# Taylor Sailfish Optimizer-Based Deep Stacked Auto Encoder for Blackhole Attack Detection in Wireless Sensor Network

Mandeep Kumar[1,*] and Jahid Ali[2]

[1]*Computer Science & Engineering, I.K. Gujral Punjab Technical University, Jalandhar – Kapurthala Highway, VPO – Ibban, Kapurthala-144603, India*
[2]*Computer Applications, Sri Sai Iqbal College of Management and Information Technology, V.P.O Badhani, Tehsil & Dist – Pathankot, Punjab, India*
*E-mail: mandeep_recj@yahoo.com; zahidsabri@rediffmail.com*
[*]*Corresponding Author*

Received 29 October 2021; Accepted 27 December 2021;
Publication 08 March 2022

## Abstract

Sensor nodes in Wireless sensor network (WSN) are distributed over a large area for sensing the pressure, temperature, humidity, and so on. They are at risk due to several attacks. In an attack like a black hole, the malicious node captures the whole data without any consideration of the active route, thus the source node are secured for communication. Hence, a new method name, Taylor SailFish Optimizer (TaylorSFO) is proposed to predict blackhole attacks in WSN. The training of the Deep stacked autoencoder is done through proposed Taylor-SFO, which is the integration of Taylor Series, and SailFish Optimizer (SFO). The newly developed Taylor-SFO is then applied for routing and blackhole attack detection at the WSN base station. Overall, two phases are included in the proposed model, which involves routing and blackhole attack detection at the base station. Initially, the WSN nodes are given to the routing module. Here, the routing is done based on the proposed

*Journal of Web Engineering, Vol. 21_3,* 911–940.
doi: 10.13052/jwe1540-9589.21316

TaylorSFO. Energy, distance as well as delay are the three fitness parameters considered for the routing. The proposed method shows the lowest delay of 21.23 ms, minimal FNR of 0.083, minimal FPR of 0.134, highest PDR of 94.87%, the highest throughput rate of 119.98 kbps, respectively.

**Keywords:** Blackhole attack, Taylor series, deep stacked autoencoder, SailFish Optimizer, routing.

## 1 Introduction

WSN has many sensors nodes grouped to get several mission-critical data [2, 9]. However, the features of WSN have made special importance for health care monitoring, signaling systems of railways, coal mines, industrial data gathering, traffic monitoring, vigilance in military installations, and so on [2, 10]. WSN contains cheap, tiny devices, termed nodes that are interfaced with sensors to sense the physical changes [31]. The periodic updating of data collected is done to the high-end node is called asSink or Base Station (BS) [2, 11]. The dry cell batteries are used for charging small nodes and non-conventional energy are used for some application like solar power and so on [2]. The WSN technology provides several advantages, like reducing costs, accuracy, ease of deployment, and scalability. The technological growth makes the sensors cheaper and smaller, and they are used widely in several applications like military, the healthcare environment [33], and security [3]. WSN is utilized to perform several tracking and monitoring work assists various smart tasks [4].

The selection of efficient paths in the network is termed routing [34]. The router is utilized to find the direction of traffic activated on the web [5]. For several forms of the sensor networks [35], routing is performed containing public switched telephone networks, transportation networks, and electronic information sensor networks [4]. WSN is affected by several attacks that damage and make the network unreliable for proper working and communication [32]. Several attacks on the network layer, which include selective forwarding, wormhole, hello flood, sinkhole, acknowledgment flooding, and false routing attacks have been paid considerable attention, recently [36]. The black hole attack is considered a severe threat on the WSNs [3, 12] that exploits WSN [30]. It improves the network packet loss. Here, the blackhole node makes appear itself more attractive [13, 14]. Therefore, most network nodes route their packets through the black hole into the sink node. After the establishment of the route [29], the increased packet loss [13, 15]

is due to the reduction of data packets from the other nodes [28] by the blackhole attacks. The blackhole node commonly uses maximal or very huge sequence numbers for making itself more attractive. The black hole thus has a new route towards the sink node by detecting the blackhole by malicious manipulation.

The existing methods to prevent, and reduce the attacks are not appropriate for WSN, due to the fewer capabilities of the WSN. However, the attacks on the WSN are rapidly increasing. However, these attacks are increasing day by day in number and the attack launch complexities. Attacks are increasingly causing huge damages and losses to businesses and industries [2]. To predict black hole attacks [26, 27], a method in [2, 16] uses a new method using Support Vector Machines (SVM). Here, entire computation for intrusion detection is performed in the BS, thereby the sensor nodes do not require for contributing to the activity preserving scarce energy. For identifying the attack nodes, the black hole detection method was introduced in [5, 17] in the small network infrastructure. Machine learning techniques were utilized in [5, 18] for classifying normal and attack node accurately, but still, for detecting attacks, the time taken was higher.

This research aims to design a blackhole attack detection approach in WSN using the steps routing, and blackhole attack detection at Base Station (BS). The WSN node is initially simulated, and routing is performed using the proposed TaylorSFO where the energy, distance, and energy parameters are considered for better routing. The black hole attack is detected in the BS using Deep stacked autoencoder.

The major contribution of the proposed work is:

- ***Proposed TaylorSFO-based Deep stacked autoencoder*:** The Deep stacked autoencoder is developed for black hole attack detection. Here, Deep stacked autoencoder is trained using the proposed TaylorSFO.
- ***Taylor SFO*:** TaylorSFO is developed by com,bining the Taylor series and SFO. Fitness function of TaylorSFO is designed by considering different constraints, such as distance, energy, and delay to perform blackhole attack detection.

The structure of the manuscript is as follows: Section 2 shows a brief discussion about the conventional blackhole attack detection strategies. The WSN model is discussed in Section 3. The black hole attack detection using TaylorSFO-based Deep stacked auto-encoder is described in Section 4, and in Section 5, the efficiency analysis with various methods are depicted and at last Section 6 ends the paper.

## 2 Motivation

This part illustrates eight classical blackhole attack detection strategies along with their limitations are mentioned. These limitations are considered in research for improved attack detection.

### 2.1 Literature Survey

Few classical attack detection techniques for preventing the blackhole attacks in WSN are illustrated below: J. Sebastan Terence and Geethanjali Purushothaman [1] developed a Warning message counter method (WMC) for identifying the packet dropping attacks in WSN. In packet dropping detection, the method obtained minimum false positive and negative but failed in the detection of cooperative attacks. Abdullah Aljumah, Tariq Ahamed Ahanger [2] introduced a method for blackhole attacks prediction in WSN. In the network, the client nodes are chosen by the attacker and reconfigured for dropping the received packets which results in maximum delay and minimum throughput. It provides entire traffic coming towards it from their associated nodes, but still, the method does not increase the number of attackers to check the stability. Hanane Kalkha et al. [3] designed a Hidden Markov model for finding the malicious nodes, and for preventing blackhole attacks in WSN. This approach was utilized to design the shortest decisions path, by selecting the source node for communication. The method can improve the network performance; however important techniques are needed to be considered for performance enhancement. Deepak C. Mehetre [4] developed a dual assurance scheme and two-stage security mechanism for detecting black hole attacks. The untrusted path was identified for providing a secure routing path based on trust. The malicious nodes in the network are identified by this method with maximal energy efficiency. However, it does not execute in the real world for transmitting the secure node.

A. John Clement Sunder and A. Shanmugam [5] developed a method named Jensen–Shannon Divergence Based Independent Component Analysis (JDICA) for detecting and preventing blackhole attacks. With the physiological data collected from the biomedical sensors, the black hole attack was found. The dependence between nodes was determined using mutual probability function and probability distribution of independent functions. However, the detection time was higher. Anastasia Tsiota et al. [6] analyzed the effect of two Denial of Service (DoS) attacks, using Heterogeneous Wireless Networks (HWNs). Here, the node was modeled with a homogeneous

Poisson point process (PPP). Using the prescribed probability, the node type for the given network tier was identified. However, the optimal association policy was not considered for malicious nodes detection. M. Rajesh Babu et al. [7] developed an architecture-level solution for sustaining the network for many applications. The outputs here were followed for handling black hole attacks to prove a better solution for black hole attacks. Other domain applications, such as environmental or earth sensing, entertainment industry, and industrial monitoring, were not considered. Bindu Ran et al. [8] addressed the effect of black hole attacks in the AODV protocol with various parameters. Here, two different scenarios were taken with the range of malicious nodes from 2 to10. In the first scenario, the mobility model was static, whereas in the second scenario the mobility is mobile. The method harms the authenticity of the network and also drop packet causing no communication between source and destination node.

