Classification of Intrusion using Artificial Neural Network with GWO

Gurbani Kaur, Dharmender Kumar

ABSTRACT: In the present milieu of connected world, where security is the major concern, Intrusion Detection System is the prominent area of research to deal with various types of attacks in network. Intrusion detection systems (IDS) finds the dynamic and malicious traffic of network, in accordance to the aspect of network. Various form of IDS has been developed working on distinctive approaches. One popular approach is machine learning in which various algorithms like ANN, SVM etc. have been used. But the most prominent method used is ANN. The performance of the ANN can significantly be improved by combining it with different metaheuristic algorithms. In present work, GWO is used to optimize ANN. For this KDD-99 data-set is used to classify various types of attacks i.e. denial of service (DOS), normal and other form of attack. The present paper provides detailed analysis of the performance of Artificial Neural Network and optimized Artificial Neural Network with GA, PSO and GWO. The research shows that ANN with GWO outperform as compared to others (ANN, ANN with PSO and ANN with GA).

Keywords: ANN, DOS, GA, GWO, IDS, KDD, PSO.

I. INTRODUCTION

In the latest scenario, the use of internet is growing at a large pace with is highly developed and emerging forms of ever growing network and its connectivity but usage of internet produces a great damage to security of the system. In order to protect various firms, organisations and companies from these threats, high level of security is required. One of the difficult task among the network-security is to sustain the integrity of the IDS so as to protect the system from distinct attacks. [1-3]. The major objective of Intrusion Detection System is to find more specific form of intrusion. Various intruders or hackers have found enormous ways to exploit the system security. A number of experiments are carried out by researches to monitor the security from various intrusions. So, the main aim of Intrusion Detection System is to protect the public, governmental or private information [10]. An IDS automatically, issues an alarm or message to the authority whenever any intrusion or attack is observed in the network [3]. IDS reduces the false alarm rate to provide better detection of intrusions. The research mainly focusses upon the enhanced capabilities of the intrusion detecting system to detect the attacks effectively.

Revised Manuscript Received on April 02, 2020.
* Correspondence Author

Gurbani Kaur*, M.Tech Scholar, Department of Computer Science and Engineering,Guru Jambheshwar University of Science &Technology,Hisar, India..E-mail: gurbanichawla@gmail.com

Dharmender Kumar, Professor, Department of Computer Science and Engineering,Guru Jambheshwar University of Science & Technology, Hisar, India.E-mail: dharmindia24@gmail.com

II. STRUCTURE OF IDS

Intrusion detection system intiated its process in 1990. The IDS process generates an alarming state in case of any system or network violation like emails,messages or audio-video [6]. IDS basically is a tool which is used for system security in case of any intrusions which may interrupt the normal working of the system [7-9]. IDS function is to find or search for the different attacks prevailing in the system and thereby provide infornmation about the attacks and also provide with defence mechanism to fight these attacks. An Intrusion Detection System gives a method to protect the security of the current network safety [18].

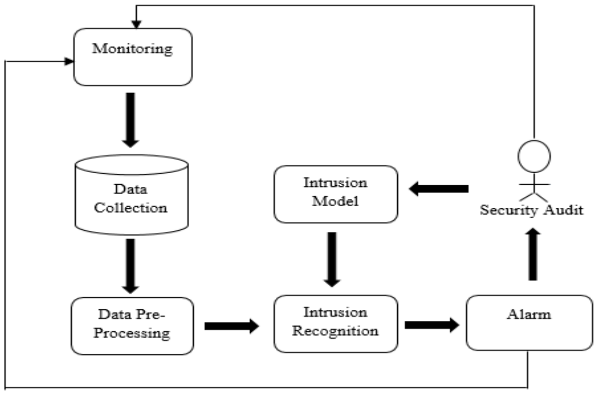

Figure 1: Basic structure of IDS

2.1 Intrusion Detection Techniques

IDS can be classified into numerous classes on the basis of detection or structure. Intrusion Detection System can be grouped on the basis of characerstics as shown below:

2.2 Based on Structure

The IDS process can be classified on the basis of its framework into three classes which are Network based Intrusion Detection System, Application Based Intrusion Detection System and Host Based Intrusion Detection System.

1. Network Based IDS [NIDS]: NIDS basically monitors or analyzes the incoming network traffic to search for an attack or intrusions and it is placed inside the router. It than generates an alarm or message to the administrator to notify about an attack.

2. Host Based Intrusion Detection System [HIDS]**:** It basically analyse or monitors the computer system and is placed in the server which is why it is called HIDS. It provides a mechanism to check the files stored in the computer or other documents so as to detect any intrusion in the files and also notify the designated authority.

DOI: 10.35940/ijeat.D7597.049420

3. Application based IDS: It analyses a particular application and the files in these applications to detect any type of intrusions so as to protect the network from such intrusions induced by an attacker. It also monitors the abnormal functions such as void file execution, exceeded permission, etc.

2.3 Based on Detection Method

In-order to build a smart IDS, the main aim of IDS is to minimise the false alarms i.e. the positive and the negative alarms. Based on the detection method the IDS is divided into two of its main categories that includes the Misuse detection and the Anomaly based detection.

