# A Modified Deep Neural Network Based Hybrid Intrusion Detection System in Cyber Security

**Thupakula Bhaskar, Tryambak Hiwarkar, K. Ramanjaneyulu**

***Abstract*: *In recent trends organizations are very much curious to protect data and prevent malware attack by using well flourished and excellent tools. Many algorithms are used for the intrusion detection system (IDS) and it has pros and cons. Here we introduced a new method of intrusion detection using Adaptive Jaya optimization (AJO) with modified deep neural network (MDNN) by hybrid optimization techniques such as Gravity search algorithm with gray wolf optimization (GSGW). In the proposed method modified deep neural network uses 4 hidden layers and has a low false alarm rate and a high detection rate. The performance evaluation is done by the feature selection in NSL-KDD dataset. In the proposed method the experimental result reveals less false alarm rate, better accuracy and high Detection when compared to previous analysis. This kind of IDS systems are used to develop extremely accurate in detecting and respond to malicious traffic/activities.***

***Index Terms*: *Intrusion Detection System, Modified Deep Neural Network, Adaptive Jaya Optimization, and Gray Wolf Optimization.***

## I. INTRODUCTION

Nowadays, Internet has become a crucial part in various organization to survive technological terms. Almost customers share their personal information through networks and also many firms depends on the internet for their daily business [1]. Cyber-attacks means the interruption of computers usual working and loss of an important data via malicious network actions remain fetching more extensive [2]. Intrusion detection (ID) is a method of detecting, discerning and analysing the actions as destruction to the policies related to security of a network environment [3] [4]. Denning presented the idea of identifying attacks in the cyber system on networks through an outline to intrusion detection system (IDS), which depends on the theory that security damages could be sensed through an audit records in monitoring system for abnormal designs of system usage [5]. NIDS (Network Intrusion Detection Systems) are characterized as follows: i) anomaly detection based NIDS (ADNIDS) ii) signature (misuse) based NIDS (SNIDS). In NIDS, Snort [1], attack signatures are pre-installed. To detect an intrusion, a pattern matching is presented for signatures related to traffic in the network [6], Usually, IDS are established for anomaly detection or signatures. In the detection of signatures, audit logs or packets are scanned for series looking of instructions or proceedings which are formerly indomitable as suggestive of an attack. In anomaly detection, IDS use performance designs and it represents malicious activities and examines past actions by recognizing whether the detected performances are normal [7]. While mentioning to IDS, two major classes are distinctly highlighted. They initially describe a profile for ‘‘behaviour related to normal’’, and then notice variations in attacks from this normal profile [8] [9].

**Revised Manuscript Received on June 07, 2019**.

**Thupakula Bhaskar**, Research-Scholar, Department of Computer Science and Engineering, Sri Satya Sai University of Technology & Medical Sciences, Bhopal, M. P. India.

**Dr.Tryambak Hiwarkar**, Professor, Department of Computer Science and Engineering, Sri Satya Sai University of Technology & Medical Sciences, Bhopal, M. P. India.

**Dr.K. Ramanjaneyulu**, Professor, Department of ECE, Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, A. P. India.

## II. RELATED WORKS

Alex Sheffield et al. (2018) [10] proposed a new approach for deep packet detecting malicious traffic on network employing artificial neural networks which was used in packet analysis based on intrusion detection systems. This method can provide accurate difference between the malicious and benign network by making use of code sets of malicious shell obtained from the available exploit, susceptibility depository exploit and some of the traffic datasets of benign network (dynamic link library files, images for selecting some other diverse files such as music files, word processing documents and logs.). The maximum accuracy obtained by this method was 98% and maximum area obtained from the recipient operand characteristic curve was 0.98 and the average false positive rate for repeated 10-fold cross validation was 2% less. This method was more precise and robust and has the ability to increase the usage of intrusion detection system which was provided to both the traffic analysis network and conventional traffic network analysis used in cyber systems like smart grids. Chuanlong Yin, et al. (2017) [11] discovered a replacement methodology for intrusion detection system supported deep learning, and intrusion was detected recurrent neural networks (RNN-IDS).The performance of this model was studied in multiclass classification and binary classification, and therefore the variety of neurons and various learning rate effects on the performance of the projected model was also noted. Our model was compared with support vector machine, random forest, artificial neural network, J48, and a few alternative machine learning ways that were projected on the benchmark data set by past workers.

