A Comparative Analysis of Artificial Neural Network Technologies in Intrusion Detection Systems

SHAHBAZ PERVEZ, IFTIKHAR AHMAD, ADEEL AKRAM, SAMI ULLAH SWATI
University of Engineering and Technology, Taxila, Pakistan

Abstract: - Intrusion Detection is a major focus of research in the security of computer systems and networks. This paper presents an analysis of Artificial Neural Networks (ANN) being used in the development of effective Intrusion Detection Systems for computer systems and computer networks. The ANNs technologies, which are discussed, are designed to detect instances of the access of computer systems by unauthorized individuals and the misuse of system resources. A review of the foundations of Intrusion Detection Systems and other ANNs, which are the focus of current development efforts, is presented. The results of comparative analysis of different ANNs in Intrusion Detection are discussed. Finally, a discussion of the future ANN technologies, which guarantee to enhance the ability of computer systems to detect intrusions is provided.

Keywords: Artificial Neural Network, Intrusion Detection, Anomaly Detection, Misuse Detection, Computer Security.

INTRODUCTION

The dependence of companies and government agencies on computers and computer networks is rising and the importance of protecting them from attacks is of great concern. A single intrusion of a computer network can result in complete loss, unauthorized utilization or modification of private data and degrades or trusts the reliability of network. Afterwards, the network users tend to distrust these resources. There are several methods of responding to a network intrusion, but they all require the precise and well-timed identification of the attack [1].

This paper discusses the current research and development efforts to detect internal and external penetrations of computer systems and networks in the field of Artificial Neural Networks. The area of Intrusion Detection is central to the concept of computer security.

This paper is divided into three primary areas. The first section provides an overview of Intrusion Detection fundamentals. These include the metrics which are commonly used for quantitative analysis of available data, the models which attempt to identify anomalies, and approaches which are utilized most often in the development of Intrusion Detection Systems. The second section describes some of the current ANN technologies and methodologies, which are being developed in the area of Intrusion Detection research. Finally, the results of comparative analysis are presented.

1. INTRUSION DETECTION FUNDAMENTALS

Growth of Intrusion Detection Mechanisms

The first major work in the area of intrusion detection was discussed by J.P Anderson in [2]. Anderson introduced the concept that certain types of threats to the security of computer systems could be identified through a review of information contained in the system's Audit Trail. Many types of operating systems, particularly the various "flavors" of UNIX, automatically create a report which details the activities occurring in the system. Anderson identified three threats, which could be identified from a concentrated review of the audit data:

1. External Penetrations - Unauthorized users of the system who try to gain access to the system.

2. Internal Penetrations - Authorized system users who utilize the system in an unauthorized manner.

3. Misfeasors - Authorized user who misuse their access privileges.

Anderson indicates that there is a particular class of external attackers, known as clandestine users who escape both system access controls and auditing mechanisms through the manipulation of system privileges or by operating at a level that is lower than what is regularly monitored by the audit trail. Anderson suggested that clandestine users could be detected by lowering the level which is monitored by the audit trail, monitoring the functions that turn off the audit systems, or through a comparison of defined "normal" usage patterns of system resources with those levels which are currently observed. Anderson's article served to initiate research into the area of Intrusion Detection. Subsequent research involved the development of automated techniques for the review of audit record data. Until recently, most Intrusion Detection mechanisms were based on an automated approach to Anderson's concepts.

Dr. Dorothy Denning proposed an Intrusion Detection model in 1987 which became a landmark for the research in this area [3]. The model which she proposed forms the fundamental core of most Intrusion Detection methodologies in use today.

