An Intrusion Detection System in Computer Networks using the Firefly Algorithm and the Fast Learning Network

Samira Rajabi*, Shahram Jamali
Department of Computer Engineering
University of Mohaghegh Ardabili
Ardabil, Iran
Samira_61R@yahoo.com, jamali@uma.ac.ir

Javad Javidan
Department of Computer Engineering
University of Mohaghegh Ardabili
Ardabil, Iran
javidan@uma.ac.ir

Received: 2020/04/18 Revised: 2020/09/20 Accepted: 2020/09/30

Abstract*—Due to the extensive use of communication networks and the ease of communicating via wireless networks, these types of networks are increasingly considered. Usability in any environment without the need for monitoring and environmental engineering of these networks has been caused increasing use of it in various fields. It also caused the emergence of security problems in the sending and receiving information that intrusion detection has been raised as the most important issue. Hence, Network intrusion detection system (NIDS) is the process of identifying malicious activity in a network by analyzing the network traffic behavior. A wireless sensor network is composed of sensors that are responsible for collecting information from the environment. These wireless networks, because of the limitation of resources, mobility, and critical tasks, are relatively high vulnerabilities in comparison to other networks. Therefore, forecasting and intrusion detection systems play an important role in providing security in wireless sensor networks that can involve a wide range of attacks. Traffic behavior in the network has many features and dimensions, so dimensionality reduction plays a vital role in IDS, since detecting anomalies from high-dimensional network traffic features is a time-consuming process. Feature selection influences the speed of the analysis and detection. For this purpose, in the current study, a new approach is proposed to predict the intrusion of wireless networks using firefly based feature selection and fast learning network. Selected features in the feature selection phase are used as inputs to the fast learning network to analyze the intrusion of the network in real-time. According to the simulation results, it can be said that the fast neural network method continues training so as to avoid overfitting error. While neural networks further learn training set features until the training process is completed. Thus, the occurrence of overfitting phenomenon in neural networks is common. Therefore, the proposed method grants better performance than the neural network method in predicting new attacks on the network.

Keywords*— *Network Intrusion Detection System, Feature Subset Selection, Firefly Optimization Algorithm, Fast Learning Neural Network.

1. INTRODUCTION

Computer networks are composed of a set of mobile hosts that are connected to each other via wireless links. Each node not only could act as a final system but could also able to send packets as a router [1]. When a source node intends to transfer information to a destination node, packets are transferred between intermediate nodes, so it is critical to search and creates a path from the source to the destination node for mobile networks [2]. Due to the nodes replacement, the mobile computer network topology may change intermittently, so with this technology, the nodes can easily change their location with local neighbors [3-5]. In the case of wireless networks, security issues, and attack prevention are much more difficult, and this problem is many times greater in mobile computer networks [6, 7].

The intrusion of malicious nodes among the network can lead to distortion or destruction all or part of the transmitted information packets. As a result, the efficiency of the whole system is threatened and may be interpreted differently [8-10]. Therefore, preventing and detecting intrusions and attacks on computer networks has become a crucial and serious challenge. Therefore, the Intrusion Detection System (IDS) plays an important role in wireless network protection and covers a wide range of attacks [11].

The IDS tried to specify whether probed user behavior or network traffic is malicious. If a malicious activity is defined, an alarm would be concluded. Several methods are introduced for IDSs' to detect an attack, such as anomaly detection or signatures recognition, also points out that the performance of IDS depends upon these techniques. One of the main factors that affect the efficiency of the IDS is the quality of the feature extraction and feature selection algorithm. In order to increase the detection rate of the IDS, a drop in the number of applicable traffic features without any negative effects on classification accuracy is needed.

In this paper, a network intrusion detection system based on the combination of Firefly Algorithm (FA) feature selection based selection and Fast Learning Neural Network (FLN) is presented. The proposed method has used the KDD Cup dataset [16] to patterns recognition of network intrusion and the test dataset prepared from this dataset, for evaluation intended purpose. Due to the variety and volume of user activity features and network's traffic, it seems necessary to select a subset of features in order to increase the classification accuracy, remove unrelated attributes and reduce the data dimension and executive and spatial complexity of the system. In addition, the feature selection can detect the implicit dependence between the data and the class label to easily predict test samples that will be added to the model in the future. So, in the proposed method, the approach of features selecting based on FA

algorithm has been adopted in order to determine the important and the related features of the class label. The remaining features of this step, which resulted in the output of the FA, are considered as the input of the fast learning network to classify the training samples accurately and predict the label of the test samples.