The result of this methodology shows that the RNN-IDS was used for modifying the classification model, wherever the accuracy was high whereas comparison with the previous ways that use multiclass and binary classification. Accuracy was improved by RNN-IDS in instruction detection that provides a replacement exploration technique for instruction detection.

## III. MOTIVATION AND PROBLEM DEFINITION

Internet is fashionable among variety of users and numerous cyber-attacks are generated against internet. A quick and economical cyber security intrusion detection may be a major recent analysis challenge because of the increasing usage of Internet primarily based services. Great deal of information are on the market in cyber infrastructure and additionally the cyber criminals are hyperbolic to realize access to the information, so we need, machine learning statistics, data processing and alternative knowledge base capabilities to face the challenges of cyber security. The aim of intrusion detection analysis is to beat the drawbacks of existing approaches in Internet security. High detection time, low accuracy and low flexibility are the common drawbacks of intrusion detection approaches. Advanced features used by intruders such as IP address spoofing, encrypted payload and dynamic ports which should be determined before any losses occur. In the above literature, some techniques detect only known attacks and some approaches learns normal behaviour from network traffic dataset. Machine learning based intrusion detection system faces problem in whole dataset because of its size and imbalanced character which results in biased performance and over-fitting. So it is needed to diagnose intrusion from intruder by proper feature learning.

## IV. PROPOSED METHODOLOGY

In this proposed methodology, we recommend an efficient intrusion detection framework with adaptive Jaya optimization (AJO) [12] to concurrently do parameter Initialization and feature selection for modified Deep Neural Network (MDNN). MDNN classifier is presented to classify the various kinds of attacks in cyber security.

### 4.1 FLOWCHART OF THE PROPOSED SYSTEM

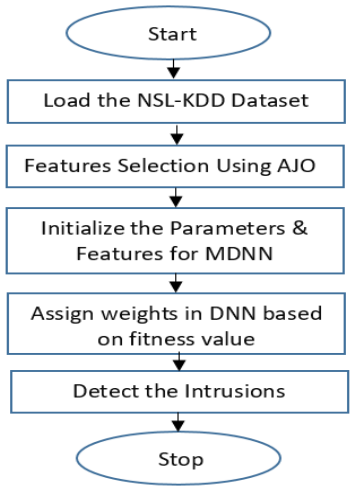


Figure1: Flow Chart of System

In the proposed System the features are selected from the NSL dataset using Adaptive Jaya optimization. The GSGW is used to calculate the fitness value and is applied to the Modified deep neural network to detect the intrusion. In the proposed system we use the NSL-KDD dataset. The fig1 shows the flow of the proposed system. Initially the data is loaded and the best features among the data is selected by using Adaptive Jaya optimization technique. In modified deep neural network it comprises input layer, four hidden layers and output layer. The increasing number of hidden layer produces better performance in the output. In each layer of the modified deep neural network a weight value is assigned based on the fitness value calculated for the particular layer. The fitness value is calculated by using hybrid Gravity search Algorithm with Gray wolf optimization (GSGW) and the modified deep neural network process the input values for all the four hidden layers and produce better output. By using the proposed system the performance in detection rate is increased and produces less false alarm rate.

### 4.2 MODIFIED DEEP NEURAL NETWORK

Neural network is termed as deep learning of a process and is composed of one hidden layer and modified deep neural network has several hidden layers. The use of multi-layer can provide better performance in the output. The layers consist of nodes and the nodes are termed as neurons in human brain. The node accept the input and process to obtain the final output. In each layer the weighted value is randomly selected based on the fittest value calculated by hybrid gravity search algorithm with gray wolf optimization (GSGW)[13].Deep neural networks are used in common places with hidden layers and these layers are known to be the depth of the network for the better pattern recognition. In olden layers the neural network with single layers but now with three layers are termed as deep neural network and with more layers are known as modified deep neural network. In this, the input is the selected best features in NSL-KDD dataset by using Jaya optimization.

