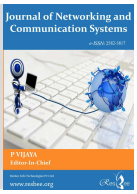
Vol.4 No.2 April 2021

Journal of Networking and Communication Systems

Received 19 December, Revised 24 February, Accepted 20 March



Deep Learning based Optimization algorithm for Cyber Security Intrusion Detection System

Manasi Gali
Georgia Institute of Technology, Georgia
manasigali10@gmail.com

Abstract: In several networks, intrusion detection plays an important role in assuring cyber security. Numerous studies deal with various cyber attacks in the data via modeling several supervised techniques; however, they have not considered the database size at the time of the optimization. As the size of data increases exponentially, it is vital to cluster the database ahead of detecting the intruder presence in the system. To overcome these confronts, and therefore this paper developed Enhanced Gravitational Search Algorithm – Adaptive Particle Swarm Optimization Algorithm (EGSA-APSO) optimization technique. With the optimization algorithm, the database is clustered into various groups by the developed Intrusion Detection System (IDS) as well as it detects the intrusion presence in the clusters with the employ of the Hyperbolic Secant-based Decision Tree (HSDT) classifier. Subsequently, to the Deep Neural Network (DNN), the compacted data is subjected and train with the optimization method to identify the intrusion detection in the whole database. The experimentation of the developed optimization technique is performed by exploiting several measures such as True Positive Rate (TPR), accuracy, and True Negative Rate (TNR), the outcomes exhibit a superior performance over the conventional models.

Keywords: Classifier, Cluster, Cyber Security, Database, Intrusion Detection

Nomenclature

Abbreviations	Descriptions
MTTC	Mean Time To Compromise
FPR	False Positive Rates
DI&C	Digital Instrumentation And Control
ADFA-LD	ADFA Linux
TNR	True Negative Rate
CFA	Cuttlefish Algorithm
ML	Machine Learning
TPR	True Positive Rate
FGLCC	Feature Grouping Based On Linear Correlation Coefficient

1. Introduction

In network security despite the considerable advancements, the conventional solutions are not capable to totally defend computer networks over malicious threats. The conventional security approaches namely user authentication, firewalls as well as data encryption are not able to adequately fulfill the protection of the network security because of the rapid advancement of intrusion approaches. Hence, novel defense models namely IDS are recommended to assist the security of the system.

In the computer infrastructures, attacks are becoming a more and more severe issue. Computer security is stated as the fortification of computing systems over threats to integrity, confidentiality, as well as availability. Confidentiality refers that information is disclosed only consistent with policy, integrity means that information is not corrupted or destroyed and that the system performs properly, availability refers that system services are available when they are required [4].

IDS are a segment of the second defense line of a system. Besides with the IDS can be deployed with security metrics namely authentication techniques, access control, and encryption models to superior secure the system over cyber attacks [1]. By exploiting the patterns of normal behavior or particular rules which describe the attacks.

https://doi.org/10.46253/jnacs.v4i2.a4

IDS can be differentiated amid normal as well as malicious actions. In general, IDS can be categorized into two classifications such as anomaly as well as signature-based detection models. By matching predefined attacks signature, the signature-based approaches detect anomalies. The most important benefits of these techniques are their low FPR, simplicity but they are not capable to detect new mimicry attacks [11]. Generally, Cybersecurity IDS needs an effectual real-time saving as well as the processing of the higher network traffic data size and verifies to recognize malicious network traffics [2] [3].

The data mining is exploited to model the knowledge discovery that can aid to deployment as well as implement the IDS with high accuracy as well as robust behavior as evaluated with the conventional IDS which might not effectual over the new sophisticated cyber attacks. Numerous studies were conducted and exhibit that the methods possess some disadvantages to valid the datasets to examine and analysis and also appropriate dataset was important confronts [10].

The main objective of this paper is to detect the intrusion in the networks, at first; this research exploits the EGSA-APSO algorithm. The developed optimization method serves as a clustering approach to divide the database into various groups. Subsequently, the developed optimization method is exploited to train the weights of the DNN model to provide information regarding the attendance of intrusion in the data.