## 2.2 Challenges

The limitations of a few conventional blackhole attack detection methods are portrayed below:

- In [2], the futuristic method is developed to prevent and detect blackhole attacks in the WSN but does not design the powerful method for defending and detecting the WSN from blackhole attacks.
- In [4], a trustable and secure routing method is devised for detecting and preventing black holes and the selective forwarding attack in the clustered WSN with the active trust. However, the non-forbearance of the possible security obstacles in the routing area is dangerous.
- In [5], JDICA is introduced to prevent and detect blackhole attacks in healthcare WSN. Although, the attack detection performance of the method was not effective as it considered only the trust node's values.
- In [6], the Multitier HWN model is developed for detecting Black Hole Attacks in HWN. However, the method unable to incorporate potential observation error for perfect detection scenario for deriving the expressions to analyze and model the performance of the network under several sophisticated DoS attacks that evolve in the time domain.
- In [7], the Proactive Alleviation Procedure is utilized for detecting maliciously behaving nodes, but still, network management and configuration was not considered for obtaining a better caliber of network and their operations.

## 3 System Model

In WSN, large distributed services, that observes the physical and environmental changes with the use of sensor nodes, which are also used for sending and receiving information using the wireless path. The arrangement of sensor nodes are at random in the terrain and key feature of the WSN are self-organizing and cooperative nodes. To carry the information, the processing capability is used by the noise and the necessary data is broadcasted only to the recipient. Limited power is needed by the sensor node and in general, they are non-replaceable. Several orders of magnitude are held by the nodes in the sensor network, such that the WSN topology changes regularly. All nodes are responsible for data exchange. Figure 1 reveals the system model of WSN.

### 3.1 Energy Model

Battery power [23] is used by sensor nodes and network lifetime is improved with the energy of nodes. In WSN, the energy model is performed in different modes like idle transmitting, receiving, and sleeping mode. For finding the

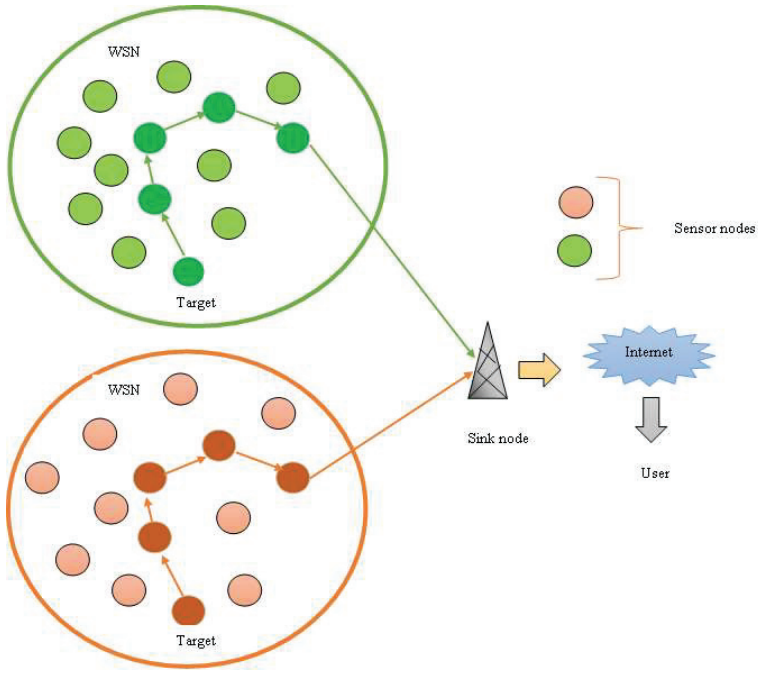



**Figure 1** System model of WSN.

route, maximal energy node is selected and for data transmission, minimum energy node is considered, which is gathered in the routing table. For different time intervals, the energy value for a node is computed and the energy-consuming node is predicted as,

$$P^a(t) = A_g^a * P_g^a + A_h^a * P_h^a \tag{1}$$

Where, the energy of $a^{th}$ node at a time $t$, is specified as $P^a(t)$ and $A_g^a$ signifies the data packets sent by $a^{th}$ node, the data packets received by $a^{th}$ node is given by $A_h^a$, $P_h^a$ and $P_g^a$ shows the energy for receiving and transmitting the packets. The term $P_g^a$ and $P_h^a$ is derived as,

$$P_g^a = A * \tau \tag{2}$$

$$P_h^a = \beta * \kappa \tag{3}$$

where, the time required for transmission is $A$ and $\beta$, wheras, $\tau$ and $\kappa$ terms the power required to send and receive the data.

$$P_\lambda = PP - P^a(t) \tag{4}$$

where, the initial sensor nodes energy is $PP$. For every node, the energy is verified with threshold value by finding the residual energy $P_\lambda$ and transmits the nodes with minimum.

### 3.2 Mobility Model

In mobility model [24], the movements of nodes are specified and evaluate the routing process for data transmission in WSN. In real-time applications, the movements of the nodes are imitated by the mobility model. An optimal analysis method is a random mobility scheme, because of its simplicity and wide availability. The term $a$ and $b$ are two sensor nodes with initial positions as $(r_1, s_1)$ and $(r_2, s_2)$. These nodes move with angle $\theta_1$ and $\theta_2$ with velocity change in the x-axis. At a time interval $t$, node $a$ and $b$ move with distance $d_1$ and $d_2$. They move to the new location, after the mobility process, at $t^{th}$ time. The distance between the nodes $a(r_1, s_1)$ and $b(r_2, s_2)$ are mentioned as,

$$\alpha_{(a,b)} = \sqrt{|r_1 - r_2|^2 + |s_1 - s_2|^2} \tag{5}$$

where the distance between the nodes $a(r_1, s_1)$ and $b(r_2, s_2)$ is specified as $\alpha_{(a,b)}$.

## 4 Proposed Blackhole Attack Detection Model Using Deep-stacked Autoencoder

This research aims to facilitate the energy-aware routing and assure the black hole attacks detection in WSN using a deep-stacked autoencoder. This research extends the network lifetime by facilitating energy-aware routing and ensuring secure communication. Here, two steps are employed for the attack detection which involves routing, and blackhole attack detection at BS. At first, the WSN is simulated and energy-aware routing and attack detection is initiated in the network. After simulated, the proposed TaylorSFO performs routing, where the fitness parameters are considered for routing are energy, distance, and delay. After that, the black hole detection is performed at the WSN base station. The data is pre-processed first at the BS, and based on the pre-processing result the feature extraction is processed. At last, by using a Deep stacked autoencoder [21, 25], the black hole attack is detected. The Deep stacked autoencoder is trained here with the proposed TaylorSFO. Figure 2 reveals the structure of the proposed black hole attack detection model.

### 4.1 Routing Based on the Proposed Taylor SailFish Optimizer-based Deep-stacked Autoencoder

Routing is essential in WSN as it assists to send data. The routing is required for transmitting data between the nodes and BS to establish communication.

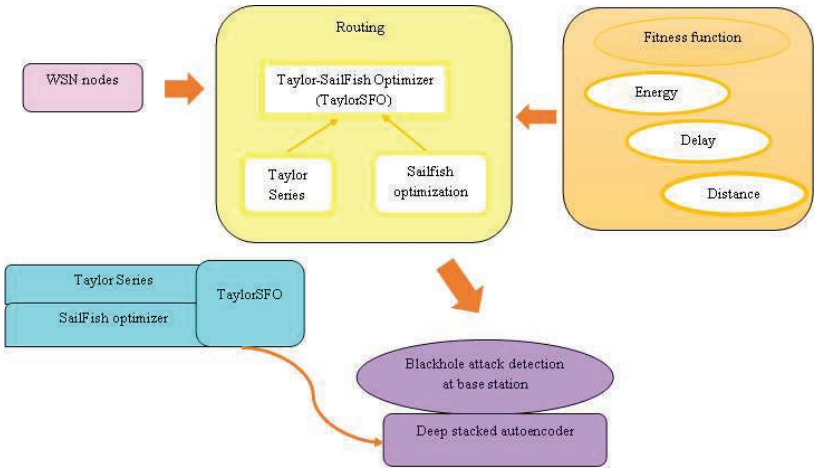



**Figure 2** Schematic view of the blackhole attack detection using the proposed TaylorSFO-based Deep Stacked autoencoder.

