INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

# Sorensen Trust Based and Invasive Weed Algorithm Based Wireless Sensor Network Optimization

**Jayant Shukla, Laxmi Singh, Sanjeev kumar Gupta**

**Department of Electronics and communication Engineering, Rabindranath Tagore University Raisen, Madhya Pradesh**

**DOI : https://doi.org/10.51583/IJLTEMAS.2024.130604**

**Received: 04 June 2024; Revised: 13 June 2024; Accepted: 21 June 2024; Published: 07 July 2024**

**Abstract:** Wireless Sensor Networks (WSNs), characterized by their openness, dynamism, and lack of infrastructure, are highly susceptible to a range of attacks due to their ad hoc nature. Routing, being a pivotal process within WSNs, relies heavily on the contribution of intermediary nodes, thereby accentuating the network's vulnerability to black and gray hole attacks. This work has proposed a Sorensen Trust and Invasive Weed based Wireless Network optimization (STIWWNO) model that estimates the confidence of the network with the social Sorensen trust evaluation function. Once the network knows the nodes trust then cluster centers selection makes easy and safe for routing of sensed data. Packet node path were generate by the invasive weed optimization genetic algorithm. Experiments were conducted under various network conditions, including different node counts and area sizes, to evaluate the effectiveness of the proposed method. The results of these experiments demonstrated that the use of the proposed Sorensen function, combined with the invasive weed optimization technique, significantly enhances the lifespan of the network. The adaptive nature of IWO allows the network to respond effectively to changes in node positions, ensuring sustained performance and energy efficiency. By applying this combined approach, the network can dynamically adjust to varying conditions, maintain optimal performance, and extend the operational life of the WSN.

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

## I. Introduction

The realm of wireless communication technologies is undergoing rapid evolution, particularly evidenced by significant advancements in the field of wireless sensor networks (WSNs) over the past few years [1]. WSNs represent a pivotal and increasingly indispensable technology in the twenty-first century. These networks consist of a multitude of inexpensive, low-power, and versatile sensor nodes, serving diverse purposes across various domains [2]. The emergence of large-scale sensor networks, linking hundreds to thousands of nodes, presents both intricate technical challenges and vast application prospects.

Given the absence of fixed infrastructure and reliance on an open wireless medium, implementing robust security measures within WSNs poses considerable challenges. In Mobile Ad hoc Networks (MANETs), each node operates both as a host and a router, facilitating packet forwarding among network nodes. However, this inherent openness renders WSNs vulnerable to an array of attacks, including active route interference, impersonation, and denial of service. Among these threats, the black hole attack stands out as particularly pernicious [3]. In a black hole attack, a malicious node deceitfully sends falsified Route REPLY (RREP) packets to a source node initiating route discovery, masquerading as a destination node. The attacker manipulates the routing process by advertising a fabricated route with minimal hop count and the highest destination sequence number to lure incoming traffic.

The black hole attack functions like a malignant void, annihilating all data packets that traverse through it [3]. Malicious nodes further disrupt route discovery, diverting network packets towards themselves. In the route discovery mechanism of Ad hoc On-Demand Distance Vector (AODV) routing protocol, intermediate nodes are tasked with identifying a valid route to the destination by exchanging "hello" packets with neighbors. However, in the presence of malicious nodes, the route discovery process is subverted as these nodes promptly reply to the source with false route information, bypassing the conventional neighbor discovery phase [4]. Consequently, the source node unwittingly directs its data packets through the malicious node, assuming it to be a legitimate route, thereby facilitating the black hole attack. This malicious behavior severely compromises the integrity of the network interface, leading to resource depletion and packet loss as nodes incessantly attempt to establish a valid path to the destination [5].

**Research gap:** Selection of cluster head should be secure as malicious node can enter into network at this point [7]. Sensor Node movement was not consider in the work. Identification of malicious node in the network should be improved [9].

**Objective**: This work overcome malicious node detection issue by implementing the trust based node identification. In order to reduce data loss virtual environment was created. For network channel optimization routing was done by the Invasive Weed optimization algorithm.