2. Literature Review

In 2020, Mohamed Amine Ferrag et al [1], presented are view based on the deep learning techniques for cybersecurity IDS. Particularly, a study regarding the IDS on the basis of the deep learning techniques was provided. Moreover, the dataset in IDS, plays a significant role, hence, a classification regarding the dataset was presented. Seven kinds of deep learning approaches were analyzed in the experimentation scenario.

In 2018, Chanyoung Lee et al [2], developed a quantitative technique to evaluate the effectiveness of the security controls for DI&C on the basis of intrusion tolerant ideas. Here, the intrusion tolerant concept was applied to the experimentation technique due to the accessibility of the systems secure functions were modeled. Here, to calculate the abstract variables, the MTTC was exploited.

In 2017, Govind P Gupta and Manish Kulariya [3], developed a model in that initially a renowned feature selection approach was exploited to select the very significant features, subsequently, classification based IDS was exploited for the rapid as well as the effectual detection of the intrusion in the massive network traffic. Here, two renowned feature selection approaches such as Chi-squared feature selection as well as correlation-based feature selection were exploited.

In 2015, Adamu I. Abubakar et al [4], worked on the current advances in the exploit of cybersecurity benchmark datasets for the analysis of the ML and data mining-based IDS. Moreover, the new ADFA-LD was exploited, which needs enhancements regarding the complete descriptions of its attributes. Moreover, this paper exploits the preceding studies regarding the cybersecurity benchmark data sets, which was an effectual and robust analysis of ML and data mining-based IDS.

In 2019, Sara Mohammadi et al [5], developed an IDS on the clustering as well as feature selection approaches by exploiting the wrapper as well as filter techniques. The CFA, and Filter, and wrapper methods are named FGLCC approaches were exploited for both wrappers as well as filter techniques. Additionally, the decision tree was exploited as the classifier.

3. Proposed model for Intrusion Detection System in the Network

In this paper, the developed IDS are used to identify the intrusion presence in the system, and it offers cybersecurity for the network users.

The network comprises various users, as well as they, have to communicate with each other serve or user with the employ of the authentication key that is presented by the network server. To the network, the intruders try to enter, and also they will attempt to hack or steal the information which is available in the database. The developed IDS system identifies the intruder presence in the network by adopting the DNN technique and the weights are trained by the DNN model using the EGSA-APSO technique. At first, to the clustering, the database is fed by means of the developed optimization technique as the database available in the network possesses a higher size. Subsequently, the technique exploits the HSDT classifiers to detect the intrusions presence within the cluster and the information of intrusion from each cluster is gathered together to make the compact data. Fig 1 demonstrates the architecture model of the proposed method.

