A New Method for Intrusion Detection Using Genetic Algorithm and Neural Network

M.R. Hosseinzadeh Moghaddam

Department of Computer Engineering, Central Tehran Branch ,Islamic Azad University, Tehran, Iran

S. Javad Mirabedini

Assistant Professor of Computer Engineering, Central Tehran Branch, Islamic Azad University, Tehran, Iran

T. banirostam

Assistant Professor of Computer Engineering, Central Tehran Branch, Islamic Azad University, Tehran, Iran

ABSTRACT

The article attempts to have neural network and genetic algorithm techniques present a model for classification on dataset. The goal is design model can the subject acted a firewall in network and this model with compound optimized algorithms create reliability and accuracy and reduce error rate couse of this is article use feedback neural network and compared to previous methods increase accuracy classification rate and reduce error rate. The proposed method increased with simulation accuracy of 99.97 percent.

Keywords

Intrusion Detection System, Neural Network, Genetic Algorithm, Clustring and Gravitational Search Algorithm.

INTRODUCTION

This document is a establishment security, determine the appropriate access level and identify gaps to intrusion is the most important component that should be considered in network security.main idea intrusion systems just is not prevention attack but they are task discovery and probably identify attacks and security difficult is in system or computer networks.knowing it is important for the manager.

With the increase use of telecommunication and information technology networks and modern communication tools with computer for example smartphone and other electronic devices driven to a security threat and cyber attacks. A new problem is in network security that eith the method learning machine can use subject for developing research in classification. This method cause of improvement classification accuracy and performance ration

In the article suggested techniques on public data ratio to performance extraction with using genetic algorithm and neural network will do it. So may useful information security engineering and developers is prior to the network is committed to the operation guide.

First of all in second part is the literature reviewer then in third part proposed method and in fourth part methodology and in the end of article conclusions of the discussion method do..

An overview on related works

so far a number of researchers using acombination of genetic algorithm and neural network for intrusion Detection've done.each of these studies is to provide better result in achieving useful patterns are in intusion Detection System.

Gong et al(2009) presented method based of community rules and genetic algorithm programming for detection influsion in network with combination of abuse and anomalies.this method is development of genetic algorithm programming which could detection normaldata,known attacks and unknown attacks.[1]

Yang et al(2010) presented a intrusion detection system combination of using protocol analusis techniques and datamining in this method detection abuse and anomaliesthen yang using decision tree for example Chaid, Ques, C&R was tested on sample data.[2]

Elshoush et al(2011) presented fuzzy method to reduce the rate of false detection with using events correlation that this method has disadvantage because it is impossible to completely prevent computer attacks,intrusion detection system for reducing damages due to computer attacks is logged in the important role if plays with two method.

- Abuse method
- Anomaly method

Elshoush in this article forinflusion detection in networking using CITDS for this above two method. Results arisen from this method has satisfied a unique tracing performance and also in CITDS method with two important points to be raised.

- System architecture CIDS
- Community alarm algorithm

In the result for this article multiple security system increase community alarm because this method just softcomputing for problem provide intrusion detection system. This article using fuzzy logic, softcomputing and another intelligent techniques because of was reduse detection false rate with keep increase detection extraction rate and this result will be an opportunity to acquire large scale CITDS solution.[5]

Li et al(2012) presented method based of svm and remove feature techniques that this method using with combination clustering and PSO algorithm and SVM techniqes couse of increase intrusion detection rate.[17]

Horng(2011) presented method based of combination hierarchical clustering algorithm,simple attribute selection procedure and SVM techniques. That with high quality hierarchical clustering sample data provided by SVM rechniques. In the result this method provide reduce training time, performance. In horng's article using hierarchical clustering algorithm because of a statistical method for grouping data with observation and this subject due to the similarity of this matter and the degree of their proximity to the algorithm is done. Second advantage of this method is blancing between accuracy and complexity in networking that consider thhe impact of its importance does not reduce and third of advantage is decide on the number of clusters ratio to the distance between nodes.[7]

Zhang and chang(2012) presented mehd using algorithm association rules for intusion detection. This method recognized number of attacks and using roughest algorithm for intrusion detection good performance in networking and this method could detection all of them attack.[8]

