МИНОБРНАУКИ РОССИИ

Федеральный исследовательский центр «Информатика и управление» РАН
Национальный комитет РАН по распознаванию образов
и анализу изображений
Институт информационных технологий Министерства науки и образования
Азербайджанской Республики
Институт проблем передачи информации им. А. А. Харкевича РАН
Белорусский государственный университет
Национальный исследовательский Томский государственный университет
Федеральный исследовательский центр «Карельский научный центр РАН»
Ошский государственный университет
Юго-Западный государственный университет

ОПТИКО-ЭЛЕКТРОННЫЕ ПРИБОРЫ И УСТРОЙСТВА В СИСТЕМАХ РАСПОЗНАВАНИЯ ОБРАЗОВ И ОБРАБОТКИ ИЗОБРАЖЕНИЙ

Распознавание – 2023

Сборник материалов XVII Международной
научно-технической конференции

12–15 сентября 2023 года

Курск
ЮЗГУ
2023

Distributed VAS allows to determine scenarios for the operation of algorithms based on data obtained from different sources of information.

The principle of distribution makes the system more fault-tolerant, scalable and accurate.

The use of several sources of information and the identification of key features makes it possible to improve the quality of the principles and algorithms used without upgrading the VAS hardware.

The implementation of a distributed VAS can be applied in various areas where it is necessary to make decisions based on several sources of information.

It is planned to build and test VAS with a higher quality of determining the traffic flow parameters and good scalability for use in metropolis.

REFERENCES

1. Кременец Ю. А. Технические средства организации дорожного движения. М.: Академкнига, 2005. 279 с.

2. Власов В. М., Ефименко Д. Б., Богумил В. Н. Информационные технологии на автомобильном транспорте. М.: Academia, 2014. 256 с.

3. Методы автоматического обнаружения и сопровождения объектов. / Б. А. Алпатов, П. В. Бабаян, О. Е. Балашов, А. И. Степашкин // Обработка изображений и управление ими. М.: Радиотехника, 2008. 176 с.

4. Alpatov B. A., Babayan P. V., Ershov M. D. Vehicle detection and counting system for real-time traffic surveillance // Proceedings of 7th Mediterranean Conference on Embedded Computing (MECO), 10–14 June 2018. Budva, Montenegro: IEEE, 2018. P. 120–123. DOI 10.1109/MECO.2018.8406017

UDC 004.048

R. H. Shikhaliyev[1]
e-mail: shikhramiz61@gmail.com

[1]*Institute of Information Technology, Baku, Republik of Azerbaijan*

COMPUTER NETWORKS SECURITY MONITORING MODEL BASED ON DEEP LEARNING

This article presents a computer network security monitoring model based on a deep learning model. Convolutional Neural Networks and Long Short-Term Memory models are used, which allow classifying network security data and detecting CN anomalies.

Due to the increasing scale, complexity, and ever-increasing interconnectedness of modern computer networks (CNs), as well as the volumes of data generated daily, monitoring their security becomes a very difficult task. This is mainly because traditional network monitoring methods face the challenge of accurately and

efficiently processing more data in real time. Therefore, it is necessary to develop new methods for non-invasive monitoring of cybersecurity, for which deep learning is more suitable.

Deep learning is effectively used for big data analysis and knowledge extraction to recognize hidden and complex patterns and detect anomalies in time-ordered data [1]. When monitoring CN security based on deep learning, network security attacks that cannot be detected at the network level can be detected.

The purpose of this article is to develop a model for monitoring CN security based on deep learning. This model allows for the collection of network security data and classifies anomalies by training.

Untimely detection of problems related to the security of the CN can lead to network faults, poor provision of network services, and a decrease in the CN's security. Therefore, it is required to find and solve such problems before they arise, i.e., a system for intellectually monitoring the security of the CN is required.

A conceptual model is proposed for monitoring the security of the CNs (Fig.).

