https://www.proconference.org/index.php/usc/article/view/usc25-00-002
DOI: 10.30888/2709-2267.2024-25-00-002

UDC 004.056.53:[004.7:004.032.26]

STUDY OF THE CONFIGURATION OF THE NEUROFUZZY NETWORK TO DETERMINE THE DEGREE OF CONFIDENCE IN THE INPLEMENTATION OF A DOS ATTACK

ДОСЛІДЖЕННЯ КОФІГУРАЦІЇ НЕЙРОНЕЧІТКОЇ МЕРЕЖІ ДЛЯ ВИЗНАЧЕННЯ СТУПЕНЯ ВПЕВНЕНОСТІ ЗДІЙСНЕННЯ DOS АТАКИ

Victoria Pakhomova / Вікторія Пахомова
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0002-0022-099X
Yegor Govorukha / Єгор Говоруха
student / студент
ORCID: 0009-0007-0617-0886
Ukrainian State University of Science and Technology,
Dnipro, Lazaryan, 2, 49010
Український державний університет науки і технологій,
Дніпро, Лазаряна, 2, 49010

Abstract. *As a research method, ANFIS configurations 4-5-12-81-81-1 were used, where 4 is the number of input neurons; 5 – total number of layers; 12 – the number of neurons of the first hidden layer; 81 – the number of neurons of the second hidden layer; 81 – the number of neurons of the third hidden layer; 1 – the number of resultant neurons created using the Fuzzy Logic Toolbox of the MatLAB system, the resulting characteristic is the degree of confidence that the DoS attack occurred at the following terms: low; medium; high. Using the open database of NSL-KDD network traffic parameters, a study of the number of terms of input neurons on the created ANFIS1 (three terms each) and ANFIS2 (two terms each) was carried out with the Gaussian function of neuronal membership on samples of different lengths (100, 200 and 300 examples) using different methods of training optimization (Backpropa and Hybrid). It was determined that the smallest values of errors of the first and second kind were three terms for input neurons on the generated ANFIS1 under the Hybrid method.*

Keywords: *DoS attack, degree of confidence, NSL-KDD, terms, Gaussian function, error of the first kind, error of the second kind.*

Анотація. *У якості методу дослідження використана ANFIS конфігурації 4-5-12-81-81-1, де 4 – кількість вхідних нейронів; 5 – загальна кількість шарів; 12 – кількість нейронів першого прихованого шару; 81 – кількість нейронів другого прихованого шару; 81 – кількість нейронів третього прихованого шару; 1 – кількість результуючих нейронів, що створена за допомогою пакета Fuzzy Logic Toolbox системи MatLAB; за результуючу характеристику взято ступень впевненості, що DoS атака відбулася за наступними термами: низький; середній; високий. З використанням відкритої бази даних параметрів мережевого трафіку NSL-KDD проведено дослідження кількості термів вхідних нейронів на створених ANFIS1 (по три терми) та ANFIS2 (по два терми) при Гаусовської функції приналежності нейронів на вибірках різної довжини (100, 200 та 300 прикладів) за різними методами оптимізації навчання (Backpropa and Hybrid). Визначено, що найменші значення помилок першого та другого роду отримані при використанні трьох термів для вхідних нейронів на створеній ANFIS1 при гібридному методі оптимізації навчання.*

Ключові слова: *DoS атака, ступень впевненості, NSL-KDD, терми, Гаусовська функція, помилка першого роду, помилка другого роду.*

Introduction

Formulation of the problem. Every year, the number of network attacks, including DoS attacks, increases, which in turn requires the organization of research using neural network technologies.

Analysis of the latest research. A review of scientific sources [1-5] showed that the following neural networks can be used to detect DoS attacks: Multi Layer Perceptron (MLP); Kohonen network Self-Organizing Map (SOM); Radial Basis Function network (RBF); Adaptive Network Based Fuzzy Inference System (ANFIS). In [4], a study was conducted on the possibility of using the ANFIS of configuration 4-5-8-16-16-1 (where 4 is the number of input neurons; 5 – total number of layers; 8 – the number of neurons of the first hidden layer; 16 – the number of neurons of the second hidden layer; 16 – the number of neurons of the third hidden layer; 1 – the number of resultant neurons) to determine the degree of confidence in the implementation of a DoS attack. However, it is also necessary to study the use of other network traffic parameters, as well as the configuration on the ANFIS.

The purpose of the article is study of the configuration of the ANFIS to determine the degree of confidence in the implementation of a DoS attack. In accordance with the purpose, the following tasks are set: creation of ANFIS; study of the number of terms of input neurons; determination of errors of the first and second kind on the created ANFIS various configurations.

