ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 7, Issue 11, November 2020

# Secured Non Cluster Whale Swarm Optimization for WSN

[1] Syed Mohd Ali, [2] Syed Abdul Sattar, [3] D. Srinivasa Rao
[1] Research Scholar, JNTU-Jawaharlal Nehru Technological University, Hyderabad, Telangana, India
[2] Principal, NSAKCET- Nawab Shah Alam Khan College of Engineering and Technology, Hyderabad, Telangana, India
[3] Professor, Electronics and Communication Engineering Department, JNTU- Jawaharlal Nehru Technological University, Hyderabad, Telangana, India

**Abstract: The developments of the Wireless Sensor Network (WSN) have made it popular in a large number of applications. In the WSN setting, however, security is a key challenge as the cluster of sensor nodes in the network faces several problems with the information that makes it difficult to estimate the distance through BS to other node numbers by using distance rate, and it becomes difficult to determine the neighbor list. For such a limited range, most sensor networks will just have to send the data to only the corresponding CH and NCH, the network faces several problems that can lead to security breaches. We suggested a protected whale swarm optimization model (S-WSA) based on two trust factors to solve this problem; the first is a network model that provides routing hops, and the next is a security model that provides a routing protocol multi-objective. Therefore, simulation is achieved by considering two confidence metrics, making our model a stable model.**

**Keywords: WSNs, CH, NCH security model, network model, multi objectives.**

## I. INTRODUCTION

The Wireless Sensor Network (WSN)[1] is capable of actually perceiving objects for observing and gradually communicating data. WSN has the characteristic of ease of maintenance, easy improvement, and highly reliable. We were largely made up of wireless sensors, lightweight, inexpensive as well as energy-limited environmental monitoring but also communication devices [2]. The protection device as well as visual detectors could be utilized to create an overlay network to detect encroachments. Mini detectors may be used to track detection accuracy as well as diagnostic devices. The connection here between nodes of the detector as well as the access point is costly when there are no high-energy networks where contact may continue. Dependable energy audit becomes critical for such a range of business including defense applications [3]. Such a system includes much life of the network constraints, like computing capacity, storage, including receiver capacity. Safety was described mostly as a core problem throughout the architecture as well as the management of such systems.

The clustering strategy decreases the number of radio transmissions and increases the lifespan of the sensor network. As a result, the clustering technique can dynamically adjust the lifetime of different sensor applications such as network performance, lower energy consumption, fault tolerance, reliability, and low latency. The concept of clustering is like grouping the network into many clusters, and the cluster head (CH) is selected to be one node in each cluster. Communication between the networks inside the groupings including processing for its information, which is also referred to that as inter-cluster synchronization, was carried around by the cluster head (CHs) but also an interaction between outside group monitors was referred to only as multi-hop communication. Throughout grouping, most detectors around the system were clustered across groups, including one with a cluster head (CH) detector, cluster members (CM), and non-cluster members (NCM). The grouping head function is cluster management; cluster members collect data and send it to the base station (BS). Several algorithms for clustering have been introduced in the wireless sensor network in recent years. Based on the Base Station location, we estimated the distance across BS to other numbers of nodes, using distance rate, and we determine the neighbor list. Throughout comparison, because most sensor networks would only have to send the information to just the corresponding CH for such a small range, the network faces many issues that can lead to security breaches [4].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 7, Issue 11, November 2020

Secured route selection must be done from Non-cluster Member (NCM) to Cluster head (CH); Cluster head (CH) to Base station (BS). Thus, dynamic multipath clustering must be designed to improve the secured efficiency of cluster selection by using Whale swarm optimization for non-cluster members selection must be made from Non-Cluster Member (NCM) to Cluster Head (CH); Cluster Head (CH) to Base Station (BS). This can be done with a Whale optimization for non-cluster members, which is a global technique of optimization [5] based on the optimization models. Whale optimization for non-cluster members tends to optimize many elements in designing network routes. Whale optimization for non-cluster members is suitable for Data Network routing and high performance. Thus, our model for Whale optimization for non-cluster member's optimization can simplify the routing problem [6]. Certain limitations of cluster quality, energy bandwidth, and average inter-cluster distance are defined throughout this paper which analyzes the reliability

## 2. RELATED WORK

Because CH nodes play a larger role throughout the hierarchical WSN system relative to regular nodes in a network. As a consequence, the efficient implementation of the system implies the existence of such installed. Present grouping algorithms, For example, Low Energy Adaptive Clustering Hierarchy (LEACH), Thresholds Responsive Energy Efficient sensor Network (TEEN), Hybrid Energy Efficient Distributed (HEED) including Responsive Thresholds Responsive efficient System were known to be among the most successful algorithms to enhancing energy efficiency [1]. Investigators working on many nature-inspired algorithms including computational intelligence strategies to saving energy in WSNs [2][3].