1. Misuse detection: It is also called as the signature-based IDS designed to compare the signatures or the patterns that are made over the incoming path of the traffic network. These signatures help in detecting the attacks in a very accurate manner. Misuse detection helps in finding the eminent forms of attack.

2. Anomaly IDS: This term anomaly IDS is also known as statistical IDS i.e. it monitors the network traffic identified as a normal method deriving a potential base-line. During the normal operation, if there is any kind of inconsistency caused by the system, then the system produces an alarm automatically [10-13]. Anomaly IDS comprises of the abnormal intrusive activity of the system.

2.4 Based on attack

The attack-based IDS are categorized as follows [4]

1. Normal Category: This category does not have any form of data attack. It consists of a state where the system has no alteration and no such kind of abnormality occurs in the state of the system.

2. DOS-Attack: This is generally called as the denial of service (DOS) attack. Here, in this form of attack, the hacker or the attacker of the system perform various form of illegal activities such as illicit calculations, makes the data memory typically jammed by sending the malignant data sources or the data packets in such that it is not able to maintain the authentic activity of the system. The attacker performs a Botnet attack and takes the advantage of the distance. The process of DoS consists of various types of attacks [9]:

3. Probe Attack: This type of attack consists of collecting the information, analyzes the network operation in order to extract the valid form of IP address to pin-point the distinct services used for the network for performing a smart and wise attack on these services [24].

4. Remote to Local (R2L) Attack: The R2L attacks commonly includes getting access through phf attack software that grants the users or the attackers to perform the inconsistent command operations on the server of the system and the other R2L attacks involves the password-guessing mechanism i.e. the guest and dictionary attacks.

5. User to Root (U2R) Attack: The process of user to root attack defines the activity where an attacker opens a fake account, make the system weak or creates the bugs into the system by squandering the authorization processes. The most commonly used U2R attack is the flow of the buffer where an attacker takes the advantage of the fault occurring in the program and congregate the additional information into a buffer i.e. kept on an execution stack.

