Computers, Materials & Continua CMC, vol.65, no.2, pp.1097-1111, 2020

Towards Improving the Intrusion Detection through ELM (Extreme Learning Machine)

Iftikhar Ahmad[1, *] and Rayan Atteah Alsemmeari[1]

Abstract: An IDS (intrusion detection system) provides a foremost front line mechanism to guard networks, systems, data, and information. That's why intrusion detection has grown as an active study area and provides significant contribution to cyber-security techniques. Multiple techniques have been in use but major concern in their implementation is variation in their detection performance. The performance of IDS lies in the accurate detection of attacks, and this accuracy can be raised by improving the recognition rate and significant reduction in the false alarms rate. To overcome this problem many researchers have used different machine learning techniques. These techniques have limitations and do not efficiently perform on huge and complex data about systems and networks. This work focused on ELM (Extreme Learning Machine) technique due to its good capabilities in classification problems and dealing with huge data. The ELM has different activation functions, but the problem is to find out which function is more suitable and performs well in IDS. This work investigates this problem. Here, Well-known activation functions like: sine, sigmoid and radial basis are explored, investigated and applied to measure their performance on the GA (Genetic Algorithm) features subset and with full features set. The NSL-KDD dataset is used as a benchmark. The empirical results are analyzed, addressed and compared among different activation functions of the ELM. The results show that the radial basis and sine functions perform better on GA feature set than the full feature set while the performance of the sigmoid function is almost equal on both features sets. So, the proposal of GA based feature selection reduced 21 features out of 41 that brought up to 98% accuracy and enhanced overall efficiency of extreme learning machine in intrusion detection.

Keywords: Accuracy, extreme learning machine, sine function, sigmoid function, radial basis, genetic algorithm, NSL–KDD.

1 Introduction

Intrusion is the earliest problem of a security hole and critical concern in security [Ahmad, Basheri, Iqbal et al. (2018a)]. A single intrusion can remove or destroy data or information from computers and networks in a limited time [Ahmad (2014a)]. It can also

[1] D.I.T, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia.

[*] Corresponding Author: Iftikhar Ahmad. Email: iakhan@kau.edu.sa.

Received: 26 May 2020; Accepted: 10 July 2020.

harm the hardware of the systems, can cause an immense failure financially, and can damage the Information Technology infrastructure of the critical organizations that may lead to information inadequacy in the cyber-war [Gautam and Om (2016); Kabir, Hu, Wang et al. (2018); Subba, Biswas and Karmakar (2018)]. So, this is a critical concern that needs to be handled to secure the information in systems and the information available on the network media [Jayshree and Ragha (2013); Modi, Patel, Borisaniya et al. (2013a); Wang, Gu and Wang (2017a)].

Diverse intrusion detection methods are being used but the major challenge is their accuracy which based on accurate detection rate and less false alarms rate [Douzi, Benchaji and ElOuahidi (2018); Inaba, Salles, Perron et al. (2018); Modi, Patel, Borisaniya et al. (2013b)]. To overcome such problems, many researchers have applied various machine techniques to develop their systems [Bhattacharjee, Fujail and Begum (2017); Tavallaee, Bagheri, Lu et al. (2009)]. Recently, ELM has been used to improve intrusion detection [Ahmad, Basheri, Iqbal et al. (2018b)]. But the ELM has different activation functions and a study is required to explore which activation function of ELM is better in performance for IDS. For this purpose, different ELM activation functions are explored, investigated and implemented which haves proven their worth in classification problems of different domains.

Mostly, Intrusion detection systems used standard datasets for validation purposes. The KDD dataset is also ordinarily accepted as a benchmarked dataset, but it has some concerns of redundancy, duplication, and randomization as notified and highlighted by several researchers [Al-Yaseen, Othman and Nazri (2017a); Imamverdiyev and Sukhostat (2016a); Ku, Zheng and Yun (2017a)]. This work utilized the NSL-KDD dataset which is an improved reproduction of the original dataset-KDD. Further, this dataset has been utilized as a popular symbol and reference point in the validation of intrusion detection schemes [Atli, Miche, Kalliola et al. (2018a)].

This paper falls into five different parts and sections. Section 2 deals with literature review while Section 3 provides step by step methodological procedure of ELM based IDS with its various activation functions. Section 4 discusses analysis and experimental results. Finally, Section 5 sums up the whole discussion and paves the way for future research.

2 Related work

Presently, intrusion detection approaches have acquired a significant importance in security infrastructure. This section discusses multiple variation of machine learning techniques for the purpose of threat or attack detection.

Roshan et al. [Roshan, Miche, Akusok et al. (2018a)] presented a model on ELM for network intrusion detection, and their claim about the model is that it has the capability to detect novel as well as familiar attacks. It also has the ability to update the new signature attack in an adequate way. The results show that their system detected the activities as normal and intrusive up to 89%. In the training process, they applied supervised and unsupervised learning methods with the detection rate of 77% and 70% respectively.