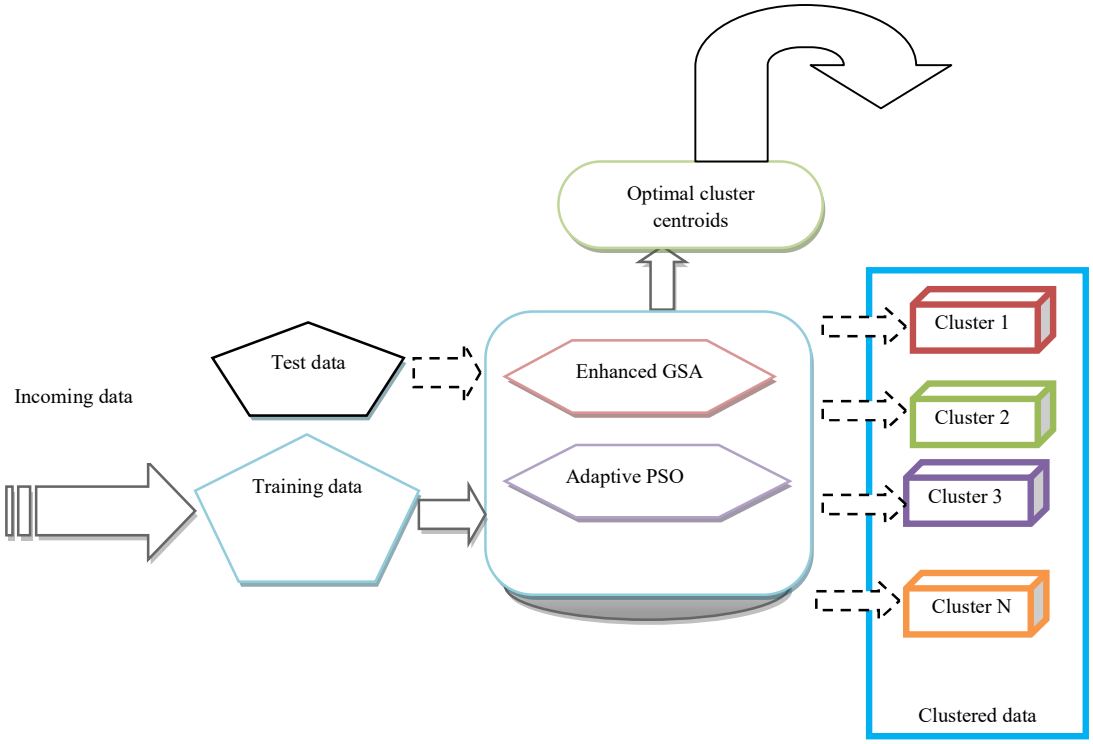


Fig. 1. *Architecture model of the proposed model*

Moreover, to present the ultimate intrusion/information class the DNN is exploited in the compact data, as well as this is performed DNN weights are trained using the developed optimization algorithm.

3.1. Proposed Optimization model for clustering the data

Let the network possess each user pass over Q data samples, Y indicates the count of users in the network. From each user, the data is gathered, I represents the database is modeled, and therefore, I possesses size of $Y \times Q$. The data perform over the network, which posse's higher size, and therefore, the intrusion detection in the higher database I is a complex procedure. Therefore, this paper clusters the database into N number of clusters using the developed optimization approach to minimize the IDS complexity. Here, the developed optimization approach performs as a clustering approach to group the database into N clusters, each of size $\mathbf{1} \times Y$ and the clusters formulation from the proposed model is stated as below,

$$I = \{X_{\mathbf{1}}, X_{\mathbf{2}}, \ldots, X_i, \ldots, X_N\} \tag{1}$$

where X_i refers to the data in the i^{th} cluster

3.2. Proposed Enhanced GSA and adaptive PSO

(i)Enhanced GSA

The agent velocity value in eq. (2), because of the arbitrary number, creates the agent oscillates and moves exterior the search space and therefore in [7]developed restricts for the velocity of the agent to indicate the enhanced GSA:

$$v_i(k+\mathbf{1}) = r \times v_i(k) + a_i(k) \tag{2}$$

$$-v_{max} \le v_i \le v_{max} \tag{3}$$

$$v_{max} = \sigma(x_u - x_l)\left[\mathbf{1} - \left(k/k_{max}\right)^{\rho}\right] \tag{4}$$

Whereas, v_{max} indicates the maximum velocity of the agent, ρ, σ indicates the positive constants less than equivalent unity, x_u, x_l indicates the upper as well as lower limits of the agent. The eq. (4), the utmost velocity decreases with maximizing the iteration number, and therefore the agent's exploitation fades, when their exploration fades out.

(ii) Adaptive PSO

For adaptive and superior PSO [6] approach, the coefficients c_1 c_2 vary linearly with iteration number in such a fashion that c_1 ; x decrease when c_2 increases with the iteration number k as:

$$c_1 = c_1^{max} - \left(c_1^{max} - c_1^{min} \right) \left(k / k_{max} \right) \quad (5)$$

$$c_2 = c_2^{max} - \left(c_2^{max} - c_2^{min} \right) \left(k / k_{max} \right) \quad (6)$$

$$\omega = \omega^{max} - \left(\omega^{max} - \omega^{min} \right) \left(k / k_{max} \right) \quad (7)$$

whereas max and min indicates the maximal and maximal values of the parameter. The adaptive PSO routine continues till the halting condition is attained.

