Detection of network attacks in cyber-physical systems using a rule-based logical neural network

Vira Titova[1,*,†], Yurii Klots[1,†], Victor Cheshun[1,†], Nataliia Petliak[1,†] and Abdel-Badeeh M. Salem[2,†]

[1] *Khmelnytskyi National University, 11 Institutska Street, Khmelnytskyi, 29000, Ukraine*
[2] *Ain Shams University, Egypt*

Abstract

This article discusses the network attacks detection in cyber-physical systems using neural networks based on logical rules. The object of the study was cyber-physical systems of varying degrees of heterogeneity. The study purpose is the cyber-physical system functioning process in a normal state and under conditions of network attacks on it.

The authors analyzed the most common methods of presenting data circulating in cyber-physical systems and highlighted the main advantages and disadvantages of using each method. The authors also reviewed the most common network attacks detecting methods in cyber-physical systems and identified the advantages and disadvantages of these methods.

As a result of the work, taking into account the previous analysis, a method of detecting network attacks in cyber-physical systems based on the use of a rule-based logical neural network was developed, implemented and researched. The authors also evaluated the accuracy of the method.

Keywords

Multivariate Time Series, Cyber-Physical Systems, Neural Networks, Rule-based Logic, Network Attacks

1. Introduction

Cyber-physical system (CPhS) are used in many different sectors and critical infrastructures, including manufacturing, distribution and transportation.

A typical CPhS structure contains remote diagnostic tools, multiple control and redundancy loops, a user interface for input/output, logging, maintenance and supervisory control tools. Often, implementations of these tools are performed on multiple network protocols using multi-layer networking paradigms and architectures.

Control loops typically use data obtained from actuators, sensors, and programmable logic controllers. Sensors in this context are understood as devices that measure some physical quantity, property and/or parameter and then send the resulting data of fixed discrete

ICyberPhyS-2024: The 1st International Workshop on Intelligent and CyberPhysical Systems, June 28, 2024, Khmelnytskyi, Ukraine

* Corresponding author.
† These authors contributed equally.
titovav@khmnu.edu.ua (V. Titova); klots@khmnu.edu.ua (Y. Klots); cheshunvn@khmnu.edu.ua (V. Cheshun); npetlyak@khmnu.edu.ua (N. Petliak); abmsalem@yahoo.com (Abdel-Badeeh M. Salem);
0000-0001-8668-4834 (V. Titova); 0000-0002-3914-0989 (Y. Klots); 0000-0001-5971-4428 (V. Cheshun); 0000-0002-3935-2068 (N. Petliak); 0000-0003-0268-6539 (Abdel-Badeeh M. Salem)

variables to a logic controller for subsequent processing. Next, the logical controller processes the received data and generates the necessary commands, based on the final algorithms and control and decision-making mechanisms. The received commands are sent to the input of actuators, which are used to control controlled processes.

The end observer (operational engineer) can interact with the input/output and display interfaces to obtain current data about the state of the system. It is also possible to manually configure set values or scheduled events, change control and/or operating algorithms. The user interface can additionally be used for communication with neighboring devices or remote control of the latter. It is common practice to use diagnostic and maintenance utilities to prevent, identify, and resolve abnormal operation or failures.

Often, control loops are executed in a modular hierarchy: they can be either nested or executed in cascade, while the given values may be indirectly dependent on the values used between the loops if the system is not implemented in a single-level process execution. Lower-level circuits usually operate continuously from the beginning of the technical process until its end, and the execution time of a given circuit can range from several machine cycles to several days. Figure 1 shows a typical logical structure of the CPhS and the operations performed on it [1, 2, 3].

