Adil Hussain Mohammed , 2021, 9:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

Fish Schooling And Sorensen Trust Based Wireless Sensor Network Optimization

Adil Hussain Mohammed
DC Access System (DCAS) Linux Engineer
Department of Health Care Finance (DHCF) DHCF's headquarters 955 L'Enfant Plaza, SW, 3rd Floor, Washington, DC 20024

Abstract- Computing services are developing rapidly, so adhoc networks and wireless networks grow in general. However, there are still security concerns when it comes to wireless sensor networks due to its vulnerability to numerous attacks. In this paper a detail list of various attacks were explained. Paper has summarized techniques adopt by the scholars to prevent or detect such attacks in the network. This paper has proposed a fish schooling genetic algorithm for packet routing. Routing path reduces spectrum waste and increases the life span of the network as well. Further to detect some of node present in the network that perform malicious activity Sorensen function was adopt. Based on the node activity Sorensen trust value was estimate in fix life span interval (sessions). Experimental work was done on different set of nodes, network size and paths. Result shows that proposed Fish Schooling Sorensen Trust Network Optimization (FSSTNO) model is better as compared to other existing algorithms.

Index Terms- Sink hole attack, Gray Hole attack, Genetic Algorithm, Wireless Sensor Network, Trust Based Model.

I. INTRODUCTION

Large numbers of tiny sensor nodes in a network make it possible to obtain data about physical occurrences that was difficult or not possible to obtain in more conventional ways. In the coming years, as developments in micro-fabrication technology allow the cost of manufacturing sensor nodes to continue to drop, growing deployments of wireless sensor networks are projected, with the networks eventually growing to large numbers of nodes.
After the initial deployment (typically ad hoc), sensor nodes are responsible for self organizing a proper network arrangement, often with multihop connections between sensor nodes. In wireless Sensor Networks, the nodes use the open air medium to communicate with each other, in doing so they face sensitive security examine the traffic throughout the network or to crash packets selectively or totally to affect the flow of information. The security mechanisms that are used for wired systems such as authentication and encryption are useless under hidden mode of attack because the nodes do not modify their headers but only forward these packets. But the attack in participating mode is more complicated, because if it once launched, it is difficult to detect. WSN platforms generally have limited processing capability and memory. The design of WSN devices usually favors decreased cost over increased capabilities.

II.RELATED WORK

Nayyar et al. [7] compared the benefits and drawbacks of each enlisted protocol for UWSN based on several parameters such as routing

International Journal of Science, Engineering and Technology

An Open Access Journal

technique, packet delivery ratio, energy efficiency, packet latency, and localisation.

John et al. [8] addressed the operation of different location-based opportunistic routing algorithms proposed for UWSNs and analysed the performance of two key methods, VBF and HH-VBF, using Aqua-Sim simulations, although the performance of these protocols is hampered by network communication voids.

The random walking approach using camouflage packets and genuine packets is also used by J. Wang et al. in [9]. The real data packets would walk in a random direction to mask the transmission direction, while the camouflage data packets would be inserted into the intersections of two or more shortest paths to prevent the attacker from determining the real path.

In [10], Osanaiye et al. focused on one of the most common assaults on WSN, the DoS Jamming attack. This attack operates by flooding the node with fraudulent traffic in order to suffocate legitimate traffic and, as a result, the network. The exponentially weighted moving average (EWMA) technique introduced in this article is used to detect abnormal variations in the strength of jamming attacks. The defence against dual attacks for BHA and GHA has been described by Pooja Rani et al. in [11] publication using the notion of Artificial Neural Network (ANN) as a deep learning algorithm and the swarm-based Artificial Bee Colony (ABC) optimization technique.

III.PROPOSED METHODOLOGY

Whole work was divide into two section first was to generate the trsust and other was to generate path. In first section a observation window was create to find the trust of the wireless nodes. Working steps of model is shown in fig. 1. Second section finds the route from the source to destination in wireless network with an objective of optimizing the channel utilization.

