https://www.sworldjournal.com/index.php/swj/article/view/swj16-01-036
DOI: 10.30888/2663-5712.2022-16-01-036

УДК 004.056.53:[004.7:004.032.26]

STUDY OF THE POSSIBILITY OF USING THE RBF NETWORK TO DETECT U2R CATEGORY NETWORK ATTACKS

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВИКОРИСТАННЯ RBF МЕРЕЖІ ДЛЯ ВИЗНАЧЕННЯ МЕРЕЖЕВИХ АТАК КАТЕГОРІЇ U2R

Victoria Pakhomova / Вікторія Пахомова
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0002-0022-099X
Victoria Kulyk / Вікторія Кулик
second degree holder / здобувач другого ступеня
Ukrainian State University of Science and Technology, Dnipro, Lazaryan St., 2, 49010
Український державний університет науки і технологій, Дніпро, вул. Лазаряна, 2, 49010

Abstract. *The "RBF U2R" program based on the implementation of the RBF network, the configuration of which is N-M-K (where N is the number of input neurons; M is the number of basic functions; K is the number of resulting neurons) was created in Python for detecting the following classes of attacks: Buffer_overflow; Loadmodule; Perl; Rootkit; Normal and using network traffic parameters from the open KDDCup database. Studies of the accuracy parameter were carried out during the training epochs of the neural network on the created program.*

Keywords: *attack, class, traffic, Gaussian function, training, testing, accuracy.*

Introduction

Formulation of the problem. The creation of an effective network attack detection system requires the use of qualitatively new approaches to information processing, which should be based on adaptive algorithms capable of self-learning. The most promising direction in the creation of similar network attack detection systems is the use of neural network technology.

Analysis of the latest research. At the current stage, there are various methods of detecting network attacks: the method of support vectors; clustering algorithm; genetic algorithms; neural networks. Previously, we have already considered the use of some neural networks (NN): Multi Layer Perceptron (Multi Layer Perceptron, MLP) [5] to detect DoS, U2R, R2L, Probe network attacks. Kohonen network or self-organizing map (Self Organizing Map, SOM) [1]; neural fuzzy network (Adaptive Network Based Fuzzy Inference System, ANFIS) [2]. But there are also other NNs, in particular the radial basis function network (RBF) [6]. In addition, none of the methods provides a complete guarantee of detection of attacks, while different neural networks detect different network classes of attacks in different ways.

The purpose of the article is to investigate the possibility of using the RBF network to identify network attacks of the U2R category.

1. Statement of the problem and mathematical apparatus

The rapid development of computer networks and information technology causes a number of problems related to the security of network resources, which require effective approaches. The use of neural network technology is the most rational, because neural networks have the following advantages: solving problems with unknown patterns; resistance to input data noise; adaptation to changes in the environment; potential ultra-high speed. In this paper, it is necessary to identify

network attack classes of the U2R category. U2R network attacks are system attacks in which a hacker starts a system with a normal user account and tries to abuse vulnerabilities in the system to gain superuser privileges. This type of attack is divided into the following classes: Buffer_overflow, Loadmodule, Perl, Rootkit.

As a mathematical apparatus, the RBF network, the structure of which is shown in Figure 1 [6]. The RBF network by its structure refers to a two-layer network, which uses a hidden layer with a fixed nonlinear transformation of the input vector with constant weighting coefficients.

