A Heuristic Intrusion Detection System for Internet-of-Things (IoT)

Ayyaz-ul-Haq Qureshi(✉), Hadi Larijani, Jawad Ahmad, and Nhamoinesu Mtetwa

School of Computing, Engineering and Built Environment (SCEBE),
Glasgow Caledonian University, Glasgow G4 0BA, UK
ayyaz.qureshi@gcu.ac.uk

Abstract. Today, digitally connected devices are involved in every aspect of life due to the advancements in Internet-of-Things (IoT) paradigm. Recently, it has been a driving force for a major technological revolution towards the development of advanced modern computer networks connecting physical objects around us. The emergence of IPv6 and installation of open access public networks is attracting cyber-criminals to compromise the user specific security information. This is why the security breaches in IoT devices are dominating the headlines lately. In this research we have developed a random neural network based heuristic intrusion detection system (RNN-IDS) for IoTs. Upon feature selection, the neurons are trained and further tested at different learning rates with NSL-KDD dataset. Two methods are adopted to analyse the proposed scheme where the accuracy of RNN-IDS increased from 85.5% to 95.25%. Results also suggest that upon comparison with other machine learning algorithms, the proposed intelligent intrusion detection has higher accuracy in recognition of anomalous traffic from normal patterns.

Keywords: Intrusion detection systems · NSL-KDD · Machine learning · Random Neural Networks · Cyber-Security · IoT security

1 Introduction

To provide intelligent services to the end users, Internet-of-Things (IoT) provides a platform where information networks are seamlessly integrated into the physical ones. To impart such ubiquitous services, data collected from participating sensor nodes must be fused and analysed. There are number of security threats in the way of successful implementation trust management in IoTs [1]. In order to achieve the effective defence against cyber-attacks, the Intrusion Detection Systems (IDS) certainly perform a crucial task. Today, the wide use of computer aided programs and networks provide the low cost solutions to the end user problems in a short interval of time which has made the digital world

© Springer Nature Switzerland AG 2019
K. Arai et al. (Eds.): CompCom 2019, AISC 997, pp. 86–98, 2019.
https://doi.org/10.1007/978-3-030-22871-2_7

an integrated part of the physical world. Extensive usage of internet connected smart devices means that, massive data is shared among them which gives rise to vulnerabilities [2]. Hence, the need to secure the end user information is now higher than ever. The extent of research work in the field of computer security has increased many folds over last few decades but rapid attacks on networks has made the mitigation of network attacks a challenging task.

A system which acts as a front line defence against network intrusion must satisfy the principles of information confidentiality, integrity, and availability commonly known as CIA architecture [3]. Hackers pose serious threats to existing networks after bypassing these three components in a deceptive manner. Such occurrences has made the availability of Intrusion Detection Systems (IDS) a vital task [4]. As discussed above, an efficient IDS has to perform a critical role in order to ensure safety towards user information. Based on the practicality, IDS are classified as mis-used based (MIDS) and anomaly based intrusion detection systems (AIDS) [5].

The mis-used based intrusion detection systems (MIDS) which are commonly known as signature based IDS, use the existing signatures to analyse the incoming network traffic. These are the universally known attack patterns which are collected based on the type of protocols and applications used hence constantly need updation [6]. On the contrary, anomaly based intrusion detection systems (AIDS) use the classification approach to detect the malicious activity happening in the network [3].

Although there are various challenges involved in the successful deployment of AIDS, but several of them are categorised as follows:

1. Complexity in establishment of profiles to distinguish between normal and sceptical traffic patterns.
2. Irrelevant feature selection and incomplete datasets result in high false positive rates.
3. Platform dependencies decline the performance in real-time detection of anomalies.
4. Ineffective design results in redeployment of IDS which results in significant performance degradation.

