International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel Artificial Fish Integrated Particle Swarm Optimization (AFIPSO) and Random Artificial Neural Network Combined Gradient Descent (RANN-GD) Algorithm for WSN Security

S.Ramani[1], S.P.V.Subba Rao[2], Sahukar Latha[3], L.V.R.Chaitanya Prasad[4]

Submitted: 10/09/2022 **Accepted:** 20/12/2022

Abstract: Intrusion detection and classification is one of the most essential and challenging process in the Wireless Sensor Network (WSN). Typically, the wireless networks are highly susceptible to different types of network attacks, because which reduces the lifetime of entire network by interrupting the data transmission and communication operations. Hence, the conventional works intends to develop an efficient Intrusion Detection System (IDS) frameworks by using the optimization and classification methodologies. Still, it facing the problems of high complexity in operations, more time for data training, high error rate, and inefficient detection. So, this research work objects to develop an intelligent and advanced IDS framework by implementing the novel optimization based classification methodologies. For this purpose, a hybrid Artificial Fish Integrated Particle Swarm Optimization (AFIPSO) mechanism is deployed to optimally select the features for training the data models of classifier. Consequently, the Random Artificial Neural Network Integrated Gradient Descent (RANN-GD) is implemented for accurately spotting the intrusions from the given IDS datasets based on the optimal number of features. For testing and validation, three different and emergent IDS datasets such as NSL-KDD, UNSW-NB 15 and WSN-DS have been utilized in this work. During evaluation, the performance of both existing and proposed techniques are validated and compared by using various performance measures.

Keywords: *Wireless Sensor Network (WSN), Intrusion Detection System (IDS), Artificial Fish Integrated Particle Swarm Optimization (AFIPSO), Random Artificial Neural Network Integrated Gradient Descent (RANN-GD), Security, and Classification.*

1. Introduction

Wireless Sensor Network (WSN) [1, 2] has been increasingly utilized in many applications such as environmental monitoring, healthcare systems, transportation and logistics, military environment, and industrial systems. Because, it provides an enormous benefits such as high flexibility, more suitable for large-scale systems, increased speed in process, less maintenance, and reduced cost. Generally, the WSN [3, 4] is a kind of special communication network that comprises the large number of sensor nodes that are connected with each other through wireless. In this environment, the nodes are more responsible for accomplishing the general tasks such as tracking and monitoring. The general communication architecture [5] of WSN is shown in Fig 1, where the sensor nodes are interlinked with the gateway systems for communication.

[1]*Sreenidhi Institute of Science & Technology, Hyderabad-501301, Telangana, Email: ramanis@sreenidhi.edu.in*
[2]*Sreenidhi Institute of Science & Technology, Hyderabad-501301, Telangana, Email: spvsubbarao@sreenidhi.edu.in*
[3]*Sreenidhi Institute of Science and Technology, Hyderabad-501301, Telangana, Email: lathasahukar@gmail.com*
[4]*Sreenidhi Institute of Science and Technology, Hyderabad-501301, Telangana, Email:lvrchaitanya@sreenidhi.edu.in*

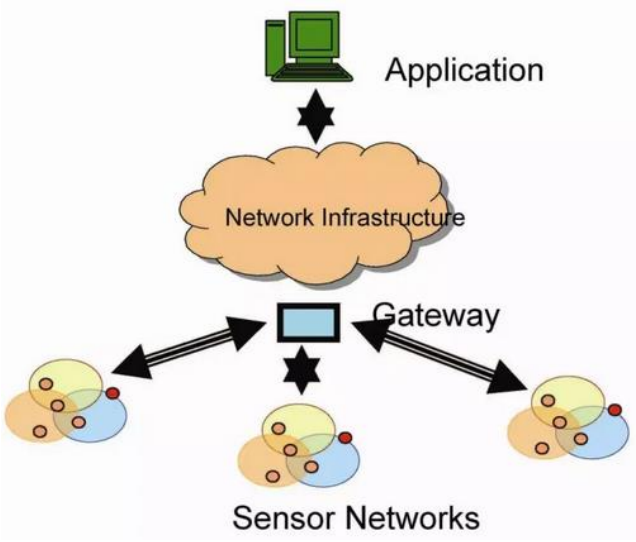

Fig 1. General structure of WSN

But, providing security [6-8] to this type of network is one of the most challenging and difficult task due to the random positioning of nodes. Typically, the intrusions or attackers can target to affect the communication of network by interrupting the normal operations [9, 10]. Also, it may affect the lifetime of both communicating nodes and network. Hence, it is more essential to increase the security of WSN against the network attacks. For this

purpose, there are different types of attack detection and classification methodologies have been developed in the conventional works. The existing approaches [11, 12] are mainly focusing on developing the classification methodologies for identifying the intrusions from the datasets. Yet, it facing some of the challenges [13-15] in intrusion detection and classification, which includes difficult computational operations, requires more time consumption, increased misclassification results, and error rate. Hence, the proposed work intends to develop an advanced Intrusion Detection System (IDS) framework for accurately locating and categorizing the types of intrusions from the given IDS datasets with reduced complexity and increased detection efficiency. The primary objectives of this research methodology are listed as follows:

- To avoid the misclassification rate and error rate, the input IDS datasets have been preprocessed by using the min-max normalization.
- To select the optimal number of features according to the global best fitness value, an intelligent and hybrid Artificial Fish Integrated Particle Swarm Optimization (AFIPSO) mechanism is developed.
- To accurately predict the classified label based on the optimal features set, an advanced Random Artificial Neural Network Integrated Gradient Descent (RANN-GD) based machine learning model is implemented.
- To assess the detection performance and efficiency of the proposed methodology, various evaluation metrics have been validated during analysis.

The remaining portions of this paper are segregated into the following sections: the existing optimization and classification techniques used for developing an IDS framework in WSNs are surveyed with its advantages and disadvantages in Section II. The clear working description of the proposed methodology is presented with its appropriate flow of illustration in Section III. The performance and comparative analysis of the proposed intrusion detection methodology are validated by using various measures in Section IV. Finally, the overall paper is summarized with its future scope in Section V.

2. Related Works

This unit investigates some of the conventional optimization and classification methods used for ensuring the security of WSN against the harmful network intrusions. Also, it analyzes the advantage and disadvantages of each mechanism according to its features and characteristics.