III. RELATED WORK

Dias GV et.al [1] conducted a study indicated an intrusion detection system based on SVM methodology that combines an algorithm (hierarchical clustering), feature selection method and the technique of SVM. The algorithm i.e. used helps in providing the support vector machine with maintaining an abstracted form of high level of trained examples obtained from the trained set-up of KDD Cup 1999. The study indicates high level performance of SVM based technology which further resulted in a reduced form of training-time. The method of feature-based selection was adopted to remove the un-necessary features of the training set in order to maintain the levels of accuracy. The dataset of KDD cup-1999 was used to analyze the proposed system. When the system was compared with the other forms of data set, the experimental analysis showed that the result based on the performance analysis was not so good as compared to KDD Cup-1999 dataset. So, the methodology based on this dataset showed better analysis in detection of probe and DoS based attacks, maintaining accuracy globally. Cannady et.al [2] proposed a study on the process of misuse detection which is defined as a process to recognize the instances of different types of attacks by measuring the unexpected activity and the activity that is going currently. Mostly, the present processes based on misuse detection uses a technology of rule-based systems with the aim to identify the provoked nature of the attacks known to us. But the above process was less reliable to guess the forms of distinct attacks done on the system. The use of ANN technology gave a potential to search and identify the activities of the network that rely on the incomplete, non-linear, and limited amount of sources. Kemmerer et.al [3] presented a study by framing a simple question of why there is a need of intrusion detection system. Suppose, the owner of a house is out of town and he has locked his home with all the windows and doors closed. But, there is someone outside his home who wants to enter. Firstly, he rings the bell and checks the main door if it is locked or not then after sometime he checks the windows of the house that too are locked which makes sure that the house is safe. So, the question is why an alarming bell is installed. This question particularly sticks to the IDS. Why there is a need to plant the detection systems if the security is tight and secure. The reason to install these detective systems is that the intrusions still exist because sometimes the people may forget to lock their doors or windows, the same case occurs with the computer based networks which do not provide us 100% security of the system to work accurately. So, based on this study the researchers has tried to explain the techniques based on IDS to deal with these kind of intrusions present in the network.Steven T et.al [4] proposed a study on an application of STATL that represents a descriptive language based on a transition-based attacking system that is constructed to support the IDS. This form of descriptive language describes a process of penetration done to the computer network implemented by a hacker. These type of penetrations includes attacking activities performed by the hacker. The STATL description is used by the IDS to extract the stream events and the ongoing intrusions occurring in the system. As the IDS works under distinct environments such as Windows NT, Linux etc. and the domains like the host or the network. So, this extensible form of language helps in dealing with different targets as required. This language basically describes both the host and the network attacks. Here, in this paper an IDS based tool-set i.e. based on the descriptive language has been executed. This tool-set depicts various favorable and the desires results. There is a deep study of syntax based on the STATL language. Common real examples of both the network and the host are also described in the paper. Pi-Cheng et.al [5] conducted a research based on two of its issues related to the IDS designs. The two issues include the selection based on optimization of rule-based selection and the discovery in case of attack. This type of approach provides a connection between the junked packets. An algorithm is implemented for the attack identification and the rule based selection. The study is performed on the threats and describes the relationship for an application based web-server and the gateway. The algorithm is implemented over a signature-based IDS for having the better form of results. Cavusoglu et.al [6] conducted a research on security systems of IT. The information technology firms rely on various forms of technologies such as IDS and the firewalls to manage the risks of the organizations. There exists some most interesting facts related to security alerts in IT industries. This paper presented a study to demonstrate the values of IDS adopted in an IT company. The configuration of IT was represented by the true-positive and the false-positive rates which further consists of determining the negative or the positive rates of an organization. It was shown specifically that an organization or a firm experiences a positive-rate from an IDS based on one of the condition that the rate of detection is more than the critical value. When a firm experiences a positive or a negative value, an IDS prevents the occurrence of hackers that means an IDS targets the hacker's activity whether the alarm is positive or negative as the rate of detection is same. The results so obtained showed that the positive rate detected by an IDS is the result of increased amount of deterrence enabled by its improved detection. The use of optimized form of IDS indicates that the firm experiences a value i.e. non-negative in nature Chebrolu, Srilatha et.al [7] conducted a research on IDS that examined all the features of data to detect misuse or intrusion patterns. Some of its features may be of redundant nature or donate small quantity to the detection process. The study purpose was to classify unique input features in building an IDS i.e. efficient and effective computationally. An investigated was done based on the performance of algorithms based on feature-selection. The first one was the Bayesian networks (BN) and the other was the CART i.e. classification and regression trees including both the BN and CART in the form of an ensemble. The results showed that input feature-selection was mainly required to design an IDS i.e. light in weight, effective and, efficient for real scenario detection techniques. In the end, the researchers proposed an architecture i.e. hybrid in nature for joining the different algorithms of feature-selection for current scenario of IDS. Kim, Dong Seong, et.al [8] projected a technique based on Genetic Algorithm to revamp SVM i.e. Support Vector Machines based IDS. The SVM denotes a novel technique of classification that has revealed a high class performance in various applications. The security-based scholars have proposed SVM based IDS. Here, they have used the fusion of SVM and GA to boost the global performance. This type of inter-mixing resulted in a model based on "optimal detection" for SVM classifier where this method not only represented the "optimized-parameters" for SVM but also resulted in an "optimized-feature set" among the data-set. A demonstration was done to check the feasibility of the method by performing experiments on data-set named KDD 1999 for detection of intrusions in the system. Carl, Glenn, et.al [9] suggested a study based on detection using Denial-of-service (DoS) techniques that includes change-point detection, activity profiling, and a signal analysis (wavelet-based) that further faced a major challenge to analyze the attacks on network that generated from the sudden unexpected activities or flash-events. This survey of techniques and testing results provided a mechanism to identify DoS based flooding attacks. As the detectors used in the process are quite good but none of them has shown the complete accurate detection. The adjoining of various methodologies with smart and intelligent network handlers would definitely produce excellent results. Wolfgang Banzhaf, et.al [16] researched on Intrusion detection based that relies on the computational-based intelligence In order to build a good model of IDS, it should include the important features of computational intelligence (CI) systems that consists of high computational speed, fault tolerance, adaptation, and error resilience properties. Here, the study has provided an overview to the problem of intrusion detection based on CI systems. The scope has encompassed CI core-method, including evolutionary computation, ANN, soft computing etc. The research has summarized that allowed us to clarify the research challenges that are existed already, and highlights the methods by promising new research solutions. The findings survey has provided useful methods to conduct the research in the current IDS technology. Zhou, Chenfeng Vincent, et.al [17] worked on attacks that are coordinated in nature such as DDoS attacks, worm-outbreaks, and large-scale scans, that occur in simultaneous way in case of multiple-networks. Such type of attacks are very hard to identify and with the use of intrusion detection systems (IDSs) i.e. isolated, the researchers has monitored only a limited part of the internet. This paper has summarized the current research in detecting using collaborative forms of intrusion detection systems (CIDSs). Specifically, two major challenges have been discussed. One was the architecture of CIDS and the other was alert correlation algorithms. The conclusion highlights on the opportunities for a collaborative study of intrusion detection systems. Tzong-Wann Kao, et.al [18] suggested a model upon SVM strategy that was predicated on intrusion detection program that joined an algorithm of clustering symbolizing a hierarchical assembly, a method of SVM, and the task of basic feature assortment. The algorithm based on hierarchical-based clustering provided with Support vector machine, introspective, or highly trained situations which were extracted by KDD Cup 99 training dataset. It enhances the performance of the SVM. The procedure of feature-based selection process was put on eliminating insignificant features coming from the set of established therefore the acquired SVM unit could sort out

the network traffic info more precisely.