Here, TaylorSFO algorithm is employed for initiating routing for transferring collected data to BS. TaylorSFO is introduced by incorporating the Taylor series [19] in SFO [20]. Taylor series deals with the higher-order term. SFO inspires the hunting behaviour of sailfish. Intensification and diversification are the two population tips considered in SFO. Sailfish is the fastest fish that can reach the maximum speed of about 100 km per hour. On the surface, they hunt the sardines. They injure many sardines, taps, by making the slashing motion, and weaken the sardine. By using the populations of predator and prey, the hunting behaviour in SFO is simulated. However, with the alternation of attacks, the prey grouping is broken. The integration of Taylor series with SFO boosts the performance of accuracy in classification with the use of the parametric features from the inherited optimization. The algorithmic steps involved in TaylorSFO algorithm is illustrated below:

***(i) Population initialization:*** The sailfish and sardine population is initialized randomly as,

$$Z = \{Z_1, Z_2, \ldots, Z_\ell, \ldots, Z_\kappa\} \tag{6}$$

where $Z_\ell$ indicate $\ell^{th}$ solution and $\kappa$ represent total solutions.

***(ii) Determination of fitness***

The fitness measure computes the finest solution to find the blackhole attack. Based on distance, energy, and delay the fitness is computed, and the maximal fitness is considered as the best solution, which is mentioned as,

$$F = \frac{1}{3}[P_\alpha + (1 - D_\alpha) + (1 - J)] \tag{7}$$

where, $P_\alpha$ denotes the energy, $D_\alpha$ indicates the distance, and $J$ is represented as delay.

***(iii) Elitism***

Elitism gets the same solution of fittest into further generation. In SFO, elite considers the optimal location of sailfish for all iteration. During the attack, the elite sailfish affect the maneuverability, as they are the fittest sailfish. By slashing motion, the sardines get injured in group hunting, with the sailfish's rostrum. Thus for every iteration, the location of the injured sardine are stored and selects the best target. The highest fitness at $j^{th}$ iteration considering the location of elite sailfish is $Z^j_{elite-sf}$ and injured sardine is $Z^j_{injured-s}$.

***(iv) Attack alternation strategy***

Mostly, the prey is attacked by the sailfish when there are no compatriots. That is, the success rate in the hunting of sailfish is promoted with temporally

coordinated attacks. The sailfish's location is adjusted with respect to other hunter's locations around prey schools. Thus, SFO exhibits that when hunting is performed in groups, the sailfish's attack in an alternate approach. Every sardine in the imitating process upgrades the current optimal location and attack power. Update equation of SFO is,

$$Z^j_{\tau+1} = Z^j_{elite-sf} - \beta_j(rand(0,1)) \left( \frac{Z^j_{elite-sf} + Z^j_{injured-s}}{2} \right) - Z^j_{\tau} \tag{8}$$

where $Z^j_{elite-sf}$ represents the elite sailfish's location, $Z^j_{injured-s}$ refers to the location of injured sardine, $rand(0,1)$ signifies the number in random between 0 and 1, and $\beta_j$ indicates coefficient at $j^{th}$ iteration.

To get globally optimal solutions, the Taylor series [19] is used, which shows the position update as,

$$\begin{aligned} Z^j_{\tau+1} = {} & 0.5Z^j_{\tau} + 1.3591\, Z^j_{\tau-1} - 1.359\, Z^j_{\tau-2} + 0.6795Z^j_{\tau-3} \\ & - 0.2259\, Z^j_{\tau-4} + 0.0555Z^j_{\tau-5} \\ & - 0.0104Z^j_{\tau-6} + 1.38e^{-3}Z^j_{\tau-7} - 9.92e^{-5}Z^j_{\tau-8} \end{aligned} \tag{9}$$

$$Z^j_{\tau} = 2 \begin{bmatrix} Z^j_{\tau+1} - 1.3591\, Z^j_{\tau-1} + 1.359\, Z^j_{\tau-2} - 0.6795Z^j_{\tau-3} \\ +0.2259\, Z^j_{\tau-4} - 0.0555Z^j_{\tau-5} \\ +0.0104Z^j_{\tau-6} - 1.38e^{-3}Z^j_{\tau-7} + 9.92e^{-5}Z^j_{\tau-8} \end{bmatrix} \tag{10}$$

Substituting Equation (10) in Equation (8),

$$Z^j_{\tau+1} = Z^j_{elite-sf} - \beta_j \left( \begin{array}{l} rand(0,1) \left( \dfrac{Z^j_{elite-sf} + Z^j_{injured-s}}{2} \right) \\ \qquad -2 \begin{bmatrix} Z^j_{\tau+1} - 1.3591\, Z^j_{\tau-1} + 1.359\, Z^j_{\tau-2} \\ -0.6795Z^j_{\tau-3} + 0.2259\, Z^j_{\tau-4} \\ -0.0555Z^j_{\tau-5} + 0.0104Z^j_{\tau-6} \\ -1.38e^{-3}Z^j_{\tau-7} + 9.92e^{-5}Z^j_{\tau-8} \end{bmatrix} \end{array} \right) \tag{11}$$

$$Z^j_{\tau+1} = Z^j_{elite-sf} - \beta_j \left( rand(0,1) \left( \frac{Z^j_{elite-sf} + Z^j_{injured-s}}{2} \right) \right) + \beta_j 2 Z^j_{\tau+1} - 2\beta_j \begin{bmatrix} 1.3591\, Z^j_{\tau-1} - 1.359\, Z^j_{\tau-2} + 0.6795 Z^j_{\tau-3} \\ -0.2259\, Z^j_{\tau-4} + 0.0555 Z^j_{\tau-5} \\ -0.0104 Z^j_{\tau-6} + 1.38e^{-3} Z^j_{\tau-7} \\ -9.92e^{-5} Z^j_{\tau-8} \end{bmatrix} \tag{12}$$

$$Z^j_{\tau+1}\left[1 - 2\beta_j\right] = Z^j_{elite-sf} - \beta_j \left( rand(0,1) \left( \frac{Z^j_{elite-sf} + Z^j_{injured-s}}{2} \right) \right) - 2\beta_j \begin{bmatrix} 1.3591\, Z^j_{\tau-1} - 1.359\, Z^j_{\tau-2} + 0.6795 Z^j_{\tau-3} \\ -0.2259\, Z^j_{\tau-4} + 0.0555 Z^j_{\tau-5} \\ -0.0104 Z^j_{\tau-6} + 1.38e^{-3} Z^j_{\tau-7} \\ -9.92e^{-5} Z^j_{\tau-8} \end{bmatrix} \tag{13}$$

The final update equation is expressed as,

$$Z^j_{\tau+1} = \frac{1}{1-2\beta_j} \left\{ Z^j_{elite-sf} - \beta_j \left( rand(0,1) \left( \frac{Z^j_{elite-sf} + Z^j_{injured-s}}{2} \right) \right) - 2\beta_j \begin{bmatrix} 1.3591\, Z^j_{\tau-1} - 1.359\, Z^j_{\tau-2} + 0.6795 Z^j_{\tau-3} \\ -0.2259\, Z^j_{\tau-4} + 0.0555 Z^j_{\tau-5} \\ -0.0104 Z^j_{\tau-6} + 1.38e^{-3} Z^j_{\tau-7} \\ -9.92e^{-5} Z^j_{\tau-8} \end{bmatrix} \right\} \tag{14}$$

where, $\beta_j = 2rand(0,1)QB - QB$. Here, $QB$ refer to prey density, which portrays several preys at every iteration. When prey count is minimized at

group hunting, the $QB$ is utilized to update the location of sailfish. The prey density equation is expressed as,

$$QB = 1 - \left( \frac{M^{sf}}{M^{sf} + M^{s}} \right) \tag{15}$$

where, for each cycle, $M^{sf}$ and $M^{s}$ represents the amount of sardines and sailfish.

***(v) Hunting and catching prey***

Initially, the potential for escape and power of sardines for the attack is normally maximum. Thus, in the beginning, the sailfish injures the sardines without catching them. The power of sailfishes during attack will reduce the escaping ability of sardines and when they get injured in its body it takes the alternation strategies of the attacks. This shows that the last stage to escape. Thus, the success rate is maximum and each sardine's location is updated using the below equation,

$$Z^{j}_{\tau+1} = s \times (Z^{j}_{elite-sf} - Z^{j}_{\tau} + BA) \tag{16}$$

where, the current location of sardine $j$ is represented as $Z^{j}_{\tau+1}$ and $Z^{j}_{\tau}$. The term $s$terms the number in random between 0 and 1, the optimal location of elite sailfish is termed as $Z^{j}_{elite-sf}$. $BA$ terms the amount of sailfish attack power for each iteration and is expressed as,

$$BA = B \times (1 - (2 \times Itn \times \eta)) \tag{17}$$

where, $B$ and $\eta$ are the coefficients minimizing the power attack value, and $itn$ terms the current iteration. Based on the amount of sailfish attack power $BA$, the location update using the last stage of the hunt is mentioned as,

$$\mu = M^{s} \times BA \tag{18}$$

$$\lambda = b_{j} \times BA \tag{19}$$

where, $\mu$ represents the location of sardine, and $\lambda$ defines sardine variables, the iteration $j$ variables are expressed as $b_j$ and $M^s$ terms the sardines in each cycle. When $BA < 0.5$, sardines with $\mu$ variables are updated, if $BA \geq 0.5$, then update all sardines location.

