Feed forward network with ST neurons for distinguishing normal traffic from icmp-echo attack

P. STOYNOV, N. MASTORAKIS,
Technical university of Sofia, Clement Ohridski 8, Sofia, 1000, BULGARIA

Abstract: —In this article we apply ST-based (Switch-Time-based) neurons in neural networks and check efficiency of these networks for distinguishing normal traffic from icmp-echo attack in computer networks.

Keywords:—ST activation function, DST01 neurons, DST01LU neurons, normal traffic, icmp-echo attack

Received: March 13, 2024. Revised: November 6, 2024. Accepted: December 10, 2024. Published: January 29, 2025.

1. Introduction

IN this article we apply ST-based neurons in neural networks and check efficiency of these networks for investigation of network traffic based on indicator variables. The article is further development of the research in [8], [9], [10], [4], [5] and [6].

A random variable ξ with a switch-time distribution ST(n,ß) has a density

$$f_{\xi}(x) = \begin{cases} C(n,\beta)e^{-\beta x}(1+x)^n, \; x \geq 0 \\ 0, x < 0, \end{cases}. \tag{1}$$

where $C(n,\beta)$ are normalization coefficients for which

$$C(n,\beta) = \frac{1}{I(n,\beta)} \tag{2}$$

and

$$I(n,\beta) = \frac{1}{\Gamma(1)}\int_0^{\infty} e^{-\beta t}(1+t)^n\,dt = \int_0^{\infty} e^{-\beta t}(1+t)^n\,dt \tag{3}$$

Using the ST distribution thus represented, an ST activation function with a threshold of zero can be introduced where

$$N_{kt} = \begin{cases} \int_0^{n_{kt}} C(n,b)e^{-bt}(1+t)^n\,dt, \; n_{kt} \geq 0, \\ 0, \; n_{kt} < 0. \end{cases} \tag{4}$$

This function depends on two parameters - parameter n and parameter b. Standard ST activation functions can be obtained by certain selection of these two parameters.

The double ST distribution (DST distribution) has the density function

$$s_{\xi}(x) = \begin{cases} \frac{1}{2}C(n,b)e^{-bx}(1+x)^n, \; x \geq 0, \\ \frac{1}{2}C(n,b)e^{bx}(1-x)^n, \; x < 0. \end{cases} \tag{5}$$

This distribution permits to define non-threshold ST activation functions. The general appearance of the non-threshold ST activation function is:

$$N_{kt} = \int_{-\infty}^{n_{kt}} s(x)\,dx = \\ = \begin{cases} \frac{1}{2} + \frac{1}{2}\int_0^{n_{kt}} C(n,b)e^{-bx}(1+x)^n\,dx, \; n_{kt} \geq 0, \\ \frac{1}{2}\int_{-\infty}^{n_{kt}} C(n,b)e^{bx}(1-x)^n\,dx, \; n_{kt} < 0. \end{cases} \tag{6}$$

The neurons using ST and DST activation function we call ST and DST neurons correspondingly. The neurons using activation functions combining ST and DST with other activation function we call ST-based neurons.

In some of the types of ST neurons, the speed of convergence of the activation function is lower, and therefore a larger number of iterations is needed when training the neural networks.

Therefore, when a higher convergence rate is sought, ST neurons are more useful in combination with neurons with other activation functions, such that ST neurons can be used in the output layers of the network, while the hidden layers can use, for example, a hyperbolic tangent as activation function.

Another possibility is to combine an activation function of type ST with popular types of activation functions such as RELU. Thus, the activation function of a DST01LU neuron is set by the equality

$$N_{kt} = \begin{cases} n_{kt}, \; n_{kt} \geq 0, \\ \frac{1}{2}\int_{-\infty}^{n_{kt}} e^x\,dx - \frac{1}{2} = \frac{1}{2}e^{n_{kt}} - \frac{1}{2}, n_{kt} < 0. \end{cases} \tag{7}$$

DST01LU neurons and similar to them are interesting alternatives of the standard conventional neurons used today in neural networks.