The rest of the paper organizes as following. In section 2 will review some of the intrusion detection systems in computer networks. In Section 3, the details of the proposed method will be presented. In Section 4, we will model and evaluate the performance of the proposed method. Finally, in Section 5, the conclusion of the paper and future work will be expressed.

2. Related Works

The high-speed services requirement in network for businesses and other services is a fundamental factor of network. IDSs are an important tool for network protection that examine and analyze the entrance pathways of nodes in connections and decide whether these pathways to the system contain an attack. If the IDS detects an attack, it announces the alert. Traditionally, IDSs use deep inspection of packets or analysis statistical protocols to detect attacks in network traffic. Deep inspection is not possible when network traffic is encrypted. A complete inspection of computer components also leads to cost and a big problem in high-speed networks. Complete analysis of protocols is considered to determine the characteristics and scope of each intrusion. Protocol decomposition and analysis techniques can also have a computational cost [11].

In [7] an extended learning model for Fast Learning Network (FLN) based on particle swarm optimization (PSO), called PSO-FLN, was proposed. This method was adopted to solve the intrusion detection issue and implemented on the KDD99 dataset. This method was compared via large number of meta-heuristic algorithms for training and classification accuracy. In [17] a hybrid method based on combination of filter and wrapper based feature selection was used to network intrusion detection. The main idea of this paper is to reduce the number of features and increase the output of detection rate. This method has focuses on FA based feature selection and C4.5 classifier in comparison on Bayesian network method. In [15] a hybrid method based on combination of a multilayer perceptron network and artificial bee colony and fuzzy clustering algorithms has been introduced. This method has divided network traffic to two types of packets by the MLP, normal and abnormal so that the core of multilayer perceptron network training has applied by the artificial bee colony algorithm through optimizing the values of weights and biases in layers. In [19] a near optimal method to detect anomaly in the network has proposed using back propagation neural network that employed a novel architecture for that network. This method, for the first time, builds all possible combinations of related features of the parameters in the classification that affect performance in anomaly detection, data normalization, and network activation function. In [20] the lazy learning methods have been used to improve overall IDS performance. In this method heuristic weight-based indexing method has been used to overcome the curse of search space that is inherent in lazy learning. IBk and LWL are two popular lazy learning algorithms that have been applied to the NSL-KDD dataset to simulate a real-world scenario and compare its relative performance with hw-IBk. In [21], in order to prevent network attacks, a machine learning algorithm has been proposed to achieve better accuracy and faster detection Convergence. The use of machine learning is another major advantage in that advanced knowledge is not required as much as the black and white list model. Extreme Learning Machines (ELMs) are single-layer artificial neural networks that do not require iterative training. Therefore, their learning speed is high, and speed is very important in the success of network intrusion detection systems, and they defend a quick and effective response. In [22] a fuzzy based semi-supervised learning method has been presented to improve the classification rate for the IDSs. A feed-forward neural network has utilized to training feature vector and the instance division on unlabeled data by using the fuzzy quantity. The classification method, after categorizing each category separately into the original training set, retrains on the data to improve the detection rate.

A. Maintaining the Integrity of the Specifications

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

3. Proposed Method

Wireless networks given to variable topology and lake of specific infrastructure, are constantly under attack by malicious nodes. Easy access to networks and the ability to quickly connect to other nodes make these types of networks exposed to attacks. These networks are often created without prior planning and require security for a short time. Because mobile ad hoc networks without infrastructure and don't use any equipment such as routers or switches for routing, the nodes themselves participate in routing. Each node can act as a router to send packets between the source and the destination. The presence of a malicious node in the network, not only could disrupt the process of sending and receiving information packets but could also lead to the destruction of the network [23, 24]. Therefore, in this research, a network intrusion detection system based on the combination of FA based feature selection and fast learning neural network has been proposed. In the rest of this chapter, we'll take a brief look at the features selection, Firefly Algorithm, neural networks, fast learning neural network, and description of the proposed method.

