International Research Journal of Computer Science (IRJCS)
Issue 09, Volume 4 (September 2017)
ISSN: 2393-9842
www.irjcs.com

NEURAL NETWORKS IN CYBER SECURITY

J.Rubina Parveen
Assistant Professor, PG Department of Computer Science
Mohamed Sathak Arts and Science College,
Shollinganallur, Chennai

Manuscript History
Number: **IRJCS/RS/Vol.04/Issue09/SISPCS10095**
Received: 08, September 2017
Final Correction: 13, September 2017
Final Accepted: 20, September 2017
Published: September 2017
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract-- Today's IT leaders face many challenges and rapid changes with respect to Internet Security. They have to protect enterprise, customer, citizen, and member and employee data, while upsetting attacks from cyber criminals. One of the mature technology architecture, Intrusion Detection system (IDS) primarily designed to protect the network from external cyber threats. The neural network concepts are adapted to identify and classify network activity based on limited, incomplete and nonlinear data sources related to the network security.

Keywords: Internet security, Intrusion detection system, Cyber threats.

I. INTRODUCTION

Protecting digital assets and intellectual property is becoming challenging for organizations. Recent studies describe external hacking as the primary cause of data loss in the corporate industry. Organizations are expected to take adequate measures to protect data from loss or leakage. Quite often, unchecked IT cyber security risk factors that remain unmitigated for too long-something that happens in almost all business are the cause for unexpected cyber attacks. Intrusion Detection Systems (IDS) are now mainly employed to secure company networks. An IDS is highly recommended to detect all attempted intrusions, and to protect the organization from the attack.

II. ARTIFICIAL NEURAL NETWORK IN NETWORK SECURITY

The artificial neural network is playing an increasingly important role in network management. Most of the research in the area of intrusion detection system relies extensively on AI techniques to design, implement and enhance security monitoring system [1]. Studies have shown that the current anomaly detection IDSs are failing to reach adequate detection rate while having few false alarm [2, 3]. In this paper, the commercial and research tools, and a new way to improve false alarm detection using neural network approach in IDS and the merits and demerits are presented. IDS will achieve a certain, well defined level of security and an adaptive AI system will make it more flexible for upcoming new challenges.

Intrusion Detection System

An Intrusion Detection System is a device which is used to monitors activity to identify malicious or suspicious events in a computer network [4].

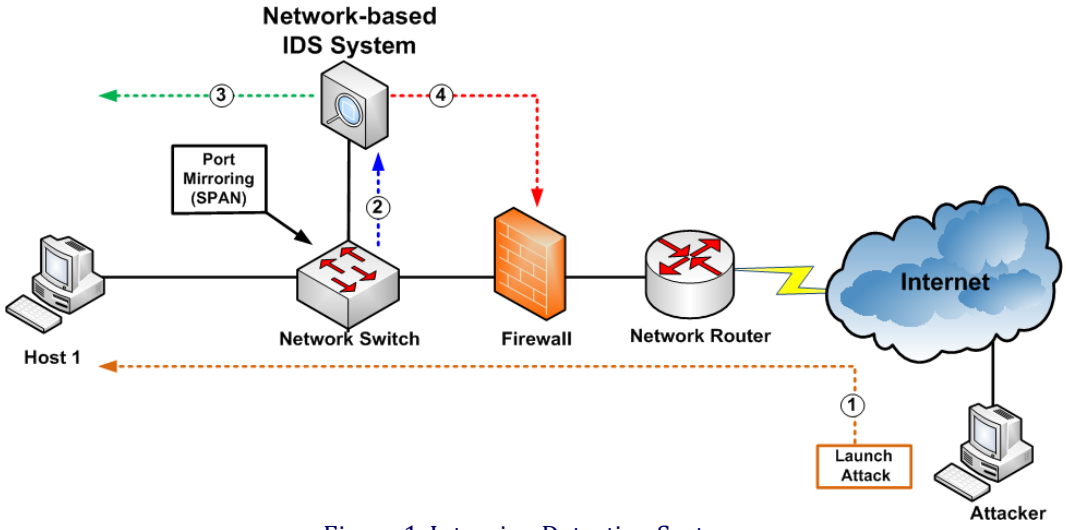

Figure 1. Intrusion Detection System

Classification of Intrusion Detection Systems

A guidance document on Intrusion Detection Systems is available from National Institute of Standards and Technology (NIST) organization [5].