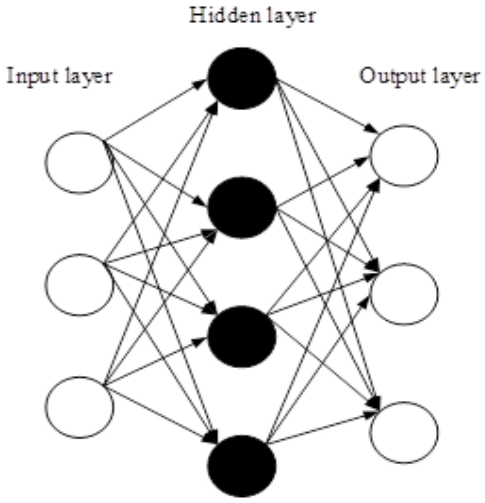


Figure 2: Neural Network Architecture

The figure2 represents the neural network with single hidden layer. In the modified deep neural network let M denotes the quantity of layers. The layer one is termed as input layer and therefore the layer m is termed as output layer. The mediate hidden layers are painted as layer2 and layer M-1. The value of every node is calculated by multiplying the value with the load W1,W2…Wm. The load is updated within the modified deep neural network by exploitation (GSGW).The values for every node is denoted as Ci,j. The process is recurrent for every layer and therefore the values are calculated. The load for every layer won't be of zero entities. The network is of totally connected is shown in figure 3.

The formula used to calculate the attacks in the modified deep neural network is termed as

$$H = f(G_1^1 Z_1 \mid G_1^2 Z_2 \mid G_1^3 Z_3 \mid .....G_1^m Z_m)$$

$$H = f(\sum\nolimits_j G_i^j Z_j)$$

G represents the load allotted to the link between the layers and Z represents the neurons present within the network.

The softmax function is applied to each hidden layers in the modified deep neural network. The values are calculated by using the formula

$$P(y = j \mid \theta^i) = \frac{e^{\theta(i)}}{\sum_{j=0}^{k} e^{\theta_k(i)}}$$

Where $\theta = W_0 X_0 + W_1 X_1 + ..... + W_k X_k$

$$\theta = \sum_{i=0}^{k} W_i X_i = W^T X$$

The value is calculated for each and every neurons present in the hidden layer and is represented as $Y_i$, $e^{\theta_k(i)}$.

### 4.3 EXPERIMENTAL SETUP

In this proposed system, We used anaconda tensor flow platform for implementing MDNN (Modified Deep Neural Network) Technique. Process Flow the same is mentioned below.

Step 1: The databases which we used for intrusion detection is collected from network traffic dataset.

Step 2: Next, data analytic method is enhanced by developed algorithms for obtained dataset. For that, the dataset should be separated into training and testing. In this paper we have used 125973 training samples and 22543 testing samples of NSL –KDD Dataset for MDNN (Modified Deep Neural Network) implementation.

Step 3: Adaptive Jaya Optimization (AJO) to simultaneously do parameter setting and feature selection. As a result, the Adaptive Jaya optimization better the searching ability, as well as reducing the number of the searching agents, number of iterations and computational burden.

Step 4: MDNN classifier is proposed to classify the different security attacks. The weight values are updated using Gravity Search Algorithm with Gray Wolf Optimization (GSGW) to minimize the classification error. This MDNN classifier takes into account trade-off between the maximizing the detection rate and minimizing the false alarm rate with better accuracy.

The feature selection is performed on 41 features and best 17 features were selected on best score after 24th iteration. Every iteration least score feature was eliminated. The below MDNN Classifier Architecture will give sample calculation of each layer to classify 4 types intrusions like Probe,DoS,U2R,R2L attacks.

