A Modular Intrusion Detection System based on Artificial Neural Networks

Antonios S. Andreatos and Vassilios C. Moussas

Abstract—This paper proposes a novel Intrusion Detection System (IDS) based on Artificial Neural Networks (ANNs). The proposed multi-ANN system is modular, parallel and easily expandable in order to detect additional types of attacks. Three types of attacks have been tested so far: DDoS, PortScan and Web attacks. The experimental results obtained by analyzing and testing 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 existing single-ANN systems.

***Keywords*—**Intrusion Detection Systems, Anomaly-based IDS, Cyber Attacks, DDoS, Neural Networks, PortScan, Web Attacks.

I. Introduction

A. Growth of Internet attacks

During the last decade, cyber attacks, especially those targeting systems that keep or process sensitive information, are becoming more sophisticated [1]. Critical national infrastructures are the main targets of cyber attacks as they handle sensitive information or services. Therefore, their protection becomes an important issue for both nations and organizations [2].

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 drove to the development of more complex systems such as Hybrid IDS and ANN-based systems which will be discussed in this work.

B. Limitations of existing IDS

Signature-based IDS 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 also need regular updating of attack signatures.

Anomaly detection IDS use no predefined signatures, a fact which enables them to classify or detect any type of intrusion. Anomaly-based approaches can be used to detect zero-day attacks [3], 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 a 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 shorter detection time are required. IDS specifically for wireless networks and large-scale computer networks have also gained increased research attention [1].

C. Recent research on IDS

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 [4], [5], [6]. Deep learning is an area of machine learning which applies neuron-like structures for learning tasks [7]-[10].

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 IDS.

A learning ANN-based IDS is best suited for new, sophisticated attacks and malware because of the dynamically changing behavior of modern malware. Researchers have also suggested the use of IDS to counter correlated attacks such as large-scale stealthy scans, worm outbreaks and DDoS attacks [11]. This work focuses on the detection of three major types of attacks, namely DDoS, Port Scanning and Web attacks, using ANN-based systems.

II. Literature Review

Shenfield, Day and Ayesh [12] present a novel approach to detecting malicious network traffic using artificial neural networks suitable for use in deep packet inspection based IDS. The proposed artificial neural network architecture is a non-signature based detection mechanism for malicious shell code built around ANNs. Results presented show that this novel classification approach is capable of detecting shell code with extremely high accuracy and minimal numbers of false identifications.

Amruta and Talha [13] present a Denial of Service Attack

A. S. Andreatos is with the Div. of Computer Engineering and Information Science, Hellenic Air Force Academy, Dekeleia, Attica, Greece (phone: +30 210 8192360; fax: +30 210 8074606; e-mail: antonios.andreatos@hafa.haf.gr).

V. C. Moussas is with the Univ. of West Attica, School of Engineering, 12210 Egaleo-Athens, Attica, Greece (e-mail: vmouss@uniwa.gr).

Detection system using Artificial Neural Network for wired LANs. The proposed ANN classifier gives ninety six percent accuracy for their training data-set.

Naseer et al. [7] 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 the NSLKDD training dataset and evaluated on both test datasets provided by NSLKDD namely NSLKDDTest+ and NSLKDDTest21. To make model comparisons more credible, they implemented conventional machine learning (ML) IDS models with different well-known classification techniques including Extreme Learning Machine, k-NN, Decision-Tree, Random-Forest, Support Vector Machine, Naive-Bayes 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 [7]. 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.* [14], using a GPU-powered test-bed. NSLKDD is derived from KDDCUP99 [15] which was generated in 1999 from the DARPA98 network traffic.

III. The Proposed Intrusion Detection System

The proposed system uses ANNs in order to classify the attacks. Currently, it consists of two ANN modules, each one specializing in a specific attack type, namely DDoS and PortScan. Both ANN 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. In addition, a single ANN system is also implemented for comparison purposes, trained to detect the aforementioned types of attacks. All the Intrusion Detection Systems presented here were simulated in Matlab [16].