Penda et al(2012) presented method for intrusion detection using combination classifiers rather than ne classifier. This method do based of detection security computer and network according to the growth of internet in everyday life. Often using simple classifier algorithm in network of data traffic on the network can recognize normal and anormal behavior but this algorithm does not recognize attacks with false alarm rate so to solve this problem this article using combine intelligent classification for intrusion detection in networks. This method in addition to increase performance can in supervised algorithm or learning couse of data filtering with using sample dataset filtering follow then output datas in network using with two clusters and with 10-fold strategy and valid method to produce the final formulation of a group of normal and anormal behavior based of NSL-KDDCUP99 dataset.[9]

Srinivasu and avadhani(2012) presented using genetic algorithm for shipping weight in neural network to intrusion detection. Neural network and genetic algorithm are techniqes for learning and optimized. This article for recognize intrusion using genetic algorithm then using combined neural network this method. In the result recognize normal and anormal behavior with provide classification weight, accuracy and presion.[10]

Horng et al (2011) presented method based of combined hierarchical clustering algorithm as well as a number of important features and simple function that selects and eventually this features combine a series of SVM techniques.this article is couse of reduce train time and increase performance and using KDDCUP99 dataset to check accuracy operation. This method has been performance in detection just Dos attacks and Prob attacks.[12]

Salama et al (2011) presented for detection intrusion using Deep Belief network.this article do reduce features space by SVM techniqes tried to divide samples dataset into 5 categories, researchers in order to train and test recommended system using KDDCup99 dataset until speed and accuracy calculate.[13]

Muda et al(2011) presented recommended system solution for intrusion detection in networking with using supervised learning and unsupervised learning. Muda's article using k-means algorithm for unsupervised train and naïve Bayes algorithm for supervised learning.

First level of algorithm with using k-mean algorithm for grouping data to normal mode or other attacks then with using Naïve Bayesian algorithm for classification nodes.the result to type of attacks of KDDCup99 dataset for used to assess. But this solution is not practical for the actual networks because k-mean algorithm is need more time for processing large data in real networking. That this problem cal leading to bottleneck and impact the system. For this reason to improve method using LBG algorithm that generated k-mean algorithm.

Hanguang, li ,Niyu(2012) presented method for

intrusion detection using roughest algorithm for finding the optimal set theory couse of this article has best operation for all of them recognize attacks.[12]

Zhang (2012) presented method based of incremental decision tree that based on roughset. This method using incremental learning is datamining. Components this method also roughset method for remove redundant features and eventually using reduce features that cause of improved recognition accuracy shang is using invremental learning until intrusion detection. Finally this method in hanguang's article using decision tree and roughset with discretization features can better than other techniques but classification accuracy this algorithm is not the same as the first algorithm (with ID3,DTRS,C4.5) and construction time new model is less than other techniques.[13]

Diyodi, terapati(2015) presented the events correlation techniqes in IDS in networking that there are two basic reasons for intrusion detection. Firest one detection attacks in network are usually based of information and data received through distributed sensors in intrusion detection system, that during the attack in between events are generate so there is aproblem here and it is difficult to access the status od an extensive network attacks. IDS type of snort correlate result with sample event and data collection (Darpa dataset) are train in this article and have in network different times by IpAddress relevant warnings and cause of remove duplicate alerts and additional time will be reduced by the network administrator.that this article network activities in this architecture contains.

- Classified as a low level layer protocos as standard ISO in link layer,network layer and transport layer.
- Application level protocol(example,SMTP,HTTP,FTP)
- The content of email or webpages.

That in this architecture, host activities are contain client,server and router. In this activity user operation to enter the network or sytems are contain. Operation systems and applications software that identified.[14]

Wang,gang,et al(2010) presented this article about set of activities that aims to protect and maintain safe access to the resources developed states and intrusion detection systems to lay down certain rules on the monitoring of their performance limit users that with using neural network to develop a IDS in network is used. These neural network techniques for intrusion detection is composed of a cluster fuzzy and neural networks offerd two reasons for the development of the system.

- Increase accuracy system for detection attacks with reduce repetitions.
- Improve system stability.

In this article in addition to the neural network has also been used genetic algorithm until one of the problems using neural networks to detection intrusion is proper size and its weight of network be solved then in this article genetic algorithm is used to optimize network.

Finally in article comparison with methods that have been proposed in the field of intrusion that each has advanteges and disadvantages are shown in talble1.

