Model for Detection and Classification of DDoS Traffic Based on Artificial Neural Network

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 for a 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 a model of a system based on ANN for detection of DDoS traffic and its classification in order to increase the 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 of current interest 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.

Research on implementation of ANN for the detection and classification of unwanted DDoS traffic has become topical 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.

Research [1] shows the 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 shortcoming 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 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 (TTL), 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 deficiency of the research. The additional shortcoming of the research are sets of data used in research because they were 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 the used data set is not relevant.

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

Paper received April 26, 2017; revised July 13, 2017; accepted July 24, 2017. Date of publication July 31, 2017. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Zorica Nikolić.

This paper is a revised and expanded version of the paper presented at the 24th Telecommunications Forum TELFOR 2016 [18].

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).

the development of detection method we have used parameters such as average packet size, packet sequence number, time variance of packet arrival, size variance of packet, etc. Simulation has proved the accuracy of the developed detection method for DDoS attack of 96.5% in one data set and 98.2% accuracy in the second data set. The shortcoming 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 it is possible to divide traffic into 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 we analyzed the sample of 4986 network traffic records 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 the 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 and used as an input to the developed ANN model. Validation of developed model is conducted through computer simulation which proved high accuracy of implementation of this type of expert system in the detection and classification of DDoS attack.

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

II. DDoS TRAFFIC CLASSES OF RESEARCH INTEREST

Reliable detection of illegitimate DDoS traffic is a problem in the protection of information resources from these types of attacks. In addition to the problem of differentiating the two basic classes of traffic, legitimate and illegitimate, distinguishing classes of illegitimate DDoS traffic shown in Fig. 1 also represents a problem.

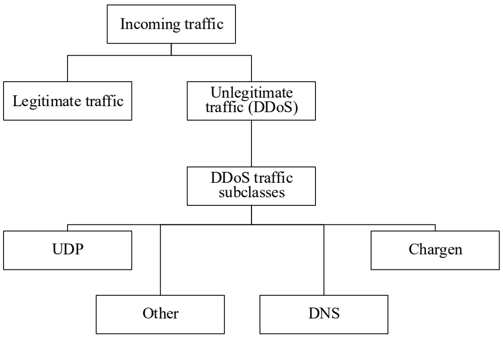


Fig. 1. DDoS traffic subclasses.

If the illegitimate traffic class is successfully detected it is necessary to identify to which subclasses illegitimate traffic belongs, so adequate protection methods can be deployed.

A. Resource overflow using UDP protocol

UDP is a connectionless oriented protocol which means providing transport services without establishing a connection as is the case with the TCP protocol, and thus does not guarantee the delivery nor allows retransmission of undelivered packages. The structure of the UDP header is simpler than the TCP header. It comprises four fields (source and destination communication port, length and checksum). For simplicity and connectionless orientation it is often used in DDoS attacks directed on flooding the network resources [7], [8].

DDoS attack using UDP protocol is usually carried out by sending large amounts of UDP packets with spoofed IP address at random communication ports of the target device. The device that is receiving UDP packets does not have the capacity to handle the incoming traffic capacity while attempting to respond with a large number of ICMP *destination host unreachable* packets that generates additional network congestion [9].

B. Resource overflow using DNS protocol

Resources overflow is simply to carry out through the DNS protocol. The last few years the DNS is one of the leading protocols in amplification of DDoS attacks. The amplification attacks are exploiting the amplification factor of the generated traffic. In addition to standard components of classic DDoS attacks amplifiers are used as an additional layer between the attacker and the attack target.

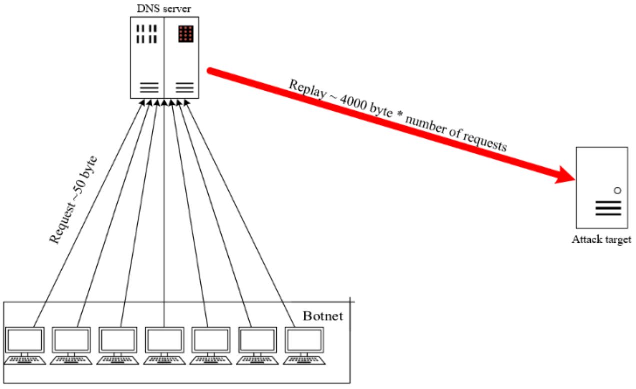


Fig. 2. DNS DDoS attack process.

