Sublime Design of an Encroachment Perception System

G. Brindha* and T. Hemalatha

Abstract

The rapid growth and deployment of network technologies and Internet services has made security and management of networks a challenging research problem. This growth is accompanied by an exponential growth in the number of network attacks, which have become more complex, more organized, more dynamic, and more severe than ever. These attacks can easily cause millions of dollar damage to an organization. Detecting these attacks is an important issue of network security. Current network protection techniques are static, slow in responding to attacks, and inefficient due to the large number of false alarms. Therefore there is an increasing need for building effective security monitoring and detection system such as Intrusion Detection System to prevent such illicit accesses. Intrusion Detection System provide defense mechanism which monitors (oversees) user activity and network traffic to identify suspicious activity or patterns that may suggest potential intrusion or attack. Intrusion Detection attempts to detect computer and network traffics by examining various data records observed in processes on the network. Intrusion Detection System is split into two groups misuse detection system and anomaly detection system.

We present two network Intrusion Detection models which can efficiently detect both known and unknown types of network attacks with a high detection rate and low false alarms. The first model is signature based intrusion detection using neural networks. We have used two neural networks, the first one is traditional Hamming net and MAXNET. The second one is multi layer Perceptron with different architecture and training algorithms to find the best one, and we have compared between the two networks. After that we do an enhancement to the hamming network to give better performance.

The second model is anomaly based intrusion detection using neural network. We used two networks, the first one is hamming net and MAXNET, the second one is multi layer Perceptron. After that we do an enhancement to the model to make it work better. We use hybrid fuzzy clustering with neural network to produce a new model with better performance. We used the data for training and testing the models from KDD Cup99 data set.

We have successfully implemented Intrusion Detection models. The experimental results of the intrusion detection model shows that the system can efficiently and effectively detect and protect against any type of network attacks.

Keywords: Sublime design.

Introduction

The Internet is pervading almost every aspect of life and business, and along with this exponential growth comes the critical need to secure these systems from unauthorized disclosure, transfer, modification, or destruction. In the meantime, the networks inevitably become the targets of computer attacks and the attacks can easily cause millions of dollar damage to an organization. According to the annual report from the Computer Emergency Response Team (CERT) [20], only 8 computer security incidents were documented in 1988 but over 130,000 in 2003. Since 2004, CERT no longer publishes the number of incidents because the attacks against Internet-connected systems have become so commonplace. Not only are those attacks increasing in a fast pace, they are also becoming more sophisticated with the advances of technology [89].

Network attacks typically exploit vulnerabilities in networks, system software and protocols. For example, some attacks misuse network resources’ limitations, protocol vulnerabilities, or application vulnerability to reach their goals. Furthermore, these attacks also vary in their speed, complexity, and dynamicity [101]. The increase in the number of attacks and their complexity is due to an increase in the number of applications with vulnerabilities and the number of attackers equipped with fast networks and processing units. Complex network attacks like these present a significant threat to
the security of information infrastructure and can lead to catastrophic results [101]. Therefore, we must try to detect these attacks/intrusions as they occur so system administrators can take actions to repair the damage and prevent further harm.

Intrusions are actions that attempt to bypass security mechanisms of computer systems. So they are any set of actions that threatens the integrity, availability, or confidentiality of a network resource [94]. Confidentiality requires that information be accessible only to those authorized for it, integrity requires that information remain unaltered by accidents or malicious attempts, and availability means that the computer system remains working without degradation of access and provides resources to authorized users when they need it [78].

Intrusion falls into two categories: outsiders and insiders. Outsiders are intruders who approach other's system from outside their network and who may attack their external presence. They may also try to go around the firewall and attack machines on the internal network. Insiders, in contrast, are legitimate users of other's internal network who misuse privileges, impersonate higher privileged users, or use proprietary information to gain access from external sources [48].

Many organizations have developed a variety of technologies to secure their systems and information against intruders. These technologies protect systems and information, detects unusual or suspicious activities, and respond to events that affect security [64]. One of the commonly applied technology is the firewall. A firewall is a collection of hardware and software designed to examine a stream of network traffic and service requests [64]. Traditionally, the firewall is considered as the first line of defense, but the unsophisticated firewall policy cannot meet the requirements of some organizations, which need high security [3]. However, firewalls can not provide complete protection against intrusions. A firewall can serve as an effective noise filter, stopping many attacks before they can affect an organization's network. However, firewalls are vulnerable to errors in configuration and suffer from ambiguous or undefined security policies [69].

Thus, it is very important to design a security mechanism for preventing unauthorized access to the system resources and data. Intrusion Detection (ID) has been at the center of intense research in the last decade owing to the rapid growth of these attacks. Typically Intrusion Detection refers to a variety of techniques for detecting attacks in the form of malicious and unauthorized activities both at the network and host level [45].

**Conclusion**

In this paper, the two intrusion detection models were designed. The first model is signature-based intrusion detection and the second model is anomaly-based intrusion detection.

**Signature-based id model**

The signature-based ID model was implemented by using neural networks. Two models were designed; the first model used traditional hamming and MAXNET networks and the second model used MLP network.

The experiments made in chapter 5 signifies that the model does not give 100% detection rate, therefore an enhancement to traditional hamming network was made. The first change that was incorporated in to hamming network was the input value. It was not converted into binary bipolar values, it was converted to binary when the input was compared with exampler. The second change was to the examplar matrix, it took the same value of input (without converting to binary bipolar). In the examplar matrix the signature of attacks was stored. The result of new hamming network is better than the traditional one, it had 100% detection rate with 0 false alarm.

The packet sniffer for capturing packet director from the internet was also designed, that may helps the other researchers to capture and control the incoming and outgoing packets between the computer and the internet.

**Anomaly-based id model**

The anomaly-based intrusion detection model was also implemented by using neural networks. Two models were designed; the first model used hamming network and the second model used MLP network.

The first model was used to classify normal packet and the four types of attack, the result is low detection rate with high false positive and false negative.

In the second model many experiments were conducted to find out the best architecture with best classification and it was found that MLP was very good in classification of attack types and low performances in classification attack types with normal packets.

**Future work**

During the development of this work, we found some ideas and suggestions which can be used in future developments.
These enhancements are listed below:

1. Use the two enhancement models in one model and then use it for distributed systems and mobile agents.
2. Use fuzzy logic or Fuzzy Inference Systems such as Sugeno and Mamdani Methods.
3. Use petri net theory in intrusion detection system modeling.

References


20. CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University. URL: http://www.cert.org (Last browsed in May 2010).
25. Dima novikov, Roman V.Yampolskiy, and Leon Reznik, "Anomaly Detection based


ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449 (ISRA), Impact Factor: 2.114


51. McCulloch W. S. and W. Pitts, A logical calculus of the ideas immanent in nervous
53. Moazzam Hossain, "Intrusion Detection with Artificial Neural Network", University of Denmark, Denmark, 2004.
60. Qinglei Zhang, "A New Intrusion Detection System Based on the Combination of Support Vectors and Ant Colony: Algorithm and Implementation", Trent University, Peterborough, Ontario, Canada, 2009.