Crosby et al.[4] suggested the geographic routing framework dependent by confidence for such a collection of trusted entities named CHs. Such activity is designed that discourages the fraudulent but also infected nodes about being chosen as that of the head node. Such a trust-based program accurately manages targeted activity through encouraging the SNs can exchange the integrity-related information they obtain through the corresponding head nodes.

The credibility-based trust method was constructed in [5] like an expansion of the decentralized trust-based system (mentioned previous section). Throughout this trust-based reference implementation, that SN provides a list of the project assets of its neighbor node for the collection of trusted nodes with CHs.

Trust-based Low-Energy Adaptive Cluster Hierarchy (LEACH) proposed by Song et al.[6] would be an enhancement to just the traditional LEACH protocol to create stable but also trusting relationships between nodes on the network. The author has suggested a simple contextual confidence formative assessment by combining the trust organizational structure only with a confidence-based routing element.

The respect-based approach proposed through Bao et al.[7] recognizes either QoS confidence including mutual cohesion to fault current network nodes. Fairness, resources, but also co-operation were considered for elements of trust. BS chooses CHs first as well as a network monitoring system is used by the chosen CH nodes to determine the stability of the SNs in its cluster. The efficacy of the suggested remote monitoring method is analyzed through designing a theoretical framework focused around stochastic Petri nets.

Duan et al.[8] completed the energy-aware confidence deviation mechanism in 2014 that compels IoT security using a game-theoretical approach. The operation amongst these networks was a step - up by the model of the strategic plan. The workload in the network resulting from the confidence deviation scheme was minimized by the theoretical approach to the game. Also, from the simulation results that have been obtained, the leading output of the trust deviation method has been accredited.

The hotspot problem can be effectively solved by grid-based protocols such as the EEBCDA (Energy Efficient and Balanced Cluster-Based Data Aggregation Algorithm)[7] and the EEBCDA Multi-Hop[8]. An enhancement based on EEBCDA is Multihop EEBCDA. This divides the network area into several rectangles, each of which has a compared to the average of grids, and the nodes in each row form a cluster. This strategy dramatically reduces the amount of energy consumption and increases the lifespan of the network. And although the number of grids is an incoherent per rectangle, excessive forwarding between all the layers is taking place. There is a situation where the upper layer nodes expired and data cannot be transmitted by the lower layer nodes that means a lot of energy waste.

The enhanced channel-aware routing protocol (E-CARP) was developed in 2016 by Zhou et al.[9] to produce and use the underwater internet. The major goal of the analysis was to achieve a system with cost-effective data transmission and reduced energy consumption. In the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 7, Issue 11, November 2020

traditional PING-PONG solution, the drawbacks occurred and Carp was resolved through this developed framework. EEMRP[10] proposed a grid clustering algorithm for the distribution of multi-hop data transmission through clustering and proposed communication management (CM) nodes. This technique efficiently tries to maintain the network's energy consumption, because the CM nodes share the CH nodes ' workload.

## 3. PROPOSED METHODOLOGY

In this section, using the newly developed optimization algorithm, the security-aware multi-hop routing protocol based on multiple objectives in WSN is illustrated. A trust model is used here, taking into account different trust factors, along with direct trust, indirect trust, integration factor, and forward rate factors, along with other parameters, including distance, delay, intra-cluster distance, the lifetime of interaction, energy, and distance between clusters. The trust model for providing the network with high security is included. Then, the proposed protected whale swarm algorithm (SM-WSA) performs the multihop routing. To perform security-aware multi-hop routing in WSN, the proposed Protected Whale Swarm Algorithm (SM-WSA) and the multi goals are used. The two measures for multihop routing are considered. In the first step, with all the routing maps, CH is selected using the configured network protocol to obtain the optimal CH. The second stage is then advanced by the safety model on the planned multi-objective that protects our model. Fig. Fig. 1 displays a schematic diagram using the Whale Swarm Algorithm (S-WSA) for the proposed Secured Model