There are a lot of approaches that have been used to develop the intrusion detection systems. After the proposition of theory of deep learning [7], the era of machine learning has been revolutionised. In this paper we tend to use classification techniques to detect the anomaly from normal traffic patterns. In [5], the authors have reduced high number of false positive rates and false negative rates in intrusion detection systems by developing a hybridised approach to estimate the optimal performance. Dataset is pre-processed with Information Gain and Vote Algorithm to extract usable features. The dataset is then used to train several classifiers. The authors concluded that detection time is significantly reduced while the accuracy increased using the hybrid approach for data dimensionality reduction. J48 outperforms all other classifiers in detection of malicious patterns in both binary class and multi-class of NSL-KDD dataset.

In [8], the authors have proposed a novel attack detection mechanism to achieve high accuracy and low false positives rates. In order to transform correlated features in the dataset, principle component analysis (PCA) has been used. Long Short-Term Memory based Recurrent Neural Network (LSTM-RNN) based model is implemented on tensor flow and results are compared with KNN, SVM, GRNN and PNN classifiers. The results shows that higher accuracy is achieved with low false positive alarms and high true positive rates with the overall precision of 99.46%. But this technique is more dependent upon types of features selected via PCA before feeding them to train input layer neurons.

As mentioned before, most of the times, the intrusion detection systems produce high false alarms due to inefficient and incompetent datasets. In [9], a detailed analysis of KDDCUP'99 dataset is done. Several machine learning classifiers such as J48, SVM, NB Tree, MLP, RF and RF Tree are trained using the dataset. Based on the low accuracy achieved, the authors concluded that original KDDCUP'99 has many limitation due enormous number of redundant records and uneven distribution of data. Hence, a new benchmark dataset NSL-KDD is proposed which increased the accuracy of classifiers and reduce the training time subsequently.

In [10], an Artificial Neural Network (ANN) based IDS is developed and trained with NSL-KD dataset. The IDS is tested for both binary class and multi-class attack types of NSL-KDD dataset which include U2R, R2L, Probe and DoS. ANN-IDS is trained with quasi-Newton back propagation (BFGS) and Levenberg-Marquart (LM) algorithms. Feature selection is done and model is trained for both reduced and full features on different number of input and hidden layer neurons for all attack types. Results reveal that although the detection rate for U2R and R2L attacks is very low, the model has produced accuracy of 79.9% and 81.2% for multi-class and binary class respectively.

Since the real world data is huge in quantity and classified as 'Big Data', deep learning solutions are required to analyse the incoming traffic for malicious activities. In [11] the authors have used deep learning to develop a Recurrent Neural Network based intrusion detection system (Recurrent-NN). NSL-KDD dataset is used to train the proposed model. Network is trained with different number of hidden layer neurons and learning rates for both binary-class and multi-class of the dataset. The performance of proposed model is compared with SVM, MLP, RF, Bayesian and several other machine learning architectures. The results revealed that recurrent neural network based IDS has surpassed all other classifiers. Although high accuracy is achieved for different attack classes but excessive training time and vanishing gradient remained the key problems for this scheme.

It is evident from literature that, intrusion detection has been performed from various machine learning algorithms. In this paper we propose a heuristic intrusion detection system for IOT paradigm using Random Neural Network [12] (RNN-IDS). NSL-KDD dataset is used for training the feed-forward neural network. Attributes are selected and data is normalised before its trained and tested against malicious attacks on network. Although RNN is substantially used in the deployment of Heating, ventilation, and air conditioning (HVAC) [13,14], occupancy detection [15] and pattern recognition [16] etc. but there is a lot of potential to use its features in the implementation of scalable intrusion detection systems.

The main contributions of this research are:

- A novel heuristic intrusion detection system for IoTs using random neural networks (RNN-IDS) has been developed and implemented.
- Enhanced performance is achieved by comparing the reduced and complete features of the NSL-KDD dataset.
- Critical comparisons are conducted after training the system with randomised data using a fixed number of hidden layer neurons and different learning rates.
- Performance of the proposed RNN-IDS has been compared with Support vector machine, naive bayes, J48 (decision tree), multi layer perception and various other ML methods.