Amplifiers are devices (servers) outside the botnet networks that provide responses to the inquiry. The process of implementing a DNS DDoS attack is shown in Fig. 2. Botnet agents sending a query are spoofing IP address of the source (attack target address) which results in sending a response from the amplifier to the IP address of the attack target [10]. Fig. 3 shows the statistics of protocol application which allows attack amplification where it can be seen that the DNS protocol is most used for conducting amplification of DDoS attacks.

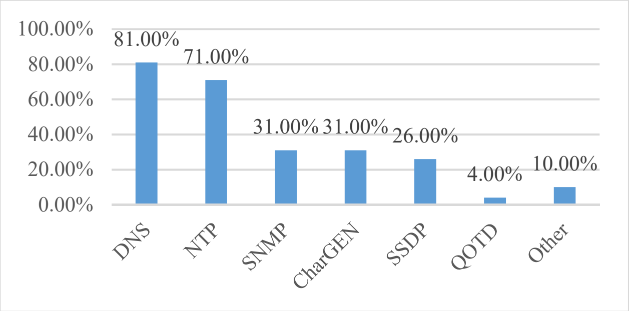


Fig. 3. Protocols used in amplification DDoS attacks.

Attack on Spamhaus Company, one of the largest DDoS attacks with traffic volume of 300 Gbps was carried out using DNS protocol for amplification [12]. Bandwidth amplification factor (BAF) is 28 to 54, and represents a ratio of the UDP length (bytes) sent by the amplifier to attack target and UDP length (byte) sent by the attacker to amplifier.

C. Resource overflow using Chargen protocol

CharGen is a protocol designed for debugging the network, generating content and testing the capacity of the communication link. The protocol generates package contents from 0-512 random characters in response to the request sent to UDP or TCP port 19. The bandwidth amplification factor is 358.8 [13]. If an attacker sends a TCP request to a server that supports CharGen protocol server starts sending random characters in response to a request continuously until the connection is closed. In case of sending UDP queries server responds randomly selected characters each time it receives a UDP datagram [14].

III. 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. 4.

The first activity of the model development represents collecting data sets that contain records of network traffic. The collected data were subject to 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.

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 online sources. Four publicly available datasets were used from which we created a unique dataset of 4986 network traffic records [15], [16], [17]. 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 of 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 model is based on previous studies and the association with displayed parameter set and sequentially appearance of certain values in time.

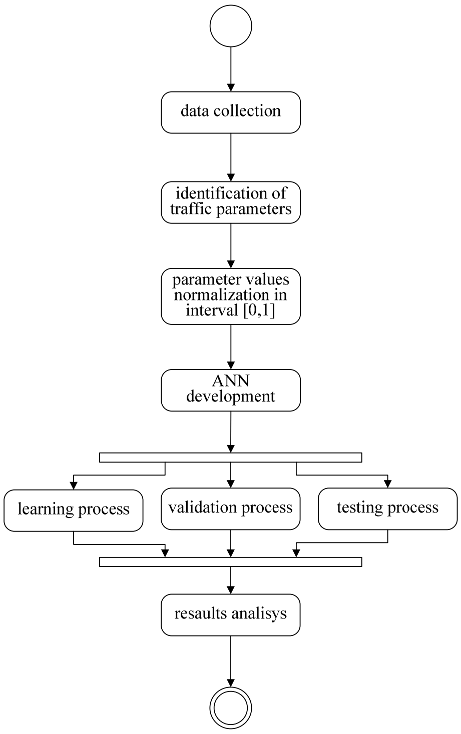


Fig. 4. UML Activity diagram of proposed model development.

