DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4305

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ON APPLICABILITY OF NEURAL NETWORK IN INTRUSION DETECTION AND PREVENTION

Ahmed Abdul Zahra A.Alhello
Department of Computer Science
Jamia Hamdard
New-Delhi, India

Dr.Harleen Kaur
Department of Computer Science
Jamia Hamdard
New-Delhi, India

Abstract—— Intrusion Detection and Prevention Systems (IDPS) are used to capture anomalies and suspicious activities in the computer networks. IDPS are one of the important security mechanism used for the network security within an organization.There are various tools and techniques that exist in the literature and the market but still there is a need for proposing the robust model for Intrusion Detection. Some of the tools are limited to detect Intrusion in some protocols. However, No such tools exists that can check Intrusion in all the networking protocols. This work gives the systematic literature review of the techniques that are used for Intrusion and Detection using Artificial Neural Networks. Furthermore, Artificial Neural Network based Intrusion detection model is proposed and implemented**.**

keywords- IDS, IPS, IDPS, Intrusion Detection Systems, Intrusion Detection and Prevention Systems, NIDPS, HIDPS, ANNs,Artificial Neural Networks.

I. INTRODUCTION

The network security is a serious concern for the companies these days. Many techniques are used by the companies to counterfeit inside and outside attacks. The primary objectives are to achieve Confidentiality, Integrity and Availability. It is evident from the annual security reports of fortune 500 companies that the increase in Network based attacks and Dos (Denial of Services) are rapid. The most common is via web applications. "Wanna cry" ransonware is one of the recent examples. For securing the networks, many techniques are used by the companies like Firewall, Honeypots, and Honeynets etc. However Intrusion Detection if used correctly is the most efficient techniques for mitigation of network based attacks.

Intrusion Detection and Prevention Systems (IDPS) are the security techniques that company used to protect its networks before the attack happens. It detects the anomaly and unusual behavior of the network or host. IDPS is actually a database that stores the known attack patterns and signature, while analyzing the network traffic, if the patterns and signature matches it give alert and notifications. Next step is now incident response.

Artificial Neural Networks (ANNs) are the crucial area of Artficial Intelligence that depicts the human brain and are capable of learning, and therefore can predict the outputs and results based on the learning. ANNs has various applications in data analytics, prediction modeling, and pattern recognition and so on. This work gives the systematic literature review of techniques that are proposed in the literature for Intrusion Detection and Prevention using Artificial Neural Networks. The objective is to find further research scope and gaps in research if exists. Finally, ANNs based model for Intrusion detection is implemented using MATLAB.

The work has been organized as follows: Section 2 explains Intrusion Detection and Prevention Systems (IDPS), their types and implementation. Section 3 Artificial Neural Networks. Section 4 gives a systematic literature review. Section 5 presents proposed model for Intrusion Detection using ANNs and the last section concludes.

II. INTRUSION DETECTION AND PREVENTION SYSTEMS

Intrusion Detection is the technique of rectifying the anomalies in the behavior of network or host. The concept of Intrusion can be understood with an example of access control for manufacturing departments and Finance department in an organization. If finance is accessing Payroll database, there is no intrusion as they have access for it. Now, consider someone in your organization from manufacturing department is accessing payroll database, this is an Intrusion as manufacturing department doesn't have access for it and there is no relevance. IDPS are the tools that actually implement Intrusion Detection. It must be noted that IDS is capable of only detecting and notifying Intrusions, the tools and systems which are capable of preventing Intrusion is known as Intrusion Prevention Systems (IPS). Generally, The Intrusion Detection and Prevention Systems (IDPS) are used practically which is capable of detection as well as prevention. IDPS are generally deployed between the intranet and internet of the network. It is placed in the DMZ so that it can efficiently analyses internal traffic and external traffic. However, it can be placed according to the needs and security of the organization [1]. However, there is a difference between misuse detection and intrusion detection. Misuse detection is generally targeted towards individuals while Intrusion detection targets individual with no authorized access.