The popular dataset i.e. KDD99 was mainly used for carrying out experimentation in system. Overall accuracy and performance of the system was improved, thus improving detection of Probe and DOS attacks as compared to the other systems. Muhammad Hilmi Kamarudin, et.al [19] proposed their study on technology of network security that has become a supreme method for the protection of information or the data. With the excessive growth of internet technology, various forms of attack cases are observed in a day to day life. So, to tackle such kind of attacks, a methodology of IDS is adopted and the process of Machine Learning is the most used technology in the IDS. The study based on recent years has shown that the Machine Learning IDS provides a good detection rate and a high accuracy. Thus this paper includes performance analysis based on Machine Learning algorithm known as Decision Tree (J48) where a comparison has been done with two of the other machine learning algorithms named as the NN and the SVM's. These algorithms were tested on the strategy of false alarming rate, rate of detection, and accuracy of four classes of attacks. From the experimental analysis it was detected that the J48 (Decision-tree) algorithm performed well as compared to the other two machine learning algorithms.

IV. THE PROPOSED METHOD

4.1 Proposed Methodology

1.Input the KDD Data set to ANN.

2.Label the KDD dataset accordingly into three classes.

3.Initialize the ANN parameters randomly.

4.Learn by sigmoid function and make the model for the classification.

5.Analysis the model.

6.Use GWO for optimizing ANN parameters.

7.Then fitness value is calculated.

8.Discover the effective parameters $\{y_1, y_2, y_3 \dots \dots . y_n\}$.

9.Check the Iteration < Iteration Max if yes go to next step otherwise go to step 4.

10.Analysis the accuracy, precision and recall.

4.2 Proposed methodology: Flowchart

Steps of proposed flow chart are shown below:

1. KDD-99 Data Set: This is a type of data-set used for the competition based on Third International Knowledge Discovery and Data Mining Tools, held in aggregation with KDD-99 (The Fifth International Conference on Knowledge Discovery and Data Mining). The major task was to build a network based on intrusion detection, and to predict a model i.e. capable of discriminating a good or a bad form of data-set. This form of data-set maintains a standard including a wide variety of network based intrusions.

2. Label Features: Features are labelled so as to provide information about the data set. Research work is categorized into three different types i.e. normal category, other type of attack and DOS attack. Normal category consists of a state where the system has no alteration and no such kind of abnormality occurs in the state of the system. In DOS attacks, the hacker of system perform various form of illegal activities such as illicit calculations, makes the data memory typically jammed by sending the malignant data sources or the data packets in such that it is not able to maintain the authentic activity of the system. Other types of attack includes remote to local attack, probe attack and user to root attack.

3. Initialize Parameters of ANN: ANN represents biologically inspired information processing system. In this step initialize number of input layer, hidden layers and weights according to gradient factor. The basic processing unit of ANN is artificial neurons which is simply called nodes. They perform the summing and mapping function. These neurons operate in parallel and setup in regular architecture. Neurons are organized in layers and have feedback connection within the layer and for next layer.

4. Optimization with GWO: GWO is the most recent bio-inspired algorithm. The primary idea of GWO is to simulate the behaviour of grey wolves. The leader of the pack is known as Alpha and takes all the decisions in the pack. The next level subordinate wolves are known as the beta. 3rd subaltern levels wolves are known as Delta. Delta includes scouts, caretakers, sentinels, hunters and elders as their members. Scouts have responsibility of monitoring boundary regions. Wolves have their own position and velocity to explore solution which is better.

5. Updation of fitness function: It decides how good an individual solution can handle the given problem.

6. Classifier Model: It is used to classify the data into different types of attacks.

7. Results: Precision, Accuracy, Recall and F-score is calculated. Optimized ANN using GWO provides effective results. The objective is optimized.

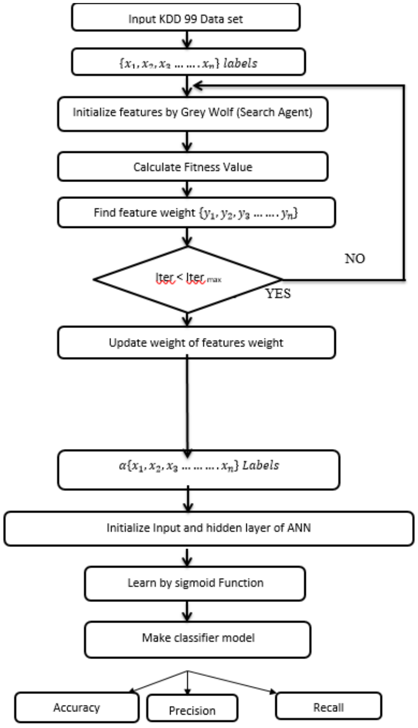
Input KDD 99 Data set
$\{x_1, x_2, x_3 \dots \dots . x_n\}$ labels
Initialize features by Grey Wolf (Search Agent)
Calculate Fitness Value
Find feature weight $\{y_1, y_2, y_3 \dots \dots . y_n\}$
Iter < Iter max
NO
YES
Update weight of features weight
$\alpha\{x_1, x_2, x_3 \dots \dots \dots . x_n\}$ Labels
Initialize Input and hidden layer of ANN
Learn by sigmoid Function
Make classifier model
Accuracy
Precision
Recall

Figure 2: Proposed Flowchart

Proposed Algorithm:

Algorithm

Step 1: Input KDD-99 data to ANN. Preprocess the data set to remove the noisy data.

