Applicability investigation of heterogeneous neurosystem elements for cyber threats detection in large self-organizing communication networks

Dmitry P. Zegzhda, Maxim O. Kalinin, Vasiliy M. Krundyshev, Evgeniy A. Zubkov
Peter the Great St.Petersburg Polytechnic University
St.Petersburg, Russia
project@ibks.spbstu.ru

***Abstract*—The paper reviews the basic issues of using artificial neural networks (ANN) for solving the task of detection of the cyber threats in large self-organizing network infrastructures such as VANET/MANET networks, wireless sensor networks – WSN, Internet of Things – IoT, smart homes and smart buildings. The results of investigation of the applicability of traditional ANN are presented in comparison with current ANNs: recurrent, deep-learning, LSTM neural networks in requirements of quick processing and readiness to big data. The experimental estimations of the applicability of modern neural networks in the heterogeneous neural network of detection of cyber threats in large self-organizing communication networks is substantiated, and a construction of a neuronet ensemble of recurrent and LSTM ANNs is grounded.**

Keywords—black hole; deep-learning; cyber threat; ensemple; LSTM; neural network; recurrent neural network; IDS; IoT; MANET; VANET; WSN.

I. Introduction

Self-organizing communication networks (VANET – vehicular network, FANET – aircraft network, MARINET – inter-vessel network, WSN – wireless sensor network, IoT/MANET – mobile Internet of Things) are characterized by peer-to-peer infrastructure, net node moving and dynamic routing topology. Functional advantages of such networks are the possibility of communication in the absence of stationary radio-stations and the reliable data transfer when nodes move [1]. The new network technologies grow, the new cyber threats raise: for instance, interception of traffic for moving car, control of data flow between smart home and car, remote control and management of smart building devices, organization of botnets from IoT, denial of cyberphysical system service.

Integration of security features into a self-organizing network is a complex theoretical and applied issue, for the characteristics of these networks and the inadequacy of computational resources of the devices at the nodes of the network. In this regard, for such networks, *a-priori* protection methods have to be developed to ensure the prevention of cyber threats. Despite the fact that artificial neural networks (ANN) have been used for a long time to solve this task, new neuronets have recently appeared, for which investigations of their applicability for the detection of cyber threats in self-organizing networks have not yet been carried out. Among the new ANNs are deep-learning ANN, recurrent ANN, LSTM neural network.

II. The Related Works

The goal of any intrusion detection system (IDS) is to classify the cyber threat by known datasets (samples) of characteristic values (signs) [3]. The widely known approaches to solving this problem are as follows:

- a statistical method [3, 4], which is based on the creation of a normal profile, the etalon of the behavior of the system, and control of deviations from it. This method allows the intruder to drag the IDS onto the average profile and pass the attacks;
- a predicting pattern [3, 5], in which the IDS predicts the system states in the future, approximating the trace of the system states. A lot of modern cyber attacks can not be specified in such manner, and they will be missed by the IDS;
- an artificial neural network (ANN) [3, 6-8]. Associative model of knowledge in the form of neural networks is known for a long time and provides opportunities for parallel data processing and non-algorithmic classification of data. The classification procedure consists of selecting the identifying signs of cyber threats, training the neuronet on the given dataset, and the standard of the safe state of the system is marked. In the process of work, real data is supplied to the input of the ANN, and it determines their belonging to the determine classes of cyber threats.

Despite the fact that neural networks have been developing for many decades, researching activity has just recently been observed in this field. It is caused by the development of new computational technologies and the necessity for processing big data. For example, VANET of 1000 connected cars, each with an inner CAN control bus and 20 OBU controllers,

Project is financially supported by Ministry of Education and Science of Russian Federation, Federal Program "Researching and Development in Priority Directions of Scientific and Technological Sphere in Russia within 2014-2020" (Contract No. 14.575.21.0131, September 26, 2017, the unique identifier of the agreement RFMEFI57517X0131).

