IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

ID-WNFS: Intrusion Detection Using Whale Neuro-Fuzzy System In Wireless Sensor Network

Rakesh Sharma[1*], Vijay Anant Athavale[2]

[1]Department of Computer Science &Engg., I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India
[2]Department of Computer Science & Engg., Gulzar Group of Institutes, Khanna, Punjab, India

[*]Corresponding Author: rakeshsharma3112@gmail.com

Available online at: www.ijcseonline.org

Accepted: 12/Nov/2018, Published: 30/Nov/2018

Abstract**—**Intrusion detection in wireless sensor network (WSN) is a challenging research area, as the WSN has vast area, and lot of nodes. The wireless communication among the nodes, and the battery life of the nodes, makes the researchers difficult to establish a proper communication through the routing mechanism. This research develops the intrusion detection model by using the Neuro fuzzy model. The proposed Intrusion detection using Whale Neuro-Fuzzy System (WNFS) (ID-WNFS) is developed here for detecting the intruders present in the WSN environment. The proposed ID-WNFS has two components, sniffer for creating the log file, and detector for anomaly detection. The sniffer creates the log file by examining the transmission information and extracts the necessary features. The extracted features are sent to the detector, which has the WNFS for the anomaly detection. The proposed WNFS is created by including the properties of the whale optimization algorithm (WOA) with the Neuro fuzzy architecture. The optimization algorithm selects the appropriate fuzzy rules for the detection. The proposed ID-WNFS notifies the simulation protocol about the anomaly behaviour, and thus the routing path is built for the WSN. The entire simulation of ID-WNFS is done by introducing various attacks on nodes and the result reveal that, the ID-WNFS has achieved with the network lifetime as 43.989, energy as 7.106808 and the detection accuracy as 0.787191.

Keywords**—**Intrusion detection, wireless sensor network (WSN), routing, Neuro-Fuzzy System, whale optimization algorithm

I. Introduction

Due to the rapid development in the digital technology, it is made possible to interconnect large number of sensor devices through the wireless platform and name it as wireless sensor network (WSN). WSN due to vast structure and simplicity has found its significance in large number of services [1]. The wide applicability of the WSN has given rise to the security concerns as the data communicated over the network are high valued and critical [2]. Some of the common applications adopting the WSN network for the communication are disaster management, environment monitoring, military surveillance, habitat monitoring, health care, vehicle traffic monitoring etc [3]. Further the communication based services, they aid in the monitoring and the tracking operations, as they have small, low cost, resource-constrained devices, commonly referred as sensors. The open platform of the WSN may invite the malicious attacks, and thus the intruders may hack the information [4]. The attacks in the WSN fall under two categories 1) active and 2) passive attack. While deploying the WSN as the hostile environment like as target tracking, battlefield surveillance, using the intrusion detection mechanism is necessary. The need for protecting the sensor readings is more important for the stability of WSN [4].

The WSN becomes more vulnerable to the hackers based on the following two reasons. The prime reason is the presence of the basic processing capabilities having the limited energy. Secondly, the WSN are not interconnected with the outside environment providing the additional security, and also it lacks in inbuilt security services [6]. While the WSN is under the attack, it affects the reliability, integrity and availability of the sensor information, and further reduces the life time of the network [7]. Intrusion in the WSN can be referred to the external activity of stealing the information. In the passive type of intrusion, attacks such as information gathering, eavesdropping are common, and in the active type more vigorous attacks such as harmful packet forwarding, packet dropping, hole attacks are done. Thus, to avoid these attacks, it is necessary to build the Intrusion Detection System (IDS)[8]. IDS inform the network members about the intrusion information [9]. IDS also can be considered as the monitoring framework in the WSN that detects the intruder. The intrusion detection application concerns how fast the intruder can be detected by the WSN [10].

An Intrusion Detection System (IDS), which has been successfully implemented in wired networks, can detect the misbehaviour of participating nodes and notify other nodes in the network to take appropriate countermeasures [11]. Therefore, two factors are needed to ensure effective Intrusion Detection System (IDS). Firstly, the IDS should be able to deliver reliable detection outcomes. The detection methods have to be effective in identifying intrusions since poor detection performance will ruin the trustworthiness of the IDS. Secondly, the IDS should survive in hostile environments. However, maintenance of high detection accuracy is challenging [12]. Generally, the IDSs can be briefly classified into two categories: signature-based detection schemes and anomaly-based detection schemes. Both of the two categories focus on identifying behaviours of malicious nodes. They consume a large amount of energy to monitor suspicious nodes [13]. In WSNs, the use of regular IDSs [14] may be compromised by frequent detection flaws and false alarms. Improving IDS effectiveness can be achieved through by using Trust management protocol [5], Computational Intelligence methods [15], clustering mechanism [16], probabilistic model [17], etc.

The primary intention of this research is to design and develop an intrusion detection system in wireless sensor network. Here, Whale Neuro-Fuzzy System (WNFS) will be newly developed for detecting intrusion in wireless sensor networks. Accordingly, neuro fuzzy system will be modified by integrating with whale optimization [18] for optimally generating fuzzy structure. The newly developed Whale Neuro-Fuzzy System (WNFS) will be then applied for intrusion detection in wireless sensor network. Overall, two major components will be included in the proposed intrusion detection system. In first component (sniffer), every packet will be examined and the required information will be stored as log file. In second component (detector), the WNF detector module detects the anomaly behaviour using the trained Whale Neuro-Fuzzy System. To evaluate the performance of the proposed system, the Low Energy Adaptive Clustering Hierarchy (LEACH) will be simulated for routing and the proposed system will be included within the network. The proposed WNFS will be compared against other existing soft computing methods, such as fuzzy logic controller (FLC), artificial immune system (AIS), Fuzzy artificial immune system (FAIS) [19] and neural network, in terms of detection accuracy, counter-defense, network life time and energy consumption, to demonstrate its efficiency and viability. The implementation will be done using MATLAB.

The major contribution of this research is the development of the ID-WNFS for detecting the nodes affected by the intruder in WSN. Here, the ID-WNFS detects the intruder node, and pass the information to the routing protocol and hence avoids the interruption during the communication.

The rest of the paper is organized as follows, Section I contains the introduction of intrusion detection system in wireless sensor network, Section II gives a description to eight works related to the intrusion detection and some of the challenges prevailing in this research are also discussed. Section III describes the wireless sensor network model. Section IV briefly describes about the proposed ID-WNFS for the intrusion detection and the results of the same are discussed in section V. Section VI concludes the paper.

II. Related Work

Some of the works related to the intrusion detection are discussed below:

Noureddine Assad et al. [1] proposed the Probabilistic based model for detecting the intrusions present in the WSN nodes. Using the probabilistic technique helped in improving the sensing range of the WSN, buts the robustness of the connectivity gets affected. The transmission range after the detection was very small, and hence need to be overcome.

Michael Riecker et al. [20] developed the Energy-efficient based intrusion detection system. The mobile agents were deployed in the system for detecting the intruders and the energy measurement was done through the linear regression model. The false positive rates of the model was low, meanwhile it incurs unreliable and bursty links.

Hussein Moosavi and Francis Minhthang Bui [2] have presented the Game-theoretic framework for dealing with the data uncertainty issues prevailed in intrusion detection. Further, it accounts with the various security parameters for addressing the proposed model. The model achieved design stability and thus provides improved security. But, the schemes increase the count of compromised nodes.