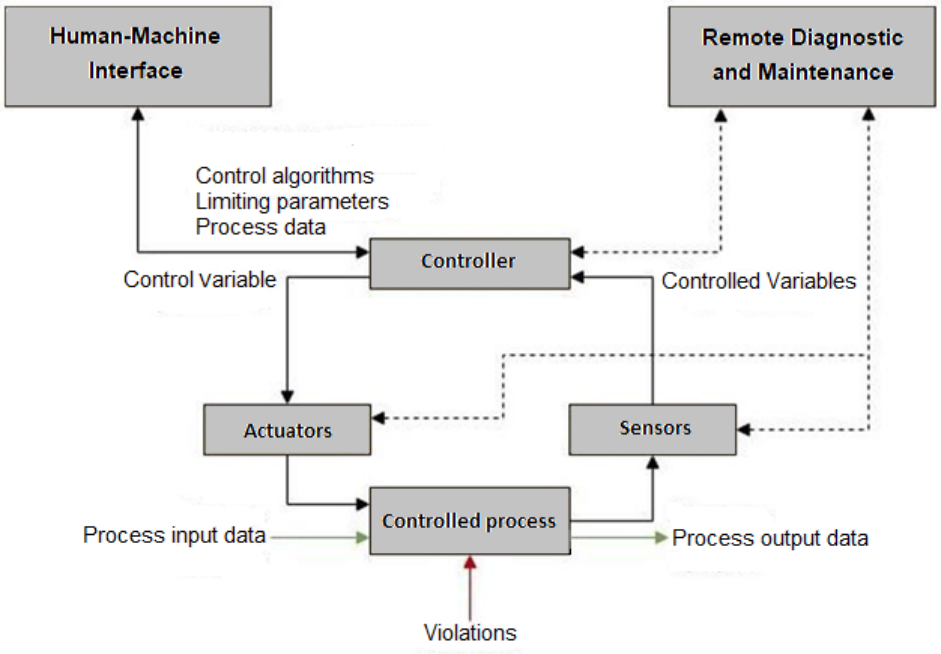

Figure 1: Logical structure of the CPhS.

When developing the logical structure of the functioning and/or interaction of the CPhS, it is worth observing the principle of isolation: separation of the end-system network from the corporate, enterprise or global network. The functional component of circulating commands in networks varies - access to the global network, mail servers, data exchange and remote access are usually legitimate in an enterprise network, but clearly should not have a place in special-purpose CPhS. In an enterprise network, it is acceptable to lack strict procedures for monitoring the configuration of network equipment, policies for updating and operating software, etc. However, if you allow access to CPhS from the global network, additional risks

in the operation of the CPhS could arise: the possibility of network attacks, illegitimate access and changes in functioning, etc.

Practical considerations, such as the cost of setting up a public Internet connection or maintaining a flat network infrastructure, often mean that a connection between the CPhS and corporate networks is required. This connection poses a significant security risk and must be secured. If networks must be connected, it is highly recommended to allow only minimal connections and establish the connection through a firewall and DMZ (Demilitarized Zone). It is recommended to place servers that process CPhS data, which can be accessed from the enterprise network, in a DMZ.

From the above, the following main components of the CPhS security architecture can be identified [4]:

1. Network segmentation. Dividing the CPhS into security domains and separating it from other networks, such as the corporate network. Each network is divided into critical parts after an analysis of operational risk. Segmentation involves dividing a network into smaller networks.
2. Protecting the boundaries of security domains. Edge protection devices manage the flow of information between security domains to protect the CPhS from cyberattacks, unauthorized logical and physical errors and accidents.
3. Firewalls. These software packages allow you to administer network flows within target systems based on selected security policies.
4. Intrusion detection systems.
5. Layered architecture. Its includes the use of firewalls, demilitarized zones, and intrusion detection capabilities.
6. Authentication and authorization.
7. Monitoring, logging and auditing. These architectural elements are necessary to understand the current state of the CPhS and confirm that the system is operating normally, correctly and in normal mode.
8. Abnormal operation detection, response and system recovery.

2. A problem formulation

The use of the security mechanisms described above allows you to divide the enterprise network into zones with different security policies, control the flow of information transmitted from one zone to another, and detect unauthorized access to the enterprise network, anomalous conditions and network attacks. Also, thanks to the introduction of defense in depth, it provides a fairly high level of security due to redundancy. However, some CPhS security threats may provide the opportunity for a successful attack even if all of the previously listed security mechanisms are in place. Such threats include: human factor, vulnerabilities of existing protocol implementations, vulnerabilities of firewalls and edge protection equipment, zero-day vulnerabilities, etc. That is, an attacker has the potential to gain full access to the operator's terminal and manipulate input values to disrupt the normal flow of physical and logical processes of the system.

Thus, attacks are possible in which none of the security mechanisms detects a violation - the only data on the basis of which anomalies can be detected are indicators of the current state of processes. Since the restoration of physical processes is extremely difficult and

expensive, it is necessary to detect an anomaly as early as possible. This article is dedicated to this task.

3. Overview of existing solutions

Detection of anomalies in the flow of processes on a cyber-physical system of an enterprise can be based on the methods of presenting data within the system. Creating a full-fledged model of complex physical processes is a very non-trivial task: such an approach requires a deep understanding of the system and its implementation, and, consequently, an individual approach to each system separately or to a certain set of typical systems. In practice, they are often limited to methods for detecting anomalous CPhS states, based on methods of data presentation and their processing.

