Applying Methods of Machine Learning in the Task of Intrusion Detection Based on the Analysis of Industrial Process State and ICS Networking

Alexander N. Sokolov
Head of Information Security Department
South Ural State University
School of Electrical Engineering and
Computer Science
Russia

Ilya A. Pyatnitsky
PhD student at the Information Security
Department
South Ural State University
School of Electrical Engineering and
Computer Science
Russia

Sergei K. Alabugin
PhD student at the Information Security
Department
South Ural State University
School of Electrical Engineering and
Computer Science
Russia

Modern industrial control systems (ICS) are increasingly becoming targets of cyber attacks. Traditional security tools based on a signature approach are not always able to detect a new attack, the signature of which has not yet been described. In particular, this occurs during targeted attacks on industrial facilities. Cyber attacks can cause anomalies in the operation of an industrial control system and process equipment under its control. Therefore, to detect attacks, it is advisable to use an approach based on the detection of anomalies. A reasonable way to implement this approach is to use machine learning techniques. The paper deals with the most common methods of machine learning (decision tree algorithms, linear algorithms, support vector machine) and neural networks. To assess their applicability in the problem of detection of ICS anomalies, the Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation and Gas Pipeline datasets were used.

Keywords: *ICS security, intrusion detection, machine learning, neural networks, anomaly detection*

1. INTRODUCTION

For a long time, Industrial Control Systems (ICS) have been isolated from outer networks, especially the Internet. Currently, according to the Interconnection principle of Industry 4.0, there is a tendency to integrate industrial and corporate networks. This is due to various reasons, such as the geographical remoteness of the components of the ICS, the need to receive software updates over the Internet, and economic feasibility. For this purpose, ICSs use the traditional technologies, as a rule, proprietary, developed without taking into account the requirements of information security [1]. A low level of information security culture is a typical problem for the industry as a whole [2]. This is especially true for the rapid development of security updates by manufacturers and the timely installation of these updates by ICS operators. The problems mentioned are the causes of ICS vulnerability for an attacker.

Since the ICS of many industrial enterprises are part of the critical information infrastructure, their proper operation ensures the quality of life and the well-being of people and the region or the country as a whole. This implies the possibility for an enterprise and its ICS to be a target of cyber attacks. It is very important that a successful attack can result in such physical consequences as stopping production, a technological disaster, etc. [3-5].

Traditional systems of intrusion detection based on a signature approach are not able to detect an attack without a signature described. Considering that cyber attacks become targeted and widespread, may be of new types and have heavy, is reasonable to use an anomaly-based approach to detect intrusions [6].

A modern ICS is not only a data system but also a physical one and includes hardware and software to control an industrial process. Due to this fact, the attacks targeting ICSs may reveal themselves in uncharacteristic behaviour of network infrastructure devices and equipment directly involved in the process, for example, abnormal changes in sensor readings or controller scenarios. Thus, to detect intrusions (attacks) in ICS, it makes sense to analyze not only network traffic, but also the state of the process.

A process controlled by an ICS is usually characterized by a significant number of parameters [7, 8], the regulatory values of which can vary during changing the process structure. Manual creation of rules describing the normal industrial process operation and normal network interaction scenarios is high costs and requires knowledge of a specific ICS structure. Therefore, it is reasonable to use machine learning methods to detect anomalies in the operation of ICS. Also, such machine learning based approach fit into the decentralized decision principle of Industry 4.0 and makes ICS security more autonomous.

Methods of machine learning usually reduce the problem of ICS intrusion detection to one of standard tasks of machine learning, namely, classification, clustering, or detection of anomalies. The results of applying some classical machine learning algorithms (K-means, Naive Bayesian, GMM, PCA-SVD) are presented in [9] using the example of the Gas Pipeline dataset. Fully connected evolutionary based neural

Received: February 2019, Accepted: June 2019
Correspondence to: Ph.D. Eng. Alexander N. Sokolov
Dept. of Information Security, South Ural State
University, Chelyabinsk, 454080, Russia
E-mail: sokolovan@susu.ru
doi:10.5937/fmet1904782S

networks are used in [10] to detect anomalies. In particular, the Gray Wolf Optimize algorithm is used to increase the speed of network learning. In [11], the Random Forest and Support Vector Machine algorithms are applied to identify anomalies, and the methods of data gap processing and data normalization are analyzed to improve the algorithms. The paper [12] proposes to use a new approach based on Spiking Neural Network in the frame of one-class classification to detect anomalies in order to obtain a practically applicable algorithm that does not need data on the ICS abnormal state.

The contributions of this paper are as follows:

1) Comparison of the efficiency with which fully connected neural networks and other methods of machine learning can be applied for detecting anomalies in the ICS operation process. The considered methods are classification algorithms. The algorithms are selected from among the most frequently used in practice (linear classification methods, methods based on decision trees, neural networks).

