Devikrishna K S, Ramakrishna B B / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 4, Jul-Aug 2013, pp. 1959-1964

An Artificial Neural Network based Intrusion Detection System and Classification of Attacks

Devikrishna K S*, Ramakrishna B B**
*(M.Tech, Department of Computer Science, VTU University, Belgaum,
** (Assistant Professor, Department of Computer Science, VTU University, Belgaum)

ABSTRACT

Network security is becoming an issue of paramount importance in the information technology era. Nowadays with the dramatic growth of communication and computer networks, security has become a critical subject for computer system. Intrusion detection is the art of detecting computer abuse and any attempt to break the networks. Intrusion detection system is an effective security tool that helps to prevent unauthorized access to network resources by analyzing the network traffic. Different algorithms, methods and applications are created and implemented to solve the problem of detecting the attacks in intrusion detection systems. Most methods detect attacks and categorize in two groups, normal or threat. One of the most promising areas of research in the area of Intrusion Detection deals with the applications of the Artificial Intelligence (AI) techniques. This proposed system presents a new approach of intrusion detection system based on artificial neural network. Multi Layer Percepron (MLP) architecture is used for Intrusion Detection System. The performance and evaluations are performed by using the set of benchmark data from a KDD (Knowledge discovery in Database) dataset. The proposed system detects the attacks and classifies them in six groups.

Keywords **–** Artificial Neural Network, Multilayer Perceptron, KDD, Intrusion Detection System, Network Security

I. INTRODUCTION

The ubiquity of the Internet poses serious concerns on the security of computer infrastructures and the integrity of sensitive data. With the rapid expansion of computer networks during the past decade, security has become a crucial issue for computer systems. Different soft-computing based methods have been proposed in recent years for the development of intrusion detection systems. The highly connected computing world has also equipped the intruders and hackers with new facilities for their destructive purposes.

Intrusion Detection Systems are designed to identify - preferably in real time unauthorized use, misuse and attacks on information system. IDSs maintains a set of historical profiles for users, matches an audit record with appropriate profile, update the profiles whenever necessary, and reports any anomalies detected. IDS dies not usually perform any action to prevent intrusions; its main function is to alert the system administrators that there is a possible security violation; as such it is a proactive tool rather than a reactive tool. Proposed system is a Network Intrusion Detection System using an Artificial Neural Network approach.

1.1 Classification of Intrusion Detection System

A few number of taxonomies [5] of IDS proposed by different researchers at different time have been describe in this section.

1.1.1 Host-Based Intrusion Detection

A host based IDS resides on the system being monitored and tracks changes made to important files and directories. It takes a snap shot of existing system files and matches it to the previous snap shot. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. Zirkle described host-based IDS as "loading a piece of software on the system to be monitored". This software, which is generally defined as either host wrappers/personal firewalls or agent-based software, performs the following:

- Uses log files and or the system's auditing agents as sources of data and also traffic in and out of a single computer.
- Checks the integrity of system files, and watches for suspicious processes, including changes to system files and user privileges.

1.1.2 Network-Based Intrusion Detection

A network-based intrusion detection system (IDS) monitors and analyzes the traffic on its network segment to detect intrusion attempts. IDS can be made of many sensors, each sensor being in charge of monitoring the traffic passing through its own segment.

The sensors cannot monitor anything outside their own segment or switch. Northcutt described network based intrusion detection system (NIDS) as an ID system that monitors the traffic on its network segment as a data source. Implementation requires:

- The network interface card is placed in promiscuous mode to capture all network traffic

that crosses its network segment; and packets traveling on that network segment.

- A sensor, which monitors the objective, is to determine if packet flow matches with a known signature.
- There are three signatures that are particularly important: first the string signatures that look for a text string that indicates a possible attack. Second the port signatures simply watch for connection attempts to well known, frequently attacked ports. Third the header signatures that watches for dangerous or illogical combinations in packet headers.

