A Novel Intrusion Detection System Based on Neural Networks

Antonios Andreatos[1,*], *Vassilios* Moussas[2]

[1]Div. of Computer Engineering and Information Science, Hellenic Air Force Academy, Dekeleia, Attica, Greece
[2]Univ. Of West Attica, School of Engineering, Campus 1, 12210 Egaleo, Athens, Greece

Abstract. This paper proposes a novel intrusion detection system (IDS) based on Artificial Neural Networks (ANNs). The system is still under development. Two types of attacks have been tested so far: DDoS and PortScan. The experimental results obtained by analyzing the proposed IDS using the CICIDS2017 dataset show satisfactory performance and superiority in terms of accuracy, detection rate, false alarm rate and time overhead, compared to state of the art existing schemes.

1 Introduction

1.1 Growth of internet attacks

During the last decade cyber attacks, especially those targeting systems that keep or process sensitive information, are becoming more sophisticated [Singh]. Critical National Infrastructures are main targets of cyber attacks, since essential information or services depend on their systems and their protection becomes a significant issue for both nations, as well as, organisations [1].

Intrusion detection systems (IDS) are typically classified into two types:

- Signature-based IDS
- Anomaly-based IDS

The growth of internet attacks in volume and diversity drived to the development of more complex systems such as Hybrid IDS and ANN-based systems which will be discussed in this work.

1.2 Limitations of existing IDSs

Signature-based IDSs use predefined patterns (signatures) of known malicious code pieces. From the review of past research, it comes out that the signature-based approaches have high detection rate for known attacks, but these techniques fail miserably for unknown threats. These types of approaches need regular updating of attack signatures.

Anomaly detection IDS use no predefined signatures, fact which enables them to classify or detect any type of intrusions. Anomaly-based approaches can be used to detect zero-day attacks [2], but these have a high rate of false alarms. Anomaly detection techniques also experience low accuracy rate. Hybrid approaches can be used to find known and unknown attacks but are quite complex and take longer time to generate alerts.

These issues are open research challenges in the field of anomaly-based IDS. Anomaly detection techniques with high accuracy, less false alarms and lower detection time are required. IDSs specifically for wireless networks and large-scale computer networks have also gained increased research attention [3].

1.3 Recent research on IDSs

Many supervised and unsupervised techniques have been devised by researchers from the discipline of machine learning and data mining to achieve reliable detection of anomalies. Deep learning is an area of machine learning which applies neuron-like structures for learning tasks [4 -7].

The self-adaptive nature of ANNs makes them capable of capturing highly complex and non-linear relationships between both dependent and independent variables without prior knowledge; hence, ANN-based intrusion detection systems will be able to detect new threats with unknown signatures, in contrast to signature-based IDSs.

A learning ANN-based IDS is best suited for attacks and malware because of the dynamically changing behavior of modern malware and internet attacks. Researchers have also suggested the use of IDS to counter correlated attacks such as large-scale stealthy scans, worm outbreaks and DDoS attacks [8]. This work focuses on detecting two major types of attacks, namely DDoS and Port Scanning using ANN-based systems.

2 Literature Review

Shenfield, Day and Ayesh [9] present a novel approach to detecting malicious network traffic using artificial neural networks suitable for use in deep packet inspection based intrusion detection systems. The proposed artificial neural network architecture is a non-

* Corresponding author: antonios.andreatos@hafa.haf.gr

signature based detection mechanism for malicious shellcode based around ANNs. Results presented show that this novel classification approach is capable of detecting shellcode with extremely high accuracy and minimal numbers of false positives.

Amruta and Talha [10] present a Denial of Service Attack Detection using Artificial Neural Network for Wired LANs. The proposed ANN classifier gives ninety six percent accuracy for their training data set in less time.