2) Consideration of the LSTM and GRU recurrent neural networks applicability is for intrusion detection. This approach is based on forecasting and allows to take into account information about past states of the ICS. Two cases are considered separately: the case when the analysis object is exclusively the industrial process and the case when the network object of the analysis is the ICS network traffic containing information on the state of the industrial process and the interaction of the ICS components.

The experiments were conducted on the Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation and Gas Pipeline datasets, respectively. Accuracy and recall metrics were used to estimate the algorithm performance. Accuracy is a ratio of the number of objects correctly determined by the algorithm to the number of all objects of the test sample.

To define recall correctly, we introduce a number of notations. Suppose that there is a class of objects A, in which:

TP is the number of class A objects correctly classified by the algorithm;

FN is the number of objects incorrectly classified by the algorithm that do not belong to the class A.

Taking into account the introduced notation, we define recall as ratio of *TP* and sum of *TP* and *FN.*

2. METHODS OF MACHINE LEARNING

The study uses several methods of machine learning. In general, the considered methods relate to supervised learning and solve the problem of classification. Additionally, we consider recurrent neural networks used to detect the presence of attack.

2.1 Linear classification methods

Linear classification methods are based on construction of a linear or piecewise linear function describing a surface that separates different classes in the feature space. Among linear methods, there are quite simple ones, such as Logistic Regression and Lasso, which allow solving relatively simple classification problems with good results. However, if the features, with which such methods work, correlate, it is difficult to achieve acceptable accuracy.

Linear classification methods also include the support vector machine method (SVM) [13, 14]. This method is successfully applied in various problems, since the classification is carried out in a space of a higher dimension than the dimension of the original feature space. However, this method does not work well if there are outliers in the training set.

2.2 Decision trees

This group of methods is based on a concept of a decision tree, that is, binary tree with logical predicates in its nodes and class marks in leaves [13]. The great advantage of such methods is their ability to work with data that has gaps. Unlike other methods of machine learning, algorithms based on the concept of the decision tree can also work with samples, in which the values of various attributes differ by orders of magnitude, without loss of accuracy.

The paper discusses the decision tree method that is a single decision tree and three ensemble methods based on the composition of several decision trees: Adaptive Boosting, Gradient Boosting and Random Forest.

2.3 Fully connected neural networks

Deep neural networks (DNN) are the development of classical neural networks with complicated architecture and a large number of layers [15]. That is, DNNs contain more than one hidden layer. Compared with classical methods of machine learning, such models have a number of distinctions, in particular, the ability to learn from data for which no feature extraction have been carried out. Since neural networks have high generalization ability, they are able to extract the necessary features from the raw data. For example, it is possible to solve the problem of object classification in an image using the values of image pixels as features.

However, the more complex the problem to be solved, the more data is required for learning and the more computing power is needed to obtain an acceptable result. The paper discusses the neural networks with fully connected architecture, i.e. the network is a sequence of related layers of neurons.

2.4 Recurrent neural networks

Recurrent neural networks (RNN) are a class of machine learning models characterized by the presence of feedback in its architecture. Feedback makes it possible to analyze serial data (time series) since a network with feedback can store the history of the sequence used for prediction. In particular, using a recurrent neural network, we can analyze the sequence of ICS states by training the network from data extracted from network traffic. By analyzing the sequence of network packets and the state of the process, the network learns to predict the contents of the next network packet. Thus, in the case when the prediction of the neural network differs from the network packet being analyzed, an anomaly is recorded, which means an invasion. The paper considers two architectures of neural networks: Long Short Term memory (LSTM) [16] and Gated recurrent units (GRU) [17].

3. ADDITIONAL TENNESSEE EASTMAN PROCESS SIMULATION DATA FOR ANOMALY DETECTION EVALUATION

Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation [18] is a modified version of the classical dataset based on the Tennessee Eastman Process model [19]. This model describes the industrial process in a chemical plant.

The process is a controlled chemical reaction, in which several substances denoted as A, B, C, D, E, F, G, and H, participate. The purpose of the chemical process is to obtain two substances (G and H). The reagents are substances A, C, D, and E. Substance B is formed in the reaction and is inert, and substance F is a co-product of a chemical reaction. The process flow diagram is presented in Fig. 1. The main units, in which the reaction takes place, are a reactor, a condenser, a vapor-liquid separator, a compressor, and a stripper. Substances A, D, and E, in the form of gas, are placed in the reactor, where during a chemical reaction they are converted into steam. Next, the steam enters the condenser and then moves to the vapor-liquid separator. The compressor returns the steam to the reactor for the next iteration of the process while the liquid enters the stripper, where impurities are removed from it and a chemical reaction takes place with substance C.