Based on their descriptive nature, methods of presenting data in CPhS can be fundamentally divided into those using:

- multivariate time series without transformation with subsequent analysis;
- compressed, aggregated or otherwise processed multivariate time series;
- fractal representation of the system topology;
- graph structures of different types.

In [5, 6, 7], the proposed approach considers data from actuators, PLCs (programmable logic controllers), and sensors. The authors of these works perform transformations of data received from the CPhS, the latter are converted into multidimensional time series. The use of multivariate time series is justified by the following principle: this method retains greater information content for further analysis by preserving connections between devices. In order to identify deviations in the operation processes of the CPhS, a forecast of the following state of the system is performed using a trained multidimensional time series forecasting model. The input of the model is the readings of the current state, and the output is the predicted result. Next, the divergence is calculated - the difference between the real value of the CPhS state and that predicted using the trained model. If the divergence value is above the threshold value, the system detects an abnormal condition.

To predict the state of system components, in [8, 9, 10] it is used the mathematical apparatus of the Kalman filter, which has found wide application in problems of predicting the coordinates of a body moving in space. The data of the system components are presented in the form of a chaotic trajectory of motion of a certain body with variable speed in one-dimensional space using the classical physical equations of path, speed and acceleration of a material point.

The authors in [11, 12] followed different approaches. They propose to analyze the traffic received in the CPhS using discrete wavelet transform (DWT) of the sequence of data received from the inspected packets. Additionally, the authors perform a statistical analysis of various parameters of network packets obtained from the CPhS.

In [13, 14], the authors use the method of multifractal data analysis to identify anomalies in the traffic of backbone networks. According to the authors, this approach adequately detects network problems or attacks. The values of the characteristics of the multifractal spectrum are used as signal metrics.

The work [15, 16] considers the possibility of using classical graph structures to model the network infrastructure of complex large-scale objects (including critical ones. The authors also supplement classical graphs with the target function of the object and unary operations on the graph, reflecting cyber-attacks.

In works [17, 18], the authors consider a graph-event model for presenting data in CPhS. This approach allows you to analyze the behavior of programs based on events generated during the operation of the system. The authors also present the system architecture and list the events that are monitored at the appropriate levels. Additionally, metrics are analyzed that allow one to evaluate the similarity of the resulting graph and the structure of the graphs of given applications. Experimental results are presented that illustrate the effectiveness and accuracy of the developed approach.

The methods most suitable for CPhS include event graphs, signal graphs and their combination with multidimensional time series. For greater clarity, the main advantages and disadvantages of methods for presenting data in the CPhS, additional notes and other materials are given in Table 1.

Analyzing the mechanisms, tools and mathematical apparatus used in methods for detecting network attacks aimed at CPhS, the following approaches can be distinguished in principle:

- assessment of system self-similarity criteria;
- prediction of the system state based on statistical tools;
- prediction of system state based on machine learning.

Advantages of the first [19, 20] and second methods [21, 22]:

- high speed of processing results;
- low demands on the system's computing resources;
- high accuracy of assessment in short time intervals – positive results in cases of detecting anomalies of short duration.

Disadvantages of the first [19, 20] and second methods [21, 22]:

- weak analysis or complete absence of analysis in the low-level segment of the system;
- the difficulty of detecting long-term anomalies, provided they appear smoothly and have a relatively low growth rate.

Advantages of the third method [23, 24, 25]:

- high variability of the designs used and, as a result, the possibility of choosing between speed, quality and resource requirements of the system;
- the possibility of the most in-depth and reliable detection of anomalies in the system low-level segment;
- the ability to put the most in-depth analysis and improve the level of system security.

Disadvantages of the method [23, 24, 25]:

- initial complexity of settings;
- the need for system training;
- increased requirements for system resources in comparison with all other solutions;
- impossibility of transferring the trained model to a new topology (unlike most other approaches), the need for retraining.

Table 1
Main characteristics of methods for presenting data in CPhS

Task\Method of representation	Time series	Kalman algorithm	DWT	Fractals	Graphs
Variability	+	+	+	-	+
Short-term attacks	+	+	+	+	+
Long-term attacks	+	+	-	+	+
Data Aggregation	+	+	+	+	+
Performance	+	+	+	+	+
Accounting for nonlinear processes	+	+	-	-	-
Accounting for the system topology	+	-	-	+	-

Based on the foregoing, the authors recommend focusing on solutions based on the use of machine learning due to increased variability, in particular, artificial neural networks [26].