Al-Yaseen et al. [Al-Yaseen, Othman, Nazri et al. (2017b)] introduced multiple levels hybrid network intrusion detection models of ELM, and used support vector machine for performance improvement of known and unknown attacks. They utilized popular KDD-

cup 99 benchmark dataset for the validation of their system's performance. The results indicate this system had out class performance in both multiple level SVM (Support Vector Machine) and ELM models independently. The overall performance of system was improved and measured in terms of accuracy up to 95.75% which is greater than the individual one which is 95.57%, and 93.83% respectively.

According to Imamverdiyev et al. [Imamverdiyev and Sukhostat (2016b)], the authors suggested an ELM based model in order to discover anomalies in network traffic. They declared that their method had achieved higher level of accuracy to identify attacks in network traffic. They also analyzed various categories of network attacks such as DOS, U2R, R2L and probing by using multiple functions in ELM such as RBF, Tribas, and Gaussian. Their proposed model presented 94.33% average accuracy. The sine activation function for ELM can perform better than other functions but it was not used in their work.

In Ku et al. [Ku, Zheng and Yun (2017b)], the authors suggested a model known as SADE-ELM (self-adaptive differential evolution extreme learning machine). They used different types of extreme learning machines to analyze different types of threats. They illustrated different types of results and their outcomes indicated their proposed method had exceeded other approaches in terms of accuracy. They achieved higher accuracy on a small data set and their model was not validated on a large data set.

Atli et al. [Atli, Miche, Kalliola et al. (2018b)] stated a mechanism for network attack detection that utilized network statistics info and ELM to attain higher level of accuracy for IDS. They worked at the IP subnetworks. Moreover, dissemination of statistics are accumulated which is presented to ELM for intrusion analysis. They verified their model by using ISCX-IDS 2012 dataset. The dataset was collected by building a real-time testbed. They conducted various experiments and verified their results through various approaches. Their model attained an accuracy of 91% and an error rate of 9%.

Yu et al. [Yu, Liu, Zhao et al. (2017a)] proposed Hierarchical ELM (H-ELM) for network traffic's attack detection. They employed a conventional dataset NSL-KDD to endorse their system. They analyzed distinct machine learning approaches for instance k-Nearest Neighbor (k-NN), Random Forest (RF) and ELM with their intended methods. The results exposed that H-ELM can show better performance, with accuracy of approximately 72.87% than the previous techniques

According to Khammassi et al. [Khammassi and Krichen (2017)], the authors proposed a method for optimal feature subset selection for intrusion detection by using wrapper approach and genetic algorithm. They used genetic algorithm and wrapper method for searching, and logistic regression for learning algorithm. They experimented with KDD99 dataset though this dataset has several issues. They drew out 99.90% detection rate with the help of eighteen selected features.

Tao et al. [Tao, Sun and Sun (2018)] proposed genetic algorithm and SVM for their intrusion detection mechanism. The genetic algorithm was applied for feature subset selection, weight and other parameter optimization of the classifier. They showed 91% detection rate with GA selected features and 100% in appropriate selection of weights and SVM parameters.

Several approaches based on machine learning are available to distinguish normal and intrusive activities of the network system such as AIM (artificial immune system) [Tabatabaefar, Miriestahbanati and Grégoire (2017)], SVM [Wang, Gu and Wang (2017b)], KNN [Li, Zhang, Peng et al. (2018)], and fuzzy logic [Douzi, Benchaji and ElOuahidi (2018)]. However, the major issue with degradation of performance which can be significantly enhanced using a suitable features selection method and a right classification technique. Therefore, we have selected genetic algorithm for features selection and ELM is explored with its different activation functions for intrusion classification due to its effectiveness for solving complex classification problems. Many researchers have focused on machine learning and deep learning to develop their techniques for feature selection and classification [Liu, Yang, Lv et al. (2019); Zhang, Jin, Sun et al. (2018); Zhang, Wang, Lu et al. (2019)]. Further, there is also a trade-off between the accuracies of both learning techniques. One is suitable for classification, and the other performs better in feature transformation.

3 Methodology

The methodology is completely explained through Fig. 1 which consists of four stages: cleaning the underlined data, feature subset selection, classification, and splitting of data into training and testing. Each stage has significant impact on the performance, but the focal point is to examine different activation functions of ELM in intrusion detection.

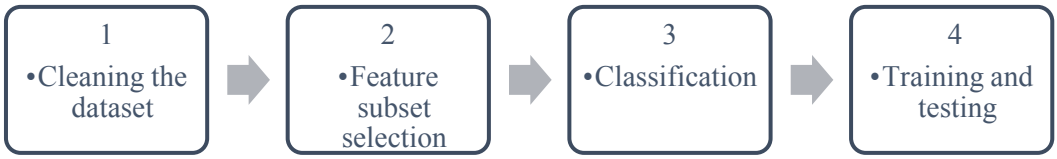

Figure 1: Methodology

3.1 Cleaning the dataset

The first step is preprocessing the raw dataset. This is an essential means in which symbolic or non-numeral features are excluded or substituted because these features are not supportive on one hand, but produce depreciation in IDS by taking more training time, increasing complexity in classifier's architecture, using more memory and consuming more computing resources on other hand. Consequently, the non-numeral features should be dismissed from the original feature set for more reliable IDS.