B. Data Pre-Processing

In recent years, a variety of classification models have been developed that perform a training process on data and able to classify and predict test data, which are unknown cases for the system. It's wealth to note, the data type used for each type of model is different. In fact, each model deals and classifies a specific type of data. In order to use the models and outperform the results of the model, it is necessary to prepare the data in a special model format. The process of preparing data for each model is called data pre-processing. Data pre-processing has

several steps. In this study, two examples of these pre-processing steps are needed, which are described as follows [25].

C. Feature Subset Selection

The pre-processing step used in this study is the feature subset selection that is directly related to the class label [25]. Given the KDD intrusion data set has 41 features that are distributed in three categories: Basic features of individual TCP connections, Content features within a connection suggested by domain knowledge, and Traffic features computed using a two-second time window. This large number of attributes can complicate the classification model. Therefore, some of these features which have an unbalanced distribution value and don't have much effect on determining the class label should be removed during the feature selection.

The aim of the feature selection is to remove unrelated and redundant features, so that not only has reduced the data dimension and system complexity, it also has possible to increase classification accuracy and convergence to the optimal solution and reduce the model's cost. In addition, feature selection can detect the implicit dependence between the data and the class label, so that the test samples can be easily categorized. In this study, unrelated features that naturally don't have much effect on the class label are removed to prevent the imposition of additional complexity on the proposed classification model [26].

D. Data Normalization

According to the selected subset of features in the previous section, it can be seen that the data distribution range in this subset of features varies. It is natural, if the values of the features are different, then the feature with the larger values domain will affect other features and will be more effective on the performance of the classification model. This effect can reduce classification accuracy and lead to an incorrect prediction of test samples. To solve this problem, data normalization is used in training and testing data set [27]. Data normalization maps values between zero and one, which eliminates the negative effect of features with higher values on outperforms. The most popular normalization methods in the literature are Gaussian and min-max normalization, which in this study, we use min-max normalization. The min-max normalization is shown as.(1) [28]:

$$MMN=(x_{i,j} - x_{min})/(x_{max} - x_{min})\, a + b = \gamma \qquad (1)$$

Where xi,j is the values of each feature for each instance, and xmin is the minimum value for a feature, and xmax is the maximum value of the feature.

E. Fast Learning Neural Network

The fast learning neural network is a parallel combination of a single learning feed-forward network and a 3 layered artificial neural network that include input, hidden and output layer. Actually, fast learning neural network is a Double Parallel Forward Neural Network (DPFNN) that is depicted in Fig.1 for using analysis of weights in neural network and utilizes the least square's evaluation criteria [29].

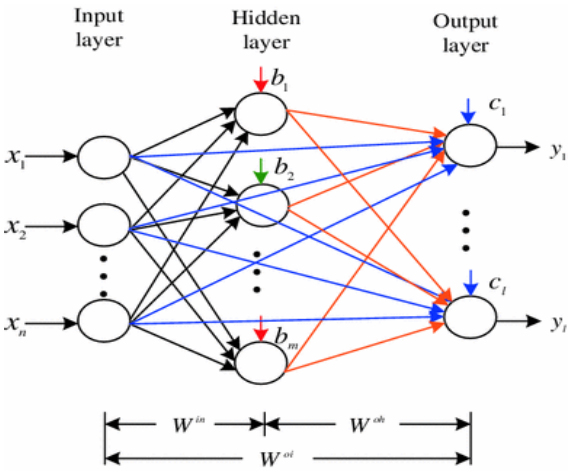

Fig. 1. Fast learning neural network structure [29]

As noted, the fast learning neural network is generally a DPFNN [16]. This describes a parallel connection of a multilayer FNN and a single-layer FNN. As mentioned, the recording external data from the hidden neurons, along with the weights and biases itself straightly from the input layer is forwarded to the output layers of the fast learning neural network.

As pointed, the fast learning neural network is similar to Extreme Learning Machine in aspect of non-optimal weights and biases, value distribution or assignment. As conclusion, the overall precision of the neural network will be descended unless an efficient method to choose the weights is utilized. A PSO-Based optimized the fast learning neural network is trained based on selecting weights using particle swarm optimization [29].