The subsequent sections of this paper are organized as follows: Section 2 provides a summary of existing attack detection methods targeting Black-Hole and Gray-Hole attacks. Section 3 outlines the proposed system for detecting individual and collusion attacks within wireless sensor networks. Section 4 elucidates the evaluation parameters utilized and presents simulation results. Finally, in Section 5, we conclude our proposed work and offer insights into potential avenues for future research.

## II. Related Work

In their research outlined in [7], M. Kumar et al. introduce the Taylor Sail Fish Optimizer (Taylor SFO) as a method for predicting black-hole attacks in Wireless Sensor Networks (WSNs). This novel approach involves training a Deep stacked autoencoder using the proposed Taylor-SFO framework, which integrates Taylor Series and Sail Fish Optimizer (SFO). The resulting Taylor-SFO

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

model is then employed for both routing and black hole attack detection at the WSN base station, encompassing two distinct phases. Initially, WSN nodes are routed through the proposed Taylor SFO algorithm, considering fitness parameters such as energy, distance, and delay.

In a separate study detailed in [8], S. Jiang et al. propose an intrusion detection model named SLGBM, which leverages a fusion of the Sequential Backward Selection (SBS) and Light GBM classification algorithms. The approach begins with SBS for selecting sensor node traffic data characteristics, effectively reducing dimensionality. Subsequently, Light GBM is employed for traffic attack detection in WSNs, aiming to enhance detection rates while maintaining a low false alarm rate. This model addresses common shortcomings of traditional intrusion detection methods in WSNs, including poor detection performance, limited real-time capability, and high complexity.

Continuing with their exploration in [9], Iraq Ahmad Reshi et al. tackle issues of black hole and selective forwarding attacks in medical WSNs for IoT applications. They propose cryptographic hash usage for addressing black hole attacks and employ a neighborhood watch coupled with threshold-based analysis to detect and mitigate selective forwarding attacks.

In [10], Khan et al. introduce a Secure, Dependable Trust Assessment (SDTS) scheme tailored for industrial WSNs. This scheme employs robust trust evaluation components to detect and counter unexpected behaviors such as on-off attacks and node misbehavior. The SDTS incorporates various trust evaluation metrics to defend against internal attacks, adjusting trust levels dynamically based on node behavior and environmental conditions.

Finally, Kosaraju Chaitanya et al. present the Multi-Level Trust Evaluation Model using Replicated Auditor Node (MLTEM-RAN) in [11]. This model aims to maximize packet delivery rates in WSNs by considering trust values and node conditions along communication paths. The proposed model outperforms existing approaches in terms of packet delivery rate by integrating historical behavior-based attack probabilities and real-time node status assessments.

In [12], Pooja Rani et. al. proposed a novel approach to safeguarding against dual attacks, specifically Black Hole Attacks (BHA) and Gray Hole Attacks (GHA), is introduced. This defense mechanism harnesses the power of Artificial Neural Networks (ANN) as a deep learning algorithm, combined with the swarm-based Artificial Bee Colony (ABC) optimization technique. By leveraging these sophisticated tools, the system enhances its performance by strategically selecting the most suitable nodes for transmitting data packets, a detailed exposition of which is provided in the results section.

**III. Proposed Methodology**

In the initial section, an observation window is constructed to evaluate the trustworthiness of the wireless nodes. This process involves monitoring the behavior of the nodes to determine their reliability and integrity. The detailed procedures for constructing this observation window and assessing node trustworthiness are illustrated in Figure 1. The subsequent section of the work aims to identify the optimal routing path from the source node to the destination node within the wireless network. This section emphasizes the importance of efficient channel utilization, which is achieved through the application of invasive weed optimization techniques. These techniques help in selecting the most efficient routes, thereby enhancing the overall performance of the network.