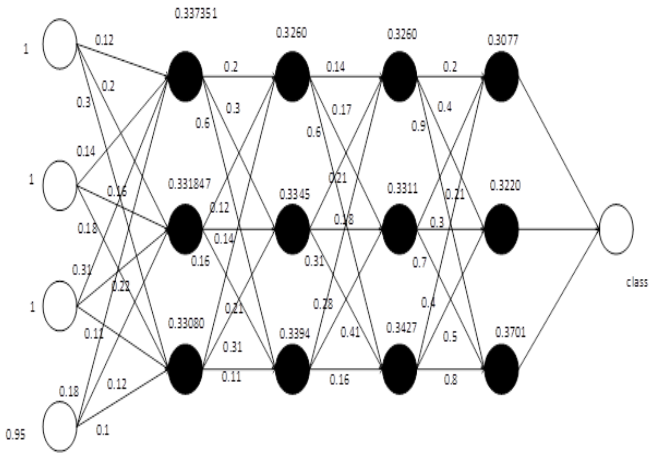


Figure3: Modified Deep Neural Network Classifier

The figure3 represents the modified deep neural network with four hidden layers. The inclusion of many hidden layers produce better performance. The fitness value calculated by GSGW is 0.35 is used for the above calculation and is multiplied with the assigned weight of range [0, 1]. Mathematical Calculation in Different Layers is as follows:

For the first hidden layer

**1.**
(1*0.12*0.35)+(1*0.14*0.35)+(1*0.31*0.35)+(0.95*0.18*0.35)= 0.25935

**2.**
(1*0.2*0.35)+(1*0.16*0.35)+(1*0.22*0.35)+(0.95*0.12*0.35)= 0.2429

**3.**
(1*0.3*0.35)+(1*0.18*0.35)+(1*0.11*0.35)+(0.95*0.1*0.35)= 0.23975

The exponential of each value

1. Exp(0.25935) = 1.296087
2. Exp(0.2429 ) = 1.274941
3. Exp(0.23975) = 1.270931

---

Sum = 3.84196

Calculate the softmax value as follows:

1 1.296087/3.84196=0.337351
2 1.274941/3.84196=0.331847
3 1.270931/3.84196=0.330803

The same way calculations can be done for other hidden layers of Modified deep neural network. Neural networks are designed to recognize patterns as the work done by the human brain. As the human brain understand the data the neural network interpret the data by machine learning. It can understand text, sound, image recognition. The neural network helps to cluster and classify the data.

## V. RESULTS AND DISCUSIONS

The MDNN (Modified Deep Neural Network) methodology produces better Detection Rate (DR), low False Alarm Rate(FAR) and high accuracy.IDSs have Four Major classes of attacks:

Probe: The intrusion will scan the network to accumulate data about the system.

Denial of service (DoS): The intrusion makes the machine unavailable to the user by engaging resources.

User to root (U2R): The intrusion access the root as normal and then attack the system privilege.

Remote to user (R2L): The intrusion try to access the remote by sending packets through network and then exploit the machine .The intruder do not have an account in the local system.

Fig 4 describes the frequency of the selected features used in the proposed system as it is described in table7. The x-axis represents the selected features from NSL- KDD dataset using AJO.

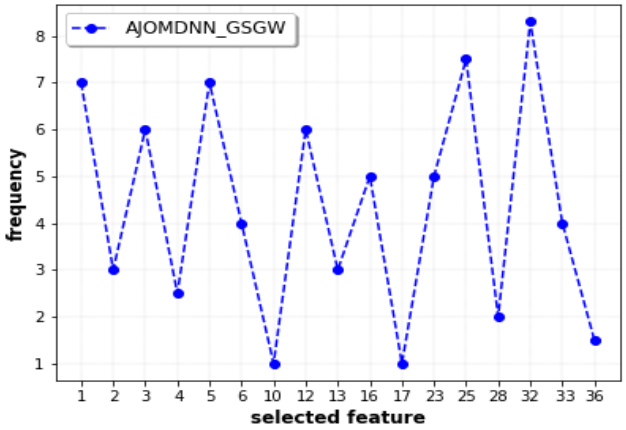


Figure 4: Feature selection using AJO

Fig5 reveals the best features selected in our proposed system from NSL-KDD dataset using AJO Technique.

| | |
|---|---|
| Basic features | {1,2,3,4,5,6} |
| Content features | {10,12,13,16,17} |
| Features of Time based traffic | {23,25,28} |
| Features of Host based traffic | {32,33,36} |

Figure 5. Selected Features by AJO

The Fig 6 reveals the performance evaluation of the detection rate,false alarm rate and accuracy of our proposed system without feature selection and with feature selection.

