

Group Search Optimization and Leicht-Holme-Newman Trust based Wireless Sensor Network Optimization

Poonam Tiwari, Professor Rani Kushwaha
Mittal Group of Institutes, Bhopal (M.P), INDIA

Abstract- Wireless sensor networks (WSNs) are vulnerable to many backdoor attacks counting malicious nodes. Malicious nodes can inject false data, drop packets, or even launch denial-of-service attacks. One way to detect malicious nodes in WSNs is to use trust-based routing protocols. Trust-based routing protocols calculate a trust value for all network nodes. This paper has developed a model that estimates trust of each node based on social behavior function Leicht-Holme-Newman. Based on the trustful nodes paths of the packet were found by the Group Search Optimization algorithm. This paper has proposed a model that reduces the energy losses of WSN network. Experiment was done on different set of network environment under varying nodes attacks. Result shows that proposed model has increased the network spectrum utilization and network life as well.

Index Terms- Sink hole attack, Genetic Algorithm, Wireless Sensor Network, Social behavior Trust.

I. INTRODUCTION

The objects processed by computer systems are mainly abstract things, and these systems do not have insight into the real physical world. Sensors are able to measure the physical quantities such as temperature, pressure, light wave, velocity, electromagnetic wave, and so on and convert the measurement results into electronic signals. Therefore, for computer systems or computable devices, sensors build a bridge from the abstract world to the real world so that the former can obtain almost all kinds of physical information in the real world. However, different from the traditional wired networks, wireless sensor networks, or WSNs, we usually do not need centralized management or fixed infrastructure such as base station and access point. Sensor nodes form the network automatically, and the network cost is relatively low [1]. Therefore, WSNs can be used in situations where there is no infrastructure, or for security reasons, the existing infrastructure does not meet certain conditions. Although WSNs are widely used, security and reliability should be the prerequisite for these applications.

WSNs contain sensors with constrained resources in terms of memory, power, and battery life [1]. These limitations make these sensors vulnerable to potential security threats [2] as they lack the capacity to run generalized security software [3]. Additionally, due to their reliance on wireless communication, WSNs are exposed to threats such as inception, interference, and disruption that may result in Denial-of-Service (DoS) attacks, data manipulation, and unauthorized access [4]. Furthermore, sensor nodes may also be vulnerable to destruction, physical attacks, and theft if the WSNs are

installed in erratic and challenging surroundings. The establishment of trust becomes essential when a WSN consists of a multitude of sensors and edge aggregators that aggregate sensor data. This concept of trust is applicable not only within WSNs but also within the wider scope of the Internet of Things (IoT) [5]. This computation of trust offers various advantages such as the ability of the sink node (aggregator) to recognize malicious or malfunctioning sensor nodes within its range. Thus, the establishment of trust among sensors in WSNs is of utmost significance in achieving secure and dependable communication while preventing and mitigating potential security threats [6]. To achieve this, a trust management framework [7] can be built where one sensor evaluates the trustworthiness of another sensor node.

Rest of paper is organized into few section where next section introduces work done by the researcher in WSN network life optimization. Further paper has brief the work done by the proposed model that reduces the energy losses and increase the life of WSN network. Whole proposed work was detailed with path generating GSO algorithm. Fourth section details the experimental work with outcome of proposed model on different parameters. Finally work was concluded with future direction of research area.

II. RELATED WORK

In [8], authors proposed, WSN is considered as an important part of the IoT network in which nodes send and receive services. Nodes' authentication is performed by the central authority due to which SPOF and trust issue arises. For that reason, an authentication mechanism is proposed that is based

on hybrid blockchain. Also, the attacks' analysis is performed to check the network robustness.

In [9], authors proposed a blockchain based trust model in which MND is performed. Also, the nodes' traceability is performed in the detection process. Three parameters, delayed transmission, response time and forwarding rate, are used to calculate the trust values of the nodes. The calculated values are stored in the blockchain, being deployed on the sink nodes. In the study, a quadrilateral measurement method is used to find unknown nodes' locations. This method finds the distance of unknown node from four known nodes. In this way, the nodes' locations are found and the information is broadcast in the network. Also, the neighbor nodes update their tables.