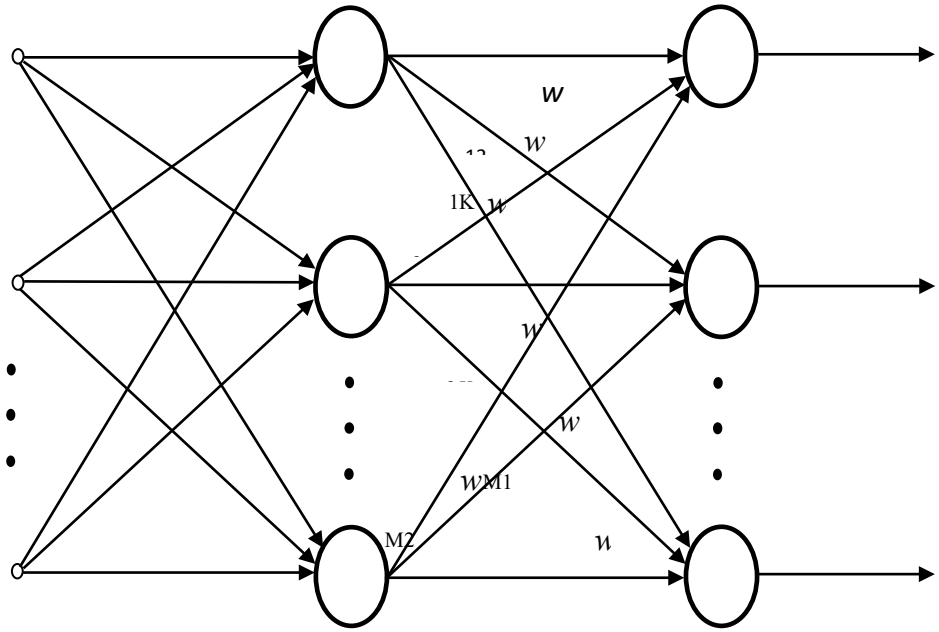

Figure 1 – RBF structure

The specificity of the RBF network is that only the weight coefficients of the linear output layer are adjusted in them, which, in turn, contributes to the rapid learning process of the network. But the problem of the RBF network is the selection of the number of radial basis functions. In [3] it is stated that the number of necessary radial basis functions grows exponentially with the increase in the number of input variables.

Network traffic parameters from the KDDCup database [4] were used as input neurons of NN $x_1 \ldots x_n$ (n=3), in particular: duration – length of the connection (number of seconds); dst_host_count – sum of connections to the same destination IP address; dst_host_srv_count – sum of connections to the same destination port number. As the resulting neurons $y_1 \ldots y_k$ (k=5), where y_1 corresponds to Buffer_overflow; y_2 – Loadmodule; y_3 – Perl; y_4 – Rootkit; y_5 – Normal (there was no attack).

The output of NN is a linear combination of a certain set of basic functions [6]:

$$y_k(x) = \sum_{j=1}^{M} w_{jk} \cdot \Phi_j(x),$$

where w_{jk} – weighting factors; $\Phi_j(x)$ – basis functions defined as:

$$\Phi_j(x) = e^{-\frac{|x-\mu_j|^2}{\sigma_j^2}},$$

where μ_j – coordinate of the center of the jth RBF function; σ_j – the radius of the jth RBF function.

2. Training and testing the neural network

To identify network attacks of the U2R category using the Python language, the program "RBF_U2R" was created, which is based on the RBF network. State-of-the-art libraries were used, thanks to which training of the RBF network is carried out quickly based on Tensorflow and Keras.

A sample of 83 examples is provided for RBF training: Normal – 56; Buffer_overflow – 10; Rootkit – 9; Loadmodule – 5; Perl – 3. In Figure 2 we can see the process of training NN. As shown, we have chosen 5000 epochs for training. We can also see the accuracy of NN on each step (epoch) of training. The average accuracy during the beginning of training is 27.27 %.