Table1-compare the approach taken and proposed intrusion detection method

Intrusion detection system techniques	Advantages	Disadvantages
Signature-based techniques	*Low cost computing *High detection rate for unknown attacks before. *Intrusion detection based of pattern matching or pre configured based of knowledgment	*known attacks can not detection *high false alarm rate.
Detection anomaly behavior techniques	*low false alarm rate for unknown attacks *testing the possibilities for intrusion detection nodes by collecting behavior	*most timing needs to identify attacks *detection accuracy based of collecting behavior or features in network.
Fuzzy logic techniques	*use a quantitative features *providing flexibility for unknown problems in the network	*low detection accuracy ratio artificial neural network.
Community rules techniques	*the use of signatures of know attacks or attacks in the differentiation of abuse detection	*all known attacks can not detection. *scanning requires a database to creat rules.
SVM techniques	*if the correct classification of Sample data network is limited. *massive data on the number of features designed to be used.	*features a separate classification done on why the need for pre-processing needs features.
Proposed method in the article	*reduce error rate *increasing the classification rate	

The proposed Method

Attacks that occure on a computer network of main threats are for network and security, usually all current intrusion detection systems all features are extracted uses from traffic networking until can assess intrusion pattern in network or following are some of the features and patten to the the main point here some of these features in dataset uses in proposed method are that unrelated and it would be

redundancy.in the article for benefit from the effectiveness in the network of intrusion detection technique combines neural network and genetic algorithm in Matlab software is used. The combination of these directions(detection based of anomaly and detection based of abuse) will enhance the intrusion detection until to increase the accuracy of recognition in intrusion detection for this reason an integrated approach to intrusion detection is presented. This proposed method with remove unimportant features and unimportant inputs to network,ability to simplify problem in intrusion detection faster and more accuracy also provide. This problem are shown Block diagram1 until can work manship of the proposed method which is a combination neural network and genetic algorithm we show in figure1.

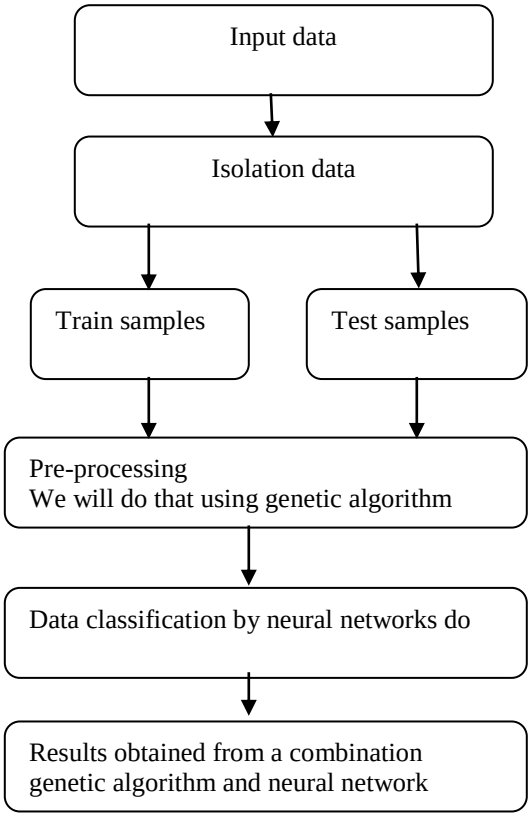

Figure1- structure of the proposed method

As shown in he Blok diagram1 proposed method in two stages do. First of all using with genetic algorithm to reduce the diminstration or apply a standard features on NSL-KDDCup99 dataset until can weight neurons in the network to minimize the maximum target weight. We show steps with genetic algorithm for diminstration in Figure2.