2. The data set

The data set used in this article is from [1]. The authors provide a realistic data with 4998 records for anomaly detection. The data is based on SNMP variables collected from network devices in a real network under test. The variables are grouped into five categories: Interface, IP, ICMP, TCP, UDP.

This data set is described in details in [5].

Here, we use the input SNMP [7] variable ipInReceivesDif to distinguish normal traffic from an icmp-echo attack using a neural network with different types of activation functions.

The icmp-echo attack is related to the Internet Control Message Protocol – ICMP [2]. This protocol is described in RFC 792 as an Internet standard. Defines different types of packets used to log problems in the Internet Protocol - IP [3].

Among the messages within ICMP are ICMP Redirect, ICMP Destination Unreachable, ICMP Time Exceeded, ICMP Echo Request, ICMP Echo Reply. The last two messages are a stimulus-response pair that is actually a ping. The ping mechanism involves two steps:

1. The client server prepares and sends an ICMP Echo Request to the accessed computer.
2. The accessed computer, upon receiving the ICMP Echo Request message, prepares and sends an ICMP Echo Reply packet to the client computer.

ICMP packets are typically 56 bits long and are supplemented with ICMP and IP packets up to 64 bits long. Accessed computers and routers can impose a limit on incoming ICMP Echo Request packets, which they accept or drop, respectively, as a precaution. Like TCP and UDP, the ICMP protocol is encapsulated in IP. Unlike them, however, it is a network layer protocol, not a transport layer protocol.

3. The model

In order to compare the performance of the proposed ST neurons compared to that of conventional neurons, it is considered how the input variable ipInReceives helps to distinguish normal traffic from an icmp-echo attack using a neural network with different types of activation functions.

Since the ipInReceives is registered cumulatively, the quantity ipInReceivesDif are formed as the differences of two consecutive values for ifOutOctets.

Differentiating normal traffic from an icmp-echo attack is based on the functional model presented in Fig. 1.

Experiment scenario includes the following steps:

1. Define SNMP variable which will be used as an input – total number of output octets (ipInReceives).

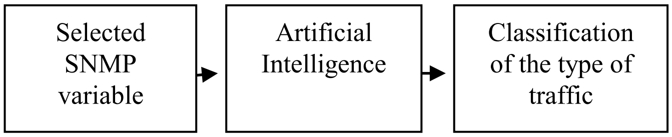

Fig.1. Classification of the type of traffic with using of selected SNMP variable and AI.

2. Define traffic categories which will be distinguished – normal and Brute Force attack.
3. Selecting the type of the neural network and simulations with it.
4. Analysis of results.

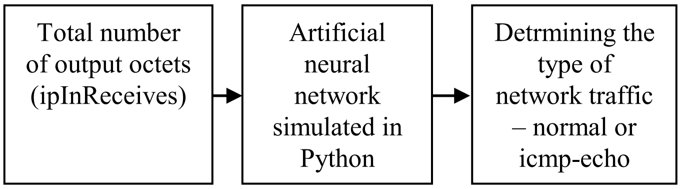
Total number of output octets (ipInReceives)
Artificial neural network simulated in Python
Detrmining the type of network traffic – normal or icmp-echo

Fig. 2. Scheme of experimental set-up for distinguishing normal traffic from icmp-echo attack attack using SNMP variable ipInReceives and artificial neural network of type Feed Forward. Source: the authors.

The experimental set-up is presented on Fig. 2. The neural network is simulated with the Python language.

4. The experiments

The values of the ipInReceivesDif variable are used as input to the neural network. The output represents the type of traffic, with normal traffic coded as 0 and icmp-echo attack coded as 1. The input variable is pre-normalized.

The input and output are split into a training set and a test set. The neural network is trained using the training set of inputs and tested for its ability to predict 100 outputs from the test set.

Three experiments are conducted with different types of neural networks:

1. Neural network with hyperbolic tangent neurons for activation functions.
2. Neural network with DST01LU neurons.
3. Neural network with neurons with hyperbolic tangent activation function in the hidden layer and with DST01LU neurons in the output layer.