Project results are achieved using the resources of supercomputer center of Peter the Great St.Petersburg Polytechnic University – SCC “Polytechnichesky” (www.spbstu.ru).

generates about 4 million parameters per minute that affect the work of the moving vehicle. The big data challenge when detecting the cyber threats significantly complicates the job of the developing modern IDS for large networks with dynamic topology and huge amounts of parameters undergoing to be controlled.

The following paper presents our attempt to estimate the applicability of modern ANNs as the functional elements of a heterogeneous neurosystem for detection of cyber threats in large self-organizing communication networks.

III. Investigation of Neural Networks for Detection of Cyber Threts

A. *The Experimental Conditions*

Traditional neural networks, e.g. perceptron with logical transfer functions [7], forward and backward propagation of errors [7], do not satisfy the increased requirements for the volume of training samples (big data saturation problem). They also have low accuracy for results, they are trained for a long time, as well as they are redundant and demanding on the amount of computing resources [8].

To determine which neural networks should be included in the heterogeneous neurosystem for detection of cyber threats in a large self-organizing communication network, the following ANNs are selected:

- classical perceptron of direct propagation of signals;
- recurrent neural network[9];
- deep-learning neural network[10]
- LSTM [11].

For the investigation, a typical cyber attack on the availability of a self-organizing network is applied – the black hole attack [12]. The black hole attack is aimed at disrupting the connectivity of the network using dynamic routing, as a result of which the intruder does not transfer (discards) incoming network packets, which it should transmit further along the route.

B. *The Training Phase*

In Table 1, there is shown the testing results obtained during the training of the studied ANNs.

TABLE I. Comparision of ANNs on the phase of training

ANN	Error for the training samples (%)	Volume of training/work dataset	Time, sec.
Deep-learning	0,1	22/11	2,2
Perceptron	0,2	22/11	3,9
Recurrent	4	4500/1500	44,5
LSTM	4	4500/1500	50,6

Perceptron and deep-learning ANN have a simple architecture and at the expense of this they benefit from modern ANNs with complex architecture. Perceptron cannot be applied to process big data, recurrent and LSTM neural networks on the contrary are good with big data. The similarity of the perceptron and the deep-learning ANN is noted (Fig. 1).

On the same sample dataset, the deep-learning ANN is trained learns faster, with less errors, while there are no sharp decreases in the error graph if increasing the sample volume.

The recurrent and LSTM neural networks (Fig. 1) are similar in their behavior, but the LSTM neural network uses a memory that allows it to memorize the training process and gently respond to changes in the sample.