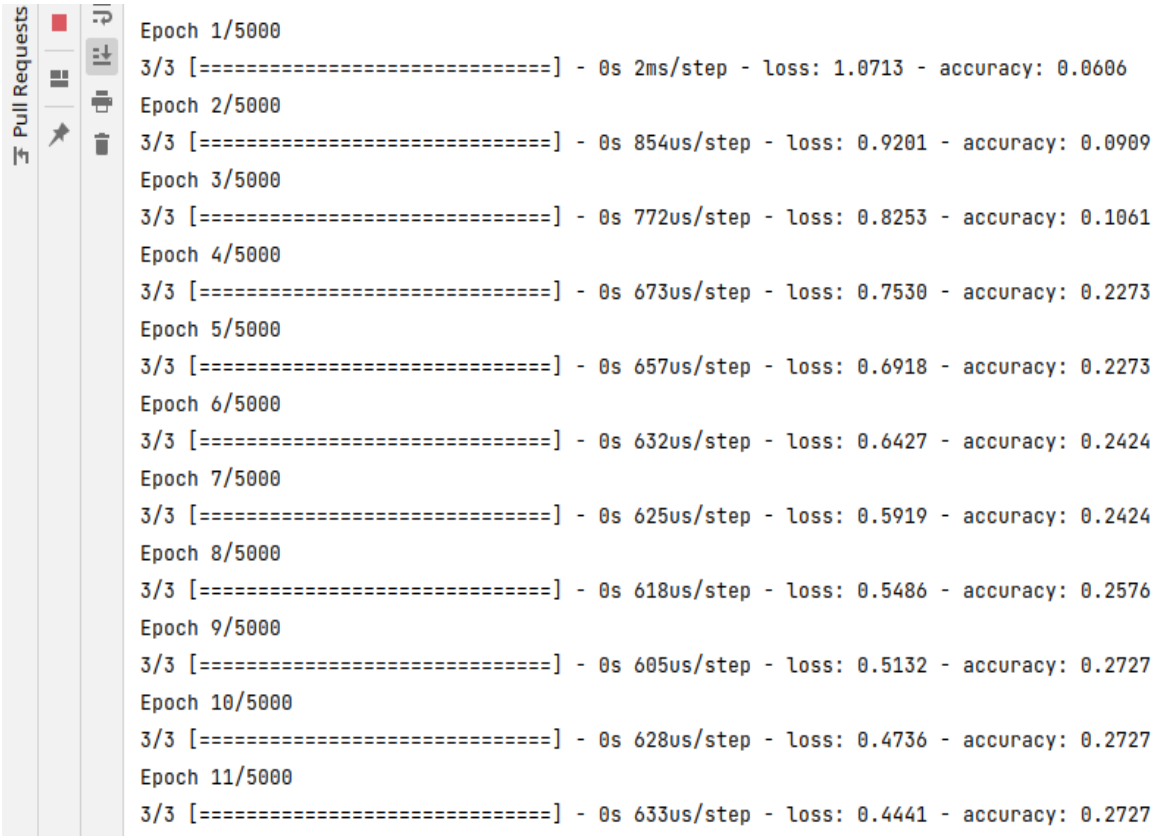

Figure 2 – Training of NN: at the beginning

In Figure 3 we see the improvement of accuracy of NN. In the ending epochs the average accuracy is 87.88 %.

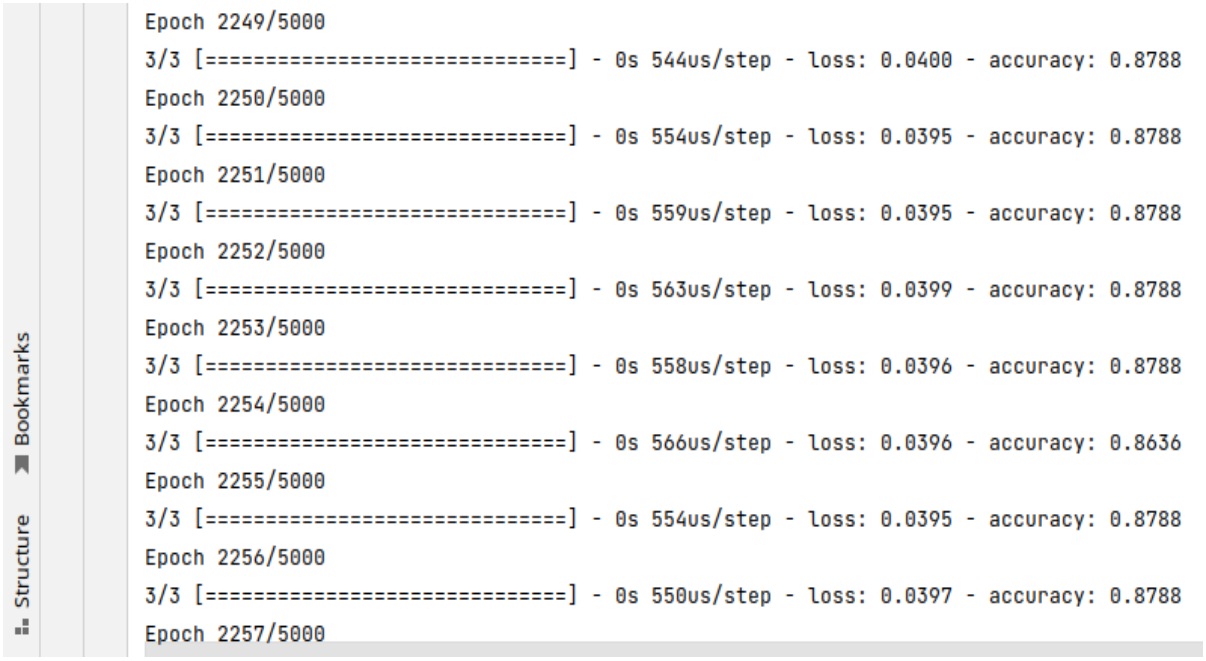

Figure 3 – Training of NN: at the end

In Figure 4 we can see the results of training. The average accuracy during training is 87.88 %, the average accuracy during testing of NN is 76.47 %.