In [10], authors analyse several attacks and propose a new security approach to prevent data change due to compromised nodes. The suggested technique is a non-cryptographic scheme which is computationally less complex. In this scheme, nodes compute trust of the neighbors and exclude hostile nodes from the probable list of forwarding nodes based on low trust value. Trust computation is carried out considering various parameters like packet drop rate, packet rejection ratio and remaining energy level of the node.

A method for detecting rank attacks [29] targeted the latter process in RPL topologies. A trust threshold was established based on the rankings of surrounding nodes. Compared to RPL not under and under attack, the simulation results demonstrated that the suggested method was more efficient than the state-of-the-art approach.

In [11], authors proposed a secure and load balanced routing (SLBR) scheme for heterogeneous clustered-based WSN. SLBR present better trust-based security metric that overcomes the problem when sensor keep oscillating for good to bad state and vice versa, and also balance load among CH. Thus, they aid in achieving better security, packet transmission, and energy efficiency performance. Experiments are conducted to evaluate the performance of proposed SLBR model over existing trust-based routing model, namely exponential cat swarm optimization (ECSO).

In [12], authors proposed a model considers a master auditor node (MAN) from the available trusted nodes that monitor the entire network analyzing each node behavior. This research proposes an Energy Efficient Master Auditor Node with Trust based Secure Routing (EE-MAN-TbSR) in Wireless Sensor Networks for trusted route selection for secured data transmission. The proposed model when contrasted with the existing models performs better in trusted route selection avoiding malicious actions in the network.

In [13], authors proposed a new trust based secure and energy efficient routing protocol (TBSEER) to solve these problems. TBSEER calculates the comprehensive trust value through adaptive direct trust value, indirect trust value and energy trust value, which can be resistant to black hole, selective forwarding, sinkhole and hello flood attacks. Moreover, the adaptive penalty mechanism and volatilization factor are used to fast identify the malicious nodes. In addition, the nodes only need to calculate the direct trust value, and the indirect trust value is obtained by the Sink, so as to further reduce the energy consumption caused by iterative calculations. Finally, the cluster heads find the safest multi-hop routes based on the comprehensive trust value, which can actively avoid wormhole attack.

III. PROPOSED METHODOLOGY

The first part of the study focuses on establishing an observation framework to assess the reliability of wireless nodes. This involves closely analyzing node behaviors to gauge their dependability and integrity. Figure 1 provides a comprehensive depiction of the methodology used to create this observation framework and evaluate node trust by Leicht-Holme-Newman. In the next phase, the research shifts towards identifying the most efficient routing path from the source to the destination within the wireless network. This stage highlights the critical role of optimizing channel usage, achieved through the implementation of group search optimization algorithms. These algorithms facilitate the selection of optimal routes, significantly improving the network's overall efficiency.

Setup Network The procedure starts by defining a virtual area designated for node deployment. A total of $N \times N$ nodes are distributed across a grid measuring $M \times M$. During this initial setup phase, each node is assigned a predefined energy level, as outlined in references [14]. Additionally, specific spectrum channels are allocated to enable communication among the nodes. This systematic configuration lays the groundwork for an organized and energy-efficient network, paving the way for reliable trust evaluation and efficient route optimization.

Leicht-Holme-Newman:

$$TL = (a \cap b) / (a \times b)$$

the number of vertices adjacent to both a and b normalized by the product of the degrees of a and b [15].

Each node in the observation framework is attributed a dynamic trust score that adjusts based on transaction results. To monitor these scores, storage tables record the data, with successful transactions labeled as T_a , T_b , and the total number of transactions as T_t . Trust calculations are performed using the cumulative Leicht-Holme-Newman Similarity metrics,

producing a single trust score for each node. This approach captures the diverse behaviors exhibited by nodes, including inconsistencies in service quality that malicious nodes may display when interacting with various network entities.