***(vi) Compute the feasibility:*** Using Equation (7), the fitness value is computed for each search agent. Here the optimal fitness measure is calculated from the maximal value generated and is taken as the best solution.

***(vii) Termination:*** The steps mentioned above will be continued till the best solution or particular iteration is obtained. The pseudo-code of developed TaylorAFO is given in Algorithm 1.

**Algorithm 1** Pseudo-code of developed model

**Input: Sailfish and sardine population** $Z = \{Z_1, Z_2, \ldots, Z_\ell, \ldots, Z_\kappa\}$
**Output: Best sailfish (solution)**
Initialize the sailfish and sardine population, and parameters
compute Fitness function
Determine optimal sailfish and sardine
**while** stopping criteria is not satisfied
    **for every sailfish**
        Compute the coefficient at $j^{th}$ iteration
        Update SFO based on Equation (8)
        Update the Taylor series using Equation (10)
        Update the TaylorSFO using Equation (14)
    **end for**
    Compute $BA$ based on Equation (17)
    **if** $BA < 0.5$
        Compute $\mu$ based on Equation (18)
        Estimate $\lambda$ based on Equation (19)
        Choose the sardine using the value of $\lambda$ and $\mu$
        update location of selected sardine using Equation (16)
    **else**
        All the location of sardine is updated using Equation (16)
    **end if**
    Re-checking the feasibility of solutions based on Equation (7)
    **if better solution is found**
        **Update the optimal sailfish with better sardine**
    **end if**
**end while**
**Return the best sailfish**
**End**

## 4.2 Blackhole Attack Detection at the Base Station Using Deep-stacked Autoencoder

Once the routing is carried out based on the proposed TaylorSFO then it is required to find the blackhole attack detection at BS. WSN is susceptible to various kinds of attacks wherein the blackhole attack is common which is complex to discover and prevent. The data is pre-processed initially, and the feature extraction is performed next to pre-processing for detecting black

hole attacks effectively. After that, a deep-stacked autoencoder is employed for detecting the blackhole attacker. This attack occurs when the sensor nodes are captured by the attacker to block packets and stop them to reach BS. This brought up the necessity to devise a deep-stacked autoencoder to find a black hole attack. The structure of deep-stacked autoencoder is illustrated below:

### 4.2.1 Architecture of the deep-stacked autoencoder

Deep stacked autoencoder, [21, 25] has $R$ input visible units, $V$ hidden and $W$ output visible units and it adapts suitable features of the input. The deep-stacked autoencoder design is portrayed in Figure 3. The operation of the autoencoder is based on input vector encoding with phase hidden version which is represented as$X$. The deterministic mapping $T_\theta$ converts the input vector $U$ into a hidden vector in the encoder, which is mentioned as,

$$U = fun(\omega_1 U + L_1) \tag{20}$$

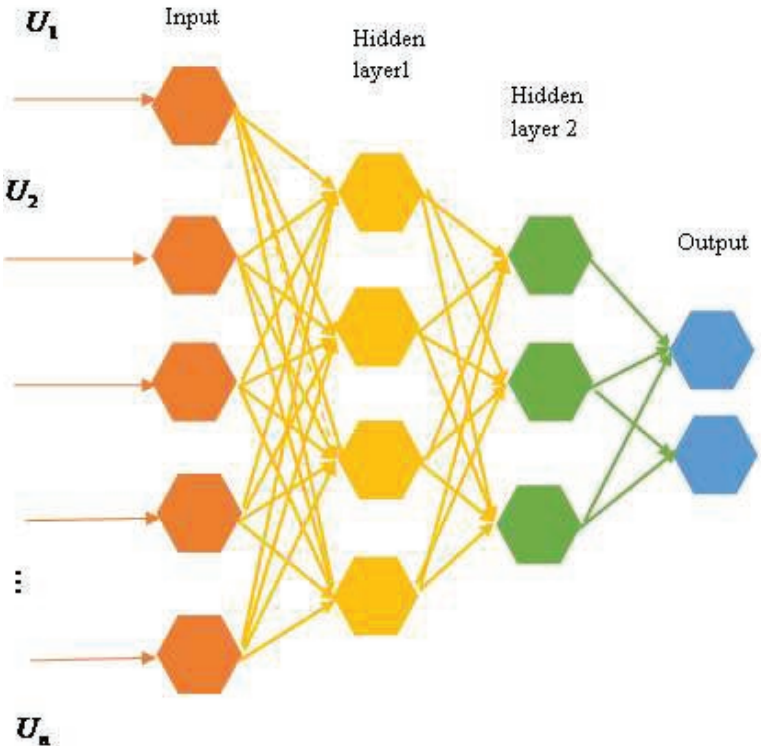



**Figure 3** The architecture of deep stack auto-encoder.

where, the weight matrix is represented as $\omega_1$, and $L_1$ and $L_2$ indicate bias vector. After decoding hidden $X$ to reconstruct $T$, the equation is expressed as,

$$\hat{Y} = fun(\omega_2 V + L_2) \tag{21}$$

where $\omega_2$ is the weight matrix, and $V$ is the hidden units.

The stacked auto-encoder uses processing steps like Initialization of parameters at first and then the hidden layer activation of the succeeding auto-encoder and then fine-tuning. Here, each parameter change at the same time to enhance the detection result.

#### 4.2.2 Training of Deep stacked auto-encoder using TaylorSFO algorithm

The proposed optimization TaylorSFO algorithm trains the Deep stacked autoencoder. The classifier's weight is trained to get the optimal solution. TaylorSFO is developed by combining the Taylor series [19] with the SFO [20] for effective optimal weight selection and to attain the update process. The algorithmic procedure of the developed TaylorSFO algorithm is briefly elaborated in Section 3.1.

## 5 Results and Discussion

The result discussion of developed TaylorSFO-based Deep stacked autoencoder for black hole attack detection in WSN is mentioned in this section.

### 5.1 Experimental Setup

The proposed method used NS2 tool with windows 10 OS, 4GB Ram, and Intel I3 processor for experimentation. Table 1 shows the simulation parameter of the developed TaylorSFO-based Deep stacked autoencoder.

### 5.2 Dataset Description

The developed TaylorSFO-based Deep stacked autoencoder is processed using KDD Cup 1999 dataset [22], which is used in Third International Knowledge Discovery and Data Mining Tools Competition conducted in conjunction with the KDD-99, fifth International Conference on Knowledge Discovery and Data Mining. It is used for designing a network intrusion detector to differentiate "bad" connections, termed attacks, and the "good" connections.

**Table 1** Simulation setup

| Parameter | Values |
|---|---|
| Channel type | WirelessChannel |
| Radio-propagation model | TwoRayGround |
| Network interface type | Phy/WirelessPhy |
| Type | Mac/802_11 |
| Interface queue type | Queue/DropTail/PriQueue |
| Layer type | LL |
| Antenna model | OmniAntenna |
| Packet size | 50 |
| Number of mobile nodes | 30 |
| Routing protocol | DSDV |
| X Dimension of topography | 1501 |
| Y Dimension of topography | 600 |
| Time of simulation end | 15 seconds |
| Duration of each transmission | 0.1 seconds |
| Time gap between two transmissions | 0.01 seconds |
| Maximum number of times the transmission simulation repeated | 10 |
| Maximum transmission at one time | 2 |

### 5.3 Evaluation Metrics

The developed TaylorSFO algorithm is performed based on delay, throughput, False positive rate (FPR), Packet Delivery rate (PDR), and False Negative Rate (FNR) by varying the rounds.

***(a) Delay:*** Delay denotes the time for data packets to reach destination.

***(b) Throughput:*** Number of data packets received at a particular time terms the throughput, which is represented by,

$$\textit{Throughput} = \frac{X}{h} \tag{22}$$

where $X$ refer received nodes at simulation time $h$.