1.1.3 Misuse based detection

This type of intrusion detection system contains a database of know vulnerabilities. It monitors traffic and seeks a pattern or a signature match. It operates in much the same way as a virus scanner, by searching for a known identity or signature for each specific intrusion event. It can be placed on a network to watch the network vulnerabilities or can be placed on a host [3]. Signature-based IDS examine ongoing traffic, activity, transaction, or behavior for matches with known patterns of even specific to known attacks and it raises alarm only when the so called match is found. This is why the number of false positive alarms is comparatively less in signature based IDS. If the system is not entirely new i.e. when it has an up to date database of signatures of known attacks, this technique works extremely well [1]. Advantage and Disadvantage:

- Low Rate of False Alarms: The main advantage of misuse detection systems is their ability to detect known attacks and the relatively low false alarm rate when rules are correctly defined. The signatures which are used in rules must be as specific as possible to prevent false alarms.
- Only Known Attacks Detection: The foremost drawback of misuse detection systems is their complete inability in detecting unknown attacks.

1.1.4 Anomaly based detection

Anomaly detection systems are also known as behaviour-based systems. They rely on the fact that intrusions can be detected by observing deviations from the expected behaviours of the system monitored. These “normal” behaviours can either correspond to some observations made in the past or to some forecasts made by various techniques. Everything that does not correspond to this “normal” pattern will be flagged as anomalous. The core process of anomaly detection is not to learn what is anomalous but to learn what is normal or expected. Advantages and Limitations are:

- Unknown Attacks Detection: The main advantage of anomaly detection systems is that, contrary to misuse detection systems, they can detect unknown or novel attacks. They do not rely on any a priori knowledge concerning the intrusions. It is also important to note that anomaly detection systems have not for main purpose to replace misuse detection systems. The very good efficiency of misuse systems in detecting known attacks makes them a perfect complement to anomaly detection systems.
- High Rate of False Alarms: Two factors may lead to a very high rate of false alarms or to a very poor accuracy of anomaly detection systems.

1.2 Artificial Neural Network IDS

The proposed system is a *Neural Network Intrusion Detection Systems*: It utilizes ANN (Artificial Neural Network) as a pattern recognition technique. Artificial Neural Network is an information processing model that is inspired by the biological nervous systems, such as brain, process information. Artificial neural network is the network of individual neurons. Each neuron is a neural network acts as an independent processing element. Each processing element (neuron) is fundamentally a summing element followed by an activation function. The output of each neuron (after applying the weight parameter associated with the connection) is fed as the input to all of the neurons in the next layer [2]. Like human or other brain, neural networks also learn by example or training, they cannot define or program to perform a specific task.

During training, the neural network parameters are optimized to associate outputs (each output represents a class of computer network connections, like normal and attack) with corresponding input patterns (every input pattern is represented by a feature vector extracted from the characteristics of the network connection record). When the neural network is used, it identifies the input pattern and tries to output the corresponding class [6]. The most commonly reported application of neural networks in IDSs is to train the neural net on a sequence of information units, each of which may be an audit record or a sequence of commands. The proposed system presents a new approach of intrusion detection system based on neural network. A multi layer Perceptron [7] is used for intrusion detection.

MLP is a layered feed forward ANN networks typically trained with back propagation. These networks have found their way into countless applications requiring static pattern classification. Their main advantage is that they are easy to use, and that they can approximate any input/output map. The proposed system detects the attacks and classifies them in 6 groups with the hidden layers of neurons in the neural network.

1.2.1 Advantages of Proposed System

The first advantage in the utilization of a neural network in the detection of the network intrusion would be the flexibility that the network would provide. Artificial neural networks are a uniquely power tool in multiple class classification, especially when used in applications where formal analysis would be very difficult or even impossible, such as pattern recognition and nonlinear system identification. Neural networks are able to work imprecise and incomplete data. It means that they can recognize also patterns not presented during a leaning phase. In that case, traditional Intrusion Detection System, based on the signatures of attacks or expert rules, may not be able to detect the new version of this attack [10].

The inherent speed of neural networks is another benefit of this approach. Because the protection of computing resources requires the timely identification of attacks, the processing speed of the neural network could enable intrusion responses to be conducted before irreparable damage occurs to the system.