Mohammad Wazid and Ashok Kumar Das [5] developed the intrusion detection by employing the K-means clustering framework. They developed the multiple anomaly detection models and hence the model was named hybrid anomaly detector. The scheme completely avoided the detection mismatch, but increases the incoming traffic.

Helio Mendes Salmon et al. [14] proposed the artificial immune inspired system for intrusion detection. The AIS adopted the danger theory inspired immune system for the detection purpose. The model achieved low false positive and thus has improved efficiency. The delay occurring during the detection is very high.

Shahaboddin Shamshirband et al. [19] improved the AIS logic by adopting the fuzzy theory and newly proposed the Fuzzy artificial immune system (FAIS). They used the fuzzy activation threshold for detecting the sensor behavior and thus have improved detection accuracy. The scheme may fail in the real time scenario as the network volume is very high.

Sutharshan Rajasegarar et al. [16] proposed the Distributed anomaly detection model based on the hyper-spectral cluster based logic. The model reduced the communication overhead and achieved high robustness during the fault detection.

Anil Kumar Sagar and D. K. Lobiyal [3] proposed the Probability based on network parameters model for the intrusion detection. This scheme adopted network parameters like as sensing radius and node density for the detection and has attained better performance. But, the model fails to detect the intruder when the distance amidst the node and the intruder is beyond the sensing range.

Intrusion detection faces wrath due to the properties of the WSN, and some of the major challenges are listed below:

- The core weakness of wireless sensor node [19] lies in the limited resource devices, i.e. power and processing units. For this reason, vulnerability to various security threats is notably high. The main security threat [5] is that the attackers or intruders are included in the WSN since each sensor node has limited battery power, memory size, data processing capability and short radio transmission range. This leads to degrade the performance and security level.
- Also, the sensors in a network are deployed in unattended environment or even hostile circumstance, and communicate with each other using wireless signal which can be eavesdropped very easily [21]. For example, bogus routing and sensed data attack, select forward attack, sink hole attack, worm hole attack, black hole attack and hello flood attack, etc.
- Another important challenge [22] in WSNs is the detection of intruders, i.e., an unusual measurement that are inconsistent with the distribution of the majority of observations. The intrusion detection has several important roles in the wireless sensor network. Hence, it is important to detect and filter those erroneous measurements, to ensure the integrity of the collected data.
- In [19], fuzzy artificial immune system was developed to identify the network intruders. In this C-AFAIS, the decision making capabilities face major challenges due to the poorly trained architecture and the missing of evolutionary optimization process.

III. SYSTEM MODEL FOR THE WSN

The WSN is the collection of various number of sensor nodes interconnected by the wireless mode. The WSN architecture with the intrusion detection module is provided in figure 1. The WSN has the base station, which controls most of the operations of the WSN communication. The IDS monitor continuously monitors the presence of the intruder node in the WSN and notifies the simulation protocol. The simulation protocol establishes the routing path amidst the source and destination nodes. The source and the destination nodes are interconnected with the various intermediate nodes. The intruder commonly affects the intermediate node and hence the activities of the nodes are monitored continuously. The nodes in the WSN are mobile and hence distributed in large network. Here, we have considered a WSN network with the B nodes. The source and the destination node are represented as B^S and B^D respectively. At the beginning of the network transmission, the energy of each node remains to be high, and the after certain time, the network energy is reduced. The IDS monitor tracks the transmission path, and tries to prevent the loss of communication. The base station controls the communication flow, and regulates the error free communication.

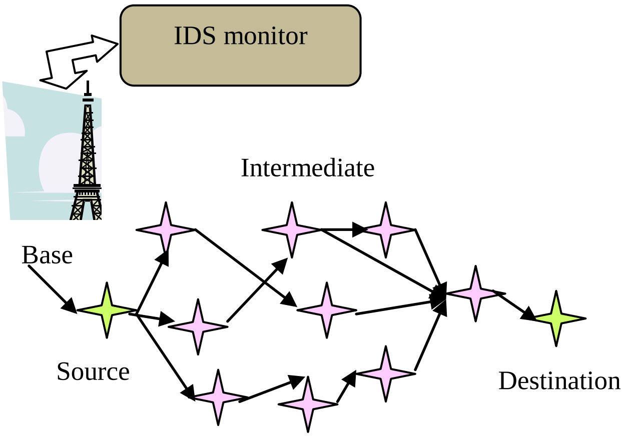


Figure 1. Architecture of the WSN model

IV. INTRUSION DETECTION MODEL BASED ON THE WHALE NEURO-FUZZY SYSTEM

Here, the intrusion detection system is built for the WSN communication, and the architecture of the proposed ID-WNFS is given in figure 2. As shown in the above figure, the proposed ID-WNFS model finds the intruder node in the WSN. The WSN source and the destination are interconnected by series of router nodes, which are affected by the intruders. For detecting the intrusion, the proposed ID-WNFS system uses the sniffer and the detector. The task of the sniffer component is to create the log information by observing the transmission and reception of bytes of information carried out in each node. The sniffer extracts 15 features from the packet information and creates the necessary log file. The log file is provided as the source for the intrusion detection to the detector component.