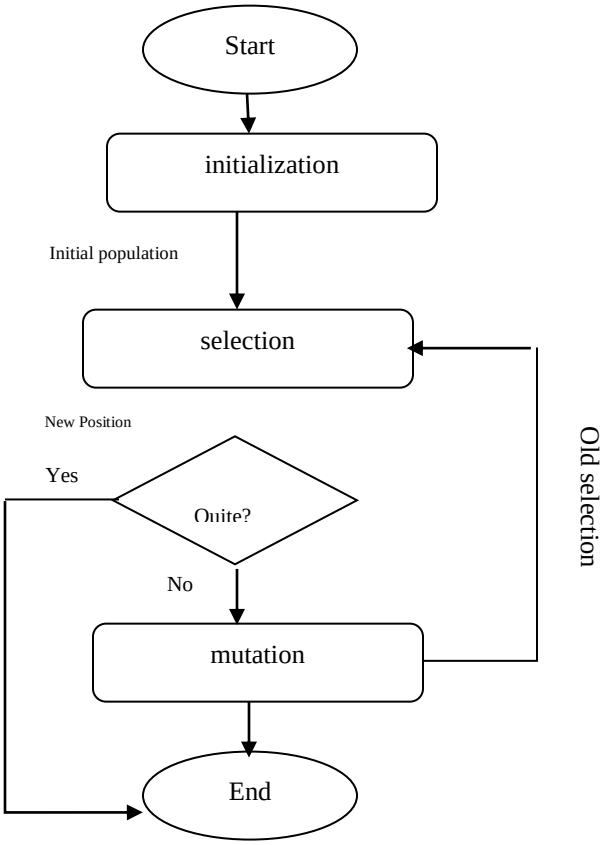

Figure2- Process flowchart genetic algorithm

After training with Genetic Algorithm for minimization weight neurons then test mode conducted with feedback neural network, it does not enhances accuracy but also increase the error rate and second stage without reduce dimension and with 9 main features in NSL-KDDCup99 dataset regarding IDS uses in the article do the test until can minimize weight neurons and with feedback neural network also able reduce error rate and increase accuracy rate. All train and test are done in matlab software and results that are achieved without reducing the demensions of the 9 main features will show better results.

The proposed method is implemented in matlab software with two sectors.

- Clustering for 4 attacks exists in network.
- Neural network interacting with genetic algorithm.

Above two sectors in the direction increasing accuracy and reduce error rate and noise in network using neural network and genetic algorithm. The reason for using genetic algorithm in this article are search , optimization and machine learning until so that we can run tasks in parallel and to identify patterns of using neural network because they are able to publicly respond to the failure of unexpected in network.

In the article presented proposed method in intrusion detection in networking until we can to act as a firewall this work done in Matlab and so using feedback neural network until reduce cost calculation and increase classification accuracy another reason in new method is if one percent of intrusion detection network left and passed the network then realized we could comeback and do a search for intrusion detection to prevent network intrusion.

Next session simulation results of the propsed method we express.

1. Experimental Results and Performance Evaluation of the proposed

In the article training and testing conducted in two steps and a teach the stages of the conclusions reached. First of all using with 9 main features in NSL-KDDCup99 dataset regarding to attacks then second stage with using reduce dimension tools and genetic algorithm done train.

According to the results achieved increase error rate and classification accuracy rate for this reason detection attacks are reduce and minimize, then the basic model is the use 9 main features in terms of classification of attacks, error rate better situation than the reduce dimensions that we will show error minimum training time in the figure3.

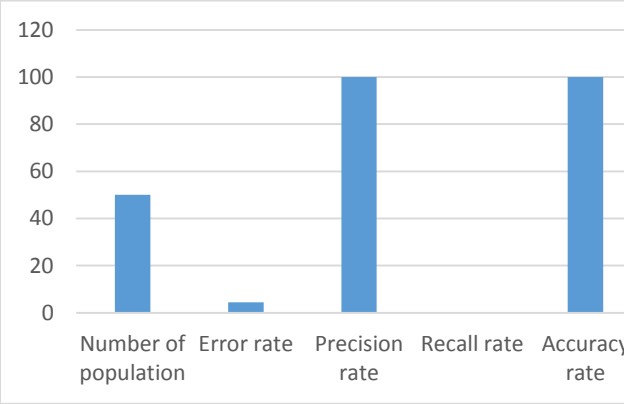

Figure3- minimum error training time

Looking at the chart1 can conclude that genetic algorithm to direction normalization features and using pca tools to reduce dimension of the training network and test it with feedback neural network do.

This work in the article cause of reduce error rate

Accuracy rate	Recall rate	Precision rate	Error rate	Number of population
99.98	0.01	100	4.42	50

and as well as attacks classification rate is too low then so to solve this problem in attacks classification to PSO algorithm with GSA to conclude classification rate near to 100 percent but increase the error rate. Eventually for solve the problem in the article we using combination PSO algorithm and GSA that to conclude classification rate near to 100percent and error rate near to zero below in figure4 we show aggregation nodes in the network.

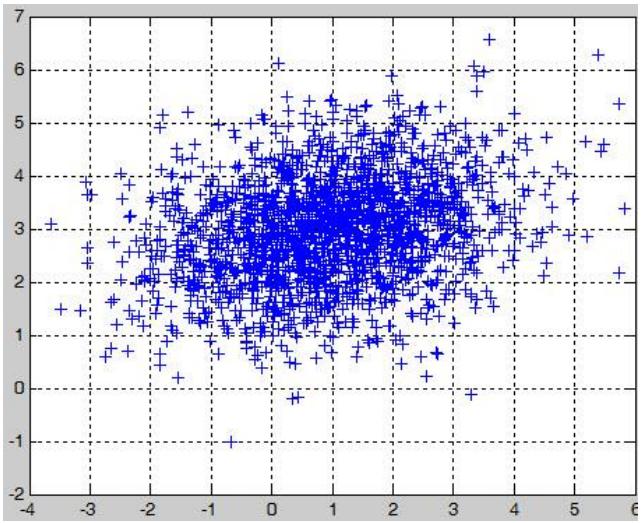

Figure4 – aggregation nodes in network

And the next session we express conclusions and recommendation for future work.