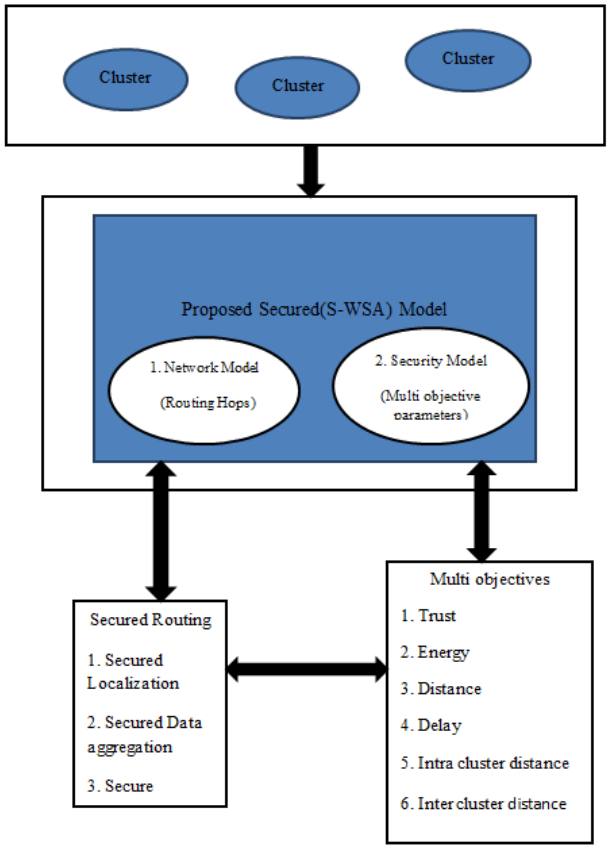


**Figure: Proposed Secured Model using whale Swarm Algorithm (SM-WSA)**

### 3. 1 NETWORK MODEL

In this paper, the proposed protocol is to provide great command of cluster heads and better scalability for network environments of various sizes and to effectively improve energy efficiency for WSNs. The clustering method, the selection algorithm for CH nodes, and the routing algorithm are mostly considered to protect the network model and extend the network lifetime.

The sensor nodes are all homogeneous.

When deployed to the field all nodes are stationary.

A single base station is placed.

All nodes have the transmitting data.

Uses the routing source. Routing in this Procedure covers path exploration and path maintenance.

A route discovery process is started by the source node, with route request and route reply (RREP) messages in this step.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 7, Issue 11, November 2020

Only the destination node may answer with a Route Reply (RREP) message to the source node. Used to shorten nodes between source and destination.
Provide multiple data paths for reaching the destination, resulting in load balancing, low latency, and better network performance.
In case of failure of any route, the multiple routing protocols also provide an alternate path.

### 3.2 CLUSTER CREATION AND FORMATION

Cluster-based architectures make more efficient use of resources and cluster creation includes cluster members (CM), cluster heads (CH), and non-cluster heads (NCM). A structured head node manages this grouping of nodes known as Cluster Head (CH) which manages the cluster, collects data from cluster members, and sends data to the base station (BS). A Cluster Head (CH) is chosen by weight that may correlate to the capacity of a node to conduct additional responsibilities such as near base station (BS), no neighbors. It can be calculated by considering factors like node residual energy with parameters cluster member (ID), Neighbor node (neighbor I d, cluster head IP), and neighbor cluster (NCH-IP, cluster gateway-IP). Based on the site of the Base Station, we calculated the distance through BS to other node numbers, using distance values, we determined the neighboring list. To determine the clusters in mathematical representation we consider the multi-object function of a network.
Following the method means the query is called Expectation-Maximization.
The E-step assigns data points to the cluster nearest to them.

$$\frac{\partial y}{\partial x} = \sum_{i=1}^{m}\sum_{k=1}^{K} ||x^i - \mu_k||^2$$

$$= w_{ik} = \begin{cases} 1 \; if k = argmin_j ||x^i - \mu_j||^2 \\ 0 \; otherwise. \end{cases} \text{---------- (1)}$$

The M-step shall compute every cluster's centroid.

$$\frac{\partial y}{\partial x} = 2\sum_{i=1}^{m} w_{ik}(x^i - \mu_k) = 0$$

$$= \mu_k = \frac{\sum_{i=1}^{m} w_{ik} x^i}{\sum_{i=1}^{m} w_{ik}} \text{---------- (2)}$$

Below is a description of how mathematically we can solve that.
The multi-objective function of it is:

$J = \sum_{i=1}^{m}\sum_{k=1}^{k} w_{ik}||x^i - \mu_k||^2$ ---------- (3)

Where $w_{ik}$ =1 belongs to cluster k, for data point xi; and again that, $w_{ik}$ =0. $\mu_k$ is also the centroid of a cluster of $x^i$. It's a two-part minimization issue. About $w^{ik}$, we first reduce J and treat $\mu_k$ set. Then we minimize J about $\mu_k$, and fix $w_{ik}$. Practically speaking, we first distinguish J w.r.t.$w_{ik}$, and update cluster assignments (E-step). After the cluster assignments from the previous step (M-step), we then separate J w.r.t.$\mu_k$and recalculate the centroid. In certain words, apply the data point xi to the nearest cluster determined by the total amount of its distance from the centroid of a cluster is being squared.