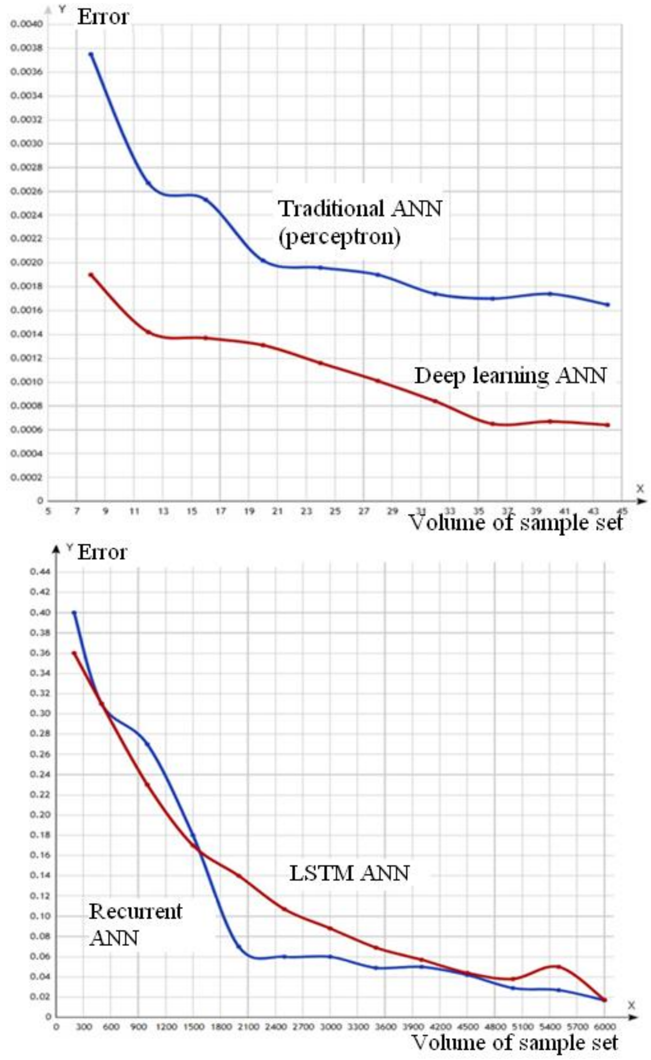

Fig. 1. Influence of the dataset volume on the quality of neural networks

C. *Big Data Processing Phase*

Taking into account the sensitivity of the neural networks to the size of the dataset, a study was performed for a big amount of input data (Table 2, the size of dataset is 4 million signs). The perceptron demonstrates a short processing time for big data, but this is accompanied by a drop in the quality of the results. A deep-learning network lacks the big data problem at the training stage, and in the working mode it also shows low performance.

TABLE II. COMPARISION OF ANNS ON THE PHASE OF WORKING WITH BIG DATA

ANN	Error for the working samples (%)	Time, sec
Perceptron	37	2,1
Deep-learning	50	3,0
Recurrent	1	28,8
LSTM	2	27,2

IV. CONCLUSION

The results of our investigation show that commonly used traditional neural networks are not suitable for solving the task of intrusion detection in large self-organizing communication networks because of their inability to work with big data.

For the task of detecting cyber threats in self-organizing networks, it is recommended to include in the heterogeneous neurosystem an ensemble of LSTM and recurrent neural networks that are capable of efficiently operating under difficult conditions, using big data, memorization and recurrent processing.

The application of modern neural networks allows the creation of IDS adequately to the threat and work conditions, which will ensure the cyber security of contemporary network environments.

REFERENCES

[1] B. Krishna, “Study of Ad hoc Networks with Reference to MANET, VANET, FANET,” International Journals of Advanced Research in Computer Science and Software Engineering, 7 (7), pp. 390-39, 2017.

[2] M. Erritali and B. El Ouahidi, “A Survey on VANET Intrusion Detection Systems,” International Journal of Engineering and Technology, 5(2), pp. 1985-1989, 2013.

[3] K.R. Karthikeyan and A. Indra, “Intrusion Detection Tools and Techniques – A Survey,” International Journal of Computer Theory and Engineering, 2(6), pp. 901-906, 2010.

[4] X. Li, “Probabilistic techniques for intrusion detection based on computer audit data,” IEEE Transactions on Systems Man and Cybernetics. Part A: Systems and Humans, 31(4), pp. 266-274, 2001.

[5] A. S. Sodiya, O. A. Ojesanmi, O. C. Akinola, and O. Aborisade, “Neural Network based Intrusion Detection Systems,” International Journal of Computer Applications, 106 (18), pp. 19-24, 2014.

[6] B. Widrow and M. A. Lehr. “30 years of adaptive neural networks: perceptron, Madaline, and back propagation,” Proceedings of the IEEE., 78 (9), pp. 1415-1442, 1990.

[7] S. Nikolenko, A. Kadurin, and E. Arkhangel’skaya, “Glubokoye obuchenie. Porguzhenie v mir neyrinnykh setey, 2018 [in Russian].

[8] A. Mallya, “Introduction to RNNs” Available at: http://slazebni.cs.illinois.edu/spring17/lec02_rnn.pdf, 2018.

[9] V. Sze, Y. H. Chen, T. J. Yang, and J. S. Emer, “Efficient processing of deep neural networks: A tutorial and survey,” Proceedings of the IEEE, 105 (12), pp. 1-31, 2017.

[10] R. Adhikari and R. K. Agrawal, “A Homogeneous Ensemble of Artificial Neural Networks for Time Series Forecasting,” International Journal of Computer Applications, 32 (7), pp. 1-8, 2011.

[11] N. K. Chaubey, “Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study,” International Journal of Security and Its Applications, 10 (5), pp. 261-274, 2016.