Appliance of Neural Networks in IDS

Vineet Srivastava
Department of Computer Science & Engineering
Dehradun Institute of Technology
Dehradun, India

Abhay Chaturvedi
Department of Computer Science & Engineering
Dehradun Institute of Technology
Dehradun, India

Abstract— With the growing reliance on the internet and other networks the security of these networks has become a major issue as almost all private and government concerns are dependent on the web. Malicious hackers pose serious threats to our networks which lead to the researches in the field of Intrusion detection. In our work we are concerned about attacks that can't be detected by the traditional approaches as intrusions are getting intelligent day by day, so we should be equipped with a more intelligent detection system. For this we are using the soft computing techniques such as artificial neural networks and Multilayer Perceptron as an approach in ANN. Different structures of MLPs are used for the classification of patterns for intrusion detection.

Keywords—IDS, MDM, ADM, Neural Network, MLP

I. INTRODUCTION

The Computing world is rapidly changing with expansion of World Wide networks. Despite of this enormous and gigantic success there are some factors that pose huge amount of threats to these networks as hackers and intruders who are technologically sound enough to use worldwide networked information system for their destructive purposes.

The overheads incurred due to damages caused by illicit access of the intruders to systems have led different organizations to introduce new system applications to observe data flow in their networks. These systems are better known as IDS (Intruder Detection System). Intrusion detection can be defined as a process of monitoring the actions occurring in a computer network or system and analyze them for signs of intrusions defined as attempts to compromise the privacy, veracity, availability, or to bypass the security mechanisms of a computer or a network. Three types of Intrusion Detection System are:

Host-based:
Evaluation of information found on a single or multiple host systems, including contents of operating system's and application files.

Network-based:
Evaluation of information gathered from network, analyzing the stream of packets traveling across the network, which are gathered with help of sensors.

Hybrid:
Evaluation of vulnerabilities in internal networks and firewalls.

Two basic models to analyze events and detect attacks are Misuse Detection Model (MDM), in which IDS detects intrusions by looking for actions that match with known signatures of intrusions or vulnerabilities and the other one is Anomaly Detection Model (ADM), which detects intrusions by searching for abnormal network traffic. Traffic pattern can be defined either as the breach of accepted thresholds for frequency of events in a connection or as a user's violation of the valid profile developed for his/her normal behavior. While anomaly detection uses threshold monitoring to point out when a certain established metric has been reached, a rule based approach is used by misuse detection. When this approach is applied to misuse detection, the rules transform to scenarios for attacks on networks. A potential attack is identified with intrusion detection mechanism if consistency is found between user's activities and the established rules. The use of comprehensive rules is critical in the application of expert systems for intrusion detection.

Commercially, only misuse detection is used instead of anomaly detector due to its limitations (false alarms due to false detections and expensive computations).Which also motivates researchers to create efforts for building anomaly detectors.

The problem we come across is that the intruders are usually intelligent and flexible while IDS follows fixed rules. Solution to this problem can be to use soft computing techniques with IDS. The idea behind the application of soft computing techniques and specifically in artificial neural networks for implementing IDSs is to including an intelligent agent in the system capable of predicting the latent patterns in abnormal and normal connection audit records, and generalizing the patterns to new connection records of the same class.

In current MLP (Multi Layer Perceptron) neural network has been used to implement an offline intrusion detection system. In this study attack type can also be identified which was not there in previous implementation and studies enabling the system to suggest proper solutions against intrusions.

Different MLP structures are inspected to trace a minimal architecture capable of classification of network connection records. The results show that a MLP having single layer of hidden neurons can generate satisfactory classification results.

The generalization capability of final system is increased with the learning procedure of ANN's which is carried out using a validation process which in turn enhances generalization capability of the IDS.

II. PLACEMENT OF IDS ON NETWORK

A. IDS

Intrusion detection can be defined as an act of detecting useless traffic on a network or a device. An IDS can be a software or a hardware device that is use to monitor network traffic for detecting the unwanted action and events such as unlawful and malicious traffic, traffic violating security policies.

Proc. of the Intl. Conf. on Advances in Electronics, Electrical and Computer Science Engineering — EEC 2012
Edited by Dr. R. K. Singh.

ISBN: 978-981-07-2950-9

As we know variety of network configurations are possible or available so in order to cater their need s different types of technologies are used in IDS. Having their own advantages and disadvantage in detection.

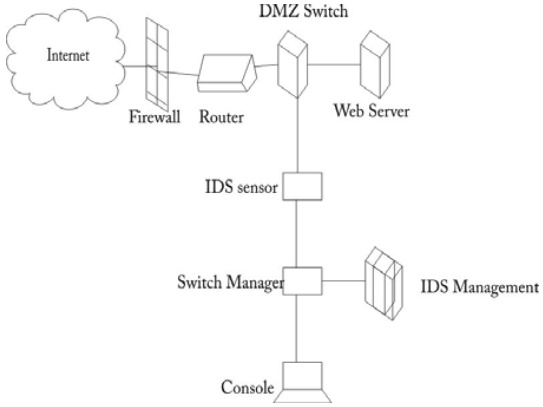

Figure1. Position of IDS sensor in network

B. *Architecture*

Architecture consists of six separate nodes:

- Sensor node:
  It is used to sense the incoming request/information.
- Analyzer node:
  It works in two phases, from client application console to knowledge database. Knowledge database consist of all the familiar and authenticated pattern of information/data analysis node used pattern matching policy to classify intruding information/data currently available at the network channel.
- Response/Control node:
  It accepts the analyzed patterns in feed-forward mode at network channel alongwith in-built policy/control features. If unfamiliar happens then an Alert is generated at network channel.