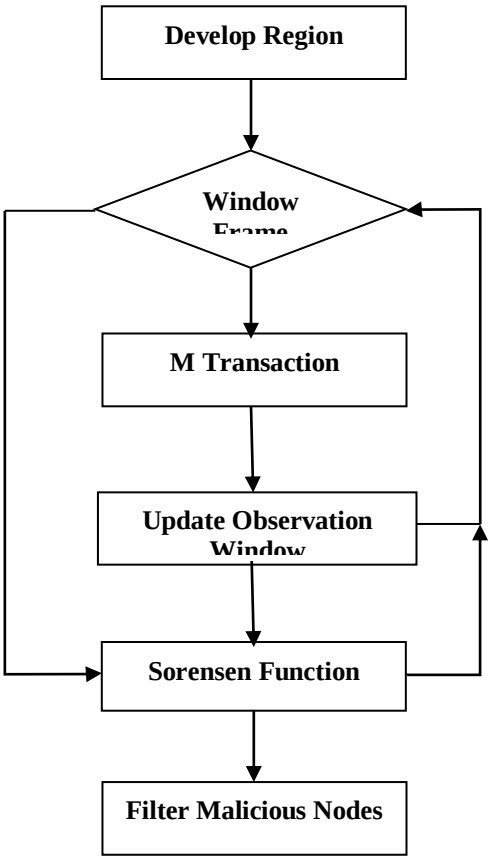


Fig.1 STIWWNO training module.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

**Development of Virtual Region and Placement of Nodes**

The process begins with the creation of a virtual region where the nodes will be placed. Specifically, N nodes are positioned within an MxM area. In the initial phase of network setup, each node is allocated a certain amount of energy, as referenced in sources [10, 11]. Furthermore, fixed spectrum channels are designated to facilitate communication between the nodes. This structured approach ensures a well-organized and energy-efficient network setup, setting the stage for effective trust establishment and optimal path finding.

**Sorensen Trust Function**

The Sorensen Trust Function is then employed to compute the trustworthiness of node transactions, utilizing the Sorensen Similarity metric [13]. This metric assesses the common transactions between nodes x and y in relation to their respective degrees.

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

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 within the observation matrix is assigned a trust value, subject to fluctuations based on transaction outcomes. Storage tables are utilized to track these values, with successful transaction counts denoted as Tsij and total transactions represented by Ttij. The estimation of trust is computed as the summation of Sorensen Similarity values, generating a singular trust value for each node, thereby accounting for varying behaviors between nodes. This comprehensive function accounts for the potential discrepancy in service quality exhibited by malicious nodes towards different network entities.

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

**Invasive Weed Algorithm**

This study employs the Invasive Weed Optimization Algorithm (IWOA) to select cluster centers, recognizing the importance of this selection process in optimizing node arrangements [14]. The IWOA algorithm operates by optimizing the distribution of "weeds," representing potential solution paths, across the network.

**Generate Weed:** Within this framework, candidate solution paths—defined as sets of nodes serving as cluster centers—are referred to as chromosomes. The population of potential solutions is randomized using a Gaussian function, as depicted in Equation 1 [15]. For instance, if there are m nodes in a path and P represents the initial population size, a solution set Cc = {N1, N5, N7,…Nm} may be considered, while P = [Cc1, Cc2,…Ccn] represents a population obtained randomly using Equation 1. Nodes with energy levels exceeding a certain threshold (TE), where m denotes the number of cluster centers and n signifies the number of chromosomes, are considered participants in the optimization process.