Paper organization is outlined as follows: Sect. 1 provides introduction to the intrusion detection and discussed about past research findings. Section 2 presents basic understanding of RNN and Gradient Decent Algorithm. Section 3 outlines the methodology adopted to implements IDS. Results are discussed in Sect. 4 while Sect. 5 concludes the paper.

2 Background

This section covers the essential knowledge related to Random Neural Networks (RNN) and Gradient Descent Algorithm (GDA).

2.1 Random Neural Network Model

In the intention to replicate how human learns the information, Artificial Neural Networks (ANN) [17] came into existence which revolutionised the area of machine learning. Gelenbe proposed a new class of ANN and named it as Random Neural Network (RNN) [12].

In RNN model, neuron are connected to each other in different layers and have excitation and inhibition states depending upon the signal potential it receives. In a network if neuron encounters a positive $(+1)$ or negative (-1) signal, it goes into excited or inhibit state respectively. Sate of the neuron n_i at time t is shown as $S_i(t)$. Neuron n_i remains in idle state as long as value of $S_i(t) = 0$ and in order to get excitation signal, it changes to $S_i(t) > 0$ because $S_i(t)$ is always considered a non-negative integer.

Upon excitation, the neuron n_i transmits impulse signal towards other neuron n_j with rate of transmission h_i. The transmitted signal may reach neuron n_j with probability of $p^+(i,j)$ as a positive signal, or probability of $p^-(i,j)$ as a negative signal or it may also leave the network with probability of $k(i)$.

Where,

$$k(i) + \sum_{j=1}^{N} p^{+}(i,j) + p^{-}(i,j) = 1, \forall i, \tag{1}$$

Weights are updated on neuron n_i and n_j as:

$$w^{+}(i,j) = h_i p^{+} + (i,j) \geq 0, \tag{2}$$

and

$$w^{-}(i,j) = h_i p^{-} + (i,j) \geq 0. \tag{3}$$

To predict the probability of signals in RNN, Poisson distribution is used. Hence, for the neuron n_i, Poisson rate $\Lambda(i)$ demonstrates the positive signal whereas negative signal is depicted by Poisson rate $\lambda(i)$
Mathematically,

$$\lambda^{+}(i) = \sum_{j=1}^{n} e(j) r(j) p^{+}(j,i) + \Lambda(i), \tag{4}$$

$$\lambda^{-}(i) = \sum_{j=1}^{n} e(j) r(j) p^{-}(j,i) + \lambda(i). \tag{5}$$

The output activation function $e(i)$ for neurons can be written as:

$$e(i) = \frac{\lambda^{+}(i)}{h(i) + \lambda^{-}(i)}, \tag{6}$$

where $h(i)$ is the transmission rate, which can be calculated by combining Eqs. 1, 2 and 3:

$$h(i) = (1 - k(i))^{-}1 \sum_{j=1}^{N} [w^{+}(i,j) + w^{-}(i,j)], \tag{7}$$

In Eq. 7, since $h(i)$ is the gain of firing rate and the probabilities of positive and negative weights updated during training RNN model, hence it can also be written as:

$$h(i) = \sum_{j=1}^{N} [w^{+}(i,j) + w^{-}(i,j)]. \tag{8}$$

Interested reader can further understand the network operation in [12].

2.2 Gradient Descent Algorithm

Random Neural Network based Intrusion Detection System (RNN-IDS) proposed in this paper has been trained using Gradient Descent Algorithm (GD). It has been used to get the local minima of function so that overall mean square error can be reduced. Weights are updated and maximum training accuracy is achieved. This algorithm has been used by researchers for iterative optimization. Error function can be denoted as [18]:

$$E_p = \frac{1}{2}\sum_{i=1}^{n} \alpha_i (q_j^p - y_j^p)^2, \alpha_i \geq 0 \tag{9}$$

where $\alpha \in (0, 1)$ shows the state of output neuron i, also q_j^p is an actual differential function and y_j^p is the predicted output value. From Eq. 9, after training the neurons a an b, weights are updated as $w^+(a, b)$ and $w^-(a, b)$, derived as [18]:

$$w_{a,b}^{+t} = w_{a,b}^{+(t-1)} - \eta \sum_{i=1}^{n} \alpha_i (q_j^p - y_j^p)[\frac{\partial q_i}{\partial w_{a,b}^+}]^{t-1}, \tag{10}$$

similarly:

$$w_{a,b}^{-t} = w_{a,b}^{-(t-1)} - \eta \sum_{i=1}^{n} \alpha_i (q_j^p - y_j^p)[\frac{\partial q_i}{\partial w_{a,b}^-}]^{t-1}. \tag{11}$$

3 Methodology

In this research, random neural network has been adopted to develop the intrusion detection system. Like any other neural network architecture, RNN is also inspired by human brain in where nodes which referred to as neurons are connected with each other. The model consists of input, hidden and output layers. To start learning, selected features becomes the input to input layer neurons. After initiating the calculation of suitable weights and biases, input layer pass this data to the hidden layer for further transformation. Learning at hidden layer is important because it has to play a vital role in prediction of the output from actual features upon testing. Hidden layer then forward the information to output layer so that a feasible output is mapped.

The proposed scheme (Fig. 1) is developed by following steps:

Data Set. In order to verify the effectiveness of proposed intrusion detection scheme, NSL-KDD dataset has been adopted. It is the refined version of KDD-CUP'99 dataset which contains various unnecessary features. Due to the deletion of redundant records the classification is reported to be less biased. Detection rates with adopted dataset is significantly higher due to less presence of duplicate records. There are 41 features containing different attributes. Corresponding labels are assigned to each feature which categorise them as normal or an attack. The 42^{nd} feature contains information about various attack classes in dataset. These attacks are recognised as Denial-of-Service (DoS), User-to-root (U2R), Root-to-local (R2L) and Probe. Rest of the records are defined as normal patterns. In this research we are using *KDDTrain20* for training the classifier as it has good quantity of anomalous records. Further information about NSL-KDD can be found in Table 1.

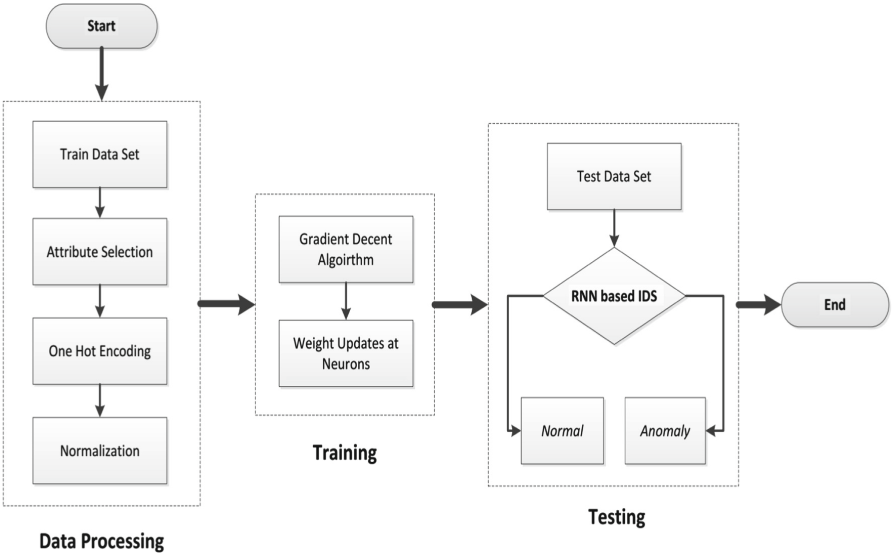

Fig. 1. Proposed RNN-IDS

Table 1. Description of dataset [6, 19]

NSL-KDD data	Data instances	Normal traffic	Attack traffic (%)
Train20	25,192	13,499	46.6
Train+	125,973	67,343	46.5
Test+	22,544	9711	56.9
Test-	11,850	2152	81.8