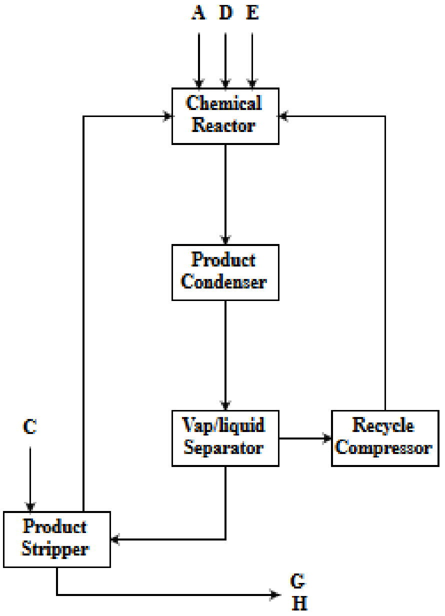

Figure 1. Tennessee Eastman Process flow diagram

In the Tennessee Eastman Process model, 41 variables, such as temperature, pressure, and other characteristics, are defined that describe the state of the process at a specific point in time. In addition, the model defines 12 variables that control the process (control variables), the values of which are set by the operator.

The software implementation of this model makes it possible to generate many different datasets. However, researchers often use a standard, previously generated set. The set used in the paper is identical to the pre-generated one, however, it is more randomized. This complicates the problem of detecting anomalies. The dataset includes records consisting of 53 features and belonging to one of twenty classes, corresponding either to one of the types of anomalies or to the normal state of the industrial process. The total number of records exceeds 15 million. Such amount requires large computational power, however, it allows unlocking the potential of deep learning models. Description of the dataset is presented in Table 1.

Table 1. Dataset Description

Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation dataset description	
56	Features
41	sensors (MEAS – measurements)
12	controls (MV – manipulated variables)
1	class label
2	service fields
4	Files
1	Training sample with anomalies – 5000000 records
1	Training sample without anomalies – 250000 records
1	Test sample with anomalies – 9600000 records
1	Test sample without anomalies – 480000 records
	Classes
	Normal operation A/C feed ratio, B composition constant (Stream 4) B composition, A/C ratio constant (Stream 4) D feed temperature (Stream 2) Reactor cooling water inlet temperature Condenser cooling water inlet temperature A feed loss (Stream 1) C header pressure loss-reduced availability (Stream 4) A, B, C feed composition (Stream 4) D feed temperature (Stream 2) C feed temperature (Stream 4) Reactor cooling water inlet temperature Condenser cooling water inlet temperature Reaction kinetics Reactor cooling water valve Condenser cooling water valve 5 Unknown faults

4. GAS PIPELINE DATASET DESCRIPTION

The Gas Pipeline dataset [20] was formed during the logging of the network traffic of the laboratory SCADA-system. It presents data corresponding to the normal operation of the system and data corresponding to various attacks. The simulated system consists of a gas pipe, a pump, a compressor, a pressure sensor, and a pressure relief valve controlled by solenoid. The system diagram is shown in Fig. 2. The required pressure level in the system is maintained using a proportional-integral-derivative control (PID). For communication, the described system uses the Modbus application layer protocol. After appropriate processing, network packets with timestamps form a dataset. Thus, a dataset record corresponds to a Modbus network packet.

Each record contains values of 17 features, some of which carry information about the network (the packet destination, the Modbus function code, etc.), and the rest characterize the state of the industrial process. The full list of features is presented in Table 2.

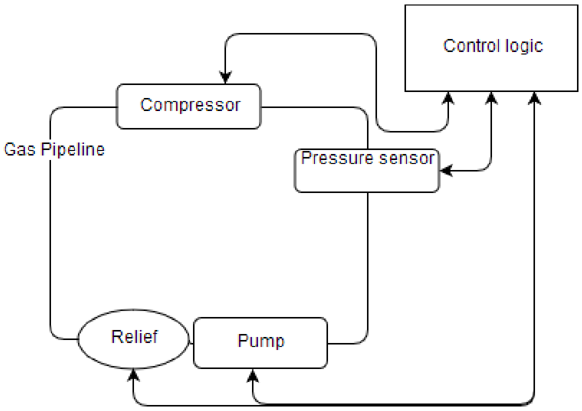

Figure 2. Gas Pipeline system diagram

Table 2. Features of the Gas Pipeline dataset

Feature	Description
address	Station address
crc rate	Packet checksum value
function	Modbus function code
length	Modbus packet length
setpoint	Set pressure value
gain	PID gain
reset rate	PID reset rate
deadband	PID dead band
cycle time	PID cycle time
rate	PID rate
system mode	Operating mode: automatic (2), manual (1) , off (0)
control scheme	Pressure control: pump (0), solenoid (1)
pump	Pump open (1) or closed(0)
solenoid	Valve open (1) or closed (0)
pressure measurement	Pipeline pressure value
command response	Package: command (1) or response (0)
Time	Time stamp

35 specific attacks were used in the dataset. Each record of the dataset corresponds to either a normal state or one of the seven types of attacks [21]. Types of the attacks are presented in Table 3. The total volume of the dataset is 274628 records, with 214580 of them corresponding to the normal state of the system and 60048 to one of the attacks.