3.2 Feature subset selection

The second most important phase consists of feature subset selection which finds only those features which are distinct, non-redundant or most significant. The performance of the classification depends on defining the features. Therefore, the selection of a discriminatory feature is very important and a very big challenge. This research work also focuses on this selection. The most recent algorithm used for feature selection is GA. Feature selection is the determination of significant features which are less than the total features set that maintains the maximum accuracy [Ahmad, Basheri, Iqbal et al. (2018c)].

The selected feature subset enhances the training and testing time complexity; also supports to develop lightweight IDS which may guarantee to provide best detection rates, and makes proposed IDS appropriate for real-time traffic detection of network attacks. Due to the above-mentioned benefits we preferred to use GA to select a subset of features here. The GA is applied on 41 features of NSL-KDD dataset, in our experiments, and helps to obtain a final feature subset of 21 features. This feature subset is presented to different activations functions of the ELM to investigate their performance.

3.3 Classification

The ultimate goal of any IDS, like intrusion analysis engine, is to split the network traffic data into either normal or intrusive nature data. Generally, ELM involves various activation functions for proper and smooth working of intrusion analysis engine. In this work, ELM is utilized to perform the important task of network related to particularly intrusion attacks data classification. The preliminary detail of ELM is provided hereunder.

3.3.1 Extreme learning machine

ELM has proved a well-known model of single or multilayer perceptron neural networks [Duan, Li, Yang et al. (2018); Inaba, Salles, Perron et al. (2018); Roshan, Miche, Akusok et al. (2018b); Song and Dai (2017); Yu, Liu, Zhao et al. (2017b)]. ELM is very effective to carry out major tasks related to supervised or unsupervised learning such as classification, regression, clustering and automatic feature engineering [Ahmad, Basheri, Iqbal et al. (2018d)]. The architecture of ELM comprises of, one input layer, one or few hidden layers and finally the output layer. The major drawback of conventional neural networks is that the convergence of all input and hidden layers' weight is computationally extensive as it gone through several stages to obtain optimization stage. Recently, this problem is addressed through SLFN (Single hidden layer feedforward neural network) by randomly picking model weights and hidden layer biases to reduce the network training time. Roshan et al. [Roshan, Miche, Akusok et al. (2018c)] introduced a model that learn faster with better generalization ability as opposed to other standard network models. Overall performance of ELM is better in many aspects than SVM and various other popular machine learning algorithms. One major benefit of ELM is to produce better results on huge and extremely complex benchmark dataset(s). The network structure of underlined system is given in Fig. 2. N input samples (z_i, y_i) are present, where $z_i = [x_{i1}, x_{i2}, \ldots\ldots, x_{in}]^T$ shows ith instance with n different attributes/features while $y_i = [y_{i1}, y_{i2}, \ldots\ldots, y_{im}]^T$ givens the original class labels of x_i with standard SLFN with M hidden neurons such as:

$$\sum_{m=1}^{M} \beta_i \, h(w_m . x_i + c_m) = \alpha_i, \qquad i = 1, \ldots\ldots\ldots, N \tag{1}$$

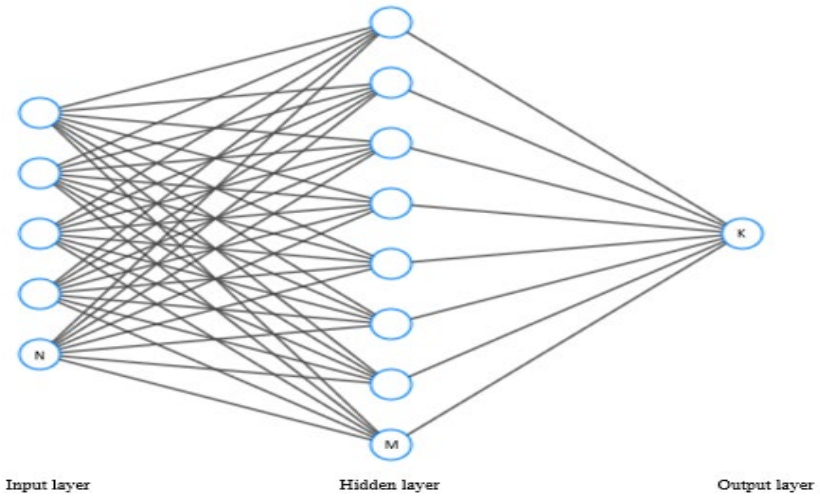

Figure 2: Sample ELM model

Here in Eq. (1), $w_m = [w_{m1}, w_{m2}, \ldots\ldots, w_{mn}]^T$ is randomly selected weights vector and shows an ith hidden neuron links with input layer neurons. $\beta_i = [\beta_{i1}, \beta_{i2}, \ldots, \beta_{im}]^T$ represents the weights vector for ith hidden and output layer neurons and c_m reflects threshold of the ith hidden layer neuron $\alpha_k = [\alpha_{k1}, \alpha_{k2}, \ldots, \alpha_{km}]^T$ is kth output layer neuron. $h(.)$ shows which activation function is applied in SLFN on M hidden layer neurons. Importantly, this activation function will work for all these N training records without any error. In literature several other popular methods have been investigated for accurate detection and classification of intrusions for wired and wireless enabled environments [Al-Yaseen, Othman, Nazri et al. (2017c); Atli, Miche, Kalliola et al. (2018c); Imamverdiyev and Sukhostat (2016c); Ku, Zheng and Yun (2017)]. The ELM is one which provides better performance but it has various activation functions required to investigate for intrusion detection which performs better in in terms of accuracy. These ELM activation functions are described here.