The most important advantage of Neural Networks in misuse detection is the ability of the Neural Network to "learn" the characteristics of misuse attacks and identify instances that are unlike any which have been observed before by the network [8]. A neural network might be trained to recognize known suspicious events with a high degree of accuracy. While this would be a very valuable ability, since attackers often emulate the "successes" of others, the network would also gain the ability to apply this knowledge to identify instances of attacks which did not match the exact characteristics of previous intrusions.

II. SYSTEM ARCHITECTURE

The main merit of the artificial neural networks includes the ability of faster information processing, the ability of classification and the ability of learning and self organization. Because of these abilities of the artificial neural networks, the network intrusion detection system can analyze the network captured packets and detect whether it would be an intrusion or not. From the view of architecture, the diagram of system includes several modules, which has shown in Fig I.

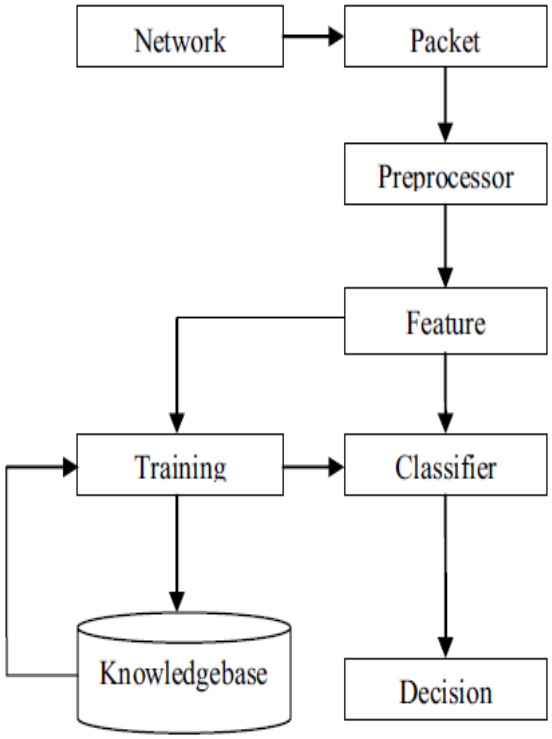

Figure I: Architecture

- **Packet Monitor**

This module monitors network stream real time and capture packets to serve for the data source of the NIDS. The packet capture library provides a high level interface to packet capture system. All packets on the network, even those destined for other hosts are accessible through this mechanism.

- **Pre-processor**

In preprocessing phase, network traffic collected and processed for use as input to the system.

- **Feature Extraction**

This module extracts feature vector from the network packets (connection records) and submits the feature vector to the classifier module. Feature extraction is an important part of a pattern recognition system. The feature extraction process consists of feature construction and feature selection. The quality of the feature construction and feature selection algorithms is one of the most important factors that influence the effectiveness of IDS. Achieving reduction of the number of relevant traffic features without negative impact on classification accuracy is a goal that largely improves the overall effectiveness of the IDS. Most of the feature construction as well as feature selection works in intrusion detection practice is still carried out through manually utilizing domain knowledge.

- **Classifier**

The function of this module is to analyze the network stream and to draw a conclusion whether intrusion happens or not. Neural network classifiers perform very successfully for recognizing and

matching complicated or incomplete patterns. The most successful application of neural network is classification or categorization and pattern recognition. The learning process is essentially an optimization process in which the parameters of the best set of connection coefficients (weighs) for solving a problem are found and includes the following basic steps [9]:

- Present the neural network with a number of inputs.
- Check how closely the actual output generated for a specific input matches the desired output.
- Change the neural network parameters to better approximate the outputs.
- Decision When detecting that intrusion happens, this module will send a warning message to the user.
- Knowledgebase

This module serves for the training samples of the classifier phase. The Artificial Neural Networks can work effectively only when it has been trained correctly and sufficiently. The intrusion samples can be perfected under user participation, so the capability of the detection can improve continually.

All of these modules together make the NIDS architecture system based on the artificial neural networks. The present study is aimed to solve a multi class problem in which not only the attack records are distinguished from normal ones, but also the attack type is identified.