Attribute Selection. There are total 41 input features and 1 output class feature in data space of NSL-KDD dataset. Some of the features have low sample to feature ratio which can result in high false positive rates during classification. Also, excluding the less important features would enable us to train RNN-IDS faster whilst reducing the training time. In [20], has summarised features such as *dst_host_rerror_rate*, *su_attempted*, *num_access_files*, *num_file_creations*, *num_outbound_cmds*, *dst_host_count*, *is_host_login* and a few others which either have zeroed values or less feature space. 29 features are extracted using different feature reduction techniques. We are training the proposed scheme with reduced features as well as complete feature of NSL-KDD.

Pre-processing with Encoding. A few features in NSL-KDD dataset such as Flag, Protocol Type and Service are not numeric and contain label values. Since the proposed IDS would be trained and tested with RNN, hence all the remaining features must be converted into numerics before training. To achieve this task, we have used one hot encoding and converted all nominal values to integer values based on their existence in dataset.

Normalization. Data Normalization is a technique used for the transformation of input data where its occurrence is highly divergent. The data is restructured before it is utilized, because without such pre-processing the classifier take more than normal time to train the proposed IDS. Min-Max Normalization technique has been utilized in this research so that input value can be mapped between [0 and 1] range effectively.

It can be denominated as:

$$v_i = \frac{u_i - \min(u)}{\max(u) - \min(u)}, \tag{12}$$

where $u = (u_1, \ldots, u_n)$ is the number of input values and $v_(i)$ is the output normalized data.

4 Experimental Results and Analysis

In this research, the proposed a heuristic intrusion detection system for IOT environment using Random Neural Network (RNN-IDS), has been trained and tested in controlled environment using MATLAB installed on Intel Core(i5) processor and 16 GB RAM. The algorithm used for training the network is Gradient Descent (GD).

The IDS would be considered accurate in classification of anomalous records from normal records if it has low false positive rates and it predicts the outcome with high precision [2]. The accuracy of IDS is interpreted by True Positives (TP) which is denominated as α, True Negatives (TN) as β, False Positives (FP) as γ while False Negative (FN) as δ, respectively. The actual intrusion patterns in NSL-KDD and predicted attacks by RNN-IDS could be represented in the form of confusion matrix as outline in Table 2. Total accuracy of proposed scheme can be calculated as:

Table 2. Confusion matrix of attack sequence

		RNN Attack Prediction		
		p	**n**	**aggregate**
Actual Intrusion	p′	True Positive	False Negative	P′
	n′	False Positive	True Negative	N′
	aggregate	P	N	

$$Accuracy\,(RNN\text{-}IDS) = \frac{\alpha+\beta}{\gamma+\delta+\alpha+\beta} \tag{13}$$

In order to completely estimate the performance, some other matrices are:

$$Precision = \frac{\alpha}{\alpha+\gamma} \tag{14}$$

$$Detection\,Rate = \frac{\alpha}{\alpha+\delta} \tag{15}$$

$$False\,Discovery\,Rate = \frac{\gamma}{\alpha+\gamma} \tag{16}$$

For the comparison of results, with same number of hidden layer neurons as used in [10], two methods have been are adopted for training and testing RNN-IDS, where system is trained with varient learning rates of 0.01, 0.1 and 0.4, respectively.

Method I. In first method, as per last contribution, the reduced features as reported in [20] are used. RNN-IDS has 29 input layer neurons which are connected by 21 hidden layer neurons. Since its a binary classification and we want to predict anomalies after testing the system with *KDDTest+* dataset, we have 1 output layer neuron which would predict the attacks from normal traffic based on information it receives from hidden layer.

Method II. In second method, the complete 41 features of NSL-KDD dataset are utilized. Here we have 41 input layer neurons connected to 21 hidden layer neurons while 1 output layer neuron is used to quantify network attack. The network is trained with given dataset and tested against *KDDTest+*.