3.3.2 Activation functions

This work used three different activation functions i.e., sine function, sigmoid function and radial basis function of ELM which is known as good classifier in the problem of classification. The graphical representation of each function is shown in Figs. 3 to 5. Fig. 3 shows the graph of sine activation function and its formula is shown in Eq. (2). The graph of sigmoid function is shown is Fig. 4 and Eq. (3) represents mathematically expression. Fig. 5 presents the graph of radial basis function and Eq. (4) stated its mathematically notation.

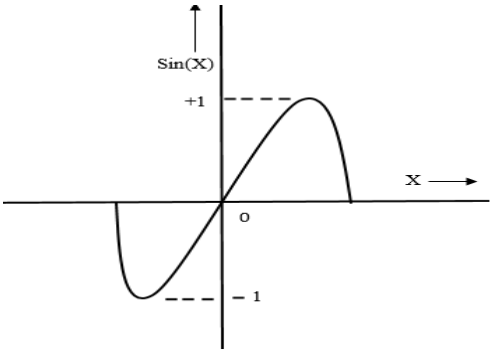

Figure 3: The graph of sine function

$$y = \mathrm{SIN}(x) \tag{2}$$

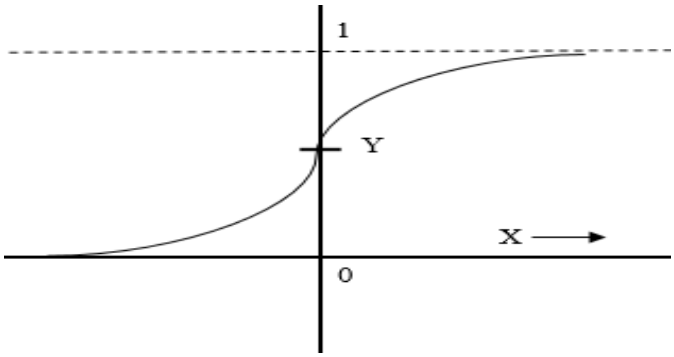

Figure 4: The graph of sigmoid function

$$y = \frac{1}{1+e^{-x}} \tag{3}$$

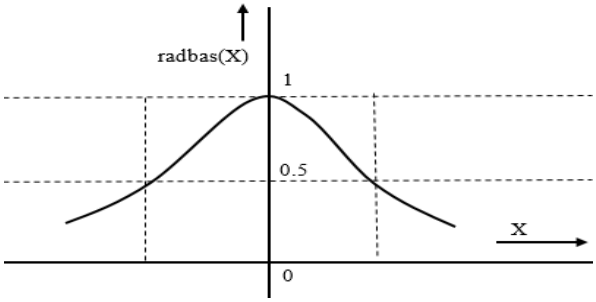

Figure 5: The graph of radial bais function

$$y = exp\left(-\frac{(x-c)^2}{r^2}\right) \tag{4}$$

The parameters are its center c and its radius r in Eq. (4).

3.4 Training and testing

The system is trained and tested on NSL–KDD benchmark dataset [Revathi and Malathi (2013); Tavallaee, Miriestahbanati and Grégoire et al. (2009)]. The data is randomly divided into two parts; the training data and the testing data. The ratio of training data is 80% and it includes 52428 instances whereas the ratio of testing data is 20% and it consists of 13,107 instances. Accuracy metric represented in Eq. (5) [Yu, Liu, Zhao et al. (2017c)] validates overall performance of this work. The mathematical notation of the accuracy is hereunder:

$$Accuracy = \frac{TP+TN}{TP+FN+FP+TN} \tag{5}$$

Here TP represents true positive, TN true negative, FN false negative and final FP false positive.

4 Results

Comparison among three different activation functions is presented in Tab. 1.

Table 1: Comparative analysis of THREE FUNCTIONS on full feature set

Hidden Neurons	Sigmoid function	Sine function	Radial basis function
20	97.9%	93.5%	96.9%
40	98.1%	94.4%	97.0%
60	98.1%	94.5%	96.3%
Average Accuracy	98.03%	94.13%	96.73%

The detail of comparative analysis of sigmoid, sine and radial basis functions with 20 neurons in hidden layer is shown in Fig. 6. The sigmoid function indicates 97.9%, the radial basis function shows 96.9% and sine function represents 93.5% accuracy. Thus, the sigmoid function outperforms the other functions with twenty neurons in hidden layer of the ELM model.

