Intrusion Detection System Using Neural Networks

Wei Chen
CS 5314 Artificial Intelligence

Overview

- Introduction
- Several Methods to detect intrusion
- A model of Intrusion detection System(IDS) using artificial neural networks(ANN)
- Analysis of IDS using ANN.
- Conclusion

Introduction

- What is Intrusion ?

  Intrusion refers to any unauthorized access, unauthorized attempt to access or damage, or malicious use of information resources.
- Necessity Intrusion Detect Systems.

1. With the growing rate of interconnections among computer systems, network security is becoming a real challenge.
2. IDSs are designed to protect availability, confidentiality and integrity of critical networked information systems.

Type of IDS

Early research into IDS suggested two major detection principles:

- Anomaly Detection

  Attempts to quantify the usual or acceptable behavior and flags other irregular behavior as potentially intrusive.
- Misuse Detection

  Attempts to flag behavior that is close to some previously defined pattern signature of a known intrusion.

Methods to detect intrusion

1. Expert System
   - Most common form of rule-based intrusion detection approache.
   - Rule-bases analysis relies on sets of predefined rules that are provided by an administrator, automatically created by the system, or both.
   - Requires frequent updates to remain current.
   - Less flexibility in the rule-to-audit record representation.
2. Statistical Method
   - Often used to measure how anomalous the behavior is.
   - Requires that the distribution of subject's behavior is known.
   - Pattern matching techniques are used to determine whether the sequence of events is part of normal behavior.

Methods to detect intrusion

3. Artificial Neural Networks
   - ANNs have recently been proposed as alternatives to the statistical analysis components of anomaly detection system.
   - Intrusion detection using neural networks is more flexible.
   - The inherent ability of neural networks can learn the characteristic of attacks.

Example: Real Time detection(NSOM)

Model:

A Real-Time Network-based Intrusion Detection System Using Self-Organizing Maps.

Hypothesis:

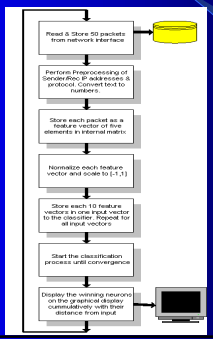
- The routine traffic that represents normal behavior would be clustered around one or more cluster centers ;
- Any irregular traffic representing abnormal and possibly suspicious behavior would be clustered outside of the normal clustering.

Data collection:

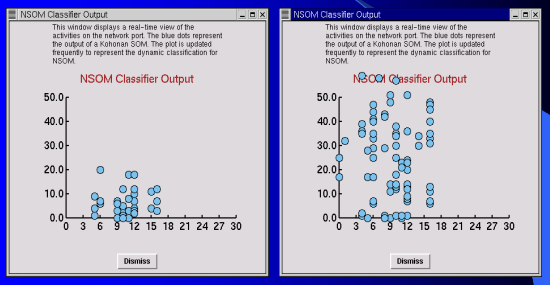
Use a host PC running Linux as the primary test bed. The system is connected to a network using Ethernet controller.

NSOM

- Data processing:



NSOM(result)



NSOM(result)

- Compare Y value on the graphs:

1. The attack neurons were much higher than normal ones.
2 Since Y values represent the distance of the winning neurons with respect to the input vector, we can conclude high Y value neurons represent uncommon and irregular behavior and therefore a possible attack.

Analysis

- This model shows that we were able to classify simulated DoS(Denial of service) attacks graphically as opposed to normal traffic, by showing different clustering of output neurons.
- Training requires more data, which may need more disk space and CPU resource.
- In order to analyze system log, the operating system must keep all performed action information.

Conclusion

- Introduced the background of intrusion detection systems.
- Analized existing methods of IDS
- Intrusion detection using neural networks displayed substantial promise and it especially suited for multi-category classification.

Reference

- [1] helman, P., Liepins, G., and Richards, W.(1992) Foundations of Intrusion Detection. *In Proceedings of the 5th Computer Security Foundations Workshop pp.114*-220
- [2] Jake Ryan, Meng-Jang Liu, *Advances in Neural Information Processing Systems 10,* Cambridege,MA: MIT Press, 1998
- [3] Denning D (Feb, 1987) *An Intrusion-Detection Model*. IEEE Transactions on Software Engineering, Vol. SE-13, No 2.
- [4] Anderson, James P., *Computer Security Treat Monitoring and Surveillance.* James P. Andderson Co., Fort Washington, Pa., 1980.
- [5] Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., and Stoner, E., *State of the Practice of Intrusion Detection Technologies.* CMU/SEI-99-TR-028, Carnegie Mellon University, Software Engineering Institute, Jua.2000.
- [6] Sebring, M., Shellhouse, E., Hanna, M.& Whitehurst, R.(1998) Expert Systems in Intrusion Detection: A Case Study. In *Peoceeding of the 11th National Computer Security Conference.*
- [7] James Cannady, Artificial Neural Networks for Misuse Detection.
- [8] Cramer, M., et. Al. (1995) New Methods of Intrusion Detection using Control-loop Measurement. In P*roceeding of the Technology in Information Security Conference* (TISC) '95.
- [9] Debar, H., Becke, M., &Siboni, D.(1992). A Neural Network Component for an Intrusion Detection System. In *Proceeding of the International Joint Conference on Neural Networks.* pp. (II) 478-483
- [10] Fox, Kevin L., Henning, Rhonda R., and Reed, Jonathan H. (1990). A Neural Network Approach Towards Intrusion Detection. In *proceeding of the 13th National Computer Security Conference.*
- [11] Rhodes B., Mahaffe J., Cannady J., Multiple Self-Organizing Maps for Intrusion Detection. *Proceeding of the NISSC 2000 conference.*