2.1 Live Data Capturing

Fig II shows a normal program flow of a Pcap application. Pcap is an open source library that provides a high level interface to network packet capture system. It is the core part of many packet sniffers such as Snort, tcpdump, ect. The main objective was to create a platform independent API to eliminate the need for system dependent packet captures modules modules in each application. Lib Pcap will also provide additional functionalities such as dumping packets to capture files, injecting packets, getting statistics, ect.

The first required thing is a network interface to listen on. It can either specify explicitly or let libcap get one for the application. Once the name of the network device is obtained, next step is to open that particular device. Then it captures the frames with in a particular time, and processes it. Then it closes the interface.

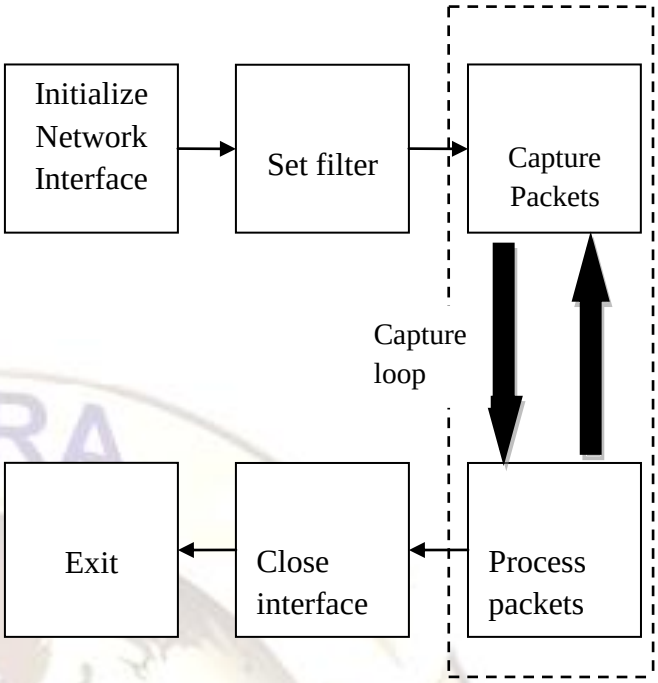

Figure II: Normal Program Flow of a Packet Application

WinPcap is state of the art software for Windows environments: it allows applications to capture and transmit network packets bypassing the protocol stack; it also has additional useful features which includes kernel-level packet filtering, a network statistics engine and support for remote packet capture.

2.2 Classifier

The number of the hidden layer: In general application, one hidden layer is enough, but here setting two hidden layers in the Classifier module, consequently we have a three layers neural network.
The dimension of the input layer and the output layer: Generally speaking, the dimension of the input layer is the number of the features selected, and the dimension of the output layer is the number of sorts that can be classified by the Classifier.
The transfer function: In general, the function *Logsig(x)* = 1/ (1+ exp (-x)) can be used in the Classifier model.
The learning function: *trainGD* function can be used in the Classifier which works based on Back-propagation algorithm.
Initialization of the weight: Initially weights are selected randomly between the values [0 to 1].

2.3 KDD Cup'99 Intrusion Detection Dataset

The dataset Network Intrusion Detection was chosen from The UCI (University of California, Irvine) KDD (Knowledge Discovery in Databases) Archive [4]. The dataset is the collection of network related information that was captured over a period of time. The data consists of a number of basic features: duration of the connection, protocol type, such as

TCP, UDP or ICMP, service type, such as FTP, HTTP, Telnet, status flag, total bytes sent to destination host, total bytes sent to source host, whether source and destination addresses are the same or not, number of wrong fragments, number of urgent packets.

Each record consists of 41 attributes and one target. The target value indicates the attack name. There are 41 features for each connection. Specifically, "a connection is a sequence of TCP packets starting and ending at some well-defined times, between which data flows from a source IP address to a target IP address under some well-defined protocol". Features are grouped into four categories:

- *Basic Features:* Basic features can be derived from packet headers without inspecting the payload. It includes the features such as protocol-type, service-type, duration, flag etc.
- *Content Features:* Domain knowledge is used to access the payload of the original TCP packets. This includes features such as number of failed login attempts.
- *Time-based Traffic Features:* These features are designed to capture properties that mature over a 2 second temporal window. One example of such a feature would be the number of connections to the same host over the 2 second interval.
- *Host-based Traffic Features:* Utilize a historical window estimated over the number of connections instead of time.