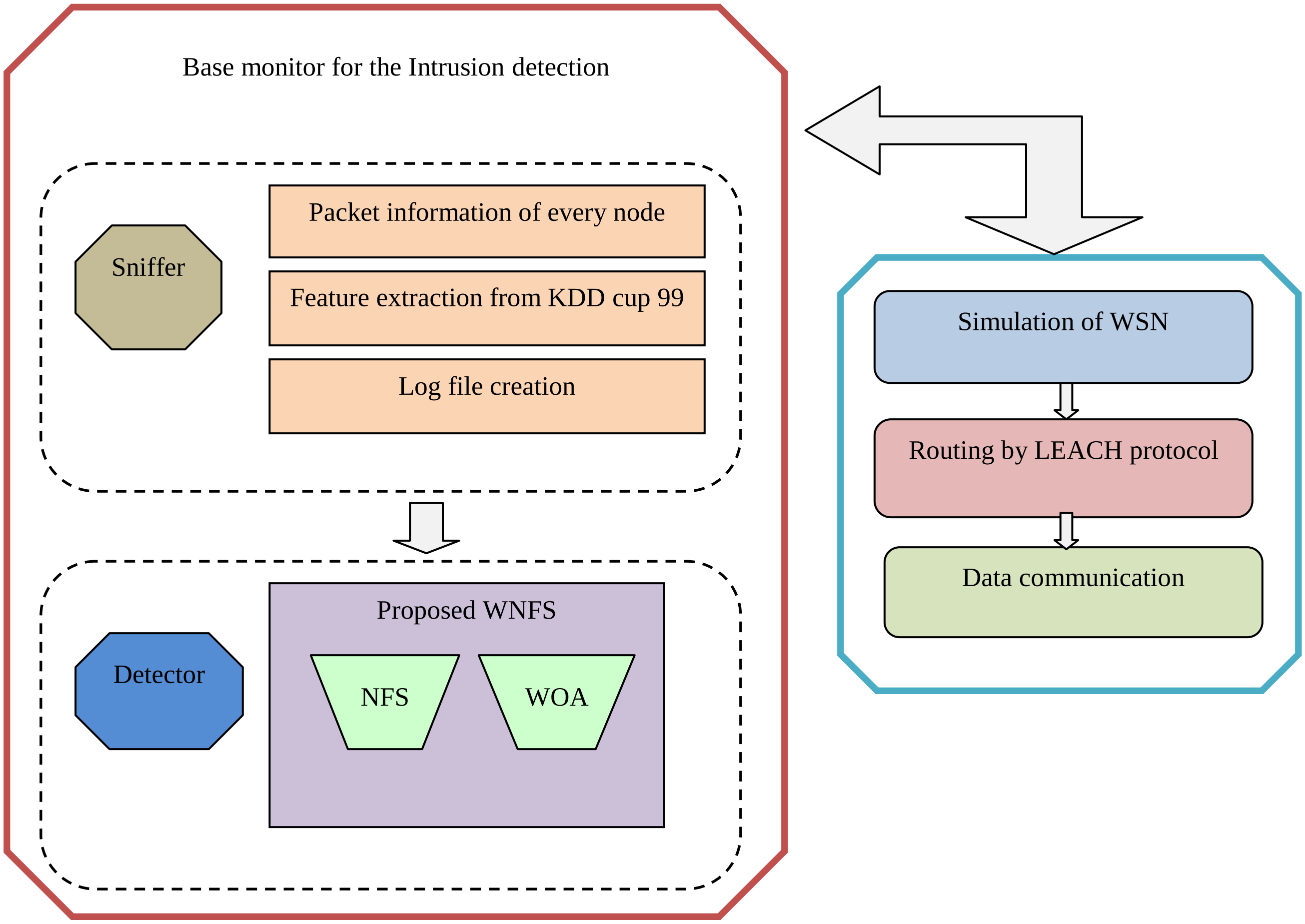

Base monitor for the Intrusion detection
Sniffer
Packet information of every node
Feature extraction from KDD cup 99
Log file creation
Detector
Proposed WNFS
NFS
WOA
Simulation of WSN
Routing by LEACH protocol
Data communication

Figure 2. Architecture of the proposed ID-WNFS based Intrusion detection system

The detector component has the WNFS algorithm, which is developed by integrating the neuro fuzzy model and the WOA algorithm. The WOA helps in choosing the optimal fuzzy rules for classifying the nodes as intruder or the normal node. In this work, the simulation of the WSN is carried out by the LEACH protocol, and thus observes the results of the ID-WNFS model and creates the routing path without any intruders.

The proposed ID-WNFS system has two components, like as sniffer and detector for effectively identifying the intruders in the WSN and each component are explained below:

A. Sniffer: Creation of the log file

The first component in the proposed ID-WNFS system is the sniffer, and as the name suggests it carefully observes the packet information of the each node. The router nodes while interconnected with the other nodes for passing the information amidst the source and destination may undergo certain changes. Also, the nodes in the WSN are mobile, and have limited energy resource. Each sensor node in the WSN has the information regarding the next node for which the packet need to be sending, and the node from which the packet is received. The sniffer component in the proposed ID-WNFS observes the transmission pattern, and stores all the packet information of the sensor node. The packet information helps in finding the suitable log file for the intrusion detection. Each node in the WSN is registered within the server, and thus by observing the log information, the intruder node can be identified and eliminated from the communication.

Feature extraction from KDD cup 99

After observing the packet information from B nodes of the WSN, the 15 features are extracted from it. The feature extraction is done based on the information available in the KDD cup 99 dataset as it can be considered as the one of the standard platform for the intrusion detection in WSN. The various features observed from the KDD cup 99 dataset are src-bytes, dst-bytes, wrong fragment, urgent, num-failed-logins, root-shell, num-access-files, is-hot-login, is-guest-login, num-file-creation, serror-rate, rerror-rate, same-srv-rate, and diff-srv-rate respectively.

src-bytes: The src-bytes feature gives the information regarding the total number of bytes of information transferred from source to destination.

dst-bytes: The dst-bytes feature gives the information regarding the total number of bytes of received by the destination nodes from the source node.

wrong- fragment: This feature contains the information related to the wrong fragments present in the communication path.

urgent: This feature notes the total number of urgent packets to be sent via the communication path.

num-failed-logins: The user tries to login into the WSN server and may fail to attempt and this is noted as the num-failed-logins.

root-shell: This feature is discrete and provides the value 1 if the root-shell is obtained else the value is 0.

num-access-files: The WSN has variety of operations in the access control files, and the total number of operations carried out in the access control files is noted in this feature.

is-hot-login: Provides the value as 1, if the login is from the hot or else the value is 0.

is-guest-login: Provides the value as 1, if the login is from the guest or else the value is 0.

num-file-creation: Has the information about the total number of file creation operations in the WSN.

serror-rate: The WSN has the synchronization error noted as ‘SYN’, and this feature gives the information about the total % of connections with the ‘SYN’ error.

rerror-rate: Other than the ‘SYN’ error, the WSN has also the rejection error noted as ‘REJ’. The rerror-rate gives the information about the total % of connections with the ‘REJ’ error.

same-srv-rate: This feature gives the information regarding the % of connections done to the same service.

diff-srv-rate: This feature gives the information regarding the % of connections done to the different service.

After identifying the 15 features from the packet information, the log file is created by the sniffer component. The log file consists of 15 features for every node. As there are B nodes in the WSN, the size of the log file created is $B \times 15$. The created log file is expressed as $L = \{l_1, l_2, \ldots l_{15}\}$ and it is fed to the detector module for identifying the intrusions.

B. Detector: Intrusion detection through proposed WNFS

The detector component comprises of the proposed WNFS network for identifying the intruder node. This work develops the WNFS network by including the optimization properties with the existing neuro fuzzy model (NFS) [23]. The existing NFS model developed in the literature combines both the neural network and fuzzy logic properties. The layers of the neural network are fed with the fuzzy rules for performing the classification. The fuzzy logic while implemented for any system provides large number of fuzzy rules in its rule base. It is practically impossible to identify the required rule base for the classification. For this purpose, this work has used the WOA algorithm for selecting the appropriate rules for the NFS system. The architecture of the proposed WNFS model is depicted in figure 3. The architecture of the proposed WNFS model is similar to the NFS, and the only change is the number of neurons provided for the training the log file created by the sniffer component.

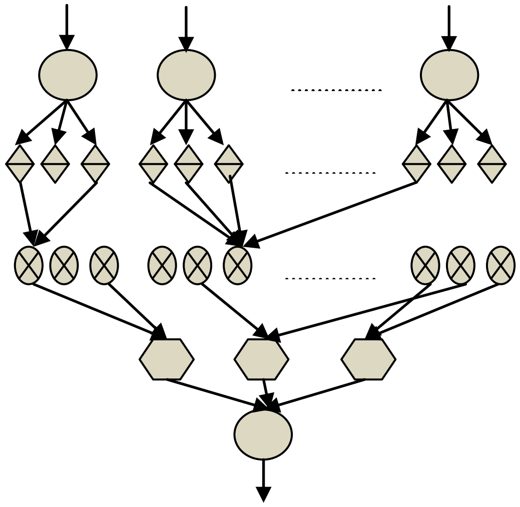


Figure 3. Diagrammatic representation of the WNFS

As shown in the figure, the log files are provided as the input to the input layer of the WNFS. The WNFS has different layers such as input, hidden and output. As the aim is to find the node to be intruder or not the WNFS has only one neuron at the output layer. The hidden layer provides optimal fuzzy rules for the modifying the input and the output are observed from the output layer. The NFS model considered in this work is the Mamdani-type model, which uses the optimal fuzzy rule base. The input to the WNFS is the log file, and as there are 15 features in the log file, the total number of input neurons is considered as 15. The input layer of the WNFS is represented as follows,

$$L = \{l_1, l_2, \ldots l_{15}\} \qquad (1)$$

where, l_1 refer to the first feature in the log file. For selecting the optimal rule base for the hidden layer, this work considers the WOA algorithm. Then, the hidden layer output is passed through the output layer and the final decision on the node is taken. The output layer provides the value as 1 for the presence of intrusion and 0 for the normal node. The output layer of the WNFS is represented as follows:

$$Q = \begin{Bmatrix} 1\,; \text{Intruder} \\ 0; \ \text{Normal} \end{Bmatrix} \quad (2)$$

where, Q indicates the output of the WNFS model. The major task lies in identifying the optimal fuzzy rules. Adopting basic fuzzy rule base complicates the learning task, as it is large in size. Here, the optimal fuzzy rules are observed based on the WOA algorithm. The WOA algorithm selects the optimal values based on the prey searching behaviour of the whale. The WOA algorithm for identifying the optimal F rule base for the hidden layers is explained as follows:

Initialization: The WOA finds optimal rule base having F number of components, and thus the solution space for the WOA is expressed as,

$$R = \{R_1, R_2, \ldots R_F\} \quad (3)$$

where, R_F refers to the components in the rule base. The WOA finds the best search agent $R*$ through the optimization.

Fitness: The next step identifies the best search agent $R*$ through the fitness criteria, and here the fitness is considered to the detection accuracy.

Update phase: The WOA updates the position of the search agent in both the exploration and the exploitation phase. The update done based on the prey search behaviour is expressed as follows:

$$\vec{Z} = \left| \vec{S}\,\vec{R}^*(t) - \vec{R}(t) \right| \quad (4)$$

$$\vec{R}(t+1) = \vec{R}^*(t) - \vec{U} \cdot \vec{Z} \quad (5)$$

where, $\vec{Z}$ indicates the modified search agent. Now the values of $\vec{U}$ and $\vec{S}$ is expressed as,

$$\vec{U} = \vec{a} \cdot \vec{b} - \vec{a} \quad (6)$$

$$\vec{S} = 2 \cdot \vec{b} \quad (7)$$

where, a indicates the constant within the range of 2 to 0. and b refer to the ranging vector [0,1]. The update in the exploitation phase can be expressed as,

$$\vec{R}(t+1) = \vec{Z}^{'} \cdot e^{st} \cdot \cos(2\pi x) + \vec{R}^*(t) \quad (8)$$

Where, $$\vec{Z}^{'} = \left| \vec{R}^*(t) - \vec{R}(t) \right| \quad (9)$$

Also, the exploration phase based update depends on choosing random search agents, and it is expressed as,

$$\vec{R}(t+1) = \vec{R}_{rand} - \vec{U} \cdot \vec{Z} \quad (10)$$

$$\vec{Z} = \left| \vec{S}\,\vec{R}_{rand} - \vec{R} \right| \quad (11)$$

Best search agent: Now, based on the fitness criteria, the best search $R*$ is found, and it replaces the previous solution.

Termination: Up to T number of iterations, the WOA algorithm is carried out, and at the end of iteration the optimal fuzzy rule base is selected and provided to the WNFS model.

C. Establishing the routing path based on LEACH protocol

After declaring the node as the ‘intruder’ or ‘normal node’ the proposed ID-WNFS system passes the information to the LEACH protocol. The LEACH protocol [24] establishes the routing path by ignoring the intruder node. The LEACH protocol gets updated from time to time and hence the WSN is free from intrusion. This work chooses the LEACH protocol as the routing algorithm, since the LEACH establishes the routing path by constructing large sized clusters. Also, the protocol updates the cluster head simultaneously and hence the chance of routing path failure is very low. The LEACH protocol can be explained in brief as follows:

LEACH protocol gets the information regarding the intruder node, and carries out the simulation for creating the routing path amidst the source and destination. The LEACH protocol creates the routing path through the clustering, and it has two phases 1) Setup phase, and 2) Steady phase.

1) Setup phase: The LEACH protocol creates the routing path by concentrating on the energy parameter and hence selects the node with the highest energy to the cluster head. The setup phase has three steps:

i) Advertisement of the cluster head: After selecting the highest energy node as the cluster head, the protocol sends the information to the other nodes regarding the cluster head node. The selection of the cluster head is restricted for the single round, and the particular node can become the cluster head after each node in the WSN acts as the cluster head.

ii) Cluster setup: The cluster is formed based on the nodes providing the response to the advertisement provided in the previous step. The non- cluster node only sends the information and hence switches off the transmission part.

iii) Creating the suitable transmission schedule: The cluster head creates the transmission path for the other nodes in the cluster.

2) Steady phase: After establishing the connection, the head node collects the information from the node and sends to the base station. The transmission path to the destination is done through the various cluster heads in the WSN.

V. Results and discussion

The simulation results of the proposed WNF intrusion detection system is presented in this section and evaluation is done by introducing various attacks on the WSN nodes.

A. Experimental setup

The WSN simulation is carried out in the MATLAB as the implementation tool, and the PC is configured with the settings such as Windows 10 OS, 4 GB RAM, and Intel I3 processor. The WSN architecture is built by considering both the 50 and 100 nodes for the simulation.

Database description

The features for building the ID-WNFS is built form the KDD cup 99 dataset [25], and here we consider a total of 15 features and provide to the intrusion detector. The KDD cup 99 dataset comprises of a predictive model for recognizing the good and the bad connections in the WSN.

5.1.2 Performance metrics

The proposed ID-WNFS model is evaluated with the metrics like as network lifetime, energy and the detection accuracy. For the improved performance, it is necessary to maintain these parameters as high as possible.

Network lifetime: The network lifetime depends on the energy of the individual nodes. During the transmission of nodes, and mobility, the node may undergo specific changes and the lifetime gets reduced.

Energy: At the beginning of the simulation, the energy of the network remains high, and reduces at the end of the simulation. The energy depends on the energy required for the transmission and reception of the byte of information.

Detection accuracy: The proposed ID-WNFS system detects the nodes affected by the intruder, and the thus detection accuracy clearly depicts the state of the proposed model. Detection accuracy defines the ratio of total nodes detected as the intruder node, to the actual number of intruder node present in the system.

Comparative methods

The proposed ID-WNFS is compared against other existing soft computing methods, such as NN, fuzzy, artificial immune system (AIS), Fuzzy artificial immune system (FAIS) [19] and the description to the comparative techniques is stated below:

NN: The NN model is adopted here for the intrusion detection, and it finds the intrusion through the error estimate.

Fuzzy: The fuzzy based model has adopted various fuzzy rules for identifying the intruder nodes in the WSN.

AIS: The AIS system adopts the artificial intelligence logic for indentifying the intruders.

FAIS: Along with the AIS, various fuzzy rules are used for the intrusion detection.

