Convolutional neural network for detecting anomalies in the control system of a machine-building enterprise

N M Kusakina¹, S P Orlov¹ and O Ja Kravets²

¹ Samara State Technical University, 244 Molodogvardeiskaia str., Samara, 443100, Russian Federation
² Voronezh State Technical University, 14 Moscow ave., Voronezh, 394000, Russian Federation

E-mail: csit@bk.ru

Abstract. The article is devoted to the study of the possibility of using machine learning methods and the apparatus of neural networks to ensure a given performance and security of the enterprise infrastructure. Continuous monitoring of computer networks and enterprise resource planning systems determines the stability of the enterprise. The infrastructure of any enterprise is gradually expanding and increasing, not only due to the growth of the geography of networks, but also due to the use of equipment from various manufacturers. Therefore, it is important to create intrusion detection and prevention systems with automated monitoring of equipment, processes and user activity. The article describes the use of convolutional neural networks for predicting indicators and technical characteristics of equipment and communication channels. An anomaly detection module structure has been developed for monitoring the operation of the enterprise resource planning system. An example of training data for a neural network is given. The experimental results confirmed the effectiveness of the proposed approach.

1. Introduction

For a long time, Enterprise Resource Planning (ERP) systems have been closed systems that are isolated from external networks when used to manage the organization’s production, labor and financial resources. However, due to the trend towards integration and globalization of systems with computer and telecommunication networks, ERPs are now considered as part of the enterprise infrastructure. In this case, the processes occurring in an organization have complex interrelation of parameters whose values are changed in real-time.

Due to access to the management of production processes, the ERP system is a critical object of industrial infrastructure. As a result, an attacker, infiltrating the computer network of the enterprise, can have access not only to data servers and control centers, but also to the settings directly processes. It is easy to imagine the global consequences of a successful hacking nuclear power plant ERP system. In addition, industrial “know-how” leakage can lead to significant financial losses for the company.

Various classes of tools are used to detect attacks from the global network to the local area network of the enterprise: comprehensive security management systems, passive and active means of monitoring the availability of network resources, intrusion detection and prevention systems [1-4]. Many studies have been devoted to the detection of anomalies and intrusions in industrial control
systems [5-9]. However, when conducting a targeted attack on ERP, it may not be detected by classical security systems based on the signature approach [10-13].

For this reason, it is important not only to use attack detection systems on the perimeter of the network, but also to monitor the state of technological processes through the measurement and analysis of their characteristics. For example, an unregulated periodic change in the sensor readings or a change in the scenarios of the operation of the controllers may indicate an intruder penetrating the network and spoofing these sensors. Thus, the detection of attacks on ERP, which manifest themselves as uncharacteristic behavior of devices connected to the network, uses systems based on methods for detecting anomalies. These methods are widespread because ERP systems are fully automated and have more regularity and predictability than typical IT systems. In general, techniques are applied using behavioral algorithms.

The rapid development of information technology makes it possible to adapt and apply artificial intelligence techniques in the analysis of data from various sources in the ERP. This article proposes an approach to the analysis of anomalies within an ERP system based on the use of convolutional neural networks. Convolutional neural networks were used in [14–16] to detect anomalies during an unauthorized access to the industrial water treatment control system. Convolutional networks also were used by the authors of this article to diagnose the states of various technical objects [17, 18]. The use of self-learning systems helps to avoid creating a huge number of handwritten rules describing the patterns of the regular functioning of the system, taking into account the existing relationships and noise in the received data.

2. ERP application in mechanical production

At present, the ERP systems are used for the segmentation of management areas, real-time monitoring of production indicators and effective management accounting following applicable law. ERP allows for:

- effective procurement and order management;
- simplification of planning and cost setting;
- automatic formation of production tasks and their actualization;
- monitoring project activities at any stage of implementation;
- consistency of various types of reporting;
- monitoring the status of equipment and systems;
- planning and implementation of timely equipment repairs;
- minimizing equipment downtime as a result of an accident.

The main criterion for the implementation of ERP system security measures is support for the integrity of the system, both during normal operation and during attacks. A typical ERP system consists of numerous control loops, remote diagnostics, sensors, and controllers, thereby expanding the perimeter of the enterprise network. Therefore, their interdependencies can be considered to detect and prevent network perimeter vulnerabilities. Figure 1 shows a simplified diagram of the perimeter of the enterprise when using the ERP system.