A. Structure of the proposed ANN system

The proposed system uses multiple ANN modules (Fig. 1a). Each ANN module consists of an input layer of size 67, a hidden layer of size 20 and an output layer of size 1 (Fig. 1b). This structure (layers and nodes) has been optimized to deal with all types of attacks considered so far in our work.

The modular structure of the proposed multi-ANN system is shown in Fig. 1a. Each ANN module is trained to detect only one type of attack or anomaly and several ANNs run in parallel to handle the different types.

For comparison reasons, a single-ANN system is also trained to detect all candidate types of attacks using only one module as shown in Fig. 1c. The single module consists of an input layer of size 67, a hidden layer of size 20 and an output layer of size 3 as shown in Fig. 1d.

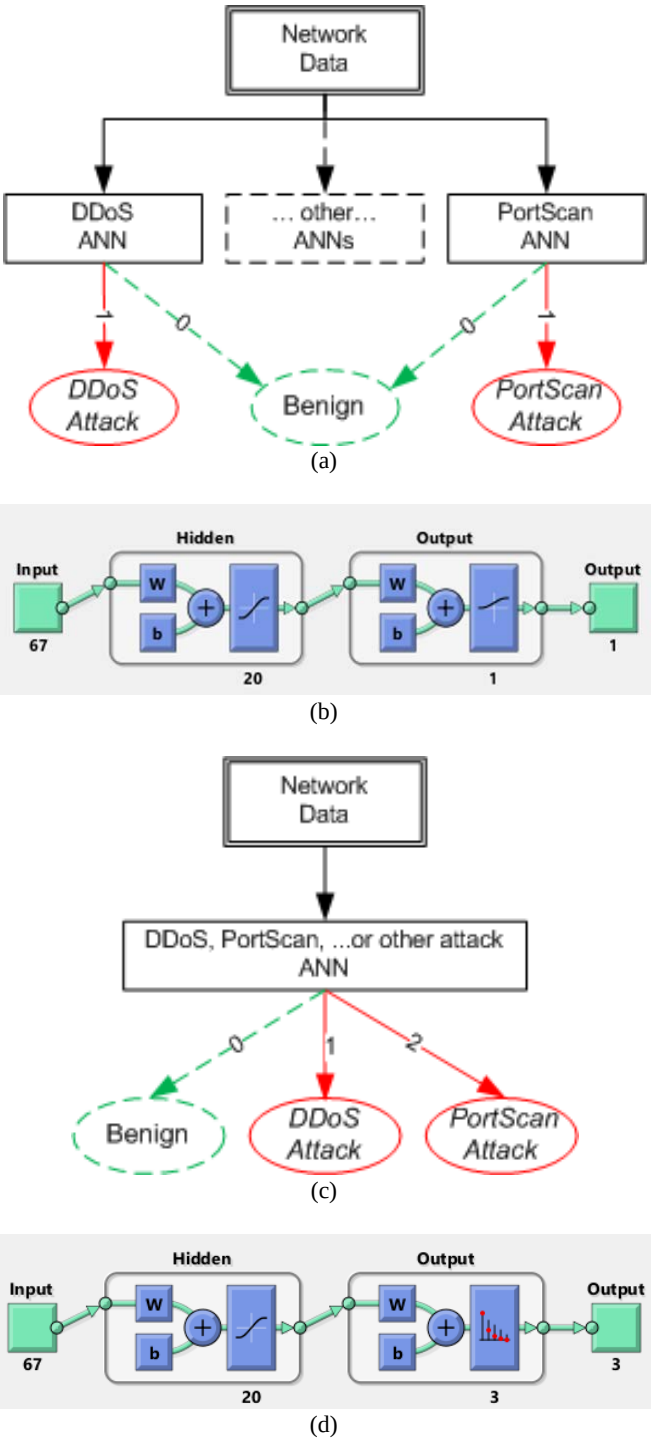


Fig. 1 (a) Overall system architecture of the proposed multi-ANN IDS; (b) ANN modules structure; (c) architecture of a single-ANN IDS; (d) Single-ANN module structure.

