8. Терещенко О.О. Фінансова діяльність суб'єктів господарювання : [навч. посіб.] / О.О. Терещенко. – К. : КНЕУ, 2003. – 554 с.
9. Оцінка вартості майна підприємства [Електронний ресурс]. – Режим доступу:http://elar.khnu.km.ua/jspui/bitstream/123456789/3145/10/%D0%A0%D0%BE%D0%B7%D0%B4%D1%96%D0%BB_9.pdf.
10.Бланк И.А. Финансовый менеджмент : [учебный курс] / И.А. Бланк. – К. : Ника-Центр ; Эльга, 1999. – 528 с.
11. Селіверстова Л.С. Управління грошовими потоками підприємства / Л.С. Селіверстова // Економіка та держава. – 2015. – № 9. – С. 20–22.
12.Фінансовий менеджмент : [підручник] / Кер. кол. авт. і наук ред. проф. А.М. Поддєрьогін. – К. : КНЕУ. – 2005. – 535 с.
13. Філіна Г.І. Фінансова діяльність суб'єктів господарювання: Навчальний посібник.-К.: ЦУЛ, 2007. - 320с

UDC 004.056.57

INTRUSION DETECTION AND PREVENTION SYSTEM BASED ON BINARY NEURAL NETWORK

Nadiia Bohoslavets

student at the Faculty of Mathematics and Computer Science

Vasyl Stefanyk Precarpathian National University

Ivano-Frankivsk, Ukraine

sendahovm@gmail.com

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 [1].

There are lots of applications where it is not possible to deploy full-sized servers dedicated for cyber security tasks due to power supply limitations, heat dissipation, and lack of needed physical space or financial reasons [1]. 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 [1].

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 [2]-[4].

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 [5] with TensorFlow 1.12 [6] as an under-layered computational engine. All parts of the data import, training, and evaluation processes are implemented with Python 3.7 using NumPy [7], 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. There is previous successful experience with model stacking in areas related to computer vision and natural language processing [8]. It is a subject of future research.

References

1. M. Kozlenko, V. Tkachuk, and M. Dutchak, "Software implementation of microcomputer based intrusion detection and prevention system with binary neural network," in *Proc. 2nd International Scientific-Practical Conference "Problems of Cyber Security of Information and Telecommunication Systems" (PCSITS)*, O. Oksiiuk et al, Eds. Taras Shevchenko National University of Kyiv, Kyiv, Ukraine, Apr. 11-12, 2019, pp. 371-373.

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

3. 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.

4. 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.

5. M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, M. Devin, S. Ghemawat, G. Irving, M. Isard et al., “Tensorflow: a system for large-scale machine learning.” in OSDI, vol. 16, 2016, pp. 265-283.

6. Chollet, Francois. Keras. [Online]. Available: https://keras.io

7. Travis E, Oliphant. A guide to NumPy, USA: Trelgol Publishing, (2006).

8. M. Kozlenko and V. Vialkova, "Software Defined Demodulation of Multiple Frequency Shift Keying with Dense Neural Network for Weak Signal Communications," *2020 IEEE 15th International Conference on Advanced Trends in*

Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2020, pp. 590-595, doi: 10.1109/TCSET49122.2020.235501.

УДК004.891.3

Інформаційні технології

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ДЛЯ ОНЛАЙН ВИКОНАННЯ ПРОТИВІРУСНОЇ ДИХАЛЬНОЇ ГІМНАСТИКИ

Дувінський Д.О.,
студент кафедри біомедичної кібернетики
факультету біомедичної інженерії,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
м. Київ, Україна

Останнім часом чимало людей страждають від інфекційних та неінфекційних хвороб. За даними ВООЗ, від хронічної обструктивної хвороби легень в 2016 р померли 3,0 млн чоловік, а від раку легенів (поряд з раком трахеї і бронхів) - 1,7 млн осіб.

Інфекції нижніх дихальних шляхів залишаються найбільш смертоносною інфекційною хворобою, від якої в 2016 р в світі померли 3,0 млн чоловік [1].

За оцінками Держстату, за 2018 рік 12,9 тисяч людей загинуло від захворювань органів дихання. Найпоширеніші – через пневмонію та ураження нижніх дихальних шляхів. Від інфекційних хвороб загинули 8,9 тисяч осіб [2],[3].

Враховуючи також епідемію COVID-19 в Україні можна зазначити що з летальних випадків, більш ніж 70% пацієнтів мали супутні хвороби легень або серцево-судинні захворювання [4].

Все це створює потребу у розвитку діагностичних засобів, зручному доступі до інформації та упереджувальній діагностиці.