5. EXPERIMENTAL STUDIES

During the experiment, the Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation was considered. The training sample used in the experiment was formed by combining two training samples of the dataset: with and without anomalies. The resulting sample size was 5250000 records. Outlying data and damaged strings were deleted from the sample, and data analysis was performed. As typical example, Fig. 3 shows the distribution of absolute frequencies of “supply of substance A” feature.

Values of feature are plotted along the X axis, and absolute frequencies of these values in the sample are plotted along the Y axis. The graph demonstrate that the features have a distribution close to normal, with sharp bursts in the minimum and maximum values, as well as most of the features of the dataset under consideration. This is most likely due to the peculiarity of the sensors: when the parameter value is outside the threshold, the sensor shows the threshold value. This pollutes the analyzed data and complicates the work of some machine learning algorithms. The feature correlation matrix, a fragment of which is presented in Table 4, shows that many variables (features) are strongly correlated with each other, up to complete coincidence, when the correlation value is equal to one. This is most likely due to the nature of the data source: the data describes the industrial process, so some variables are dependent. Since many features correlate with each other, data pre-processing and feature normalization were conducted before the machine learning methods were used.

Table 3. Types of attacks presented in the Gas Pipeline dataset

Attack type	Description
Naive Response Injection	Inject random response packets
Complex Response Injection	Hide the real state of the controlled process
State Command Injection	Inject malicious state commands
Parameter Command Injection	Inject malicious parameter commands
Function Code Injection	Inject malicious function code commands
Denial of Service	Denial of service targeting communication link
Reconnaissance	Pretend of reading from device

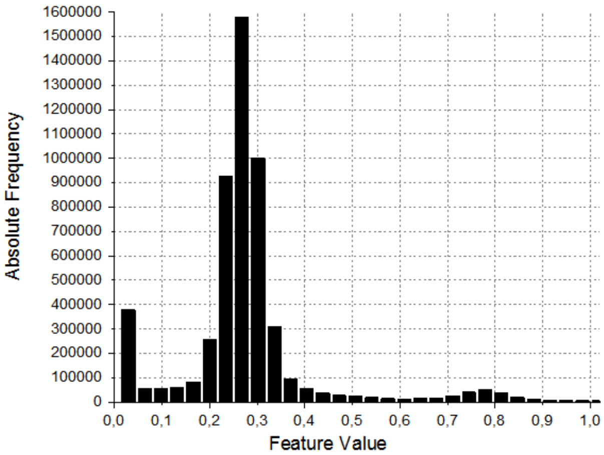

Figure 3. Supply of substance A

Then, different methods of machine learning were tested. The training sample was divided into two parts: training (70 percent) and validation (30 percent).

Algorithms were trained on 70 percent of the data, and their validation was performed on the remaining 30 percent. A number of training and validation iterations allow selection of optimal parameters for each algorithm. Next, the algorithms were applied to the dataset test sample, which includes anomalies.

Table 4. The correlation of some features of Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation

Features	1	2	3	4	5	6	7	8	9	10	11
1 A feed	-										
2 D feed	-0.16	-									
3 E feed	-0.15	0.46	-								
4 A and C feed	-0.58	0.29	0.15	-							
5 Reactor feed rate	-0.15	0.29	0.15	0.64	-						
6 Reactor pressure	-0.49	0.14	0.0054	0.48	0.25	-					
7 Reactor level	0.12	0.0081	0.32	-0.68	-0.52	-0.18	-				
8 Purge rate	0.13	0.15	0.29	0.14	0.24	-0.35	-0.076	-			
9 Product separator temperature	0.46	-0.083	0.056	-0.35	-0.16	-0.94	0.11	0.45	-		
10 Product separator pressure	-0.49	0.16	0.032	0.49	0.26	1	-0.19	-0.35	-0.93	-	
11 Product separator underflow	0.1	-0.17	-0.24	-0.2	-0.15	-0.13	0.038	-0.042	0.033	-0.14	-

The results are presented in Table 5. They show that a fully connected neural network provides the best solution of the problem. The graph in Fig. 4 presents the recall with which the neural network classifies the different classes.

Table 5. Accuracy of different methods on the Tennessee Eastman dataset

Method	Accuracy
Logistic Regression	0.46
Lasso	0.46
SVM	0.57
Decision Tree	0.23
Adaptive Boosting	0.34
Gradient Boosting	0.46
Random Forest	0.67
Fully Connected Neural Network	0.82

Then, the same methods were used on the Gas Pipeline dataset. Since gaps are common in this dataset (among the values of the features describing the process state), and the values of different features have significantly different scales, the data were preprocessed. Different ways of processing the gaps were tested, and as a result, the method used in [11] was chosen, in which the empty values of features were replaced with the feature values that occurred in the past. Such an approach assumes that although data are missed, this happens only because they cannot be represented in the network packet for some reason. Therefore, gaps are filled with the previous values of the corresponding features.