To completely demonstrate the performance of proposed scheme, Table 3 highlights the statistics collected against different performance metrics. The increase in number of true positives with change in learning rate for both methods is significant due to the fact that RNN-IDS has correctly quantified the intrusions from normal patterns. Also, the decrease in false positives indicates that the performance of intrusion detection system is improving with change in learning rate. It is evident from the previous findings, any system with low false positives is considered to be accurate and method II of proposed scheme has reduce false discovery rate to 0.09%.

Also, RNN-IDS model proved its robustness in Method-II, where the precision to detect anomalies from normal traffic is increased from 93.6% to 99.02%. Analysis of collected results suggested that, the decrease in learning rate gradually increased the detection of network attacks up-to 95%. This happened due to the fact that even though network would converge slowly, but learning algorithm is not missing any local minima in calculation of weights and biases for the neurons.

After training the system and testing it against desired *Test+* dataset, the results as shown in Fig. 2 make clear indication that the performance of RNN-IDS is more accurate in Method-II for the prediction of unknown attacks. As it

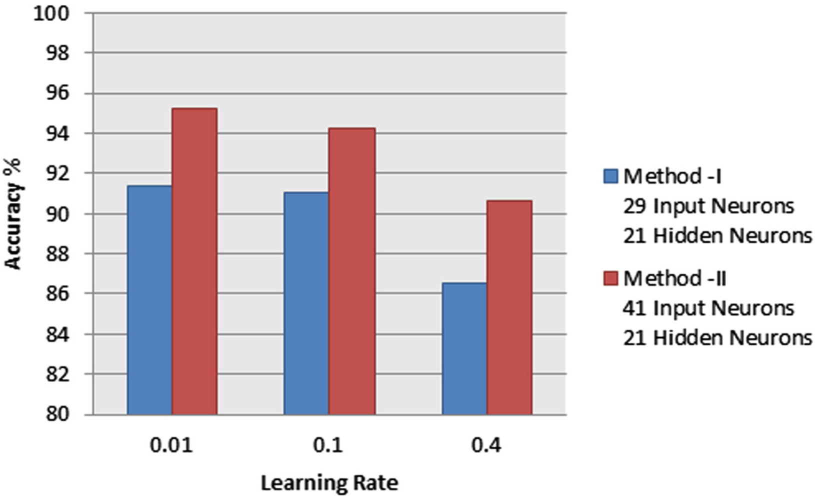

Fig. 2. Accuracy of proposed RNN-IDS model with different learning rates

Table 3. Results - RNN-IDS feature based comparison

Performance metrics	Learning rates					
	Method - I			Method - II		
	0.4	0.1	0.01	0.4	0.1	0.01
True Positive (TP)	91.72	93.36	94.24	93.96	95.68	95.58
True Negative (TN)	2.06	3.72	2.46	2.14	2.62	3.12
False Positive (FP)	6.24	2.94	3.32	3.92	1.72	0.92
False Negative (FN)	8.28	6.64	5.76	6.04	4.32	4.02
Detection Rate	91.7	93.3	94.2	93.96	95.6	95.90
Precision	93.6	96.5	96.6	96.0	98.2	99.02
False Discovery Rate	6.3	3.0	3.4	0.04	0.01	0.09
Mean Square Error	0.05	0.04	0.03	0.03	0.03	0.02
Accuracy	86.5%	91.0%	91.4%	90.6%	94.2%	95.2%

utilize full feature space and the total of 41 input neurons contributed to predict the anomaly.