1.1 Foundations of Intrusion Detection System Metrics.

Any statistical intrusion detection methodology requires the use of a set of definable metrics. These metrics characterize the utilization of a variety of system resources (i.e., CPU usage, number of files accessed, number of login attempts).These metrics usually lie in one of the following three different types. *Event Counters* identify the occurrences of a specific action over a period of time. This metric may include the number of login attempts, the number of times that a file has been accessed, or a measure of the number of incorrect passwords that are entered. The second metric, *Time Intervals* identify the time interval between two related events. Each time interval compares the delay in occurrence of the same or similar event. An example of a time interval metric is the periods of time between a user's logins. Finally, *Resource Measurement* includes the expenditure of CPU time, number of records written to a database, or the number of files transmitted over the network.

Keystroke dynamics is another method of quantifying a user's activities which offers an effective measure of user identification. The concept involves the development of an electronic signature of a user based on their individual typing characteristics. These characteristics usually include typing speed, intervals in typing, number of errors, and the user's typing rhythm. These characteristics may be verified on login and/or monitored throughout a session. Complete intrusion detection mechanisms have been developed exclusively around the use of keystroke dynamics techniques [3].

1.2 Models

The selected metrics are then used in statistical models which attempt to identify deviations from an established norm. The models which have been most frequently used include the Operational Model, Average and Standard Deviation Model, the Multivaried Model, the Markovian Model, and the Time Series Model [4]. The Operational Model makes the assumption that an anomaly can be identified through a comparison of an observation with a predefined limit. This model is frequently used in the situations where a specific number of events, (i.e., failed logins), is a direct indication of a probable attack. The Average and Standard Deviation Model is based on the traditional statistical determination. This is particularly useful in identifying what is normal for an individual user without relying on a comparison with other users.

The Multivaried Model is built upon the Average and Standard Deviation Model. The difference between these two approaches is that the Multivaried Model is based on a correlation of two or more metrics. The final model, the Time Series Model, attempts to identify anomalies by reviewing the order and time interval of activities on the network. If the probability of the occurrence of an observation is low, then the event is labeled as abnormal. This model provides the ability to evolve over time based on the activities of the users.

Profiles

These models are then used in the development of a variety of profiles, which attempt to map the non-intrusive activities of the system. The profiles serve to establish a baseline of a user's behavior, which can then be used for comparisons with the current observations. Profiles usually consist of specific characteristics, such as login information, (i.e., frequency, origin, duration), program execution information, (i.e., frequency, CPU utilization), database access information, (i.e., tables accessed, data manipulation functions), and file access information (i.e., types of files accessed, created, or destroyed).

Analysis Techniques

The final element in the basic structure of an Intrusion Detection System is determining how the collected information will be reviewed by the mechanism. Statistical Analysis involves statistical comparison of specific events based on a predetermined set of criteria.

Rule-Based Systems rely on sets of predefined rules which are provided by an administrator, automatically created by the system, or both. Each rule is mapped to a specific operation in the system. The rules serve as operational preconditions which are continuously checked in the audit record by the intrusion detection mechanism. If the required conditions of a rule are satisfied by user activity the specified operation is executed [5].

Expert Systems

The use of Expert System techniques in Intrusion Detection mechanisms was a significant milestone in the development of effective detection-based information security systems. An Expert System consists of a set of rules, which encode the knowledge of a human "expert". Unfortunately, Expert Systems require frequent updates by a System Administrator to remain current. The lack of maintenance or update will degrade the security of the entire system while the system's users believe that the system is secure, even if one of the key components becomes ineffective over time.

1.3 Approaches to Intrusion Detection

All current Intrusion Detection Systems make four assumptions about the systems that they are designed to protect:

1. Activities taken by system users, either authorized or unauthorized, can be monitored.
2. It is possible to identify those actions, which are indications of an attack on a system.
3. Information obtained from the Intrusion Detection System can be utilized to enhance the overall security of the network.
4. The system is able to make analysis of an attack in real-time.

The following are the approaches being utilized to accomplish the desirable elements of an intrusion detection system.

Anomaly Detection

Anomaly detection is the general category of Intrusion Detection, which works by identifying activities which vary from established patterns for users, or groups of users. Anomaly detection typically involves the creation of knowledge bases which contain the profiles of the monitored activities.

