Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 3, March 2013, pg.1 – 3

RESEARCH ARTICLE

Various Approaches for Detecting Attacks in Intrusion Detection System

Purva Adlakha [1], *Prof. Priti Subramanium* [2]

[1]**Department of Computer Engineering, JTM COE, Faizpur, Maharashtra, India**

purva.adlakha@gmail.com

[2]**Department of Computer and Science Engineering, SSGB COET, Bhusawal, Maharashtra, India**

pritikanna559@gmail.com

Abstract— The rapid development of computer networks and more importantly internet has created many security problems such as ever growing new intrusions on computer network systems. To secure this system strong intrusion detection system has to be build. An intrusion detection system monitors all inbound and outbound network activity and identifies suspicious activities that attempting to break and violate security of system. In this paper we have taken review of various approaches of Intrusion detection which includes SVM (Support Vector Machine) system, SOM (Self Organising maps), MLP (Multi-Layer Perceptron).For detecting intrusions this approaches goes through three phases pre-processing in which raw data is converted into machine readable form then training of data is performed and in the last measure the performance on testing data.

Key Terms: - Intrusion Detection, Multi-Layer Perceptron, Self-Organising Maps, Support Vector Machine.

I. INTRODUCTION

Because of existence of Internet and high usage of computer network for Internet by people, companies and governments security plays a highly important role to prevent the attacks. A single intrusion of a computer network can result in the drastic loss as large amounts of data is on stake which cause users to question about reliability of network on which huge amount of information lies. The cost of data loss which may be permanent or temporary is so high which cause companies to set up monitoring system that monitors data flow in their network. These systems are generally referred as Intrusion Detection System.

Intrusion Detection System (IDS) can be either software or hardware based that monitor's network activity and delivers an alert if it notices some unauthorized activity. There are two general categories of attacks which intrusion detection systems attempt to identify - anomaly detection and misuse detection. Anomaly detection identifies activities that vary from established patterns for users, or groups of users. Anomaly detection typically involves the creation of knowledge bases that contain the profiles of the monitored activities .Misuse detection involves the comparison of a user's activities with the known behaviours of attackers attempting to penetrate a system. It frequently utilizes a rule-based approach.

Current approach for detecting intrusion in Intrusion Detection System utilizes some form of rule-based analysis .Which relies on sets of predefined rules that are provided by an administrator, or created by the system, or both. For example: Expert systems are the most common rule based system. An expert system consists of a set of rules that encode the knowledge of a human "expert". These rules are used by the system to make conclusions about the security-related data from the intrusion detection system. But it requires frequent updates to remain current. At a minimum, this leads to an expert system with reduced capabilities. At worst, this will degrade the quality of the entire system by misleading the user that the system he is using is secure. Basically this system result in inefficient system that is not able to detect attacks which are slightly different from predefined rule set. Mainly expert system suffers from updating, searching and matching of the rule set.

This paper presents a review on Support vector machine, Self-organizing maps and lastly we will see Multi-layer Perceptron and analyse their applicability in identifying instances of attacks against network and also see how they overcome some of the problems faced by Rule-based system.

II. Literature Survey

A. Support Vector Machine SVM-IDS

Support vector machines (SVM) are a learning technique which has been applied in many application areas. It plots the training vectors in high dimensional feature space, labelling each vector by its class. Intrusion detection can be a two-class classification problem or multi-class classification problem. SVMs look it as a quadratic optimization problem in which they combine generalization control with a technique to prevent the “curse of dimensionality” by placing an upper bound on the margin between the different classes, making it a practical tool for large and dynamic data sets. SVM classify data by using support vectors that outline the hyper plane in the feature space. The number of parameters used in the SVMs depends on the margin that separates the data points but not on the number of input features, thus SVMs do not require a reduction in the number of features in order to avoid over fitting. SVMs provide a generic mechanism to fit the surface of the hyper plane to the data through the use of a kernel function. Its training time is significantly shorter (17.77 sec vs. 18 min)[1], and it prove advantageous in situations where retraining needs to be done quickly. The main disadvantage of SVM is that it can only make binary classification where intrusion detection requires all 22 different types of attacks.

B. Artificial Neural Network

. Artificial neural network is highly inspired by biological neuron. It tries to represent the thinking process through electronic circuit or software. It is form by collection of processing elements that are highly interconnected and transform a set of inputs to a set of desired outputs [2]. Expert systems, which can provide the user with a definitive answer on the basis of characteristics which exactly matches with the one coded in rule base, But ANN provides information analysis in the form of probability estimates that the data matches the characteristics which it has been trained to recognize. To implement ANN it requires three basic steps, the following steps are given.