Naseer et al. [4] propose Intrusion Detection models implemented and trained using different deep neural network architectures including Convolutional Neural Networks, Autoencoders, and Recurrent Neural Networks. These deep models were trained on NSLKDD training dataset and evaluated on both test datasets provided by NSLKDD namely NSLKDDTest+ and NSLKDDTest21. To make model comparisons more credible, we implemented conventional ML IDS models with different well-known classification techniques including Extreme Learning Machine, k-NN, Decision-Tree, Random-Forest, Support Vector Machine, Naive-Bays, and QDA. Both DNN and conventional ML models were evaluated using well-known classification metrics including RoC Curve, Area under RoC, Precision-Recall Curve, mean average precision and accuracy of classification. Both DCNN and LSTM models showed exceptional performance with 85% and 89% Accuracy on test dataset which demonstrates the fact that Deep learning is not only viable but rather promising technology for information security applications like other application domains.

The authors use the NSLKDD dataset provided by Tavallaee et al. [11] using a GPU-powered test-bed. NSLKDD is derived from KDDCUP99 [12] which was generated in 1999 from the DARPA98 network traffic.

3 The proposed Intrusion Detection System

The proposed system uses ANNs in order to classify the attacks. Currently, it consists of two NN modules, each one specialising a on specific attack type, namely DDoS and PortScan. Both NN modules have the same structure but different parameters. The final system is planned to be modular, i.e. easily expandable by adding more ANN modules tailored to additional types of attacks. The proposed Intrusion Detection System was simulated in Matlab [13].

3.1. Structure of the ANN

The structure of the proposed system is shown in Figure 1. It consists of an input layer of size 67, a hidden layer of size 20 and an output layer of size 1.

This structure has been optimised to deal with both types of attacks considered so far in our work.

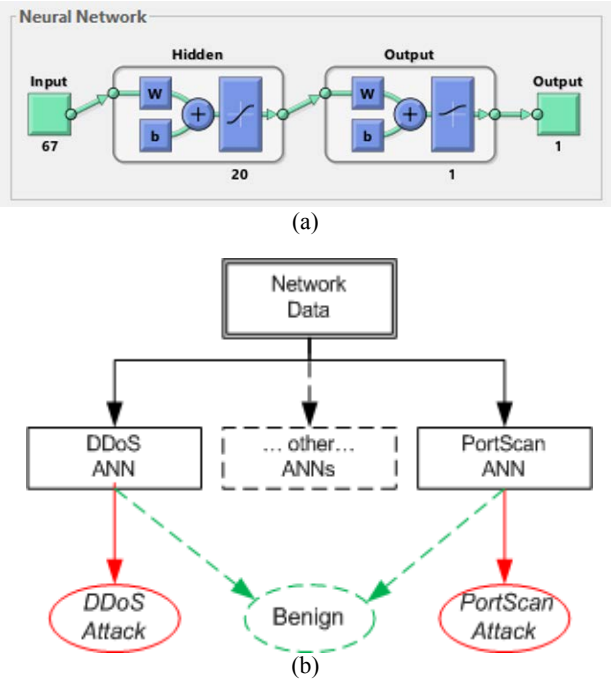

Fig. 1. ANN Structure (a) and the overal system architecture (b) of the proposed IDS

4 Simulation Results

4.1 Dataset Description

Every day new types of attacks appear and a need for continuous update of the IDS is required. Hence, recent test datasets including most recently discovered attack should be used for performance evaluation as well as training of new IDS.

A recent dataset which includes many modern attacks provided by the Canadian Institute for Cybersecurity has been used, called CICIDS2017 [14]. CICIDS2017 dataset contains benign and the most up-to-date common attacks, which resembles true real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter with labeled flows based on the time stamp, source and destination IPs, source and destination ports, protocols and attack (as CSV files).

4.2 Results

From the above dataset, DDoS and PortScan sets were selected to train the ANNs. Each case was split in three subsets, one for training (70%), one for testing (15%) and one for validation (15%). For the training, the scaled conjugate gradient backpropagation was selected to minimize memory requirements.