***(c) PDR:*** It defines the ratio of received and transmitted data.

$$PDR = \frac{\textit{Received data packets}}{\textit{Sent data packets}} \tag{23}$$

***(d) FPR:*** The FPR is the ratio of negative events count classified by mistake as positive and the entire actual negative events.

$$FPR = \frac{F^p}{T^n + F^p} \tag{24}$$

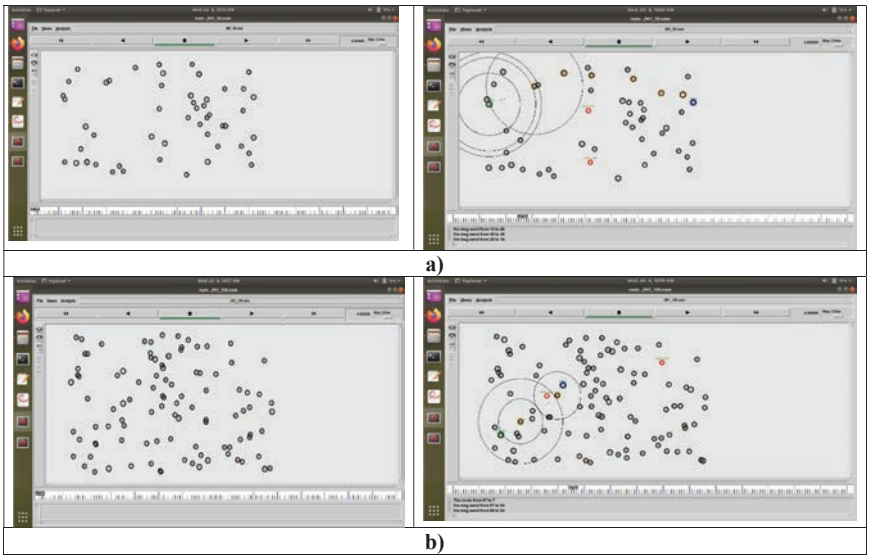



**Figure 4** Sample results using nodes, (a) 50, and (b) 100.

where $F^p$ denote false positive, $T^n$ represent true negative.

***(e) FNR***: It is defined as the rate of incorrectly identified the black hole attack out of the total attacks.

$$FNR = \frac{F^n}{T^p + F^n} \tag{25}$$

where, $F^n$ referring to a false negative, and the term $T^p$ represents true positive.

## 5.4 Experimental Results

Simulation setup for the proposed model is shown in this section. The sample results are revealed in Figure 4. Figure 4(a), and 4(b) reveals the simulation results of the developed model for 50, and 100 nodes. During transmission, the data transmitting nodes should be within the transmission range. Here, the black color circle denotes the nodes, the red color circle represents the attack node, and the blue with black circle refers to the source node.

## 5.5 Performance Analysis

This part discusses the analysis of proposed model with different hidden neurons. The analysis is done based on metrics.

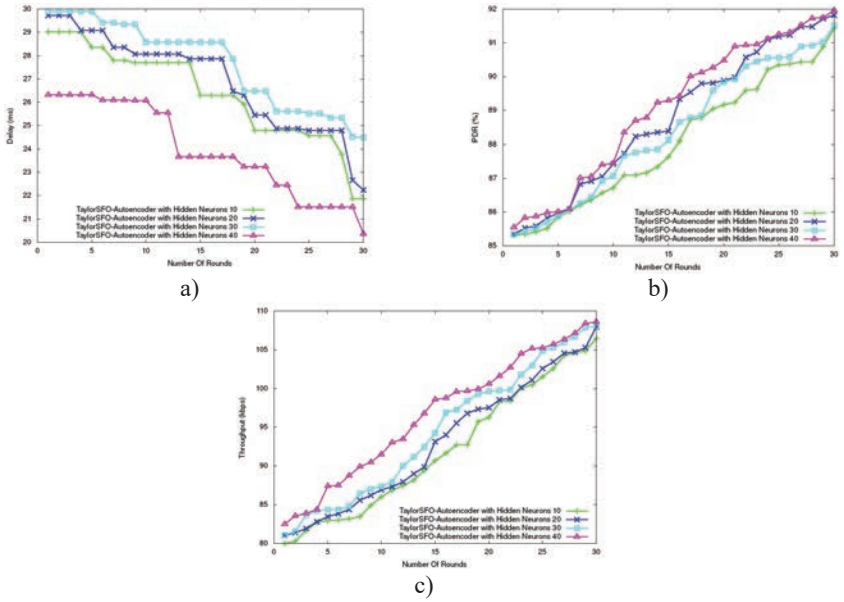



**Figure 5** Performance analysis with hidden neurons using 50 nodes (a) delay, (b) PDR, (c) and throughput.

***(a) Analysis based on 50 nodes***

The analysis with different hidden neurons based on 50 nodes is depicted in Figure 5. For the delay metric, the analysis by changing the rounds is shown in Figure 5(a). For rounds = 30, the delay values of the proposed model with hidden neurons 10, 20, 30, and 40 are 21.87 ms, 22.25 ms, 24.49 ms, and 20.37 ms. Figure 5(b) portrays the performance analysis of PDR. When a number of rounds = 30, PDR value measured by TaylorSFO-based Deep stacked autoencoder with hidden neuron 10 is 91.43%, TaylorSFO-based Deep stacked autoencoder with hidden neuron 20 is 91.81%, TaylorSFO-based Deep stacked autoencoder with hidden neuron 30 is 91.51%, and TaylorSFO-based Deep stacked autoencoder with hidden neuron 40 is 91.96%. The analysis based on throughput metrics with different rounds is shown in Figure 5(c). For the 30th round, throughput values of the proposed model with hidden neurons 10, 20, 30, and 40 are 106.47 kbps, 107.96 kbps, 108.07 kbps, and 108.61 kbps.

***(b) Analysis based on 100 nodes***

The developed model analysis with different hidden neurons based on 100 nodes is depicted in Figure 6. The analysis for delay metric by varying the

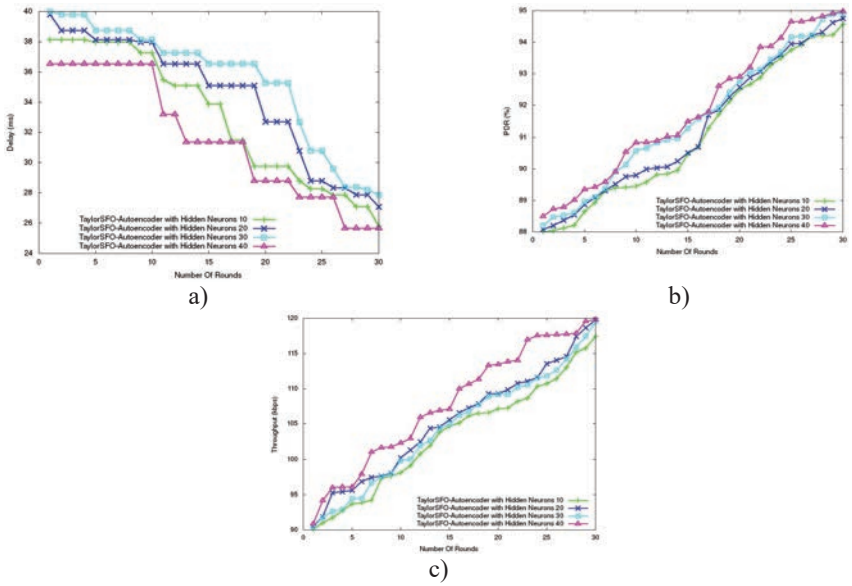
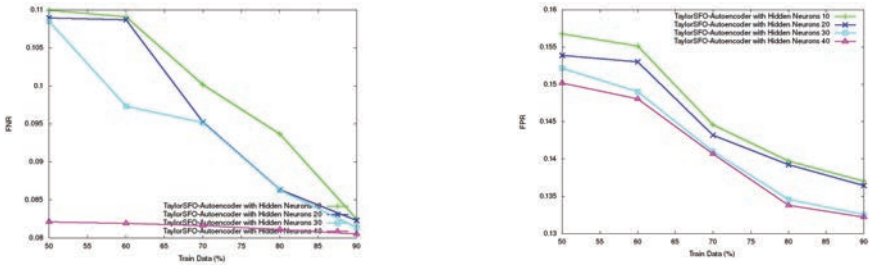



**Figure 6** Performance analysis with hidden neurons based on 100 nodes (a) delay, (b) PDR, (c) and throughput.

rounds is shown in Figure 6(a). For the 30th round, the delay values of the proposed model with hidden neurons 10, 20, 30, and 40 are 25.82 ms, 27.07 ms, 27.87 ms, and 25.68 ms. Figure 5(b) portrays the performance analysis of PDR. When a number of rounds = 30, the PDR value measured by TaylorSFO-based Deep stacked autoencoder with hidden neuron 10 is 94.56%, TaylorSFO-based Deep stacked autoencoder with hidden neuron 20 is 94.74%, TaylorSFO-based Deep stacked autoencoder with hidden neuron 30 is 94.96%, and TaylorSFO-based Deep stacked autoencoder with hidden neuron 40 is 94.97%. The analysis based on throughput metrics with different rounds is shown in Figure 6(c). When rounds are 30, the throughput values of the proposed model with hidden neurons 10, 20, 30, and 40 are 117.46 kbps, 119.78 kbps, 119.50 kbps, and 119.79 kbps.