- Firstly, number of inputs are present to the network
- Secondly, evaluate how closely the actual output generated for a specific input matches the desired output.
- Thirdly, change the parameters of neural network to better approximate the outputs

ANN comprise of two different learning methods: supervised and unsupervised. In supervised learning method, the network learns the desired output for a given input or pattern. Example of supervised neural network is the Multi-Layer Perceptron (MLP); the MLP is used for Pattern Recognition problems. In unsupervised learning method, the network learns without specifying desired output. Example of unsupervised neural network is Self-Organizing Maps (SOM). SOM are used for classification problems.

1. Self-Organizing Maps

Self-Organizing Map uses a single layer of neurons to represent knowledge from a particular domain in the form of a geometrically organized feature map. The network was designed to learn the characteristics of normal system activity and identify statistical variations in the form clusters from the norm that may be an indication of a virus. Basically in this routine traffic that represents normal behaviour would be clustered around one or more cluster centers and any irregular traffic representing abnormal and possibly suspicious behaviour would be clustered outside of the normal clustering. It provides a simple and efficient way to classify data sets in real-time, SOMs to be best suited as Intrusion detection system due to their high speed and fast conversion rates [3]. SOM approach is better for DOS and Probe attack as compared to user to root and root to local attack [4].

2. Multi-layer Perceptron

A Multilayer perceptron maps sets of input data onto a set of appropriate output. An MLP consists of multiple layers of nodes in a directed graph, with each layer fully connected to the next one. Except for the input nodes, each node is a neuron with a nonlinear activation function. Each of the reviewed recommenders has a different approach of applying supervised learning to intrusion detection system.

- The approach proposed in [5] utilized MLP for detecting intrusion in Intrusion detection system. The prototype designed is mainly used to identify indication of misuse. The architecture of the system consisted of four fully connected layers with nine input nodes and two output nodes. While number of hidden layers, and the number of nodes in the hidden layers, was determined based on the process of trial and error. Data for training and testing the prototype was generated using the RealSecure™ network monitor from Internet Security Systems. RealSecure™ uses an expert system that includes over 360 attack signatures that it compares with current network activity to identify intrusions. The results show that MLP correctly identify each of the imbedded attacks in the test data. But this prototype was not designed to be a complete intrusion detection system. The outcome of the proposed system clearly demonstrates the capability of a neural network to detect only individual instances of possible misuse from a network data stream.
- The author of [6] propose system based on the assumption that every time when user use the system, he leaves a print then neural network based on Multi-layer perceptron can be used to identify user based on what commands they used during a day. Then at the end of day system is run to see user session matched with normal pattern or not. If users' session does not match investigation is launched by NNID (Neural network intrusion detection system). This approach constitutes promising result to anomaly intrusion detection. The proposed system is not suitable for real time detection as it required vast training which proves it to be expensive.

The system implemented in [7] proves its validity in the field of ANN. In previous studies given in [4] [5] the implemented system had the capability of detecting normal or attack connection. But prototype designed for [6] assumes more general problem where attack type is also detected and provide preventive actions against attack type detected and the result provide approximately 90.78% accurate classification and remaining irrelevant outputs are put into false negative category.

III. CONCLUSIONS

Various approaches of detecting attacks in Intrusion Detection System helps system administrator to detect attack categorize into two main groups normal or threat. Some methods not only detect attack but, also provide information about type of the attack and preventive measures takes against the attack.

REFERENCES

[1] Srinivas Mukkamala, "Intrusion Detection Using neural networks and support vector machines," Proceeding ot he 2002 IEEE International Honolulu, HI, 2002.

[2] H.Debar, M.Becker, and D.Siboni, "A neural network component for an intrusion detection system," Proceeding of 1992 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California, pp. 240 - 250, 1992.

[3] Hamdan.O.Alanazi, Rafidah Md Noor, B.B Zaidan, A.A Zaidan, "Intrusion detection system: overview," Journal of Computing, vol 2, no.2, pp 130-133, Feb. 2010.

[4] H. Giinev Kayacik, A. Nur Zincir-Heywood, and Malcolm I. Heywood, "On the Capability of an SOM based Intrusion Detection System." Proceedings of the 2003 International Joint Conference on Neural networks. vol 3, pp 1808 – 1813, July 2003

[5] James Cannady, "Artificial Neural Network for misuse detection." Pro ceeding of the 1998 National Information System Conferences (NISSC'98), Arlington, VA, 1998.

[6] J. Ryan, M. Lin, and R. Mukkulainen, "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.

[7] Norouzian, M.R.; Merati, S., "Classifying Attacks in a Network Intrusion Detection System Based on Artificial Neural Networks" Proceedings of the Advanced Communication Technology (ICACT), 2011 13th International Conference on Publication Year: 2011, Page(s): 868 – 873, 2011.