4. Method for detecting network attacks on CPhS, based on the use of a rule-based logical neural network

After a thorough analysis of the existing methods of presenting data in CPhS, the advantages of these methods, their disadvantages and areas of application, we can proceed to the development and implementation of our method of detecting network attacks in CPhS.

The described method is based on processing the received time series from CPhS actuators and sensors, using a logical neural network to predict the following state of the system and calculating the divergence between the predicted and real values.

The data processing and aggregation included the following steps:

1. Assigning identification numbers to each of the devices (id, numbering was performed arbitrarily, but maintaining the logical connection “sender-receiver”).

2. Changing the status indicators for those devices that cannot measure the degree of their "load", but can measure the degree of power discharge.

Considering the previously discussed existing data presentation methods advantages and disadvantages, the authors decided to focus on the use of multivariate time series. The main reasons for this are: used data used variability, the possibility of manual adjustment of the solver parameters and high degree of method variability.

When using multivariate time series, a neural network is usually trained on valid data to predict the system following state and calculate the divergence between the predicted and actual state. By analyzing the divergence, anomalous states in the system are detected.

A classic multivariate time series is the following set:

$$X = \{X^{(1)}, X^{(2)}, \dots, X^{(m)}\},$$

where each value at time ti is represented by a vector:

$$X = \{x_1^{(i)}, x_2^{(i)}, \dots, x_n^{(i)}\}$$

For ease of use the initial data received from system objects are normalized as follows:

$$x_i = \frac{x_i - x_{min}}{x_{max} - x_i}$$

The CPhS system under consideration included 3 devices, each with 3 basic characteristics: the object state, the object load, the object physical data measured. Based on these parameters, the load level of a particular device is determined. The system load is determined by the maximum load value among all devices.

Figures 2-4 provide examples of displaying normalized data about the state of the system during 24 hours, includes its operation in a normal state and in anomalous behavior.

The collected statistics became the basis for creating training and test samples.

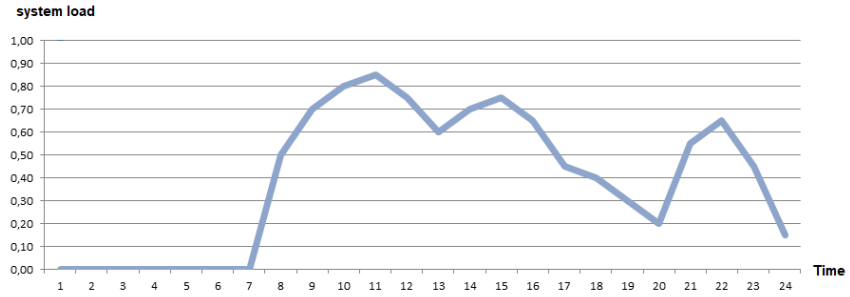

Figure 2: Example of system operation in normal state.

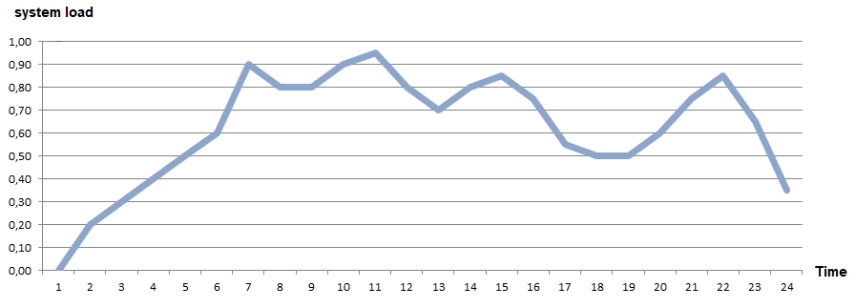

Figure 3 Example of system operation with Backdoor attacks.

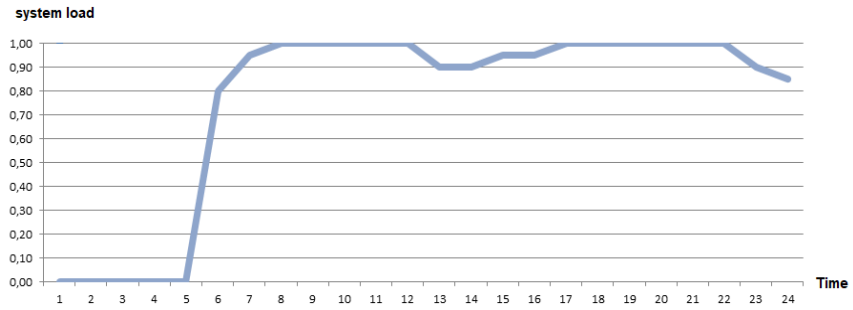

Figure 4 Example of system operation with DoS attacks.

