ORIGINAL RESEARCH ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

Black Hole Attack Detection in Wireless Sensor Networks Using Hybrid Optimization Algorithm

Dlsoz Abdalkarim Rashid[1]*, Marwan B. Mohammed[2]

[1]Department of Computer Science, College of Science, University of Sulaimani, Sulaimani, Iraq, [2]Department of Computer Science, College of Science, University of Al-Nahran, Baghdad, Iraq.

ABSTRACT

One of the types of denial of service attacks that target wireless sensor networks (WSNs) are black hole (BH) attacks, which are widely targeted at this form of network today. In this attack, data are blocked in the network, malware is installed on a group of nodes in the network, and ultimately, the data packet is blocked before reaching its destination. In other words, data cannot be transmitted in the vicinity of BH nodes. Because of the nature of WSNs that are readily available, these networks cannot be optimized without compromising energy consumption, and this problem becomes a non-deterministic polynomial-time hard problem. Despite some models that have been presented to resolve this issue, most of them have not had sufficient performance in dealing with BH attacks. Thus, we have presented a new and powerful model based on the hybrid meta-heuristic algorithm depending on the sine and cosine algorithm (SCA) and the whale optimization algorithm (WOA). This algorithm has been combined in such a way that the increase in computational load has been prevented, in addition, two algorithms are included in one algorithm in this case, using the positive features of these two algorithms, it escapes from the local optimal trap in the solution of the algorithm and also benefits from a very good convergence. Because the new production solutions have a good diversity and the intensification component also has a good performance the main goal of this article is to present a new type of robust optimization algorithm for BH detection in WSN. This model has been tested and evaluated using a network and compared with three other meta-heuristic algorithms to make a fair comparison. The results obtained from the proposed model indicate a high-quality performance of this model in detecting BH attacks. The proposed model can detect more than 85% of the BH nodes and the total warning rate in the proposed model is equal to 0.866.

Index Terms: Whale Optimization Algorithm, Sine and Cosine Algorithm, Black Hole Attack, Wireless Sensor Networks, Meta-Heuristic

1. INTRODUCTION

Wireless sensor networks (WSNs) consist of a set of sensors, each of which has a transmitter, and this processor is also used to communicate, observe, and respond to events in the environment [1]. In other words, these types of networks usually have more than tens of thousands of sensors that are responsible for collecting information from nature and transmitting this information to the central device. WSN is a type of new technology that is widely used in various fields, including vehicles, health-care monitoring, accident detection, and emergency response at high speed [2]. Considering that these networks are very important, security is also of particular importance in these networks, and also, creating security in WSN can be a challenging operation. Regarding that WSN is physically interacting with the environment, network information can be at risk from security threats. In addition, the main goal of increasing security in WSN is to protect data and available resources against attacks and malicious behavior of hackers. Hence, in this case, reliable methods should be used to maximize security [3]. Not only

Access this article online

DOI:10.21928/uhdjst.v8n1y2024.pp142-150

E-ISSN: 2521-4217

P-ISSN: 2521-4209

Corresponding author's e-mail: Dlsoz Abdalkarim Rashid, Department of Computer Science, College of Science, University of Sulaimani, Sulaimani, Iraq. E_mail: dlsoz.rashid@univsul.edu.iq

Received: 12-12-2023 Accepted: 22-04-2024 Published: 09-05-2024

providing a reliable and efficient model to increase security in WSN is a vital thing, but also analyzing the security method against security threats is very necessary.

Overall, trust in WSN can be separated into two groups: System reliability and user trust. In the proposed model, it is tried to propose a routing for the network and the system will receive a warning against malicious nodes [4]. Moreover, due to the nature of WSN, secure routing in WSN can be very challenging because resources are limited in these networks. In addition, due to limitations in processing capacity, data storage, and battery in sensor nodes are weak against attacks because they are placed in open environments and are attacked physically or by software. Hence, reliability in data transmission and security in these networks are not guaranteed [5]. In this paper, we have used the combined algorithm based on the whale optimization algorithm (WOA) and the sine and cosine algorithm (SCA) to detect black holes (BHs). In this model, the information of the requested messages, which include the ID of the sender, and the ID of the base station, are recorded. Then, if the requested message is received in any node, the sending node is added to the list that contains the information of the senders. If the requested message is found, it will be referred to the information in the list, and if the sender's information was in the list of previous senders, the normal procedure will continue. However, if there is no information in the list, a value is added to the variable related to the suspiciousness of the node. Then, it begins the optimization phase using the proposed hybrid algorithm, in which the node is tracked and surrounded, and then, the node is attacked. Finally, this node is included in the list of exclusions and attackers [6].

The proposed optimization algorithm is utilized to reduce the computational overhead to increase the accuracy in detecting BH attacks in WSN. This article has tried to eliminate the weaknesses of other methods that have less accuracy or lack of detection of multiple attackers. For this reason, to increase the accuracy in detecting attacks, we have used input parameters with many details obtained from the attackers' behavior. This approach not only increases accuracy but multi-attacker attacks are also detected. The output is evaluated with a threshold and if the output is large, the node is considered a BH node. This method is such that the input parameters of all three input variables are created and then optimized using the proposed optimizer algorithm, which also optimizes the number of attacks.