Misuse Detection

The second general approach to Intrusion Detection is misuse detection. This technique involves the comparison of a user's activities with the known behaviors of attackers attempting to penetrate a system. Misuse Detection also utilizes a knowledge base of information.

Combined Anomaly/Misuse Detection

Research has also been conducted into Intrusion Detection methodologies, which combine the Anomaly Detection approach and the Misuse Detection approach [6]. The combined approach permits a single Intrusion Detection System to monitor for indications of external and internal attacks.

Pattern Recognition

In this approach, a series of penetration scenarios are coded into the system. Pattern recognition possesses a distinct advantage over anomaly and misuse detection methods in that it is capable of identifying attacks, which may occur over an extended period of time, a series of user sessions, or by multiple attackers working in concert. This approach is effective in reducing the need to review a potentially large amount of audit data.

Network Monitoring

A final method of detecting system intrusions, which is currently in use, is the use of various network-monitoring techniques. [7] These methodologies passively monitor network activity for indications of attacks. The greatest advantage of network monitoring mechanisms is their independence on audit data. Because these methods do not require input from any operating system's audit trail they can use standard network protocols to monitor heterogeneous sets of operating systems and hosts.

2. ARTIFICIAL NEURAL NETWORKS

An Artificial Neural Network consists of a collection of processing elements that are highly interconnected and transform a set of inputs to a set of desired outputs. The result of the transformation is determined by the characteristics of the elements and the weights associated with the interconnections among them. By modifying the connections between the nodes the network is able to adapt to the desired outputs [8, 9].

Unlike expert systems, which can provide the user with a definitive answer if the characteristics, which are reviewed exactly, match those, which have been coded in the rule base, a neural network conducts an analysis of the information and provides a probability estimate that the data matches the characteristics, which it has been trained to recognize. While the probability of a match determined by a neural network can be 100%, the accuracy of its decisions relies totally on the experience the system gains in analyzing examples of the stated problem. The Neural Network gains the experience initially by training the system to correctly identify pre-selected examples of the problem. The response of the Neural Network is reviewed and the configuration of the system is refined until the neural network’s analysis of the training data reaches a satisfactory level. In addition to the initial training period, the neural network also gains experience over time as it conducts analyses on data related to the problem.

2.1 Neural Network Intrusion Detection Systems

A limited amount of research has been conducted on the application of neural networks to detecting computer intrusions. Artificial Neural Networks offer the potential to resolve a number of the problems encountered by the other current approaches to intrusion detection. Neural networks were specifically proposed to identify the typical characteristics of system users and identify statistically significant variations from the user's established behavior.

Artificial Neural Networks have also been proposed for use in the detection of computer viruses. In [10] and [11] Neural Networks were proposed as statistical analysis approaches in the detection of viruses and malicious software in computer networks. The Neural Network architecture which was selected for [11] was a self-organizing feature map which uses a single layer of Neurons to represent knowledge from a particular domain in the form of a geometrically organized feature map. The proposed network was designed to learn the characteristics of normal system activity and identify statistical variations from the norm that may be an indication of a virus.

2.2 Advantages of Neural Network-based Intrusion Detection Systems

The first advantage in the utilization of a neural network in the detection would be the flexibility that the network would provide. A Neural Network would be capable of analyzing the data from the network, even if the data is incomplete or distorted. Similarly, the network would possess the ability to conduct an analysis with data in a non-linear fashion. Further, because some attacks may be conducted against the network in a coordinated attack by multiple attackers, the ability to process data from a number of sources in a non-linear fashion is especially important.

The inherent speed of Neural Networks is another benefit of this approach. Because the output of a Neural Network is expressed in the form of a probability the Neural Network provides a predictive capability to the detection of instances of misuse. A Neural Network-based misuse detection system would identify the probability that a particular event, or series of events, was indicative of an attack against the system. As the Neural Network gains experience it will improve its ability to determine where these events are likely to occur in the attack process. This information could then be used to generate a series of events that should occur if this is in fact an intrusion attempt. By tracking the subsequent occurrence of these events the system would be capable of improving the analysis of the events and possibly conducting defensive measures before the attack is successful.