Based on previous studies, it was evident that multivariate time series are the best used with neural networks due to the fact that the latter have shown quite high accuracy in detecting network attacks when combined with the use of this data description method in CPhS.

To avoid the previously listed disadvantages of using neural networks, especially the initial complexity of settings and the topology compiling complexity of the neural network, the authors was decided to use a rule-based logical neural network.

The structure of this network is shown in Figure 5.

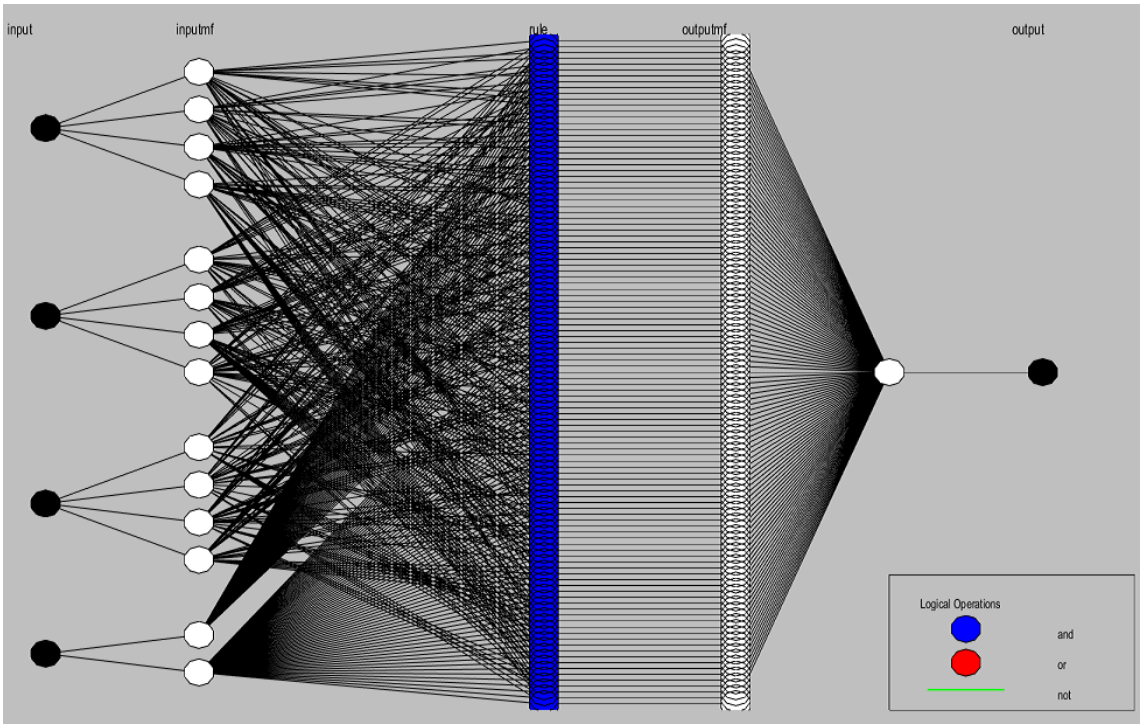

Figure 5 Neural network structure.

The neural network has 5 inputs, four of which receive data on the load of each device, obtained by converting the characteristics of the device using a clock series. The fifth input supplies data about the current time. The only output of the neural network determines the

predicted load value of the system as a whole and, based on this, makes a conclusion about the presence/absence of an attack.

The results of the developed neural network work are presented in the form of surfaces (Fig. 6 and Fig. 7).

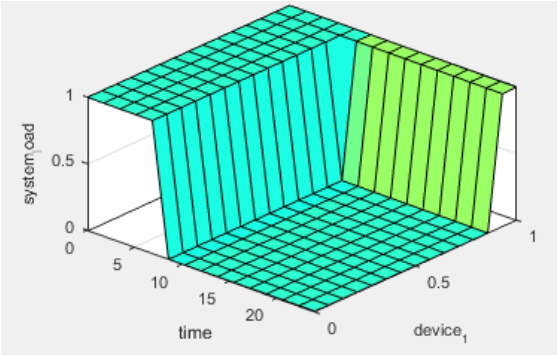

Figure 6 Results for the ratio device 1/time.

