Neural Network-Based Anomaly Intrusion Detection System

Yousef Abuadlla1,*

1 Faculty of Electrical Engineering, University of Al Jafara, Zahra, Libya.

*** abouadlla@aju.edu.ly**

الملخص

مع استمرار زيادة عدد مستخدمي الإنترنت وشبكات الكمبيوتر ، هناك طلب متزايد على أنظمة مراقبة أمنية فعالة، مثل أنظمة الكشف عن الشبكات. يركز العديد من الباحثين على هذا المجال ويستكشفون طرقا مختلفة لتطوير أنظمة كشف قوية يمكنها حماية شبكات الكمبيوتر من الهجمات باستخدام التقنيات التقليدية. هناك طرق حديثة لأنظمة الكشف عن التطفل باستخدام مقاييس حركة المرور المجمعة وهو نظام الكشف عن التسلل القائم على التدفق. يقدم هذا البحث نظاما للكشف عن التطفل القائم على الشبكة العصبية لتحديد هجمات حركة مرور الشبكة باستخدام إحصائيات التدفق. تشير النتائج التجريبية إلى أن النماذج المطورة تحقق معدلات منخفضة من الإشارات الإيجابية الخاطئة مع إظهار دقة واعدة ووقت حوسبة فعال .

Abstract

As the number of Internet users and computer networks continues to increase, there is a growing demand for effective security monitoring systems, such as network detection systems. Many researchers are concentrating on this area and exploring various approaches to develop robust detection systems that can protect computer networks from attacks using traditional techniques. A new approach to system detection that utilizes aggregated traffic metrics is the flow-based intrusion detection system.

This research presents a neural network-based anomaly detection system for identifying network traffic attacks using flow statistics. The experimental results indicate that the developed models achieve low false positive rates while demonstrating promising accuracy and efficient computing time.

Keywords: Intrusion Detection System, Network flows, Neural Network, Flow-based datasets, Anomaly detection.

1. Introduction

Attacks on our computer networks are increasingly becoming a significant concern for network users. Regardless of the attackers' skill level, they generate unwanted traffic that can negatively impact the performance and reliability of existing services. To address this issue, operators utilize intrusion detection systems to identify and potentially filter out suspicious traffic.

The continuous increase in network traffic with high-speed network equipment [12] poses challenges to traditional packet-based intrusion detection systems.

These systems rely on deep packet payload inspection, which does not scale effectively in a high-speed environment. In such contexts, flow-based approaches, which utilize aggregated traffic metrics, show significantly better scalability and more promising techniques. The key advantage of flow-based methods is that they require analyzing only a fraction of the total data, making them more efficient.

A flow is a one-way stream of packets that share common properties, such as source and destination addresses, ports, and protocol type. In addition, the stream includes aggregated information about the number of packets and number of bytes that belong to the stream, as well as its duration. Flows are often used to monitor the network to get a real-time overview of the state of the network. Most known tools that rely on network flow are NFsen [24] and flow-scan [6], while the actual standard technology in this area is Cisco NetFlow, in particular its version five and nine [2.5], and the IPfix working group [13].

There are two main categories of intrusion detection techniques based on the modeling methods used: anomaly detection and misuse detection. Misuse detection involves comparing usage patterns to identify known methods for compromising computer security.

While a misuse detection system is effective for known types, it cannot identify new attacks that have not been predefined. In contrast, an anomaly detection system addresses the issue by searching for deviation from established usage patterns.

While misuse detection is effective for known intrusion types, it cannot identify new attacks that have not been predefined. In contrast, anomaly detection addresses the issue by searching for deviations from established usage patterns.

Anomaly detection systems can identify new attacks but may also result in many false alarms due to the wide variation in normal behavior. Additionally, obtaining a comprehensive understanding of what constitutes normal behavior can be challenging. Intrusion detection systems can be classified into three architectural types: network-based intrusion detection systems, host-based intrusion detection systems, and hybrid intrusion detection systems [14][8].

The network-based intrusion detection system relies on network traffic information as the main source of data. In contrast, the host-based intrusion detection system uses audit trails for the operating system as the primary source of data. The hybrid intrusion detection system incorporates these two methods [19].

This paper discusses the detection of anomalies with the use of NetFlow data set. It has been proposed to use multilayer neural network algorithms to build an effective network anomaly detection model based on neural networks.