In this study, Firefly Algorithm (FA) has used as one of the new methods of artificial intelligence. This algorithm is inspired by the social behavior of firefly swarms. This method, like other intelligent optimization methods, begins with the initial population of instances. In this method, the two insects are compared together, the insect which is less attractive moves towards the more attractive insect. Finally, an insect has been chosen as the most attractive insect, which is the optimal answer to the problem.

Nature has been an inspiration to the introduction of many meta-heuristic algorithms. It has managed to find solutions to problems without being told but through experience. Natural selection and survival of the fittest was the main motivation behind the early metaheuristic algorithms, Evolutionary algorithms. Besides, most of the metaheuristic algorithms are inspired by a given natural scenario. Firefly algorithm is a swarm-based metaheuristic algorithm which is introduced by Yang (2008). The algorithm mimics how fireflies interact using their flashing lights. The algorithm assumes that all fireflies are unisex, which means any firefly can be attracted by any other firefly; and the attractiveness a firefly is directly proportional to its brightness and depends on the objective function. Firefly will be attracted to a brighter firefly. Furthermore, the brightness, or light intensity, decreases through distance based on inverse square law, as given in (2).

$$\alpha + \beta = \chi. \qquad (1)$$

$$\beta = \beta_0 . e^{-\gamma . r} \qquad (2)$$

Where β_0 expresses maximum attractiveness and has value in the range [0, 1], γ indicates the absorption coefficient and

has some range [0,∞), r indicates the distance between the insects, for example, on a two-dimensional scale, the distance of the insect i from the insect j is calculated as (3):

$$r_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (3)$$

The movement of ith insect towards the jth insect is also obtained from (4):

$$X_i = X_i + \beta_0 e^{-\gamma . r} (X_j - X_i) + \alpha . (rand - 0.5) \quad (4)$$

The values of α, β_0 and γ are considered constant in the firefly algorithm. A and β_0 are selected in the range [0,1] and γ in the range [0,∞). Where xi,j is the values of each feature for each instance and xmin is the minimum value for a feature and xmax is the maximum value of feature.

4. Implementation

In order to implement the proposed method, the MATLAB software version 2015 has been used. In this study, the standard kddcup dataset has used that access in the standard UCI data repository. In the FA based feature selection method, firstly the continuous features related to the data set are separated. Then, for the values within each of the features, the lowest and highest values of the features are calculated for normalization according to (1). After normalization the data in continuous features, this data is presented as input to the FA. The task of the FA in this paper is to find the relationship between features and training data class label. In fact, FA due to the fitness function according to (4), calculates the correlation between features and data class label by calculating the movement of insects according to (2) and the distance of insects according to (3). FA has been collected around effective features based on the characteristics of the features and the correlation of each feature with the class label. Therefore, important features for network intrusion classification can be determined based on the output of the proposed FA optimization.

As shown in Table 1, the values of the correlation weights are calculated for features. The highest value is related to the feature that is most correlated to the class label. Fig. 2 also shows a bar chart showing the correlation weight of features to the class label.

As shown in Fig. 2, by determining the threshold, important, relevant features can be selected in the data set related to network intrusion detection. The value of this threshold should be chosen so that the selected features are considered as the main data representative and do not affect the accuracy of network intrusion detection. Therefore, in this paper, the threshold value α = 0.9 is used to select the features. In fact, attributes that have a correlation weight greater than 0.9 remain in the data set, and the rest of the attributes are removed from the data set. This threshold value is based on simulation and determining the maximum accuracy of the remaining features. Based on this, 11 important features are remained to detect the intrusion of wireless networks, and the rest are eliminated. The remaining features are used as the input of neural networks and the proposed fast neural learning network.

In the artificial neural networks, data sets are divided into three parts: training, validation, and testing. The validation section is for measuring the performance of the model for the training data. Artificial neural networks in the middle layer learn a model based on the features of the training data. The validity of this model in the first stage is done through a part of the data, which is called validation. When the performance accuracy of the training model for training data is acceptable, the accuracy of the model performance for test data and unknown data is measured through another part of the data called the test. Fig. 3 shows the neural networks developed in this study.

As shown in Fig.3, the neural networks used for this study include three layers input, middle, and output, with the number of nodes in the input layer equal to the number of features used after the default step and reducing the dimensions using the Firefly optimization algorithm.