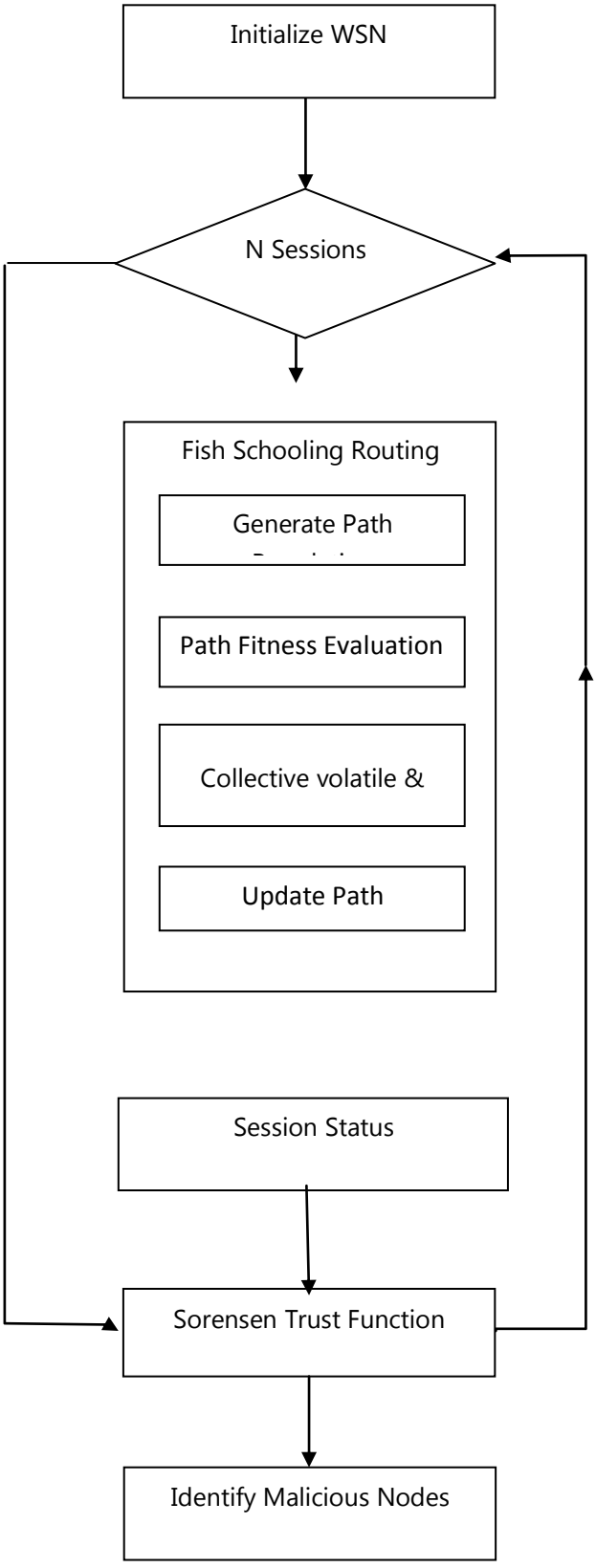

Fig.1 FSSTNO training module.

International Journal of Science, Engineering and Technology

An Open Access Journal

1.Develop Virtual Region and Place Node position
This work start with placement of N number of nodes and in an MxM region. In order to assume the initial stage of the network some energy need to be set for each node in the network [10, 11]. Each link between node have fix spectrum channel to communicate.

2. Observation Window- It's a centralized data storage in manage by fusion center where each transaction related information was maintain. fusion center store node specific transaction count, successful transaction count, failed transaction count and transaction node ID. This bridge store data as per window. After completion of window trust value of the nodes were evaluate as per the trasaction behavior done by node in window. Wireless radio needs a fix size time. So in one window more than one node may initiate a transaction.