This paper will be organized as follows: Section two will review previous works, Section three will offer a brief introduction to neural networks, Section four will explain the design and training of the Neural Network Model, Section five will discuss the experimental results, and finally, the paper will conclude.

2. Previous Work

Specifically, numerous methods based on neural networks have been used to detect intrusion. Tie and Li [32] employed the BP network with GAs and various attack techniques with specific KDD data properties to improve BP. Accordingly, the detection rates for Peral, Satan, and Guess-password were 90.79, 85.60, and 90.97 respectively. With a false alarm rate of 7.35, the overall detection rate accuracy is 91.61. The classification result is 25/25 according to Jimmy and Heidar [15], who employed feed-forward neural networks with the back propagation training algorithm and certain features from the TCP dump.

Novikov, Yampolskiy, and Reznik [7] used a Multi-layer Perceptron and Radial Basis Function neural network to identify five different types of attacks. Their result shows that the accuracy of classifying these attacks was 93% for both models of neural networks with low in false alarms.

In 2007 [31], researchers developed an artificial neural network intrusion detection system designed to detect and classify two types of attack based on normal behavior. The system was trained using the backpropagation algorithm. The results show that it achieved a 94% detection rate for classifying records. Y Abuadlla, G Kvascev, S Gajin, Z Jovanovic [33] proposed a two-stage neural network anomaly intrusion detection system based on the NetFlow dataset. The results obtained from the proposed system show a detection rate of 94.4% for anomaly detection at stage one and 99.4% for classification at stage two.

Mukkamala, Andrew, and Ajith [27] employed the Backpropagation Neural Network with multiple learning algorithms, resulting in a network performance of 95.0%. The RPBRO classification yielded an overall accuracy of 97.1% and demonstrated a low false alarm rate. In 2008, Kukielka & Kotulski [17] analyzed various neural network architectures for their proposed system. The training dataset used was KDD99. Results indicated that the multilayer perceptron was the most efficient, utilizing less CPU power and memory.

Due to its efficiency, they tested the network without dividing the dataset into smaller subsets. S. Jimmy and A. Heidar [28] used a neural network for classifying unknown attacks, resulting in a correct classification rate of 76%.

In a study conducted by Vallipuram and Robert [20], the backpropagation neural network was designed to analyze all features of the KDD dataset. The results showed a classification rate of 100% for normal traffic, 80% for known attacks, and 60% for unknown attacks. Another study by Dima, Roman [8], and Leon focused on using a Radial Basis Function and a Multilayer Perceptron neural network for attack classification using a KDD dataset. The classification accuracy was 93.2% using the Radial Basis Function neural network and 92.2% with the Multilayer Perceptron neural network. Novikov, Roman, and Reznik [23] used Multilayer Perceptron and Radial Based Function neural networks to classify five types of attacks. Ahmed, Ullah, and Mohsin [1] utilized the Resilient Backpropagation algorithm to detect network intrusion attacks with greater accuracy by leveraging the capabilities of this learning algorithms. M. Mohamed and T. Jawhar [21] utilized Fuzzy C-Means and neural network algorithms, achieving an overall classification accuracy of 99.9% with a low false rate. Rodrigo Braga [26] employed OpenFlow and a Self-Organizing Map unsupervised neural network, achieving a detection rate comparable to other approaches. Other researchers [3],[9] use different neural network approaches for attack classification.

3. Neural Network

Neural Networks have gained more attention than other techniques, primarily due to their strong discrimination and generalization abilities for classification tasks [22]. In recent years, research has increasingly explored the use of Neural Networks for intrusion detection. When properly designed and implemented, neural networks can effectively address many issues faced by rule-based approaches. The neural network approach is designed to understand the typical characteristics of system users and detect significant variations from their usual behavior. To apply this method to intrusion detection, we need to include data that represents both attacks and non-attacks when training the neural network. This will allow the network to automatically adjust its coefficients during the training phase. In addition, it is necessary to collect data representing normal and abnormal behavior and train the Neural Network. After the training is complete, performance tests using actual network traffic and attacks should be conducted [8]. Neural network-based models analyze multiple hypotheses simultaneously using interconnected computational elements. This enables quicker processing of malicious traffic [29].

In this study, an offline intrusion detection system is implemented using a Multi-Layer Perceptron neural network. The neural network is trained with NetFlow data.