However, 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 have been observed before by the network. The probability of an attack against the system may be estimated and a potential threat flagged whenever the probability exceeds a specified threshold.

2.3 Disadvantages of Neural Network-based Intrusion Detection Systems

There are two primary reasons why Neural Networks have not been applied to the problem of misuse detection in the past. The first reason relates to the training requirements of the Neural Network. Because the ability of the Artificial Neural Network to identify indications of an intrusion is completely dependent on the accurate training of the system, the training data and the training methods that are used are critical. The training routine requires a very large amount of data to ensure that the results are statistically accurate. The training of a Neural Network for misuse detection purposes may require thousands of individual attacks sequences, and this quantity of sensitive information is difficult to obtain.

However, the most significant disadvantage of applying Neural Networks to intrusion detection is the "black box" nature of the Neural Network. The "Black Box Problem" has overwhelmed Neural Networks in a number of applications [12]. This is an on-going area of Neural Network research.

3. CURRENT ANN INTRUSION DETECTION TECHNOLOGIES

A Back-propagation Neural Network called NNID (Neural Network Intrusion Detector) was trained in the identification task and tested experimentally on a system of 10 users. The system was 96 % accurate in detecting unusual activity with 7 % false alarm rate. This suggests that learning user profile is an effective way for detecting intrusions. The NNID system works in three steps i.e. collecting data, training data and performance. If NN suggestion is different from the actual user then indicate anomaly. If NN activation is greater then 0.5 then identification was correct otherwise less then 0.5 then anomalies are detected. It provides high degree of accuracy out of 24 intruders the network identified 22. It operates offline on daily logs not in real-time [13].

Multiple Self Organizing Maps (MSOMS) were also used with unsupervised learning to identify anomalies. It measures a 10 % difference between the measures of fit for the same vector on different runs. In case of data and particular distance measures all of the normal traffic scored between 0 and 3. Roughly 7 packets transmitted to accomplish the exploit, 2 registered just above 80, indicating they did not fit well on the map at all and 2 other registered above 630 indicating external anomaly. It can also be applied for analysis of data colleted from network monitoring. The ratio of normal to intrusive packets was computed. The overflow is also detected by this NN. By learning to characterize normal behavior, it completely prepares itself to detect any abnormal network activity. [14]

CMAC (Cerebellar Model Articulation Controller) uses adaptive NN to Intrusion Detection that is capable of learning new attacks rapidly through the use of a modified reinforced learning method that uses feedback from the protected system. It provides online learning of attack patterns. It has rapid learning of data. It is extremely accurate in identify priori attack patterns. This modified reinforce learning approach resulted in an average error of 3.28-05 %, compared with an average error of 15 % in existing intrusion detection. The average error rate is 2.199 % that identify new attacks based on its experience. [15]

This prototype used a MLP (Multi Level Perceptron) architecture that consists of four connected layers with 9 inputs and 2 output nodes. The training of the Neural Network was conducted using a Back-propagation algorithm for 10,000 iterations of the selected training data. Like the feed-forward architecture of the neural network, the use of a back-propagation algorithm for training was based on the proven record of this approach in the development of neural networks for a variety of applications [9]. Of the 9,462 records, which were preprocessed for use in the prototype, 1000 were randomly selected for testing and the remaining were used to train the system. The training/testing iterations of the neural network required 26.13 hours to complete. At the conclusion of the training the following results were obtained:

- ➢ Training data root mean square error = 0.058298
- ➢ Test data root mean square error = 0.069929
- ➢ Training data correlation = 0.982333
- ➢ Test data correlation = 0.975569

The figures matched very closely with the desired root mean square (RMS) error of 0.0 and the desired correlation value of 1.0 [16]

4. RESULTS

The NNID used learning algorithm of Back-propagation and gives 96 % accuracy and about 6 % error. The MSOMS used unsupervised learning and is best for data analysis (collected from network monitoring) and overflow detection. It prepares itself to detect any abnormal activity by learning over experience. The CMAC is an adaptive Neural Network. It has online and rapid learning rate to detect attacks. The average error rate is 2.199 % that identify new attacks based on its experience. The MLP architecture also used Back-propagation algorithm. But the time required for training is about 26 hours that is an overhead.