In order to test the operation of proposed random neural network based IDS we have compared the results with different machine learning algorithms such as J48, Support Vector Machine (SVM), Naive Bayes (NB). Naive Bayes Tree, Multi Layer Perceptron (MLP), Random Forest (RF), Random Forest Tree, Recurrent Neural Network and Artificial Neural Network (ANN), respectively. Different performance matrices are used to estimate the overall efficiency of RNN-IDS such as detection rate, false negative rate, detection rate, precision,

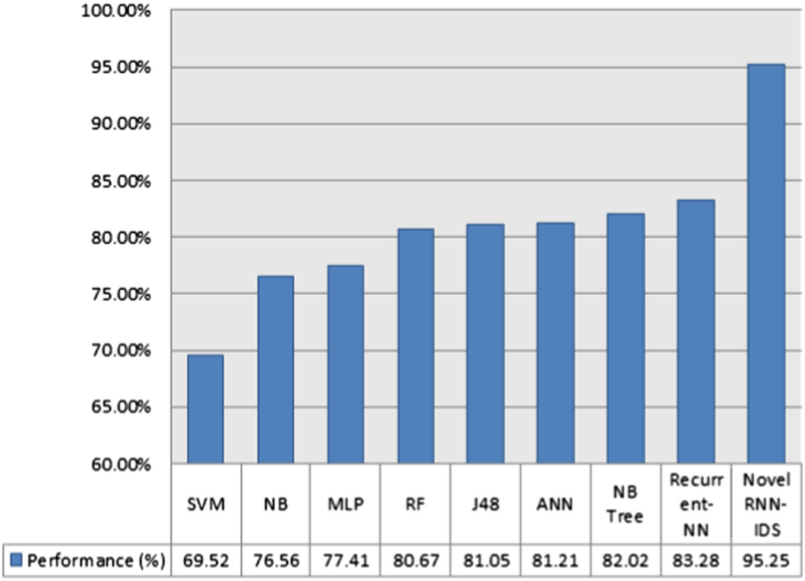

Fig. 3. Comparison of proposed RNN-IDS with several ML methods

false discovery rate and mean square error which would account towards the calculation of accuracy in detection of attacks. The results revealed that RNN-IDS has the highest accuracy of 95.2% for detecting novel attacks with next best of 83.2% in case of Recurrent Neural Networks.

Based on the results shown in Figs. 2, 3 and Table 3, the following facts can be inferred:

- Mean Square Error is decreased when learning rate is reduced. Although learning is slow but RNN-IDS has performed classification more accurately and false positives are reduced.

$$Mean\,Square\,Error = \frac{1}{n}\sum_{i=1}^{n}(\pi_{RNN} - \pi_a)^2 \tag{17}$$

  Where, π_{RNN} is the predicted intrusion based on trained RNN-IDS system while π_a is an actual intrusion.

- In comparison of reduced and complete features, the accuracy of RNN-IDS is increased from 86.5% to 95.25%, where it has classified intrusions in the network with high precision rate of 99.02%.
- The proposed RNN-IDS has performed many folds better than traditional machine learning algorithms such as J48, Support Vector Machine (SVM), Naive Bayes (NB). Naive Bayes Tree, Multi Layer Perceptron (MLP), Random Forest (RF), Random Forest Tree, Recurrent Neural Network and Arti-

ficial Neural Network (ANN), with higher accuracy and low false positive rates.

5 Conclusion

In this research we have proposed a novel intrusion detection system using the feed-forward nature of Random Neural Networks (RNN-IDS). Two methods were adopted to estimate the performance relating to different number of input, but identical hidden layer neurons. The proposed model was trained and further tested with NSL-KDD dataset. The comparison of empirical results trained with different learning rates revealed that RNN-IDS accuracy reached up to 95.2%. The performance is also compared with other machine learning algorithms such as J48, SVM, NB, NB Tree, MLP, RF, RF Tree, recurrent neural network and ANN, where proposed RNN-IDS scheme has surpassed all of them for the detection of anomalies in network.