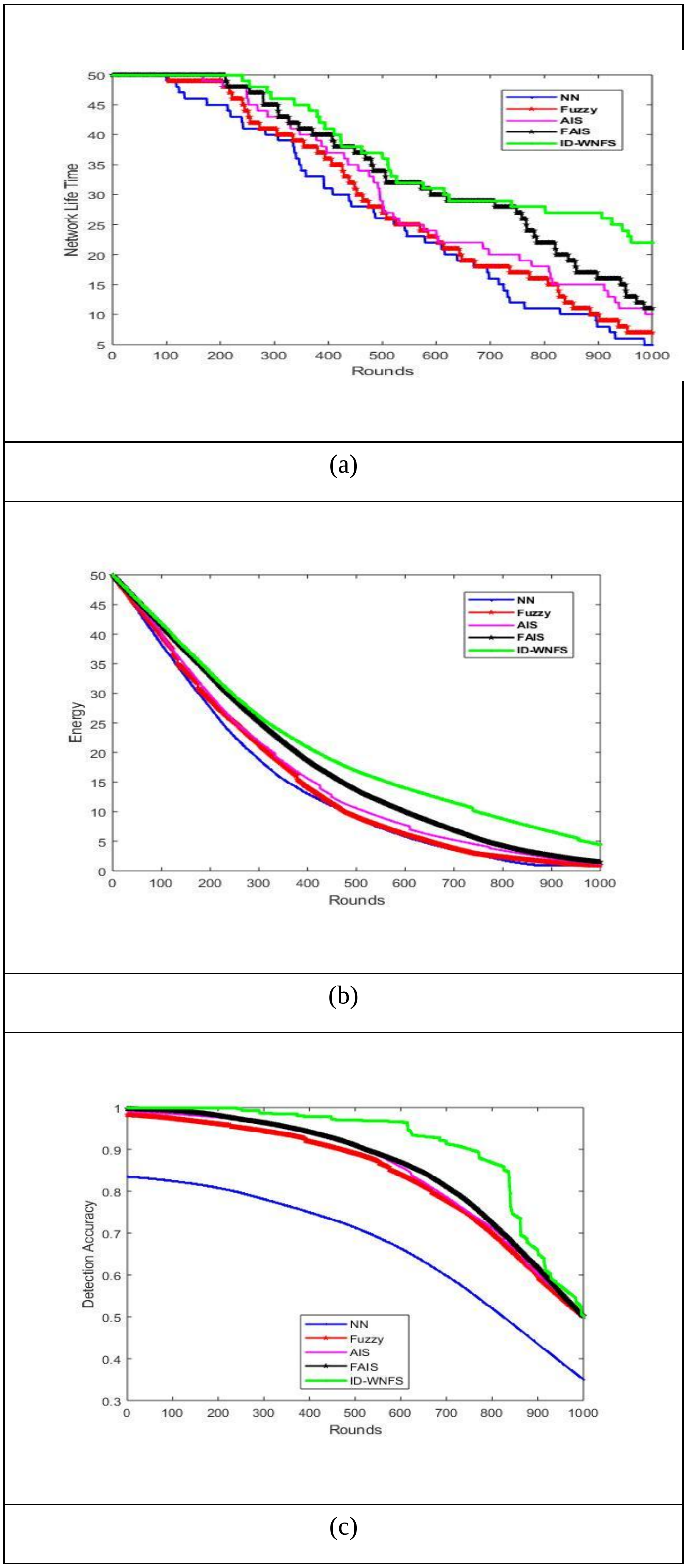
B. Comparative analysis

Here, the comparative analysis of the proposed ID-WNFS logic has been evaluated. Two kinds of attack such as DOS and the black hole attack have been introduced on the system. Total node count on the WSN is varied as 50 and 100.

Comparative analysis with the WSN of 50 nodes

i. Under the influence of the DOS attack

Figure 4 presents the comparative analysis of the ID-WNFS model to identify the intrusions in the WSN with the 50 nodes and the influence of the DOS attack. Figure 4.a depicts the analysis based on the network life time against various simulation rounds. The simulation is carried out for 1000 rounds, and at 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the network lifetime of 26, 27, 29, and 34. At the same round, the proposed ID-WNFS has the improved network lifetime of 36, and thus having improved performance. At the end of the simulation, i.e. at 1000 rounds, the existing models NN, fuzzy, AIS, and the FAIS has the network lifetime of 5, 7, 10, and 11 respectively, while the proposed ID-WNFS has the network lifetime of 22. Figure 4.b shows the analysis of ID-WNFS based on the energy against various simulation rounds. The simulation is carried out for 1000 rounds, and at 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the energy value of 8.950311, 9.163273, 10.58637, and 13.67748. At the same round, the proposed ID-WNFS has the improved energy of 16.87607, and thus overpowers other models. At 1000 rounds, the existing models NN, fuzzy, AIS, and the



(a)

(b)

(c)

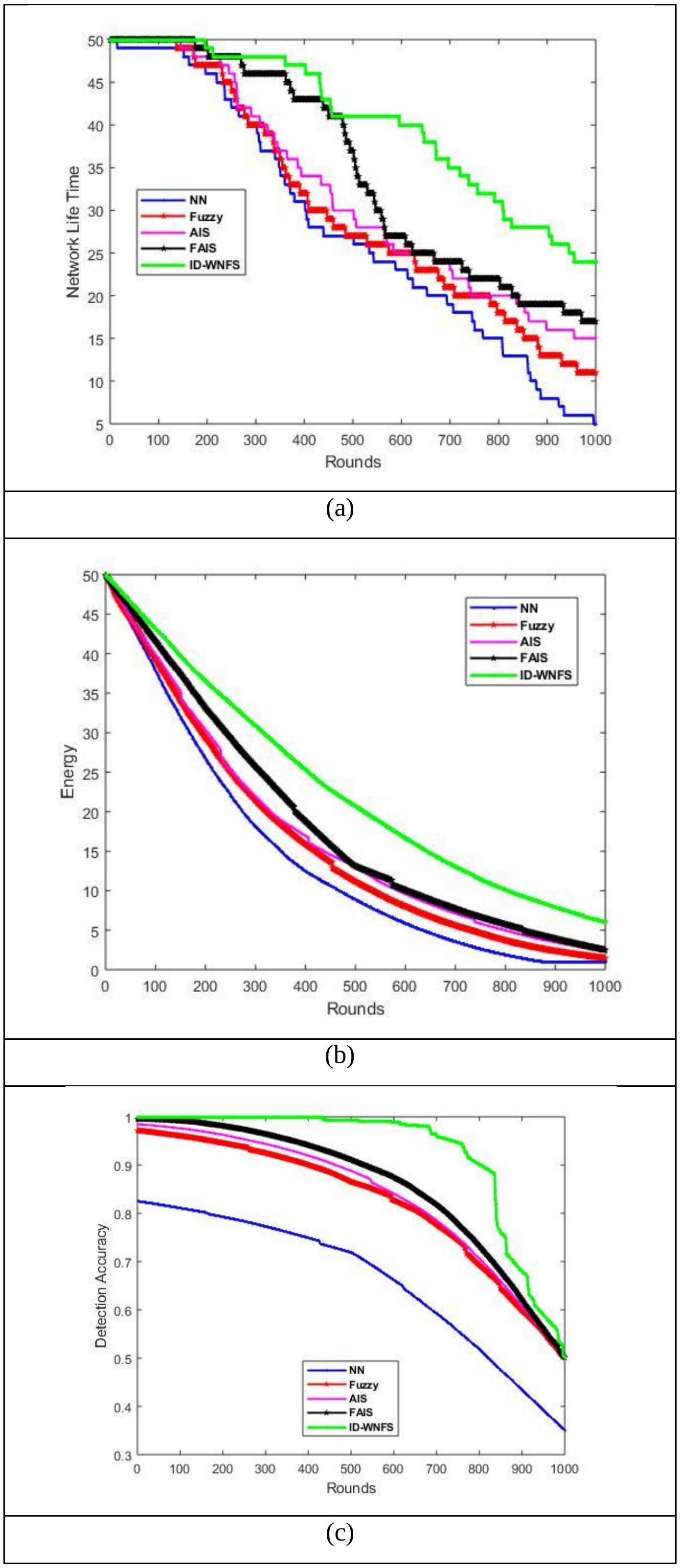
Figure 4. Comparative analysis with the WSN of 50 nodes with the DOS attack, (a) Network life time, (b) energy, and (c) detection accuracy