1. Statement of the problem and mathematical apparatus

The category of DoS (Denial of Service) attacks includes a wide range of methods that are aimed at ensuring that the resource is unavailable to legitimate users. These attacks are used to overload the network or servers, resulting in reduced functionality and availability. The following network attack classes fall into the DoS category: Back; Land; Neptune; Pod; Smurf; Teardrop.

As a mathematical apparatus, the ANFIS system, combining the methods of a neural network and the Takagi-Sugeno fuzzy inference logic system. ANFIS of configuration 4-5-12-81-81-1, where 4 is the number of input neurons; 5 – total number of layers; 12 – the number of neurons of the first hidden layer; 81 – the number of neurons of the second hidden layer; 81 – the number of neurons of the third hidden layer; 1 – the number of resultant neurons is shown in Figure 1.

The input neurons of the first layer are the following parameters: X1 (count) – the number of connections per host in the current session in the last two seconds; X2 (serror_rate) – percentage of connections with a host with SYN errors; X3 (diff_srv_rate) – percentage of connections to different services; X4 (dst_host_diff_srv_rate) – percentage of connections to different services by dst_host_srv_count.

The second layer (inputmf) has 4*3=12 neurons; three terms (MIN – minimum, AVR – average, MAX – maximum values) to each of the neurons.

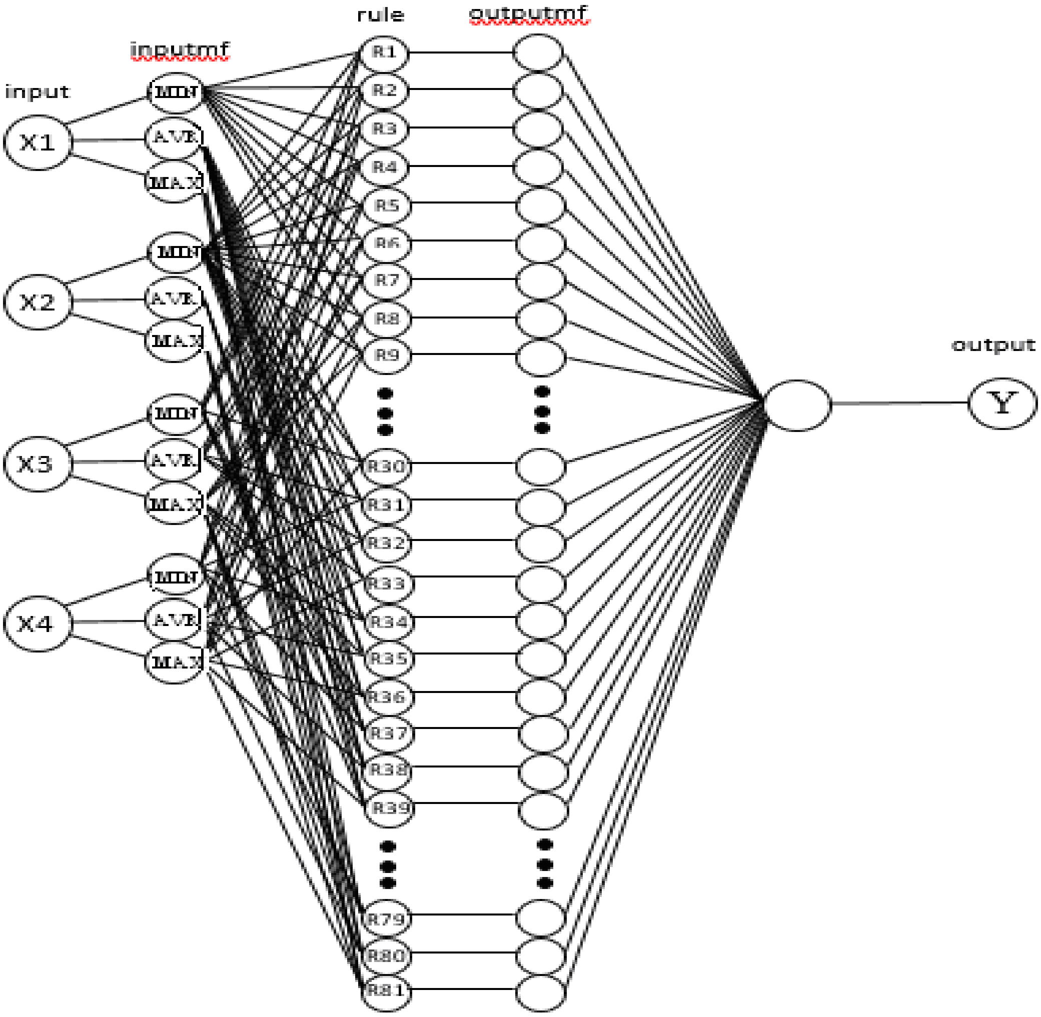


Figure 1 – ANFIS1 configuration 4-5-12-81-81-1

The third layer (rule) has $3^4 = 81$ rules, as an example:

if X1=MIN1 I X2=MIN2 I X3=MIN3 I X4=MIN4, then there is a low degree of confidence in the implementation of a DoS attack;

if X1=AVR1 I X2=MIN2 I X3=MIN3 I X4=MIN4, then there is a low degree of confidence in the implementation of a DoS attack;

if X1=AVR1 I X2=AVR2 I X3=AVR3 I X4=AVR4, then the medium degree of confidence of carrying out a DoS attack;

if X1=AVR1 I X2=AVR2 I X3=AVR3 I X4= MAX4, then the medium degree of confidence of carrying out a DoS attack;

if X1=AVR1 I X2=MAX2 I X3=MAX3 I X4=MAX4, then a high degree of confidence in carrying out a DoS attack; **… ;**

if X1=MAX1 I X2=MAX2 I X3=MAX3 I X4=MAX4, then a high degree of confidence in carrying out a DoS attack.

The fourth layer (outputmf) is function of belonging to each rule, i.e. their 3^4 .

The fifth layer (output) is represented by the resulting neuron Y – the degree of confidence that the attack has taken place. This neuron has three terms: low; medium; high, used to express a level of confidence.

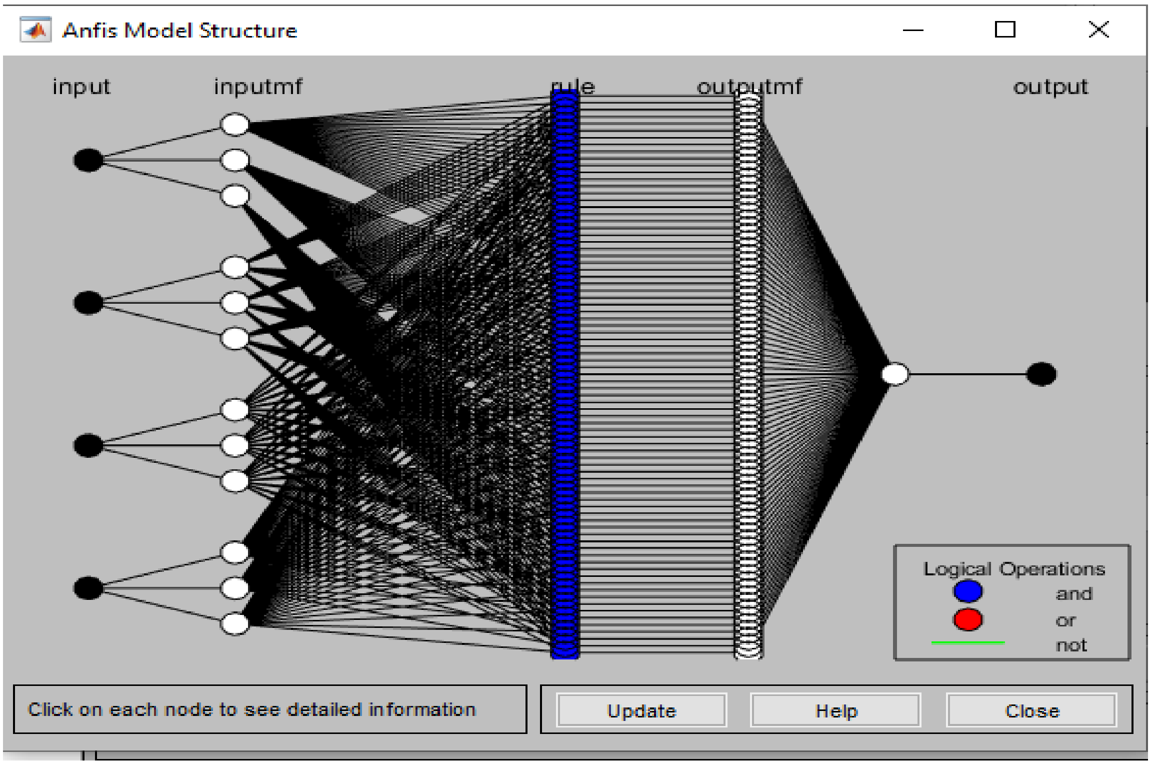
2. Sample preparation

To create samples, an open database NSL-KDD (Network Security Lab-KDD Cup) [3] was used, which contains data on network traffic during its normal activities, as well as during an attack. The training sample consisted of 100 examples: for each network attack class (Back, Land, Neptune, Pod, Smurf, Teardrop), as well as for the normal state (no network attack, Normal).