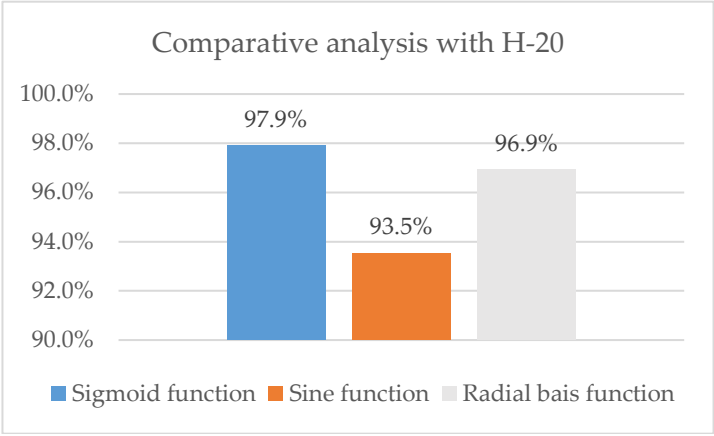

Figure 6: The graph of sigmoid, sine and radial basis functions

Fig. 7 elaborates a comparison among sigmoid, sine and radial basis with 40 neurons in hidden layer. The sigmoid function shows the highest accuracy 98.1% than radial basis and

sine functions which indicate 97.0% and 94.4% respectively. This comparative study indicates that increasing hidden layer neurons size improves the overall efficiency and performance of ELM.

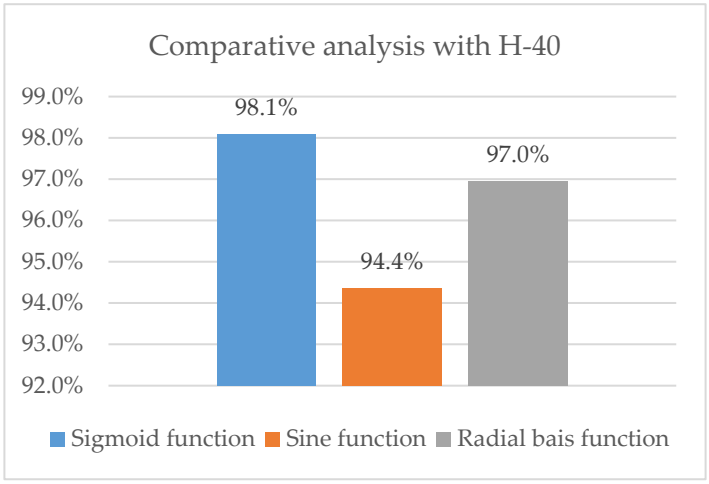

Figure 7: The graph of sigmoid, sine and radial basis functions

Sigmoid, sine and radial basis functions with 60 neurons in hidden layer have been compared Fig. 8. The sigmoid function shows better performance in accuracy with 98.1% than radial basis and sine functions which represent 96.3% and 94.5% accuracy.

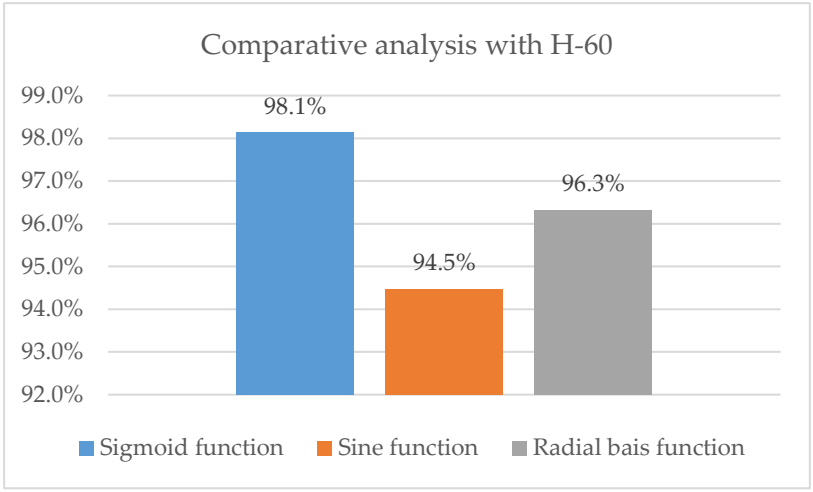

Figure 8: The graph of sigmoid, sine and radial bais functions

The sigmoid and sine functions sustained their performance with 20, 40 and 60 hidden neurons, while the radial base function decreases its performance with 20 and 60 hidden neurons, but it performs better with 40 neurons in hidden layer of ELM.

Tab. 2 figures out how these three functions perform with genetic algorithm.

Table 2: Comparative analysis of THREE FUNCTIONS on selected feature set

Hidden Neurons	Sigmoid function	Sine function	Radial basis function
20	97.40%	95.0%	95.90%
40	98.00%	94.9%	95.00%
60	97.70%	95.2%	97.30%
Average Accuracy	97.70%	95.03%	96.07%

Fig. 9 explains comparative analysis of three functions with 20 neurons in hidden layer on GA selected features. Sigmoid function indicates 97.40%, accuracy, sine 95.0% and radial basis 95.90%.