The weight values of the classes in the middle layers are checked based on the mentioned training function and for each of the features, the weight is transferred to the next layer.

TABLE 1. Output Of Firefly Algorithm

Feature number	Firefly weight	Feature number	Firefly weight	Feature number	Firefly weight
1	0.48	14	0.59	27	0.057
2	0.54	15	0.57	28	0.35
3	0.44	16	0.57	29	0.0098
4	0.49	17	0.57	30	0.13
5	0.53	18	0.60	31	0.2
6	0.58	19	0.98	32	0.19
7	0.49	20	0.45	33	0.6
8	0.51	21	0.018	34	0.74
9	0.46	22	0.82	35	0.44
10	0.54	23	0.73	36	0.46
11	0.56	24	0.4	37	0.41
12	0.48	25	0.91	38	0.52
13	0.59	26	0.89	-	-

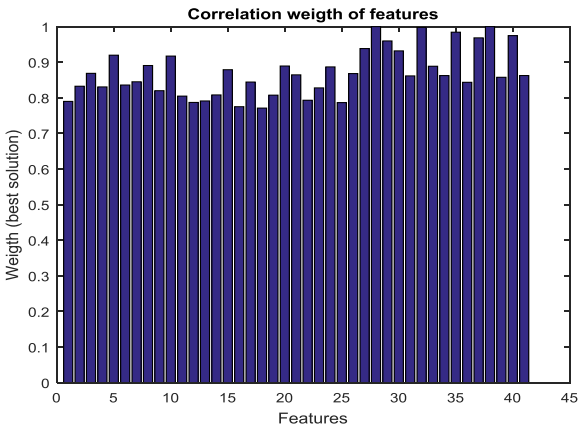

Fig. 2. Chart of features correlation to the class label

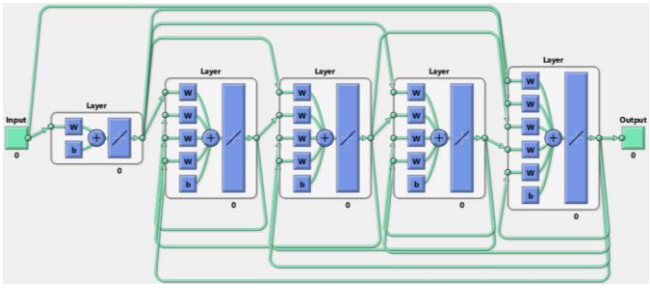

Fig. 3. Proposed neural network

Finally, the amount of weight for each class is sent from the middle layer to the outer layer. By applying these weights to the values of the features, they are assigned to the weight class if the results are true on the specified threshold. In fact, it can be said that the greater weights in results of multiplying in the adjective values of a sample for each class, the desired sample will be assigned to that class.

5. Evaluation Of The Proposed Method

To evaluate the accuracy of the proposed model in this study, the correct prediction rate of the samples in the model training stages on the training, validation and test data in the model repetition stages are examined. For this purpose, a matrix called the confusion matrix is drawn in which the number of correctly classified data versus the incorrectly classified data in the stages of training, validation and data testing is determined [31, 32]. This matrix includes the four elements as True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN) as follows:

- TP: normal nodes whose real class is also normal.
- TN: intrusion nodes whose real class is normal.
- FP: intrusion nodes whose real class is an intrusion.
- FN: normal nodes whose real class is an intrusion.

After extracting the parameters of the confusion matrix, the evaluation criteria can be obtained based on the confusion matrix. These criteria include Accuracy, Recall, Precision, Classification Rate, Detection Rate, Positive Error Rate, and F-measure. Fig.4 shows a comparison of the confusion matrix associated with the proposed method and the neural network.

As shown in Fig.4, in the proposed method, 96.7% of the total data in the data set, which includes training, validation, and test data, were properly classified. The neural network, on the other hand, classified 94.9 percent of the data correctly. Table 2 shows a comparison of the values for the proposed method and the neural network.

As shown in Table 2, the proposed method performs better than the neural network in terms of evaluation criteria. Fig.5 shows a comparison diagram between the proposed method and the neural network in ten steps of 10-fold Cross-validation. The classification rate in the proposed method is given as the rate of detection of normal nodes and intrusion nodes among all nodes in the collection.