After all the gaps were filled, the data were divided into training and test samples in the ratio of 80%: 20%. All features were normalized to the training sample. In the case of the Gas Pipeline dataset, all the considered methods were tested both on the full set of features and on abbreviated set, which included only features describing the state of the process.

Table 6. Accuracy of different methods on the Gas Pipeline dataset with all features

Method	Accuracy (all features)	Accuracy (Industrial process features)
Logistic Regression	0.8062	0.7808
Lasso	0.8076	0.7808
SVM	0.9022	0.7889
Decision Tree	0.9502	0.7866
Adaptive Boosting	0.7925	0.7813
Gradient Boosting	0.8270	0.7877
Random Forest	0.9823	0.7850
Fully Connected Neural Network	0.9528	0.7981

The problem presented 36 classes: the normal state of the system and 35 different attacks. The results of the experiment are shown in Table 6. As can be seen from Tables 6 and 7, when using only features describing the state of the industrial process, the accuracy of all methods drops significantly.

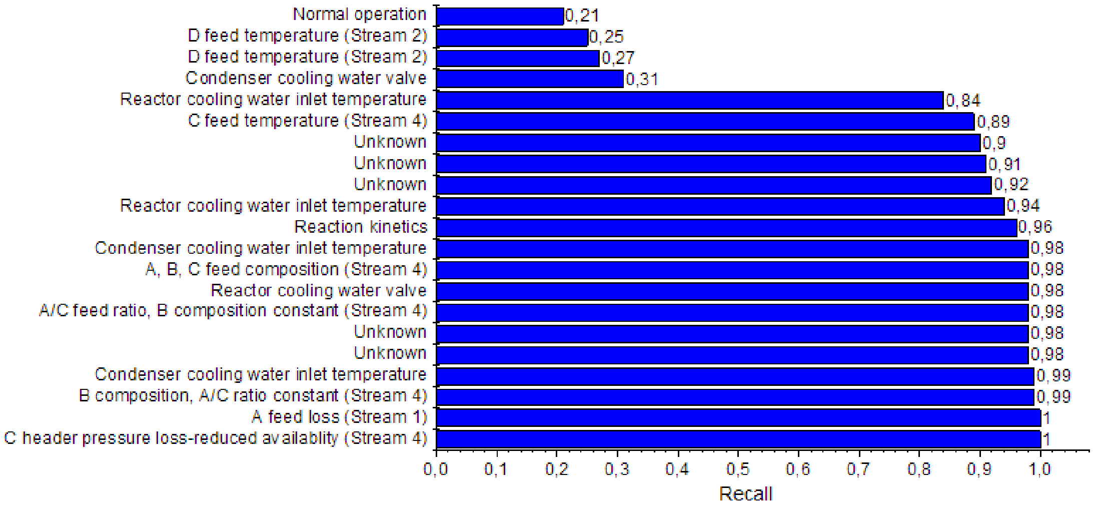

Figure 4. Recall of a fully connected neural network on different classes (Additional Tennessee Eastman ...)