$$N_{ij} = \sum_{l=1}^n T_{Ln} \text{ ----Eq. 4.1}$$

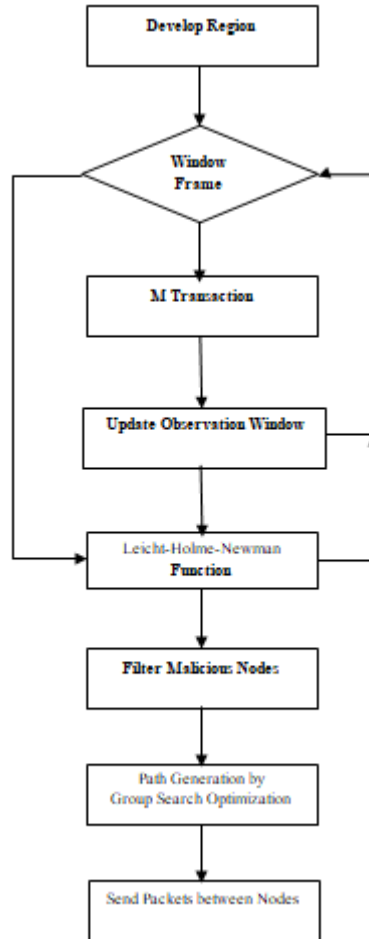


Fig.1 STIWWNO training module

Group Search Optimization

In this step of the module packet route generate by the Bootstrap model were further optimized to reduces the makespan time of the job execution. So finds all set of job combination and evaluate each is time taken process that reduces the utility of the network. So this work adopts group search genetic algorithm that gives suitable packet route set in less latency time. Group search finds the food to eat where searching member is at any of three state first is producer, second is scrounging and third is ranging. In this work food source is set of packet route as per edge resources and job requirement. In whole process of Forgaing (Searhcng of food to eat) objective is to finds the good food source [16]. So to clear more about the terms used in the algorithm and its relation with our work:

Food Source: Single dimension vector having elements of packet route status of nodes. If any element state is change then this new vector is separate food source.

Member: It's a chromosome position in the population that points a food source. A member can point different food source at different iteration of algorithm.

Group Member

Collection of such members is group member. Hence in this algorithm population is group and elements present in group is member. Out of various food sources available some random sources were point by the member. Representation of this population is shown in eq. 1.

$$GM \square \text{Gaussian_Group_Generation}(N)$$

Where in Eq. 1 m is number of member in the population/group, n is number of jobs. In order to generate random food source point Gaussian function was used

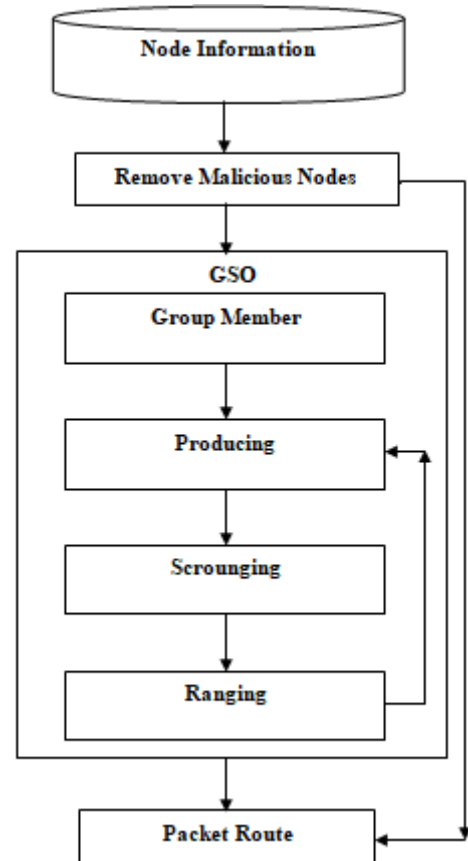


Fig. 2 Packet route generation by proposed model.

Producing Evaluation of various food point identify by the members was done in this step of the model. In terms of

genetic algorithm this step is fitness evaluation function. Producer selection is done in this step as per fitness values.

Scrounging (Crossover) Scroungers Producer finds the good food points and other member in the p group is considers as the scroungers. All scroungers join the food source search by the producer. So producer stop searching the food source in this iteration and other members change their food print as per producer. This change is termed as crossover operation in the group [17]. To understand this let P is producer, Mm is mth member in population then change occur at random job position as per producer job set.

$$M'm[1 r] \square Mm[1 r] + P[1,r]$$

New food point obtained from the crossover operation. Where r is random position value range from 1 to n. One more step is to check that new food point is better food source or not. For this evaluate its fitness value as done in algorithm 1. Better food source were point by the member.