Table 1: Initial data structure

Network traffic parameters					Class of traffic			
Time	Source	Destination	Protocol	Length	Chargen	DNS	NormalAct	UDP
0.010089	251.250.184.247	227.213.154.245	UDP	219	1	0	0	0
0.010187	251.250.184.247	227.213.154.245	UDP	219	1	0	0	0
0.010795	251.250.184.247	227.213.154.245	UDP	219	1	0	0	0
0.011035	251.250.184.247	227.213.154.245	UDP	219	1	0	0	0
0.011389	251.250.184.247	227.213.154.245	UDP	219	1	0	0	0
0.014978	113.65.235.209	227.213.154.245	IPv4	1514	0	1	0	0
0.016457	161.89.95.149	227.213.154.245	IPv4	1514	0	1	0	0
0.074867	251.210.182.191	227.213.154.241	DNS	87	0	1	0	0
0.076185	251.210.182.191	227.213.154.241	DNS	87	0	1	0	0
0.084141	251.210.182.191	227.213.154.241	DNS	87	0	1	0	0
0.097482	251.194.221.205	227.213.154.241	DNS	103	0	1	0	0
0.208218	249.221.174.183	227.213.154.241	DNS	103	0	1	0	0
0.208957	249.221.174.183	227.213.154.241	DNS	103	0	1	0	0
0.229240	249.221.174.183	227.213.154.241	DNS	103	0	1	0	0
0.008582	249.199.122.251	227.213.154.245	UDP	950	1	0	0	0
0.008970	249.199.122.251	227.213.154.245	UDP	950	1	0	0	0
0.009058	249.199.122.251	227.213.154.245	UDP	950	1	0	0	0
0.010361	249.199.122.251	227.213.154.245	UDP	961	1	0	0	0
0.089050	247.239.203.145	227.213.154.241	DNS	103	0	1	0	0
0.091093	247.239.203.145	227.213.154.241	DNS	103	0	1	0	0

The initial structure of the collected data, shown in table 1, is not suitable for input in the ANN because of the variety of data types of each parameter (text, integer, real, etc.) as well as the value interval.

One of the value intervals 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

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).

TABLE 2: DATA STRUCTURE AFTER NORMALIZATION

Network traffic parameters					Class of traffic			
Time	Source	Destination	Protocol	Length	Chargen	DNS	NormalAct	UDP
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
0,000913	0,991836	1,000000	1,000000	0,612105	0	1	0	0
0,000954	0,991836	1,000000	1,000000	0,612105	0	1	0	0

Table 2 shows parameters values after data normalization. Additionally, affiliation to a certain class of DDoS traffic and legitimate traffic was assigned to a particular traffic record (1 – belongs to, 0 – does not belong).

B. *Model development*

An ANN is designed in order to detect DDoS traffic and its sub-classification. For the design of the ANN we used Matworks programming tool MatLab v.R2016a (9.0.0.341360) that has integrated modules for classification by recognizing patterns by using ANN (Neutral Pattern Recognition – nprtool).

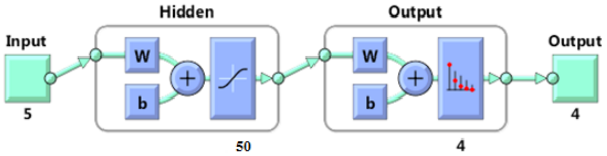


Fig. 5. Architecture of ANN for pattern classification.

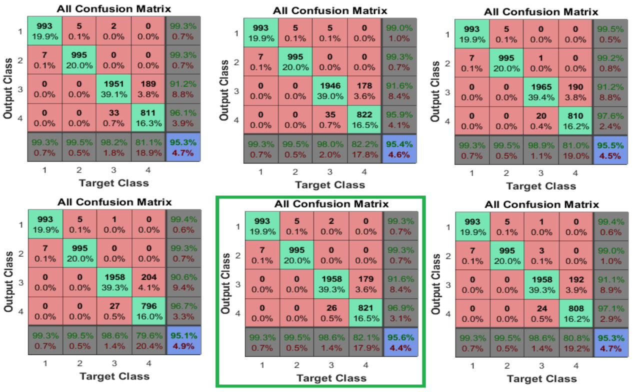
Fig. 5 shows the architecture of ANN that is used to detect illegitimate DDoS traffic, i.e. its classification into four categories. Presented architecture corresponds to the multilayer perception (MLP), type of ANN that has input signals (Input) presented with the set of input data of one hidden layer, one output layer and output. The input data set represents a previously created matrix that contains a 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 the calculation of transfer function f(net). The transfer function is a sigmoid or logistic function. The advantage of using this type of transfer function is the allowed area of uncertainty within a 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, sotfmax transfer function was used. 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 a defined measure of reliability of the output. The outcome of the output represents one of the four defined traffic classes.