$\frac{1}{m_k}\sum_{i=1}^{m_k} ||x^i - \mu_{c^k}||^2$ ---------- (4)

### 3.3 CLUSTER HEAD (CH) SELECTION

Cluster head selection mainly contains the following parameters Clusterhead (CH) →(cluster member IP), Neighbor node→ (neighbor node IP, cluster head IP), and Neighbor cluster→ (NCH IP, cluster gateway IP). Cluster selection of dynamic multipath routing protocol performs few
computational works to measure the energy consumption ratio (ECR) for each selection of the cluster heads:

$ECR\ (m) = \frac{E_0}{E_0 - E_r}$ ----------(5)

DMPRP calculates their residual energy transmission rati o (RETR) after calculating the ECR:

$RETR\ (m) = \frac{E_r}{ECR X d_{toBS}}$ ---------- (6)

Where$d_{toBS}$ is a distance of CLN$m$ from BS. If we add the ECR equation,theRETRwillbe

$RETR\ (m) = \frac{E_r}{E_0/(E_0 - E_r) X d_{toBS}}$ ---------- (7)

When ECR and RETR are determined for the current round, DMPRP calculates the combined value of the ECR and RETR nodes over a certain duration of the instance. Because the rate of energy consumption is power p= $E_{r/T}$, the Riemann sum is used by the total power degenerate over time. This ECR may be determined as an approximation overtime period of an instance (Einstance).

$E_{instance} - ECR = \sum_{r=0}^{R_{instance}} p(t_i)\Delta t_i$ ---------- (8)

Where$E_{instance}$-ECR is exclusively ECR.The energy consumption incorporated over some time

$E_{instance} - ECR = \int_{r=0}^{R_{instance}} p(t)dt$.---------- (9)

Likewise, DMPRP calculates the previous instance RETR to the above equations; thus BS selects a set of appropriate nodes with the lowest energy consumption and optimum residual energy. Also, the distance factor plays a role to choose a CLN as a CH node for the node in

ISSN (Online) 2394-2320

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 7, Issue 11, November 2020

the central region. The pseudo-code for the selection of DMPRP CHs is shown below. Such following work-steps reflect the procedure of section CHs indicated by the algorithm.

### 3.4 SECURITY MODEL

In terms of security, WSN apps, such as military systems and medical monitoring systems, are very responsive. Traditional protection mechanisms cannot be used in WSNs because of the limited resources of the sensor nodes. The protection mechanisms of WSNs should therefore be built with limited resources and malicious sensors in mind. To secure any WSNs networks we need to focus mainly on all these factors like secure localization: is the process that sensors can obtain their locations in the presence of malicious attacks. Secure data aggregation: The secure data aggregation technique is for improving the security and focusing on the attacks that make the aggregation highly vulnerable Secured routing: The protocols designed to combat routing attacks that interrupt route discovery are reliable routing protocols in ad hoc networks.

### 3.5 SELECTION OF CLUSTER HEAD (CHs) AND NON CLUSTER HEAD (NCHs) USING SM-WSO ALGORITHM

1. start
2. Initially, location-awareness of nodes distributes nodesintoCHs
3. $t_o$=threshold valve, and CHs=$t_0$, CHs generate random number say=CHs(x)
4. Calculate CHs probability say P (CHs).
5. CHs(x)== $t_0$
6. if(CHs(x)< $t_0$)
7. select nodes themselves as CHs
8. Else
9. select nodes themselves as NCHs
10. BS computes ECR for CHs from EQ
11. $ECR\ (m) = \frac{E_0}{E_0 - E_r}$
12. BS computes $E_{instance}$-ECR from equation $E_{instance} - ECR = \int_{r=0}^{R_{instance}} p(t)dt.$
13. Generate potential (CHS)
14. The base station finally selects the $P\times$ CHs or $P\times$ NCHs as CHs for the best selection.
15. stop

### 3.6 PARADIGM BY SECURED NON CLUSTER WHALE SWARM OPTIMIZATION ALGORITHM (SNC-WSOA)

INPUT- MULTI OBJECTIVE PARAMETERS, WHALE SWARM (Ω)

OUTPUT- THE MULTIPLE OBJECTIVE OPTIMIZATIONS

1. Start
2. Trust, energy, distance, load, delay, inter-cluster distance, intracluster distance initialization parameters.
3. Place initialization of whales
4. The fitness qualities of all whales are measured.
5. Conduct do when terminating the loop
6. For (j=1) to the location of the WHALE SWARM |Ω|; do (j=1)
7. Get the location of the nearest and finest whale, say as Z of $\Omega_j$;
8. Where there is the nearest and finest whale position (Z);
9. The position of the whale (Z) will shift under the equation direction-(3)
10. The WHALE SWARM calculation ((Ω))
11. If the loop ends
12. For ending loops
13. while loop ends
14. Reverse the optimization of Multi-Goal

End

The popular SNC-WSOA paradigm is developed using multi-objective cluster head selection parameters. We portray the variables, positions of whales, etc. here. While moving through any iteration, as seen in the algorithm, each whale needs to find its " best and nearest " multi-objective optimization' whales.