FAIS has the energy of 1, 1, 1.158272, and 1.519641 respectively, while the proposed ID-WNFS has energy of 4.416784. Figure 4.c depicts the analysis based on the detection accuracy against various simulation rounds. At 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the detection accuracy of 0.713225, 0.890513, 0.907986, and 0.91026. At the same round, the proposed ID-WNFS has the high detection accuracy of 0.969954, and thus having improved performance. At the end of the simulation, i.e. at 1000 rounds, the existing models NN, fuzzy, AIS, and the FAIS has the detection accuracy of 0.350863, 0.500867, 0.500889, and 0.501223 respectively, while the proposed ID-WNFS has the detection accuracy of 0.501365.

ii. Under the influence of the black hole attack

Figure 5presents the comparative analysis of the ID-WNFS model to identify the intrusions in the WSN with the 50 nodes and the influence of the Black hole attack. Figure 5.a depicts the analysis based on the network life time against various simulation rounds under the influence of the black hole attack. The simulation is carried out for 1000 rounds, and at 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the network lifetime of 27, 27, 30, and 37. At the same round, the proposed ID-WNFS has the improved network lifetime of 41, and thus having improved performance. At the end of the simulation, i.e at 1000 rounds, the existing models NN, fuzzy, AIS, and the FAIS has the network lifetime of 5, 11, 15, and 17 respectively, while the proposed ID-WNFS has the network lifetime of 24. Figure 5.b shows the analysis of ID-WNFS based on the energy against various simulation rounds under black hole attack scenario. The simulation is carried out for 1000 rounds, and at 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the energy value of 8.856812, 11.16387, 13.10064, and 13.10916. At the same round, the proposed ID-WNFS has the improved energy of 20.68005, and thus overpowers other models. At 1000 rounds, the existing models NN, fuzzy, AIS, and the FAIS has the energy of 1, 1.455657, 2.296838, and 2.493823 respectively, while the proposed ID-WNFS has energy of 6.007708. Figure 5.c depicts the analysis based on the detection accuracy against various simulation rounds under the influence of the black hole attack. At 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the detection accuracy of 0.501365, 0.86537, 0.88808, and 0.911162. At the same round, the proposed ID-WNFS has the high detection accuracy of 0.992307, and thus having improved performance. At the end of the simulation, i.e. at 1000 rounds, the existing models NN, fuzzy, AIS, and the FAIS has the detection accuracy of 0.350732, 0.500776, 0.500804, and 0.500921 respectively, while the proposed ID-WNFS has the detection accuracy of 0.50204

.



(a)

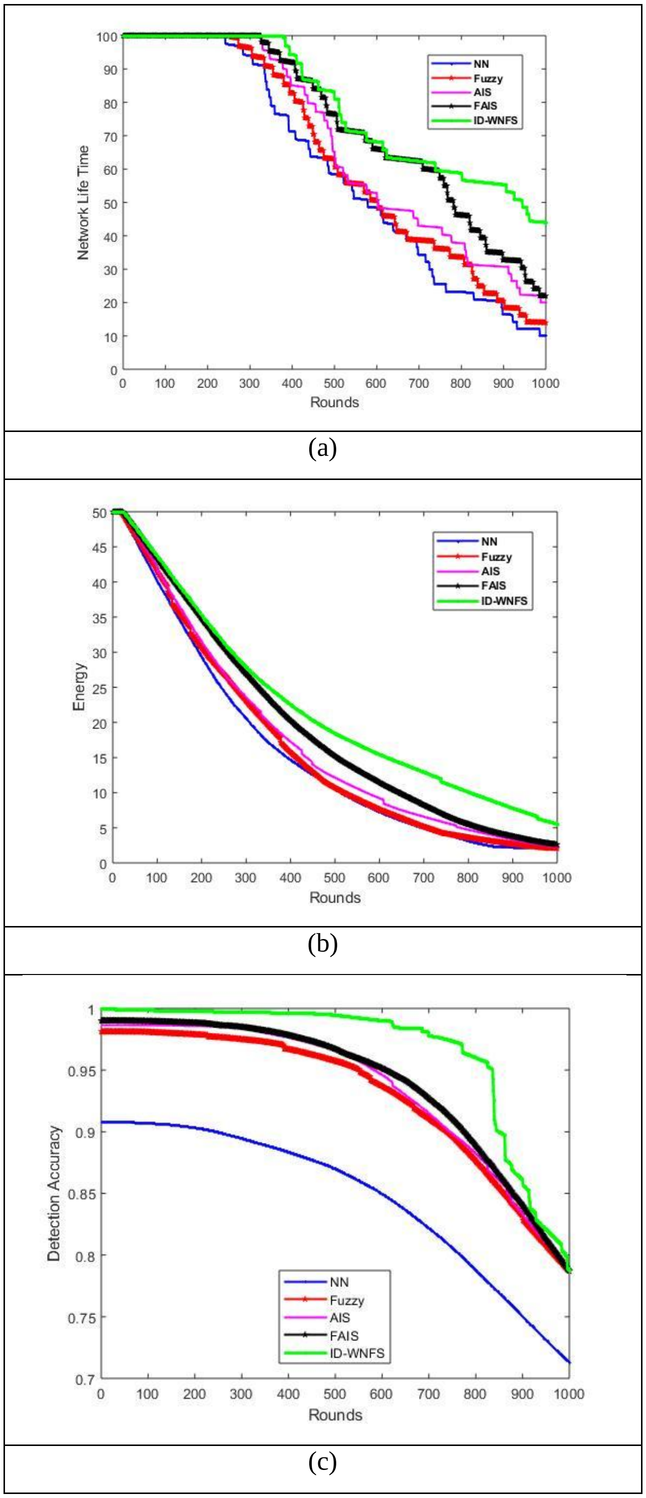
(b)

(c)

Figure 5. Comparative analysis with the WSN of 50 nodes with the Black hole attack, (a) Network life time, (b) energy, and (c) detection accuracy

5.2.2 Comparative analysis with the WSN of 100 nodes

i. Under the influence of the DOS attack



(a)

(b)