Some of the innovations made in this article are explained below.

- Providing a new optimization algorithm based on WOA and SCA algorithms
- BH attack detection
- Evaluation using the provided hypothetical network
- Comparison with the use of other optimization algorithms
- Display results using different graphs.

This article is divided in such a way that in the next section, the previous works are discussed and reviewed; then, the basic concepts are explained and the proposed model is fully explained. In the next section, the proposed model and other methods will be tested and compared, and in the final section, future works and conclusions will be elaborated.

2. RELATED WORKS

WSNs are vital in today's world. These networks also have some weaknesses that can be considered a very good target for hackers. For this reason, many models have been proposed to strengthen security in WSNs, each of which has advantages and disadvantages. In the following, various types of security-enhancing systems in WSN will be discussed. WSNs are applied in many fields, including industrial, commercial, and health. Previous studies show that the proposed models to avoid BH attacks suffer from very few false positives [7]. In Tripathi *et al.* [8], one of the popular clustering protocols in WSN, which is LEACH, is explained and it is explained how the network can be compromised by BH and gray hole attacks. In BH attacks, the hacker tries to take control of several sensors and then reprograms these sensors to prevent sending data packets to the main base. In Wazid *et al.* [9], the influence of BH attacks on the network is evaluated and then a new model for detecting BH attacks in WSN is presented. Radio communications are very vulnerable to wide and various attacks, one of which is BH attacks. In Kaushik and Sharma [10], the attacks carried out in the network layer that are related to BH attacks have been evaluated, and the security measures that lead to the reduction of the destructive effects of such attacks have been discussed.

In Pawar and Anuradha [2], a new system that depends on a deep learning model is presented to prevent and detect BH attacks in WSNs. In this model, different phases are considered, which are equal to collecting data assigning nodes identifying BH attacks, and mitigating BH attacks. This model initially considers a series of nodes to establish communication in the WSN. In this system, attacks are explored using the Bait approach, and wormhole attacks are explored using round-trip validation operations. Data collection is also done using the round-trip time and Bait. Finally, the collected data are trained to utilize the long short-term memory (LSTM) deep learning model, the attack detection operation is performed, and the attacks are eliminated from the network by applying optimal and correct path detection. In Khare *et al.* [11] of this model, the shortest path is discovered using the WOA algorithm. To increase security in WSN, the BH optimization algorithm is presented to detect the attack node. Furthermore, this algorithm is implemented on a vertex participation function. An improved check agent method for detecting BH attacks is presented in Saputra Andika [12], which performs the discovery operation by sending a search agent to search for the malicious node. The implementation of this model is based on the WSN created using ZigBee technology. The topology of this model can have more than one routing table.

In Khan *et al.* [13], iterative route configuration based on reactive routing protocol and ant colony algorithm is used to avoid BH attacks in mobile networks. In Srinivas and Manivannan [14], a new method for finding and preventing BH attacks in WSN is presented, and this model has five different stages. In the first step of this method, cluster heads are selected, and then k-routing paths are created, and after that, security against BH attacks is created. The fourth stage is related to creating security for the selective sending attack, and finally, in the last stage, the most optimal possible path is discovered. In this model, a topology is created to discover cluster heads and then create an optimal path, which ultimately leads to the discovery and avoidance of BH attacks using the baiting process. A validation process based on sent and received packets has been used to detect selective sending attacks. Elliptic curve cryptography is used to maximize security. In this model, a combined algorithm based on the dragonfly algorithm and the Deer hunting optimization algorithm is used to discover the shortest possible path based on parameters such as trust and delay, packet loss ratio, and distance. In Pawar and Jagadeesan [15], a BH detection model based on a deep learning algorithm in WSN is presented. To discover useful features, the feature selection technique has been used using a self-adaptive-multi-verse optimization meta-heuristic algorithm. In the next step, the features discovered in the previous step are used to train and test the deep belief network (DBN) algorithm. Furthermore, to increase the detection rate, the optimizer algorithm is utilized to enhance the DBN to optimize the number of hidden neurons.

In Rani *et al.* [16], a deep learning algorithm and ant colony optimization algorithm are used to increase security in mobile *ad hoc* networks. In this model, to increase the efficiency, the best nodes are selected to transmit data packets, and the results have been shown to signify the good ability of this model. BH attacks in the demand, distance vector routing protocol have been evaluated in Pullagura and Dhulipalla [17], which are discovered and avoided using a threshold mechanism of the intrusion detection system. Furthermore, maximum objectives are calculated using linear regression. Adaptive Taylor Sail fish optimizer algorithm is used to detect and prevent Sybil and BH attacks, routing is done using this optimizer algorithm, and the optimization parameters are energy, delay, and distance.