We got the following details without feature Selection Accuracy 99.71 and with (AJO Technique) feature selection Accuracy is 99.87.Following formulas used in the system.

FAR= ((FP+FN)/ (TP+TN+FN+FP))*100

DR = (TP/ (TP+FP))*100

ACC = (TP+TN)/ (TP+FP+FN+TN)*100

Actual samples of various attacks in our Dataset are:

9698+7448+219+2756+2422= 22543

FP Values: [14 11 18 13 15]

FN Values: [26 19 1 11 14]

TP Values: [9684 7437 201 2743 2407]

TN Values: [12819 15076 22323 19776 20107]

FAR Value: ((14+26)/ (9684+12819+26+14))*100

0.17743867275872777

Like the same way for all classes (Attacks) values were calculated. Finally we got below results mentioned in fig: 7 with feature selection comparing with existing system.

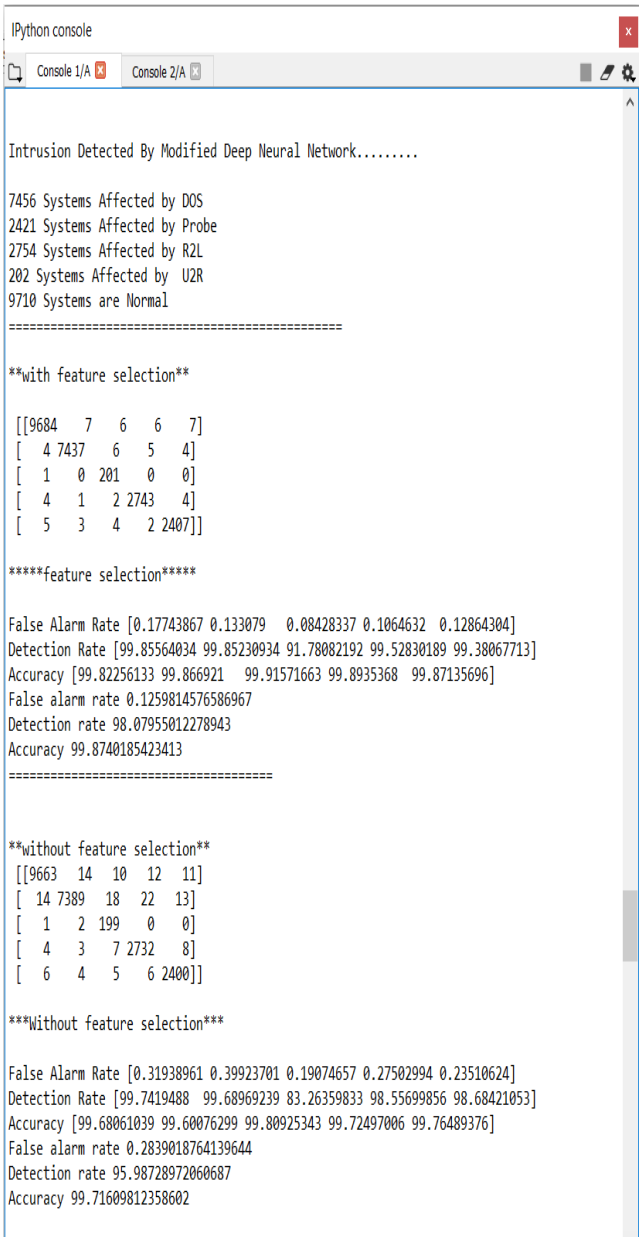


Figure 6: Screen shot of MDNN Implementation

| | Existing System | Proposed System |
|---|---|---|
| FAR | 2.41 | 0.125 |
| DR | 97.23 | 98.07 |
| Accuracy | 96.88 | 99.87 |

Figure 7: Compare Results with Feature Selection

The Fig 7 disclose the results between existing system (TVCPSO -MCLP) [1] and proposed (Modified Deep Neural Network Based) system.