IDPS Types

The Intrusion Detection and Prevention Systems (IDPS) can be classified into two types depending upon their aims for security [2]:-

- ***Network-Based Intrusion Detection and Prevention Systems (NIDPS)***

This type of IDPS checks intrusion and anomaly in the network and the traffic. NIDPS inspect the packet in the network and further analyze it for the known attack patterns. This is done by the already stored data of the attacks and

vulnerabilities. NIDPS is deployed in the computer having NIC in the promiscuous mode so that it can accept all the packets in the network. Depending upon the requirement HIDS can be deployed with Hubs, Switch, Router, VLAN or ports depending upon system on which it is operating on.
One of the biggest advantages of NIDPS is that it can carry many sensors for monitoring DMZ (Demilitarized Zone) by the system which is working towards HIDPS. However, HIDPS cannot detect certain types of traffic for intrusion like encrypted traffic. Also, it cannot detect attacks and intrusion made by the specific host in the networks. There are many NIDPS tools available in the market some of them are SNORT, Cisco Intrusion Detection System and Symantec Net Prowler.

.

- ***Host-Based Intrusion Detection and Prevention Systems (HIDPS)***

This type of IDPS can only inspect traffic on one specific system. The scope of HIDPS is limited to the one host on which it is working. HIDPS not usually put NIC on promiscuous mode as it doesn't have to deal with network traffic like NIDPS. The intention of deploying HIDPS is to check unauthorized access and activities. It can be thought of as checking and securing one specific machine for intrusion and detection. For example, if thousands of mail is sent by the word processor, the HIDPS will give alert and notification. Some of tools widely used for HIDPS are Tripwire, Real Secure and Swatch.

IDPS Techniques

The Intrusion detection techniques can be divided into two types namely:-

- *Signature Based or Pattern Matching IDS*

In this type of intrusion detection techniques the data of known attacks uploaded into the database as a signature. The alerts can be generated on the basis of fragmented IP packets, malformed ICMP packets and Streams of SYN packets. These alerts are used to change the firewall configuration so that attacks can be mitigated. However, signature based IDPS is tightly coupled with some disadvantages for example it can only deal with intrusions similar to loaded signatures, rest of the traffic would be passed further.
The disadvantages of this type of IDS are that it can detect only signatures that are stored. Obfuscated attacks cannot be recognized by Signature based IDS [2]. The Figure.1 Below depicts the working of Signature Based IDS:-

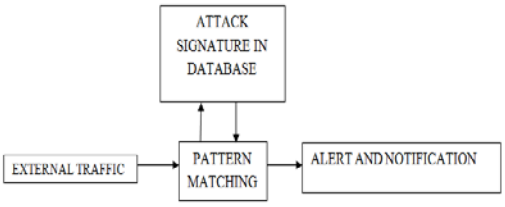

Figure.1 Signature based IDPS

- ***Anomaly based IDS***

This approach identifies the abnormal activity by comparing it with normal activities. This type of IDS analyses the behavior of the systems. It captures and stores the trends and behavior of the protocols with respect to situations and attacks. Accordingly it will generate alert and notifications depending upon the behavior of that protocol. For example, if the group of daytime employees starts logging in at night time, the IDPS will generate an alert. It is widely used to inspect attacks on application layer protocols like DNS, HTTP, SMTP, DHCP etc. The Figure.2 Below shows the working of Anomaly-Based IDS [2].

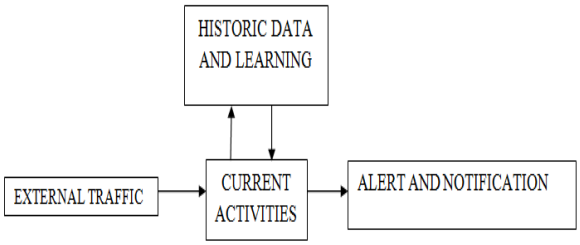

Figure.2 Anomaly based IDPS

III. ARTIFICIAL NEURAL NETWORK

Artificial Neural Network (ANNs) is the Artificial Intelligence techniques that work similar to human brain. Human brains consists of billion nerve cell namely neurons. Neurons on other hand are connected to other cells called Axons. Dendrites receive input and pass it into the neural network. Each neuron is capable of transferring information from one to another.
ANNs are connected to each other similar to biological neurons. They receive input and pass it to further to process and give output. Neurons are connected with some weights on the link. ANNs are capable of learning with adjustment of weights in the links. They receive input and based on input it can give output or can predict the same. This is done by the mechanisms of learning by the ANNs.
There are two types of topologies that are widely used in ANNs namely FeedForward and FeedBack.
FeedForward- In this topologies, the direction of information is unidirectional, there is no loop. This kind of network has applications in Classification, Pattern Recognition etc.