2. Conclusions

So far, many solution have been presented in the field of computer network intrusion detection each of solution regarding IDS has its own advantages and disadvantages but can not they see the method that which can optimize both accuracy and speed parameters. In the article using combination PSO algorithm and feedback neural network on NSL-KDDCup99 dataset and in the case evaluated 80

percent of dataset for train done in matlab and 20 percent for test by neural network proposed method in the article can using with 9 main features of 41 the correct classification of sample to size 99.98 percent almost to near 100 percent rises. The proposed solution can also increase the speed of detection and at the same time in parallel two parameters speed and accuracy makes optimal.

REFERENCES

1) Y. Gong, S. Mabo, C. Chen, (2009). "Intrusion detection system combining misuse detection and anomaly detection using genetic network programming", ICROS-SICE international joint conference,pp. 3463-3467.
2) J. Yang, X. Chen, X._Xiang,_J. Wan, (2010)." HIDS-DT: An effective hybrid intrusion detection system based on decision tree", IEEE international conference on communications and mobile computing, pp. 70-75.
3) H.T. Elshoush, I.M. Osman,(2011)." Alert correlation in collaborative intelligent intrusion detection systems : A survey", applied soft computing, Elsevier, pp. 221-238
4) H.T. Elshoush, I.M. Osman, (2011)." Reducing false positives through fuzzy alert correlation in collaborative intelligent intrusion detection systems : A review", IEEE international conference on fuzzy systems , pp. 1-8
5) Li, Yinhui, et al. (2012). "An efficient intrusion detection system based on support vector machines and gradually feature removal method." Expert Systems with Applications , pp. 424-430.
6) J.Zhang, and X.Chen,(2012)."Research on Intrusion Detection of Database based on Rough Set" , International Conference on Solid State Devices and Materials Science, Physics Procedia ,pp.1637-1641.
7) Panda, Mrutyunjaya, Ajith Abraham, and Manas Ranjan Patra, (2012). "A Hybrid Intelligent Approach for Network Intrusion Detection." Procedia Engineering,pp.1-9.
8) P.Srinivasu, and S. Avadhani. (2012). "Genetic Algorithm based Weight Extraction Algorithm for Artificial Neural Network Classifier in Intrusion Detection."Procedia Engineering, pp.144-153.
9) Horng, Shi-Jinn, et al, (2011). "A novel intrusion detection system based on hierarchical clustering and support vector machines." Expert systems with Applications , pp. 306-313.
10) Salama, A.Mostafa, et al. (2011). "Hybrid Intelligent Intrusion Detection Scheme." Soft Computing in Industrial Applications. Springer Berlin Heidelberg, pp-293-303.
11) Z.Muda, et al, (2011)."Intrusion detection based on K-Means clustering and Naïve Bayes classification." Information Technology in Asia (CITA 11), 7th International Conference on. IEEE.
12) Hanguang, Li, and Ni Yu, (2012). "Intrusion Detection Technology Research Based on Apriori Algorithm." Physics Procedia, pp-1615-1620.
13) J.Zhang, and X.Chen, (2012). "Research on Intrusion Detection of Database based on Rough Set ", International Conference on Solid State Devices and Materials Science, Physics Procedia, pp. 1637-1641.
14) S. Singh And R. Singh Kushwah , (2014).”A Study on Intrusion Detection in wireless network by using Genetic Algorithm Application” , International Conference on Computation Intellegence & Communication Network.
15) G. Poojitha And K. Naveen kumar And P. JayaramiReddy , (2010). ” Intrusion Detection using Artificial Neural Network ” , Second International conference on Computing, Communication and Networking Technologies .
16) Wang, Gang, et al ,(2010)."A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering." *Expert Systems with Applications*,
17) Neelam Dwivedi and Aprna Tripathi, (2015)." Event Correlation for Intrusion Detection Systems. " IEEE International Conference on Computation & Communication Technology .