## VI. CONCLUSION AND FUTURE WORKS

In this paper the proposed methodology includes an intelligent intrusion detection context with Adaptive Jaya Optimization (AJO) to concurrently initialize parameters and features selection for Modified Deep Neural Network (MDNN). MDNN classifier is presented to classify the various kinds of attacks in cyber security. Here we used 17 best features from KDD cup data set for high DR and low FAR. In future work a new set of features can be selected by using another technique for even better performance.

## ACKNOWLEDGMENT

"**A Machine Learning Based Hybrid Intrusion Detection System in Cyber Security**" has been a subject with tremendous scope to research upon, which leads to explore new heights in the field of Computer Science & Engineering, and its miscellaneous applications. I 'm thankful to my Research guide: Dr.Tryambak Hiwarkar & Research Co-guide:Dr.K. Ramanjaneyulu whose guidance helped me to work successfully. Their guidance will always encourage me to do work perfectly and professionally.

## .REFERENCES

1. Bamakan, Seyed Mojtaba Hosseini, Huadong Wang, Tian Yingjie, and Yong Shi. "An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization." Neurocomputing 199 (2016): 90-102.
2. Ben-Asher, N. and Gonzalez, C., 2015. Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, pp.51-61.
3. Ashfaq, R.A.R., Wang, X.Z., Huang, J.Z., Abbas, H. and He, Y.L., 2017. Fuzziness based semi-supervised learning approach for intrusion detection system. Information Sciences, 378, pp.484-497.
4. Masud, Mehedy, Bhavani Thuraisingham, and Latifur Khan. Data mining tools for malware detection. Auerbach Publications, 2016.
5. Xia, H., & Hoi, S. C. (2013). MkBoost: A framework of multiple kernel boosting. IEEE Transactions on Knowledge and Data Engineering, 25(7), 1574–1586.
6. I. Syarif, A. Prugel-Bennett, and G. Wills, "Unsupervised Clustering Approach for Network Anomaly Detection," in Networked Digital Technologies, pp. 135–145, Springer, 2012.
7. Lin, W.C., Ke, S.W. and Tsai, C.F., 2015. CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-based systems, 78, pp.13-21.
8. Elhag, S., Fernández, A., Bawakid, A., Alshomrani, S. and Herrera, F., 2015. On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems. Expert Systems with Applications, 42(1), pp.193-202.
9. Kevric, J., Jukic, S. and Subasi, A., 2017. An effective combining classifier approach using tree algorithms for network intrusion detection. *Neural Computing and Applications*, *28*(1), pp.1051-1058.
10. Chen, H.-J., Yang B., Wang, S.-J., Wang G., Liu, D.-Y., Li, H., and Liu, W.-B. Towards an optimal support vector machine classifier using a parallel particle swarm optimization strategy. Applied Mathematics and Computation, 239:180– 197, 2014.
11. Yin, C., Zhu, Y., Fei, J. and He, X., 2017. A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, pp.21954-21961.
12. R. Venkata Rao Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems. International Journal of Industrial Engineering Computations 7 (2016) 19–34
13. E. Emary, Hossam M. Zawbaa, and Crina Grosan Experienced Gray Wolf Optimization through Reinforcement Learning and Neural Networks. IEEE transactions on neural networks and learning systems, vol. 29, no. 3, march 2018

## AUTHORS PROFILE

**Thupakula Bhaskar** is currently a PhD student in Sri Satya Sai University of Technology & Medical Sciences, Bhopal, M.P., and India. He received his M.Tech (CSE) from JNTU Hyderabad, India in 2011. His current research interests include Machine Learning, Deep Learning and Cyber security. He has presented and published more than 20 papers at National and International level.

**Dr.Trayambak Hiwarkar** was born in Maharashtra, India in 1965. He received the B.Tech (1994), M.tech (1996) & Ph.D. Degree (2003) in CSE from Bundelkhand University Jhansi. He was published many papers in National / International level Journals. He has life memberships in IEEE, ACM, Institution of Engineers (India), MCSI, IETE and many more etc.

**Dr.K.Ramanjaneyulu** received the Ph.D. degree from CoE, Andhra University, Visakhapatnam, Andhra Pradesh, India, in 2012. He is currently working as professor in PVPSIT,Vijayawada,AndhraPradesh,India.He was published 18 papers in National and International Journals and 22 papers presented in various conferences National and International level.