Step 2:. Randomly initialize parameters of ANN.

Step 3: Learning and testing Model is made using ANN and then the result is calculated.

Step 4: Apply weighted GWO for optimizing ANN to produce effective result.

Step 5:. Extract the Features and make the matrix.

Step 6: Generate optimize feature weights matrix.

With optimization model $\boldsymbol{min_{\omega,\xi,Q}P(\omega,\xi)}$ we describe the model of ANN classification.

$$\boldsymbol{min_{\omega,\xi,Q}P(\omega,\xi_r) = \frac{1}{2}\omega^g\omega + \frac{1}{2}\gamma\sum_{r=1}^{n}\xi_r{}^2}$$

$$\boldsymbol{s_r[\omega^t\phi(u_r) + Q = 1 - \xi_r, r = 1, 2, \ldots\ldots, n}$$

$$\boldsymbol{\xi = (\xi_1, \xi_2, \ldots \ldots . \xi_n)}$$

Where

$\boldsymbol{\xi_r}$←input parameters

Q←Offset

$\boldsymbol{\omega}$←Hidden layers

$\boldsymbol{\gamma}$← Parameter used as classification for keeping a balance between the model complexity and fitness error.

$\boldsymbol{\omega^g}$←Updated weight of training data.

$\boldsymbol{s_r}$ ← Output of sigmoid function

$\boldsymbol{\omega^t}$ ← Updated weight at time t

$\boldsymbol{\phi}$← Kernel function

Then, describing the classification output function:

$$\boldsymbol{F(z_r) = sgn(\sum_{r=1}^{n}\alpha_r s_r L(q, q_r) + Q)}$$

$\boldsymbol{sgn}$← Sigmoid function

$\boldsymbol{\alpha_r}$← weight at instance r

Step 7:. Analyze the Precision, Accuracy, Recall and f-measure.

V. RESULT ANALYSIS

Description of dataset

Since discussions over experiments is usually implemented through the use of KDD-99 which usually having forty one feature units. These features are utilized for learning and marketing and today they will accustomed to evaluate in conditions of assault. In this function we use to judge the rate of accuracy within an IDS. Inside the evaluation put into effect data based on number of attacks. Episodes are usually fall into 4 groups 1) Probe, 2) Dos, 3) U2R 4) R2L. Inside our evaluation all of us uses three classes 1) another attack that contains probe, U2R and R2L 2) DoS-attack 3) Regular attacks. Various parameters are measured in a variety of cases

Table 1: KDD CUP 99 dataset-based attack type

PARAMETERS	ANN	ANN with GA	ANN with PSO	ANN with GWO
Accuracy	89.32	93	90	96.23
Precision	88.45	91	90.38	97.33
Recall	87.12	92	92	98.33
F-measure	85.89	94	87	93.13

Table 1 shows comparison among different techniques like ANN and combination of ANN with GA, PSO and GWO based on parameters like accuracy, precision, recall and F-measure. ANN with GWO provides effective results. Overall value of accuracy of ANN with GWO is 96.23, precision is 97.33, recall is 98.33, F-measure is 93.13.

Table 2: Algorithm Types vs. Types of attack

Algorithm type	Types of attack	Accuracy	Precision	Recall	F-measure
ANN	Other attack	87	84	87	83
	Dos Attack	88	87	89	84
	Normal Attack	90	87	86	86
ANN with GA	Other attack	94	88	85	87.23
	Dos Attack	89	91	86	86.23
	Normal Attack	90	90	83	89.13
ANN with PSO	Other attack	92	90	85	84.23
	Dos Attack	95	89	87	83.23
	Normal Attack	91	89	90	87.34
ANN with GWO	Other attack	98.62	96.23	97.33	95.23
	Dos Attack	92.23	90.23	96.33	95.13
	Normal Attack	97.23	96.13	99.56	92.23

Table 2 represents attacks in three different groups such as Other attacks, Dos attacks and Normal attacks. Different techniques such as ANN.ANN with GA, ANN with PSO and ANN with GWO are used to classify these attacks.

Simulation is used to study the statistical data in this section. Table 1 and 2 results are stated using process of simulation which is presented in graphical form.