Ranging (Mutation) Rangers

Each group member except producer participate in this step of algorithm. As ranger will find new food point as by their random behavior hence producer not help them. Member modify the state of the job at some random position by swapping new job with existing. This change of state gives new food location in the search space to the members. Swaping operation were perform in the step of algorithm.

$$M'm[1 r] \square \text{Swap}(Mm[1 r])$$

New member food search point need to check as done in scrounging phase. Food point having better fitness value obtained is consider as the final member food point in current iteration. After sufficient number of iterations algorithm stops to get the final packet route JS.

Proposed Algorithm

Input: N, Pos, P // Nodes, Position, Path

Output: Rt//Route

1. IN □ Initialize_Network(N, Pos)
2. Loop 1:M //M: Window of M transaction
3. S □ Sender_Node()
4. R □ Receiver_Node()
5. T[M] □ Transaction(S,R)
6. End
7. TL □ Leicht-Holme-Newman(R,M) //NT: Node Trust
8. Rt □ GSO(TL,PN,Pos) □ Best_Path(Wp)

IV. EXPERIMENT AND RESULTS

Tool Required

The numerical implementation of the model was carried out using MATLAB software, renowned for its proficiency in

engineering and scientific computations due to its high-level programming capabilities. The tests were conducted on a computing platform featuring a 2.27 GHz Intel Core i3 processor, 4 GB of RAM, and operating on the Windows 7 Professional platform. The performance of the implemented model was compared with that of the previous model model proposed in [13].

Results

Table 1 WSN variable environment spectrum utilization based comparison of models.

Experimental Setup (Area,Nodes,Path)	Proposed Model	Previous Model
100x100, 6, 100	83.4998	50.1663
100x100, 6, 120	83.4998	66.8332
100x100, 6, 140	83.4998	66.8332
100x100, 6, 160	83.4997	50.1665
100x100, 7, 100	70.2997	60.2997
100x100, 8, 100	70.2996	40.2996

Table 1 shows spectrum utilization of the different comparing models. It was found that use of trust model has increases the malicious node detection accuracy that ultimately decreases the spectrum wastage. Table 1 shows that proposed model has increases the spectrum utilization by 29.49%, as compared to existing model in [13].

Table 2 WSN variable environment throughput based comparison of models.

Experimental Setup (Area, Path, Nodes)	Proposed Model	Previous Model
100x100, 6, 100	96.6521	63.3042
100x100, 6, 120	96.6521	79.9854
100x100, 6, 140	96.6521	79.9854
100x100, 6, 160	93.317	63.3188
100x100, 7, 100	89.9804	79.9804
100x100, 8, 100	93.9654	63.9654

Throughput based comparison of proposed model was under different set of nodes and paths. It was found that use of Leicht-Holme-Newman function has increases the throuput of network by removing malicious nodes. Further it was found that use of Group Search Optimization in proposed model has increases the throughput value by 24.09% as compared to existing model.

Table 3 WSN variable environment transfer time based comparison of models.

Experimental Setup (Area,Nodes,Path)	Proposed Model	Previous Model
100x100, 11, 100	0.073398	143.2146
100x100, 15, 100	0.30071	143.2146
100x100, 20, 100	0.30105	143.2146
100x100, 10, 120	0.29262	143.1979
100x100, 10, 140	0.2793	147.4558
100x100, 10, 160	0.24257	112.5643

Table 3 shows transfer time of the different comparing models. It was found that use of trust model has reduces the malicious node detection accuracy that ultimately decreases the spectrum wastage.

V. CONCLUSION

As malicious nodes can introduce false data, drop packets, or even initiate denial-of-service (DoS) attacks. To counter such threats, trust-based routing protocols can be employed for detecting malicious nodes. These protocols assign a trust value to each network node. This study presents a model that calculates the trust value of nodes using the Leicht-Holme-Newman social behavior function. Utilizing trustful nodes, the Group Search Optimization algorithm identifies reliable paths for packet transmission. The proposed model aims to minimize energy consumption in WSNs. Experiments were conducted in diverse network environments with varying attack scenarios. The results indicate that the model enhances both network spectrum utilization and the overall lifespan of the network. Result shows that use of Group Search Optimization in proposed model has increases the throughput value by 24.09% as compared to existing model.