Wp←Rand(m, n)----Eq. 1

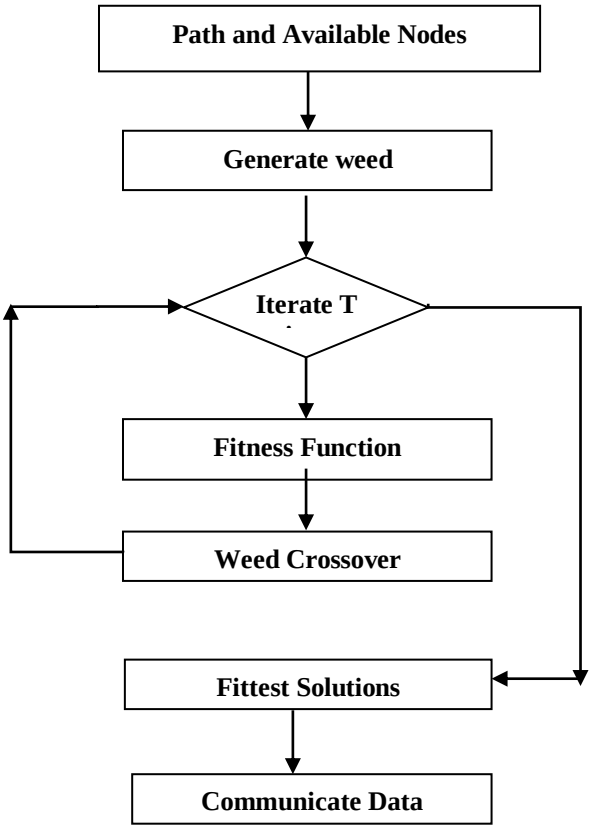


Fig. 2 Nodes routing path generation.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

**Fitness Function**

In situations where multiple transmissions happen at the same time, how well a link performs doesn't just depend on its own settings. It's also affected by other links using the same channel. We use something called Signal-to-Interference plus Noise Ratio (SINR) to measure how good the communication is [12]. For a link (i; j) using channel m, its SINR can be calculated like this:

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

Here, P_i is the power of sender i. We assume all senders use the same power level. h_ij is the strength of the signal between sender i and receiver j, and it can be represented as k/d_ij^σ. In this formula, k is a constant that represents how much signal is lost as it travels. d_ij is the distance between sender i and receiver j. σ^2 is also a constant representing thermal noise. The Σ notation represents all the interference coming from other links transmitting on the same channel. I(m) represents the set of all links sharing channel m.

To make sure the link's transmission is effective, the receiver needs to be able to decode the intended signal. There's a specific value for SINR, denoted by β, that tells us when decoding is successful. So, for link (i, j) trying to use channel m, we need to satisfy this constraint:

$SINRij(m) > \beta$

For link (*i*; *j*), the efficient link transmission opportunity *Tij* is de_ned as follows:

$Tij = \min(Ti; Tj)$

Tij tells us how often both sides of the link (i, j) can send data. If this link sends data with a flow called f on channel m, its maximum data rate is shown by:

Rij(m) = Tij x Cij(m)

Because of resource competition, the link (i, j) can only use a part of its capacity for sending the flow.

$F_{1\_max} = \max(Rf)$

$F_{1\_min} = \min(Rf)$

$F_{2\_max} = \max(|L|/|M|)$

$F_{2\_min} = \min(|L|/|M|)$

if (F1 max-F1 min) Not Equal 0

$$D = \sum_{k=1}^{2} \frac{R_n + R_{n+1}}{\mathrm{F_{k\_Max}} - \mathrm{F_{k\_Min}}}$$

End If

$$D = D + \sum_{k=1}^{2} \frac{(|L|/|M|)_n + (|L|/|M|)_{n+1}}{\mathrm{F_{k\_Max}} - \mathrm{F_{k\_Min}}}$$

Fitness ←Sort(D)

**Weed Crossover** In the Weed Crossover process, the top-ranked paths with the lowest fitness values are identified as the local best weeds. These top paths serve as benchmarks for other potential solutions. The selected top weeds then undergo a transformation process, wherein a fixed number of nodes are replaced with those from other paths. Through this process, all potential solutions, acting as chromosomes, learn from the best-performing paths.

**Final Solution** Ultimately, after a significant number of iterations, the best possible cluster centers are determined. Nodes are then assigned to these clusters, with each cluster represented by its respective center. This final solution represents an optimized arrangement of cluster centers and associated nodes within the network.

**Communicate Packet:** In this step selected path nodes is consider as the cluster center of that cluster. As node position feature was used to find the path from sender to receiver.