***(c) Analysis using training data percentage***

The analysis by changing the training data is revealed in Figure 7. The analysis for FNR by varying the rounds is shown in Figure 7(a). For 90% training data, the FNR values of proposed model with hidden neurons 10, 20, 30, and 40 are 0.0824, 0.0822, 0.0813, and 0.0805. Figure 7(b) gives the analysis of FPR. For 90% training data, the FPR value measured by




a) b)

**Figure 7** Performance analysis with training data percentage (a) FNR, and (b) FPR.

TaylorSFO-based Deep stacked autoencoder with hidden neuron 10 is 0.137, TaylorSFO-based Deep stacked autoencoder with hidden neuron 20 is 0.136, TaylorSFO-based Deep stacked autoencoder with hidden neuron 30 is 0.1325, and TaylorSFO-based Deep stacked autoencoder with hidden neuron 40 is 0.1322.

## 5.6 Comparative Methods

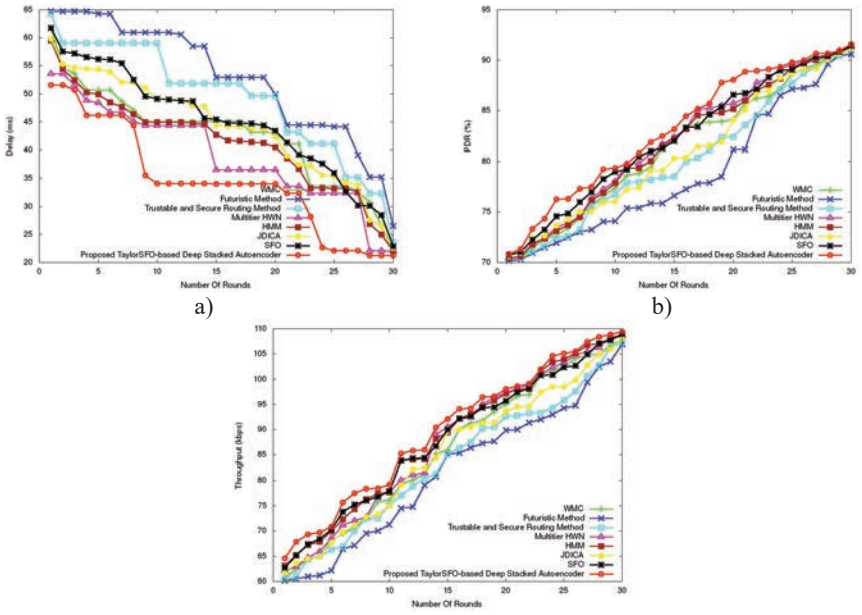
The developed method is compared with the existing method like WMC [1], Futuristic method [2], Trustable and secure routing method [4], and Multitier HWN [6], Hidden Markov Model (HMM) [3], Jensen–Shannon Divergence Based Independent Component Analysis (JDICA) [5], SFO [20].

## 5.7 Comparative Analysis

The comparative analysis is described in this section for the developed TaylorSFO-based Deep stacked autoencoder approach with different performance metrics by varying number of rounds.

***(a) Analysis using 50 nodes***

The analysis for different rounds using 50 nodes is deliberated in Figure 8. The analysis for delay is given in Figure 8(a). The delay for round = 30 measured by WMC, Futuristic method, Trustable and secure routing method, Multitier HWN, HMM, JDICA, SFO, and the proposed model are 0 ms, 22.11 ms, 26.48 ms, 23.56 ms, 21.92 ms, 22.00 ms, 22.56 ms, 22.92 ms, and 21.23 ms. The PDR analysis is revealed in Figure 8(b). For round = 30, the PDR measured by WMC, Futuristic method, Trustable and secure routing method, Multitier HWN, HMM, JDICA, SFO, and the proposed model is 91.17%, 90.59%, 91.10%, 91.38%, 91.27%, 91.13%, 91.41%, and 91.57%.




a) b)

**Figure 8** Comparative analysis with 50 nodes by varying rounds (a) Delay, (b) PDR, and (c) throughput.

The throughput analysis is portrayed in figure 8c). When round = 30, the throughput measured by WMC, Futuristic method, Trustable and secure routing method, Multitier HWN, HMM, JDICA, SFO, and the proposed model is 107.94 kbps, 106.97 kbps, 107.30 kbps, 108.58 kbps, 108.87 kbps, 108.198 kbps, 108.96 kbps, and 109.40 kbps.

***(b) Analysis using 100 nodes***

The analysis for performance metrics by varying the rounds using 100 nodes is given in Figure 9. In terms of delay, the analysis result is illustrated in Figure 9(a). When round = 30, the delay measured by WMC, Futuristic method, Trustable and secure routing method, Multitier HWN, HMM, JDICA, SFO, and the proposed model are 28 ms, 28.17 ms, 30.66 ms, 26.63 ms, 27.42 ms, 28.23 ms, 28.63 ms, and 24.31 ms. The analysis for PDR is illustrated in Figure 9(b). For round = 30, the PDR measured by WMC, Futuristic method, Trustable and secure routing method, Multitier HWN, HMM, JDICA, SFO, and the proposed model is 94.77%, 94.09%, 93.06%, 94.85%, 94.83%, 94.53%, 94.35%, and 94.87%. The analysis for

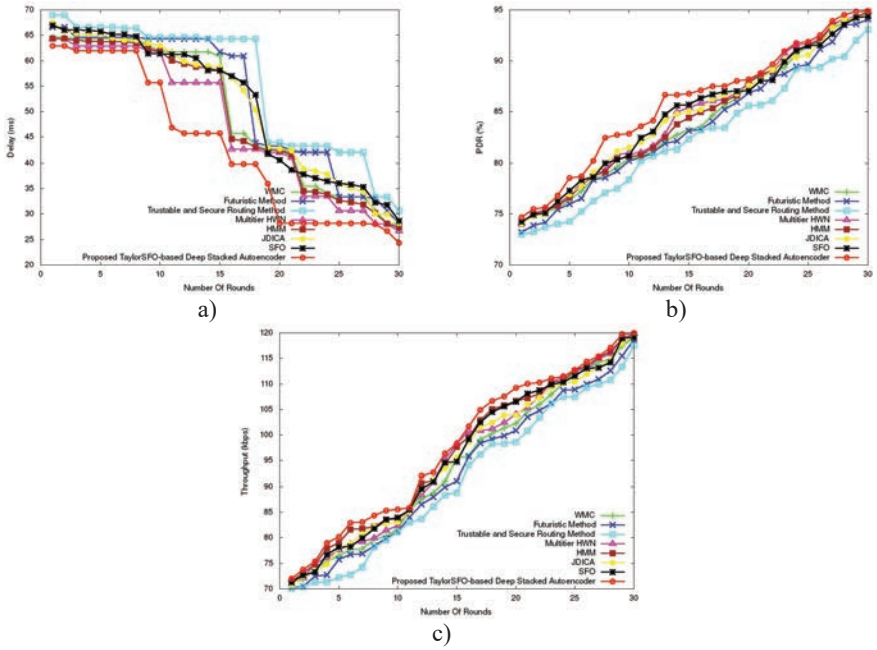
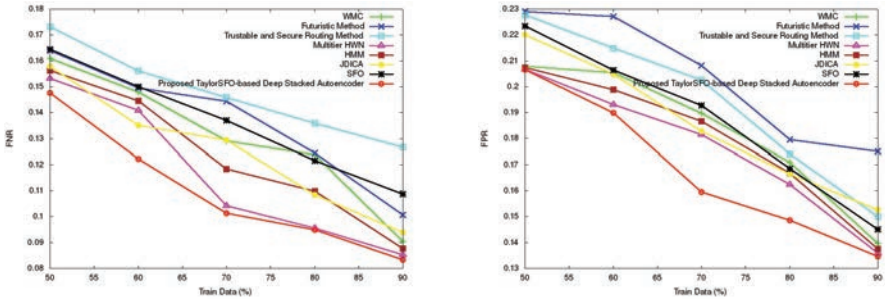



**Figure 9** Comparative analysis with 100 nodes by varying rounds (a) Delay, (b) PDR, and (c) throughput.

throughput is illustrated in Figure 9(c). When round = 30, the PDR measured by WMC, Futuristic method, Trustable and secure routing method, Multitier HWN, HMM, JDICA, SFO, and the proposed model is 119.14 kbps, 118.62 kbps, 117.53 kbps, 119.83 kbps, 119.64 kbps, 119.38 kbps, 119.14 kbps, and 119.98 kbps.