In Webber *et al.* [18], a new algorithm based on proportional overlapping score-based Minkowski K-means clustering was introduced for BH detection in beam sensor networks, which was the main goal of BH detection in health-care applications and it has little computational complexity. In another article [19], Bayesian theory and deep recurrent neural networks have been used to discover malicious nodes and BH in WSN by calculating the path discovery time. After removing the attacker node, a new optimal path is created using the grasshopper optimization algorithm.

According to the discussion and investigation, the presented models often have weaknesses, the main weakness of which is the long execution time. Because deep learning algorithms are often used and these models require a lot of time to train. Furthermore, in some cases, the selected optimizer algorithms have weaknesses in the exploration and exploitation phases, which, if faced with this problem, can in turn cause a decrease in the accuracy rate. In some cases, the optimization algorithms do not have good capabilities in the components of diversity and intensification, which easily causes the solutions to fall into the trap of local optimization during the optimization operation and does not happen with fast convergence. For this reason, the production solutions can have little diversity, which leads to the fact that the entire problem space is not explored. On the other hand, in the low number of iterations, the algorithm cannot discover high-quality solutions, which causes the algorithm to run in a large number of iterations, which increases the execution time. Therefore, choosing optimization algorithms to solve different problems can be a challenging task because each optimization algorithm has a series of strengths and weaknesses. Furthermore, by combining the two algorithms, the positive features of the two algorithms can be integrated and a powerful algorithm with a high search capability can be achieved. The proposed algorithm has very good capabilities in the exploration and exploitation phases because each of the SSA and WOA algorithms has strong points that the WOA algorithm works better in the exploitation phase and SSA in the exploration phase. According to the combined method, the proposed algorithm has a better execution time than other optimization algorithms, and the production solutions have a very good variety, which has led to an increase in the accuracy rate of the proposed model.

In this paper, we have developed a new type of hybrid optimization algorithm with low execution time to detect and prevent BH.

3. PROPOSED METHODOLOGY

In this subsection, the basic concepts in the proposed model will be discussed and each of the mechanisms will be fully explained in the corresponding subsections.

3.1. BH Attack

BH attacks are carried out based on malicious nodes that repeatedly send information to neighboring nodes. This node receives sensitive and important data from neighboring nodes and refrains from sending it to other nodes. These nodes are called BH nodes and the areas close to these nodes are called BH regions. In Fig. 1 these attacks are shown.

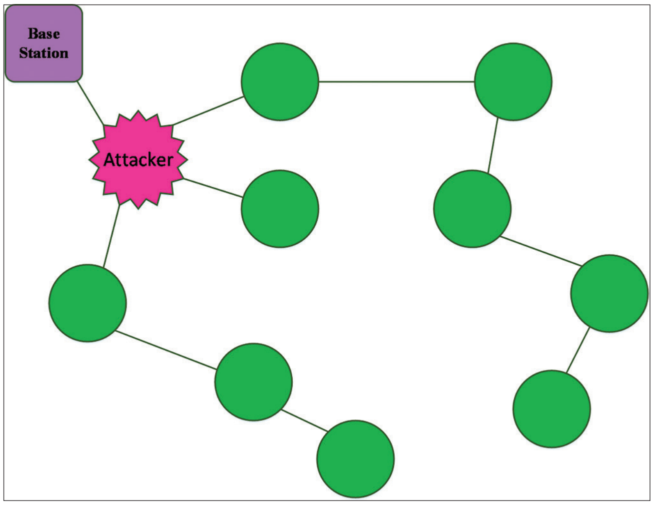

Fig. 1. Occurrence of black hole attack in wireless sensor networks.

In Fig. 1, the green areas are the sensor nodes and the red area is the BH region. If a node chooses a path to send data and there is a BH node in its path, if the data reaches the BH node, all the data received in this node will be lost and will not be transmitted. In this example, as can be seen, a large number of nodes are no longer able to send data outside the network. This type of attack takes place in the third layer of the network layer OSI model. Because these attacks take place in the network layer, all the activities in the network are disrupted, and functions such as delay, throughput, and packet loss take place in the network.

3.2. SCA

Meta-heuristic algorithms have shown very good performance in solving optimization problems and are a perfect option for solving problems in different optimization spaces. The SCA [20] is one of the powerful optimization algorithms that use cosine and sine functions to solve optimization problems. This algorithm has performed very well due to its approach to solving highly complex problems because it has a good capability in the diversity component. This algorithm mainly uses Eq. (1) to solve problems.

$$x_i(t+1) = \begin{cases} x_i(t) + r_1 \times \sin(r_2) \times |r_3 P_i(t) - x_i(t)|, & r_4 < 0.5 \\ x_i(t) + r_1 \times \cos(r_2) \times |r_3 P_i(t) - x_i(t)|, & r_4 \geq 0.5 \end{cases} \tag{1}$$

In Eq. (1), *sin* and *cos* represent the sine and cosine functions, and represents the location vector of the superior solution in the entire population, whereas represents the current solution. Furthermore, *r* depicts the random number generated between 1 and 0. This algorithm uses Eq. (2) to change the exploration and exploitation phases and create balance.

$$r_1 = a - t\frac{a}{T} \tag{2}$$

In Eq. (2), a is a variable that must be set with a constant value before starting the optimization procedure, and *t* signifies the current iteration number and T indicates the value of all iterations for optimization reasons.