### 3.7 TRANSMISSION DELAYS

In only a packet switching based device, the average time required to drive the bit of a whole packet was transmission length, this would be the delays caused by a data rate. Delay transmission is a packet length vector and has nothing to do with the spectrum of both networks. The delays are often nearly equal to the length of the packet in proportion,

It is given by the following formula:

$T_d = \frac{NB}{RT}(seconds)$ ---------- *(10)*

Where in seconds, Td = transmission delays

NB = Bit Number

RT= rate of transmittance

ISSN (Online) 2394-2320

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 7, Issue 11, November 2020

Take into account the two machines that can send data packets at different speeds and thus have different delays in transmission. The transmission delays are defined as:
Let us assume that transmission delays for two devices are distributed geographically and separately with parameters μ1 Δt and μ2 Δt respectively, as 1 and 2.
The probability that it takes X time slots to transmit a packet by device 1 is given as.
The likelihood that the transmission of a packet by device 1 needs X time slots is given as

$P\ (d_{tr,1} = X\Delta_t) = \mu_1\Delta_t(1-\mu_1\Delta_t)^{X-1},\ X=1,2,3....$ ---------- *(11)*

The likelihood that the transmission of a packet by device 1 needs X time slots is given as

$P\ (d_{tr,2} = X\Delta_t) = \mu_2\Delta_t(1-\mu_2\Delta_t)^{X-1},\ X=1,2,3....$ ---------- *(12)*

Say that a time t0 begins sending a packet at system 1 and the likelihood of sending the packet at a time = t0 +Δt
Evaluate the possibility

$P\ (t_0 + d_{tr,1 \le t0} + \Delta_t) = P(d_{tr,1} \le \Delta_t)$ ---------- *(13)*

Where $d_{tr}$ is the transmission delay of the packet

$P\ (d_{tr,1} \le \Delta_t) = P(d_{tr,1} = \Delta_t) = \mu_1\Delta_t$ ---------- *(14)*

So equal Probability (dtr, 1 = X Δ t) P (dtr,1 = X Δ t) is that in P(dtr,1 = X Δ t) P(dtr,1 = XΔt) opportunity, it takes XX times to transmit the entire packet itself through system 1. (Failure to send a packet (X-1) (X-1) twice and failure to send it for the last time ΔX-1 +1 = X-1 +1 = X)

$P\ (t_0 + d_{tr,1 \le t0} + \Delta_t) = P(d_{tr,1} \le \Delta_t)$ ---------- *(15)*

- Where t0 ————->time transmission starts;
- dtr,1dtr,1 ————->transmission packet delay time;
- $\Delta_t\Delta_t$ ————->One time slot length;
- t0+dtr,1 ————->time of arrival of the packet;
- t0+dtr,1 ————- > transmission time + pause in transmission;
- t0 + Δt ————- > the latest packet arrival time;
- t0 + t ————— > transmission period + one time slot;
- {t0+dtr,1, Δt0 + Δ1}{t0+dtr,1, Δ t0 + Δ 1} is the case that packets are delayed after transmission starts no later than one slot. We're looking at the likelihood of this occurrence.
- Dtr,1 Δ 1}{dtr,1 Δ 1} is a case in which the packet is not delayed by more than a one-time slot.

$\therefore P\ (t_0+d_{tr,\ 1\le t0} + \Delta_t) = P\ (d_{tr,1} \le \Delta_t\ )$ ---------- (16)

$\therefore P\ (t_0+d_{tr,\ 1\le t0} + \Delta_t) = P\ (d_{tr,1} \le \Delta_t)$ ---------- (17)

We can determine this event's likelihood. This will be the same case since the delay in transmission is probably independent of the transmission time.

### 3.8 PROBABILITY FOR TRANSMISSION LOAD

We can measure the likelihood of these load transmission events if x and y are the active and reactive components of loads at any point. The equation below is described as

$Z_i = S_{Di} = X_i + j_i$ ----------*(18)*

Then, by measuring the moments of transmission loads,

$M_t\ (S_{Di}) + a_i^n S_{Di}{}^1 P_i$ ---------- *(19)*

Where $m_t$=moment of order
$S_{pi}$=load at the particular node
$P_i$=probability of having $S_{pi}$

### 3.9 ALGORITHM FOR BEST AND Closest WHALE Locating

INPUT- WHALE 'S SWARM Location ((Ω)) AND WHALE ((Ωp))
OUTPUT-BEST AND NEAREST WHALE is defined as ((Ωp))

1. start
2. Define variable say int a=0;
3. Define variable say float $b_{tmp}=\infty$;
4. For (j=1) to WHALE SWARM position |Ω|; do
5. If $f(\Omega_j) < f(\Omega_p)$then
6. If $(dis(\Omega_j)f(\Omega_p) < b_{tmp})$ then
7. a=i;
8. $b_{tmp=}\ dis(\Omega_j)f(\Omega_p)$;
9. if loop ends
10. If loop ends
11. For loop ends
12. revert $(\Omega_{a)}$;
13. end