***(c) Analysis using training data percentage***

The developed model with training data percentage analysis is shown in Figure 10. The analysis for the FNR metric is revealed in Figure 10(a). When training data percentage = 90, the FNR measured by WMC, Futuristic method, Trustable and secure routing method, Multitier HWN, HMM, JDICA, SFO, and the proposed model are 0.0904, 0.010, 0.126, 0.085, 0.088, 0.094, 0.109, and 0.083. Figure 10(b) portrays the performance analysis of FPR. When training data percentage = 90, the FPR value measured by WMC, Futuristic method, Trustable and secure routing method, Multitier HWN, HMM, JDICA, SFO, and the proposed model is 0.140, 0.175, 0.150, 0.136, 0.137, 0.153, 0.145, and 0.135, respectively.




a) b)

**Figure 10** Comparative analysis with different training data percentages (a) FNR, and (b) FPR.

## 5.8 Comparative Discussion

Table 2 shows the discussion of the comparative result for previous WMC, Futuristic method, Trustable and secure routing method, Multitier HWN, HMM, JDICA, SFO, and the proposed model considering the performance metrics for 50, and 100 nodes by varying the rounds. The minimal delay for the developed TaylorSFO-based Deep stacked autoencoder is 21.23 ms, whereas the delay values of WMC, Futuristic method, Trustable HMM, JDICA, SFO, and secure routing method, and Multitier HWN are 22.11 ms, 26.48 ms, 23.56 ms, 22.00 ms, 22.56 ms, 22.92 ms, and 21.92 ms considering 50 nodes. The maximal PDR was obtained by the developed model with a value of 94.87%, whereas the WMC, Futuristic method, Trustable and secure routing method, HMM, JDICA, SFO, and Multitier HWNacquired the PDR of 94.77%, 94.09%, 93.06%, 94.85, 94.83%, 94.53%, and 94.35%, based on 100 nodes. The maximal throughput for the developed TaylorSFO-based Deep stacked autoencoder is 119.98 kbps, whereas the WMC, Futuristic method, Trustable and secure routing method, HMM, JDICA, SFO, and Multitier HWNacquired the throughput of 119.14 kbps, 118.62 kbps, 117.53 kbps, 119.83 kbps, 119.639%, 119.38%, and 119.14%, respectively.

Table 3 shows the comparative discussion in terms of FNR, and FPR. The minimal FNR for the developed TaylorSFO-based Deep stacked autoencoder is 0.083, whereas the FNR of existing WMC, Futuristic method, Trustable and secure routing method, Multitier HWN HMM, JDICA, and SFO are 0.090, 0.100, 0.126, 0.085, 0.088, 0.094, 0.109, respectively. In addition, the minimal FPR achieved by the developed TaylorSFO-based Deep stacked autoencoder is 0.134, FPR of existing WMC, Futuristic method, Trustable

**Table 2** Comparative analysis based on nodes

| Number of Nodes | Metrics | WMC | Futuristic Method | Trustable and Secure Routing Method | Multitier HWN | HMM | JDICA | SFO | Proposed TaylorSFO-based Deep Stacked Autoencoder |
|---|---|---|---|---|---|---|---|---|---|
| **50** | **Delay (ms)** | 22.11 | 26.48 | 23.56 | 21.92 | 22.00 | 22.56 | 22.92 | **21.23** |
| | **Packet delivery rate (%)** | 91.17 | 90.59 | 91.10 | 91.38 | 91.27 | 91.13 | 91.41 | **91.57** |
| | **Throughput (kbps)** | 107.94 | 106.97 | 107.30 | 108.58 | 108.87 | 108.20 | 108.96 | **109.40** |
| **100** | **Delay (ms)** | 28 | 28.17 | 30.66 | 26.63 | 27.42 | 28.23 | 28.63 | **24.31** |
| | **Packet delivery rate (%)** | 94.77 | 94.09 | 93.06 | 94.85 | 94.83 | 94.53 | 94.35 | **94.87** |
| | **Throughput (kbps)** | 119.14 | 118.62 | 117.53 | 119.83 | 119.34 | 119.38 | 119.14 | **119.98** |

**Table 3** Comparative analysis based on training data percentage

| Metrics | WMC | Futuristic Method | Trustable and Secure Routing Method | Multitier HWN | HMM | JDICA | SFO | Proposed TaylorSFO-based Deep Stacked Autoencoder |
|---|---|---|---|---|---|---|---|---|
| ***FNR*** | 0.090 | 0.100 | 0.126 | 0.085 | 0.088 | 0.094 | 0.109 | **0.083** |
| ***FPR*** | 0.139 | 0.175 | 0.150 | 0.135 | 0.137 | 0.153 | 0.145 | **0.134** |

**Table 4** Computational time analysis

| Methods | Computational Time (sec.) |
|---|---|
| WMC | 12.00 |
| Futuristic method | 9.24 |
| Trustable and secure routing method | 6.91 |
| Multitier HWN | 7.97 |
| HMM | 9 |
| JDICA | 8.24 |
| SFO | 6.91 |
| Proposed TaylorSFO-based Deep stacked autoencoder | 5.02 |

and secure routing method, Multitier HWN HMM, JDICA, and SFO, are 0.139, 0.175, 0.150, 0.135, 0.137, 0.153 and 0.145 respectively.

### 5.9 Computational Time

The computational times defines the time taken for processing. Table 4 shown below provides the time taken for the proposed and the existing methods, in which the proposed method shows better result with minimum computational time. From Table 4, the proposed method shows minimum time of 5.02 sec and the existing methods like WMC, Futuristic method, Trustable and secure routing method, Multitier HWN HMM, JDICA, and SFO shows the time of about 12 sec, 9.24 sec, 6.91 sec, 7.97 sec, 9 sec, 8.24 sec, and 6.91 sec, respectively.

## 6 Conclusion

This paper introduced a new method for finding black hole attack using the proposed TaylorSFO-based Deep stacked autoencoder. This method is utilized to maximize network lifetime by facilitating energy-aware routing with secured communication. The fitness function considers the parameters,

such as delay, distance, and energy; thus the overall network performance is improved. Initially, the WSN is simulated, and then the routing is based on the developed TaylorSFO algorithm. The TaylorSFO is designed by incorporating the Taylor series with SFO. After routing, the blackhole attack detection is performed at the BS. Here, the data is pre-processed, and then, the features are extracted to detect the blackhole attack effectively. Based on the extracted features, the blackhole attack is detected by a Deep stacked autoencoder. The developed TaylorSFO-based Deep stacked autoencoder shows effective results with minimal delay of 21.23 ms, minimal FNRof 0.083, minimal FPR of 0.134, maximal PDR of 94.87%, the maximal throughput rate of 119.98 kbps, respectively. The proposed method has the advantages, such as higher accuracy, ease of deployment, continuous, non-separable, non-convexhas improved execution time, and scalable. The proposed black hole attack detection method can be used in applications like unmanned aerial vehicles, military applications, healthcare, and so on. In the future, blackhole attack detection will be improved by using some other optimization algorithms, such as the ant colony optimization algorithm, Firefly algorithm, or Cuckoo Search algorithm for attaining better performance.

## References

[1] J. Sebastan Terence and Geethanjali Purushothaman, "A novel technique to detect malicious packet dropping attacks in wireless sensor networks", Journal of Information Processing Systems, vol. 15, no. 1, 2019.

[2] Abdullah Aljumah, Tariq Ahamed Ahanger, "Futuristic Method to Detect and Prevent Blackhole Attack in Wireless Sensor Networks", IJCSNS International Journal of Computer Science and Network Security, vol. 17, no. 2, February 2017.