IV. Simulation Results

A. 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.

In this work, a recent dataset which includes many modern attacks provided by the Canadian Institute for Cybersecurity has been used, called CICIDS2017 [17]. CICIDS2017 dataset contains most up-to-date common attacks, which resembles true real-world data (packet capture files, pcap). It also includes the results of the network traffic analysis using CICFlowMeter with labeled flows based on the timestamp, source and destination IPs, source and destination ports, protocols and attack (as csv files).

The csv files are organized as pcap files, i.e., the columns are the traffic parameters and the rows represent the packets. The CICIDS2017 dataset csv files have 85 columns. The 67 of these columns are the inputs of our NN modules.

B. Results for the multi-ANN system

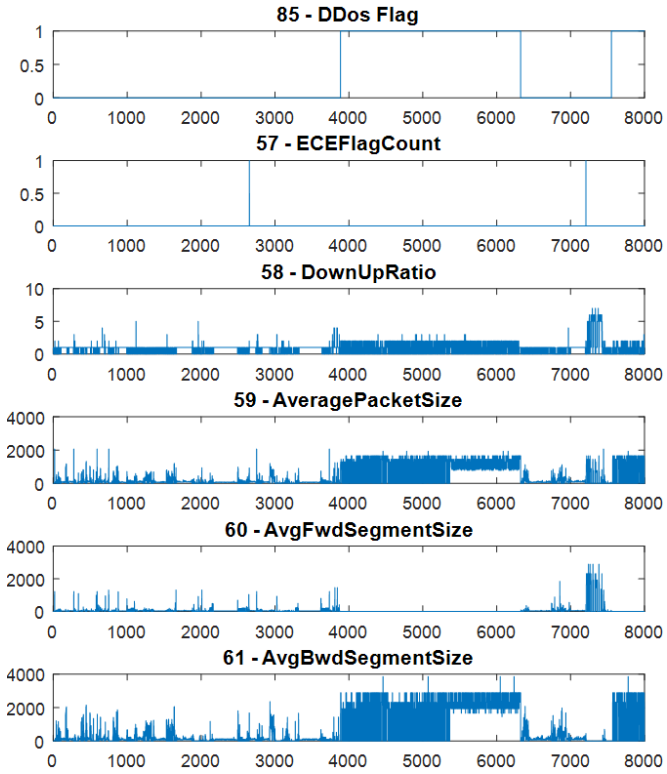
From the above dataset, DDoS and PortScan sets were first selected to train the ANNs. Each case was split into three subsets, one for training (70%), one for testing (15%) and one for validation (15%). For the training, the scaled conjugate gradient back propagation was selected to minimize memory requirements.

All available parameters in the dataset were used as inputs to the ANNs. Although some of them demonstrate higher correlation 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 Fig. 2.

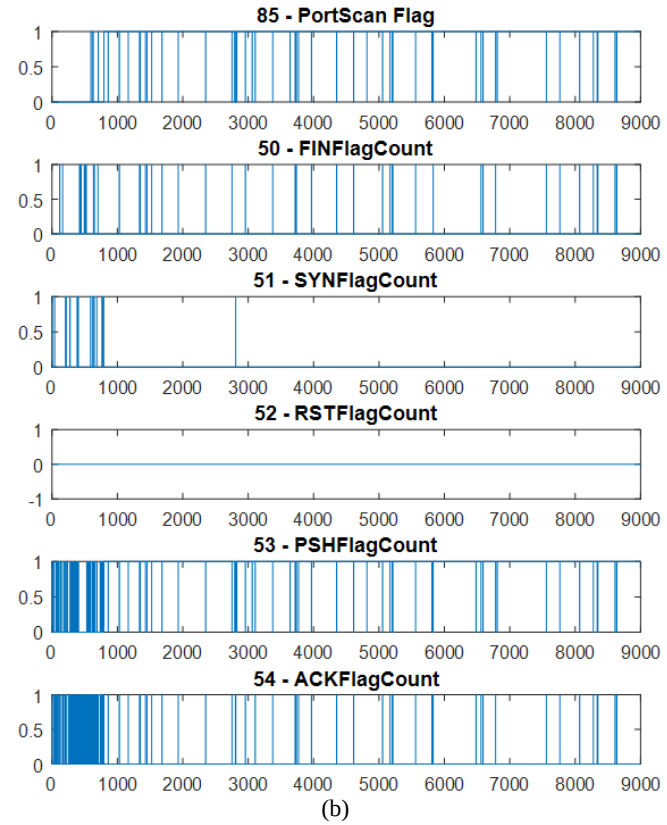
The total dataset size is too large (over 500k samples) for a typical PC, so a part of it, about 5% (25k samples), was finally used to test the ANN tool, due to time and space restrictions.