Kavousi-Fard, et al [16] implemented a Lower and Upper Bound Estimation (LUBE) model for detecting anomalies from the given dataset. This work mainly contributes to improve the accuracy and detection efficiency of anomaly prediction system by using the Symbiotic Organisms Search (SOS) model. Also, this paper investigated the different types of cyber-attacks with its effect in WSN that includes slammer worm, DoS attack, Havex malware, and DDoS attack. Moreover, the performance of this work was validated according to the measures of hit rate, false alarm rate, miss rate, and correct rejection rate. Yet, this paper limits with the major problems of increased error value and inefficient detection performance. Ahmad, et al [17] implemented a k-medoid customized clustering technique for developing a hybrid anomaly detection framework. Typically, the performance of WSN could be highly affected by the hybrid anomalies, because which interrupts the normal operations of the network. The key benefits of using the k-medoids clustering technique are as follows: increased convergence rate, fast in process, and easy to implement. Yet, it facing the problems related to the issues of reduced network scalability, reliability, and high delay in processing. Baig, et al [18] developed an intelligent attack detection framework for identifying the DoS attacks in the network. The main purpose of this work was to ensure the security properties of data integrity, confidentiality, and availability during transmission and communication. Here, two different types of techniques such as volume based detection and feature based detection have been investigated for spotting the attacks according to the volume of traffic. Moreover, the average dependency estimator has been utilized for exactly differentiating the legitimate and attack traffic. Despite of advantages, it has some other drawbacks in complex computational operations, and increased misclassification results.

Nancy, et al [19] employed a fuzzy temporal decision tree classification mechanism for developing an intrusion detection framework in WSN. In this system, the dynamic recursive feature selection mechanism has been utilized for selecting the most optimal features in order to improve the performance of classification. Moreover, an intelligent decision tree based machine learning mechanism was also used for predicting the normal and attacking data. Premkumar and Sundararajan [20] developed a Deep Learning based Defense Mechanism (DLDM) for accurately predicting the DoS attacks in WSN. Here, the different types of networking attacks have been examined with its appropriate defense models. It includes the types of flooding, de-synchronization, blackhole, collision, haming, exhaustion, and unfairness. The key benefits of this model were ensured detection performance, minimized false positives, and increased accuracy. Tan, et al [21] deployed a Synthetic Minority Oversampling Technique (SMOTE) incorporated with the random forest algorithm for an efficient intrusion detection system. The purpose of this paper was to provide the suitable solution for solving the class imbalance problem with ensured performance rate. Typically, the random forest was a kind of ensemble based learning methodology and, mainly used for solving the multi-objective classification problems. Here, the SMOTE analysis was performed for improving the training model of attack detection. The limitations behind this work were inability in handling large dimensional dataset, reduced accuracy, and complexity in tree construction.

Lima Filho, et al [22] implemented a machine learning based intrusion detection methodology for identifying the DoS attacks in the WSN. This paper highly intended to reduce the false alarm rate and network traffic with better attack detection performance. For this purpose, an automatic feature selection mechanism was utilized in this paper, which helps to determine the signature for adopting the smart detection. Based on the session value of extracted packets, the normal and attacking traffic have been effectively segregated by using this model. The primary advantages of this work were optimal performance, better accuracy in detection, and it enabled the smart detection process. Otoum, et al [23] deployed a Restricted Boltzmann Machine based Clustered IDS (RBC-IDS) methodology for infrastructure of WSN in order to prevent it from the harmful attacks. For improving the detection performance, the clustering methodology has been implemented, where the cluster head selection could be

performed based on the mobility factor, cumulative time, and weight value. Yet, the efficiency of this system was not up to mark, which degrades the performance of entire system.

Wazid, et al [24] developed a new intrusion detection framework, named as, Routing Attack Detection and Edge based – IoT (RAD-ET) for ensuring the security of WSNs. The main purpose of this work was to design an efficient anomaly detector for categorizing the legitimate and suspecting nodes from the network. Also, it objects to increase the packet delivery ratio by identifying the abnormal traffic flow. The benefits of this work were minimized computation and communication cost consumption. Hongsong, et al [25] utilized a Hilbert Huang Transform (HHT) based time frequency signal analysis method for identifying the low-rate DoS attacks with reduced false positives. Also, a spark based correlation coefficient model was employed for increasing the detection accuracy of IDS. In addition to that, the pearson correlation coefficient and spearman rank correlation coefficient have been estimated for validating the performance of this system. Still, it has the limitations of reduced speed of processing, and requires more time consumption.

Tamilarasi and Santhi [26] employed a Particle Swarm Optimization (PSO) based secured path selection mechanism for enabling the reliable data transmission in WSN. Here, the best optimal solution was identified based on the updation of weight values. This work mainly intends to obtain an increased packet delivery ratio, network throughput and network lifetime by establishing the valid and secured data transmission across the nodes in the network. However, it has the key problems of reduced speed, and increased energy consumption, which affects the performance of overall networking systems. Jiang, et al [27] developed a Sequence Backward Selection (SBS) algorithm for spotting the intrusions from the WSN. This work analyzed the different types of attacks that interrupts the regular operations of network, which includes blackhole, grayhole, flooding, and scheduling attacks. Moreover, it examined the performance of various feature selection methodologies used for selecting the suitable algorithm for attack detection and classification. Gopalakrishnan et al. (2016) discussed the detection of link failure due to the presence of malicious node by determining the gain of each link in the network. Also the detection of link failure due to the presence of malicious node by determining the gain of each link in the network

Based on this study, it is analyzed that the conventional works are highly objects to develop different types of classification algorithms for ensuring the security of WSN by protecting it from the network intrusions/attacks. However, it facing the problems related to the issues of increased complexity in algorithm design, inability to handle large dimensional datasets, increased misclassification results, and high false positives. Hence, the proposed work objects to develop an efficient and advanced mechanism for detecting intrusions in the WSN.