3.3. WOA

Meta-heuristic algorithms are modeled and then implemented based on the behavior of animals or natural events, which in the WOA [21] is inspired by group life and how these creatures hunt in nature and are implemented using mathematical equations. This algorithm generally uses two mechanisms to perform optimization operations. The first case is the web bubble attack and the second case is hunting. This algorithm uses Eq. (4) to perform the first phase of its optimization.

$$\vec{D} = \left|\vec{C}.\overrightarrow{X_p}(t) - \vec{X}(t)\right| \tag{3}$$

$$\vec{X}(t+1) = \overrightarrow{X_p}(t) - \vec{A}.\vec{D} \tag{4}$$

In Eqs. (3 and 4), X represents the current solution and X_p represents the vector of the best solution, whereas C and A are both coefficient vectors that are calculated using Eqs. (5 and 6).

$$\vec{A} = 2\vec{a}.\overrightarrow{r_1} - \vec{a} \tag{5}$$

$$\vec{C} = 2.\overrightarrow{r_2} \tag{6}$$

Where a is a coefficient vector that decreases linearly from the value of 2 to 0.

In the WOA, the spiral mathematical equation of the logarithm is used to perform the optimization operation, and this mathematical equation is shown in Eq. (7).

$$\vec{X}(t+1) = \overrightarrow{D'}.e^{bl}.\cos(2\pi l) + \overrightarrow{X_p}(t) \tag{7}$$

In Eq. (7), D' refers to the distance between search agents and hunting, and b is a variable with a constant value, which must be set before starting the optimization procedure. In Eq. (8), two mechanisms used in the exploitation phase are shown, the first of which is related to the contraction mechanism.

$$\vec{X}(t+1) = \begin{cases} \overrightarrow{X_p}(t) - \vec{A}.\vec{D} \\ \overrightarrow{D'}.e^{bl}.\cos(2\pi l) + \overrightarrow{X_p}(t) \end{cases} \tag{8}$$

In Eq. (8), P refers to the random number generated between 0 and 1.

In the natural world, whales often search for food randomly in the natural environment. The same thing has been modeled in the WOA, and if the value of vector A is >1, the optimization algorithm enters the discovery phase, and the mathematical equation that models this behavior is shown in Eq. (9).

$$\vec{D} = \left|\vec{C}.\overrightarrow{X_{rand}} - \vec{X}\right|$$

$$\vec{X}(t+1) = \overrightarrow{X_{rand}} - \vec{A}.\vec{D} \tag{9}$$

In Eq. (9), X_{rand} refers to a search factor among the whole population which is randomly selected.

3.4. Proposed Model

Each optimization algorithm has a series of strengths and weaknesses, which can show very different and diverse effects when faced with different problems. The main reason for this behavior can be the search algorithm of these algorithms in solving different problems. Because, each of these algorithms can be superior in one of the phases of exploitation or exploration, and in solving problems that one of these two cases can achieve good results, the efficiency of the algorithm is also better in the same problem. However, the problem of avoiding the BH requires good performance in both phases of exploitation exploration, and we have combined two SCAs and a WOA to solve this case. Because the SCA has a relative superiority in the exploration phase and the WOA has a better performance in the exploitation phase. Furthermore, the approach used to combine these two algorithms in this paper is to avoid increasing the computational complexity half of the population enters the SCA in each iteration, and the other half of the population enters the whale optimizer algorithm to perform optimization operations. In such a situation, the computational complexity is not increased and the optimization capabilities are maintained in both algorithms. Fig. 2 illustrates the general outline of the proposed optimizer algorithm.

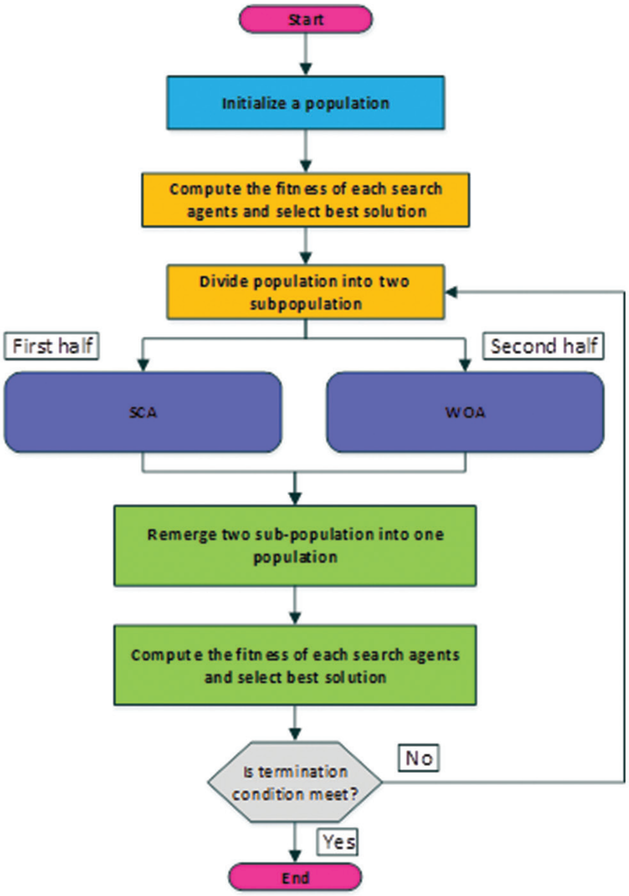
Start
Initialize a population
Compute the fitness of each search agents and select best solution
Divide population into two subpopulation
First half
Second half
SCA
WOA
Remerge two sub-population into one population
Compute the fitness of each search agents and select best solution
Is termination condition meet?
No
Yes
End