For each attack type an ANN was trained to classify the data either as attack (1) or benign traffic (0). The Confusion Matrices of both ANNs indicate a satisfactory rate of detection with over 99.7% accuracy, as well as very high precision and sensitivity (above 97%).

The confusion matrices for the DDoS-ANN and the PortScan-ANN are shown in Fig. 3a and 3b respectively. Finally, Fig. 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 MSE is calculated taking into account the difference between the results obtained from the validation test and the expected ANN results. From Fig. 4 it is evident that the ANN performance evolves through epochs. For the DDoS case the MSE reaches a stable value around 0.014 near 100 epochs; for the PortScan case the MSE reaches a stable value around 0.005 near 90 epochs.

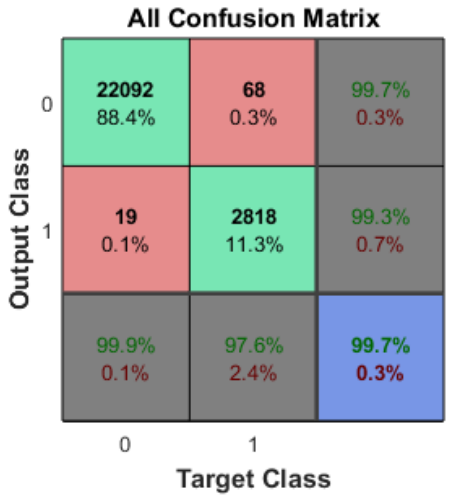


(a)

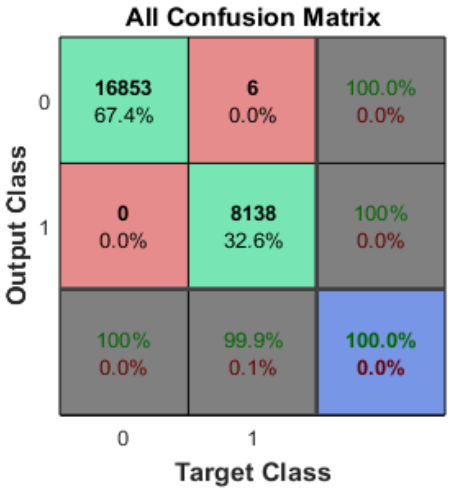


(b)

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

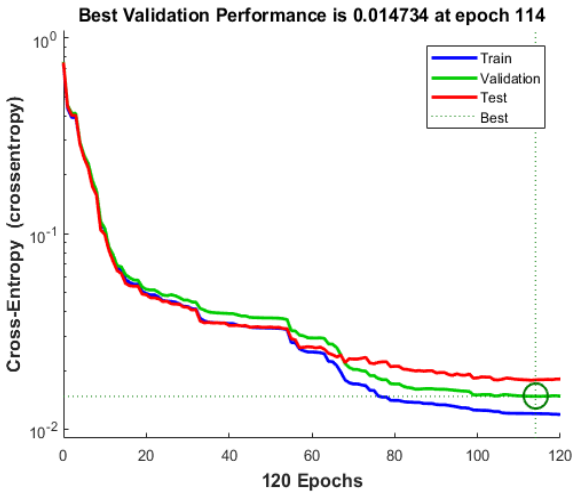


(a)