In contrast, many previous studies [17], [30], utilized a neural network with the DARPA dataset [10,18].

3.1 Multi-Layer Perceptron

A multilayer perceptron (MLP) is a class of feedforward artificial neural networks consisting of multiple layers of nodes, each fully connected to the next. This structure allows the network to model complex relationships within the data. The MLP is a foundational architecture in neural networks, characterized by its use of multiple layers of interconnected nodes arranged in an input layer, one or more hidden layers, and an output layer, as shown in figure 1, each consisting of interconnected neurons that enable complex function approximation. The activation function plays a crucial role in the performance of multi-layer perceptron by introducing non-linearity into the model, allowing the network to learn intricate patterns in data [25,16].

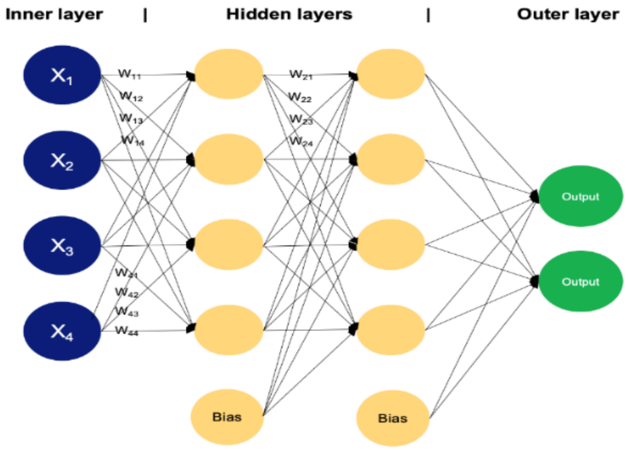

Figure 1: A multilayer perceptron with two hidden layers.

Training a Multi-Layer Perceptron involves several essential steps, including selecting an appropriate dataset, initializing weights, and applying optimization algorithms to adjust those weights during the training process [4]. The backpropagation algorithm is the most commonly used method for training MLPs, although it can be slow. In contrast, the Levenberg-Marquardt algorithm [11] is known for its accuracy and faster performance than the backpropagation algorithm.

4. Proposed Anomaly Detection System

We suggested a module to detect abnormal network traffic. This traffic often originates from malicious activities, including DoS/DDoS attacks, worms, and port scanning. The anomaly detection module, shown in Figure 2, comprises three main modules. The following subsections will provide detailed descriptions of these modules.

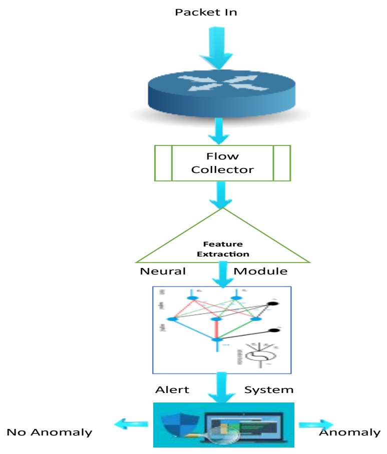

Figure 2: Proposed Anomaly Detection System

4.1 Flow Collector and Extractor Module

The flow collector and extractor module is tasked with generating a flow by gathering a series of packets. The flow is extracted periodically and stored in the flow database. The extraction frequency can be configured according to the flow timeout, enabling the flow information to be collected over a specified period, such as one minute.

4.2 Feature Extraction Module

The main function of this module is to process collected flows to extract key features for anomaly intrusion detection. It then organizes these features into 6-tuples, as described in Table 1, which are forwarded to the neural network anomaly detection module.

Table 1. Selected Features

No	Feature	Description	Possible attack
1	PN	Packet Number	DoS attack
2	PS	Packet Size	Flooding attack
3	FZ	Flow Size	Low size (attack)
4	FSD	Flow to same Destination IP	Flood attack, Port scan attack
5	FDD	Flow to Different Destination IP	System attack
6	Syn/Ack	Syn bit and Ack bit	DoS attack

4.3 Neural Network Anomaly Detection Module

The proposed Intrusion Detection Systems (IDSs) include a crucial component known as the detection module, which analyzes and identifies intrusions through an artificial neural network. We chose a neural network for the detection module due to its flexibility. The objective of this module is to develop a security mechanism capable of intelligently detecting both known and unknown attacks. To accomplish this, we utilize a Multilayer perceptron neural network and a Resilient backpropagation activation algorithm for the anomaly detection module. The network was trained and tested using a NetFlow dataset. The architecture, including the number of hidden layers and the number of nodes within those layers, was determined through a trial-and-error approach. During the training stage, the neural network was provided with the labeled dataset, consisting of attack and nonattack records. After the training process, the weight values were stored for use in the recall stage. We examined the neural module with various network architectures and different activation algorithms.