References

1. Conti, M., Dehghantanha, A., Franke, K., Watson, S.: Internet of Things security and forensics: challenges and opportunities. Future Gener. Comput. Syst. **78**, 544–546 (2018). https://www.sciencedirect.com/science/article/pii/S0167739X17316667
2. Saeed, A., Ahmadinia, A., Javed, A., Larijani, H.: Intelligent intrusion detection in low-power IoTs. ACM Trans. Internet Technol. **16**(4), 1–25 (2016). http://dl.acm.org/citation.cfm?doid=3023158.2990499
3. Moustafa, N., Creech, G., Slay, J., Moustafa, N., Creech, G., Slay, J.: Big data analytics for intrusion detection system: statistical decision-making using finite Dirichlet mixture models (2017). https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/
4. Qureshi, A.U.H., Larijani, H., Ahmad, J., Mtetwa, N.: A novel random neural network based approach for intrusion detection systems. In: 2018 IEEE 10th International Computer Science and Electronic Engineering Conference (CEEC). IEEE, September 2018
5. Aljawarneh, S., Aldwairi, M., Yassein, M.B.: Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. J. Comput. Sci. **25**, 152–160 (2018). https://linkinghub.elsevier.com/retrieve/pii/S1877750316305099
6. Kwon, D., Kim, H., Kim, J., Suh, S.C., Kim, I., Kim, K.J.: A survey of deep learning-based network anomaly detection. Cluster Comput. 1–13 (2017). https://doi.org/10.1007/s10586-017-1117-8
7. LeCun, Y., Bengio, Y., Hinton, G.: Deep learning. Nature **521**(7553), 436–444 (2015). http://www.nature.com/articles/nature14539
8. Meng, F., Fu, Y., Lou, F., Chen, Z.: An effective network attack detection method based on kernel PCA and LSTM-RNN. In: 2017 International Conference on Computer Systems, Electronics and Control (ICCSEC), pp. 568–572. IEEE, December 2017. https://ieeexplore.ieee.org/document/8447022/

9. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A.: A detailed analysis of the KDD CUP 99 data set. Technical report. http://nsl.cs.unb.ca/NSL-KDD/
10. Ingre, B., Yadav, A.: Performance analysis of NSL-KDD dataset using ANN. In: 2015 International Conference on Signal Processing and Communication Engineering Systems, pp. 92–96. IEEE, January 2015. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7058223
11. Yin, C., Zhu, Y., Fei, J., He, X.: A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access **5**, 21 954–21 961 (2017). http://ieeexplore.ieee.org/document/8066291/
12. Gelenbe, E.: Random neural networks with negative and positive signals and product form solution
13. Javed, A., Larijani, H., Ahmadinia, A., Emmanuel, R., Mannion, M., Gibson, D.: Design and implementation of a cloud enabled random neural network-based decentralized smart controller with intelligent sensor nodes for HVAC. IEEE Internet Things J. **4**(2), 393–403 (2017). http://ieeexplore.ieee.org/document/7740096/
14. Javed, A., Larijani, H., Ahmadinia, A., Gibson, D.: Smart random neural network controller for HVAC using cloud computing technology. IEEE Trans. Ind. Inform. **13**(1), 351–360 (2017). http://ieeexplore.ieee.org/document/7529229/
15. Ahmad, J., Larijani, H., Emmanuel, R., Mannion, M., Javed, A.: An intelligent real-time occupancy monitoring system using single overhead camera. In: Proceedings of SAI Intelligent Systems Conference, pp. 957–969. Springer (2018)
16. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition, September 2014. http://arxiv.org/abs/1409.1556
17. Khan, G.M.: Artificial Neural Network (ANNs), pp. 39–55. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-67466-7_4
18. Ahmad, J., Larijani, H., Emmanuel, R., Mannion, M., Javed, A., Phillipson, M.: Energy demand prediction through novel random neural network predictor for large non-domestic buildings. In: 2017 Annual IEEE International Systems Conference (SysCon), pp. 1–6. IEEE, April 2017. http://ieeexplore.ieee.org/document/7934803/
19. NSL-KDD—Datasets—Research—Canadian Institute for Cybersecurity. http://www.unb.ca/cic/datasets/nsl.html. Accessed 03 May 2018
20. Bajaj, K., Arora, A.: Improving the intrusion detection using discriminative machine learning approach and improve the time complexity by data mining feature selection methods. Int. J. Comput. Appl. (975–8887) **76**(1) (2013). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.481.8435&rep=rep1&type=pdf