3. Creation, training and testing the ANFIS1

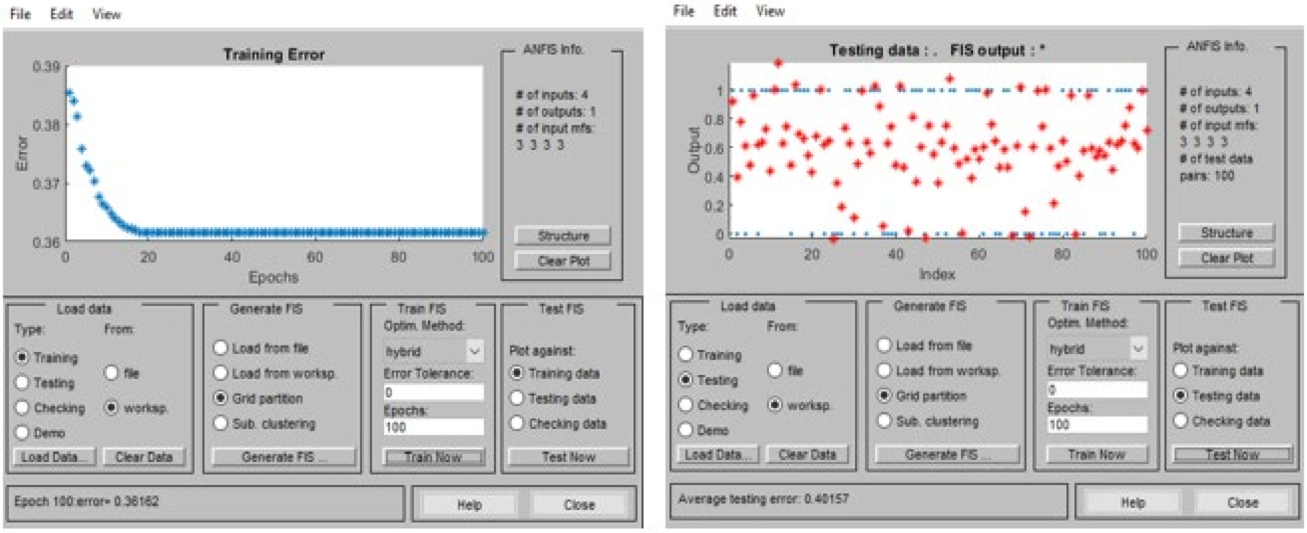
With the help of the Fuzzy Logic Toolbox package, MatLAB created ANFIS1 configuration 4-5-12-81-81-1, which is shown in Figure 2.

The results of ANFIS1 training and testing are presented in Figure 3. As can be seen from the figure, the error of ANFIS1 was 0.36 during training and 0.40 during testing (with the Gaussian function of neuronal belonging; according to the Hybrid method of learning optimization).



Click on each node to see detailed information

Figure 2 – Created by ANFIS1 in the MatLAB system



# of inputs: 4
# of outputs: 1
# of input mfs:
3 3 3 3

Type: ● Training ○ Testing ○ Checking ○ Demo

From: ○ file ● worksp.

○ Load from file ○ Load from worksp. ● Grid partition ○ Sub. clustering

Optim. Method: hybrid

Error Tolerance: 0

Epochs: 100

Plot against: ● Training data ○ Testing data ○ Checking data

Epoch 100 error= 0.36162

# of inputs: 4
# of outputs: 1
# of input mfs:
3 3 3 3
# of test data pairs: 100

Type: ○ Training ● Testing ○ Checking ○ Demo

From: ○ file ● worksp.

○ Load from file ○ Load from worksp. ● Grid partition ○ Sub. clustering

Optim. Method: hybrid

Error Tolerance: 0

Epochs: 100

Plot against: ○ Training data ● Testing data ○ Checking data

Average testing error: 0.40157

Figure 3 – ANFIS1: Training & Testing

4. Study of the number of terms of input neurons

In addition, during the training and testing of ANFIS1 configuration 4-5-12-81-81-1 and ANFIS2 configuration 4-5-8-16-16-1, studies of its error were carried out on samples of different lengths (100, 200 and 300 examples) using various methods of learning optimization: Backpropa (method of Backpropagation of an error based on the ideas of the fastest descent method); Hybrid (that combines the

Backpropagation method of error with the method of least squares). The smallest ANFIS1 error values are achieved when using Hybrid (Table 1), and the sample length should be at least 100 examples.