4.4 Alert System

This stage marks the final step of the proposed system. It involves identifying the events that have occurred, presenting the observed network status to the administrator, and generating alarms when necessary.

5. Experiment and Results

In this section, we experimentally evaluate the proposed intrusion detection system based on the NetFlow dataset and compare the results for different types of neural networks. The experiments and evaluation have been conducted using the MATLAB Neural Network Toolbox version R2011b, (i5-10210U CPU, RAM:8 GB).

The primary function of the neural network module is to detect attacks by distinguishing between normal and abnormal data flows. Training and testing were conducted using the NetFlow dataset, which utilizes six selected features. The Neural Network module comprises one input layer, one hidden layer, and one output layer, consisting of 71, 50, and 2 nodes, respectively. The number of nodes in the hidden layer was determined through a series of experiments. The training, validation, and testing results for the neural network detection module are presented in Table 2 and Figure 3.

Table 2. Results of the Neural Detection Module

Neural Network Architecture	Training Algorithm	Training dataset	Validation Data	Testing Data	Epoch	Time	Hidden Layer	Detection Rate
Multilayer perceptron	Resilient B.propagation	72705	10908	10908	201	08:05	50	92.712%
	Levenberg-Marquardt	72705	10908	10908	109	4:03	50	92.2%
	Radial Basis Function Net	72705	10908	10908	-	0:55	20	91.1%

In Table 2, the total input data consists of 72705 records, out of which 48426 records were attacks, and 24279 records were classified as normal. 10908 records were used to test the neural network, comprising of 7272 attack records and 3636 normal records. The results from numerous tests showed that 6723 records were identified as attacks and 3545 records were identified as normal. The attack detection rate was calculated using the following equation:

$$\text{Detection Rate}=\frac{\text{No of detected attacks}}{\text{Total No. of normal attacks}} * 100 \quad [\%]$$

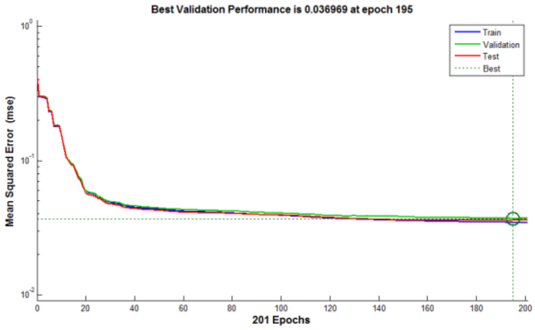

Figure 3. Performance of the proposed system

6. Conclusion

Our work introduced a neural network-based system for detecting anomalous intrusion attacks. Our system demonstrated that using a neural network based on the NetFlow dataset with the most relevant features helps to detect anomalies with low overhead compared to approaches based on the KDD-99 dataset. The detection rate of 92.5% obtained is remarkably good, closely aligning with the results of other approaches using different training datasets (such as DARPA) and similar training datasets (NetFlow).

The future work will focus on developing a more accurate model that significantly decreases computational costs and classifies the type of attack.

7. REFERENCES

[1] Ahmad I., Ullah S., Swati, and Mohsin S., "Intrusions Detection Mechanism by Resilient Back Propagation (RPROP)", European Journal of Scientific Research, vol. 17, No.4, pp. 523-531, 2007.

[2] B. Claise. Cisco Systems NetFlow Services Export Version 9. Request for Comments: 3954, October 2004. IETF. nfsen.sourceforge.net, April 2008.

[3] 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), Guwahati, 2016, pp.1-6.doi: 10.1109/NCC.2016.

[4] Cybenko, G. 1989. Approximation by superpositions of a sigmoidal function, Mathematics of Control, Signals, and Systems, 2(4), 303–314

[5] Cisco IOS NetFlow Configuration Guide. www.cisco.com, April 2008.

[6] D. Plonka. Flowscan. www.caida.org/tools/utilities/flowscan/, April 2008.