The neural network is simulated with Python code. Training is performed with 1000 iterations.

The values that are output are between zero and one. They are modified such that those less than or equal to 0.5 are treated as zeros and those greater than 0.5 as ones.

Table 1 presents the percentages of correctly classified data in each of the three cases.

The data in Table 1 show that networks with a hyperbolic tangent activation function in the hidden layer and with DS01LU neurons at the output show similar performance in predicting the test data to those with conventional hyperbolic tangent neurons as the activation function.

TABLE I
PERCENTAGE OF CORRECTLY CLASSIFIED TRAFFIC IN THE THREE CASES OF THE TYPE OF NEURONS USED TO DISTINGUISH A NORMAL SCHEDULE FROM A ICMP-ECHO ATTACK. SOURCE: THE AUTHORS

Network type	Percentage of test records correctly classified
Neural network with Hyperbolic tangent for activation function	96%
Network with DST01LU neurons	49%

Hyperbolic tangent neural network for activation function in the hidden layer and DST01LU neurons in the output layer	91%

The main conclusion that can be drawn from this experiment is that a network with hyperbolic tangent activation function neurons in the hidden layer and DST01LU neurons in the outer layer correctly classifies the traffic type 91% of the time, which is comparable to the correct rate of a neural network where all neurons are hyperbolic activation function tangent.

5. Conclusion

The general conclusion that can be drawn from the experiments conducted in this article is that neural networks which use ST-based neurons can be applied with similar efficiency to distinguish normal network from icmp-echo attack.

Further research can be provided to distinguish other specific types of intrusion against normal network traffic using neural networks with ST-based neurons.

References

[1] Al-Kasassbeh, Al-Naymat, Al-Hawari, “Using machine learning methods for detecting network anomalies within SNMP-MIB”, in International Journal of Wireless and Mobile Computing, vol. 15, No. 1, 2018.

[2] ICMP (1981) Internet Control Message Protocol –ICMP. Protocol Specification. RFC 792. https://www.rfc-editor.org/rfc/rfc792. Last seen: 17.03.2023.

[3] IP (1981) Internet Protocol. RFC 791. https://www.rfc-editor.org/rfc/rfc791. last seen: 17.03.2023.

[4] N. Mastorakis and P. Stoynov, “Feed forward network with ST neurons implementing XOR function”,in *8th International Conference on Mathematical Modelling, Computational Techniques and Simulation for Engineerin,* 2024. Accepted for printing.

[5] N. Mastorakis and P. Stoynov, “Feed forward network with ST neurons for investigation of network traffic”, in *AIP Conference Proceedings. International Conference on Applied Physics, Simulation and Computing (APSAC), 20-22 June, 2024, Rome, Italy*. 2024. Accepted for printing.

[6] N. Mastorakis and P. Stoynov, “Feed forward network with ST neurons for distinguishing normal traffic from Brute Force attack”,in *Proceedings of 13th International Conference on Modern Circuits and System Technologies (MOCAST) , 26-28 June, 2024, Sofia, Bulgaria*. 2024. Accepted for printing.

[7] SNMP, Simple Network Management Protocol https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol last seen: 17.03.2023.

[8] P. Stoynov, (2016) “Switch Time Family of distributions and processes and their applications to reflected surplus models”, in *Annual of the Faculty of Economics and Business Administration, Sofia University “St. Kliment Ohridski” - Sofia*, 2016, pp. 255-285.

[9] P. Stoynov, “Applications of ST Distributions to Neural Networks and Regression Models”, in *Proceedings of Eighth International Conference on New Trends in the Applications of Differential Equations in Science (NTADES’21), 6-9 September, St. Constantine and Helena, Bulgaria*. 2021.

[10] P. Stoynov, (2022) “Switch Time Activation Function and Stopit Regression – Some Examples”, in *Proceedings of XXXI International Scientific Conference Electronics-ET2022, 13-15 September 2022, Sozopol, Bulgaria*. 2022.