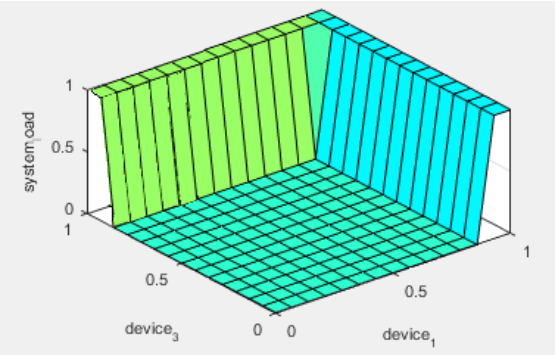

Figure 7 Results of work for the ratio device 1/device 3.

The described method is based on processing the resulting multidimensional time series, compiled from data circulating within the CPhS, predicting the following state of the system using a logical neural network and analyzing the divergence that arise - the discrepancies between the real values of the system state and the predicted ones.

The methods include 2 stages - preparatory and working. The preparatory stage is aimed at automatically training the neural network and involves the following steps:

1. Preparation of test data - normalization and compilation of multivariate time series.
2. Transfer of input data in the form of a multidimensional series to the input of a neural network.
3. Training the neural network on the transmitted data until the specified accuracy is achieved on the test data.

The working stage involves the direct detection of network attacks aimed at the CPhS and includes the following steps:

1. Preparation of real data from a functioning CPhS – normalization and compilation of multidimensional time series.
2. Transfer of input data in the form of a multidimensional series to the input of a neural network.
3. Prediction of the following state of the system by a neural network based on inputted multidimensional time series.
4. Calculation of the divergence between the predicted system state and the real one.
5. Recording the presence or absence of attacks on the CPhS based on the received divergence.

As previously noted, data that has undergone the normalization procedure must be preprocessed: for all points in the time series, a predicted value is determined, as shown in Figure 8.

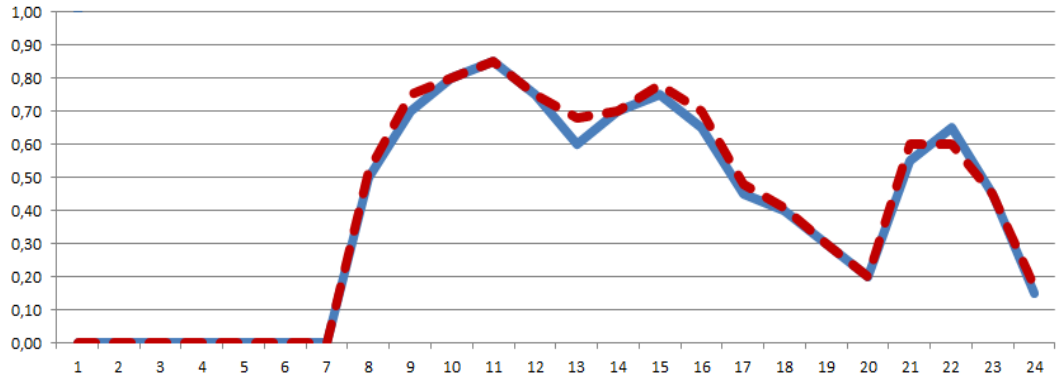

Figure 8 Example of system state prediction.

To assess the developed method accuracy, the following parameters were calculated:

1. Accuracy: A = (TP + TN) / (P + N);
2. Precision: Pr = TP / (TP + FP);
3. True Positive Rate: TPR = TP / (TP + FN);
4. True Negative Rate: TNR = TN / (TN + FP);
5. False Positive Rate: FPR = FP / (FP + TN);
6. False Negative Rate: FNR = FN / (FN + TP);
7. Positive Predictive: $PPred$ = 1 − FP / (FP + TP);
8. Negative Predictive: $NPred$ = TN / (TN + FN);
9. F-Score = $2TP$ / ($2TP + FP + FN$);

where TP – the number of correct detections system normal state (True Positive); TN – number of correct detections of attacks on the system (True Negative); FP – number of unrecognized attacks (False Positive); FN – the normal system states number recognized as attacks (False Negative); P – total number of normal CPhS states (Positive); N – total number of CPhS states, including attacks (Negative).

Below are the values for all considered time periods in the form of tables. These values are broken down by attack type. After each table with the results of calculations, the authors give conclusions about the accuracy of the developed method.

On the segment without attacks, the overall accuracy (Precision) turned out to be equal to one. According to the authors, this result is due to the false positives (FP) absence, since there were no attacks in this segment. The closeness of the solution (accuracy) allowed the authors to conclude that some disagreement (FN) was present – but the model was not retrained.