[7] D. Novikov, V. Roman Yampolskiy, and L. Reznik, "Anomaly Detection Based Intrusion Detection", IEEE computer society.2006.

[8] D. Novikov, V. Roman Yampolskiy, and L. Reznik,"Artificial Intelligence Approaches For Intrusion Detection", IEEE computer society.2006.

[9] D, Vrushali & Pawar, Anomaly based IDS using Backpropagation Neural Network. International Journal of Computer Applications.2016, 136. 29-34. 10.5120/ijca2016.

[10] DARPA1998 http://www.ll.mit.edu/IST/ideval/docs/1998

[11] Hagan, M.T., and M. Menhaj, "Training feed-forward networks with the Marquardt algorithm," IEEE Transactions on Neural Networks, Vol. 5, No. 6, 1999, pp. 989–993,

[12] Internet2 NetFlow: Weekly Reports. netflow.internet2.edu/weekly, April 2008.

[13] IP Flow Information Export Working Group www.ietf.org/html.charters/ipfix-charter.html, April 2008.

[14] J., Muna. M. and Mehrotra M., "Intrusion Detection System: A design perspective", 2rd International Conference On Data Management, IMT Ghaziabad, India. 2009.

[15] J. Shum and A. Heidar Malki, "Network Intrusion Detection System Using Neural Networks", Fourth International Conference on Natural Computation, IEEE computer society.2008.

[16] Java neural network framework, http://neuroph.sourceforge.net/

[17] Kukiełka, P. & Kotulski, Z. (2010). Adaptation of the neural network-based IDS to new attacks detection. arXiv - Cornell University. Retrieved October 26, 2011.

[18] KDDCup1999: http://kdd.ics.uci.edu/databases

[19] M. Khattab Ali, W. Venus, and M. Suleiman Al Rababaa, "The Affect of Fuzzification on Neural Networks Intrusion Detection System", IEEE computer society.2009.

[20] M. Vallipuram and B. Robert, "An Intelligent Intrusion Detection System based on Neural Network", IADIS International Conference Applied Computing.2004.

[21] Muna Mhammad T. Jawhar," Design Network Intrusion Detection System using hybrid Fuzzy- Neural Network", International Journal of Computer Science and Security, Volume (4).2009

[22] M. Al-Subaie, "The power of sequential learning in anomaly intrusion detection", degree master thesis, Queen University, Canada.2006.

[23] Novikov D., Roman V., Yampolskiy, and Reznik L., "Anomaly Detection Based Intrusion Detection", IEEE Third International Conference on Communication, Networking & Broadcasting, ITNG, pp 420-425, 2006.

[24] P. Haag. Nfsen: Netflow sensor.

[25] Rosenblatt, Frank. x. Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms. Spartan Books, Washington DC, 1961

[26] Rodrigo Braga," Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow", 35th Annual IEEE Conference on Local Computer Networks LCN 2010, Denver, Colorado

[27] S. Mukkamala, H. Andrew Sung, and A. Abraham, "Intrusion detection using an ensemble of intelligent paradigms", Journal of Network and Computer Applications 28. pp167–182.2005.

[28] S. Jimmy and A. Heidar, "Network Intrusion Detection System using Neural Networks", IEEE computer society.2008.

[29] S. Lília de Sá, C. Adriana Ferrari dos Santos, S.Demisio da Silva, and A. Montes, "A Neural Network Application for Attack Detection in Computer Networks", Instituto Nacional de Pesquisas Espaciais – INPE, BRAZIL.2004.

[30] Srinivas Mukkamala, "Intrusion detection using neural networks and support vector machine," Proceedings of the 2002 IEEE International Honolulu, HI, 2002

[31] Sammany, M., Sharawi, M., El-Beltagy, M. & Saroit, I. Artificial Neural Networks Architecture For Intrusion Detection Systems and Classification of Attacks. Faculty of Computers and Information Cairo University. (2007).

[32] T. Zhou and LI Yang, "The Research of Intrusion Detection Based on Genetic Neural Network", Proceedings of the 2008 International Conference on Wavelet Analysis and Pattern Recognition, Hong Kong, IEEE.2008.

[33] Y. Abuadlla, Kvascev, G., Gajin, S., & Jovanovic, Z. (2014). Flow-based anomaly intrusion detection system using two neural network stages. *Computer Science and Information Systems*, *11*(2), 601-622.