3. Proposed Methodology

This section discusses about the working methodology and operations of the proposed intrusion detection system with its appropriate flow and illustrations. The key contribution of this paper is to develop an optimization based classification methodology for accurately predicting the intrusions from the given datasets with reduced false positives and error values. For this purpose, an intelligent Artificial Fish Integrated Particle Swarm Optimization (AFIPSO) and Random Artificial Neural Network Integrated Gradient Descent (RANN-GD) techniques have been implemented in this work. Here, there are two different and most popular IDS datasets such as NSL-KDD, UNSW-NB15, and WSN-DS have been utilized for testing and validating the proposed IDS framework. The overall working flow of the proposed system is shown in Fig 2, which includes the following modules:

- Dataset preprocessing
- AFIPSO based feature selection
- RANN-GD based classification

After obtaining the dataset, it has been preprocessed for normalizing the attributes and features, because the original dataset is unbalanced and random. Hence, it must be preprocessed before using it for further operations, which helps to improve the accuracy of classification. Consequently, the set of most optimal number of features have been extracted and selected from the preprocessed dataset by using the AFIPSO mechanism. It elects the optimal features according to the global best fitness value, which are used for training the classifier. Here, a hybrid and advanced RANN-GD based machine learning classifier is employed for exactly predicting the intrusions with reduced computational complexity and increased detection efficiency. The primary advantages of using the proposed AFIPSO with RANN-GD mechanisms are listed in below:

- Optimal performance outcome
- Improved detection accuracy
- Minimal time consumption and complexity
- Ability to handle large dimensional datasets
- Increased convergence rate and speed of processing

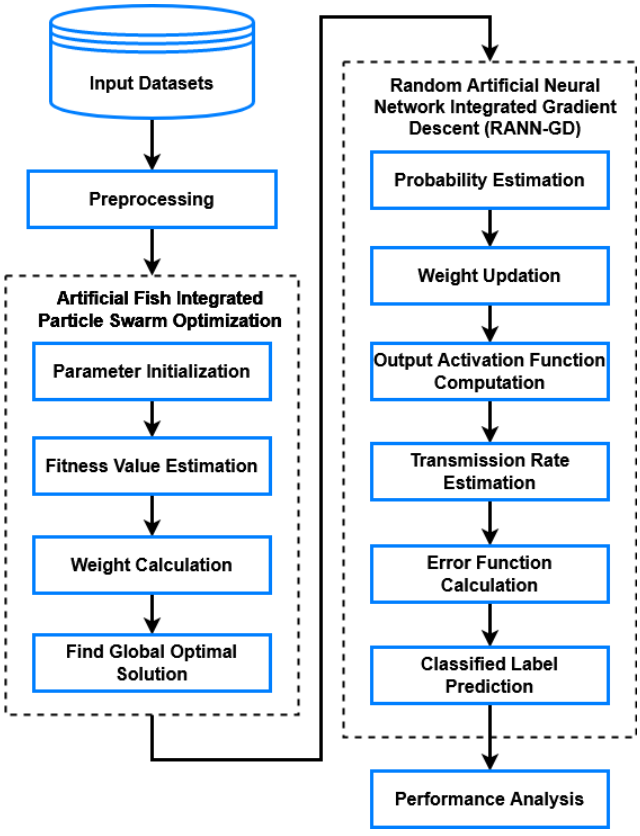

Fig 2. Working flow of the proposed methodology

3.1 Dataset Preprocessing

At first, the popular IDS datasets such as NSL-KDD, UNSW-NB15, and WSN-DS are considered as the inputs for processing. Typically, the raw datasets have some missing attributes, random values, and irrelevant information, which affects the performance of attack detection and classification. Hence, it must be preprocessed before using it for further operations, because the overall performance of IDS framework is highly depends in the input datasets. During this processing, the data normalization, filling the missing values, eliminating the unwanted information, and random values removal have been performed. Also, the min-max normalization is applied for avoiding the loss of information or features. The main advantage of using this technique is, it efficiently improves the performance of classification with reduced information loss and increased accuracy. Here, the minimum and maximum values are calculated for the given dataset as shown in below:

$$\mathrm{DS}_{\mathrm{h}}^{*}=\frac{\mathrm{r_h}-\mathrm{Min_h}}{\mathrm{Max_h}-\mathrm{Min_h}} \tag{1}$$

Where, $\mathrm{DS}_{\mathrm{h}}^{*}$ indicates the normalized dataset having h number of features, $\mathrm{r_h}$ is the original data of h dimensional features, $\mathrm{Max_h}$ and $\mathrm{Min_h}$ denotes the minimum and maximum values of h dimensional features respectively. This normalized dataset can be used for further attack detection and classification operations.

3.2 Artificial Fish Integrated Particle Swarm Optimization (AFIPSO) based Feature Selection

After preprocessing the dataset, the most optimal number of features are selected by using the AFIPSO technique. Typically, the increased dimensionality of dataset features can affect the performance of classifier with increased time consumption and reduced speed of processing. Hence, the feature selection or optimization is considered as one of the most essential process of any prediction/classification frameworks. So, the proposed work intends to implement an efficient and advanced optimization methodology for selecting the most suited features according to the identified global optimal solution. Here, the AFIPSO technique is developed by integrating the functionalities of two different optimization techniques such as Fish Swarm Optimization (FSO) and Particle Swarm Optimization (PSO). Normally, these are the kind of meta-heuristic optimization techniques and extensively utilized in many application systems for solving the multi-objective optimization problems. Due to its increased convergence rate, speed of processing, and efficient solution, the proposed work objects to incorporate these two methodologies for developing an accurate IDS framework. In this system, the parameters of PSO could be optimized by using the FSO for identifying the optimal particles.