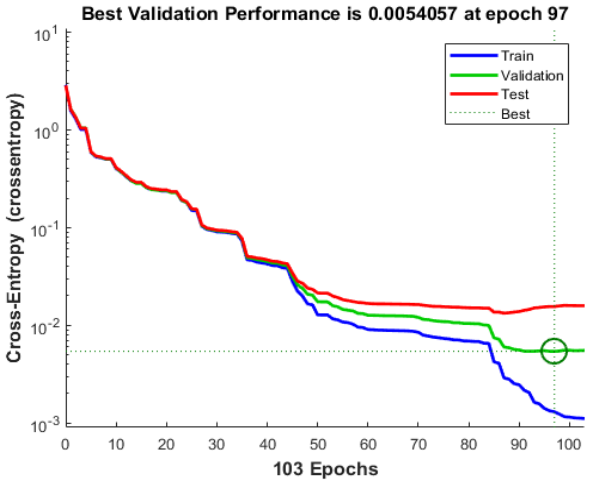


(b)

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



(a)



(b)

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.

C. Results for the single-ANN system

From the same dataset, the DDoS and PortScan datasets used above were merged to form one larger dataset in order to train the single ANN for both attacks (PortScan & DDoS). Again, all available parameters in the datasets were used as inputs to the ANN. The training of the single-ANN system required over 20 sec on average while each one of the simple modules of the proposed system needed 12.5 sec on average on a typical PC.

The Confusion Matrix of the ANN indicates also a satisfactory overall rate of detection of 99.3%, as shown in Fig. 5, and a high precision and sensitivity (above 95%). The MSE versus the amount of ANN training epochs is also low as shown in Fig. 6, and reaches a stable value around 0.01 near 150 epochs.

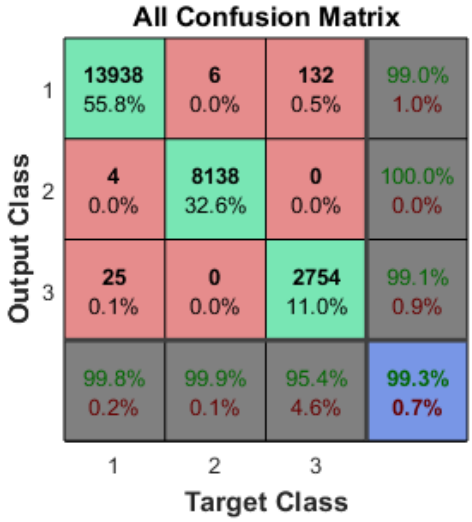


Fig. 5 Confusion Matrix of the single ANN-IDS for Benign (1), PortScan (2), and DDoS (3) attacks.

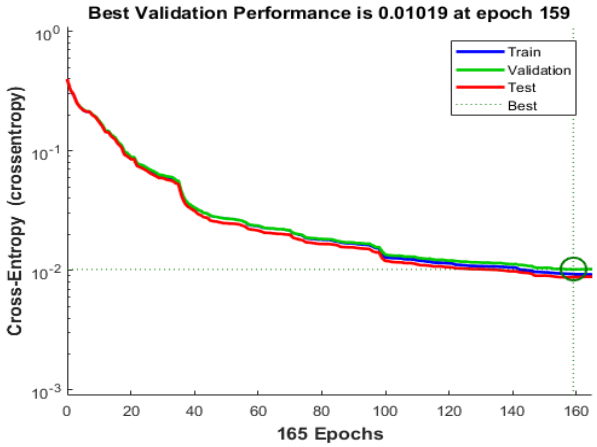


Fig. 6 Mean Squared Error vs the number of Training Epochs for the single ANN-IDS for both DDoS and PortScan attacks, using 20 neurons in the hidden layer.

D. *Tool expansion for Web Attacks*

To demonstrate the flexibility of the proposed system, a third dataset containing Web Attacks is used from the same data source. A sample of the dataset parameters is shown in Fig. 7.