3. Sorensen Trust Function
The value of the node transaction is is in integer form and differ node to node, so the Sorensen Similarity [12]: generate from the observation window dataset:

$$SS = \frac{N(x) \cap N(y)}{d(x) + d(y)}$$

Where $N(x) \cap N(y)$ is number of transaction between x and y. d(x) is degree of x and y. So Sorensen Similarity is ratio of common transaction between x, y to the sum of nodes.
Each node in the observation matrix has a trust value. This value may increase or decrease as per the behavior of the nodes in form of transaction success. Storage tables were used to evaluates this value of work. So let successful transaction count between i, j node is represent by Ts_{ij} and total number of transaction represent by Tt_{ij} [45]. Estimation of this trust done by:

$$D_{ij} = \sum_{i,j=1}^{n} SS_{ij} \text{----Eq. 4.1}$$

Above eq. gives n number of trust value for each node, but behaviors of node with node may be different. As malicious node provide good service to some node and poor service to others. This function takes all Sorensen value of a node and generates a single value of the node as per different behavior operations done by node with other nodes.

4. Fish Schooling Genetic Algorithm
4.1 Generate Path Population- Primary unit of genetic algorithm work is chromosome and in FSGA algorithm group of fish was chromosome, where each fish was node in the network. Number of fish in chromosome are depend on path. So a random Path Population (PP) set was develop by the FSGA. PP is matrix of having m number of rows representing a row and St number of column represent a node.

FP←Generate_Fish(P, St)------Eq. 1

4.2 Fitness Function
In concurrent transmissions, the performance of a link not only depends on its own setup but also the influence factors from other links sharing the same channel. Signal-to interference plus-noise ratio (SINR) is used to measure the quality of communications [14, 15]. For a link (i; j) on spectrum channel m, its SINR can be calculated as follows:

$$SINR_{ij}(m) = \frac{h_{ij} P_i}{\sigma^2 + \sum_{(a,b)\in I(m)} h_{aj} P_a} \text{----Eq. 2}$$

where pi denotes transmission power of sender i. In this paper, assume that the transmission power of all links is at the fixed level. hij represents the channel gain between sender i and receiver j, which can be denoted by k/d_{ij}^{σ} . Here k is the path loss constant. dij is the distance between i and j. σ^2 is the path loss exponent. The thermal noise that can be considered as a constant, and sigma notation presents the aggregate interference at receiver j, which is generated by the links transmitting concurrently on the current spectrum channel. Here, I (m) presents the set of links sharing spectrum channel m.

International Journal of Science, Engineering and Technology

An Open Access Journal

4.3 Collective Volitive Movement

Searching of a food done by collective operation where each chromosome undergoes in assembly or dispersion. In case a fish found a barry center then assembly of other fish done by reducing there distance with other fish. This assembly operation was perfrom by eq. 3. In case food not found than distance between the fish increases as per eq. 4 *[16]*. So if fitness value of t^{th} iteration is higher than t+1 than apply case 1 otherwise case2.

Case1

$$x(t+1) = x(t) - M_{vol} \times R \times \left(\frac{x(t) - B(t)}{Distance(x(t), B(t))}\right)$$

Case2

$$x(t+1) = x(t) + M_{vol} \times R \times \left(\frac{x(t) - B(t)}{Distance(x(t), B(t))}\right)$$

$$B(t) = \frac{\sum_{i=1}^{N} x(t)W(t)}{\sum_{i=1}^{N} W(t)}$$

Feeding Operator

$$W(t+1) = W(t) + \left(\frac{\Delta f}{max(|\Delta f|)}\right)$$

$$\Delta f = F(t+1) - F(t)$$

$$M_{vol} = M_{vol} - \frac{M}{Iteration_{max}}$$

Where

M_{vol}: Maximum displacement perform in a operator.

X(t): Random position of a phrase in the t^{th} iteration.

W(t): Summation of fitness value.

4.4 Crossover

As per new position of fish x(t) in t^{th} iteration values range between from null to St. This value modify the fish in chromosome. As per best chromosome in a current population of t^{th} iteration other chromosome fish values were modified. So result of this step was new chromosome sets. Population updation was done by evaluating fitness value of child chromosome if child chromosome value is better than keep the child and parent chromosome remove from population. Otherwise if parent chromosome fitness value is better than child chromosome was remove from population.

4.5 Final Path- After sufficient number of T iterations fish schooling algorithm get stop. Best store fish path P, obtained from eq. 3 act as node path of the work. As per obtained path each node in the path was further check by trust value. In this check if trust value of a node crosses a threshold value then consider it as real node otherwise malicious node. So if a path have malicious node in the route then packet was not transfer in the route. Based on trust value decision of malicious node was taken.