In this technique, the parameters such as $\mathrm{s_i^x}, \mathrm{s_i^{x+1}}$ are considered as the integers ranging from minimum to maximum values. Here, the fitness function is computed by using the following model:

$$Fit_V=(1-w1-w2-w3-w4-w5)\times E_R+w1\times \frac{N_L}{maxdim}+w2\times\frac{sum\,(s_i)}{N_L\times max_n}+w3\times FP_R+w4\times FN_R+w5\times D_R \tag{2}$$

Where, $w1, w2, w3, w4$ and $w5\in[0,1]$ indicates the weight values, E_R is the error value, N_L denotes the number of hidden layers, max_n defines the maximum number of neurons, and $sum\,(s_i)$ denotes the total number of layers in the network model that is estimated as follows:

$$sum\,(s_i)=\sum_{j=1}^{n}N(hid_{ij}) \tag{3}$$

Consequently, the position and speed of optimization have been computed by using the following models:

$$MS_{ij}^{x+1}=we_i\times MS_{ij}^{x}+L_1\times ran_{i1}\times\left(pb_{ij}^{x}-s_{ij}^{x}\right)+L_2\times ran_{i2}\times\left(gb_{j}^{x}-s_{j}^{x}\right) \tag{4}$$

$$s_{ij}^{x+1}=s_{ij}^{x}+MS_{ij}^{x+1} \tag{5}$$

Where, x indicates the number of iterations ranging from i = 1, 2, 3… p (p indicates the number of all particles), j = 1, 2, 3 … d (d indicates the total number of dimensions), ran_{i1} and ran_{i2} are the random numbers lies between the range of 0 and 1, pb_{ij}^{x} is the optimal position of i[th] particle and j[th] dimension, gb_j^x defines the global optimal position of swarm, L_1, L_2 are the learning factors, and MS_{ij}^{x} denotes the moving speed of i[th] particle with x[th] iteration. According to the convex function, the inertial weight value is estimated with respect to the number of iterations as shown in below:

$$we_i=(we_{max}-we_{min})\times\left(1-\frac{itr}{max_{itr}}\right)^3+we_{min} \tag{6}$$

Where, we_{max} and we_{min} denotes the minimum and maximum weight values respectively, and max_{itr} indicates the maximum number of iterations. After that, the particles can learn themselves, where the learning factor L1 can decrease and L2 can get increase according to the exploration of particles. Finally, the learning factors are updated with respect to the iteration and maximum number iterations as shown in below:

$$L1=Con_1-Con_2\times\left(\frac{itr}{max_{itr}}\right) \tag{7}$$

$$L2=Con_2+Con_1\times\left(\frac{itr}{max_{itr}}\right) \tag{8}$$

Where, Con_1 and Con_2 indicates the constant values, and $Con_1 > Con_2$. Subsequently, the global best optimization of particles is estimated as follows:

$$s_i^{x+1}=s_i^{x}+(s_j-s_i^{x})\times ran \tag{9}$$

Where, ran indicates the random function that generates the random values from 0 to 1 and is updated as shown in below:

$$s_k=s_i^{x}+2\times(ran-0.5).Vis \tag{10}$$

Where, Vis indicates field of vision of fish that is computed as follows:

$$s_i^{x+1}=s_i^{x}+2\times(ran-0.5)\times St_{fish}\times(s_k-s_k^{x}) \tag{11}$$

Where, St_{fish} denotes the step size of fish as shown in below:

$$s_i^{x+1}=s_i^{x}+2\times(ran-0.5)\times St_{fish} \tag{12}$$

Based on the updated value, the global best optimal solution is calculated by using the AFIPSO mechanism, and the obtained solution can be used to select the optimal number of features for classification. In this model, the main reason of using this optimization technique is to reduce the dimensionality of

features, because the high number of features can increase the complexity of data training. Hence, the proposed system objects to select the optimal number of features for improving the performance of intrusion detection and classification.

3.3 Random Artificial Neural Network Integrated Gradient Descent (RANN-GD) Classification

After selecting the optimal number of features, the RANN-GD classification approach is applied to accurately classify the intrusions from the preprocessed datasets. The RANN-GD is a kind of machine learning based classification technique, which is developed based on the integration of Artificial Neural Network (ANN) and Gradient Descent Boost (GDB) classification techniques. Here, the main purpose of using this technique is to predict the intrusions from the IDS datasets with reduced error rate, false positives, and computational complexity. The key benefits of using the proposed RANN-GD classifier are as follows:

- Distributed operating nature
- Ability to handle large size data with reduced computational operations
- Increased accuracy and detection performance
- Minimal computational time
- Better predictive results due to the probability and non-negativity constraints

According to the potentiality of received data, the exhibition and inhibition states of neurons exist in the different layers have been determined. If it's a positive value, it can proceed with the exhibition state; otherwise, it can goes to the inhibition state. Based on the received data, the positive or negative data is determined with the probabilities of $pro^{+}(a,b)$ and $pro^{-}(a,b)$, and its probability function is estimated as shown in below:

$$p(a) + \sum_{b=1}^{N} pro^{+}(a,b) + pro^{-}(a,b) = 1, \ \forall_a \quad (13)$$

Subsequently, the weight values are updated as shown in below:

$$we^{+}(a,b) = trs_a pro^{+} + (a,b) \geq 0 \quad (14)$$

$$we^{-}(a,b) = trs_a pro^{-} + (a,b) \geq 0 \quad (15)$$

Similar to that, the probability of data is computed by using the poisson distribution function. Hence, the positive and negative values of neuron is determined by using the Poisson rate $\Lambda(a)$ and $\Gamma(a)$ correspondingly. Then, these values are mathematically represented as shown in below:

$$\lambda^{+}(b) = \sum_{b=1}^{n} e(b) ran(b) pro^{+}(b,a) + \Lambda(i) \quad (16)$$

$$\lambda^{-}(b) = \sum_{b=1}^{n} e(b) ran(b) pro^{-}(b,a) + \Lambda(i) \quad (17)$$

Based on the probability values, the transmission rate is estimated by using the following equation:

$$e(a) = \frac{\lambda^{+}(b)}{pro(a) + \lambda^{-}(a)} \quad (18)$$

Moreover, the probability of transmission rate is computed as follows:

$$pro(a) = (1 - k(a))^{-}1 \sum_{b=1}^{N} [we^{+}(a,b) + we^{-}(a,b)] \quad (19)$$

Then, the weight of positive and negative values are updated as shown in below:

$$we(i) = \sum_{b=1}^{N} [we^{+}(a,b) + we^{-}(a,b)] \quad (20)$$

Here, the overall MSE of classification is reduced by computing the local minima with the help of GD model as shown in below:

$$Err_P = \frac{1}{2} \sum_{a=1}^{n} \beta_i (pr1_b^{op} - pr2_b^{op})^2 \ \ \beta_i \geq 0 \quad (21)$$

Where, the β_i indicates the output state of neuron that lies in the range of (0, 1), $pr1_b^{op}$ and $pr2_b^{op}$ are the predicted output values. After the training the neurons q and r, the weight values of $we^{+}(q,r)$ and $we^{-}(q,r)$ are estimated by using the following equations:

$$we_{q,r}^{+x} = we_{q,r}^{+(x-1)} - \eta \sum_{i=1}^{n} \beta_i (pr1_b^{op} - pr2_b^{op}) \left[\frac{\partial pr1_a}{\partial we_{q,r}^{+}}\right]^{x-1} \quad (22)$$

Similar to that, the negative weight value is updated as shown in below:

$$we_{q,r}^{-x} = we_{q,r}^{-(x-1)} - \eta \sum_{i=1}^{n} \beta_i (pr1_b^{op} - pr2_b^{op}) \left[\frac{\partial pr1_a}{\partial we_{q,r}^{-}}\right]^{x-1} \quad (23)$$

According to this weight value, the RANN-GD model can predict the accurate classified label with reduced error value and increased accuracy.