Industrial control systems previously consisted of only two components: dispatch control hardware and data collection, which receive information from sensors and then control mechanical machines. Nowadays, ERP systems have become complex open infrastructure multi-agent facilities, and Internet access makes them even more vulnerable to cybercriminals.

The potential consequences of attacks on the ERP can be a destructive force, and they differ on the impact and scope: from short-term malfunction to complete the liquidation process. Therefore, there is a need for a self-learning intrusion detection system that can use both the available signature databases and the patterns of regular network operation.
3. Anomaly detection module
Intrusion detection tools are used to identify information security incidents. Such modules are one of the main components of the infrastructure protection system of an industrial enterprise. Figure 2 shows the anomaly detection process carried out by the detection module.

It performs the following functions:
- collection of data from the enterprise network.
- extracting feature vectors from collected or observed data.
- processing the resulting vector using the selected algorithm. Machine learning methods can be used here.
- decision making to identify anomalies.
- notification of an information security event.
- responding to an information security event.

4. Modelling the process of anomaly detection module
The report examined the use of the anomaly detection module to determine illegitimate remote sessions performed on the organization equipment. Since the enterprise has remote entry points, it is necessary to analyze the traffic passing through them. This will reveal compromises, the use of vulnerable software, and irrelevant device firmware. It is such violations that most often become the catalyst for a successful attack.
The implementation of the module is as follows:

- data collection from the enterprise network (pre-collected network traffic dump containing both normal traffic flows and abnormal connections).
- preliminary processing of the dump in MS Office (Excel), where each line of the document is represented by a separate feature vector.
- using the machine learning method, namely, training a convolutional neural network implemented in TensorFlow.

The following features were selected for training the network:

- IP address of source and destination;
- total number of transmitted packets and bits;
- the number of compounds for a given pair of source and destination for a selected period of study time; date.

### Table 1. Training data example.

| Client IP      | Server IP  | Bits/sec | Total Packets | Total Connects | Total Pakets/Sec | Date       | Anomalies |
|----------------|------------|----------|---------------|----------------|------------------|------------|-----------|
| 91.238.28.253  | 10.5.10.6  | 11 619 000 | 62 594 000    | 23             | 1 449           | 28.02.19   | 0         |
| 109.73.5.210   | 10.5.10.6  | 11 671 000 | 725 000       | 134            | 1 678           | 28.02.19   | 0         |
| 194.88.14.178  | 10.5.10.6  | 11 814 000 | 66 623 000    | 16802          | 115 422         | 28.02.19   | 1         |
| 77.50.114.12   | 10.5.10.6  | 12 144 000 | 58 363 000    | 216            | 1 351           | 28.02.19   | 0         |
| 83.219.23.230  | 10.5.10.6  | 13 159 000 | 77 655 000    | 31             | 1 798           | 28.02.19   | 0         |
| 94.79.2.131    | 10.5.10.6  | 13 325 000 | 6 303 000     | 8              | 1 459           | 28.02.19   | 0         |

The peculiarity of convolutional neural networks is the ability to tune with the help of a training sample to highlight the characteristic "features" in the data presented. To convert traffic dumps from the .pcap format to the training dataset, we used the ISCX Flowmeter open-source program, which converted the collected files to the .xml format. Then, the payload data was converted to a NumPy array with dimensions of 50x50x3. After that, the vertical addition of arrays was performed with the addition of a column that contained attribute 1 if the packet is abnormal, and 0 if normal. The resulting training dataset was saved in .npy format so that it could be used as input for the deep learning model.

The convolutional neural network VGG16 was selected for research. This network was pre-trained on a million images of the ImageNet base.

The structure of the implemented artificial neural network is shown in figure 3.

![Figure 3. The structure of the neural network VGG16.](image)
The network is represented by sixteen layers, has an input image size of 224x224 and uses 3x3 convolution kernels. The latter characteristic determines its performance. The network was trained on the collected data set to identify suspicious (illegitimate/compromised) user sessions. It confirmed that the model successfully detects illegitimate connections. However, to build a full-fledged module for detecting anomalies, it is advisable to conduct further testing and, if necessary, retrain on new data sets.