Table 1 – Error values for ANFIS1 and ANFIS1 (by the Hybrid method)

Number of examples	ANFIS1 4-5-12-81-81-1		ANFIS2 4-5-8-16-16-1	
	Training	Testing	Training	Testing
100	0.36	0.40	0.45	0.56
200	0.39	0.43	0.47	0.57
300	0.41	0.41	0.48	0.56

Authoring

At the end, the studies were carried out simultaneously on the created ANFIS1 and ANFIS2 (with the Gaussian function of neuronal belonging; according to the Hybrid method of learning optimization; a sample of 300 examples); the results obtained are summarized in Table 2 (snippet shown).

Table 2 – The results obtained on the created ANFIS1 and ANFIS2

Network Class	[X1 X2 X3 X4]	Result		Degree of Confidence	
		ANFIS1	ANFIS2	ANFIS1	ANFIS2
Back	[27 0 0.20 0]	0.22	0.56	Low	Medium
Back	[79 0 0 0.03]	0.42	0.57	Medium	Medium
Land	[61 1 0 0]	0.41	0.59	Medium	Medium
Land	[215 1 0.20 0]	0.31	0.48	Low	Medium
Neptune	[38 0 0.60 0.27]	0.02	0.51	Low	Medium
Neptune	[140 0 0.15 0]	0.35	0.57	Medium	Medium
Smurf	[135 1 0 0]	0.51	0.62	Medium	Medium
Smurf	[53 1 0.40 0.72]	0.09	0.43	Low	Medium
Pod	[223 0 0 0]	0.41	0.66	Medium	Medium
Pod	[21 0 0.44 0]	0.04	0.56	Low	Medium
Teardrop	[38 1 0 0.92]	0.75	0.84	High	High
Teardrop	[24 1 0 0.03]	0.33	0.59	Low	Medium
…	…	…	…	…	…

Authoring

The quality parameters of determining the degree of DoS attacks on the created ANFIS1 (three terms for input neurons) and ANFIS2 (two terms for input neurons) were evaluated. On ANFIS1 and ANFIS2, first-kind errors were approximately 17 % and 25 %, respectively, and second- kind errors were approximately 21 % and 22 %, respectively.

Conclusions

To determine the degree of confidence of a DoS attack using the NSL-KDD database, it was created using the Fuzzy Logic Toolbox of the MatLAB system ANFIS1 configuration 4-5-12-81-81-1, the Gaussian function was taken as a function of neuronal affiliation. On the basis of the created ANFIS1 (three terms for input neurons) and ANFIS2 (two terms for input neurons), an error study was carried out on samples of different lengths (100, 200 and 300 examples) using different optimization methods: Backpropa and Hybrid. The smallest values of errors of the first and second kind are achieved at ANFIS1 (with three terms for input neurons).

References

1. Alguliyev R. M., Imamverdiyev Y. N. & Sukhostat L. V. (2018). An improved ensemble approach for DoS attacks detection. *Radioelectronics, informatics, upravlins* [Radio Electronics, Informatics, Control]. No. 2. pp. 73-82. DOI: 10.15588/1607-3274-2018-2-8

2. Karpinski M., Shmatko A., Yevseiev S., Jancarczyk D. & Milevskyi S. (2021). Detection of Intrusion Attacks Using Neural Networks. *Miznar. nauk.-pract. conf. «Information bezpeka tha information technology», Kharkiv-Odessa* [Intl. Scin.-Pract. Conf. Information Security and Information Technologies, Kharkiv-Odesa]. pp. 117-124.

3. NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB. *University of New Brunswick | UNB*. URL: https://www.unb.ca/cic/datasets/nsl.html

4. Pakhomova V. & Kovalov R. (2023). Investigation of the possibility of using neurofuzzy network to determine the extent of DoS attack. *SworldJournal:* Bulgaria. Issue 21. Part 1. pp. 92-98. URL:

https://www.sworldjournal.com/index.php/swj/article/view/swj21-01-037

5. Saied A., Overill R. E. & Radzik T. (2016). Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing*. Vol. 172. pp. 385-393. URL: https://doi.org/10.1016/j.neucom.2015.04.101