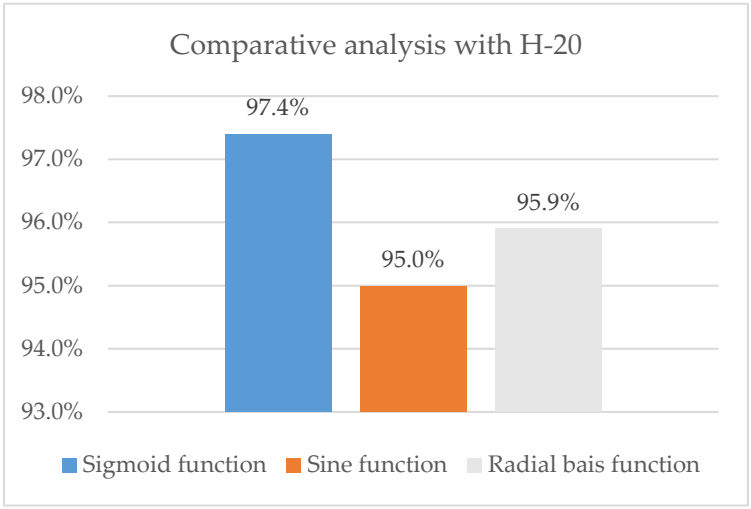

Figure 9: The graph of three sigmoid, sine and radial bais functions

The detail of comparative analysis of sigmoid, sine and radial basis functions with 40 neurons in hidden layer on GA selected features set is shown in Fig. 10. The accuracy of sigmoid, sine and radial basis functions is 97.40%, 95% and 95.90%.

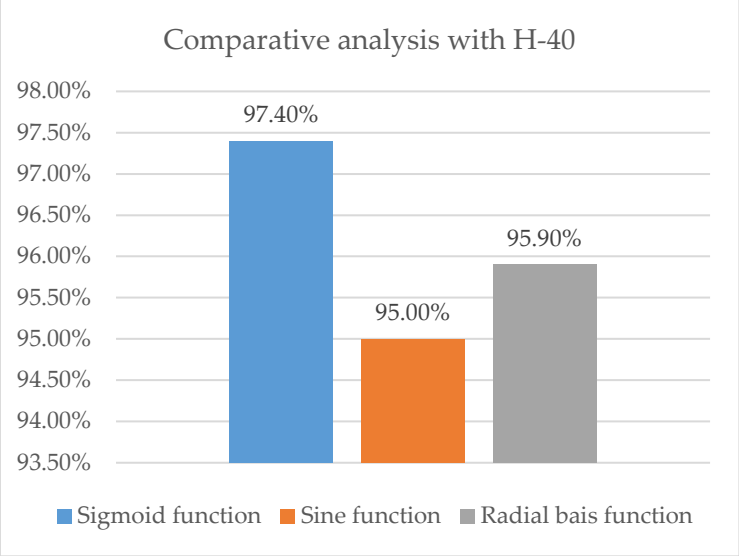

Figure 10: The graph of three sigmoid, sine and radial bais functions with 60 neurons

Fig. 11 highlights a comparative analysis of these functions with 60 neurons in hidden layer on selected features. The sigmoid shows 97.70%, the radial basis indicates 97.30% and sine function represents 95.20% accuracy.

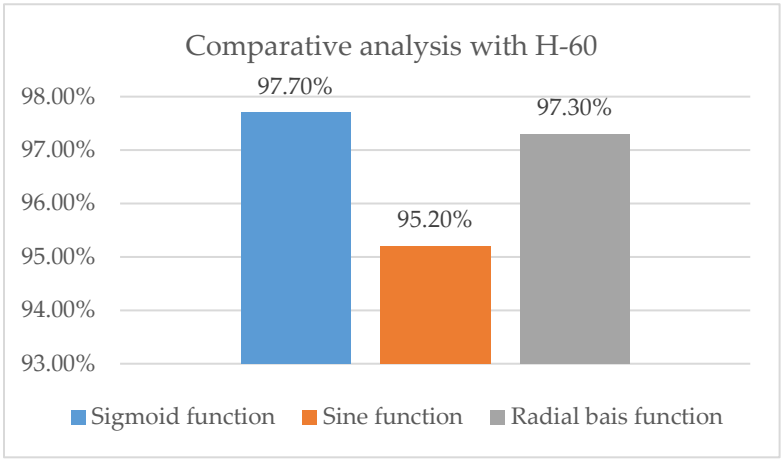

Figure 11: The graph of sigmoid, sine and radial bais functions

Fig. 12 manifests a comparative analysis of sigmoid with different size of neurons in hidden layer with full features set and GA feature set. The sigmoid function shows best performance on 40 and 60 hidden neurons on full features set while it outperforms on GA selected features set with 60 hidden neurons.

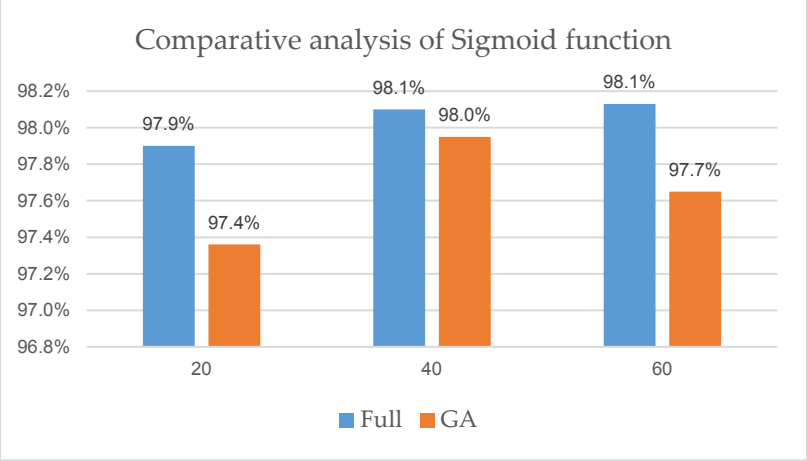

Figure 12: The graph of sigmoid function with variable number of hidden layers, with full features, and with GA features subset

The detail of comparative analysis of sine function with different size of neurons in hidden layer with full features set and GA feature set is shown in Fig. 13. The sine function outperforms on 20 and 40 hidden neurons on GA feature set.