4. Results and Discussion

This section discusses about the simulation results and comparative analysis of both conventional and proposed methodologies by using various evaluation measures. In order to prove the effectiveness and superiority of the proposed model, some of the recent state-of-the-art IDS models have been considered for comparative analysis. During validation, the measures such as accuracy, precision, recall, f-measure, False Acceptance Rate (FAR), Area under Curve (AUC), True Positive Rate (TPR), and False Positive Rate (FPR) have been considered. For assessing the performance, there are different and popular IDS datasets such as NSL-KDD, UNSW-NB 15, and WSN-DS have been considered. The simulation setup of the proposed network environment is shown in Table 1.

Table 1. Simulation setup

Parameters	Specifications
Simulation time	1000 s
Total number of nodes	100
Number of attackers	10
Field size	1000 m × 1000 m
Routing protocol	AODV
MAC	IEEE 802.11
Mobility model	RWP
Speed of moving	10 m/s

Fig 3 and Table 2 compares the conventional [28] and proposed intrusion detection and classification methodologies based on the measures of accuracy, precision, recall, and f-score for the NSL-KDD dataset. Normally, the overall efficiency and detection performance of IDS methodologies are highly depends on the measures of accuracy, precision, recall and f-measure. Then, these parameters are increasingly utilized in many applications

for validating the effectiveness of classifier, which are calculated as follows:

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \quad (24)$$

$$Precision = \frac{TP}{FP+TP} \quad (25)$$

$$Recall = \frac{TP}{FN+TP} \quad (26)$$

$$F1-measure = 2 * \frac{Precision \times Recall}{Precision+Recall} \quad (27)$$

Where, TP – True Positives, TN – True Negative, FP – False Positive, and FN – False Negative. According to this evaluation, it is observed that the proposed AFIPSO integrated with RANN-GD technique outperforms the other models with increased values of accuracy, precision, recall, and f-score.

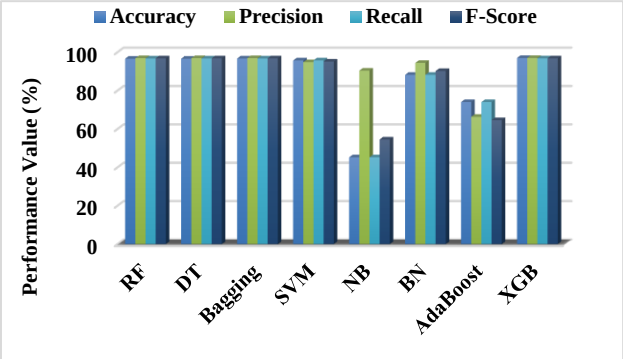

Fig 3. Comparative analysis between conventional and proposed intrusion detection techniques using NSL-KDD dataset

Table 2. Comparative analysis for NSL-KDD

Techniques	Accuracy	Precision	Recall	F-Score
RF	96.6	96.9	96.7	96.8
DT	96.6	96.9	96.7	96.8
Bagging	96.7	96.9	96.7	96.8
SVM	95.7	94.8	95.7	95.1
NB	45.2	90.4	45.2	54.5
BN	88.2	94.4	88.2	90.2
AdaBoost	74	66.3	74	64.6
XGB	97	97	96.8	96.8

Fig 4 and Table 3 compares the TPR, FPR, MCC, and AUC of existing and proposed intrusion detection methodologies by using the NSL-KDD dataset. The measures are computed as follows:

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (28)$$

$$FPR = \frac{FN}{FN+TN} \quad (29)$$

$$TPR = \frac{TP}{TP+FN} \quad (30)$$

Moreover, these parameters are mainly evaluated for validating that how the proposed detection approach could accurately detects the attacks from the given dataset. Based on these results, it is evident that the proposed AFIPSO integrated RANN-GD technique outperforms the other techniques with improved results.

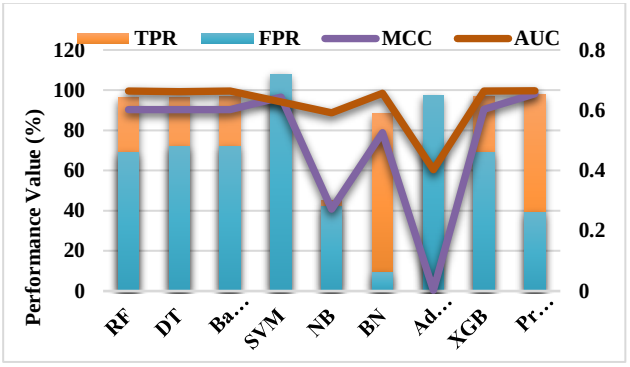

Fig 4. Detection efficiency analysis using NSL-KDD dataset

Table 3. Analysis based on TPR, FPR, MCC, and AUC for NSL-KDD dataset

Techniques	TPR	FPR	MCC	AUC
RF	96.6	0.46	90.3	99.5
DT	96.6	0.48	90.3	99.3
Bagging	96.7	0.48	90.4	99.5
SVM	95.7	0.72	96.5	94.2
NB	45.2	0.28	40.7	88.8
BN	88.2	0.06	78.9	98.5
AdaBoost	74	0.65	38	60.4
XGB	97	0.46	90.5	99.6
Proposed	98	0.26	98.2	99.7

Fig 5 and Table 4 compares the values of precision, recall, FAR, f-measure, and AUC of both existing [13] and proposed intrusion detection methodologies by using the NSL-KDD dataset. For validating the results, some of the most widely used machine learning classifiers have been considered for comparison. The obtained results indicate that the proposed technique provides an improved performance outcomes, when compared to the other techniques. Because, in the proposed scheme, the dataset training has been performed by using the optimal number of extracted features, which helps to improve the accuracy of classification with reduced time consumption.