IV. 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. 6 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 its classification were shown by 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 is 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).



All Confusion Matrix

Output Class

	1	2	3	4	
1	993 19.9%	5 0.1%	2 0.0%	0 0.0%	99.3% 0.7%
2	7 0.1%	995 20.0%	0 0.0%	0 0.0%	99.3% 0.7%
3	0 0.0%	0 0.0%	1951 39.1%	189 3.8%	91.2% 8.8%
4	0 0.0%	0 0.0%	33 0.7%	811 16.3%	96.1% 3.9%
	99.3% 0.7%	99.5% 0.5%	98.2% 1.8%	81.1% 18.9%	95.3% 4.7%

Target Class

All Confusion Matrix

Output Class

	1	2	3	4	
1	993 19.9%	5 0.1%	5 0.1%	0 0.0%	99.0% 1.0%
2	7 0.1%	995 20.0%	0 0.0%	0 0.0%	99.3% 0.7%
3	0 0.0%	0 0.0%	1946 39.0%	178 3.6%	91.6% 8.4%
4	0 0.0%	0 0.0%	35 0.7%	822 16.5%	95.9% 4.1%
	99.3% 0.7%	99.5% 0.5%	98.0% 2.0%	82.2% 17.8%	95.4% 4.6%

Target Class

All Confusion Matrix

Output Class

	1	2	3	4	
1	993 19.9%	5 0.1%	0 0.0%	0 0.0%	99.5% 0.5%
2	7 0.1%	995 20.0%	1 0.0%	0 0.0%	99.2% 0.8%
3	0 0.0%	0 0.0%	1965 39.4%	190 3.8%	91.2% 8.8%
4	0 0.0%	0 0.0%	20 0.4%	810 16.2%	97.6% 2.4%
	99.3% 0.7%	99.5% 0.5%	98.9% 1.1%	81.0% 19.0%	95.5% 4.5%

Target Class

All Confusion Matrix

Output Class

	1	2	3	4	
1	993 19.9%	5 0.1%	1 0.0%	0 0.0%	99.4% 0.6%
2	7 0.1%	995 20.0%	0 0.0%	0 0.0%	99.3% 0.7%
3	0 0.0%	0 0.0%	1958 39.3%	204 4.1%	90.6% 9.4%
4	0 0.0%	0 0.0%	27 0.5%	796 16.0%	96.7% 3.3%
	99.3% 0.7%	99.5% 0.5%	98.6% 1.4%	79.6% 20.4%	95.1% 4.9%

Target Class

All Confusion Matrix

Output Class

	1	2	3	4	
1	993 19.9%	5 0.1%	2 0.0%	0 0.0%	99.3% 0.7%
2	7 0.1%	995 20.0%	0 0.0%	0 0.0%	99.3% 0.7%
3	0 0.0%	0 0.0%	1958 39.3%	179 3.6%	91.6% 8.4%
4	0 0.0%	0 0.0%	26 0.5%	821 16.5%	96.9% 3.1%
	99.3% 0.7%	99.5% 0.5%	98.6% 1.4%	82.1% 17.9%	95.6% 4.4%

Target Class

All Confusion Matrix

Output Class

	1	2	3	4	
1	993 19.9%	5 0.1%	1 0.0%	0 0.0%	99.4% 0.6%
2	7 0.1%	995 20.0%	3 0.1%	0 0.0%	99.0% 1.0%
3	0 0.0%	0 0.0%	1958 39.3%	192 3.9%	91.1% 8.9%
4	0 0.0%	0 0.0%	24 0.5%	808 16.2%	97.1% 2.9%
	99.3% 0.7%	99.5% 0.5%	98.6% 1.4%	80.8% 19.2%	95.3% 4.7%

Target Class

Fig. 6. Confusion matrix for 30, 35, 40, 45, 50 and 55 neurons in hidden layer, respectively.