All available parameters in the dataset were used as inputs to the ANNs. Although some of them demonstrate higher corellation to each attack, our aim is to create a

more generic tool that processes all available data. A sample of these data is shown in figure 2.

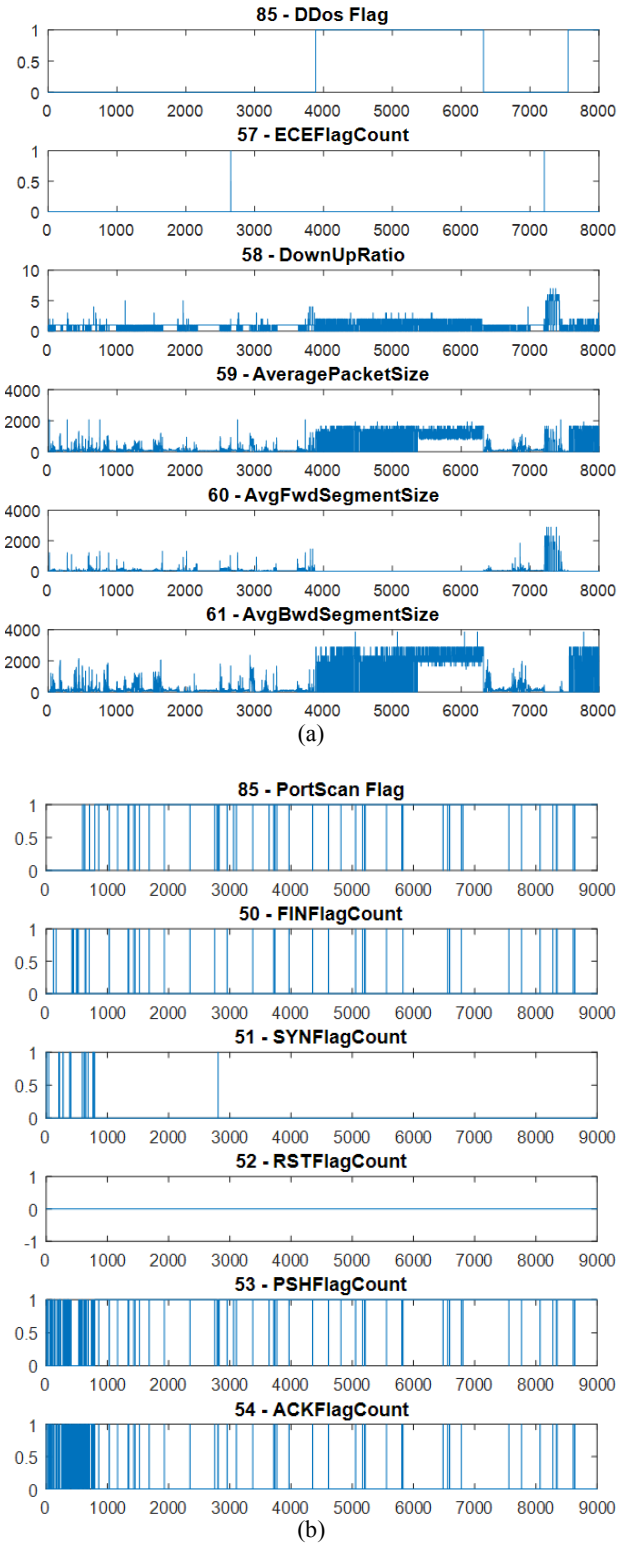

Fig. 2. Samples of the DDoS (a) and PortScan (b) datasets

The Confusion Matrices of both ANNs indicate a satisfactory rate of detection with over 99.8% accuracy, as well as a very high precision and sensitivity (above 95%).

The two confusion matrices for the DDoS-ANN and the PortScan-ANN are shown in figures 3a and 3b respectively.