Three different categories of Intrusion Detection Systems:

- **Host-based IDS,** evaluate information found on a single or multiple host systems, including contents of operating systems, system and application files [8].
- **Network-based IDS**, evaluate information captured from network communications, analyzing the stream of packets traveling across the network. Packets are captured through a set of sensors [8].
- **vulnerability-assessment IDS**, the vulnerabilities on internal networks and firewalls are detected

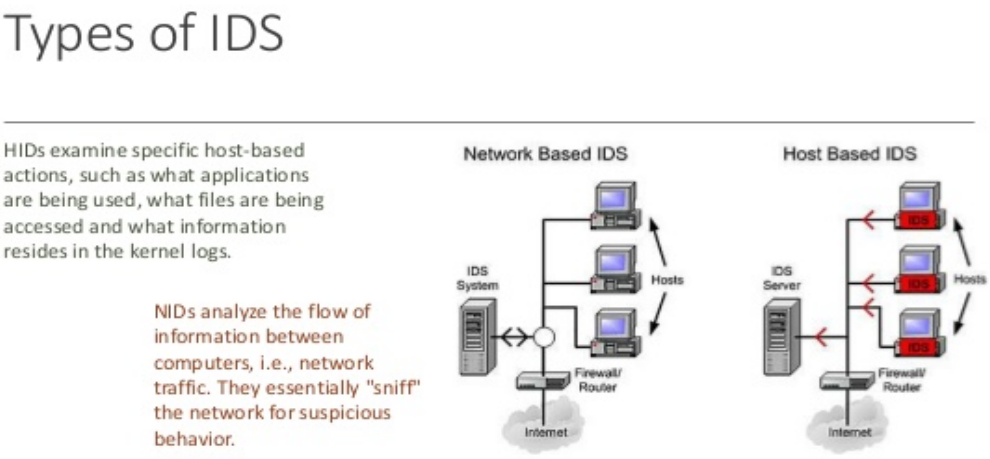

Figure 2. Types of IDS

Primary models in IDS to analyzing events to detect attacks:

- **misuse detection model** : IDS detect intrusions by looking for activity that corresponds to known signatures of intrusions or vulnerabilities
- a**nomaly detection model** : IDS detect intrusions that vary from established pattern for users

Examples of commercial IDS tools based on the models

- **Host based tools:** Host based IDS system detect intrusion for an individual system using system logs and operating system audit trials.

- Examples of host based commercial tools are: Cybercop from Network Associates (NAI) (http://www.pgp.com), KaneSecurity Monitor (KSM) from RSA Security (http://www.rsasecurity.com)[8]
- **Network-based IDS tools:** Network-based IDS systems detect attacks by capturing and analyzing network packets, by using sensors placed at various points in a network. Examples of commercially available Network-based tools are: RealSecure from Internet Security Scanner (ISS)(http://www.iss.net), Cisco Secure IDS or NetRanger from Cisco Systems(ex: Wheel Group Corporation).A popular and freely-available Network-based IDS is Snort, a lightweight IDS (http://www.snort.org)[8].
- **Vulnerability-assessment tools:** Vulnerability-assessment tools acts like a security scanners used to detect known vulnerabilities on specific Operating System's configuration. Examples of popular vulnerability-assessment tools are: CyberCop Scanner from PGP Security (a Network Associates Division) and SecureScan NX from Networks Vigilance (formally known as NV e-secure)[8].

Approaches of primary models in IDS

The Center for Education and Research in Information Assurance and Security (CERIAS) has produced a review of IDS research prototypes [8], and a few are now commercial products.

Approaches for misuse detection

- **expert systems**, containing a set of rules that describe attacks against a network
- **signature verification**, where attack scenarios are translated into sequences of audit events
- **petri nets**, where known attacks are represented with graphical petri nets
- **sate-transition diagrams**, representing attacks with a set of goals and transitions using use cases

Approaches for anomaly detection

Anomaly Detection in Network-based or Host-based IDS includes:

- **threshold detection** the abnormal activity on the server or network is detected, for example abnormal consumption of the CPU for specific server, or abnormal saturation of the entire network
- **statistical measures**, data learned from historical values
- **rule-based measures,** rules formed with expert systems
- **non-linear algorithms ,**algorithms like Neural Networks or Genetic algorithms

III. NEURAL NETWORK APPROACH FOR INTRUSION DETECTION

An artificial Neural Network consists of a collection of iterations to transform a set of inputs to a set of desired outputs, through a set of simple processing units, or nodes and connections between them. Subsets of the units in the iteration are input nodes, output nodes, and nodes between input and output form hidden layers; the connection between two units assigned some weight, used to determine how much one unit will affect the other.

Two types of architecture of Neural Networks can be distinguished:

- **Supervised training algorithms**, the network learns the desired output for a given input or pattern in the learning phase. The well known architecture is the Multi-Level Perceptron (MLP) which is employed for Pattern Recognition problems [8].
- **Unsupervised training algorithms**, the network learns without specifying desired output in the learning phase. The Self-Organizing Maps (SOM) algorithm is used to find a topological mapping from the input space to clusters. SOM are employed for classification problems [8].