REFERENCES

1. Namasudra, S.; Devi, D.; Choudhary, S.; Patan, R.; Kallam, S. Security, privacy, trust, and anonymity. In *Advances of DNA Computing in Cryptography*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2018; pp. 138–150.
2. Das, S.; Gangwani, P.; Upadhyay, H. *Integration of Machine Learning with Cybersecurity: Applications and Challenges*; Springer: Berlin/Heidelberg, Germany, 2023.
3. Huanan, Z.; Suping, X.; Jiannan, W. Security and application of wireless sensor network. *Procedia Comput. Sci.* 2021, 183, 486–492.
4. Fang, W.; Zhang, W.; Chen, W.; Pan, T.; Ni, Y.; Yang, Y. Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey. *Wirel. Commun. Mob. Comput.* 2020, 2020, 2643546.
5. Das, S.; Namasudra, S.; Deb, S.; Ger, P.M.; Crespo, R.G. Securing IoT-Based Smart Healthcare Systems by Using Advanced Lightweight Privacy-Preserving Authentication Scheme. *IEEE Internet Things J.* 2023, 10, 18486–18494.
6. Kim, T.-H.; Goyat, R.; Rai, M.K.; Kumar, G.; Buchanan, W.J.; Saha, R.; Thomas, R. A Novel Trust Evaluation Process for Secure Localization Using a Decentralized Blockchain in Wireless Sensor Networks. *IEEE Access* 2019, 7, 184133–184144.
7. Z. Cui, X. U. E. Fei, S. Zhang, X. Cai, Y. Cao, W. Zhang, et al., "A hybrid blockchain-based identity authentication scheme for multi-WSN", *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241-251, Apr. 2020.
8. AMoinet, B. Darties and J.-L. Baril, "Blockchain based trust & authentication for decentralized sensor networks", arXiv:1706.01730, 2017.
9. A Sreevidya, Dr.M. Supriya. "Malicious Nodes Detection and Avoidance Using Trust-based Routing in Critical Data Handling Wireless Sensor Network Applications". *Journal of Internet Services and Information Security*, Volume 14 - Issue 3 August 2024.
10. Boudouaia M.A., Abouaissa A., Ali-Pacha A., Benayache A., Lorenz P. RPL rank based-attack mitigation scheme in IoT environment. *Int. J. Commun. Syst.* 2021.
11. Thaniyath, Gousia. "An Efficient Trust-Based Routing Model for Clustered-Based Hetrogeneous Wireless Sensor Network." *IJBDCN* vol.16, no.2 2020: pp.84-101.
12. Reddy, D. M. K. ., Sathya, R. ., & Lakshmi, V. V. A. S. . (2023). An Energy Efficient Master Auditor Node with Trust Based Secure Routing in Wireless Sensor Networks. *International Journal of Intelligent Systems and Applications in Engineering*, 11(3), 519–529.
13. H. Hu, Y. Han, M. Yao and X. Song, "Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks," in *IEEE Access*, vol. 10, pp. 10585-10596, 2022.
14. Arjunan, S.; Pothula, S. A survey on unequal clustering protocols in Wireless Sensor Networks. *J. King Saud Univ.-Comput. Inf. Sci.* 2019, 31, 304–317.
15. E. A. Leicht, P. Holme, and M. Newman. Vertex similarity in networks. *Phys. Rev. E*, 73, 2006.
16. Ali I.M., Sallam K.M., Moustafa N., Chakraborty R., Ryan M., Choo K.-K.R. An automated task scheduling model using non-dominated sorting genetic algorithm II for fog-cloud systems *IEEE Trans. Cloud Comput.*, 10 (4) (2022), pp. 2294-2308.
17. Yang, P.-Y.; Yang, K.-Y.; Ho, W.-H.; Chou, F.-I.; Chou, J.-H. Improvement Technique for Group Search Optimization Using Experimental Design Method. *Appl. Sci.* 2023, 13, 3205.