Fig. 7 shows the effects of varying thresholds of normal values on the specificity of the test (Receiver Operating Characteristics) or ROC curve. 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 classifications that are conducted by developed ANN show satisfactory results due to almost completely flattened curves of the traffic classes 1 and 2.

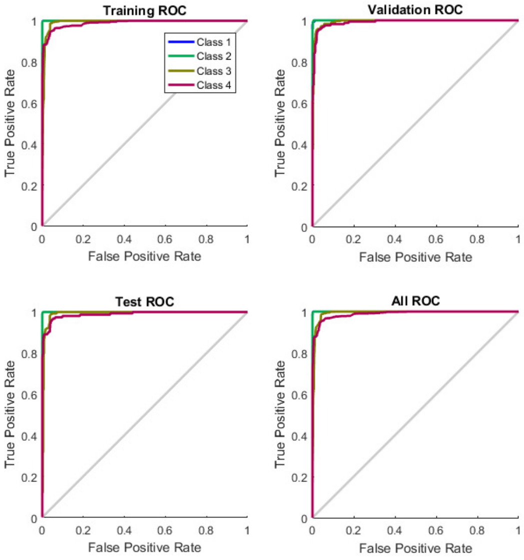


Fig. 7. ROC curve for ANN with 50 neurons in hidden layer.

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

Cross-entropy error is shown in Fig. 8 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 as to achieve optimum of the transfer function i.e. to minimize the transfer function.

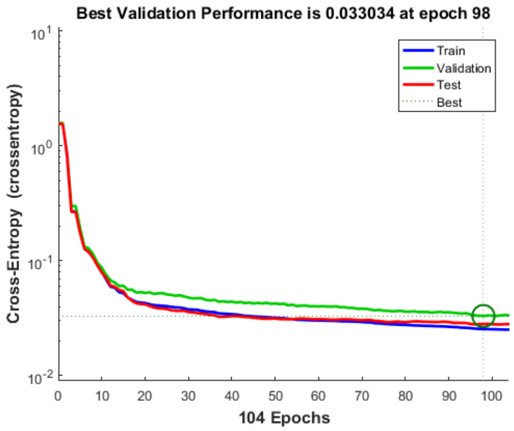


Fig. 8. Cross-entropy error for ANN with 50 neurons in hidden layer.

From the displayed figure we can see the minimum of transfer function (local minimum) in the 98th iteration where cross entropy error is 0.033034. Iteration that shows the minimum of transfer function indicates the iteration after which six consecutive validation tests gave a greater error of cross-entropy.

V. Application Possibilities of Developed Model

The application of the developed model of system for the detection and classification of DDoS traffic based on ANN is possible on the perimeter of local information and communication (IC) infrastructure. An example of implementation is seen in Fig. 9 where the developed system is a module of device located on the perimeter. Examples of such devices are a border router, firewall, intrusion detection and protection system (IDS and IPS) or other device that represents a network node to which incoming traffic is entering from the public communications network. When traffic is entering the network node with the implemented detection and classification system for DDoS traffic, inspection of network packets and extraction values of defined parameters is carried out. Then, the collected values are normalized and classified by the ANN model. If ANN detects legitimate traffic it is then forwarded to the area of local IC infrastructure. Otherwise, the DDoS traffic class is determined and a protection mechanism is activated based on which further incoming traffic is managed.