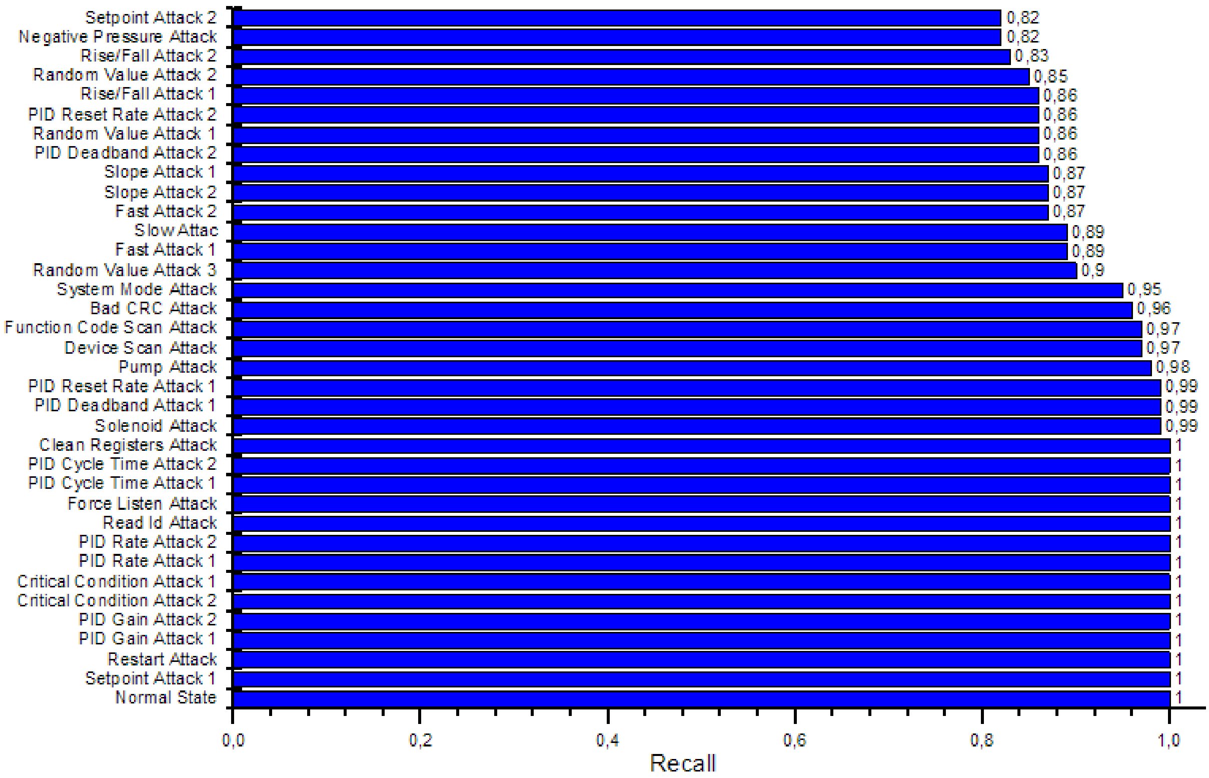

Figure 5. Recall of Random Forest on different classes (Gas Pipeline)

In the case of using all available features, the best accuracy was achieved using a Random Forest. For this reason, Fig. 5 presents a graph showing the recall with which the Random Forest classifies the various attacks and the normal state.

In addition, to detect attacks, recurrent neural networks based on the LSTM and GRU architectures were also tested on the Gas Pipeline dataset. Since recurrent neural networks process data sequences, the training and test samples were transformed into sequences. It makes sense to take the sequence length a multiple of four since four packets corresponding to the operations of reading and writing data on the process state are constantly repeated in the network traffic. In conducted experiments, the length of the sequence was eight records.

After preprocessing the data and normalizing the features, the LSTM and GRU networks were tested to detect attacks. The data were divided into two classes: normal traffic and attack. Several iterations of learning and validation allowed us to select optimal hyperparameters for each network. The results obtained in the experiments for the LSTM and GRU networks are presented in Table 7. For comparison, Figures 6 and 7 demonstrate the graphs of accuracy and loss functions for the LSTM and GRU networks at the learning stage.

Table 7. LSTM and GRU results

Architecture	Accuracy	Precision	Recall
LSTM	0.9068	0.9042	0.9068
GRU	0.9170	0.9177	0.9170

6. ANALYSIS OF THE RESULTS

From the experiments, it follows that the detection of anomalies arising in the ICS operation as a result of cyber attacks should be performed using not only the process state data, but also information on networks interactions between the ICS components. In particular, the experiments on the abbreviated Gas Pipeline dataset showed accuracy close to 0.78, which indicates that algorithms can distinguish only the normal state of an ICS, but they can't classify attacks correctly.

The experiments also demonstrated that linear algorithms are generally poorly suited to both detecting process anomalies and detecting anomalies of an ICS as a whole. In cases of Lasso and Logistic Regression, despite a small number of coefficients in a linear model and possibility to achieve the maximum accuracy for such algorithms on a small subset of the training set, an acceptable accuracy could not be obtained even after a long learning process. In case of SVM, the acceptable accuracy on Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation dataset was not achieved (0.57), apparently due to excess amount of features. Results of SVM on Gas Pipeline dataset (which has fewer number of features) are much better (0.9022).

The decision tree applied to the Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation dataset turned out to be highly subject to overtraining: it was easy to choose such parameters of the algorithm that it could work exactly on the training data, but show much worse results on the test data. In this regard, it is expedient to use more advanced decision tree algorithms and their modifications. Thus, Random Forest, Adaptive Boosting and Gradient Boosting show much lower accuracy on the training data, but generalize the real industrial process much better. This has a positive effect on the accuracy of predictions, which is in the range from 0.23 to 0.67.

In case of Gas Pipeline dataset, the best accuracy score was achieved using a Random Forest (0.9823) while other methods based on the decision tree concept had worse or comparable results. Fig. 5 shows that the Random Forest recognized correctly most objects in most classes, proving to be the best method considered for anomaly detection in the ICS operation in case of a relatively small number of features. However, the amount of RAM needed for training and operation of algorithms based on decision trees depends polynomially on the size of the training set, which can significantly worsen the running time in case of a large amount of data.