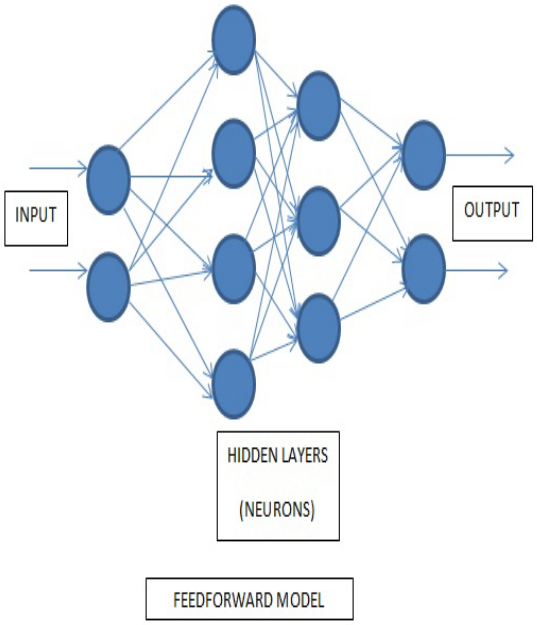

Figure.3 FeedForward Model ANNs

FeedBack- This topology has feedback options. The direction of information is bidirectional. It has application in prediction models.

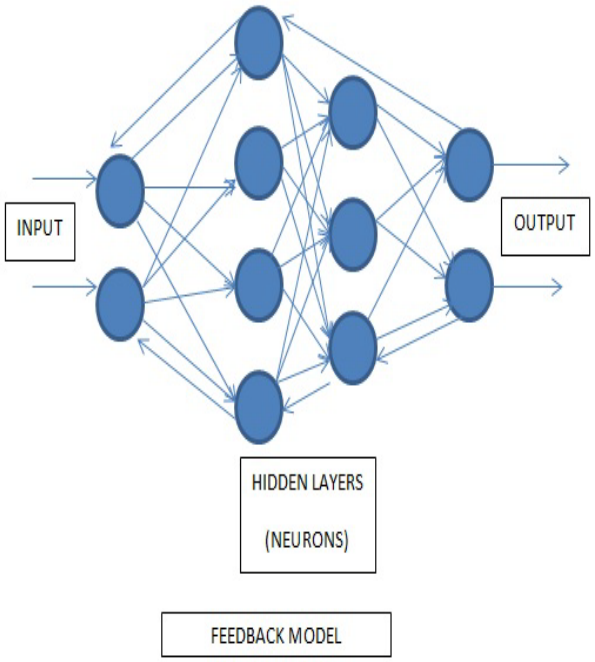

Figure.4 FeedBack Model ANNs

ANNs can be trained to do specific tasks depending upon the situation and circumstances. This is done by the process of learning. Learning is the process similar to our brain, for example if we are blocking TCP protocol in firewall and still not able to mitigate attacks, next time we will not block TCP protocol, this is learning from the situation. Similarly ANNs learns from the situations and circumstances and can predict the future. Learning in ANNs can be classified as:-

- *Supervised Learning*: - Training by giving inputs and outputs.
- *Unsupervised Learning*: - Training when there is no training data is giving. ANNs finds itself the best answer.
- *Reinforcement Learning*: - it is inspired by the behaviorist psychology. Training by giving ANNs some specific tasks and giving ANNs time to itself analyze the change and behavior.

However, depending upon the requirements and problems, one can use any type of learning and models of ANNs to solve real world problems. The role of ANNs in the field of computer science is emerging these days. It is seen in past decade that application of ANNs in computer science and biotechnology is increasing. However, still there is a need of exploring this algorithm of Artificial Intelligence so that it can apply to problems of scientific research.

IV. LITERATURE REVIEW

.The literature review has been carried out in an order to find out existing techniques related to Intrusion Detection using Artificial Neural Network. The top journals of the computer science domain has been explored and verified to get legit information about the topic excluding papers exists in a grey literature. However, the paper with good citations is considered. The literature review is performed in following five journals:-

1. IEEE Xplore
2. ACM Digital Library
3. Science Direct
4. Wiley Online Library
5. Springer

The search term while doing literature review was “Intrusion Detection using Artificial Neural Network”. The relevant papers then filtered out to get exact papers related to the Intrusion Detection. It is seen in the literature review that IEEE Xplore has shown maximum papers related to Intrusion Detection. Table.1 summarizes the literature review:-