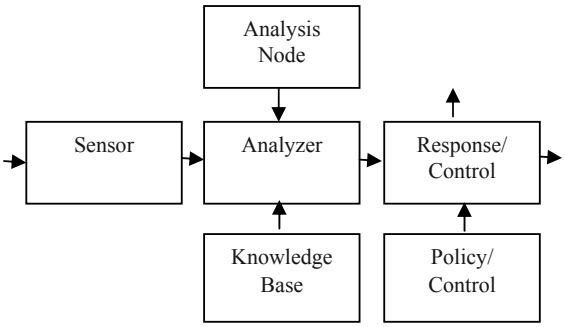

Figure2. IDS working-flow

C. *Types of Attacks*

As we know that there are various types of intrusions/attacks possible like DOS, IP Sweep attacks, POD (Ping of death), Satan, Neptune attack etc which can be classified based on two different models TCP and UDP. A layer wise classification is given in the below table.

TABLE1. TYPES OF ATTACKS AT UDP AND TCP

Layers	UDP	TCP
Application layer	Ping flood attacks	Ping of death,
Transport layer	ICMP attack, Smurf attack, ICMP tunneling,	Port sweep ,IP sweep attack, Neptune,
Network Layer	UDP flood attack	Smurf attacks
Link layer	MAC attacks, ARP attack	Spanning tree protocol attacks, VLAN attacks, DHCP Attacks

III. NEURAL NETWORK APPROACH

Artificial neural networks can be defined as mathematical algorithms that approach the functionality of small neural clusters in a very elementary manner. An Artificial Neural Network is a collection of treatments to convert a collection of inputs into a set of searched outputs with the help of simple processing units or nodes and connections between them.
The artificial analogue of the biological neuron is referred to as a Processing Element s. A neural network comprise of small numbers of PEs (up to thousands). A PE has many input paths from neighboring PEs outputs. Input signals are pooled usually by simply summing up and are transferred to the following PE through the output path.

Neural Networks architectures can be classified into two categories:

D. *Supervised Training Algorithm*

In which there is learning phase, a concerned network learns preferred outputs for a given patterns and inputs. The famous architecture for supervised neural network is a MLP (Multilevel Perceptron). Patterns Recognition requires applicability of MLP.

E. *Un-supervised Training Algorithm*

In which network learns without identifying desired output SOM are most popularly used algorithms in this category of unsupervised training .Topological mapping is found from the input space to clusters with the help of Self Organizing maps, basically employed for classifying problems.

An automatic learning and retaing data coefficient is the most important property of neural networks in accordance with inputs and outputs.

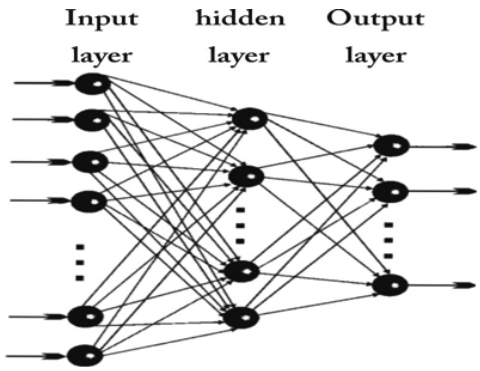

Figure3. Basic Neural Network Architecture

Application of the Neural Network approach to Intrusion Detection requires exposure Neural Networks to normal data and to attacks to automatically regulate coefficients of the neural networks in the phase of training. Performance tests are then conducted with real network traffic and attacks. Neural Networks have been largely employed with success.

IV. MULTI LAYER PERCEPTRON APPROACH

Multilayer perceptron represents the most prominent and well researched class of artificial neural network in classification, implementing a feed-forward, supervised and hetero-associative paradigm. MLPs consist of several layers of nodes, interconnected through weighted acyclic arcs from each preceding layer to the following, without lateral or feedback connections. Each node calculates a transformed weighted linear combination of its inputs of the form, with the vector of output activations from the preceding layer, the transposed column vector of weights, and a bounded non-decreasing non-linear function, such as the sigmoid, with one of the weights acting as a trainable bias connected to a constant input. Three layered MLP showing the information processing within a node, using a weighted sum as input function, the hyperbolic function as sigmoid activation function and an identity output function in Fig.4

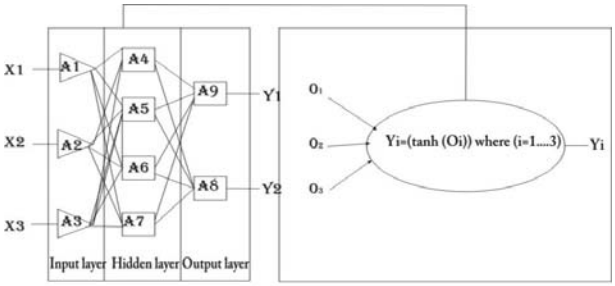

Figure4. Three layer MLP Topology

For pattern classification, MLPs adapt the free parameter through supervised training to partition the input space. To separate distinct classes, MLPs approximate a function of the form which partitions the X_i space inputs into O_i different types of patterns which is processed with help of an intermediate sigmoid function to provide an output in the form of Y_i .