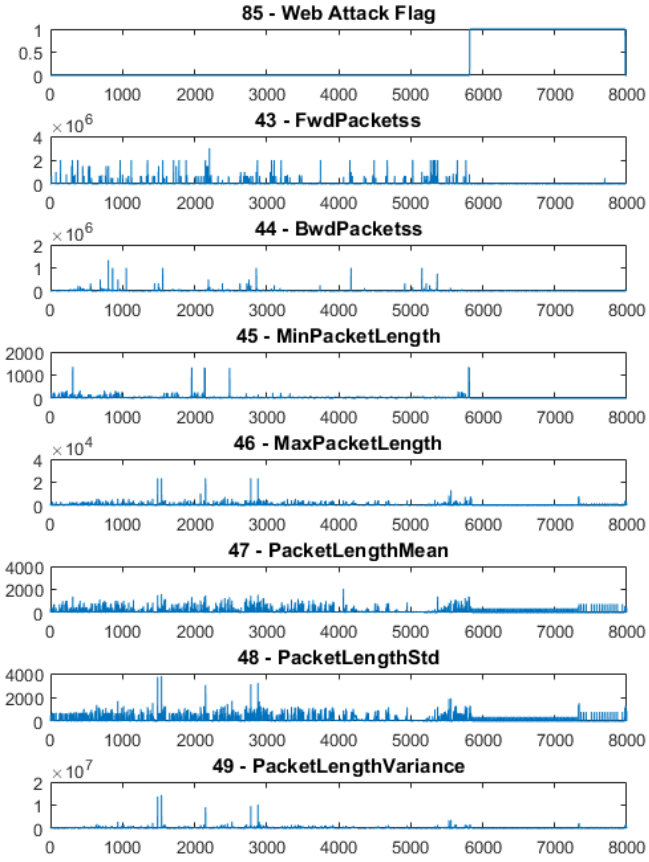
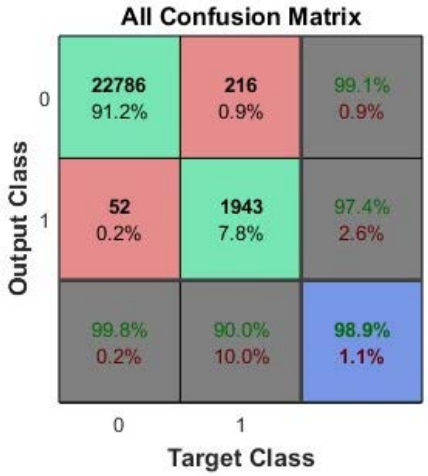
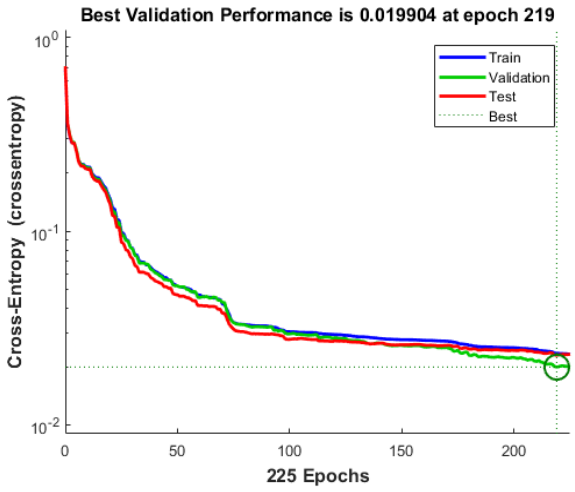


Fig. 7 Sample of the Web Attacks dataset

The proposed multi-ANN system needs only one new module tailored to the specific type of Web Attacks. The module training for the Web Attacks dataset required a few seconds (11 sec on average) with an overall rate of detection of 98.9%, and an MSE value of 0.02 after 200 epochs as shown in Fig. 8.



(a)



(b)

Fig. 8 (a) Confusion Matrix and (b) Mean Squared Error vs the number of Training Epochs of the ANN module for Web Attacks.

The single-ANN, on the other hand, has a more complex structure (Fig. 9a) that needs the recalculation of the entire NN for training, using all the attack types datasets, while the training required 36 sec on average, with an overall rate of detection of 98.5%, and an MSE value of 0.01 after 240 epochs as shown in Fig. 9b and 9c.