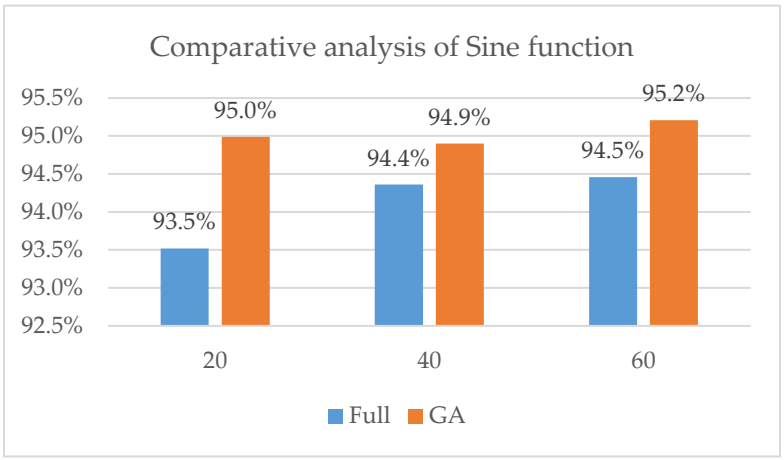

Figure 13: The graph of sine function with variable number of hidden layer on full features set and GA features subset

Fig. 14 reveals analytical study of radial basis function with different number of neurons in hidden layer with full features set and GA feature set. This function achieves performance on GA selected features set with 60 hidden neurons.

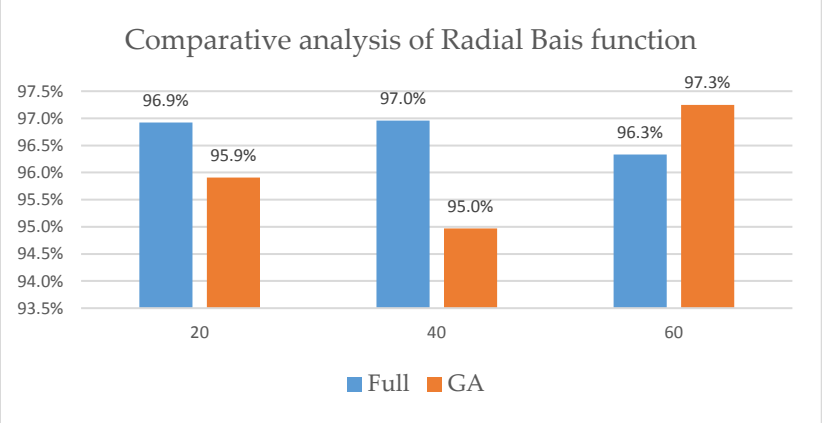

Figure 14: The graph of radial bais function with variable number of hidden layer on full features set and GA features subset

5 Conclusion

Intrusion detection system provides the main defense line to protect networks, systems, data and information. To empower the IDS to work on huge data, extreme learning machine is used. ELM has different activation functions such as sine, sigmoid and radial basis. These functions are applied on standard dataset; NSL-KDD with full features set which consists of 41 features to investigate their accuracy. The results show that the sigmoid function outperforms with 98.1% accuracy on full features while radial basis and sine functions show 97.0% and 94.5% accuracy. These functions are also tested on GA features set which consists of 21 features. The sigmoid function also outperforms here with 98.0% accuracy while radial basis and sine functions show 97.3% and 95.2% accuracy respectively. Further, the radial basis and sine functions performs better on GA feature set as compared to full feature set. The performance of the sigmoid function is almost equal on both features sets. So the idea of feature selection is important which reduces features and also demonstrates better accuracy to improve the efficiency, performance and complexity of extreme learning machine.

Acknowledgment: This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah under grant no. G: 656-611-1439. The authors, therefore, acknowledge with thanks DSR for technical and financial support.

Funding Statement: This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah under grant no. G: 656-611-1439.

Conflicts of Interest: We declare that we have no conflicts of interest to report regarding the present study.

References

Ahmad, I. (2014): Enhancing MLP performance in intrusion detection using optimal feature subset selection based on genetic principal components. *Applied Mathematics & Information Sciences*, vol. 8, no. 2, pp. 639-649.

Ahmad, I.; Basheri, M.; Iqbal, M. J.; Rahim, A. (2018): Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. *IEEE Access*, vol. 6, pp. 33789-33795.

Al-Yaseen, W. L.; Othman, Z. A.; Nazri, M. Z. A. (2017): Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system. *Expert Systems with Applications*, vol. 67, pp. 296-303.