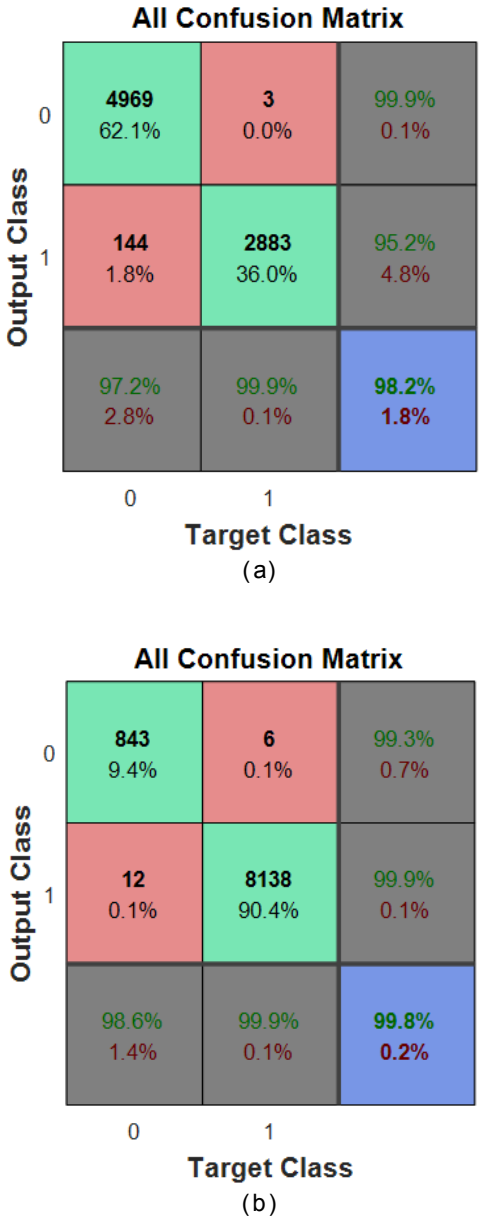

Fig. 3. Confusion Matrix of the ANN-IDS (a) for DDoS, (b) for PortScan Attacks

Finally, figure 4 shows the mean squared error (mse) versus the amount of ANN training epochs for the two ANNs with 20 neurons in the hidden layer.

The mean squared error is calculated taking into account the difference between the results obtained from the validation test and the expected ANN results. From the displayed figure, it is clear that the ANN performance evolves through epochs, and also that, for the DDoS case close to 55 epochs, the MSE reaches a stable value around 0.04, and for the PortScan case close to 70 epochs, the MSE reaches a stable value around 0.014.

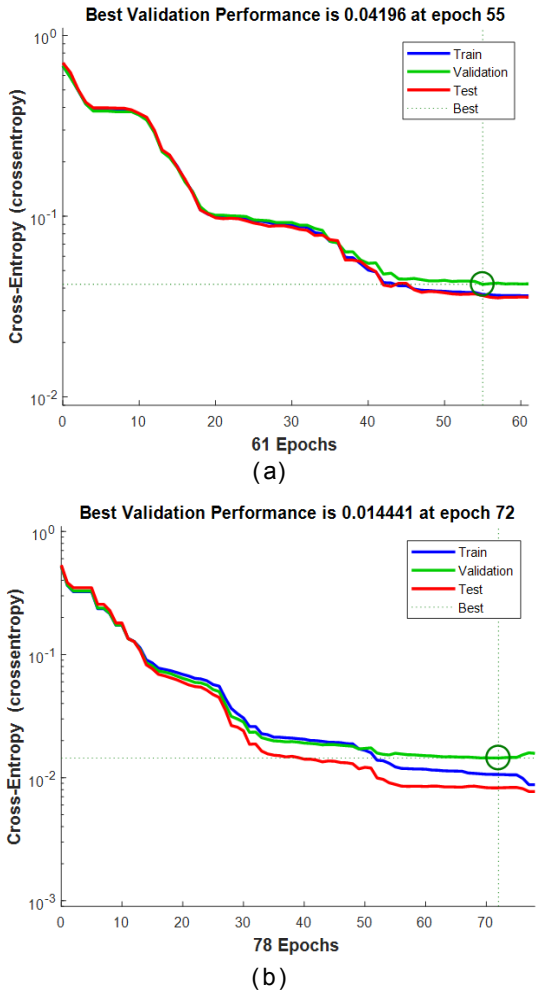

Fig. 4. Mean Squared Error vs the number of Training Epochs for: (a) the ANN for DDoS and (b) the ANN for PortScan, both using 20 neurons in the hidden layer.