As shown in Fig.5, the proposed method has improved in terms of classification rate (accuracy) compared to the neural network method. In the neural network method, the model may be overfitting due to the fact that the training process is complete. In this phenomenon, the model focuses on educational models and learns all the features and relationships between educational models, and its accuracy in classifying educational models reaches its maximum value. However, when new test specimens that the model has not previously seen enter the system, the model may not be careful in distinguishing between the features of the new specimens, which are different from the instructional specimens. And reduce system performance. Therefore, in order to prevent overfitting and increase the performance of the network penetration detection system, the proposed method continues the training process to the extent that the desired accuracy is achieved. Therefore, the accuracy diagram of the proposed method is better than the artificial neural network method. In fact, the proposed method has been able to correctly identify a higher percentage of attack nodes and healthy nodes.

After evaluating the proposed method using conventional criteria in the field of network penetration detection systems, now it is time to compare the proposed method with other previous methods to evaluate the improvement of the proposed ratio method and other methods. Given the importance of network intrusion detection systems mentioned in previous chapters, many researchers have tried to compare the proposed method with some of these methods in order to investigate its weaknesses and deaths. Since the greater effort of network intrusion detection systems is to increase the predictive accuracy of destructive nodes in the network, then comparisons are based on disturbance matrix criteria that include classification rate, detection rate, accuracy, accuracy, sensitivity, error detection rate, and The criterion is F, it is stable. Therefore, Table 3 shows a comparison of the proposed method with the previous methods [29, 33, 34].

As shown in Table 3, the proposed method performs better than previous methods in terms of time and negative error rate, and sensitivity criterion. It is generally comparable to other intrusion detection systems.

Fig. 4. Comparison of the confusion matrix for the proposed method and the neural network

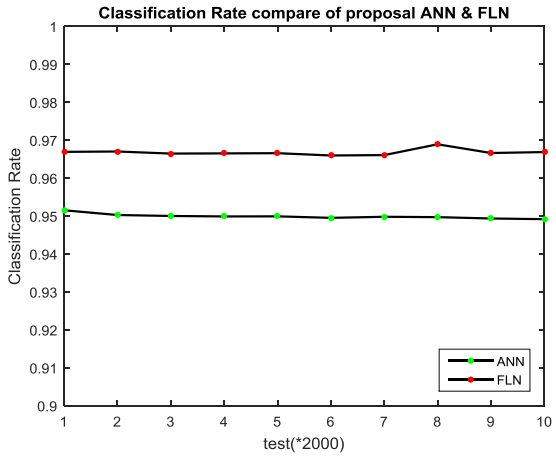

Fig. 5. Comparison of classification rate (accuracy) of the proposed method and neural network

TABLE 2. VALUES OF EVALUATION

Criteria	Proposed method	Neural Network
CR (Accuracy)	99.68%	94.92%
FPR	0.0431%	0.0653%
TPR	99.95%	98.32%
Precision	95.69%	81.29%
DR (Recall)	99.82%	100%
F-measure	97.71%	89.68%

TABLE 3. VALUES OF EVALUATION

Criteria	Time (s)	F-measure	DR (Recall)	Precision	TNR	FPR	CR (Accuracy)
Proposed method	74.4814	97.71%	99.82	95.23	99.95	0.0431	96.68
Neural network	87.3064	89.68	100	81.29	98.32	0.0653	94.92
CAI	239.96	98.48	99.13	98.33	99.08	0.92	98.92
SVM	2939.88	99	99.24	99.78	98.86	1.14	99.04
MLP	7622.15	99.11	98.63	99.08	99.15	0.085	99.14
HSO based FLN	-	97.19	95.82	98.61	99.92	0.0766	95.4
ATLBO based FLN	-	92.17	92.74	91.61	89.99	0.1001	91.48
GA based FLN	-	96.64	94.74	98.61	99.83	0.166	95.35
PSO based FLN	-	95.99	93.64	98.45	99.82	0.178	95.71
DBN	204600	97.47	97.91	97.81	99.79	0.21	97.9
S-NDAE	2446	98.15	97.85	99.99	99.78	0.215	97.85

