# Artificial Neuron Network Implementation in Detection and Classification of DDoS Traffic

Dragan Peraković, *Member, IEEE,* Marko Periša, Ivan Cvitić and Siniša Husnjak

***Abstract* —Detection of DDoS (Distributed Denial of Service) traffic is of great importance for the availability protection of services and other information and communication resources. The research presented in this paper shows the application of artificial neural networks in the development of detection and classification model for three types of DDoS attacks and legitimate network traffic. Simulation results of developed model showed accuracy of 95.6% in classification of pre-defined classes of traffic.**

***Keywords* — ANN, DDoS, network traffic, network security**

## I. Introduction

Detection of illegitimate DDoS traffic presents a problem in protection of information and communication resources. Constant increase of DDoS attacks (in number and volume) since its first appearance in 2000 is a direct evidence of rising problem, despite the continuous research of the problem field and development of the new detection and protection methods. A large number of different DDoS attack classes resulted in the development of methods that are utilized to specific class of the attack. Except detection of DDoS traffic, their correct classification for applying appropriate methods of protection also represents a problem.

Hypothesis of this research is that with extracted parameters of collected traffic and implementation of artificial neural networks (ANN), it is possible with high accuracy to classify DDoS traffic on a new set of data.

The goal of this research is to develop model of a system based on ANN for detection of DDoS traffic and its classification in order to increase accuracy of detection of certain classes of DDoS traffic and application of appropriate methods of protection.

### *A. Previous research*

The problem of detection and classification of DDoS traffic is still actual since the first DDoS attack in year 2000. Development and increasing application of ANN as an expert systems method in different areas and fields leads to the more frequent use in field of traffic and transport technology and telecommunication industry.

Researches on implementation of ANN for the detection and classification of unwanted DDoS traffic are actual in the last few years. A large number of methodologies that have a goal to reduce negative effects of DDoS attacks in different information and communication environments were analyzed, proposed and evaluated.

The research [1] shows developed model of ANN that can detect known and unknown DDoS attacks in real-time. Detection of the attacks was based on the extraction of relevant parameters (source and destination IP address, packet length, destination port and sequential number of packets, etc.) which can be used to define samples of DDoS and legitimate traffic. Parameter values were used for the training of developed ANN model. The developed model was used to detect attacks based on TCP, UDP and ICMP protocols. The evaluation model has proved 98% accurate detection of DDoS attacks. The lack of this research is the inability to classify the exact type of DDoS attack.

Detection of DDoS attacks based on the analysis of traffic patterns is shown in the research [2]. It is based on the fact that traffic generated on the source of DDoS attacks can be joined to certain patterns. The research identified parameters such as IP address, Time to Live (TLL), used protocol and port numbers. Based on these parameters, two methods are proposed for detecting known traffic parameters by using correlation coefficients. As in the previous research, traffic is classified exclusively as legitimate and illegitimate and that is considered as a lack of the research. The additional lack of the research are sets of data used in research because they have been collected in 1998. Traffic characteristics (protocol representation, the number of devices that generate traffic, the amount of generated traffic, integration of a large number of services over IP networks, such as IPTV, VoIP and other services) have drastically changed because of which used data set is not relevant.

The research [3] proposes a method for detecting DDoS attacks based on Radial Basis Function (RBF) ANN. For

Dragan Peraković is with the Department of information and communication traffic, Faculty of Transport and Traffic Sciences, University of Zagreb, Vukelićeva 4, 10000 Zagreb, Croatia (phone: 385-1-2457915 e-mail: dragan.perakovic@fpz.hr).

Marko Periša, is now with the Department of information and communication traffic, Faculty of Transport and Traffic Sciences, University of Zagreb, Vukelićeva 4, 10000 Zagreb, Croatia (phone: 385-1-2457914 e-mail: marko.perisa@fpz.hr).

Ivan Cvitić, is now with the Department of information and communication traffic, Faculty of Transport and Traffic Sciences, University of Zagreb, Vukelićeva 4, 10000 Zagreb, Croatia (phone: 385-1-2457943 e-mail: ivan.cvitic@fpz.hr).