V. Conclusions and Further Work

In this paper we have presented an ANN based IDS for detecting Port Scanning, DDoS and Web attacks. Experimental results obtained from the CICIDS2017 dataset show high detection rates, as well as low positive rates.

The proposed system currently consists of multiple identical NN modules programmed with different parameters

each. This modular architecture is easily expandable, facilitating the incorporation of additional modules detecting other types of attacks. The modular architecture enables the modules to work in parallel; hence the response time is limited and the incorporation of additional modules does not slow down the system. The modular architecture is also particularly suitable for FPGA implementation.

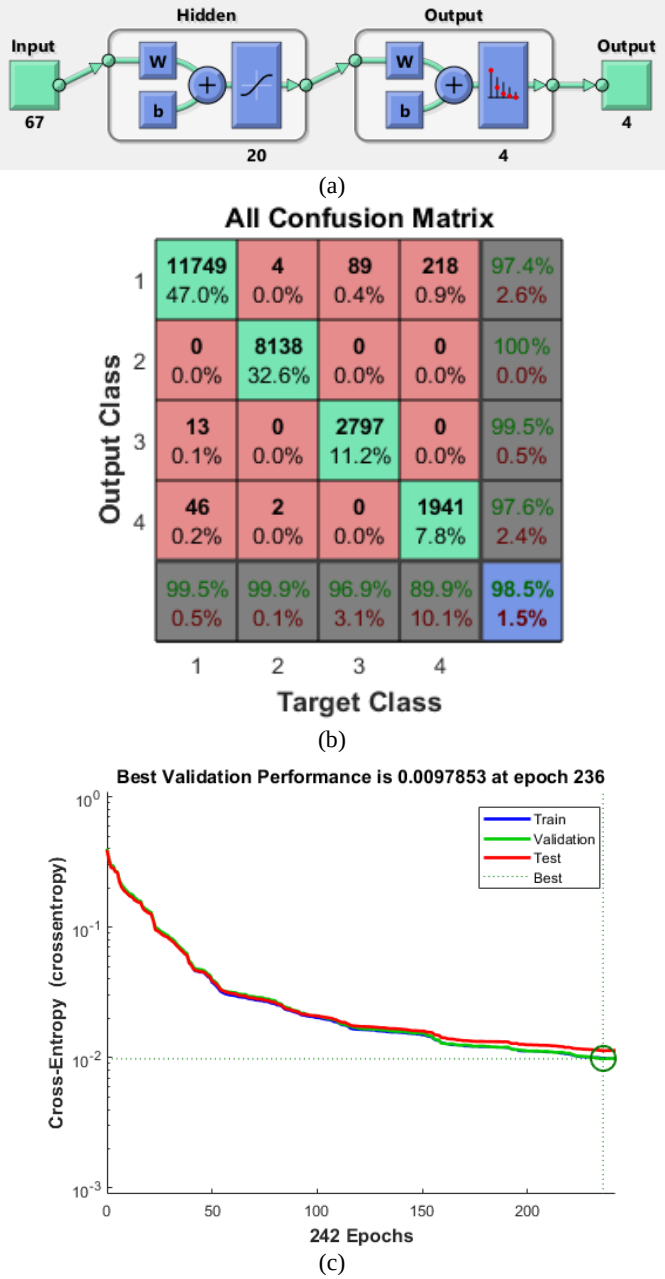


Fig. 9 Mean Squared Error vs the number of Training Epochs for the single ANN-IDS for both DDoS and PortScan attacks, using 20 neurons in the hidden layer.

The comparison to a single-ANN system indicates the general superiority of the proposed multi-ANN system in performance. Each ANN module of the multi-ANN tool performs better than the single-ANN tool. In addition, the single-ANN requires more training time, due to the recalculation of the entire module for each new attack type added, while the proposed multi-ANN system requires only the training of one subsystem each time for the new attack type, thus requiring fewer data and less time to train. Moreover, the increased complexity of the single-ANN to handle more attack types, leads to the reduction of successful detection rate and/or an increase of false positives. Finally, in the proposed multi-ANN system, each module can be updated and optimized independently, without altering the performance of other parts of the tool.