Fig. 2. Overall overview of the proposed model.

Different steps in the proposed model to discover the BH or avoid the BH, there are different steps, and each step has different processes, which are fully explained below. The proposed model goes through the following steps:

- Several nodes are randomly distributed in a square-shaped environment with adjustable dimensions
- Some of the nodes are considered BH randomly. These nodes do not send messages and by creating a hypothetical neighbor and inserting the ID of this hypothetical node in the list, they cause deception in the nodes that send the message. Because of this, the return time of the packets is very fast regardless of the specified path and can be used as a tip
- Normal nodes in the network have normal routing behavior and the return time of packets is also standard. If the packet return time from these nodes is less than the threshold, these nodes can be considered BH
- A central station undertakes the task of detecting BH using the proposed optimizer algorithm
- AODV algorithm is used for routing
- Identification stage, after detecting the suspicious nodes based on the response time, a command is issued through the central station to attack the neighboring nodes, which is the best solution of the central station in the proposed model. If the central node is adjacent to the suspicious node, the central station itself also participates in the attack process. The nodes that have the most warning and reception compared to the node in question are considered the three best nodes
- The top three nodes can change based on criteria at any moment. After being selected, these nodes start sending routing packets to discover BH nodes in a small range. In this phase, BH nodes that have not yet been definitively discovered may be present in the attack and disrupt the discovery of suspicious nodes of their colleagues
- If the number of warnings received in each enclosing node exceeds the first threshold value, it starts sharing this node with its neighbors. If the number of warnings received for the BH node exceeds the third threshold, this node will be saved as a BH node in its list. Furthermore, if the number of warnings of the first three solutions is greater than or equal to the third threshold, the suspicious node is considered a BH node. In addition, in the first three solutions, although the masked nodes warn their neighbors, the first node determines whether a node is a BH and transmits it to the hub. Then, after the definite discovery of a BH node, the station node warns this node to the neighbor so that the neighboring nodes are aware of the said node being a BH
- Neighboring nodes continue to communicate with all their neighboring nodes until the third threshold is reached, even if these nodes are suspicious nodes or BH nodes. However, when the warning level reaches the set value, these nodes are ignored
- In addition to the routing table, each node has another table called blacklist, in which the specifications of suspicious nodes are entered
- In each repetition of the simulation operation, the position of the nodes is updated, and the suspicious nodes are closely related to the number, type, and position of their neighboring nodes.

4. RESULTS AND DISCUSSION

In this section, the suggested model is tested and evaluated and the outcome gained from this evaluation will be depicted in tables and graphs. Furthermore, for a fair test, the results gained from the suggested model have been compared with gray wolf optimization [22], giant trevally optimizer [23], and particle swarm optimization (PSO) [24] algorithms. In addition, to perform this experiment, a computer with RAM 8 specifications and a Cori3-4005U CPU was used, and the implementation was done in MATLAB version 2016b. In this paper, we have used the face-centered central composite design [25] method to find the best parameter value. The best parameter value obtained from this experiment is shown in Table 1. The scenario used to test the proposed model is in the form of a virtual network, in which network nodes are randomly distributed in the network space every time it is executed. The network settings used for the experiment are shown in Table 1.

Regarding Table 2, this table shows the ratio of true and false alarms obtained from this test by the proposed model and other algorithms compared.

Focusing on the results demonstrated in Table 2, the proposed model has been able to show the best performance and is superior to other algorithms. The second-best performance is related to the PSO algorithm, which also has an acceptable rate. In the following, the proposed model has been carefully evaluated for a more accurate evaluation using different charts, which is shown in Fig. 3.

Fig. 2 shows the graphs of the cost and cumulative cost function. Considering that it is very difficult to discover BH nodes in the early stages, after each iteration, the values have decreased dramatically. In other words, in the initial stages, the values were equal to 0.25, in the later stages of optimization, this value reached below 0.05. According to the cumulative cost diagram, the value of the cumulative function was more than 12 in the first stage. It has been minimized to zero in the next stages, which shows the convergence process of the cost function.