Siniša Husnjak, is now with the Department of information and communication traffic, Faculty of Transport and Traffic Sciences, University of Zagreb, Vukelićeva 4, 10000 Zagreb, Croatia (phone: 385-1-2457918 e-mail: sinisa.husnjak@fpz.hr).

978-1-5090-4086-5/16/$31.00 ©2016 IEEE

the development of detection method were used parameters such as average packet size, packet sequence umber, time variance of packet arrival, size variance of packet, etc. Simulation has proved the accuracy of the developed detection method for DDoS attack with 96.5% accuracy in one data set and 98.2% accuracy in the second data set. The lack of research is shown in the deficiency of accurate classification of DDoS attack types.

A large number of researches are dealing with the issue of DDoS attack detection using ANN that have the same or approximately the same parameters on the basis of whose value is possible to divide traffic to legitimate and illegitimate. Most frequently, these parameters are packet sequence number, arrival time of the packet, used protocol, destination port, source and destination IP address etc. [4], [5], [6].

### *B. Research methodology and constraints*

For the purpose of this research, data sets were collected from multiple sources. Collected data contains a large number of network traffic collected during the DDoS attack as well as normal network activity. Through the research collected data was sorted out and analyzed the sample of 4986 network packages that allowed identification of parameters for modeling three classes of DDoS traffic (Chargen, DNS and UDP) and normal network traffic. In order to exploit data for classification of DDoS attacks, normalization and classification of data was conducted for the purpose of getting the values of all identified parameters in mutual ratio. The values of identified parameters are structured in a matrix form in which are used as an input in the developed ANN model. Validation of developed model is conducted with computer simulation which proved high accuracy of implementation of this type of expert system in detection and classification of DDoS attack.

Because of the available data sets, conducted research is limited to three above mentioned classes of DDoS traffic.

## II. MODEL DEVELOPMENT FOR DETECTION AND CLASSIFICATION OF DDOS TRAFFIC

Detection system modeling and classification of DDoS traffic consists of several key activities that are presented by UML activity diagram in Fig. 1. First activity of the model development represents collecting data sets that contain records of network traffic. Over the collected data was conducted normalization of parameter values so they can be used in ANN.

The next activity involves the development of the ANN model which involves determining a number of hidden layers, a number of neurons in the hidden layer, a definition of the transfer functions in hidden and output layers. The last activity of development process is analysis of the results.

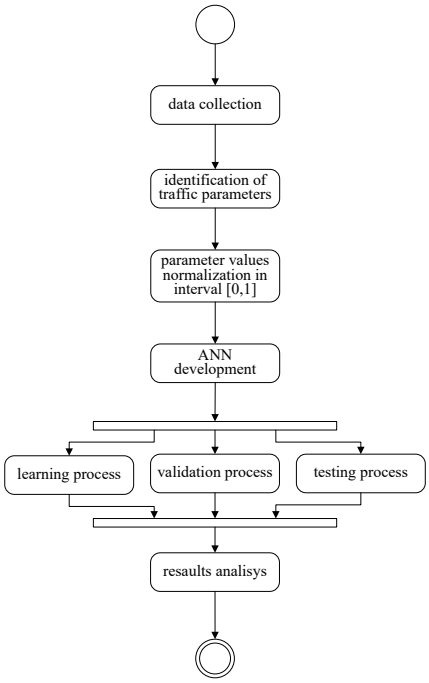


Fig. 1. UML Activity diagram of proposed model development

After development of the ANN comes a division of previously collected and standardized data into subsets for learning, validation and testing of the network so that the validation of developed model can be conducted.

### *A. Data collection and normalization*

Data used in this research were collected through an online sources. Four publicly available datasets were used from which were created unique set of 4986 recordings of network traffic [7], [8], [9]. Each of the used sets of records contained certain classes of traffic:

1. class – DNS DDoS attack (DDoS traffic),
2. class – CharGen DDoS attack (DDoS traffic),
3. class – UDP DDoS attack (DDoS traffic) and
4. class – normal traffic (legitimate traffic).

Traffic classes (legitimate and DDoS) included in this study are defined based on the analysis of collected data sets (secondary data). With the analysis of the observed data sets it was identified that traffic parameters which values are subsequently used as input to an ANN with the aim of detection and classification illegitimate DDoS traffic. Parameters used for classification are packet arrival time, source IP address (Source), destination IP address (Destination), used protocol and packet length. The reason for the application of the selected parameters in the development of models is based on previous studies and the association with displayed parameter set and sequentially appearance of certain values in time.