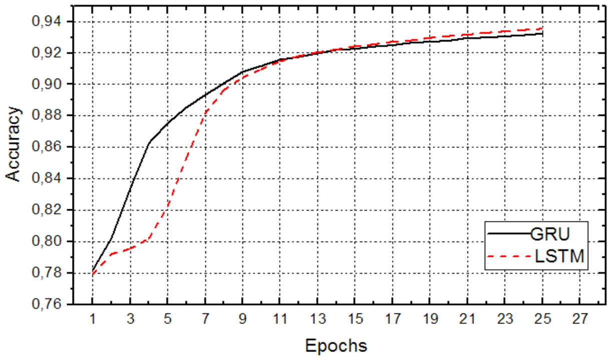

Figure 6. Accuracy of GRU and LSTM networks

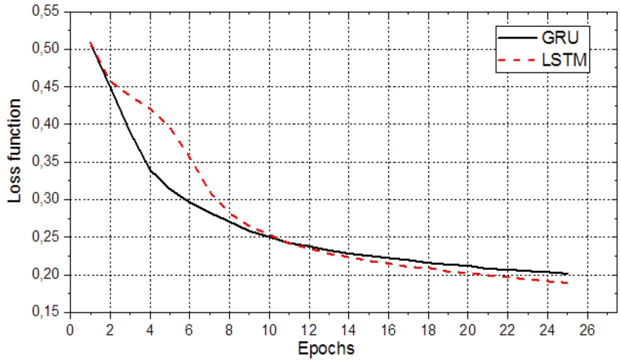

Figure 7. Loss function of GRU and LSTM networks

The best result on the Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation dataset (0.82) was attained by deep learning of the fully connected neural network. However, as it is shown in Fig. 4, the network is mediocre in recognizing the normal state, so it cannot be implemented in practice. In this case, a possible way to increase accuracy is to decompose the original problem into several simpler ones. For example, the industrial process can be divided into separate stages, and anomalies can be detected at each stage.

On the Gas Pipeline dataset, the fully connected neural network allowed for an accuracy of 0.9528, which is not the best result. Apparently, the reason for this is the amount of data. Perhaps, if the size of the training set were comparable with the size of the sample built from the Additional Tennessee Eastman Process Simulation Data for Anomaly Detection Evaluation dataset, the result would be better.

The results show that the performance of the LSTM and GRU networks in detection of attack presence is comparable, and there is no significant difference between the accuracy of different architectures, though the GRU network provided slightly better results. The graphs of accuracy and loss function in Figures 6 and 7 demonstrate that, during the first 11 epochs, the GRU network learns faster than the LSTM network, but later, after the 12th learning epoch, the situation changes. At about the same time, there is an overtraining effect. Generally, the GRU network learns and operates a little faster, since due to the absence of a state cell, fewer operations are required per epoch. Therefore, in case of the Gas Pipeline dataset, the GRU network is a better solution than the LSTM network. Nevertheless, if there are no limitations on computation power and there is a big set of training data, the use of the LSTM is preferred.

7. CONCLUSION

Despite the described shortcomings, the deep learning models showed the highest efficiency in detecting anomalies in the process compared to linear algorithms and algorithms based on decision trees. In case of detecting anomalies in the work of ICS as a whole, including the data describing networking, the results were not the best, but acceptable. For more data, the accuracy would probably be higher. Therefore, it can be argued that the use of deep learning is a promising way to improve the ICS security and to solve problems associated with the transition towards an Industry 4.0. However, it is also possible to predict that in the future, in order to obtain more practical results, the solutions proposed by the researchers will become more complex and will combine different techniques and machine learning concepts.

As further research directions, it is proposed to try to find a fully connected neural network architecture that would be better able to detect anomalies in the process. In addition, it is possible to attempt to apply convolutional and recurrent architectures of neural networks. Thus, the paper considered recurrent neural networks with the LSTM and GRU architectures in order to detect the presence of an attack. The obtained results indicate that recurrent neural networks can be used for intrusion detection in ICS. However, to obtain practically applicable results, a more thorough study is required.

To improve accuracy, it may also be useful to combine different methods of machine learning, for example, neural networks and decision tree algorithms.

In addition, within the framework of the described approach, it is planned to consider various ways of decomposing the problem of detecting anomalies in the process, since this may help in obtaining the results that can be implemented in practice.

ACKNOWLEDGEMENT

The work was supported by Act 211 Government of the Russian Federation, contract № 02.A03.21.0011.

REFERENCES

[1] Byres, E.: The air gap: SCADA's enduring security myth: Attempting to use isolation as a security strategy for critical systems is unrealistic in an increasingly connected world, Communications of the ACM, Vol. 56, Issue 8, pp. 29-31, 2013.

[2] Luiijf, E.: Cyber (in-) security of industrial control systems: A societal challenge in *International Conference on Computer Safety, Reliability, and Security*, 23-25.09.2015, Delft, pp. 7-15.

[3] Falliere, N., Murchu, L.. O., Chien, E.: W32.stuxnet Dossier, White paper, Symantec Corp., Security Response, T. 5, No. 6, 2011.

[4] Lee, R. M., Assante, M. J., Conway, T.: German steel mill cyber attack, Industrial Control Systems, Vol.30, 2014.

[5] Lee, R. M. et al.: Analysis of the cyber attack on the Ukrainian power grid, Electricity Information Sharing and Analysis Center, 2016.

[6] Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., Vazquez E.:Anomaly-based network intrusion detection: Techniques systems and challenges, Computers & Security, vol. 28, no. 1-2, pp. 18-28, 2009.