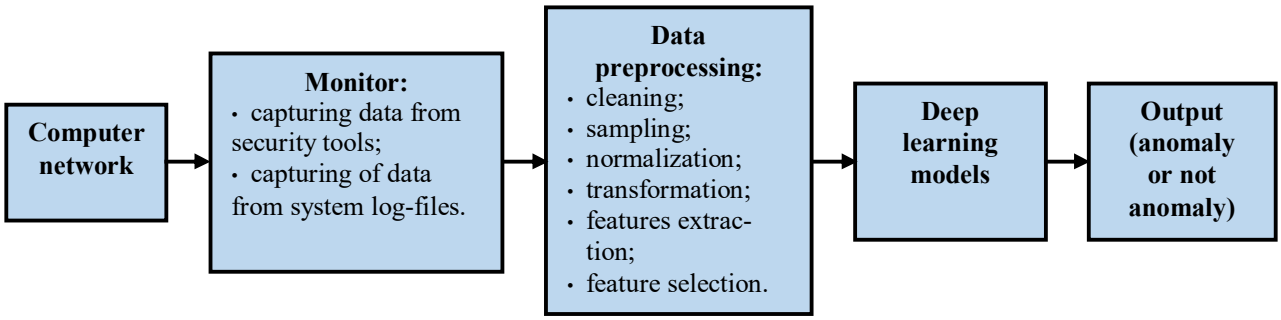

Fig. Model for monitoring the security of the CN based on deep learning

At the same time, the concept of monitoring CN security consists of collecting data from security events, extracting features, and training the neural network model.

The proposed conceptual model consists of several components. First, the monitor collects security event data from CN security tools such as intrusion detection systems and firewalls, as well as from system log files. At the same time, it is necessary to standardize and integrate security events from various heterogeneous sources. Next, the security event data is pre-processed, i.e., cleaning, sampling, normalization, transformation, feature extraction, and feature selection are performed. Finally, deep learning models perform security data classification and anomaly detection. Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) models are used [2], the combination of which allows classifying network security data and detecting CN anomalies. At the same time, the spatio-temporal characteristics of anomalies can be obtained using training, which can improve the overall performance of CN anomaly detection. LSTM solves the problem of gradients disappearing or exploding after training in time series modeling [3].

One of the main problems of CN security monitoring is recognizing the relationship between several events over a certain period of time, that is, the event pattern. The use of deep learning models significantly improves the efficiency of pattern recognition and rule building, which allows for the automatic creation of detection models. It is suitable for both anomaly detection and abuse detection and can effectively detect known and unknown attack patterns.

REFERENCES

1. Gamboa J. C. B. Deep learning for time-series analysis / Cornell University. 2017. arXiv:1701.01887. DOI 10.48550/arXiv.1701.01887.

2. Yen S., Moh M., Moh T.-S. CausalConvLSTM: Semi-supervised log anomaly detection through sequence modeling. // IEEE International Conference On Machine Learning and Applications. 6-19 December 2019. Boca Raton, FL, USA, IEEE, 2019. P. 1334–1341.

3. Buczak A. L., Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection // IEEE Communications Surveys & Tutorials. 2016. Vol. 18, no. 2. P. 1153–1176.

UDC 621.397.01

V. S. Usatyuk[1], S. I. Egorov[1]
e-mail: L@Lcrypto.com

[1]*Southwest State University, Kursk,* Russian Federation

DEEP NEURAL NETWORK FOR WIRELESS CHANNEL ESTIMATION

We applied residual deep neural network for uplink and downlink MIMO channel estimation. Proposed deep neural network channel estimation shows more than 2 dB gain under EPA uplink channels compare to MMSE channel estimation and ability to work on wireless channels that have not previously been trained.

The quality of channel estimation is crucial to the throughput of MIMO wireless communication systems. The wireless channels are time-varying and frequency-selective, so there are limited resources for channel estimation before it changes.

An OFDM based MIMO transmission system with N transmit (TX) and M receive (RX) antennas, where $N \le M$, is considered. The received frequency domain (FD) signal vector $y(n)$ on the m_R-th received antenna at discrete time index n after the discrete Fourier transform can be described as $y_m(n) = X(n)\underline{F}h_{m_R}(n) + w_{m_R}(n)$, where $X(n) = [X_1,\ldots,X_N] \in \mathbb{C}^{P\times NP}$ is the transmitted signal over P subcarriers and N transmit antennas, $w_{m_R} \in \mathbb{C}^P$ contains