Table 2
Received data in the “without attacks” segment

Parameters	Values	Parameters	Values
All	86 400	Accuracy	0,90
Positive	86 400	Precision	1,00
Negative	0	True Positive Rate	0,90
True Positive	77 414	True Negative Rate	-
True Negative	0	False Positive Rate	-
False Positive	0	False Negative Rate	0,10
False Negative	8 986	Positive Predictive	1,00
		Negative Predictive	0,00
		F-Score	0,95

Analyzing the “DoS attack” segment, we can say that here the method showed positive results. These are confirmed by high closeness of solutions (Accuracy) and high general accuracy of classification (Precision). False Positive Rate is less than 0.1 and False Negative Rate is less than 0.1, both are very close to each other. This indicates that the false detection rate is a small fraction of the total number of attacks.

Table 3
Received data in the “DoS attack” segment.

Parameters	Values	Parameters	Values
All	86 400	Accuracy	0,92
Positive	34 747	Precision	0,89
Negative	51 653	True Positive Rate	0,93
True Positive	32 258	True Negative Rate	0,92
True Negative	47 644	False Positive Rate	0,08
False Positive	4 009	False Negative Rate	0,07

False Negative	2 489	Positive Predictive	0,89
		Negative Predictive	0,95
		F-Score	0,91

In the segment with Backdoor attacks, the method showed the lowest accuracy (Precision) and proximity of solutions (Accuracy). About a third of the attacks were incorrectly classified by the system as a normal CPhS state. The authors explain this by the fact that in this case, backdoor attacks were understood as resending the package after certain time intervals. To improve the performance of the method, the authors recommend using additional attack detection criteria or using an event handler to retransmit previously received packets.

Table 4
Received data in the "Backdoor attacks" segment.

Parameters	Values	Parameters	Values
All	86 400	Accuracy	0,79
Positive	55 829	Precision	0,84
Negative	30 571	True Positive Rate	0,84
True Positive	47 065	True Negative Rate	0,70
True Negative	21 523	False Positive Rate	0,30
False Positive	9 048	False Negative Rate	0,16
False Negative	8 765	Positive Predictive	0,84
		Negative Predictive	0,71
		F-Score	0,84

5. Conclusions

The work results are the development, implementation and research of the implemented method of detecting network attacks in the CPhS. The method involves using a rule-based logical neural network.

Detection of network attacks carried out on the CPhS consists of the following stages:

1. Data are processed and presented in the form of multidimensional time series
2. Developing a neural network based on the plural of rules.

3. Training a developed neural network on a test samples.
4. Prediction of the following state of the system.
5. Calculation of the divergence between the predicted and actual states of the system.

The average value of accuracy (Precision; 0.91) and proximity of solutions (Accuracy; 0.87), as well as the values of False Positive Rate (0.13) and False Negative Rate (0.11) indicate the absence of model overtraining and the method high reliability.

References

[1] M. K. Gautam, A. Pati, S. K. Mishra, B.Appasani, E. Kabalci, N. Bizon, P. Thounthong. A Comprehensive Review of the Evolution of Networked Control System Technology and Its Future Potentials. Sustainability. 2021, 13(5), 2962; https://doi.org/10.3390/su13052962

[2] A. Platzer. Logical Foundations of Cyber-Physical Systems. 2018. doi:10.1007/978-3-319-63588-0.

[3] P. Juhás, K. Molnár. Key Components of the Architecture of Cyber-physical Manufacturing Systems. International Scientific Journal "Industry 4.0". 2017. Issue 5, PP. 205-207.

[4] K. Stouffer, J. Falco, K. Scarfone. Guide to Industrial Control Systems (ICS) Security – Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, URL: doi:10.6028/NIST.SP.800-82.

[5] B. Cao, C. Li, Y. Song,Y. Qin, C. Chen. Network Intrusion Detection Model Based on CNN and GRU. Appl. Sci. 2022, 12(9), 4184; doi:10.3390/app12094184

[6] M. Kravchik, A. Shabtai. Detecting Cyber Attacks in Industrial Control Systems Using Convolutional Neural Networks. 2018. 72-83. doi:10.1145/3264888.3264896.

[7] G. Fortino, C. Greco Claudia, A. Guzzo, M. Ianni. “Identification and prediction of attacks to industrial control systems using temporal point processes”. Journal of Ambient Intelligence and Humanized Computing. 2022. 14. 1-13. 10.1007/s12652-022-04416-5.