In the near future we plan to expand this project to include more datasets and additional types of attacks in order to make it more practical and useful. Combined attacks are also under investigation, as each attack is shown to correlate to different dataset parameters.

Another area 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] R. Singh, H. Kumar, R. Singla, and R. Ketti, "Internet attacks and intrusion detection system". *Online Information Review*, [Online]. *41(2)*, 2017, pp. 171-184 Available: https://doi.org/10.1108/OIR-12-2015-0394

[2] 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 *Proc. of SecRIoT 2019, 1st International Workshop on Security and Reliability of IoT Systems*. Santorini Island, Greece, May 29-31 (2019).

[3] Technopedia, "Zero day attack", Definitions [Online]. Available: https://www.techopedia.com/definition/29738/zero-day-attack

[4] J. M. Vidal, A. L. S. Orozco, and L. J. G. Villalba, "Quantitative criteria for alert correlation of anomalies-based NIDS", *IEEE Latin Amer. Trans.*, vol. 13, no. 10, 2015, pp. 3461-3466

[5] W. Yassin, N. I. Udzirl, Z. Muda, and Md.N. Sulaiman, "Anomaly based intrusion detection through k-means clustering and naïve Bayes classification", in *Proc. 4th IEEE International Conference On Computing and Informatics (ICOCI)*, Sarawak, Malaysia 2013, pp. 298-303.

[6] A. P. Leros and A. S. Andreatos, "Network traffic analytics for internet service providers - Application in early prediction of DDoS attacks", in: G. Tsihrintzis, D. Sotiropoulos, and L. Jain (eds), *Machine Learning Paradigms.* Intelligent Systems Reference Library, vol. 149, ch. 10, Springer, Cham, 2019, pp. 233-267. Available: https://doi.org/10.1007/978-3-319-94030-4

[7] 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* vol. 6, pp. 48231-48246, Sept. 2018. DOI: 10.1109/ACCESS.2018.2863036.

[8] T. Auld, A. W. Moore and S. F. Gull, "Bayesian neural networks for internet traffic classification", *IEEE Transactions on Neural Networks*, vol. 18, no. 1, pp. 223-239, Jan. 2007.

[9] B. Shah and B. H. Trivedi, "Artificial neural network based intrusion detection system: A survey", *International Journal of Computer Applications (0975 – 8887)*, vol. 39, no. 6, pp. 13-18, Feb. 2012.

[10] N. El Kadhi, K. Hadjar and N. El Zant, "A mobile agents and artificial neural networks for intrusion detection", *Journal of Software*, vol. 7, no. 1, pp. 156-160, Jan. 2012.

[11] C. V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection", *Computers and Security*, vol. 29, no. 1, pp. 124-140, Feb. 2010. DOI: doi:10.1016/j.cose.2009.06.008

[12] A. Shenfield, D. Day, and A. Ayesh, "Intelligent intrusion detection systems using artificial neural networks", *ICT Express*, vol. 4, no. 2, pp. 95–99, May 2018. DOI: https://doi.org/10.1016/j.icte.2018.04.003

[13] M. Amruta and N. Talhar, "Effective Denial of Service attack detection using artificial neural network for wired LAN", in *Proc. 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)* pp. 229-234. DOI: https://doi.org/10.1109/SCOPES.2016.7955826

[14] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set", in *Proc. 2nd IEEE Intl Conf. on Comput. Intell. Secur. Defense Appl. (CISDA'09)*, Ontario, July 2009. Piscataway, NJ, USA: IEEE Press, (2009), pp. 53–58. Available: http://dl.acm.org/citation.cfm?id=1736481.1736489

[15] 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 Explorations Newsletter*, vol. 2, no. 2, pp. 14-18, Dec. 2000.

[16] Mathworks®, Matlab® Neural Network & Deep Learning toolboxes. Available: https://uk.mathworks.com/products

[17] Canadian Institute for Cybersecurity, Intrusion detection evaluation dataset CICIDS2017. Available: https://www.unb.ca/cic/datasets/ids-2017.html