TABLE.1 LITERATURE REVIEW

S.No.	AUTHOR NAME	TECHNIQUE USED
[3]	Tamilarasan et al	Artificial Neural Network.
[4]	Hodo et al	Artificial Neural Network
[5]	Poojitha et al	Artificial Neural Network.
[6]	Abas et al	Artificial Immune System
[7]	Choudhary and Swarup	Neural Network
[8]	El Farissi	Neural Networks.
[9]	Esmaily et al	ANNs and Decision Tree
[10]	Kim et al	Deep Neural Network
[11]	Jing-xin	Neural Network Back
[12]	G. Kumar and K. Kumar	AI based supervised classifiers
[13]	Kumar and Yadav	Neural Network
[14]	Liang Hu	Neural Network regression
[15]	Zhang et al	Probabilistic Neural Network
[16]	Sen et al	Multi-Layer Backpropagation Neural Network Algorithm
[17]	J. Spencer	Artificial Neural Network
[18]	Subba et al	Neural Network

There are many techniques and tools are available for intrusion detection. However, the following are the famous techniques used for the intrusion detection using Artificial Neural Networks:-

1. Probabilistic Artificial Neural Network.
2. Artificial Neural Network with Fuzzy Logic.
3. Ant Colony Optimization
4. Forward Feed Network of Neural Network.
5. Genetic Algorithm with neural network.

However, the robust model with Feedback Architecture of Artificial Neural Network still not exist which can efficiently detect intrusion in the network. It is seen that further research in this field can be done. Moreover, algorithms like Genetic Algorithm, Ant Colony Optimization, and Glow worm Optimization can be integrated with ANNs to make it more robust.

V. PROPOSED MODEL

The proposed model is based on the Feedback architecture of Artificial Neural Network which is famous for its predictions and regression applications. In this model we feed 100 datasets (Patterns of Attacks, Signatures, Behavior etc) to the Feedback architecture of ANNs so that model can learn about the inputs and their outputs. During monitoring, if it get similar patterns of input. Automatically it predicts the output as a notification of Intrusion. This model can be implemented for both Signature based IDS and Anomaly based IDS. However, ANNs learning and training datasets should be efficient and correct otherwise the IDPS can give false positive alerts and notification. The work has been implemented in the Neural Network Toolbox in MATLAB environment. The model is easy to build and it follows a simple step by step approach. First and foremost, the system is deployed between the extranet and intranet (DMZ), to capture the traffic and protocols going in and out. This system is placed in DMZ to analyses the intrusion in a better way. While analyzing traffic, every incoming and outgoing traffic and passed through this ANNs based model installed on the system. It analyses behavior, packets, protocols, signatures, patterns etc and predict the intrusion and gives alerts and notification. Also, if integrated with firewall it can block the suspicious activities as well. The following are the steps for the implementation of ANNs based IDPS.

Steps:-

- Create datasets of about 100 inputs and outputs and store them in ANNs. Start the learning process and train the ANNs.
- Store this training data in Intrusion Detection Tool.
- While real time traffic analyses if Intrusion Detection Tool found similar and matching patterns and signature. It will generate alert.
- The case is then monitored and analyzed for Incident response.

The Figure.20 Illustrates the working of the model:-

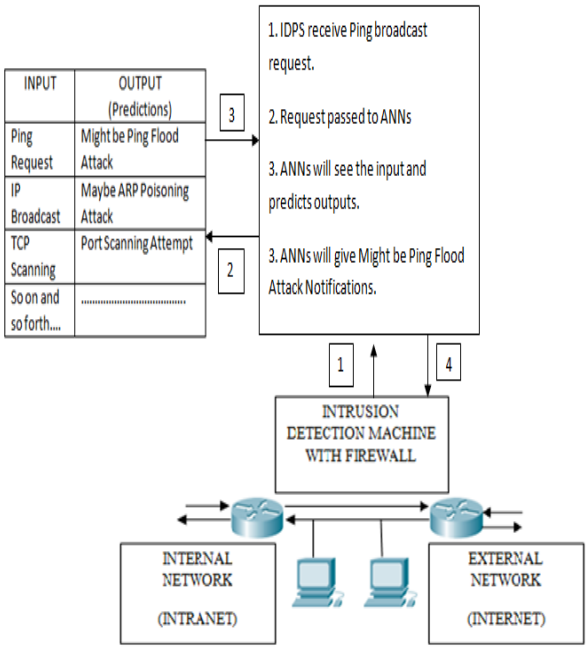

Figure.5 Artifical Neural Network Based IDPS

VI. CONCLUSION AND FUTURE SCOPE

The ANNs based model can easily be implemented in the MATLAB environment. The ANNs based model is capable of detecting intrusion in the system and giving alerts. In this work we trained data of 100 datasets and trained it for ANNs learning, moreover the results are encouraging. This model could be used as a robust IDPS.