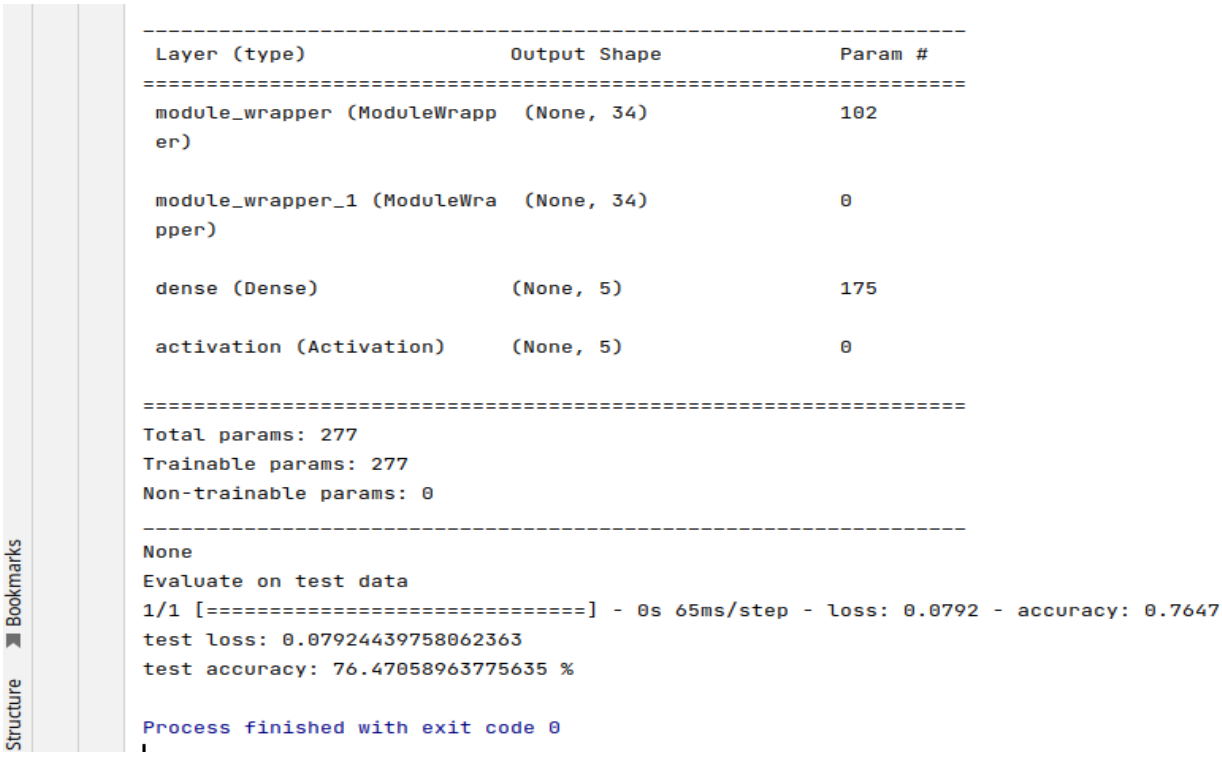

Figure 4 – Testing of NN

3. Research

The created program "RBF_U2R" was used to study the accuracy parameter of the neural network during training for 5000 epochs (Figure 5).