5 Conclusions and Future Work

In this paper we have presented an ANN-based IDS for detecting DDoS and Port Scannning attacks. Experimental results obtained from the CICIDS2017 dataset show high detection rates, as well as, low false-positive rates. In the near future we plan to expand this project to additional types of attacks in order to become more practical and useful. Combined attacks are also under investigation, as each attack is shown to correlate to different dataset parameters.

Another area identified for further work is the application of the intelligent approach to intrusion detection outlined here to other areas of network security such as the detection of cross-site scripting attacks.

References

1. A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour and H. Janicke, A Novel Hierarchical Intrusion Detection System based on Decision Tree and Rules-based Models. In Proceedings of *SecRIoT 2019, 1st International Workshop on Security and Reliability of IoT Systems*. Santorini Island, Greece, May 29-31, 2019.
2. https://www.techopedia.com/definition/29738/zero-day-attack.
3. R. Singh, H. Kumar, R. K. Singla, R. R. Ketti, Internet attacks and intrusion detection system: A review of the literatur, Online Information Review, **41**, 2, pp. 171-184, (2017) https://doi.org/10.1108/OIR-12-2015-0394 Permanent link to this document: https://doi.org/10.1108/OIR-12-2015-0394.
4. S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal and K. Han, Enhanced Network Anomaly Detection Based on Deep Neural Networks. IEEE Access, Special section on cyber-threats and countermeasures in the healthcare sector.
5. T. Auld, A. W. Moore and S. F. Gull, Bayesian Neural Networks for Internet Traffic Classification. IEEE Transactions on Neural Networks, **18**, 1 (2007).
6. B. Shah and B. H. Trivedi, Artificial Neural Network based Intrusion Detection System: A Survey. International Journal of Computer Applications (0975 – 8887), **39**, 6 (2012).
7. N. el Kadhi, K. Hadjar and N. el Zant, A Mobile Agents and Artificial Neural Networks for Intrusion Detection. Journal of Software, **7**, 1 (2012).
8. C. V. Zhou, C. Leckie and S. Karunasekera, A survey of coordinated attacks and collaborative intrusion detection. Computers and Security, **29**, 1, pp.124-140 (2010).
9. A. Shenfield, D. Day and A. Ayesh, Intelligent intrusion detection systems using artificial neural networks. ICT Express **4,** pp. 95–99 (2018).
10. M. Amruta and N. Talhar, Effective Denial of Service Attack Detection using Artificial Neural Network for Wired LAN. In Proceedings of *SCOPES - International conference on Signal Processing, Communication, Power and Embedded System* (2016).
11. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, A detailed analysis of the KDD CUP 99 data set, in Proc. *IEEE Symp. Comput. Intell. Secur. Defense Appl. (CISDA)*. Piscataway, NJ, USA: IEEE Press, 2009, pp. 53–58. [Online]. Available: http://dl.acm.org/citation.cfm?id=1736481.1736489.
12. S. D. Bay, D. Kibler, M. J. Pazzani, and P. Smyth, The UCI KDD archive of large data sets for data mining research and experimentation, ACM SIGKDD Explor. Newslett., **2**, 2, pp. 81–85, 2000.
13. Mathworks, Matlab neural network toolbox. https://uk.mathworks.com/products/neural-network.html, 2016.
14. Canadian Institute for Cybersecurity, CICIDS2017 dataset.Available: https://www.unb.ca/cic/datasets/ids-2017.html.