Atli, B. G.; Miche, Y.; Kalliola, A.; Oliver, I.; Holtmanns, S. et al. (2018): Anomaly-based intrusion detection using extreme learning machine and aggregation of network traffic statistics in probability space. *Cognitive Computation*, vol. 10, no. 5, pp. 848-863.

Bhattacharjee, P. S.; Fujail, A. K. M.; Begum, S. A. (2017): A comparison of intrusion detection by K-means and fuzzy C-means clustering algorithm over the NSL-KDD dataset. *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 1-6, Coimbatore,Tamil Nadu, India.

Douzi, S.; Benchaji, I.; ElOuahidi, B. (2018): Hybrid approach for intrusion detection using fuzzy association rules. *The 2nd Cyber Security in Networking Conference*, pp. 1-3, Paris, France.

Duan, M.; Li, K.; Yang, C.; Li, K. (2018): A hybrid deep learning CNN-ELM for age and gender classification. *Neurocomputing*, vol. 275, pp. 448-461.

Gautam, S. K.; Om, H. (2016): Computational neural network regression model for host based intrusion detection system. *Perspectives in Science*, vol. 8, pp. 93-95.

Imamverdiyev, Y.; Sukhostat, L. (2016): Anomaly detection in network traffic using extreme learning machine. *IEEE 10th International Conference on Application of Information and Communication Technologies*, pp. 1-4, Baku,Azerbaijan.

Inaba, F. K.; Salles, E. O. T.; Perron, S.; Caporossi, G. (2018): DGR-ELM-distributed generalized regularized ELM for classification. *Neurocomputing*, vol. 275, pp. 1522-1530.

Jayshree, J.; Ragha, L. (2013): Intrusion detection system using support vector machine. *International Journal of Applied Information Systems*, vol. ICWAC, no. 3, pp. 2249-0868.

Kabir, E.; Hu, J.; Wang, H.; Zhuo, G. (2018): A novel statistical technique for intrusion detection systems. *Future Generation Computer Systems*, vol. 79, pp. 303-318.

Khammassi, C.; Krichen, S. (2017): A GA-LR wrapper approach for feature selection in network intrusion detection. C*omputers and Security*, vol. 70, pp. 255-277.

Ku, J.; Zheng, B.; Yun, D. (2017): Intrusion detection based on self-adaptive differential evolutionary extreme learning machine. *The International Conference on Computer Network, Electronic and Automation*, pp. 94-100, Xi'an, China.

Li, L.; Zhang, H.; Peng, H.; Yang, Y. (2018): Nearest neighbors based density peaks approach to intrusion detection. *Chaos, Solitons & Fractals*, vol. 110, pp. 33-40.

Liu, J.; Yang, Y.; Lv, S.; Wang, J.; Chen, H. (2019): Attention-based BiGRU-CNN for Chinese question classification. *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-12.

Modi, C.; Patel, D.; Borisaniya, B.; Patel, H.; Patel, A. et al. (2013): A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42-57.

Revathi, S.; Malathi, A. (2013): A detailed analysis on NSL-KDD dataset using various machine learning techniques for intrusion detection. *International Journal of Engineering Research & Technology*, vol. 2, no. 12, pp. 1848-1853.

Roshan, S.; Miche, Y.; Akusok, A.; Lendasse, A. (2018): Adaptive and online network intrusion detection system using clustering and extreme learning machines. *Journal of the Franklin Institute*, vol. 355, no. 4, pp. 1752-1779.

Song, G.; Dai, Q. (2017): A novel double deep ELMs ensemble system for time series forecasting. *Knowledge-Based Systems*, vol. 134, pp. 31-49.

Subba, B.; Biswas, S.; Karmakar, S. (2018): A game theory based multi layered intrusion detection framework for VANET. *Future Generation Computer Systems*, vol. 82, pp. 12-28.

Tabatabaefar, M.; Miriestahbanati, M.; Grégoire, J. C. (2017): Network intrusion detection through artificial immune system. *The Annual IEEE International Systems Conference*, pp. 1-6, Montreal, Québec, Canada.

Tao, P.; Sun, Z.; Sun, Z. (2018): An improved intrusion detection algorithm based on GA and SVM. *IEEE Access*, vol. 6, pp. 13624-13631.

Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A. A. (2009): A detailed analysis of the KDD CUP 99 data set. *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, pp. 1-6, Ottawa, Canada.

Wang, H.; Gu, J.; Wang, S. (2017): An effective intrusion detection framework based on SVM with feature augmentation. *Knowledge-Based Systems*, vol. 136, pp. 130-139.

Yu, L.; Liu, Y.; Zhao, W.; Liu, Q.; Qin, J. (2017): A highly efficient intrusion detection method based on hierarchical extreme learning machine. *International Conference on Extreme Learning Machine*, *Proceedings in Adaptation, Learning and Optimization*, vol. 10, pp. 317-326.

Zhang, J.; Jin, X.; Sun, J.; Wang, J.; Sangaiah, A. K. (2018): Spatial and semantic convolutional features for robust visual object tracking. *Multimedia Tools and Applications*, vol. 79, pp. 15095-15115.

Zhang, J.; Wang, W.; Lu, C.; Wang, J.; Sangaiah, A. K. (2019): Lightweight deep network for traffic sign classification. *Annals of Telecommunications*.