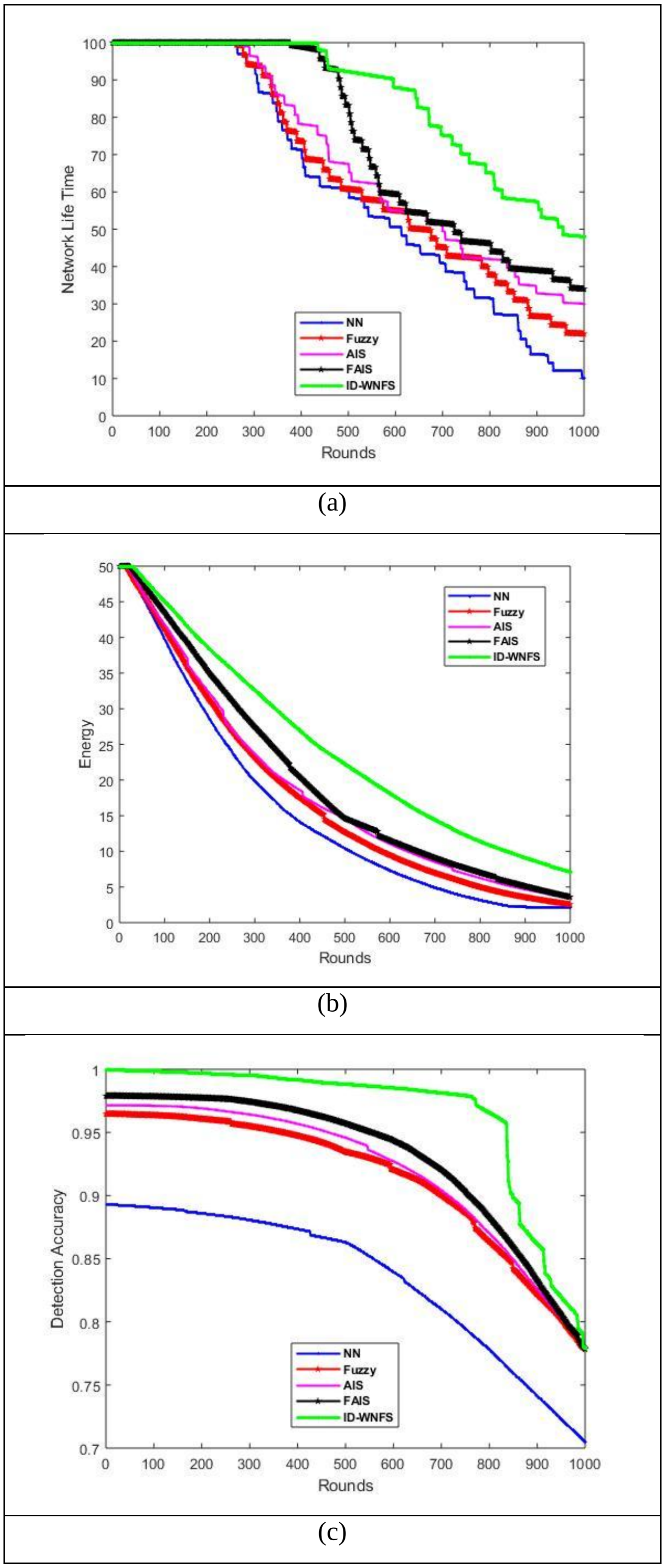
(c)

Figure 6. Comparative analysis with the WSN of 100 nodes with the DOS attack, (a) Network life time, (b) energy, and (c) detection accuracy

Figure 6 presents the comparative analysis of the ID-WNFS model to identify the intrusions in the WSN with the 100 nodes and the influence of the DOS attack. Figure 6.a depicts the analysis based on the network life time against various simulation rounds. The simulation is carried out for 1000 rounds, and at 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the network lifetime of 58.487, 60.7365, 65.2355, and 76.483. At the same round, the proposed ID-WNFS has the improved network lifetime of 80.982, and thus having improved performance. At the end of the simulation, i.e at 1000 rounds, the existing models NN, fuzzy, AIS, and the FAIS has the network lifetime of 9.9975, 13.9965, 19.995, and 21.9945 respectively, while the proposed ID-WNFS has the network lifetime of 43.989. Figure 6.b shows the analysis of ID-WNFS based on the energy against various simulation rounds. The simulation is carried out for 1000 rounds, and at 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the energy value of 10.49941, 10.71237, 12.13547, and 15.22658. At the same round, the proposed ID-WNFS has the improved energy of 18.42517, and thus overpowers other models. At 1000 rounds, the existing models NN, fuzzy, AIS, and the FAIS has the energy of 2.0991, 2.0991, 2.257372, and 2.618741 respectively, while the proposed ID-WNFS has energy of 5.515884. Figure 6.c depicts the analysis based on the detection accuracy against various simulation rounds. At 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the detection accuracy of 0.869725, 0.957418, 0.966061, and 0.967186. At the same round, the proposed ID-WNFS has the high detection accuracy of 0.994435, and thus having improved performance. At the end of the simulation, i.e. at 1000 rounds, the existing models NN, fuzzy, AIS, and the FAIS has the detection accuracy of 0.712747, 0.786944, 0.786955, and 0.78712 respectively, while the proposed ID-WNFS has the detection accuracy of 0.787191.

ii. Under the influence of the black hole attack

Figure 7 presents the comparative analysis of the ID-WNFS model to identify the intrusions in the WSN with the 100 nodes and the influence of the black hole attack. Figure 7.a depicts the analysis based on the network life time against various simulation rounds. The simulation is carried out for 1000 rounds, and at 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the network lifetime of 60.7365, 60.7365, 67.485, and 83.2315. At the same round, the proposed ID-WNFS has the improved network lifetime of 92.2295, and thus having improved performance. At the end of the simulation, i.e at 1000 rounds, the existing models NN, fuzzy, AIS, and the FAIS has the network lifetime of 9.9975, 21.9945, 29.9925, and 33.9915 respectively, while the proposed ID-WNFS has the network lifetime of 47.988. Figure 7.b shows the analysis of ID-WNFS based on the



(a)

(b)

(c)

Figure 7. Comparative analysis with the WSN of 100 nodes with the Black hole attack, (a) Network life time, (b) energy, and (c) detection accuracy

energy against various simulation rounds. The simulation is carried out for 1000 rounds, and at 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the energy value of 10.40591, 12.71297, 14.64974, and 14.65826. At the same round, the proposed ID-WNFS has the improved energy of 22.22915, and thus overpowers other models. At 1000 rounds, the existing models NN, fuzzy, AIS, and the FAIS has the energy of 2.0991, 2.554757, 3.395938, and 3.592923 respectively, while the proposed ID-WNFS has energy of 7.106808. Figure 7.c depicts the analysis based on the detection accuracy against various simulation rounds. At 500 round, the existing algorithms such as NN, fuzzy, AIS, and the FAIS has the detection accuracy of 0.863016, 0.934671, 0.945782, and 0.957075. At the same round, the proposed ID-WNFS has the high detection accuracy of 0.988165, and thus having improved performance. At the end of the simulation, i.e. at 1000 rounds, the existing models NN, fuzzy, AIS, and the FAIS has the detection accuracy of 0.704906, 0.778314, 0.778327, and 0.778385 respectively, while the proposed ID-WNFS has the detection accuracy of 0.778932.

C. Comparative discussion

Here, the comparative discussion of the performance of the various existing models and the proposed ID-WNFS model is discussed. As depicted in table 1, the performances of the models are observed for the simulation round of 1000. From the below table, it is evident that the intrusion detection is more effectively performed by the proposed ID-WNFS scheme.

Table 1. Comparative discussion

Methods	Evaluation metrics		
	Network life time	Energy	Detection accuracy
NN	9.9975	2.0991	0.712747
Fuzzy	13.9965	2.554757	0.786944
AIS	19.995	3.395938	0.786955
FAIS	21.9945	3.592923	0.78712
Proposed ID-WNFS	43.989	7.106808	0.787191

Among the existing works, the FAIS model has the competitive performance with the values of 21.9945, 3.592923, and 0.78712 as the network life time, energy and detection accuracy. The NN model has the overall worst performance, and the fuzzy based scheme has average performance. The proposed ID-WNFS model can be concluded to have best performance, as the detection accuracy, energy and the network lifetime are comparatively high than the existing works. The proposed ID-WNFS model has gained improved performance in the intrusion detection with the network lifetime as 43.989, energy as 7.106808 and the detection accuracy as 0.787191.