Proposed Algorithm **STIWWNO**

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

**Output:** P//Path

1. IN←Intialize_Network(N, Pos)
2. Loop 1:M //M: Window of M transaction
3. S←Sender_Node()
4. R←Receiver_Node()

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

5. T[M]←Transaction(S,R)
6. End
7. NT←Sorensen(R,M) //NT: Node Trust
8. FN←Filter Nodes(NT,N) // FN: Filter Nodes
9. Wp←Generate_weed(FN, P)
10. Loop 1:itr
11. F←Fitness_Value(Wp, IN)
12. Wp←Weed_Crossover(F,Wp)
13. EndLoop
14. P←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 ABC-NN model proposed in [12]

### Results and Analysis

Table 1 Spectrum utilization of WSN optimization models comparison.

| Network Dimension | Path | Nodes | STIWWNO | ABC-NN |
|---|---|---|---|---|
| 100x100 | 6 | 100 | 100 | 83.33 |
| 100x100 | 6 | 120 | 50.4986 | 33.832 |
| 100x100 | 6 | 140 | 66.9992 | 33.832 |
| 100x100 | 6 | 160 | 50.4989 | 33.6662 |
| 100x100 | 7 | 100 | 85.8571 | 71.5714 |
| 100x100 | 8 | 100 | 75.2494 | 25.2494 |
| 100x100 | 9 | 100 | 66.9997 | 44.7775 |

Table 1 demonstrates that the proposed STIWWNO model significantly enhances the spectrum utilization of the Wireless Sensor Network (WSN) compared to the existing model. This improvement is primarily due to the implementation of an invasive weed optimization model, which is used for the efficient selection of paths for nodes from the source to the destination. Additionally, the paper highlights that the identification of malicious nodes within a virtual window further boosts the network's spectrum utilization by 24.26 % as compared to ABC-NN.

Table 2 Throughput based WSN optimization models comparison.

| Network Dimension | Path | Nodes | STIWWNO | ABC-NN |
|---|---|---|---|---|
| 100x100 | 6 | 100 | 100 | 83.33 |
| 100x100 | 6 | 120 | 83.258 | 66.5914 |
| 100x100 | 6 | 140 | 89.9479 | 66.5914 |
| 100x100 | 6 | 160 | 83.2676 | 63.2926 |
| 100x100 | 7 | 100 | 91.4256 | 77.1399 |
| 100x100 | 8 | 100 | 89.9658 | 39.9691 |
| 100x100 | 9 | 100 | 82.2093 | 57.7681 |

Table 2 illustrates that the proposed model significantly enhances work performance through the use of a trust-based Sorensen function. This function effectively reduces spectrum losses, thereby boosting the overall efficiency of the system. Moreover, Table 2 reveals that the STIWWNO model improves the throughput by an impressive 26.205% compared to the previous model, ABC-NN. This considerable increase in throughput underscores the effectiveness of the STIWWNO model in optimizing network performance.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue VI, June 2024

Table 3 Transfer time based WSN optimization models comparison.

| Network Dimension | Path | Nodes | STWOWNO | ABC-NN |
|---|---|---|---|---|
| 100x100 | 6 | 100 | 0.30119 | 135.9611 |
| 100x100 | 6 | 120 | 0.22802 | 122.9569 |
| 100x100 | 6 | 140 | 0.27972 | 122.9569 |
| 100x100 | 6 | 160 | 0.1818 | 120.5494 |
| 100x100 | 7 | 100 | 0.27792 | 164.1036 |
| 100x100 | 8 | 100 | 0.1103 | 146.5703 |
| 100x100 | 9 | 100 | 0.13761 | 115.3176 |

It was also found that transfer time of the model was reduced by the proposed STIWWNO model. Hence use of trust based node selection for packet transfer has increases the work performance. While use of packet route generation by invasive weed optimization algorithm.