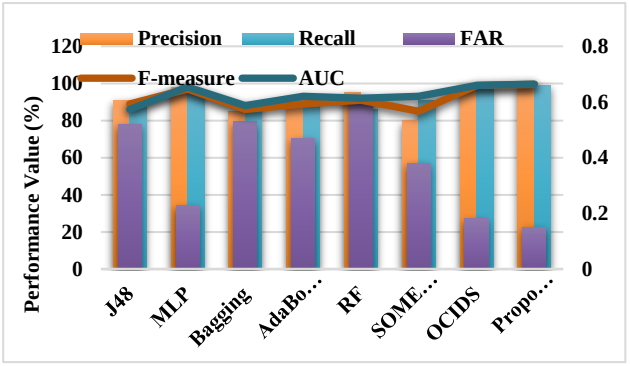

Fig 5. Overall performance evaluation for existing and proposed classification approaches using NSL-KDD dataset

Table 4. Comparative analysis based on precision, recall, f-measure and AUC for NSL-KDD dataset

Techniques	Precision	Recall	FAR	F-measure	AUC
J48	91	89	0.52	89	86
MLP	98	97	0.23	97	98
Bagging	85	88	0.53	86	88
AdaBoost	89	90	0.47	89	93
RF	95	86	0.62	91	92

SOMET + RF	80	91	0.38	85	93
OCIDS	99	98	0.18	99	99
Proposed	99.3	99	0.15	99.5	99.6

Fig 6 (a & b), and Table 5 compares the DR and FAR of both existing and proposed classification techniques with respect to different types of attacks in the NSL-KDD dataset. For this assessment, the attacks such DoS, Probe, U2R, and U2L have been considered. Normally, the DR and FAR measures are mainly calculated for validating the overall detection efficiency of IDS frameworks. These results also indicate the proposed AFIPSO-RANN-GD technique provides an improved results over the other mechanisms.

Table 5. Detection rate and false acceptance rate with different types of attacks in NSL-KDD dataset

Techniques	DoS		Prob		U2R		U2L	
	DR	FAR	DR	FAR	DR	FAR	DR	FAR
ACO	91.7	5.9	87.9	6.8	62.4	39.6	93.9	7.42
BP	89.3	6.4	85.6	9.2	56.6	48.3	93.7	9.8
OCIDS	97.9	1.9	96.8	4.7	82.3	17.6	98.4	6.1

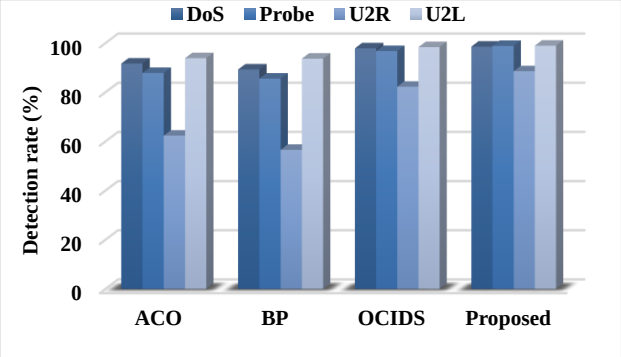

Fig 6 (a). Detection rate with respect to varying types of attacks in NSL-KDD dataset

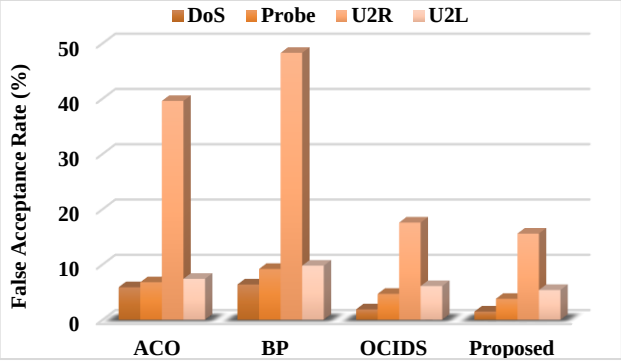

Fig 6 (b). False acceptance rate with respect to varying types of attacks in NSL-KDD dataset

Table 6 and Fig 7 estimates the accuracy, Mean F1-Measure (MFM), Attack Detection Rate (ADR), and FAR for both existing [29] and proposed intrusion detection and classification methods using the UNSW-NB 15 dataset. These measures are also mainly used for testing the effectiveness of attack detection methodologies. According to the obtained results, it is observed that the proposed AFIPSO-RANN-GD technique provides an improved performance results, when compared to the other techniques. Due to the proper selection of features and training of data model, the performance of the proposed IDS is higher than the other methodologies.

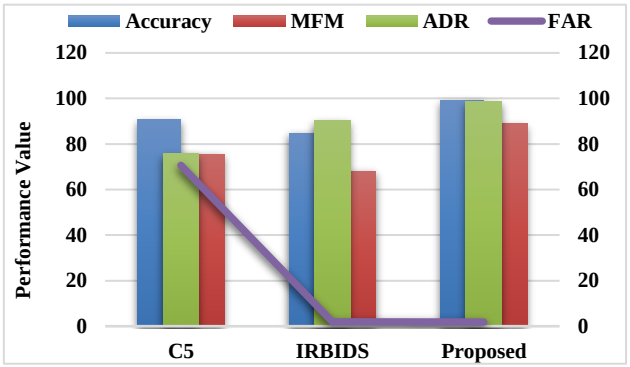

Fig 7. Comparative analysis between existing and proposed classification techniques using UNSW-NB15 dataset

Table 6. Performance analysis using UNSW-NB15 dataset

Techniques	Accuracy	MFM	ADR	FAR
C5	90.74	75.54	75.8	70.65
IRBIDS	84.83	68.13	90.32	2.01
Proposed	99.3	88.9	98.5	1.86

Fig 8 and Table 7 compares the accuracy, error rate, precision, recall, and f1-score of both existing [30] and proposed classification techniques by using the WSN-DS dataset. Typically, the reduced value of error rate indicates the efficient performance of the proposed scheme. The obtained values show that the proposed AFIPSO-RANN-GD technique provides the better performance results over the other techniques with increased accuracy, precision, recall, f-measure and reduced error rate.