Also, the systematic literature review has been carried out in an order to find techniques that still exists for the intrusion detection. There are various techniques that have limitations and there is no strong ANNs based model for Intrusion Detection that exists. Therefore, need for proposing new technique arises. It may be seen that various work has been done using Artificial Neural Network. Therefore, robust model using ANNs can be built. Also, Genetic Algorithm can be applied for the optimization using ANNs.

REFERENCES

[1] Corey Schou and Steven Hernandez, “Information Assurance Handbook”, 2014.

[2] Whitman and Mattord, “Principles of Information Security”, 2003.

[3] A. Tamilarasan, S. Mukkamala, A. Sung and K. Yendrapalli, "Feature Ranking and Selection for Intrusion Detection Using Artificial Neural Networks and Statistical Methods", The 2006 IEEE International Joint Conference on Neural Network Proceedings, 2006.

[4] E. Hodo, X. Bellekens, A. Hamilton, P. Dubouilh, E. Iorkyase, C. Tachtatzis and R. Atkinson, "Threat analysis of IoT networks using artificial neural network intrusion detection system", 2016 International Symposium on Networks, Computers and Communications (ISNCC), 2016.

[5] G. Poojitha, K. Kumar and P. Reddy, "Intrusion Detection using Artificial Neural Network", 2010 Second International conference on Computing, Communication and Networking Technologies, 2010.

[6] E. Abas, H. Abdelkader and A. Keshk, "Artificial immune system based intrusion detection", 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS), 2015.

[7] A. Choudhary and A. Swarup, "Neural network approach for intrusion detection", Proceedings of the 2nd International Conference on Interaction Sciences Information Technology, Culture and Human - ICIS '09, 2009.

[8] I. El Farissi, M. Saber, S. Chadli, M. Emharraf and M. Belkasmi, "The analysis performance of an Intrusion Detection Systems based on Neural Network", 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), 2016.

[9] J. Esmaily, R. Moradinezhad and J. Ghasemi, "Intrusion detection system based on Multi-Layer Perceptron Neural Networks and Decision Tree", 2015 7th Conference on Information and Knowledge Technology (IKT), 2015.

[10] Jin Kim, Nara Shin, S. Jo and Sang Hyun Kim, "Method of intrusion detection using deep neural network", 2017 IEEE International Conference on Big Data and Smart Computing (BigComp), 2017.

[11] W. Jing-xin, W. Zhi-ying and D. Kui, "A network intrusion detection system based on the artificial neural networks", Proceedings of the 3rd international conference on Information security - InfoSecu '04, 2004.

[12] G. Kumar and K. Kumar, "AI based supervised classifiers", Proceedings of the International Conference on Advances in Computing and Artificial Intelligence - ACAI '11, 2011.

[13] S. Kumar and A. Yadav, "Increasing performance Of intrusion detection system using neural network", 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, 2014.

[14] Liang Hu, Zhen Zhang, Huanyu Tang and NannanXie, "An improved intrusion detection framework based on Artificial Neural Networks", 2015 11th International Conference on Natural Computation (ICNC), 2015.

[15] Ming Zhang, JunpengGuo, BoyiXu and Jie Gong, "Detecting network intrusion using Probabilistic Neural Network", 2015 11th International Conference on Natural Computation (ICNC), 2015.

[16] R. Sen, M. Chattopadhyay and N. Sen, "An Efficient Approach to Develop an Intrusion Detection System Based on Multi-Layer Backpropagation Neural Network Algorithm", Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research - SIGMIS-CPR '15, 2015.

[17] J. Spencer, "Use of an Artificial Neural Network to Detect Anomalies in Wireless Device Location for the Purpose of Intrusion Detection (Non-Refereed)", Proceedings. IEEE SoutheastCon, 2005..

[18] B. Subba, S. Biswas and S. Karmakar, "A Neural Network based system for Intrusion Detection and attack classification", 2016 Twenty Second National Conference on Communication (NCC), 2016.