The initial structure of the collected data is not suitable for input in the ANN because of variety of data types of each parameters (text, integer, real, etc.) as well as the value interval. One of the value interval that is possible to

use as an input in ANN is [0, 1] and this is the reason why it is necessary to standardize the data collected by linear transformation.

$$x_{i,[0,1]} = \frac{x_i - x_{min}}{x_{max} - x_{min}} \quad (1)$$

Where:
$x_i$ – value of data $i$
$x_{min}$ – minimum data value in observed set
$x_{max}$ – maximum data value in observed set
$x_{i,[0,1]}$ – value of data $i$ after normalization in [0, 1] interval

TABLE 1: DATA STRUCTURE AFTER NORMALIZATION

| Network traffic parameters | | | | | Class of traffic | | | |
|---|---|---|---|---|---|---|---|---|
| Time | Source | Destination | Protocol | Length | Chargen | DNS | UDP | NormalAct |
| 0,001073 | 1,000000 | 1,000000 | 1,000000 | 0,109354 | 1 | 0 | 0 | 0 |
| 0,001083 | 1,000000 | 1,000000 | 1,000000 | 0,109354 | 1 | 0 | 0 | 0 |
| 0,001148 | 1,000000 | 1,000000 | 1,000000 | 0,109354 | 1 | 0 | 0 | 0 |
| 0,001174 | 1,000000 | 1,000000 | 1,000000 | 0,109354 | 1 | 0 | 0 | 0 |
| 0,001211 | 1,000000 | 1,000000 | 1,000000 | 0,109354 | 1 | 0 | 0 | 0 |
| 0,021712 | 0,999960 | 1,000000 | 0,083333 | 0,029574 | 0 | 1 | 0 | 0 |
| 0,023703 | 0,999960 | 1,000000 | 0,083333 | 0,029574 | 0 | 1 | 0 | 0 |
| 0,007963 | 0,999841 | 1,000000 | 0,083333 | 0,018569 | 0 | 1 | 0 | 0 |
| 0,008103 | 0,999841 | 1,000000 | 0,083333 | 0,018569 | 0 | 1 | 0 | 0 |
| 0,008949 | 0,999841 | 1,000000 | 0,083333 | 0,018569 | 0 | 1 | 0 | 0 |
| 0,010368 | 0,999777 | 1,000000 | 0,083333 | 0,029574 | 0 | 1 | 0 | 0 |
| 0,022145 | 0,991924 | 1,000000 | 0,083333 | 0,029574 | 0 | 1 | 0 | 0 |
| 0,022224 | 0,991924 | 1,000000 | 0,083333 | 0,029574 | 0 | 1 | 0 | 0 |
| 0,024381 | 0,991924 | 1,000000 | 0,083333 | 0,029574 | 0 | 1 | 0 | 0 |
| 0,000913 | 0,991836 | 1,000000 | 1,000000 | 0,612105 | 1 | 0 | 0 | 0 |
| 0,000954 | 0,991836 | 1,000000 | 1,000000 | 0,612105 | 1 | 0 | 0 | 0 |
| 0,000963 | 0,991836 | 1,000000 | 1,000000 | 0,612105 | 1 | 0 | 0 | 0 |
| 0,001102 | 0,991836 | 1,000000 | 1,000000 | 0,619670 | 1 | 0 | 0 | 0 |
| 0,009471 | 0,984035 | 1,000000 | 0,083333 | 0,029574 | 0 | 1 | 0 | 0 |

Data normalization allows representation of each parameter value in the [0, 1] interval and quantifies values of a qualitative nature. Described normalization was carried out according to (1) and it is showed in table 1.

### B. *Model development*

An ANN is designed in order to detect DDoS traffic and his sub-classification. For the design of the ANN was used Matworks programming tool MatLab v.R201a (9.0.0.341360) that has integrated modules for classification by recognizing patterns by using ANN (Neutral Pattern Recognition – nprtool).

