У зв’язку з цим, зважаючи на те, що потреба в безпеці, зокрема у кіберпросторі, належить до базових, першочергових потреб людини, ця сфера потребує подальших розробок та уточнень.

Література

1. Філософія права: підручник для ВНЗ / В.С. Нерсесянц. – 2-е вид., перероб. та доп. – М. : Норма: НВЦ Інфра – М., 2013. – 848 с.
2. А. Маслоу «Мотивація і особистість». – [Електронний ресурс]. – Режим доступу: http://psylib.org.ua/books/masla01/txt04.htm.
3. Богуш, В. Інформаційна безпека держави / В. Богуш, О. Юдін; [гол. ред. Ю.О. Шпак]. – К. : МК-Прес. – 432 с.
4. Горбатюк, О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О. М. Горбатюк // Вісн. Київ. ун-ту ім. Т. Шевченка. Сер. : Міжнар. відносини. – Вип. 14. – С. 46-48.
5. Про основні засади розвитку інформаційного суспільства на 2007-2015 роки: закон України від 09.01.2007 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.
6. Про основні засади забезпечення кібербезпеки України закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.

UDC 004.056.57

M.I. Kozlenko, V.M. Tkachuk, M.S. Dutchak
Vasyl Stefanyk Precarpathian National University
kozlenkomykola@ukr.net

SOFTWARE IMPLEMENTATION OF MICROCOMPUTER BASED INTRUSION DETECTION AND PREVENTION SYSTEM WITH BINARY NEURAL NETWORK

Network Intrusion Detection System (NIDS) is a software application that monitors a network for malicious actions and issues alerts when undesired activity has been discovered. Intrusion prevention systems (IPS) respond to such activity by rejecting the potentially malicious traffic.

There are lots of applications where it is not possible to deploy full-sized servers dedicated for cybersecurity tasks due to power supply limitations, heat dissipation, lack of needed physical space or financial reasons. That situation is common in industrial field sensor networks, distributed environmental monitoring systems, wireless control systems of unmanned vehicles and aerial drones, other applications where devices are limited in terms of size, power, and computational performance. All such systems are definitely a target for possible attacks and need sufficient protection against threats.

In such cases, a possible solution is to use industrial linux-based microcomputers, such as Orange, Raspberry Pi or others for IDS/IPS systems. As a rule those microcomputers are equipped with all necessary network connectivity devices both for Ethernet and for wireless communication. But the limitation factors are the low performance, absence of GPU, limited number of CPU cores, very low size of RAM. It makes it difficult to use conventional deep neural networks and common used frameworks in prediction time for malicious pattern recognition and general anomaly detection due to vast memory and computation requirements.

Using of a Binary Neural Network (BNN) has been proposed by the authors of this work as a base for a network intrusion detection/prevention system.

In contrast to traditional approaches, BNN uses binary weights and activations instead of full precision floating point values. It allows achieve lower memory usage and acceleration. But the disadvantage is a significant decrease in performance metrics.

The proposed system uses regular linux server, equipped with Tesla K80 GPU, in training time. It is based on Keras framework with TensorFlow 1.12 as an under-layered computational engine. All parts of the data import, training, and evaluation processes are implemented with Python 3.7 using NumPy, pandas, SciPy, scikit-learn packages with Jupyter Lab as a development environment.

After binarization, in predict time, the model is used on Raspberry Pi connected to the port mirroring network switch for pattern recognition of malicious TCP traffic. Port mirroring sends a copy of all network packets to the port, where the packets can be analyzed.

The following outcome has been achieved on the task of detection of the patterns of the famous network worm.

The achieved overall accuracy value is 0.92. The recall value is about 0.96, and the precision value is about 0.64 on the test set.

It is obvious that system gives a lot of false positives. Possible solution is to stack another model (classification, etc.) on top of the detection model in order to perform additional filtering. The authors have previous successful experience with model stacking in areas related to computer vision and natural language processing. It is a subject of future research.

References

1. Galloway, A., Taylor, G. W., and Moussa, M. (2018). Attacking binarized neural networks. In International Conference on Learning Representations.

2. Hubara, I., Courbariaux, M., Soudry, D., El-Yaniv, R., and Bengio, Y. (2016). Binarized neural networks. In Advances in neural information processing systems, pages 4107–4115.

3. Zhou, S., Wu, Y., Ni, Z., Zhou, X., Wen, H., Zou, Y.: DoReFa-Net: Training Low Bitwidth Convolutional Neural Networks with Low Bitwidth Gradients. 1 (2016) 1–14.

4. Yang, H., Fritzsche, M., Bartz, C., Meinel, C.: Bmxnet: An open-source binary neural network implementation based on mxnet. In: Proceedings of the 2017 ACM on Multimedia Conference, ACM (2017) 1209–1212.

5. Alexander G. Anderson and Cory P. Berg (May 2017), The High-Dimensional Geometry of Binary Neural Networks. CoRR, abs/1705.07199.