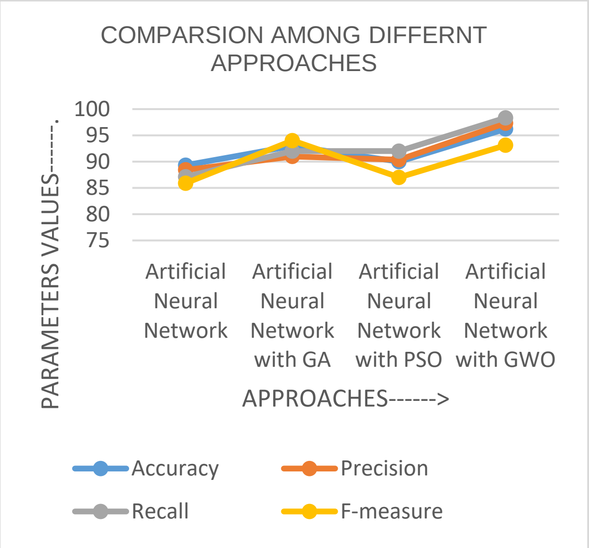

Figure 3: Simulated graph of table 1

Figure 3 displays simulated evaluation of table 1 particular in conditions. This figure evaluates effectiveness i.e. is usually revealed coming from all of the four algorithms which are Artificial Neural Network displayed by green colour, Artificial Neural Network along with PSO presented simply by purple colour, Artificial Neural Network in conjunction with GA presented by red colour and Artificial Neural Network with GWO represented by blue colour. Evaluation exhibits that the ANN with GWO provides better effect when it comes to all of the four guidelines (precision, accuracy, recall, F-measure). Artificial Neural Network with Grey Wolf Optimization provides more effective results as compare to other algorithms. ANN with GWO classify the attacks into normal, denial of service and other attacks accurately without producing false alarm rate.

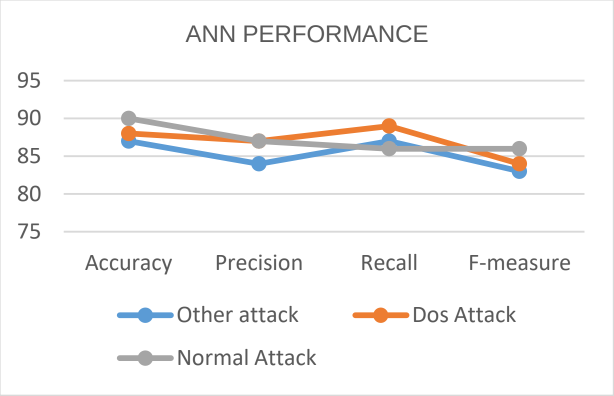

Figure 4: Analysis of ANN

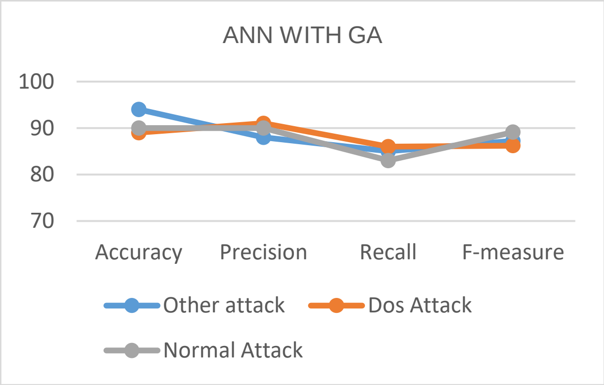

Figure 5: Examination with ANN _GA

Figure 4 and 5 investigate parameters of various proposed approaches like ANN and ANN with GA. In case of investigating parameters such as exactness etc is given by classifiers. Result shows that ANN with GA is better than ANN. ANN with GA reduces the false alarm rate and provides more effective results than ANN. X axis represents the parameters such as Accuracy, Precision, Recall, F-measure. Y axis represents the value of the parameters. Results shown in figure 4 and 5 is represented by different colors. Blue color represents the other attacks, red color represents DOS attacks. Normal attacks are represented by green colors.

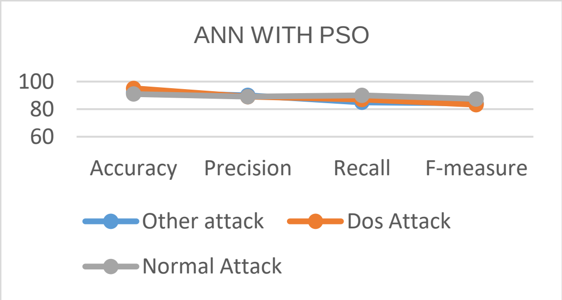

Figure 6: Analysis of ANN _PSO

Figure 6 shows the results of ANN with PSO. ANN with PSO provides more accurate results in classifying DOS attacks and normal attacks i.e. 95 and 91 respectively.

Finally comparing all four algorithms it is analyzed that ANN_GWO algorithm provides results which are better among all the algorithms for all the attacks we considered in our work. In figure 7 insight investigation of every one of the three classes are given. The analysis endeavoured is used to specify what the cruciality of the methodology used. ANN_GWO performs better than other techniques in terms of different parameters mentioned. On the off chance that examination through DOS assault, ANN with GWO gives higher level of exactness. Proposed methodology decreases the false positive rate in detecting the intrusions in different assaults like DOS assaults etc. So GWO streamlining is great however GWO provides effective results.