### 3.10 FOR SNC-WSO WHALE SWARM ALGORITHM

INPUT- FUNCTION OBJECTIVE AND WHALE SWARM ((Ω))
OUTPUT- PARAMETERS FOR MULTI OBJECTIVE OPTIMIZATION

1. Start
2. Initialization of parameters
3. Initialization of whales
4. Evaluate the fitness values of all whales

ISSN (Online) 2394-2320

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 7, Issue 11, November 2020

5. Check while termination loop, if not satisfied do
6. For (j=1) to WHALE SWARM position |Ω|; do
7. Get the location of the nearest and finest whale, say as Z of j;
8. If there is a whale position (Z), then
9. Create a copy of the statement R (?? j);
10. R moves according to the above equation for Z
11. R enhance;
12. $\Omega_i$.d=0;
13. If f(R) < f ((Ωi))then f(r) < f (ΩI)
14. I = R;
15. else
16. Verify the iterative counter of the loop (ΩI)
17. If the loop ends
18. Else if
19. Verify the iterative counter of the loop (ΩI)
20. If loop ends
21. For ending loops
22. While loop ends
23. The best multiple optimizations is to check each whale almost
24. MULTI OPTIMIZATION Return
25. end

### 3.11 FOR WHALE 'S ITERATIVE COUNTER ALGORITHM

REQUIREMENTS:

WHALE SOLUTION (S), STABILITY THRESHOLD TS

1. Starting
2. Then if (R.d # Ts)
3. Else
4. R-Multioptimization check;
5. Initialize R with re;
6. R enhance;
7. End If
8. End

### 3.12 ALGORITHM FOR FINDING SNC-WSOA MULTI OPTIMIZATION

REQUIREMENTS:

S SOLUTION (S); THRESHOLD FITNESS ($T_f$); $Multi_{optimization}=f_{mulbest;}$

1. Start
2. If $f(S)<f_{mulbest}$ then
3. If $f_{mulbest-}$ $f(S)>T_f$ then
4. Clear multi $_{optimization;}$
5. end if
6. $f_{globest=}$ f(S);
7. Add S TO multi $_{optimization;}$
8. Else
9. If f(S)---- $f_{mulbest<=}T_f$ then
10. Add S TO multiobjective $_{optimization;}$
11. If loop ends
12. If loop ends

## 4 EXPERIMENTAL MODEL AND PERFORMANCE EVALUATION

In order to determine the efficiency of our proposed model Secured Non-Cluster Whale Swarm Optimization (SNCWSO), we simulate our experiment in Network Simulator Version-2 (NS2). To simulated our proposed model SNCWSO, first we configure a wireless sensor network, by adopting WSN features in NS2, we designed a hybrid WSN model, where we consider a sensor nodes with different energy rates, channel rates and bandwidth rates. All the sensor nodes are randomly scattered in a network and occupied with different wireless sensing features. In this experiment we varied a network with different nodes, topographies, energy rates and communication ranges. The basic idea is, how effectively the proposed model improves the communication efficiency for different scenarios. The below table-1 presents the simulation parameters, and the routing protocol was configured in NS2. The configured protocol was described with SNCWSO features

| | |
|---|---|
| Sensor nodes | 50 to 200 |
| Network Area | 1000 X 1000 |
| Mac Model | 802.11 |
| Radio Range | 250m |
| Total Simulation Time | 200 sec |
| Traffic Source | CBR |
| Packet Size | 512 |
| Receiving Power | 0.395J |
| Transmission power | 0.660J |
| Idle Power | 0.035 |
| Initial Energy | 10.3 J |
| Rate | 2Mbps |
| Protocol | SNCWSP |
| Bandwidth | 2Mbps |

**Table 1: Simulation Settings**

### 4.1 Performance Metrics

In this experiment we considered these following parameters, energy consumed, routing overhead, end-to-end delay, communication delay, and packet delivery

ISSN (Online) 2394-2320

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)

Vol 7, Issue 11, November 2020

ratio to determine the performance of proposed SNCWSO by comparing with

In our first experiment we vary the number of nodes as 50,100,150 and 200. Some of the metrics are as follows which are used for understanding the performance of routing approach and for comparing it with nest-sites selection process based approach NEST[11] and Energy Centers Searching using Particle Swarm Optimization (EC-PSO) [12]. We considered two different scenarios, number of nodes and of number of rounds