5. FUTURE WORK

The efficient Intrusion Detection Systems can be developed that have very low error rate, adaptability, high learning rate and quick Intrusion Detection by using other Neural Networks based on Adaptive Resonance Theory and Multi-channel Adaptive Resonance Theory.

6. CONCLUSION

We have presented an overview of Intrusion Detection System and Artificial Neural Network technologies that are being used these days. The different Artificial Neural Network technologies for Intrusion Detection are also compared. Finally, a discussion of the future ANN technologies, which promise to enhance the ability of computer systems to detect intrusions is provided.

7. REFERENCES

[1] Cannady J. Artificial Neural Networks for misuse detection. National Information Systems Security Conference; 1998. p. 368–81.

[2] Anderson, J.P. (April, 1980). Computer Security Threat Monitoring and Surveillance. Technical Report, J.P. Anderson Company, Fort Washington, Pennsylvania.

[3] Denning, Dorothy. (February, 1987). An Intrusion-Detection Model. IEEE Transactions on Software Engineering, Vol. SE-13, No. 2.

[4] Castano, S., Fugini, M., Martella, G. & Samarati, P. (1995). Database Security. Addison-Wesley Publishing Company, New York.

[5] Page, J., Heaney, J., Adkins, M. & Dolsen, G. (1989). Evaluation of Security Model Rule Bases. Technical Report. Planning Research Corporation.

[6] Lunt, T.F. (1989). Real-Time Intrusion Detection. Proceedings from IEEE COMPCON.

[7] Mukherjee, B., Heberlein, L.T. & Levitt, K.N. (May/June, 1994). Network Intrusion Detection. IEEE Network. pp. 26-41.

[8] Fox, Kevin L., Henning, Rhonda R., and Reed, Jonathan H. (1990). A Neural Network Approach Towards Intrusion Detection. In Proceedings of the 13th National Computer Security Conference.

[9] Hammerstrom, Dan. (June, 1993). Neural Networks At Work. IEEE Spectrum. pp. 26-53.

[10] Denault, M., Gritzalis, D., Karagiannis, D., and Spirakis, P. (1994). Intrusion Detection: Approach and Performance Issues of the SECURENET System. In Computers and Security Vol.13, No. 6, pp. 495-507

[11] Fox, Kevin L., Henning, Rhonda R., and Reed, Jonathan H. (1990). A Neural Network Approach Towards Intrusion Detection. In Proceedings of the 13th National Computer Security Conference.

[12] Fu, L. (1992). A Neural Network Model for

Learning Rule-Based Systems. In Proceedings of the International Joint Conference on Neural Networks. pp. (I) 343-348.

[13] Ryan, J., Lin, M., and Miikkulainen, R. (1997). Intrusion Detection with Neural Networks. AI Approaches to Fraud Detection and Risk Management: Papers from the 1997 AAAI Workshop (Providence, Rhode Island), pp. 72-79. Menlo Park, CA: AAAI.

[14] Rhodes, B., Mahaffey, J., & Cannady, J. (2000, October). Multiple Self-Organizing Maps for Intrusion Detection. Proceedings of the 23rd National Information Systems Security Conference.

[15] Cannady, J. (2000, October). Next Generation Intrusion Detection: Autonomous Reinforcement Learning of Network Attacks. Proceedings of the 23rd National Information Sy stems Security Conference.

[16] Cannady, J. (1998). Neural Networks for Misuse Detection: Initial Results. Proceedings of the Recent Advances in Intrusion Detection '98 Conference, 31-47.