3.3. HSDT classifier for Decision Tree

In this paper, the HSDT classifier is exploited to identify the intrusion presence in eachcluster, which is recognized to model the optimization approach. The HSDT classifier exploits the secant entropy function to modify the functional tangent probability used in this paper [8]. Based on the hyperbolic secant function, the entropy function is stated as below:

$$fn\left(prob^i \right) = \frac{1}{2}\left[\log\left(prob^i \right) - 2 aSech\left(prob^i \right) \right] \quad (8)$$

whereas, $aSech(.)$ indicates hyperbolic secant function for the HSDT classifier. On the basis of the entropy function values which are stated in the eq. (8), for each cluster data, the decision tree is modeled. Thisproduces the needed intrusion information in every cluster.

3.4 Compact data Generation

The HSDT classifier presents the information regarding the intrusion presence in each cluster on the basis that the compact data is modeled. The compact data consists of each HSDT classifier output present in the cluster. The formulation of the compact data is stated as below,

$$F = \{F_1, F_2, \ldots, F_i, \ldots, F_N\}; 1 \le i \le N \quad (9)$$

whereas F_i indicates the information regarding the intrusion presence in the cluster i as stated using the HSDT classifier, and N indicates the total number of clusters.

4. Integration of both Optimization Model and DNN for IDS

In this section, the model of DNN is presented beside the optimization approach to identify the intrusion presence within the database.

4.1 DNN model

The DNN training is on the basis of the back-propagation approach [9]. Individually, training classifier instances checks the current NN settings are accurate. For an instance, if the prediction is similar to the true label, nothing is altered.

If the samples are misclassified, the NN weights require to be updated. The back-propagation approach is performed hierarchically.

Initially, the weights update in the output layer and subsequently proceed to the subsequent shallow hidden layer. During this procedure, each output neuron error is allocated to every hidden neuron. In general, it requires numerous iterations to regulate the weights to attain the optimum.

The ReLU is exploited as an activation function. Additionally, it is named the Rectified Linear Unit, which is a piecewise linear function that recompenses for the vanishing of the Sigmod function gradient and Tanh function. The ReLU computation is stated as Eq. (10).

To choose ReLU, there are two causes are present. Generally, the feature exploited in this paper is the first few packets size. Therefore, there is no gradient disappearance issue while the inputs are all positive. Conversely, it is a great deal faster than Tanh as well as Sigmod, and since both Tanh, as well as Sigmod, require calculating exponentials. Additionally, to evade the over-fitting of the DNN, two simple processing techniques are adopted. Particularly, the initial scheme is to choose the suitable network structure to minimize the number of network layers and neurons. The next scheme is to haltprevious to time and break off the training while its performance on the test set initiates to refuse.

$$\mathrm{Re\,LU}(x)=\begin{cases} x & \text{if} \quad x>0 \\ 0 & \text{if} \quad x\le 0 \end{cases} \tag{10}$$

i) Training phase: DNN with the developed optimization model

In DNN weights get trained using the adopted optimization approach [6] and [7]. At first, the DNN uses the back-propagation approach to find the optimal weights, and here, the Enhanced GSA-adaptive PSO uses to refine the searching process.

ii) Testing phase: Detection of intrusion in the test data

For the test data L, the DNN approach presents the needed intrusion information on the basis of the optimal weights obtainable via the training procedure. The developed Enhanced GSA-adaptive PSO approach found the appropriate weights and on the basis of the weights, the DNN recognizes the intrusion information present in the test data. The ultimately developed approach output besides with the DNN will be the intrusion class stated as below,