TABLE 1: Parameter setting

Parameter name	Value
Network size	120×120
The total number of nodes	100/150
The number of black hole nodes	8/11
routing algorithm	AODV
Early warning level	2
Secondary warning level	6
Dimensions of the problem	3
Search range	(0 and 1)
The number of repetitions	50
Number of searchers	Variable and at least 3
Astana return time	25% of the shortest time interval

TABLE 2: Total warn with rate

Proposed Model	Gray wolf optimization	Particle swarm optimization	Giant trevally optimizer
0.8658	0.7458	0.8241	0.8068

Fig. 4 shows the graphs of the number of participating nodes and BH nodes in BH discovery. By referring to the diagram of the number of BH nodes, it is clear that the proposed model has been able to discover more BH nodes during the optimization operation, which indicates the good efficiency of the suggested model. According to the graph of the number of nodes that participated in BH detection, this graph is the percentage of nodes that participated in BH detection. Participated in the discovery of a BH at least once, it can be seen that most of the nodes participated during the optimization operation to discover the BH, which was almost more than 85%.

Fig. 5 shows the graphs of the total alerts received and the amount of correct and incorrect alerts. By carefully looking at the first diagram, it can be concluded that the number of warnings during the operation declined because the number

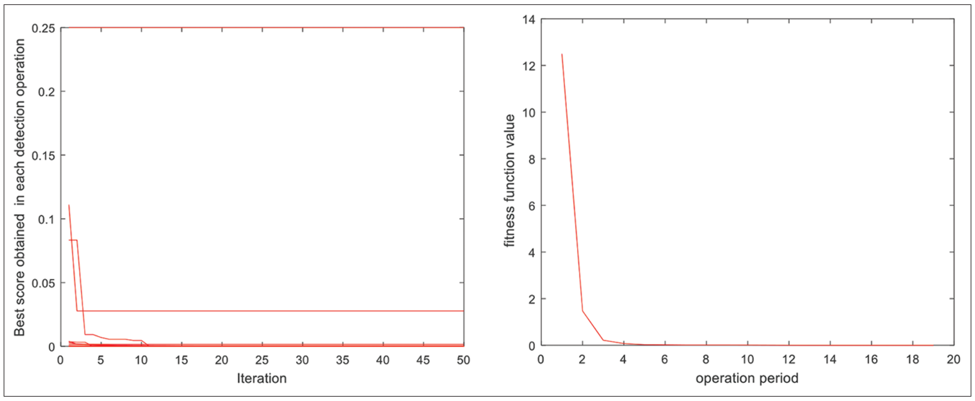

Fig. 3. Diagrams of the cost function set and the cumulative cost function.

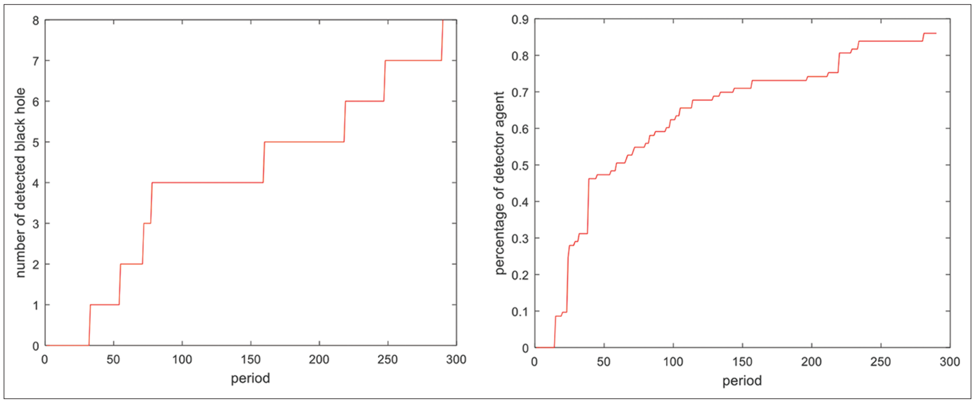

Fig. 4. Graphs of the number of detected black holes and the percentage of normal nodes detecting black holes.

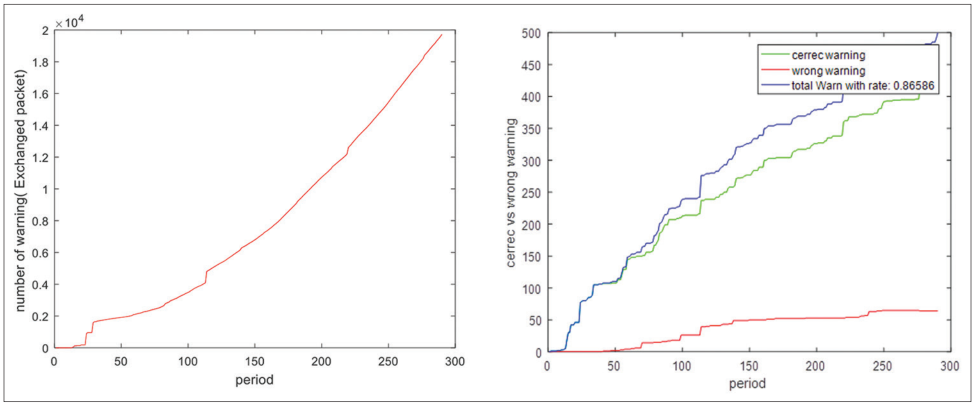

Fig. 5. Cumulative graphs of the received alarm of the whole network and the rate of false alarm and correct alarm.