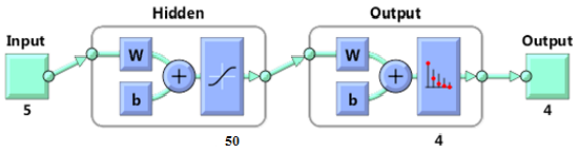


Fig. 2. Architecture of ANN for pattern classification

Fig. 2. shows the architecture of ANN that is used to detect illegitimate DDoS traffic, i.e. its classification in four categories. Presented architecture corresponds to the multilayer perception (MLP), type of ANN that has input signals (Input) presented with the set of input data of one hidden layer, one output layer and output. The input data set represents previously created matrix that contains sample of 4986 instances with values of five defined parameters [5x4986] and matrix [4x4986] which contains the values of 0 or 1, depending on the qualification of a particular class of traffic. The hidden layer has 50 neurons which, compared to other combinations, showed the best output results.

The weight sum net represents input for calculation of the transfer function f(net). The transfer function is sigmoid or logistic function. The advantage of using this type of transfer function is allowed area of uncertainty within given interval that is specified by function contribution.

The result of sigmoid transfer function in the hidden layer represents input to the output layer. Inside the output layer was used sotfmax transfer function. This type of transfer function is commonly used in the output layer of classified ANN because of the characteristics of conversion of input data in the posterior probability (change probabilities of the result under the influence of new information) which ensures defined measure of reliability of the output. The outcome of the output represents one of the four defined traffic classes.

## III. SIMULATION RESULTS ANALYSIS

Simulation of the developed ANN model with different numbers of neurons in the hidden layer (30, 35, 40, 45, 50 and 55) was carried out in this research. Fig. 3. shows the confusion matrix. Confusion matrix shows the accuracy of classification of the submitted data in predefined categories in the process of learning, validation and testing. The best results in the detection of illegitimate traffic and his classification showed AAN with 50 neurons in the hidden layer. Accuracy of classification is 95.6%, i.e. 4.4% of the data was incorrectly classified. The minimum accuracy of classification can be seen in class 4 (UDP attack) and it's 82.1%. The reason for this is matching of parameter values of this type of traffic with the parameter values of normal (legitimate) traffic (class 3).


Fig. 3. Confusion matrix for 30, 35, 40, 45, 50 and 55 neurons in hidden layer respectively

Fig. 4. shows the effects of varying thresholds of normal values on the specificity of the test (Receiver Operating Characteristics) or ROC cure. X-axis shows the specificity, and y-axis shows the sensitivity of observed model which fully reflects the performance of the test.

Performances are better as the area under the ROC curve is closer to the value 1 or when the ROC curve is flattened at the top of the graph (100% of sensitivity and 100% of specificity)

According to the above, performance of classification

that are conducted by developed ANN show satisfactory results due to almost completely flattened curves of the traffic classes 1 and 2.

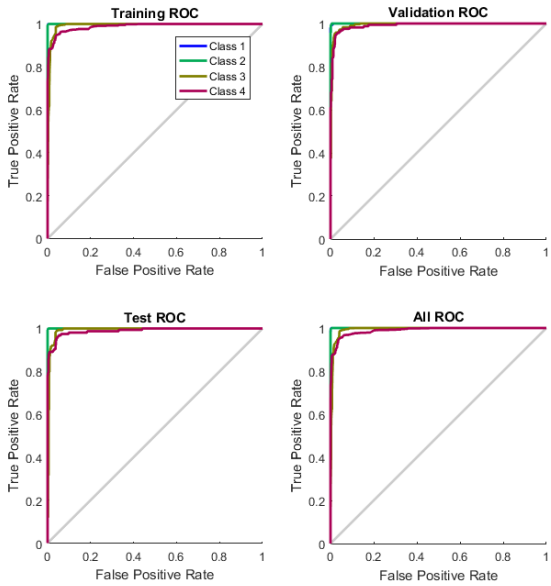


Fig. 4. ROC cure for ANN with 50 neurons in hidden layer

A little less performances, but also satisfactory, are visible to traffic classes 3 and 4 where the correspondence of ROC curve and confusion matrix can be seen.