## V. Conclusion

Wireless networks introduce a new level of flexibility in communication and address many of the challenges associated with environmental installation. Since communicating devices in these networks rely on battery power, optimizing energy utilization is crucial for the efficiency of a Wireless Sensor Network (WSN). This paper tackles the issue of energy optimization by employing clustering of nodes through the invasive weed optimization technique. In addition to clustering, another significant concern is the energy wasted by malicious nodes that transfer unnecessary packets and cause packet drops. To identify these malicious nodes, the trustworthiness of nodes was estimated using the Sorensen function. The combined use of invasive weed optimization for clustering and the Sorensen function for trust estimation enhances the accuracy of detection and extends the lifespan of the WSN. The effectiveness of the proposed model, STIWWNO, was tested under various network conditions. The experiments revealed that the STIWWNO model improved throughput by 26.205% compared to the previous model ABC-NN. Additionally, spectrum utilization saw an enhancement of 24.26% when compared to the existing algorithms. These results highlight the model's efficiency in optimizing network performance. Future researchers can build upon this work by exploring WSN networks under different environmental conditions like under water, underground. This work has limitation that each node is free to occupy channel and no collision occurs.

## References


1. Rani P, Kavita, Verma S, Rawat D and Dash S. (2022). Mitigation of black hole attacks using firefly and artificial neural network. Neural Computing and Applications. 34:18. (15101-15111).
2. Farahani G and Chaudhry S. (2021). Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks. Security and Communication Networks. 2021.
3. Malnar M and Jevtic N. (2022). An improvement of AODV protocol for the overhead reduction in scalable dynamic wireless ad hoc networks. Wireless Networks. 28:3. (1039-1051).
4. M. S. Pathan, J. He, N. Zhu, Z. Ali, M. Qasim, and A. Azmat, “An efficient scheme for detection and prevention of black hole attacks in AODV-based MANETs,” International Journal of Advanced Computer Science and Applications, vol. 10, no. 1, pp. 243–251, 2019.
5. M. B. M. Kamel, I. Alameri, and A. N. Onaizah, “STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET,” in in 2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pp. 1278–1282, IEEE, 2017.
6. G. K. Wadhwani, S. K. Khatri, and S. K. Mutto, “Trust framework for attack resilience in MANET using AODV,” Journal of Discrete Mathematical Sciences and Cryptography, vol. 23, no. 1, pp. 209–220, 2020.
7. M. Kumar and J. Ali, "Taylor Sailfish Optimizer-Based Deep Stacked Auto Encoder for Blackhole Attack Detection in Wireless Sensor Network," in Journal of Web Engineering, vol. 21, no. 3, pp. 911-940, May 2022.
8. S. Jiang, J. Zhao and X. Xu, "SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments," in IEEE Access, vol. 8, pp. 169548-169558, 2020.
9. Iraq Ahmad Reshi, Sahil Sholla, Zahoor Ahmad Najar, Safeguarding IoT networks: Mitigating black hole attacks with an innovative defense algorithm, Journal of Engineering Research, 2024.
10. Khan, T., Singh, K., Ahmad, K. et al. A secure and dependable trust assessment (SDTS) scheme for industrial communication networks. Sci Rep 13, 1910 (2023).
11. Kosaraju Chaitanya, Gnanasekaran Dhanabalan. "Secure Route Detection with Multi Level Trust Evaluation Model Using Replicated Auditor Node for Extended Packet Delivery Rate in WSN". 2023 IIETA.
12. Pooja Rani, Kavita, Sahil Verma, Gia Nhu Nguyen. “Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm With Artificial Neural Network”. IEEE Access July 16, 2020.
13. Carass, A., Roy, S., Gherman, A. et al. Evaluating White Matter Lesion Segmentations with Refined Sørensen-Dice Analysis. Sci Rep 10, 8242, 2020.
14. Mojgan Misaghi, Mahdi Yaghoobi, Improved invasive weed optimization algorithm (IWO) based on chaos theory for optimal design of PID controller, Journal of Computational Design and Engineering, Volume 6, Issue 3, 2019.