Number of nodes-

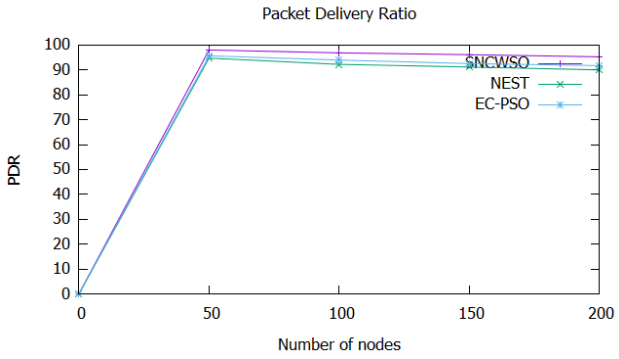


**Fig 4.1 Number of nodes vs Packet Delivery Ratio**

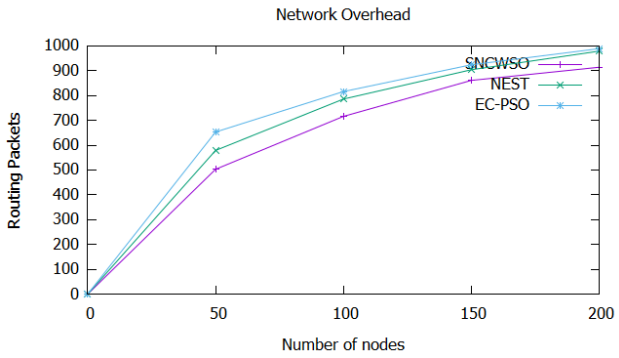


**Fig 4.2 Number of nodes vs Network Overhead**

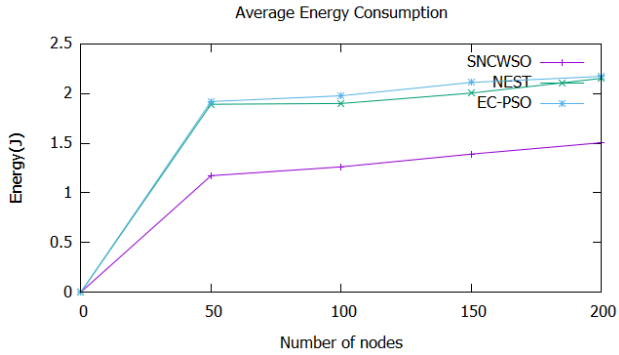


**Fig 4.3 Number of nodes vs Energy Consumption**

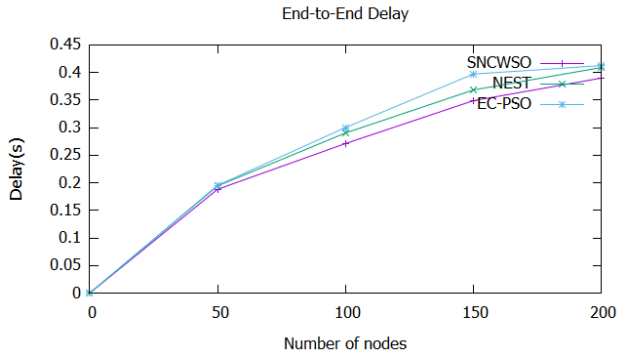


**Fig 4.4 Number of nodes vs End-to-End Delay**

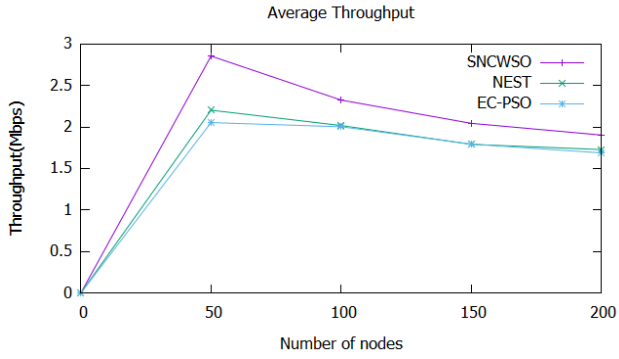


**Fig 4.5 Number of nodes vs Throughput**

The above results demonstrate the performance of proposed protocol SNCWSO, NEST and EC-PSO for different number of nodes. Based on the results the more number of Cluster Heads were taking place to distribute a data from non-cluster members zone to the nearest cluster

head. The energy consumption of overall network varied with respective of number of nodes. The Fig 4.1 Defined the number of packets were successfully distributed to the base station, based on the results the packet delivery ratio was decreased with respective of number of nodes. According to the overhead results which were presented in Fig 4.2 the overhead is increased with respective of number of nodes and rounds. When more number of nodes distributed the data, the more routing was processed which impacts more on control packets.