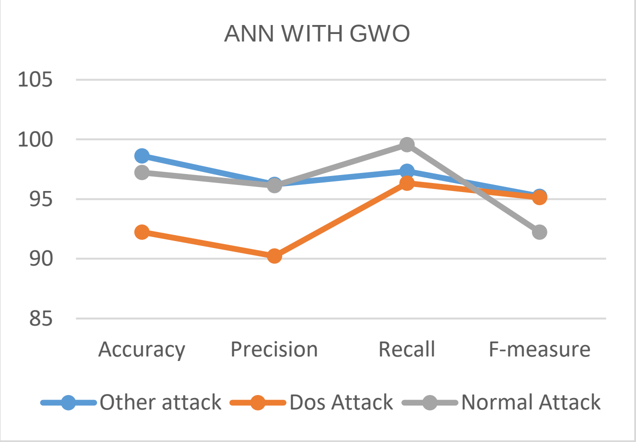

Figure 7: Analysis with ANN _GWO

VI. CONCLUSION

The present-day scenario experiences various forms of growth and developments consisting of connectivity among distinct networks. But network is exposed to different types of assaults by attackers. There are various types of IDS that can sense malicious activities prevailing in the system. Due to the lack of protection of the system and high rate of false alarms, intruders can access the system to exploit the data. Present paper proposes optimized Ann with GWO to minimise the rate of false positive alarms. The proposed analysis contains a specific data-set i.e. KDD-99 and it is concluded that ANN with GWO gives improved results in comparison to other algorithms.

FUTURE SCOPE

Performance can be further improved by combining it with other classification techniques and feature selection can be used to detect the attacks more accurately.

REFERENCES

1. Snapp, Steven R., James Brentano, Gihan V. Dias, Terrance L. Goan, L. Todd Heberlein, Che-Lin Ho, Karl N. Levitt et al. "DIDS (distributed intrusion detection system)-motivation, architecture, and an early prototype." In *Proceedings of the 14th national computer security conference*, vol. 1, pp. 167-176. 1991.
2. Cannady, James. "Artificial neural networks for misuse detection." In *National information systems security conference*, vol. 26. 1998.
3. Kemmerer, Richard A., and Giovanni Vigna. "Intrusion detection: a brief history and overview." *Computer* 35, no. 4 (2002): supl27-supl30.
4. Eckmann, Steven T., Giovanni Vigna, and Richard A. Kemmerer. "STATL: An attack language for state-based intrusion detection." *Journal of computer security* 10, no. 1-2 (2002): 71-103.
5. Hsiu, Pi-Cheng, Chin-Fu Kuo, Tei-Wei Kuo, and Eric YT Juan. "Scenario based threat detection and attack analysis." In *Security Technology, 2005. CCST'05. 39th Annual 2005 International Carnahan Conference on*, pp. 279-282. IEEE, 2005.
6. Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. "The value of intrusion detection systems in information technology security architecture." *Information Systems Research* 16, no. 1 (2005): 28-46.
7. Chebrolu, Srilatha, Ajith Abraham, and Johnson P. Thomas. "Feature deduction and ensemble design of intrusion detection systems." *Computers & security* 24, no. 4 (2005): 295-307.
8. Kim, Dong Seong, Ha-Nam Nguyen, and Jong Sou Park. "Genetic algorithm to improve SVM based network intrusion detection system." In *Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on*, vol. 2, pp. 155-158. IEEE, 2005.
9. Carl, Glenn, George Kesidis, Richard R. Brooks, and Suresh Rai. "Denial-of-service attack-detection techniques." *IEEE Internet computing* 10, no. 1 (2006): 82-89.
10. Mohammed, Muamer N., and Norrozila Sulaiman. "Intrusion detection system based on SVM for WLAN." *Procedia Technology* 1 (2012): 313-317.
11. Vinchurkar, Deepika P., and Alpa Reshamwala. "A Review of Intrusion Detection System Using Neural Network and Machine Learning." (2012).
12. Nadiammai, G. V., and M. Hemalatha. "Effective approach toward Intrusion Detection System using data mining techniques." *Egyptian Informatics Journal* 15, no. 1 (2014): 37-50.
13. Agrawal, Shikha, and Jitendra Agrawal. "Survey on anomaly detection using data mining techniques." *Procedia Computer Science* 60 (2015): 708-713.
14. Sun, C., Lv, K., Hu, C., & Xie, H. (2018, July), "*A Double-Layer Detection and Classification Approach for Network Attacks*," In 2018 *27th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-8), IEEE.
15. Aydın M. Ali, A. Halim Zaim, and K. Gökhan Ceylan, "*A hybrid intrusion detection system design for computer network security*," *Computers & Electrical Engineering* 35, no. 3 (2009): 517-526.
16. Wu Shelly Xiaonan and Wolfgang Banzhaf, "*The use of computational intelligence in intrusion detection systems: A review*," *Applied soft computing*, vol.10, no. 1, pp. 1-35, (2010).
17. Zhou Chenfeng Vincent, Christopher Leckie, and Shanika Karunasekera, "*A survey of coordinated attacks and collaborative intrusion detection*," *Computers & Security*, vol.29, no. 1, pp.124-140, (2010).
18. Horng Shi-Jinn, Ming-Yang Su, Yuan-Hsin Chen, Tzong-Wann Kao, Rong-Jian Chen, Jui-Lin Lai, and Citra Dwi Perkasa, "*A novel intrusion detection system based on hierarchical clustering and support vector machines,*" *Expert systems with Applications*, vol. 38, no. 1, pp.306-313, (2011).
19. Jalil Kamarularifin Abd, Muhammad Hilmi Kamarudin, and Mohamad Noorman Masrek, "*Comparison of machine learning algorithms performance in detecting network intrusion,*" In *Networking and Information Technology (ICNIT), 2010 International Conference on*, pp. 221-226, IEEE, 2010.
20. Elshoush Huwaida Tagelsir, and Izzeldin Mohamed Osman, "*Alert correlation in collaborative intelligent intrusion detection systems—A survey*," *Applied Soft Computing*, vol. 11, no. 7, pp. 4349-4365, (2011).
21. Mohammed Muamer N., and Norrozila Sulaiman, "*Intrusion detection system based on SVM for WLAN,*" *Procedia Technology*, vol.1, pp. 313-317, (2012).
22. Vinchurkar Deepika P., and Alpa Reshamwala, "*A Review of Intrusion Detection System Using Neural Network and Machine Learning*," (2012).