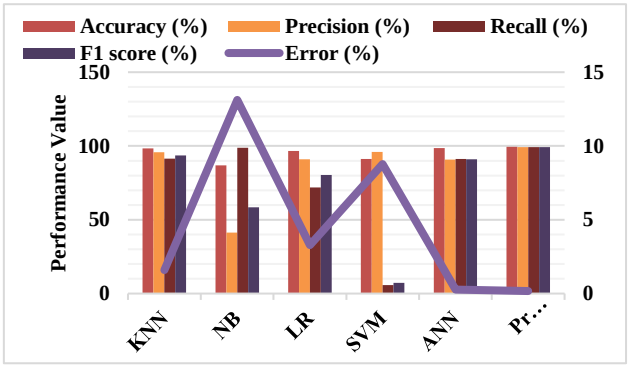

Fig 8. Comparative analysis between existing and proposed classification techniques using WSN-DS dataset

Table 7. Performance evaluation of existing and proposed classification techniques using WSN-DS dataset

Algorithms	Accuracy (%)	Error (%)	Precision (%)	Recall (%)	F1 score (%)
KNN	98.4	1.6	95.69	91.50	93.55
NB	86.88	13.12	41.39	98.87	58.35
LR	96.72	3.28	90.99	71.81	80.28
SVM	91.22	8.78	95.95	5.78	7.16
ANN	98.56	0.27	90.66	91.24	90.95
Proposed	99.5	0.17	99.3	99.2	99.2

5. CONCLUSION

This paper presents an advanced and new IDS framework for accurately detecting and classifying the intrusions from the popular IDS datasets. The key contribution of this work is to implement an intelligent optimization based classification methodology for designing an IDS framework with reduced computational complexity and increased detection efficiency. For this purpose, an AFIPSO integrated with RANN-GD mechanism is employed, which helps to exactly spot the intrusions from the different IDS datasets. Here, the NSL-KDD, UNSW-NB 15 and WSN-DS based IDS datasets have been utilized for implementing and validating the proposed IDS framework. Initially, the dataset preprocessing is performed for normalizing the attributes based on the min-max normalization. Then, the set of optimal features have been extracted from the preprocessed dataset based on the global best optimal solution provided by the AFIPSO technique. It is a kind of optimization technique and developed based on the integration of two different optimization mechanisms. In this system, the parameters of PSO could be optimized by using the FSO for identifying the optimal particles. After selecting the optimal number of features, the RANN-GD classification approach is applied to accurately classify the intrusions from the preprocessed datasets. Here, the main purpose of using this technique is to predict the intrusions from the IDS datasets with reduced error rate, false positives, and computational complexity. During validation, the performance of the proposed AFIPSO-RANN-GD technique is evaluated by using various measures, and the obtained results are compared with the some of the recent state-of-the-art IDS techniques. According to the comparison, it is identified that the proposed technique outperforms the other techniques with improved performance outcomes.

Conflict of Interest

All authors, there is no Conflict of Interest to publish this article in your Journal.

References

[1] Liu, G., Zhao, H., Fan, F., Liu, G., Xu, Q., & Nazir, S. (2022). An enhanced intrusion detection model based on improved kNN in WSNs. Sensors, 22(4), 1407. https://doi.org/10.3390/s22041407

[2] Maheswari, M., & Karthika, R. A. (2021). A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks. Wireless Personal Communications, 118(2), 1535–1557. https://doi.org/10.1007/s11277-021-08101-2

[3] Roy, R., and D. A. . Kalotra. “Vehicle Tracking System Using Technological Support for Effective Management in Public Transportation”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 2, Mar. 2022, pp. 11-20, doi:10.17762/ijritcc.v10i2.5515.

[4] Singh, A., Amutha, J., Nagar, J., Sharma, S., & Lee, C. C. (2022). LT-FS-ID: Log-transformed feature learning and feature-scaling-based machine learning algorithms to predict the k-barriers for intrusion detection using wireless sensor network. Sensors, 22(3), 1070. https://doi.org/10.3390/s22031070

[5] Wen, W., Shang, C., Dong, Z., Keh, H. C., & Roy, D. S. (2021). An intrusion detection model using improved convolutional deep belief networks for wireless sensor networks. International Journal of Ad Hoc and Ubiquitous Computing, 36(1), 20–31. https://doi.org/ 10.1504/IJAHUC.2021.112980

[6] Jin, J. (2021). Intrusion detection algorithm and simulation of wireless sensor network under Internet environment. Journal of Sensors, 2021, 1–10. https://doi.org/10.1155/2021/9089370

[7] Rui-Hong, D., Hou-hua, Y., Qiu-yu, Z., & Xue-yong, L. (2020). Distributed WSN intrusion detection model based on deep forest algorithm. Journal of Lanzhou University of Technology, 46(4), 103.

[8] Chawla, A. (2022). Phishing website analysis and detection using Machine Learning. International Journal of Intelligent Systems and Applications in Engineering, 10(1), 10–16. https://doi.org/10.18201/ijisae.2022.262

[9] Singh, V., Poonia, R. C., Raja, L., Sharma, G., Trivedi, N. K., & Mathur, G. N. (2020). Redundancy management and host intrusion detection in WSN. Advances in Wireless Technologies and Telecommunication. IGI Global, 153–167. https://doi.org/10.4018 /978-1-5225-9554-0.ch006

[10] Almomani, I., & Alromi, A. (2020). Integrating software engineering processes in the development of efficient intrusion detection systems in wireless sensor networks. Sensors, 20(5), 1375. https://doi.org/ 10.3390/s20051375

[11] Punithavathi, R., Thanga Selvi, R., Latha, R., Kadiravan, G., Srikanth, V., & Kumar Shukla, N. (2022). Robust node localization with intrusion detection for wireless sensor networks. Intelligent Automation and Soft Computing, 33(1), 143–156. https://doi.org/10.32604/iasc.2022.023344

[12] Lu, X., Han, D., Duan, L., & Tian, Q. (2020). Intrusion detection of wireless sensor networks based on IPSO algorithm and BP neural network. International Journal of Computational Science and Engineering, 22(2/3), 221–232. https://doi.org/10.1504/IJCSE. 2020. 107344

[13] Yadav, A., & Kumar, A. (2022). Intrusion detection and prevention using RNN in WSN. Lecture Notes in Networks and Systems. Springer, 531–539. https://doi.org/10.1007/978-981-16-6723-7_40

[14] Belavagi, M. C., & Muniyal, B. (2021). Improved intrusion detection system using quantal response equilibrium-based game model and rule-based classification. International Journal of Communication Networks and Information Security, 13(1), 1–8.