$$C = \mathrm{DBN}\{L\} \tag{11}$$

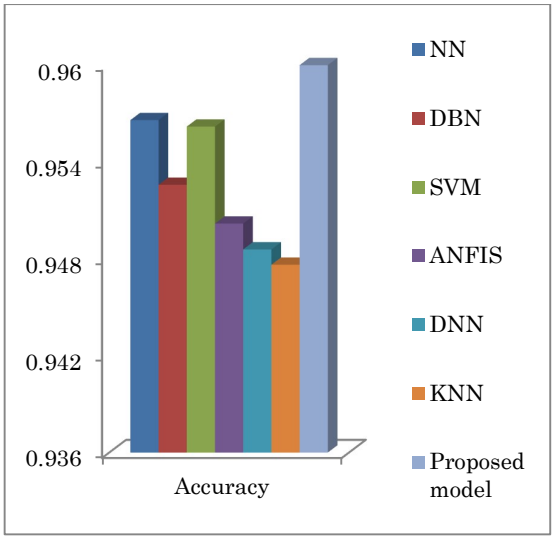
whereas, C indicates the intrusion class and L indicates the test data. The intrusion class presents the value as "one" for the intrusion presence and the value "zero" for other conditions.

5. Experimentation Procedure

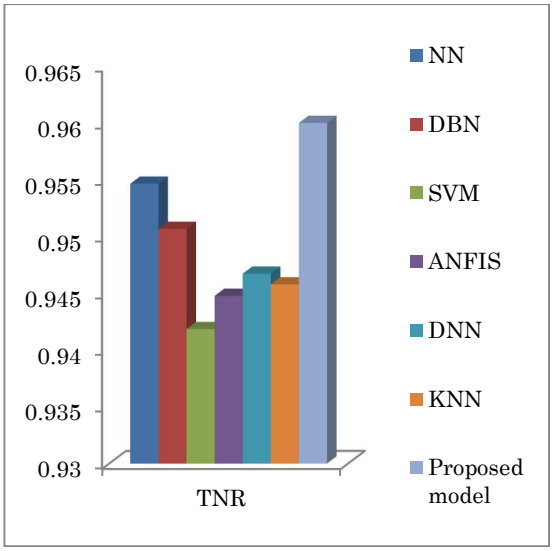
The experimentation of the developed model attained by the IDS technique was discussed in this section. On the basis of the various conditions, the developed model was carried out. Here, the proposed method was evaluated over several conventional techniques with diverse measures namely Accuracy, TNR, as well as TPR.

Fig 2(a), (b), and (c),demonstrates the performance analysis of conventional techniques over the conventional techniques on the basis of the several evaluation measures. These figures demonstrate the optimal performance of the proposed and conventional techniques over diverse cases. Fig 2 (a) shows the analysis of proposed method over the conventional method regarding the accuracy. Here the accuracy of the proposed model is 23% superior to the NN models, 18% superior to the DBN models, 23% superior to the SVM models, 15% superior to the ANFIS models, 14% superior to the DNN models, 12% superior to the KNN models. Fig 2 (b) shows the analysis of proposed method over the conventional method regarding the TNR. Here the accuracy of the proposed model is 32% superior to the NN models, 38% superior to the DBN models, 43% superior to the SVM models, 40% superior to the ANFIS models, 42% superior to the DNN models, 40% superior to the KNN models. Fig 2 (c) shows the analysis of proposed method over the conventional method regarding the TPR. Here the accuracy of the proposed model is 22% superior to the NN models, 21% superior to the DBN models, 32% superior to the SVM models, 31% superior to the ANFIS models, 26% superior to the DNN models, 23% superior to the KNN models.

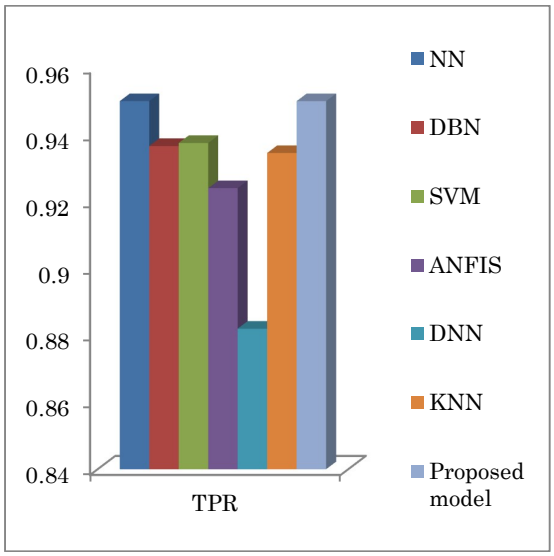
From the evaluation analysis, the developed technique has attained complete superior performance regarding the accuracy, TPR, and TNR, correspondingly.