As per the Fig 4.3 , the energy consumption increased with respective of number of sensors, the cluster head formed a connectivity of non-cluster and cluster members. Based on the energy rate level, the cluster head occupied extra energy, the proposed model optimize the communication by minimizing the routing packets for number of rounds. Fig. 4.4 Presents the end-to-end delay performance comparison of SNCWSO, NEST and EC-PRO based on the results, the proposed protocol SNCWSO end to end delay rate is increased due to the more number of participants and more number of cluster heads, which impact on the packet delay, the overall performance of SNCWSO is 12% less compare to the NEST and EC-PRO. In throughput scenario, the fig 4.5 shown the throughput variation with respective of number of nodes and number of rounds, based on the derived results, the throughput rate was slightly down, while compare to the NEST and EC-PRO the throughput rate was increased with respective of number of packets was passed on over network

## 5. CONCLUSION

The Wireless Sensor Network (WSN) can perceive objects for data observation and incremental communication in reality. WSN has the characteristics of ease of maintenance, fast and highly reliable progress. In the WSN setting, however, safety is a major challenge as the cluster of sensor nodes in the network faces several problems with the information that makes it difficult to estimate the distance through BS to other node numbers by using distance rate, and it becomes difficult to determine the neighbor list. For such a limited range, most sensor networks will just have to send the data to only the corresponding CH and NCH, the network faces several problems that can lead to security breaches. We suggested a protected whale swarm optimization model (SWSPA) based on two trust factors to solve this problem; the first is a network model that provides routing hops, and the next is a security model that provides a routing protocol multi-objective. A confidence model is used here, taking into account various confidence factors, along with direct confidence, indirect confidence, integration factor, and forward rate factors, along with other parameters, including distance, delay, intra-cluster distance, interaction lifetime, energy, and cluster distance. The trust model for providing high security for the network is included. Therefore, simulation is achieved by considering two confidence metrics, making our model a stable model.

## REFERENCES

[1]. Sharma, R., Vashisht, V., Singh, A.V., et al.: ‘Analysis of existing clustering algorithms for wireless sensor networks’ in Kapur, P., Klochkov, Y., Verma, A., et al. (Eds.): ‘System Performance and Management Analytics. Asset Analytics’ (Springer, Singapore, 2018), pp. 259–277.

[2]. Sharma, R., Vashisht, V., Singh, U., et al.: ‘Node clustering in wireless sensor networks using fuzzy logic: survey’. Int. Conf. on System Modeling and Advancement in Research Trends (SMART), Moradabad, Uttar Pradesh, India, 2018, pp. 66–72.

[3]. Sharma, R., Vashisht, V., Singh, U., et al.: ‘Nature inspired algorithms for energy efficient clustering in wireless sensor networks’. Int. Conf. on Cloud Computing, Data Science and Engineering (Confluence), Noida, Uttar Pradesh, India, 2019, pp. 365–370.

[4]. Crosby, G.V., Pissinou, N., Gadze, J., et al.: ‘A framework for trust-based cluster head election in wireless sensor networks’, Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems, Columbia, MD, 24–28 April, 2006, pp. 13–22.

[5]. Pissinou, N., Crosby, G.V.: ‘Cluster-based reputation and trust for wireless sensor networks’. 4th IEEE Consumer Communications and Networking Conf., CCNC 2007, Harrah's, Las Vegas, Nevada, 2007, pp. 604– 608.

[6]. Song, F., Zhao, B.: ‘Trust-based LEACH protocol for wireless sensor networks’. Second Int. Conf. Future Generation Communication and Networking, FGCN'08, 2008, pp. 202–207.

[7]. Bao, F., Chen, R., Chang, M., et al.: ‘Trust-based intrusion detection in wireless sensor networks’. 2011 IEEE Int. Conf. on Communications (ICC), Kyoto, Japan, 2011, pp. 1–6.

[8]. Duan, J., Gao, D., Yang, D., Foh, C.H., Chen, H.H.: ‘An energy aware trust derivation scheme

with game theoretic approach in wireless sensor networks for IOT applications'. IEEE Internet Things J. 1(1), 2014, pp.58–69.

[9]. Zhou, Z., Yao, B., Xing, R., Shu, L., Bu, S.: E-CARP: an energy efficient routing protocol for UWSNs in the internet of underwater things. IEEE Sens. J. 16(11), 4072–4082, 2016.

[10]. Latiwesh,A.;Qiu,D.'Energy efficient spectrum aware clustering for cognitive sensor networks: CogLeach-C'. In Proceedings of the 10th International Conference on Communications and Networking in China (ChinaCom), Shanghai, China, 15–17 August 2015. [CrossRef]

[11]. Ari, Ado & Labraoui, Nabila & Yenke, Blaise & Gueroui, Abdelhak. (2018). 'Clustering algorithm for wireless sensor networks: The honeybee swarms nest-sites selection process based approach'. International Journal of Sensor Networks. 27. 1. 10.1504/IJSNET.2018.092101.2018, pp.1-14.

[12]. Wang, J.; Gao, Y.; Liu, W.; Sangaiah, A.K.; Kim, H.J. 'An Improved Routing Schema with Special Clustering Using PSO Algorithm for Heterogeneous Wireless Sensor Network'. Sensors, February, 2019, 19(3), 671, pp.1-17.