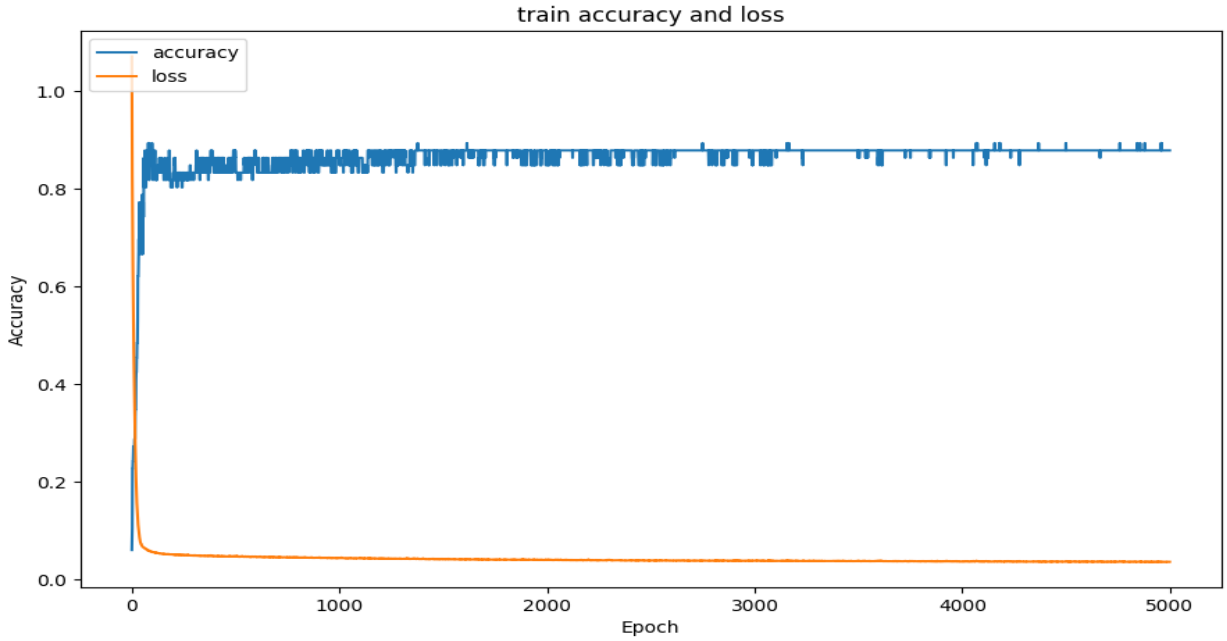

Figure 5 – Accuracy_Loss diagram during training of NN

Conclusions

To identify network attacks of the U2R category by means of the RBF network, the "RBF_U2R" program was created in Python using the KDDCup database. The average accuracy during training is 87.88 %, the average accuracy during testing of NN is 76.47 %. In addition, a study of the accuracy parameter by epochs of RBF network training based on the use of the created program was carried out.

Literature:

1. Пахомова В. М., Павленко І. І. Дослідження параметрів якості визначення мережевих атак категорії PROBE з використанням самоорганізуючої карти. SworldJournal. 2022. Issue 11. Part 1. pp. 100-104. DOI: 10.30888/2663-5712.2022-11-01-022.

2. Пахомова В. М., Маслак А. В. Визначення атак категорії Probe з використанням бази даних KDDCup99 та нейронечіткої технології. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. Том 33 (72). № 5. 2022. С. 135-140.

3. Bajer D., Zorić B., Martinović G. Automatic design of radial basis function networks through enhanced different evolution. Hybrid artificial intelligent systems: Springer. 2015. pp. 244-256.

4. KDDCup1999Data.URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

5. Pakhomova V. M., Bikovska D. G. Investigation of multilayer neural network parameters for determination of R2L category network attacks. Modern engineering and innovative technologies. Germany, Karlsruhe: Sergeieva&Co, «ISE&E». 2021. No 18-02. pp. 39-43. DOI: 10.30890/2567-5273.2021-18-02-059.

6. Wu Y., Wang H., Zhang B., Du K.-L. Using radial basis function networks for function approximation and classification. ISRN Applied Mathematics. Vol. 2012. pp. 1-34. DOI:10.5402/2012/324194.

Анотація. *Створена в Python програма «RBF U2R» на основі реалізації мережі RBF, конфігурація якої N-M-K (де N – кількість вхідних нейронів; M – кількість базисних функцій; K – кількість результуючих нейронів) для виявлення наступних мережних класів атак: Buffer overflow; Loadmodule; Perl; Rootkit; Normal та з використанням параметрів мережного трафіку із відкритої бази KDDCup. Проведено дослідження параметру Accuracy за епохами навчання нейронної мережі на створеній програмі.*

Ключові слова: *атака, клас, трафік, функція Гауса, навчання, тестування, точність.*