[3] Hanane Kalkha, Hassan Satori, and Khalid Satori, "Preventing Black Hole Attack in Wireless Sensor Network Using HMM", Procedia computer science, vol. 148, pp. 552–561, 2019.

[4] Deepak C. Mehetre, S. Emalda Roslin, and Sanjeev J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust", Cluster Computing, vol. 22, no. 1, pp. 1313–1328, 2019.

[5] A. John Clement Sunder, and A. Shanmugam, "Jensen–Shannon Divergence Based Independent Component Analysis to Detect and Prevent

Black Hole Attacks in Healthcare WSN", Wireless Personal Communications, vol. 107, no. 4, pp. 1607–1623, 2019.

[6] Anastasia Tsiota, Dionysis Xenakis, Nikos Passas, and Lazaros Merakos, "On Jamming and Black Hole Attacks in Heterogeneous Wireless Networks", IEEE Transactions on Vehicular Technology, vol. 68, no. 11, pp. 10761–10774, 2019.

[7] M. Rajesh Babu, S. Moses Dian, Siva Chelladurai, and Mathiyalagan Palaniappan, "Proactive Alleviation Procedure to Handle Black Hole Attack and Its Version", The Scientific World Journal, 2015.

[8] Bindu Rani, Harkesh Sehrawat, and Vikas Siwach, "Blackhole attack in wireless sensor network (WSN) using AODV protocol", International Journal of Advanced Science and Technology, vol. 29, no. 4, pp. 349–359, 2020.

[9] M Moshaddique Al Ameen & Jingwei Liu and Kyungsup Kwak, "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications," Journal of medical systems, vol. 36, no. 1, pp. 93–101, 2012.

[10] R. Beghdad and A. Lamraoui, "Boundary and holes recognition in wireless sensor networks," Journal of Innovation in Digital Ecosystems, vol. 3, no. 1, pp. 1–14, 2016.

[11] Vrinda Gupta, and Rajoo Pandey, "An improved energy aware distributed unequal clustering protocol for heterogeneous wireless sensor networks," An International Journal of Engineering Science and Technology, vol. 19, no. 2, pp. 1050–1058, 2016.

[12] Gurjot Singh and Jagdeep Singh, "Prevention of Blackhole Attack in Wireless Sensor Network using IPSec Protocol, "International Journal of Advanced Research in Computer Science, vol. 4, no. 11, December 2013.

[13] Abhijeet Salunke and Dayanand Ambawade, "Dynamic Sequence Number Thresholding Protocol for Detection of Blackhole attack in Wireless Sensor Network", In proceedings of 2015 International Conference on Communication, Information and Computing Technology (ICCICT), Mumbai, India, January 2015.

[14] Anu Bala, Munish Bansal, and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", In proceedings of First International Conference on Networks & Communications, 2009.

[15] Abhishek Pandey and R.C. Tripathi, "A Survey on Wireless Sensor Networks Security", International Journal of Computer Applications, vol. 3, pp. 43–49, June 2010.

[16] Jeremy Brown and Xiaojiang Du, "Detection of selective forwarding attacks in heterogeneous sensor networks", In proceedings of IEEE International Conference on Communications, pp. 1583–1587, 2008.
[17] Christoforos Panos, Chirstoforos Ntantogian, Stefanos Malliaros, Christos Xenakis, "Analyzing, Quantifying, and Detecting the Blackhole attack in Infrastructure-less Networks", Computer Networks, vol. 113, pp. 94–110, 2017.
[18] Mete Ozay, Iñaki Esnaola, Fatos Tunay Yarman Vural, Sanjeev R. Kulkarni, and H. Vincent Poor, "Machine Learning Methods for Attack Detection in the Smart Grid", IEEE transactions on neural networks and learning systems, vol. 27, no. 8, pp. 1773–1786, 2016.
[19] EsraSahin and IlkerHamzaoglu, "An Efficient Intra Prediction Hardware Architecture for H.264 Video Decoding", In proceedings of 10th Euromicro Conference on Digital System Design Architectures, Methods and Tools, IEEE, pp. 448–454, August 2007.
[20] S. Shadravan, H.R. Naji, and V.K. Bardsiri, "The Sailfish Optimizer: A novel nature-inspired metaheuristic algorithm for solving constrained engineering optimization problems", Engineering Applications of Artificial Intelligence, vol. 80, pp. 20–34, 2019.
[21] Guifang Liu, HuaiqianBao, and Baokun Han, "A Stacked Autoencoder-Based Deep Neural Network for Achieving Gearbox Fault Diagnosis", Mathematical Problems in Engineering, 2018.
[22] KDD Cup 1999 dataset taken from, "http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html", accessed on July 2020.
[23] Balachandra M., Prema K.V. and Makkithaya K., "Multiconstrained and multipath QoS aware routing protocol for MANETs", Wireless networks, vol. 20, no. 8, pp. 2395–2408, 2014.
[24] Yadav A.K. and Tripathi S, "QMRPRNS: Design of QoS multicast routing protocol using reliable node selection scheme for MANETs", Peer-to-Peer Networking and Applications, vol. 10, no. 4, pp. 897–909, 2017.
[25] Jayapriya, K. and Mary, N.A.B., "Employing a novel 2-gram subgroup intra pattern (2GSIP) with stacked auto encoder for membrane protein classification", Molecular biology reports, vol. 46, no. 2, pp. 2259–2272, 2019.
[26] Deepali Virmani, and Pranav Gupta, "Adaptive Exponential Trust-Based Algorithm in Wireless Sensor Network to Detect Black Hole and Gray Hole Attacks," Emerging Research in Computing, Information, Communication and Applications, pp. 65–73, 2016.

[27] Venkata Abhishek Kanthuru, and Kakelli Anil Kumar, "Black Hole Detection and Mitigation Using Active Trust in Wireless Sensor Networks," Advances in Distributed Computing and Machine Learning, vol. 127, pp. 25–34, 2020.

[28] Ila Kaushik, and Nikhil Sharma, "Black Hole Attack and Its Security Measure in Wireless Sensors Networks," Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's, vol. 1132, pp. 401–416, 2020.

[29] Dhananjay Bisen, Bhavana Barmaiya, Ritu Prasad, Praneet Saurabh, "Detection and Prevention of Black Hole Attack Using Trusted and Secure Routing in Wireless Sensor Network," Advances in Intelligent Systems and Computing, vol. 1179, 2020.

[30] Vahid Heydari, and Seong-Moo Yoo, "Timeout Period Analysis to Detect Black Hole Attack in Multihop Wireless Ad Hoc Networks," International Journal of Wireless Information Networks, vol. 25, pp. 15–29, 2018.

[31] Ashish Chaturvedi M. Senthil Kumar, "Energy-Efficient Coverage and Prolongs for Network Lifetime of WSN using MCP," European Journal of Scientific Research (EJSR), vol. 95, no. 2, 2013.

[32] M. Senthil Kumar, "Energy Efficient Techniques for Transmission of Data in Wireless Sensor Networks," Journal of Computing Technologies (JCT), vol. 5, no. 2, 2016.

[33] Avishek Choudhury, Onur Asan, "Role of artificial intelligence in patient safety outcomes: systematic literature review," JMIR medical informatics, vol. 8, no. 7, pp. e18599, 2020.

[34] Suresh Babu Chandanapalli,Sreenivasa Reddy E,Rajya Lakshmi D, "Convolutional Neural Network for Water Quality Prediction in WSN", Journal of Networking and Communication Systems, vol. 2, no. 3, pp. 40–47, 2019.

[35] Samar Abdulrahman Juma Al Raisi, "A Review on Congestion Management Methodologies and its Applications", Journal of Computational Mechanics, Power System and Control, vol. 3, no. 3, 2020.

[36] K.Srinivas, "Cluster Based Dense using Hybrid Genetic and Grasshopper Optimization algorithm in WSN", Journal of Networking and Communication Systems, vol. 4, no. 3, 2021.

## Biographies

**Mandeep Kumar** received B.Tech in CSE from Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India in 2003 and M.Tech in Computer Science and Engineering from Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India in 2013. Presently he is pursuing PhD from IKG PTU Kapurthala, Punjab. His research interest is in wireless sensor networks.

**Jahid Ali** has vast research, teaching and administrative experience in SSGI Badhani, since 2002. He has specialized in Speech Recognition Technology, Artificial Intelligence, Advanced Data Structures, Applied Mathematical and Programming languages. He has published about 15 papers in National Journals of repute and guiding 4 Ph.D students from IKG PTU. He has been awarded full travel grant for presenting a research paper in University of Taxas, USA by All India Council for Technical Education (AICTE).