III. CONCLUSION

An approach for a neural network based intrusion detection system, intended to classify the normal and attack patterns and the type of the attack is proposed. When the neural network parameters were determined by training, classification of a single record was done in a negligible time. Therefore, the neural network based IDS can operate as an online classifier for the attack types that it has been trained for. The proposed system presents a new approach of intrusion detection system based on neural network. Artificial neural networks are inspired by the learning processes that take place in biological systems.

Artificial neurons and neural networks try to imitate the working mechanisms of their biological counterparts. Learning can be perceived as an optimisation process. Neural networks can be considered as nonlinear function approximating tools (i.e., linear combinations of nonlinear basis functions), where the parameters of the networks should be found by applying optimisation methods. A Multi Layer Perceptron (MLP) is used for intrusion detection system. The results show that the implemented and designed system detects the attacks and classify them in six groups. KDD Data set is used for the training and evaluation of the ANN classifier.

The most commonly reported application of neural networks in IDSs is to train the neural net on a sequence of information units, each of which may be an audit record or a sequence of commands. The ability of neural networks to learn and generalize in addition to their wide range of applicability makes them very powerful tools.

From the practical point of view, the experimental results imply that there is more to do in the field of artificial neural network based intrusion detection systems especially solving irrelevant outputs. The implemented system solved classification problem. Its further development to several classes is straightforward. As a possible future development to the present study, one can include more attack scenarios in the dataset. Practical IDSs should include several attack types. In order to avoid unreasonable complexity in the neural network, an initial classification of the connection records to normal and general categories of attacks can be the first step. The records in each category of intrusions can then be further classified to the attack types.

REFERENCES

[1] James Cannady, "*Artificial Neural Networks for Misuse Detection*," Proceedings of the 1998 National Information Systems Security Conference (NISSC'98), Arlington, VA, 1998.

[2] J. Ryan, M. Lin, and R. Miikkulainen, "*Intrusion Detection with Neural Networks*," AI Approaches to Fraud Detection and Risk Management: Papers from the 1997 AAAI Workshop, Providence, RI, pp. 72-79, 1997.

[3] Srinivas Mukkamala, "*Intrusion Detection using Neural Networks and Support Vector Machine*," Proceeding of the 2002 IEEE International Honolulu, HI, 2002.

[4] Mukherjee, B., Heberlein, L.T., Levitt, K.N, *Network Intrusion Detection*. IEEE Network. pp. 28-42, 1994.

[5] Kabiri P, Ghorbani A, "A. Research in intrusion detection and response - a survey". International Journal of Network Security, 2005.

[6] Helman, P., Liepins, G., and Richards, "*Foundations of Intrusion Detection*". In Proceedings of the Fifth Computer Security Foundations Workshop pp. 114-120, 1992.

[7] K. Hornik, M. Stnchcombe and H White, *Multilayer Feed forward Networks are Universal Approximators, Neural Network*,2:pg359- 366,1989.

[8] Anderson, D., Frivoid, T. & Valdes *Next-generation Intrusion Detection Expert System* (NIDES): A Summary. SRI International Technical Report SRI-CSL-95-07, 1995.

[9] Sammany, M, Sharawi, M, El-Beltagy, M &Saroit, I. (2007). *Artificial Neural Network Architecture for Intrusion Detection Systems and Classification of Attacks.* Faculty of Computers and Information Cairo University. Retrieved October 18, 2011, from http://infos2007.fci.cu.edu.eg/Computational%20Intelligence/071777.pdf.

[10] Tavallaee, M, Bagheri, E, Lu, W & Ghorbani, A. (2009). A Detailed Analysis of Computational Intelligence in Security and Defence applications (CISDA 2009). Retreived October 25, 2011, from http:www.tavallaee.com/publications/CISDA.pdf.