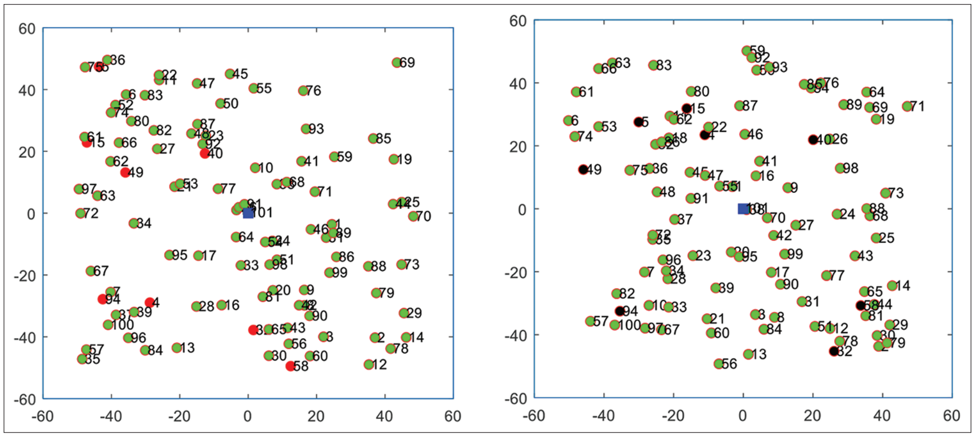

Fig. 6. Network environment before and after starting the simulation.

of BH nodes was discovered during the optimal procedure. Other normal nodes do not send information to these nodes. In the second graph, which is related to the amount of correct and false alarms, the ratio of correct alarms to false alarms is equal to 0.8658, the percentage of correct detection is equal to 100%, and the alarm ratio according to the error correction approach is equal to 0%.

Fig. 6 shows the simulation areas before and after the optimization operation. In this Fig., the suspicious nodes are shown with red circles, which change color to black if detected after the optimization operation. By looking carefully at this diagram, it is clear that the proposed model has almost been able to correctly discover all the nodes of the BH.

5. CONCLUSION AND FUTURE WORK

Minimizing energy and consumption and creating safety in WSN during the lifetime of the network is a vital issue because otherwise, the network can easily be out of reach. In this article, a novel linked optimization algorithm depends on the WOA, and SCA is used for computing and also increasing the accuracy in finding BH attacks in WSN. In addition, it has been tried to eliminate the weaknesses in other algorithms, which include low accuracy and failure to detect multiple attackers. For this reason, in this model, an attempt has been made to use more detailed input data, which leads to increased accuracy and detection of multiple attacks. The output results are compared with a threshold value, and if this value is higher, the node in question is considered a BH node. Then, three input parameters in this model are given to the proposed optimizer algorithm to perform the optimization procedure. In this paper, a new type of optimization algorithm is presented to discover BH nodes in WSN. The above algorithm has a very good ability to explore the problem space due to its hybrid nature based on WOA and SCA algorithms. The above algorithm has shown that it has a very good performance in the exploitation and exploration phases.

The results of the experiment demonstrate that the suggested model has a perfect capability of detecting BH in WSNs.

In the future, the suggested algorithm can be applied to resolve various issues, or this model can be utilized to explore various attacks in WSN. Furthermore, in the future, a multi-objective algorithm depending on the proposed optimizer algorithm can be presented to solve multi-objective problems.

REFERENCES

[1] S. Ali, M. A. Khan, J. Ahmad, A. W. Malik and A. U. Rehman. "*Detection and Prevention of Black Hole Attacks in IOT and WSN*. In: *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*". IEEE, United States, 2018.

[2] M. V. Pawar and J. Anuradha. "Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM". *International Journal of Pervasive Computing and Communications*, vol. 19, no. 1, pp. 124-153, 2023.

[3] M. Shinde and D. Mehetre. "*Black Hole and Selective Forwarding Attack Detection and Prevention in WSN. In: 2017 International Conference on Computing, Communication, Control and Automation* (*ICCUBEA*)". IEEE, United States, 2017.

[4] D. C. Mehetre, S. E. Roslin and S. J. Wagh. "Detection and prevention of black hole and selective forwarding attack in clustered WSN with active trust". *Cluster Computing*, vol. 22, pp. 1313-1328, 2019.

[5] J. Kolangiappan. "A novel framework for the prevention of black-hole in wireless sensors using hybrid convolution network". *Scientific and Technical Journal of Information Technologies Mechanics and Optics*, vol. 22, no, 2, pp. 317-323, 2022.