5. Conclusion
The developed model of an artificial neural network forms the basis for creating an anomaly detection module in the network traffic of an enterprise. In the process of research, the following problems were studied: a) the complexity of selecting a function from a network traffic data set to detect anomalies, b) the complexity of marking a traffic data set from real networks. Since attack scenarios are constantly changing and evolving, functions selected for one attack class may not work for other attack classes. Moreover, redundant and irrelevant attributes can reduce the efficiency of data mining algorithms, which will lead to unclear experimental results. Accordingly, further research will be devoted to increasing the efficiency of feature selection and classification accuracy, as well as improving the architecture of the neural network used, for example, by increasing the batch size.

References
[1] Linda O, Vollmer T and Manic M 2009 Neural network based intrusion detection system for critical infrastructure Proc. of the Neural Networks IJCNN 2009 Int. Joint Con. on IEEE 1827–34
[2] Gao W, Morris T, Reaves B and Richey D 2010 On SCADA control system command and response injection and intrusion detection Proc. eCrime Researchers Summit (eCrime) IEEE DOI: 10.1109/ecrime.2010.5706699
[3] Borges R C H, Beaver J M, Buckner M A, Morris T, Adhikari U and Pan S 2014 Machine learning for power system disturbance and cyber-attack discrimination Proc. Resilient Control Systems (ISRCS) 7th Int. Symposium on IEEE DOI:10.1109/ISRCS.2014.6900095
[4] Teixeira A, Perez D, Sandberg H and Johansson K H 2012 Attack models and scenarios for networked control systems Proc. of the 1st Int. Conf. on High Confidence Networked Systems ACM 55–64
[5] Yang D, Usynin A and Hines J 2005 Anomaly-based intrusion detection for SCADA systems Proc. of the 5th Intl Top Meet Nucl Plant Instrumentation Control Hum Mach Interface Technol (NPIC&HMIT 05) 12–16
[6] Maglaras L A and Jiang J 2014 Intrusion detection in SCADA systems using machine learning techniques Proceedings of 2014 science and information conference 626–631
[7] Chandola V, Banerjee A and Kumar V 2009 Anomaly detection: A survey ACM Comput. Surv. 41 15
[8] LeCun Y, Bengio Y and Hinton G 2015 Deep learning Nature 521(7553) 436
[9] Ahmad S, Lavin A, Purdy S and Agha Z 2017 Unsupervised real-time anomaly detection for streaming data Neurocomputing 262 134–47
[10] Esmaily J, Moradinezhad R and Ghasemi J 2015 Intrusion detection system based on multi-layer perceptron neural networks and decision tree 7th Conference on Information and Knowledge Technology DOI: 10.1109/IKT.2015.7288736
[11] Zhang J, Zulkernine M and Haque A 2008 Random-forests-based network intrusion detection systems IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 38(5) 649–59
[12] Lopez-Martin M, Carro B, Sanchez-Esguevillas A and Llore J 2017 Network traffic classifier with convolutional and recurrent neural networks for Internet of Things IEEE Access 5
18042–50

[13] Kusakina N M 2018 The classification approach to network traffic anomalies in the design of intrusion detection systems 2018 Advanced Information Technologies (PIT 2018): proceedings of the International Scientific and Technical Conference 296-8

[14] Kravchik M and Shabtai A 2018 Detecting cyber attacks in industrial control systems using convolutional neural networks ACM Proc. of the 2018 Workshop on Cyber-Physical Systems Security and Privacy 72–83

[15] Jonathan G, Sridhar A, Khurum N J and Aditya M 2016 A dataset to support research in the design of secure water treatment systems Int. Conf. on Critical Information Infrastructures Security (Springer) 88–99

[16] Inoue J, Yamagata Y, Chen Y, Poskitt C M and Sun J 2017 Anomaly detection for a water treatment system using unsupervised machine learning arXiv:1709.05342

[17] Girin R and Orlov S 2020 Convolutional neural network applied to remote technical diagnosis by thermograms Advances in Intelligent Systems and Computing, Recent Trends in Intelligent Computing, Communication and Devices. Proc. of ICCD 2018 (Springer) 1031 681-86

[18] Orlov S and Girin R 2020 Intelligent technologies in the diagnostics using object’s visual images Studies in Systems, Decision and Control Cyber-Physical Systems: Advances in Design & Modelling (Springer) 259 301-12