Retrieval Number: D7597049420/2020©BEIESP
DOI: 10.35940/ijeat.D7597.049420
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

23. Nadiammai G. V., and M. Hemalatha, *"Effective approach toward Intrusion Detection System using data mining techniques,"* *Egyptian Informatics Journal*, vol. 15, no. 1, pp.37-50, (2014).
24. Agrawal Shikha, and Jitendra Agrawal, "*Survey on anomaly detection using data mining techniques*," *Procedia Computer Science*, vol. 60, pp. 708-713, (2015).
25. J. Jabez, B. Muthukumar, "*Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach," Procedia Computer Science*, vol. 48, 2015, pp. 338-346, ISSN 1877-0509.
26. Gupta Neha, Komal Srivastava, and Ashish Sharma, "*Reducing False Positive in Intrusion Detection System: A Survey," International Journal of Computer Science and Information Technologies*, vol. 7 (3), 2016, 1600-1603.
27. Siddiqui Aafreen K., and Tanveer Farooqui, "*Improved Ensemble Technique based on Support Vector Machine and Neural Network for Intrusion Detection System," INTERNATIONAL JOURNAL ONLINE OF SCIENCE*, vol. 3, no. 11, (2017).
28. Wang Huiwen, Jie Gu, and Shanshan Wang, "*An effective intrusion detection framework based on SVM with feature augmentation," Knowledge-Based Systems*, vol. 136, pp.130-139, (2017).
29. Giorgio Giacinto, Fabio Roli, and Luca Didaci, "*Fusion of Multiple Classifiers for Intrusion Detection in Computer Networks,"Journal of Pattern Recognition Letters*, vol.24, pp.1795-1803, 2003.
30. Wang Yu, Cheng Xiaohui and Wang Sheng, "*Anomaly Network Detection Model Based on Mobile Agent," IEEE, Third International Conference on Measuring Technology and Mechatronics Automation*, 2011.
31. Muna M. Taher Jawhar and Monica Mehrotra, *"Anomaly Intrusion Detection System using Hamming Network Approach," International Journal of Computer Science & Communication*, vol. 1, no. 1, pp. 165-169, 2010.
32. Nidhi Srivastav and Rama Krishna Challa, *"Novel Intrusion Detection System integratingLayered Framework with Neural Network," IEEE 3rd International Advance Computing Conference (IACC)*, DOI: 10.1109/IAdCC.2013.6514309, 2013.
33. Heba Ezzat Ibrahim, Sherif M. Badr and Mohamed A. Shaheen, *"Adaptive Layered Approach using Machine Learning Techniques with Gain Ratio for Intrusion Detection Systems," International Journal of Computer Applications (0975 – 8887)*, vol.56, no.7, 2012.
34. Shih-Wei Lin, Kuo-Ching Ying, Chou-Yuan Lee and Zne-Jung Lee, *"An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection,"Applied Soft Computing*, vol. 12, issue 10, 2012.
35. Rajni Bala, Dr. Dharmender Kumar, "Classification Using ANN: A Review," *International Journal of Computational Intelligence Research*, vol. 13, no. 7, pp. 1811-1820, 2017.
36. Dr. Saurabh Mukherjee, Neelam Sharma, *"Intrusion Detection using Naive Bayes Classifier with Feature Reduction*," vol. 4, 2nd *International Conference on Computer Communication, Control and Information Technology (C3IT-2012)*, February 25 - 26, 2012.

AUTHORS PROFILE

Gurbani Kaur, M.Tech Scholar, Department of Computer Science and Engineering,Guru Jambheshwar University of Science &Technology,Hisar, India

Dharmender Kumar, completed his Bachelor of Technology in Computer Science & Engineering (CSE) from CRSCE Murthal, GJUS&T, Hisar, Haryana, Master of Technology in CSE from Kurukshetra University, Kurukshetra and Ph.D in CSE from GJUS&T, Hisar, Haryana, India. Currently he is working as Professor in Department of Computer Science and Engineering in GJUS&T, Hisar. His main research work focuses on Artificial Intelligence, Data Mining and Big Data Analytics.