VI. CONCLUSION

This paper introduces the intrusion detection model for detecting the intruders affecting the mode of communication in WSN nodes. The proposed ID-WNFS has been developed in this research work for intrusion detection, and model has advantages of both the neuro and the fuzzy scheme. The proposed ID-WNFS model performs the intrusion detection through the sniffer and the detector component. The sniffer component creates the log file by observing the transmission details of the nodes, and the extracts 15 features from the same. The extracted features are complied together to form the log file and provided to the detector. The detector has the WNFS module for the intrusion detection. The WNFS has the nuero fuzzy architecture, and the required fuzzy rules are generated based on the WOA algorithm. The LEACH protocol creates the routing path for the communication based on the intrusion information provided by the proposed ID-WNFS algorithm. The simulation of the proposed ID-WNFS is done by introducing various attacks. From the simulation results, it can be concluded that the ID-WNFS model has improved performance with the network lifetime as 43.989, energy as 7.106808 and the detection accuracy as 0.787191.

REFERENCES

[1] N. Assad, B.Elbhiri, M. A. Faqihi, M. Ouadou , D. Aboutajdine, "*Efficient deployment quality analysis for intrusion detection in wireless sensor networks*", Wireless Networks, vol. **22**, Issue. **3**, pp**991-1006**, **2016.**

[2] H. Moosavi,F. M. Bui, "*A Game-Theoretic Framework for Robust Optimal Intrusion Detection in Wireless Sensor Networks*", IEEE Transactions on Information Forensics and Security, vol. **9**, Issue. **9**, pp. **1367-1379**, **2014**.

[3] A. K. Sagar,D. K. Lobiyal, "*Probabilistic Intrusion Detection in Randomly Deployed Wireless Sensor Networks*", Wireless Personal Communications, vol. **84**, no. **2,** pp. **1017-1037, 2015**.

[4] L. Gheorghe, R. Rughinis , R. Tataroiu, "*Adaptive Trust Management Protocol based on Intrusion Detection for Wireless Sensor Networks"*, In proceedings of IEEE International Conference on Networking in Education and Research, pp. **1-7**, **2013**.

[5] M. Wazid, A. K. Das, "*An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks*", Wireless Personal Communications, vol. **90**, Issue **4**, pp. **1971-2000**, **2016**.

[6] A. Saeed, A. Ahmadinia, A. Javed, H. Larijani, "*Random Neural Network based Intelligent Intrusion Detection for Wireless Sensor Networks*", In proceedings of International Conference on Computational Science, vol. **80**, pp. **2372-2376, 2016**.

[7] S.Shamshirband, A. Amini, N. B. Anuar, L. M. Kiah, T. Y. Wah , S. Furnell, "*D-FICCA: A Density-based Fuzzy Imperialist Competitive Clustering Algorithm for Intrusion Detection in Wireless Sensor Networks"*, Measurement, vol. **55**, pp. **212-226, 2014**.

[8] P. Rutravigneshwaran, "*A Study of Intrusion Detection System using Efficient Data Mining Techniques',* International Journal of Scientific Research In Network Security and communication , vol. **5**,no. **6**,pp **5-8,2017.**

[9] I.Butun, Salvatore D. Morgera, R. Sankar, "*A Survey of Intrusion Detection Systems in Wireless Sensor Networks",* In proceedings of IEEE International Conference on Modeling, Simulation and Applied Optimization, pp. **1-6, 2015**.

[10] Y. Wang, X. Wang, B. Xie, D. Wang , Dharma P. Agrawal, "*Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks"*, IEEE Transactions on Mobile computing, vol. **7**, no. **6,** pp. **698-710, 2008**.

[11] A. Abduvaliyev, Al-Sakib Khan Pathan, J. Zhou, R. Roman, Wai-Choong Wong, "*On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks"*, IEEE Communications Surveys & Tutorials, vol. **15,** no. **3**, pp. **1223-1237, 2013.**

[12] Sandhya G , A. Julian, "*Intrusion Detection in Wireless Sensor Network Using Genetic K-Means Algorithm*", In proceedings of IEEE International Conference on Advanced Communication Control and Computing Teclmologies, pp. **1-4, 2014**.

[13] G. Han, J. Jiang, W. Shen, L. Shu, J. Rodrigues, "*IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks",* IET Information Security, vol. **7**, no. **2**, pp. **97-105, 2013**.

[14] H. M. Salmon, C. M. d. Farias, P. Loureiro, L. Pirmez, "*Intrusion Detection System for Wireless Sensor Networks Using Danger Theory Immune-Inspired Techniques*", International Journal of Wireless Information Networks, vol. **20**, Issue **1**, pp. **39-66, 2013**.

[15] S. Shamshirband, N.B. Anuar, M.L.M. Kiah, A. Patel, *"An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique*", Engineering Applications of Artificial Intelligence, vol. **26**, no. **9**, pp. **2105-2127, 2013.**

[16] S. Rajasegarar, C. Leckie, M. Palaniswami, "*Hyperspherical cluster based distributed anomaly detection in wireless sensor networks"*, Journal of Parallel and Distributed Computing, vol. **74**, no. **1**, pp. **1833-1847, 2014**.

[17] M. Elleuch, O. Hasan, S. Tahar, M. Abid, "*Formal probabilistic analysis of detection properties in wireless sensor networks"*, Formal Aspects of Computing, vol. **27**, no. **1**, pp. **79-102, 2015**.

[18] S. Mirjalili, A. Lewis, "*The Whale Optimization Algorithm"*, Advances in Engineering Software Vol.**95**, pp. **51–67, 2016**.

[19] S. Shamshirband, N. B. Anuar, L. M. Kiah, "*Co-FAIS: Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks*", Journal of Network and Computer Applications, vol. **42**, pp. **102-117, 2014**.

[20] M. Riecker, S. Biedermann, R. E. Bansarkhani, M. Hollick, "*Lightweight energy consumption-based intrusion detection system for wireless sensor networks*", International Journal of Information Security, vol. **14**, Issue **2**, pp.**155-167**, **2015**.

[21] Guorui Li, Jingsha He,Yingfang Fu, "*Group-based intrusion detection system in wireless sensor networks"*, Computer Communications, vol. **31**, no. **18**, pp. **4324-4332, 2008**.

[22] M. Moshtaghi, C. Leckie, S. Karunaseker , S. Rajasegarar, "*An adaptive elliptical anomaly detection model for wireless sensor networks*", Computer Networks, vol. **64**, pp. **195-207, 2014**.

[23] A. Yadav, V.K. Harit, "*Fault Identification in Sub-Station by Using Neuro-Fuzzy Technique",* International Journal of Scientific Research in Computer Science and Engineering,Vol. **4.** No. **6**,pp **1-7,2016.**

[24] W. R. Heinzelman, A. Chandrakasan, H. Balakrishnan, "*Energy-Efficient Communication Protocol for Wireless Microsensor Networks*," In Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000,IEEE,pp. **1-10,2000.**

[25] *KDD Cup 1999. Available on: http://kdd.ics. uci.edu/databases /kddcup99/kddcup99.html, October 2007.*