[7] Radojević, N., Kostadinović, D., Vlajković, H. and Veg, E.: Microclimate control in greenhouses, FME Transactions, Vol. 42, No. 2, pp. 167-171, 2014.

[8] Todorović, M. N., Ristanović, M. R., Lazić, D. V., Galić, R. D., and Bajc, T. S.: A novel laboratory set-up for investigation of intelligent automatic control in complex HVAC systems, FME Transactions, Vol.44, No. 1, pp. 65-70, 2016.

[9] Shirazi, S. N. et al.: Evaluation of anomaly detection techniques for SCADA communication resilience, in *Resilience Week (RWS)*, 16-18.08.2016, Chicago, pp. 140-145.

[10] Mansouri, A., Majidi, B., Shamisa,. A.: Metaheuristic neural networks for anomaly recognition in industrial sensor networks with packet latency and jitter for smart infrastructures. International Journal of Computers and Applications, pp.1-10, 2018.

[11] Lopez Perez, R., Adamsky, F., Soua, R. and Engel, T.: Machine Learning for Reliable Network Attack Detection in SCADA Systems, in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE),* 01-03.08.2018, New York, pp. 633-638.

[12] Demertzis, K., Iliadis, L. and Spartalis S.: A Spiking One-Class Anomaly Detection Framework for Cyber-Security on Industrial Control Systems, in *International Conference on Engineering Applications of Neural Networks*, 25-27.08.2017, Athens, pp. 122-134.

[13] Sharma, S., Agrawal, J., Agarwal, S. and Sharma S.: Machine learning techniques for data mining: A survey, in *IEEE International Conference on Computational Intelligence and Computing Research,* 26-28.12.2013, Enathi, pp. 1-6.

[14] Ruiz, Z., Salvador, J., and Garcia-Rodriguez, J.: A Survey of Machine Learning Methods for Big Data, in *International Work-Conference on the Interplay Between Natural and Artificial Computation,* 19-23.06.2017, Corunna, pp. 259-267.

[15] Deng, L. and Yu, D.: Deep learning: Methods and applications, Foundations and Trends in Signal Processing, Vol. 7, No. 3–4, pp. 197-387, 2014.

[16] Hochreiter, S. and Schmidhuber, J.: Long Short-Term Memory, Neural Computation, Vol. 9, No. 8, pp. 1735-1780, 1997.

[17] Cho, K., Van Merriënboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H., and Bengio, Y.: Learning phrase representations using RNN encoder-decoder for statistical machine translation, in *Conference on Empirical Methods on Natural Language Processing*, 25-29.10.2014, Doha, pp. 1724-1735.

[18] Rieth, C. A., Amsel, B. D., Tran, R., and Cook, M. B.: Issues and Advances in Anomaly Detection Evaluation for Joint Human-Automated Systems, in *International Conference on Applied Human Factors and Ergonomics*, 17-21.07.2017, Los Angeles, pp. 52-63.

[19] Downs, J. and Fogel, E.: A plant-wide industrial process control problem, Computers and Chemical Engineering., Vol. 17, No. 3, pp. 245-255, 1993.

[20] Morris, T. H., Thornton, Z. and Turnipseed, I.: Industrial control system simulation and data logging for intrusion detection system research, in *7th Annual Southeastern Cyber Security Summit*, 03-04.07.2015, Huntsville, pp. 1-6.

[21] Morris, T. H., Gao, W.: Industrial control system cyber attacks, in *Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research*, 16-17.09.2013, Leicester, pp. 22-29.

ПРИМЕНА МЕТОДА МАШИНСКОГ УЧЕЊА У ЗАДАТКУ ДЕТЕКЦИЈЕ НАПАДА И УПАДА (ИНТРУЗИЈЕ) НА ОСНОВУ АНАЛИЗЕ СТАЊА ИНДУСТРИЈСКОГ ПРОЦЕСА И УМРЕЖАВАЊА СА СИСТЕМОМ ИНДУСТРИЈСКЕ КОНТРОЛЕ (СИК)

А. Соколов, И. Пјатницки, С.А. Ачлбугин

Модерни Системи Индустријске Контроле (СИК) све више постају мета сајбер напада. Традиционални сигурносни алати засновани на приступу потписа не могу увек открити нови напад, чији потпис још није описан. То се нарочито дешава током циљаних напада на индустријске објекте. Сајбер напади могу проузроковати аномалије у раду индустријског контролног система и процесне опреме под њеном контролом.

Стога је за откривање напада препоручљиво користити приступ заснован на откривању аномалија. Разуман начин за имплементацију овог приступа је употреба техника машинског учења. Рад се бави најчешћим методама машинског учења (алгоритми стабала одлучивања, линеарним алгоритмима, векторском машином) и неуронским мрежама. Да би се проценила њихова применљивост у проблему откривања СИК аномалија, коришћени су подаци Додатних Симулационих Података Тенеси Истман Процеса за Процену Аномалије и подаци гасовода.