 100 rounds, the TAMRFO-SR model has provided least NODN of 0 whereas the leach, TCBMA, and BTWSN models have offered increased NODN of 20, 13, and 4 respectively. Also, with 250 rounds, the TAMRFO-SR model has provided least NODN of 51 whereas the leach, TCBMA, and BTWSN models have offered increased NODN of 82, 77, and 67 correspondingly. These results ensured the enhancements of the TAMRFO-SR model over other methods.

Table 4: Number of dead nodes analysis of TAMRFO-SR technique with distinct count of rounds

No. of Dead Nodes (%)				
No. of Rounds	Leach	TCBMA	BTWSN	TAMRFO-SR
0	0	0	0	0
25	0	0	0	0
50	0	0	0	0
75	0	0	0	0
100	16	3	0	0
125	20	13	4	1
150	28	22	12	2
175	39	34	22	8
200	57	52	45	20
225	71	65	61	38
250	82	77	67	51

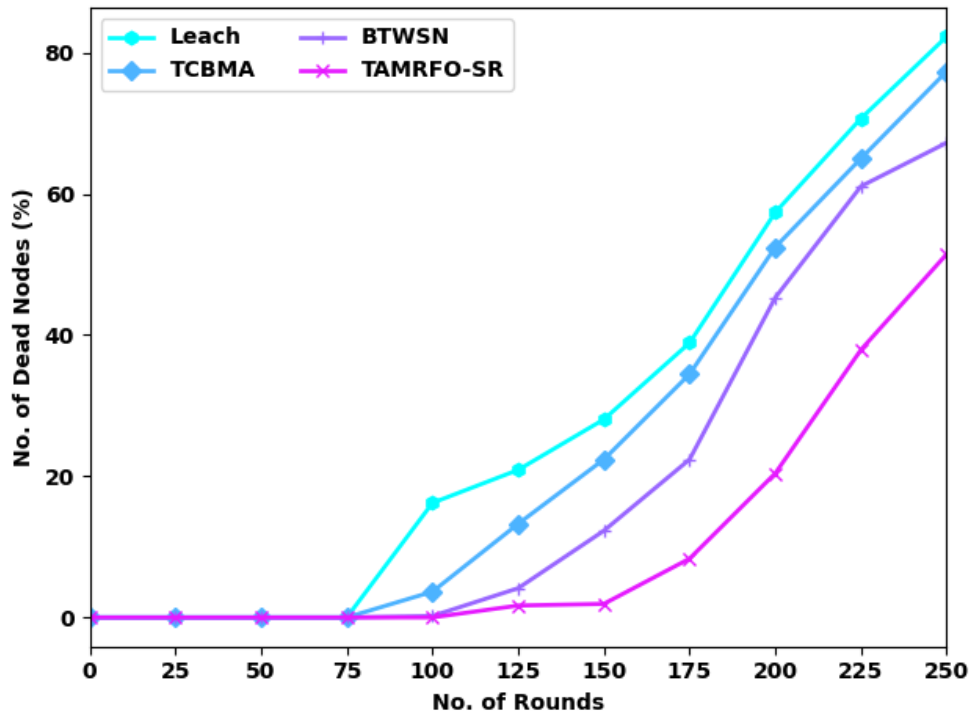


Figure 6 :NODN analysis of TAMRFO-SR technique with distinct count of rounds

#### 4. Conclusion

In this study, a new TAMRFO-SR model has been developed to accomplish optimal and secure routes for WSN. In addition, the TAMRFO-SR model is mainly stimulated by the fascinating characteristics of manta rays. Besides, the TAMRFO-SR model derives a fitness function with multiple parameters for secure route selection process. Moreover, the inclusion of trust in the route selection process assists in accomplishing enhanced security. The design of TAMRFO-SR model for secure data transmission depicts the novelty of the study. The experimental validation of the TAMRFO-SR model demonstrates better performance over the other approaches. Thus, the TAMRFO-SR model has resulted in superior outcomes over the other methods. In future, data aggregation and compression models can be included to improve network efficiency.