IV. EXPERIMENT AND RESULTS

This section of paper shows the performance of proposed FSSTNO model with other existing algorithm. Implementation was done on MATLAB software having machine configuration of I3 6^{th} generation processor and 4 GB RAM. Existing model was taken from algorithm proposed in [11].

1. Results and Analysis

Table 1 Comparison of spectrum utilization.

Environment RegionxNodexPath	FSSTNO	Previous Model [11]
100x50x5	40.598	29.92
100x50x8	62.8746	48.34
100x100x5	80.199	59.98
100x100x8	62.874	24.96
150x50x5	80.199	40.199
150x50x8	50.4991	33.1233
150x100x5	40.599	30.399
150x100x8	62.8748	47.998

Spectrum utilization values at different set of network region, number of nodes and paths were summarized in table 1. It was obtained from the table that proposed model has increase the utilization percentage by use of fish optimization genetic algorithm.

International Journal of Science, Engineering and Technology

An Open Access Journal

Table 2 Throughput comparison of Proposed and previous work.

Environment RegionxNodexPath	FSSTNO	Previous Model [11]
100x50x5	67.9416	39.965
100x50x8	82.476	4837
100x100x5	99.9718	79.9
100x10x8	82.4418	49.73
150x50x5	91.99	51.99
150x50x8	92.429	59.89
150x100x5	79.95	47.966
150x100x8	77.49	57.427

Throughput values at different set of network region, number of nodes and paths were summarized in table 2. It was obtained from the table that proposed model has increase the throughput percentage by use of fish optimization genetic algorithm. As path generation by genetic algorithm has increases the work efficiency.

Table 3 Transfer time (Second) comparison of proposed and previous work [11].

Environment RegionxNodexPath	FSSTNO	Previous Model [11]
100x50x5	124.1242	124.144
100x50x8	129.504	129.5167
100x100x5	121.534	142.836
100x10x8	117.504	117.4667
150x50x5	161.208	148.5458
150x50x8	109.53	117.06
150x100x5	122.39	122.41
150x100x8	134.373	134.38

Transfer time need for the movement of data packet was reduced by the model. It was obtained that proposed model has increases the node optimization technique and enhance the result outcomes.

V. CONCLUSION

Wireless sensor network are acting as a important portion for implementation, maintains of many application and services. Open network for communication increases its flexibility and vulnerability of attacks as well. It is critical challenge to develop the effective and lightweight security mechanism to detect and prevent various attacks for WSN Attacks were list in the paper and classified as per nature of the activity performed by malicious nodes.

This model identify infected nodes by Sorensen trust function, this detection directly increases the channel utilization and packet delivery rate. Use of fish optimization genetic algorithm for path node selection improve the work performance. Experiment was done on different set of network region, number of nodes and paths. Result shows that proposed model has increased the spectrum utilization and throughput as well.

REFERENCES

1. Wireless Sensor Networks using Intrusion Detection System G. Jegan and P. Samundiswary. "Wormhole Attack Detection in Zigbee". Indian Journal of Science and Technology, Volume: 9, Issue: 45 2016.
2. W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '05), pp. 46–57, Chicago, Ill, USA, May 2005.
3. S. Anitha, P. Jayanthi, K. Lalitha and V. Chandrasekaran. "Secured Ant Colony Optimization based on Energy Trust System for Replica Node Attack Detection". International Journal on Emerging Technologies 11(2): 2020.
4. Dr. Shweta Singh, Jamvant Omkar. "Wireless Sensor Node Energy Optimization by Packet Routing and Clustering". Ijsret.com IJSRET

International Journal of Science, Engineering and Technology

An Open Access Journal

Volume 7 Issue 4, July-Aug-202.

5. Pragya Richhariya, Dr. Shailja Sharma. "A Survey on Cloud Virtual Machine Management Techniques and Features". ijset.in IJSET, vol 9 issue 42021.

[1] T. Sorensen. A method of establishing groups of England: CRC Press.