[6] M. H. Shirvani and A. Akbarifar. "Anomaly-based detection of blackhole attacks in WSN and MANET utilizing quantum-metaheuristic algorithms". *Journal of Communication Engineering*, vol. 9, no. 1, pp. 77-92, 2020.

[7] B. K. Mishra, M. C. Nikam and P. Lakkadwala. "*Security Against Black Hole Attack in Wireless Sensor Network-a Review. In: 2014 Fourth International Conference on Communication Systems and Network Technologies*". IEEE, United States, 2014.

[8] M. Tripathi, M. S. Gaur and V. Laxmi. "Comparing the impact of black hole and gray hole attack on LEACH in WSN". *Procedia Computer Science*, vol. 19, pp. 1101-1107, 2013.

[9] M. Wazid, A. Katal, R. S. Sachan, R. H. Goudar and D. P. Singh. "*Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network. In*: *2013 International Conference on Communication and Signal Processing*". IEEE, United States, 2013.

[10] I. Kaushik and N. Sharma. "*Black hole attack and its security measure in wireless sensors networks. In*: *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*". Springer, Germany, pp. 401-416, 2020.

[11] A. Khare, R. Gupta and P. K. Shukla. *Improving the Protection of Wireless Sensor Network Using a Black Hole Optimization Algorithm (BHOA) on Best Feasible Node Capture Attack. In*: *IoT and Analytics for Sensor Networks: Proceedings of ICWSNUCA 2021*". Springer, New York City, 2022

[12] R. Saputra, J. Andika and M. "*Alaydrus. Detection of Blackhole Attack in Wireless Sensor Network Using Enhanced Check Agent. In*: *2020 Fifth International Conference on Informatics and Computing (ICIC)*". IEEE, United States, 2020.

[13] D. M. Khan, T. Aslam, N. Akhtar, S. Qadri, N. A. Khan, I. M. Rabbani and M. Aslam. "Black hole attack prevention in mobile ad-hoc network (manet) using ant colony optimization technique"*. Information Technology and Control*, vol. 49, no, 3, pp. 308-319, 2020.

[14] T. A. S. Srinivas and S. S. Manivannan. "Black hole and selective forwarding attack detection and prevention in IoT in health care sector: Hybrid meta-heuristic-based shortest path routing". *Journal of Ambient Intelligence and Smart Environments*, vol. 13, no. 2, pp. 133-156, 2021.

[15] M. V. Pawar and A. Jagadeesan. "Detection of blackhole and wormhole attacks in WSN enabled by optimal feature selection using self-adaptive multi-verse optimiser with deep learning". *International Journal of Communication Networks and Distributed Systems*, vol. 26, no. 4, pp. 409-445, 2021.

[16] P. Rani, S. Verma and G. N. Nguyen. "Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network". *IEEE Access*, vol. 8, pp. 121755-121764, 2020.

[17] J. R. Pullagura and V. R. Dhulipalla. "Black□hole attack and counter measure in ad hoc networks using traditional routing optimization". *Concurrency and Computation: Practice and Experience*, vol. 35, no. 9, p. e7643, 2023.

[18] J. L. Webber, A. Arafa, A. Mehbodniya, S. Karupusamy, B. Shah, A. K. Dahiya and B. Kanani. "An efficient intrusion detection framework for mitigating blackhole and sinkhole attacks in healthcare wireless sensor networks". *Computers and Electrical Engineering*, vol. 111, p. 108964, 2023.

[19] K. Cheena, T. Amgoth and G. Shankar. "*Deep Learning-Based Black Hole Detection Model for WSN in Smart Grid. In: Computational Intelligence: Select Proceedings of InCITe 2022*". Springer, Germany, pp. 19-30, 2023.

[20] S. Mirjalili. "SCA: A sine cosine algorithm for solving optimization problems". *Knowledge-Based Systems*, vol. 96, pp. 120-133, 2016.

[21] S. Mirjalili and A. Lewis. "The whale optimization algorithm". *Advances in Engineering Software*, vol. 95, pp. 51-67, 2016.

[22] S. Mirjalili, S. M. Mirjalili and A. Lewis. "Grey wolf optimizer". *Advances in Engineering Software*, vol. 69, pp. 46-61, 2014.

[23] B. Abdollahzadeh, F. S. Gharehchopogh and S. Mirjalili. "Artificial gorilla troops optimizer: A new nature□inspired metaheuristic algorithm for global optimization problems". *International Journal of Intelligent Systems*, vol. 36, no. 10, pp. 5887-5958, 2021.

[24] J. Kennedy and R. Eberhart. "*Particle Swarm Optimization. In: Proceedings of ICNN'95-International Conference on Neural Networks*". IEEE, United States, 1995.

[25] M. Balachandran, S. Devanathan, R. Muraleekrishnan and S. S. Bhagawan. "Optimizing properties of nanoclay-nitrile rubber (NBR) composites using face centered central composite design". *Materials and Design*, vol. 35, pp. 854-862, 2012.