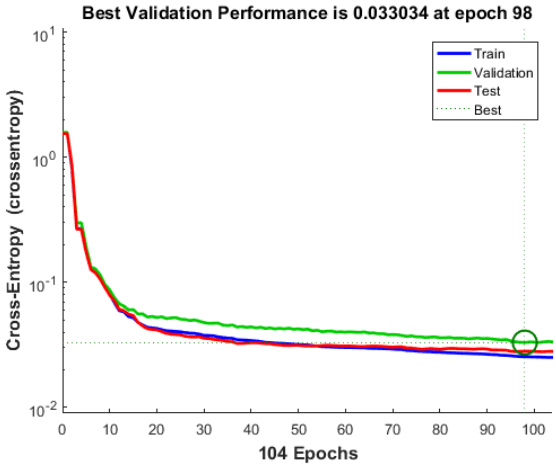


Fig. 5. Cross-entropy error for ANN with 50 neurons in hidden layer

Cross-entropy error is shown in Fig. 5. and represents the error between the results obtained by validation test and the expected results. The aim is to iteratively adjust the weight of the input signals in such a manner to achieve optimum of the transferred function i.e. to minimize the transferred function. From the displayed figure it is visible the minimum of transferred function (local minimum) in 98th iteration where cross entropy error is 0.033034. Iteration that shows minimum of transferred function indicates the iteration after which six consecutive validation tests gave a greater error of cross-entropy.

## IV. Conclusion

This research shows the development of detection and classification model systems of DDoS traffic by using artificial neural networks. The analysis of the results obtained by simulation of the model proved the hypothesis that with the extraction of collected traffic parameters and with the appliance of artificial neuron network can be, with high accuracy of 95.6%, classified DDoS traffic to the new data sets.

Model has shown lower accuracy (82.1%) in the classification of UDP DDoS attacks. The main reason is the correspondence of the values of UDP DDoS attack and legitimate traffic parameters. The problem can be solved by identifying and applying the additional parameters that characterize the UDP DDoS attack which can increase the accuracy of the model.

In future research is planned to improve the identification of the model and the inclusion of additional parameters that represents dependent variables whose dependence can be assigned to defined network packet to one of the defined classes of DDoS traffic. It is planned to define new classes of DDoS traffic that would extend the sensitivity of the model to other DDoS attacks.

## References


[1] A. Saied, R. E. Overill, and T. Radzik, “Artificial Neural Networks in the Detection of Known and Unknown DDoS Attacks: Proof-of-Concept,” Commun. Comput. Inf. Sci., vol. 430, pp. 300–320, 2014.

[2] T. Thapngam, S. Yu, W. Zhou, and S. K. Makki, “Distributed Denial of Service (DDoS) detection by traffic pattern analysis,” Peer-to-Peer Netw. Appl., vol. 7, no. 4, pp. 346–358, 2014.

[3] R. Karimazad and A. Faraahi, “An Anomaly-Based Method for DDoS Attacks Detection using RBF Neural Networks,” in International Conference on Network and Electronics Engineering, 2011, vol. 11, pp. 44–48.

[4] M. Kale, “DDOS Attack Detection Based on an Ensemble of Neural Classifier,” Int. J. Comput. Sci. Netw. Secur., vol. 14, no. 7, pp. 122–129, 2014.

[5] M. Alenezi and M. Reed, “Methodologies for detecting DoS/DDoS attacks against network servers,” in Conference on Systems and Networks, 2012, pp. 92–98.

[6] G. Preetha, B. S. K. Devi, and S. M. Shalinie, “Autonomous agent for DDoS attack detection and defense in an experimental testbed,” Int. J. Fuzzy Syst., vol. 16, no. 4, pp. 520–528, 2014.

[7] CAIDA, “CAIDA: the Cooperative Association for Internet Data Analysis,” 2008. [Online]. Available: Http://www.caida.org/. [Accessed: 01-Jan-2016].

[8] I. S. C. of Excellence, “UNB ISCX Intrusion Detection Evaluation DataSet,” 2010. [Online]. Available: http://www.unb.ca/research/iscx/dataset/iscx-IDS-dataset.html. [Accessed: 01-Jan-2016].

[9] J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, Z. Granville, and A. L. Pras, “Booters - An analysis of DDoS-as-a-Service Attacks,” in IEEE International Symposium on Integrated Network Management, 2015, pp. 243–251.