All the processing covers different level of hidden layers for one type of output pattern that's why it is more secure operation instead of neural network.

The representational capabilities of a MLP are determined by the range of mappings it may implement through weight variation. Single layer perceptrons are capable of solving only linearly separable problems. MLPs with three layers are capable to approximate any desired bounded continuous function. The units in the first hidden layer generate to divide the input space in half-spaces. Units in the second hidden layer form convex regions as intersections of these half-spaces.

Given a sufficient number of hidden units, a MLP can approximate any complex decision boundary to divide the input space with arbitrary accuracy, producing a (0) when the input is in one region and an output of (1) in the other. This property, known as a universal approximation capability i.e. the number of nodes and layers, and controlling the network training process to prevent over fitting. As perfect classification on training data does not necessitate generalization for optimal separation of previously unseen data, simpler models with fewer parameters and training using early-stopping with out-of-sample evaluation on separate datasets are generally preferred. The network paradigm of MLP offers extensive degrees of freedom in modeling for classification tasks. Structuring the degrees of freedom, each expert must decide upon the static architectural properties of the network like number of layers, number of nodes in each hidden layer and coding of output vector through nodes in the output layer, connectivity of the weight matrix like fully or sparsely connected, shortcut connections etc. and the activation strategy like feed-forward or with feedback.

Fig. 5 show the block diagram of different types of MLPs, by these types of topological structure we can solve the complexity problems of redundant knowledgebase patterns which is major difficult issues in IDS sensors because intruders generally used similar types of patterns encapsulated with an un-authorized data/information to attack on the network. Since encapsulated messages are impossible to separate from the authorized similar patterned information one can use these types of topological construct to process linear sigmoid function as a threshold of the output patterns. Because an intruder will not always familiar with the hidden topological construct of the network of information, they generally think in a common way of structured mechanism generally used for networking as LAN, WAN, MAN etc.

We use the MLP to overcome this type of problem as an better approach of artificial neural network.

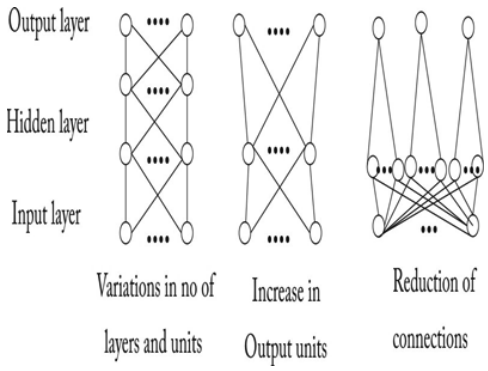

Figure5. Block Diagram of MLPs

CONCLUSION AND FUTURE WORK

In this paper we have proposed and presented techniques of neural networks in an effort towards the betterment and enhancement of the Intrusion detection system. We have presented and examined different structures of Multilayer perceptrons for classification of patterns and used MLP with three layers for training the used artificial neural network.

In near future we would be using different equations for increasing the efficiency of the IDS. Practical IDSs must have several attack types; therefore, it is possible, in future to the present study that includes more attack scenarios in the dataset. In addition to it, avoid unreasonable complexity in the neural network, reducing data further can be an important step as preprocessing of network data. Also some of the different techniques such genetic algorithms can introduced in IDS for its betterment. It is reasonable to expect an improved forensic functionality build in IDS in the near future and that will be used much more in connection in intrusion detection and prevention systems.

REFERENCES

[1] John Zhong Lei, Ali Ghorbani, Network Intrusion Detection Using Improved Competitive Learning Neural Network, 2004.

[2] Kornel Papik, Bela Molnar, Application of neural networks in medicine, 1998.

[3] Tzeyoung Max, Wu Intrusion detection systems, Information assurance tools report, 2009, IATAC6th edition.

[4] Yacine Bouzida, Frederic Cuppens, Neural networks vs. dcision trees for intrusion, 2006

[5] J. Shum and A. Heidar Malki, :Network Intrusion Detection Systems Using Neural Networks", Fourth International Conference on Natural Computation, IEEE 2008.

[6] P. Garcia-Teodoro, J. Diaz-Verdeio, Anomaly-based network intrusion detection: Techniques, systems and challenges, 2009.

[7] Mehdi moradi, Mohammad zulkemine, A Neural Network Based System for Intrusion Detection and Classification of Attacks, 2004.

[8] K. Duraiswamy, G. Palanivel, Intrusion Detection System in UDP Protocol, 2010.

[9] Wikipedia library, http://en.wikipedia.org/wikiMultilayer_perceptron.