6. CONCLUSION

Preventing and detecting intrusions and attacks on wireless sensor networks has become a vital and challenging task. On the other hand, due to the limited energy of wireless sensor nodes, the use of monitoring nodes for constant monitoring in wireless sensor networks in order to prevent and detect intrusion and attacks in this type of network is practically impossible. Therefore, a solution to overcome this problem, today, the discussion of control systems and remote monitoring, has become one of the topics of interest in various fields. Remote monitoring of the performance and behavior of nodes in wireless sensor networks, in addition to detecting malicious and abusive nodes within the network, can also predict the behavior of abusive nodes in the future. Therefore, in this study, to overcome this problem, a combined method was used based on the selection of a subset of a feature based on the firefly algorithm and the rapid neural learning network. The results of the experiments show that the performance accuracy of the proposed method was 99.9%, which is a high value and can be compared with other previous methods.

REFERENCES

[1] G. Liu, X., et al., Information-centric mobile ad hoc networks and content routing: a survey. Ad Hoc Networks, 2017. 58: p. 255-268.

[2] Rosas, E., et al., Survey on simulation for mobile ad-hoc communication for disaster scenarios. Journal of Computer Science and Technology, 2016. 31(2): p. 326-349.

[3] Rastegari, S., P. Hingston, and C.-P. Lam, Evolving statistical rulesets for network intrusion detection. Applied soft computing, 2015. 33: p. 348-359.

[4] Young, C., et al., Survey of Automotive Controller Area Network Intrusion Detection Systems. IEEE Design & Test, 2019.

[5] Fotohi, R. and S. Jamali, A comprehensive study on defence against wormhole attack methods in mobile Ad hoc networks. International journal of Computer Science & Network Solutions, 2014. 2: p. 37-56.

[6] Liu, G., Z. Yan, and W. Pedrycz, Data collection for attack detection and security measurement in mobile ad hoc networks: A survey. Journal of Network and Computer Applications, 2018. 105: p. 105-122.

[7] Gupta, A.M.V., Comprehensive survey on Blackhole attack with various Detection/Prevention techniques in Ad-hoc network. International Journal of Applied Engineering Research, 2019. 14(8): p. 2009-2017.

[8] Yeruru, S.V. and T.R. Rangaswamy, An Anomaly-Based Intrusion Detection System with Multi-Dimensional Trust Parameters for Mobile Ad Hoc Network. International Journal of Intelligence Engineering and Syatems, 2017. 10(4): p. 81-90.

[9] Rajalakshmi, D. and K. Meena, A Survey of intrusion detection with higher malicious misbehavior detection in Manet. International journal of civil engineering and technology, 2017. 8.

[10] Jamali, S. and V. Shaker, Defense against SYN flooding attacks: a particle swarm optimization approach. Computers & Electrical Engineering, 2014. 40(6): p. 2013-2025.

[11] Babasaheb, D.R. and I. Raman. Survey on Fault Tolerance and Security in Mobile Ad Hoc Networks (MANETs). in 2018 3rd

International Conference for Convergence in Technology (I2CT). 2018. IEEE.

[12] Soms, N. and P. Malathi, Evolution of Intrusion Detection System in MANETs–A Survey. International Journal of Innovations & Advancement in Computer Science (IJIACS), 2017. 6(5).

[13] Jamali, S. and R. Fotohi, DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system. the Journal of Supercomputing, 2017. 73(12): p. 5173-5196.

[14] Scholar, M.T., S. GORAKHPUR, and I.C. Choubey, A survey on malicious nodes in mobile ad hoc network. Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org, 2016. 6(3).

[15] Hajimirzaei, B. and N.J. Navimipour, Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm. ICT Express, 2019. 5(1): p. 56-59.

[16] Dhanalakshmi, K. and B. Kannapiran, Analysis of KDD CUP Dataset Using Multi-Agent Methodology with Effective Fuzzy Based Intrusion Detection System. Journal of Applied Security Research, 2017. 12(3): p. 424-439.

[17] Selvakumar, B. and K. Muneeswaran, Firefly algorithm based feature selection for network intrusion detection. Computers & Security, 2019. 81: p. 148-155.