[15] Elsaid, S. A., & Albatati, N. S. (2020). An optimized collaborative intrusion detection system for wireless sensor networks. Soft Computing, 24(16), 12553–12567. https://doi.org/10.1007/s00500-020-04695-0

[16] Narasimhan, H., R, V., & Mohammad, N. (2021). Unsupervised deep learning approach for in-vehicle intrusion detection system. IEEE Consumer Electronics Magazine, 1–1. https://doi.org/10.1109/MCE. 2021.3116923

[17] Agarwal, D. A. . (2022). Advancing Privacy and Security of Internet of Things to Find Integrated Solutions. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 05–08. https://doi.org/10.17762/ijfrcsce.v8i2.2067

[18] Kagade, R. B., & Jayagopalan, S. (2022). Optimization assisted deep learning based intrusion detection system in wireless sensor network with two-tier trust evaluation. International Journal of Network Management, e2196. https://doi.org/10.1002/nem.2196

[19] Kavousi-Fard, A., Su, W., & Jin, T. (2020). A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids. IEEE Transactions on Industrial Informatics, 17(1), 650–658. https://doi.org/10.1109/TII.2020.2964704

[20] Ahmad, B., Jian, W., Ali, Z. A., Tanvir, S., & Khan, M. S. A. (2019). Hybrid anomaly detection by using clustering for wireless sensor network. Wireless Personal Communications, 106(4), 1841–1853. https://doi.org/10.1007/s11277-018-5721-6

[21] Baig, Z. A., Sanguanpong, S., Firdous, S. N., Vo, V. N., Nguyen, T. G., & So-In, C. (2020). Averaged dependence estimators for DoS attack detection in IoT networks. Future Generation Computer Systems, 102, 198–209. https://doi.org/10.1016/j.future.2019.08.007

[22] Nancy, P., Muthurajkumar, S., Ganapathy, S., Santhosh Kumar, S. V. N., Selvi, M., & Arputharaj, K. (2020). Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks. IET Communications, 14(5), 888–895. https://doi.org/10.1049/iet-com.2019.0172

[23] Ahmed Cherif Megri, Sameer Hamoush, Ismail Zayd Megri, Yao Yu. (2021). Advanced Manufacturing Online STEM Education Pipeline for Early-College and High School Students. Journal of Online Engineering Education, 12(2), 01–06. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/47

[24] Premkumar, M., & Sundararajan, T. V. P. (2020). DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. Microprocessors and Microsystems, 79, 103278. https://doi.org/10.1016/j.micpro.2020.103278

[25] Tan, X., Su, S., Huang, Z., Guo, X., Zuo, Z., Sun, X., & Li, L. (2019). Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm. Sensors, 19(1), 203. https://doi.org/10.3390/s19010203

[26] Lima Filho, F. S. d., Silveira, F. A. F., de Medeiros Brito Junior, A., Vargas-Solar, G., & Silveira, L. F. (2019). Smart detection: An online approach for DoS/DDoS attack detection using machine learning. Security and Communication Networks, 2019, 1–15. https://doi.org/10.1155/2019/1574749

[27] Otoum, S., Kantarci, B., & Mouftah, H. T. (2019). On the feasibility of deep learning in sensor network intrusion detection. IEEE Networking Letters, 1(2), 68–71. https://doi.org/10.1109/LNET.2019. 2901792

[28] Wazid, M., Reshma Dsouza, P., Das, A. K., Bhat K, V., Kumar, N., & Rodrigues, J. J. P. C. (2019) RAD-EI: A routing attack detection scheme for edge-based Internet of Things environment. International Journal of Communication Systems, 32(15), e4024. https://doi.org/10.1002/dac.4024

[29] Hongsong, C., Caixia, M., Zhongchuan, F., & Lee, C.-H. (2020). Novel LDoS attack detection by Spark-assisted correlation analysis approach in wireless sensor network. IET Information Security, 14(4), 452–458. https://doi.org/10.1049/iet-ifs.2018.5512

[30] Tamilarasi, N., & Santhi, S. G. (2020). Detection of wormhole attack and secure path selection in wireless sensor network. Wireless Personal Communications, 114(1), 329–345. https://doi.org/10.1007/ s11277-020-07365-4

[31] Jiang, S., Zhao, J., & Xu, X. (2020). SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments. IEEE Access, 8, 169548–169558. https://doi.org/10.1109/ACCESS. 2020.3024219

[32] Liu, J., Kantarci, B., & Adams, C. Machine learning-driven intrusion detection for Contiki-NG-based IoT networks exposed to NSL-KDD dataset pp. 25–30.

[33] Kumar, V., Sinha, D., Das, A. K., Pandey, S. C., & Goswami, R. T. (2020). An integrated rule based intrusion detection system: Analysis on UNSW-NB15 data set and the real time online dataset. Cluster Computing, 23(2), 1397–1418. https://doi.org/10.1007/s10586-019-03008-x

[34] Rezvi, M. A., Moontaha, S., Trisha, K. A., Cynthia, S. T., & Ripon, S. (2021). 'Data mining approach to analyzing intrusion detection of wireless sensor network,' Indonesian J. Electric. Eng. Computer Science, 21(1), 516–523.

[35] Gopalakrishnan, S., & Kumar, P. M. (2016). Performance analysis of malicious node detection and elimination using clustering approach on MANET. Circuits and Systems, 07(6), 748–758. https://doi.org/ 10.4236/cs.2016.76064

[36] Subburayalu, G., Duraivelu, H., Raveendran, A. P., Arunachalam, R., Kongara, D., & Thangavel, C. (2021). Cluster based malicious node detection system for mobile ad-hoc network using ANFIS classifier. Journal of Applied Security Research, 1–19. https://doi.org/10.1080/19361610.2021. 2002118