#### References

- [1] Arjunan, S. and Sujatha, P., 2018. Lifetime maximization of wireless sensor network using fuzzy based unequal clustering and ACO based routing hybrid protocol. *Applied Intelligence*, 48(8), pp.2229-2246.
- [2] Khot, P.S. and Naik, U., 2022. Taylor CMVO: Taylor Competitive Multi-Verse Optimizer for intrusion detection and cellular automata-based secure routing in WSN. *International Journal of Intelligent Robotics and Applications*, pp.1-17.
- [3] Meena, U. and Sharma, P., 2022. Secret Dynamic Key Authentication and Decision Trust Secure Routing Framework for Internet of Things Based WSN. *Wireless Personal Communications*, pp.1-29.
- [4] Arjunan, S. and Pothula, S., 2019. A survey on unequal clustering protocols in wireless sensor networks. *Journal of King Saud University-Computer and Information Sciences*, 31(3), pp.304-317.
- [5] Awan, S., Javaid, N., Ullah, S., Khan, A.U., Qamar, A.M. and Choi, J.G., 2022. Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks. *Sensors*, 22(2), p.411.
- [6] Rajasoundaran, S., Prabu, A.V., Routray, S., Malla, P.P., Kumar, G.S., Mukherjee, A. and Qi, Y., 2022. Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks. *Computer Communications*, 187, pp.71-82.
- [7] Taranath, N.L., Roopashree, H.R., Yogeesh, A.C., Darshan, L.M. and Subbaraya, C.K., 2022. Design and Development of Efficient Secure Routing Mechanism for Wireless Sensor Network. In *Energy Conservation Solutions for Fog-Edge Computing Paradigms* (pp. 233-266). Springer, Singapore.
- [8] Upeksha, R.G.C. and Pamarathne, W.P.J., 2022. Ant Colony Optimization Algorithms for Routing in Wireless Sensor Networks: A Review. *Recent Advances in Electrical and Electronic Engineering and Computer Science*, pp.47-57.

- [9] Arjunan, S. and Pothula, S., 2019. A survey on unequal clustering protocols in wireless sensor networks. *Journal of King Saud University-Computer and Information Sciences*, 31(3), pp.304-317.
- [10] Famila, S., Jawahar, A., Sariga, A. and Shankar, K., 2020. Improved artificial bee colony optimization based clustering algorithm for SMART sensor environments. *Peer-to-Peer Networking and Applications*, 13(4), pp.1071-1079.
- [11] Thangaramya, K., Kulothungan, K., Indira Gandhi, S., Selvi, M., Santhosh Kumar, S.V.N. and Arputharaj, K., 2020. Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN. *Soft Computing*, 24(21), pp.16483-16497.
- [12] Khot, P.S. and Naik, U., 2021. Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection. *Wireless Personal Communications*, 119(3), pp.2405-2429.
- [13] Lazrag, H., Chehri, A., Saadane, R. and Rahmani, M.D., 2021. Efficient and secure routing protocol based on Blockchain approach for wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 33(22), p.e6144.
- [14] Alotaibi, M., 2021. Improved Blowfish Algorithm-Based Secure Routing Technique in IoT-Based WSN. *IEEE Access*, 9, pp.159187-159197.
- [15] Zhao, W., Zhang, Z. and Wang, L., 2020. Manta ray foraging optimization: An effective bio-inspired optimizer for engineering applications. *Engineering Applications of Artificial Intelligence*, 87, p.103300.
- [16] Houssein, E.H., Emam, M.M. and Ali, A.A., 2021. Improved manta ray foraging optimization for multi-level thresholding using COVID-19 CT images. *Neural Computing and Applications*, 33(24), pp.16899-16919.
- [17] Elhoseny, M., Rajan, R.S., Hammoudeh, M., Shankar, K. and Aldabbas, O., 2020. Swarm intelligence-based energy efficient clustering with multihop routing protocol for sustainable wireless sensor networks. *International Journal of Distributed Sensor Networks*, 16(9), p.1550147720949133.
- [18] Vaiyapuri, T., Parvathy, V.S., Manikandan, V., Krishnaraj, N., Gupta, D. and Shankar, K., 2021. A novel hybrid optimization for cluster-based routing protocol in information-centric wireless sensor networks for IoT based mobile edge computing. *Wireless Personal Communications*, pp.1-24.
- [19] Sahoo, R.R., Sardar, A.R., Singh, M., Ray, S. and Sarkar, S.K., 2016. A bio inspired and trust based approach for clustering in WSN. *Natural Computing*, 15(3), pp.423-434.