[8] A.-A. Bouramdane. Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. J. Cybersecur. Priv. 2023, 3(4), 662-705; doi:10.3390/jcp3040031

[9] A. Tummala, R. Inap. A Two-stage Kalman Filter for Cyber-attack Detection in Automatic Generation Control System. Journal of Modern Power Systems and Clean Energy. 2021. 10. doi:10.35833/MPCE.2019.000119.

[10] W. Li, H. Fu, S. Wu, B. Yang, Z. Liu. A Kalman Filter-Based Distributed Cyber-Attack Mitigation Strategy for Distributed Generator Units in Meshed DC Microgrids. Energies 2023, 16(24), 7959; doi:10.3390/en16247959

[11] S. Dyllon, P. Xiao. Wavelet Transform for Educational Network Data Traffic Analysis. Edited by Sudhakar Radhakrishnan, 2018. doi: 10.5772/intechopen.76455.

[12] A. Abu Nassar, W.G. Morsi. “Detection of Cyber-Attacks and Power Disturbances in Smart Digital Substations using Continuous Wavelet Transform and Convolution Neural Networks”. Electric Power Systems Research, Volume 229, 2024, 110157, ISSN 0378-7796, doi:10.1016/j.epsr.2024.110157.

[13] P. Dymora, M. Mazurek. An Innovative Approach to Anomaly Detection in Communication Networks Using Multifractal Analysis. Appl. Sci. 2020, 10(9), 3277; doi:10.3390/app10093277.
[14] G. Sebestyen, A.Hangan. Anomaly detection techniques in cyber-physical systems. Acta Universitatis Sapientiae, Informatica. 2017. 9. doi:10.1515/ausi-2017-0007.
[15] A. Kott, M. Lange, J. Ludwig. "Approaches to Modeling the Impact of Cyber Attacks on a Mission". 2017.
[16] A. Presekal, A. Stefanov, V. Rajkumar, P. Palensky. Attack Graph Model for Cyber-Physical Power Systems Using Hybrid Deep Learning. IEEE Transactions on Smart Grid. 2023. PP. 1-1. 10.1109/TSG.2023.3237011.
[17] A. Berti, J. Herforth, M.S. Qafari et al. Graph-based feature extraction on object-centric event logs. Int J Data Sci Anal, 2023. doi:10.1007/s41060-023-00428-2
[18] L. F. Sikos. Cybersecurity knowledge graphs. Knowl Inf Syst 65, 3511–3531 (2023). doi:10.1007/s10115-023-01860-3.
[19] D. Crémilleux, Visualization for information system security monitoring. Cryptography and Security [cs.CR]. CentraleSupélec, 2019. English. ffNNT: 2019CSUP0013ff. fftel-02872028f
[20] Sun Yu, Liu Xiaorong, Shen Xiaoli. "Computer Network Information Security Monitoring System Based on Big Data Era". Security and Communication Networks. 2022. 1-11. 10.1155/2022/3170164.
[21] F. Yiwei, L. Xiaoling. An online Bayesian approach to change-point detection for categorical data. Knowledge-Based Systems. 2020. 196. 105792. doi:10.1016/j.knosys.2020.105792.
[22] B. Petrik, V. Dubrovin. "Detection of Dos Attacks in Network Traffic by Wavelet Transform". Applied Questions of Mathematical Modelling, 2021, 4(1), 186-196. doi:10.32782/KNTU2618-0340/2021.4.1.20
[23] M. F. Safitra, M. Lubis, H.Fakhrurroja. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability 2023, 15(18), 13369, doi:10.3390/su151813369
[24] W. Wang, F. Harrou, B. Bouyeddou, S.-M. Senouci, Y. Sun. Cyber-attacks detection in industrial systems using artificial intelligence-driven methods. International Journal of Critical Infrastructure Protection, Volume 38, 2022, 100542, ISSN 1874-5482, doi:10.1016/j.ijcip.2022.100542.
[25] M. A. Umer, K. N.Junejo, M. T. Jilani, A. P. Mathur. Machine learning for intrusion detection in industrial control systems: Applications, challenges, and recommendations. International Journal of Critical Infrastructure Protection, Volume 38, 2022, 100516, ISSN 1874-5482, doi:10.1016/j.ijcip.2022.100516.
[26] E. M. Cherrat, R. Alaoui, H. Bouzahir, Score fusion of finger vein and face for human recognition based on convolutional neural network model. *International Journal of Computing*, *19*(1), 2020, 11-19. doi:10.47839/ijc.19.1.1688