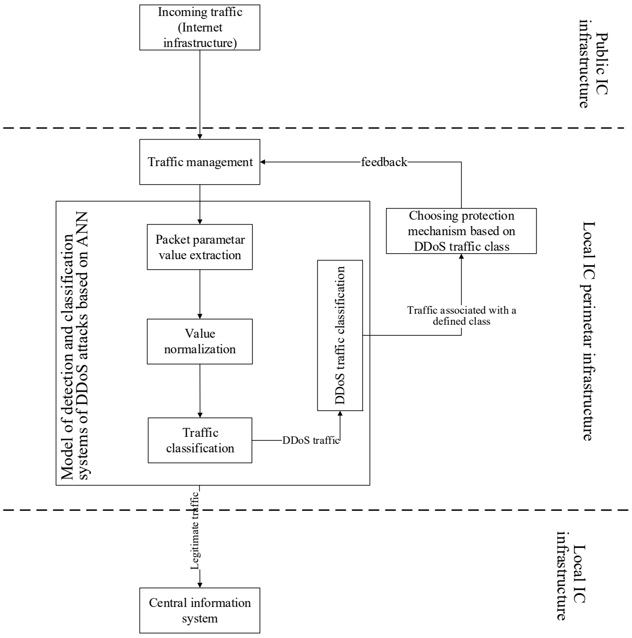

Incoming traffic (Internet infrastructure)
Public IC infrastructure
Traffic management
feedback
Choosing protection mechanism based on DDoS traffic class
Model of detection and classification systems of DDoS attacks based on ANN
Packet parametar value extraction
Value normalization
Traffic classification
DDoS traffic
DDoS traffic classification
Traffic associated with a defined class
Local IC perimetar infrastructure
Legitimate traffic
Central information system
Local IC infrastructure

Fig. 9. Example of developed model implementation.

Current applied solutions are based solely on the detection of legitimate and illegitimate traffic. Detection of illegitimate traffic discards all packets corresponding to defined characteristics. Characteristics of traffic have changed significantly with the development of IC technologies and the emergence of new concepts such as IoT (Internet of Things) and cloud computing. Such changes require a change of approach in the detection of illegitimate DDoS traffic to reduce the number of false positive and false negative results. Therefore it is not enough to classify traffic into two basic classes (legitimate and illegitimate), but it is necessary to identify the exact class of illegitimate traffic and apply a protection mechanisms based on traffic management, not only to its discarding.

The system developed in this way makes decision support which can activate an adequate protection mechanism and thus manage incoming traffic, based on the accurately detected DDoS traffic class.

VI. 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 application of artificial neuron network DDoS traffic can be, with high accuracy of 95.6%, classified 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 it is planned to improve the identification of the model and the inclusion of additional parameters that represent dependent variables whose dependence can be assigned to a 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] I. Bošnjak, “Telecommunication Traffic (Telekomunikacijski promet 2)”. Faculty of transport and Traffic Sciences, Zagreb, 2001.

[8] G. Alexandru, S. Raj, and R. Marc, “Classification of UDP Traffic for DDoS Detection,” in LEET’12 Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats, 2012, pp. 7–7.

[9] R. Kenig, D. Manor, Z. Gadot, and D. Trauner, *DDoS Survival Handbook*. Radware, 2013.

[10] C. Patrikakis, M. Masikos, and O. Zouraraki, “Distributed Denial of Service Attacks,” Internet Protoc. J., vol. 7, no. 4, pp. 13–36, 2004.

[11] M. Abliz, “Internet Denial of Service Attacks and Defense Mechanisms”. Department of Computer Science, University of Pittsburgh, Pittsburgh, 2011.

[12] Nominum, “An Introduction to DNS-Based DDoS Amplification Attacks,” 2012.

[13] S. Institute, “Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis,” 2011.

[14] C. Rossow, “Amplification Hell: Revisiting Network Protocols for DDoS Abuse,” Proc. 2014 Netw. Distrib. Syst. Secur. Symp., no. February, pp. 23–26, 2014.

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

[16] 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].

[17] 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.

[18] D. Peraković, M. Periša, I. Cvitić, and S. Husnjak, “Artificial Neuron Network Implementation in Detection and Classification of DDoS Traffic,” in 24th Telecommunications Forum (TELFOR), 2016, pp. 1–4.