A good introduction to Neural Networks is available in [9]. The most important property of a Neural Network is to automatically learn the coefficients in the Neural Network according to data inputs and data outputs.

Neural Network Intrusion Detection Systems

The amount of research has been conducted on the application of neural networks to Detect the computer intrusions is very limited. Artificial neural networks offer the potential to resolve a number of the problems encountered by the other current approaches to intrusion detection. Artificial neural networks have been proposed as alternatives to the statistical analysis component of anomaly detection systems, [10, 11, 12, and 13].

Advantages of Neural network in cyber security

Several case studies emphasize that the use of Artificial Neural Networks (ANN) can establish g pattern recognition and identify attack in situations where rules are not known [14]. A neural network approach can be adapted to certain constraints; to recognize patterns and compare recent actions happened with the usual behavior which allows resolving many issues even without human intervention. The technology promises not only to detect misuse and improve the recognition of malicious events with more consistency. A neural network is able to detect any possibility of misuse happened, which allows the system administrator to protect their entire organization through enhanced flexibility against intrusions. The experts believe that NN will function with more reliability and accuracy in identifying intrusions of insecure networks.

Disadvantages of Neural Network-based Misuse Detection System

The ability of the artificial neural network to identify indication of intrusion is dependent on the training requirement of data and methods which are very critical to use. The training requires thousands of individual intrusion in sequence which is very sensitive to obtain. The most significant disadvantage in applying neural network to intrusion detection system is the 'Black box' nature of neural network. The "Black Box Problem" has plagued neural networks in a number of applications [15]. This is an on-going area of neural network research.

IV. CONCLUSION

The security solutions for business feature a spectrum of Next Generation technologies, including intelligent behavioral analysis and machine learning algorithms. This combination of advanced technologies can be accomplished by using Artificial Intelligence and Neural network which play an important role in achieving one of the highest detection rates in the industry, as continuously demonstrated through independent tests. The research is ongoing in this field for further enhancement with more accuracy to detect complex and targeted attacks.

REFERENCES

1. Gagnon, F.|Esfandiari, B.: Using Artificial Intelligence for Intrusion Detection. In Proceeding of the 2007 Conference on Emerging Artificial Intelligence Applications in Computer Engineering, Amsterdam, The Netherlands 2007, pp. 295{306.
2. Lazarevic, A.|Ertoz, L.|Kumar, V.|Ozgur, A.|Srivastava, J.: A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection. In Proceedings of the Third SIAM International Conference on Data Mining 2003, pp. 25{36.
3. Axelsson, S.: The Base-Rate Fallacy and the Difficulty of Intrusion Detection. ACM Trans. Inf. Syst. Secure., Vol. 3, 2000, No. 3, pp. 186{205.
4. Security in computing-(3rd Edition) Charles P.Pfleeger ,Shari Lawrence Pfleeger.PHI
5. Jackson A - Intrusion Detection System (IDS) product survey - Los Alamos National Laboratory - New Mexico (http://lib-www.lanl.gov/la-pubs/00416750.pdf)
6. 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.
7. Anderson, D., Frivold, T. & Valdes, A (May, 1995). Next-generation Intrusion Detection Expert System (NIDES): A Summary. SRI International Technical Report SRI-CSL-95-07.
8. Sans Institution Infosec Reading Room 2001-available on-line at https://www.sans.org
9. Debar, H. & Dorizzi, B. (1992). An Application of a Recurrent Network to an Intrusion Detection System. In Proceedings of the International Joint Conference on Neural Networks.pp. (II)478-483.
10. Debar, H., Becke, M., & Siboni, D. (1992). A Neural Network Component for an Intrusion Detection System. In Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy.
11. Anderson J - An introduction to Neural Networks - MIT Press 1995
12. Frank, Jeremy. (1994). Artificial Intelligence and Intrusion Detection: Current and Future Directions. In Proceedings of the 17th National Computer Security Conference.
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. http://Resources.infosec institute.com
15. Addressing Cyber security vulnerabilities, Omar Y Sharkasi, ISACA Journal volume 5,2015
16. Artificial neural network for Misuse Detection, James Cannady-Research Paper
17. Bace R & Mell P - NIST Special publication on Intrusion Detection Systems (http://csrc.nist.gov/publications/drafts/idsdraf Bace R & Mell P - NIST Special publication on Intrusion Detection Systems (http://csrc.nist.gov/publications/drafts/idsdraft.pdf)