[18] Abedin, M., et al. Performance Analysis of Anomaly Based Network Intrusion Detection Systems. in The 43nd IEEE Conference on Local Computer Networks (LCN). 2018. IEEE Computer Society.

[19] Chiba, Z., et al., A novel architecture combined with optimal parameters for back propagation neural networks applied to anomaly network intrusion detection. Computers & Security, 2018. 75: p. 36-58.

[20] Gupta, A. and A. Dubey, A Survey on Various Applications and Blackhole Attack in Mobile Ad Hoc Network. Recent Trends in Parallel Computing, 2018. 5(1): p. 1-6.

[21] Chellam, A., L. Ramanathan, and S. Ramani, Intrusion Detection in Computer Networks using Lazy Learning Algorithm. Procedia computer science, 2018. 132: p. 928-936.

[22] Ashfaq, R.A.R., et al., Fuzziness based semi-supervised learning approach for intrusion detection system. Information Sciences, 2017. 378: p. 484-497.

[23] Karatas, G. and O.K. Sahingoz. Neural network based intrusion detection systems with different training functions. in 2018 6th International Symposium on Digital Forensic and Security (ISDFS). 2018. IEEE.

[24] Giokas, I., Systems and methods for self-tuning network intrusion detection and prevention. 2016, Google Patents.

[25] Al-Utaibi, K.A. and E.-S.M. El-Alfy, Intrusion detection taxonomy and data pre-processing mechanisms. Journal of Intelligent & Fuzzy Systems, 2018. 34(3): p. 1369-1383.

[26] Madbouly, A.I. and T.M. Barakat, Enhanced relevant feature selection model for intrusion detection systems. International Journal of Intelligent Engineering Informatics, 2016. 4(1): p. 21-45.

[27] Protić, D. and M. Stanković, Anomaly-Based Intrusion Detection: Feature Selection and Normalization Influence to the Machine Learning Models Accuracy. European Journal of Engineering and Formal Sciences, 2018. 2(3): p. 101-106.

[28] Jain, Y.K. and S.K. Bhandare, Min max normalization based data perturbation method for privacy protection. International Journal of Computer & Communication Technology, 2011. 2(8): p. 45-50.

[29] Ali, M.H., et al., A new intrusion detection system based on fast learning network and particle swarm optimization. IEEE Access, 2018. 6: p. 20255-20261.

[30] Tilahun, S.L., J.M.T. Ngnotchouye, and N.N. Hamadneh, Continuous versions of firefly algorithm: A review. Artificial Intelligence Review, 2019. 51(3): p. 445-492.

[31] Jamali, S. and Y.D. Navaei, A two-level Product Recommender for E-commerce Sites by Using Sequential Pattern Analysis. International Journal of Integrated Engineering, 2016. 8(1).

[32] Jamali, S. and G. Shaker, PSO-SFDD: Defense against SYN flooding DoS attacks by employing PSO algorithm. Computers & Mathematics with Applications, 2012. 63(1): p. 214-221.

[33] Gurung, S., M.K. Ghose, and A. Subedi, Deep Learning Approach on Network Intrusion Detection System using NSL-KDD Dataset. International Journal of Computer Network and Information Security (IJCNIS), 2019. 11(3): p. 8-14.

[34] Wang, C.-R., et al., Network intrusion detection using equality constrained-optimization-based extreme learning machines. Knowledge-Based Systems, 2018. 147: p. 68-80.

Samira Rajabi had graduated in B.S in Computer Engineering from Mohaghegh Ardabili University of Iran. He also has graduated in M.Sc from the same university in Computer Systems Architecture Engineering. He is interested in the field of network security and network intrusion detection systems.

Shahram Jamali is a professor leading the Autonomic Networking Group at the Department of Engineering, University of Mohaghegh Ardabili. He teaches on computer networks, network security, computer architecture, and computer systems performance evaluation. Dr. Jamali received his M.Sc. and a Ph.D. degree from the Dept. of Computer Engineering, Iran University of Science and Technology in 2001 and 2007, respectively. Since 2008, he is with the Department of Computer Engineering, University of Mohaghegh Ardabil and has published more than 150 conference and journal papers.

Javad Javidan is a professor leading the Autonomic Networking Group at the Department of Engineering, University of Mohaghegh Ardabili. He is interested in network fields and evolutionary processing methods.