(a)



(b)



(c)

Fig. 2. *Performance analysis of the proposed and conventional models (a) accuracy (b) TNR (c) TPR*

6. Conclusion

In recent times, cyber security has comes out as an recognized restraint for computer systems and infrastructures by means of a focal point on fortification of precious information stored on those systems from adversaries who want to attain, damage, corrupt, obliterate or forbid access to it. Numerous information security approaches were accessible nowadays to defend information systems over unauthorized use, duplication, destruction, alteration, and virus attacks. An IDS was a program which analyzes what occurs or has happened throughout an execution and tries to discover indications that the computer has been distorted. In this paper, the developed optimization approach was the combination of both the EGSA and APSO. Here, the database comprises the data from various users which was fed to the clustering by exploiting the developed optimization approach. Subsequently, the intrusion presence in each cluster was recognized with the aid of the HSDT classifier and each HSDT classifier result was gathered in order to create the compact data. Moreover, by exploiting the compact data and the developed optimization approach was combined with the DNN and it was exploited to train the data in order to attain the optimal weights to train the process. The experimentation of the developed technique was performed with various measures such as TNR, TPR, and accuracy and the outcomes exhibit the better performance regarding the proposed model.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] Mohamed Amine FerragLeandros MaglarasHelge Janicke,"Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study", Journal of Information Security and Applications, vol.50, December 2019.

[2] Chanyoung LeeHo Bin YimPoong Hyun Seong,"Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept", Annals of Nuclear Energy, vol,122, pp. 646-654, 8 November 2017.

[3] Govind P. GuptaManish Kulariya,"A Framework for Fast and Efficient Cyber Security Network Intrusion Detection Using Apache Spark", Procedia Computer Science, vol.93, pp.824-831, 2016.

[4] Adamu I. AbubakarHaruna ChiromaLibabatu Baballe Ila,"A Review of the Advances in Cyber Security Benchmark Datasets for Evaluating Data-Driven Based Intrusion Detection Systems", Procedia Computer Science, vol.62, pp, 221-227, 2015.

[5] Sara MohammadiHamid MirvaziriHadis Karimipour,"Cyber intrusion detection by combined feature selection algorithm", Journal of Information Security and Applications, vol. 44, pp 80-88, 1 December 2018.
[6] F. Hussin, H.A. Rahman, M.Y. Hassan, W.S. Tan, M.P. Abdullah, Multi-distributed generation planning using hybrid particle swarm optimisation- gravitational search algorithm including voltage rise issue, IET Gener. Transm. Distrib,vol. 7, no. 9, pp. 929–942, 2013.
[7] M. Khajehzadeh, M.R. Taha, A. El-Shafie, M. Eslami, A modified gravitational search algorithm for slope stability analysis, Eng. Appl. Artif. Intell, vol. 25, no. 8 , pp. 1589–1597, 2012.
[8] Suresh Babu Chandanapalli, E. Sreenivasa Reddy and D. Rajya Lakshmi, "FTDT: Rough set integrated functional tangent decision tree for finding the status of aqua pond in aquaculture", Journal of Intelligent & Fuzzy Systems, vol. 32, pp. 1821–1832, 2017.
[9] Seongji HanHee-Sun ChoiJin-Gyun Kim,"A DNN-based data-driven modeling employing coarse sample data for real-time flexible multibody dynamics simulations", Computer Methods in Applied Mechanics and Engineering, vol.373, ,21 October 2020.
[10] Heyan Zhang,"Secure Routing Protocol using Salp-Particle Swarm Optimization Algorithm", Journal of Networking and Communication Systems, vol 3, no 3, July 2020.
[11] Moresh Madhukar Mukhedkar,Uttam Kolekar,"Hybrid PSGWO Algorithm for Trust-Based Secure Routing in MANET",Journal of Networking and Communication Systems, vol 2, no. 3, July 2019.