Novelty Detection System Based on Multi-Criteria Evaluation in Respect of Industrial Control System

Jan Vávra and Martin Hromada

Tomas Bata University in Zlin
Faculty of Applied Informatics
Zlin
jvavra@fai.utb.cz

Abstract. The industrial processes and systems have become more sophisticated and also adopted in diverse areas of human activities. The Industrial Control System (ICS) or Internet of Things (IoT) have become essential for our daily life, and therefore vital for contemporary society. These systems are often included in Critical Information Infrastructure (CII) which is crucial for each state. Consequently, the cyber defense is and will be one of the most important security field for our society. Therefore, we use the novelty detection approach in order to identify anomalies which can be a symptom of the cyber-attack in ICS environment. To achieve the main goal of the article One-Class Support Vector Machine (OCSVM) algorithm was used. Moreover, the anomaly detection algorithm is adjusted via multi-criteria evaluation and classifier fusion.

Keywords: Cyber Security, Novelty detection, Anomaly Detection, Industrial Control systems, Multi-Criteria Evaluation.

1 Introduction

Emerging development in information and communication technology (ICT) caused critical changes in understanding of the ICT nature. Therefore, increasing interconnection, interdependencies, and complexity of the ICT resulted in increasing of effectiveness in a considerable number of human activities. On the other hand, this development is accompanied by new cyber threats which can result in global crisis. The newly formed "global cyber organism" has become much more vulnerable to sophisticated malware which analogic to a global human population in case of biologic viruses. The rapid development in ICT has an eminent influence on recently isolated industrial control systems (ICS) which are vital for our society. Therefore, ICS cyber security has been subject to fundamental changes which resulted in reconfiguration of "status quo". Furthermore, the malware Stuxnet was the main milestone in ICS cyber security which the led to necessary changes in cyber security.

ICS is developed in order to control of industrial processes. Moreover, according to "Guide to Industrial Control Systems (ICS) Security" [1] we can divide ICS into two main subgroups. The first is geographically independent Supervisory Control and Data Acquisition (SCADA) system, and the second is a geographically dependent

system known as Distributed Control System (DCS). [2] The boundary between these systems is often relatively insufficiently defined, which leads to the mutual misinterpretation of the groups. However, a considerable number of experts use the terminology SCADA instead of DCS. This misinterpretation occurs frequently and therefore is mostly acceptable by the experts.

The detection of cyber-attacks is one of the crucial factors of cyber security or cyber defense. Moreover, there is a considerable number of cyber security solution which can be adapted in case of ICS. However, one of the most progressive method how to defense ICS is anomaly based detection. Therefore, we are focusing on cyber defense system based on anomaly detection algorithms which can be easily adopted for intrusion detection systems (IDS). The anomaly detection involves the problem of finding patterns in a dataset that do not match the expected behavior. Moreover, every anomaly can be a symptom of the cyber-attacks. [3] Thus, the there are three main subgroups: Supervised anomaly detection, Semi-supervised anomaly detection, and Unsupervised anomaly detection which are based on differently structured datasets. This distribution is supported by a considerable number of authors [3], [4], [5], [6], [7], [8]. Taking into account the importance of various input data is crucial for every anomaly detection system. However, the anomaly detection systems have been deployed in various fields of human activities. Akoglu et al. (2015) [9] investigated the areas in which are anomaly detection system often used. We can highlight some of them: medical problems, image processing, insurance fraud, data center monitoring, image/video surveillance, etc. [9]

Stouffer et al. (2015) [1] pointed to historical developments in ICS where systems and devices are often used more than 20 years. In addition, a considerable number of ICS systems had been developed before private networks and the Internet deployment that we know today. However, these commonly used technologies are now interconnected with ICS which led to the creation of new vulnerabilities. Moreover, it is evidenced by an increasing number of vulnerabilities which are reported to ICS-CERT (753% in recent years). Pollet (2013) [10] predicted increasing interdependencies between ICS and ICT, and therefore the percentage of industrial companies providing the IDS for ICS will continually grow. Horkan (2015) [11] concluded that the IDS going to be an essential part of the ICS systems in following years. The application of IDS in ICS environment was examined by a considerable number of researchers: Verba a Milvich (2008) [12], Zhu a Sastry (2012) [13], Yang et al. (2013) [14], Maglaras a Jiang (2014) [15]. Moreover, Maglaras a Jiang (2014) [15] investigated the possibility of the OCSVM deployment in ICS environment. Unfortunately, the authors did not cover how they set Gamma parameter for OCSVM in deep. Furthermore, the computational cost of anomaly detection system was not considered.

On this basis, we established Semi-supervised anomaly detection system also known as Novelty detection. We carried out a multistep procedure in order to achieve the objectives of the research, and therefore obtain reliable as well as low computational cost of anomaly detection system. Moreover, presented predicted model is modified according to multi-criteria evaluation where we take into account computational cost.

The rest of the article is organized as follows. Section II is focused on a description of anomalies. Classification algorithm used in the research is analyzed in Section III. Section IV gives a necessary insight into methods which were used in the research. The Sections V includes results. Finally, Section VI provides the conclusion of the article.

2 Anomaly as a symptom of cyber-attack

Anomaly detection is a progressive method to find and separate patterns that deviate from normal behavior. Computer intrusion includes hacking, viruses, computer worms etc. However, the intrusion represents only a small percentage of total network and computer capacity. [16] Anomalies are relatively rare events in computer systems or networks, which can be divided into two main groups. The first group is anomalies caused by intentional human activities that involve cyber-attacks. The second group included anomalies that were caused by unintentional human activity (poor handling of the cybernetic system) or natural disasters and mistakes caused by technical error, lack of technical equipment or unintended human action.

According to E. Knapp (2011) [17] we can distinguish ICS anomalies into four main groups. The first group includes the monitoring of network traffic which includes source and destination Internet Protocol (IP) address, TCP/UDP ports, traffic volume etc.. The second groups can be characterized as a user activity which includes logins and logoffs of the users and other user activities. The third main group of monitored system behavior is Process and Control behavior which is also subject to this article. Moreover, this specific group is focused on system behavior which involves configuration of the system. Finally, the last group is focused on event and incident activity and handling, monitoring criticality, total number and severity of the incidents etc. [17]

3 Support Vector Machine

Support Vector Machine (SVM) is one best-suited classification algorithm for wide range applications. It is also an exceptional choice for high dimensional data and non-linear separation. Moreover, SVM is considered as a straightforward solution for anomaly detection system based on unbalanced dataset. All the advantages of the SVM are needed to build reliable detection system in multidimensional space for a nonlinear dataset. The predictive model is built on SVM. It classify the data into one of the predefined class. Moreover, the OCSVM is usually used for binary classification cases which are classified as +1 or -1. The SVM creates the widest margin near the boundary between two sets of data.

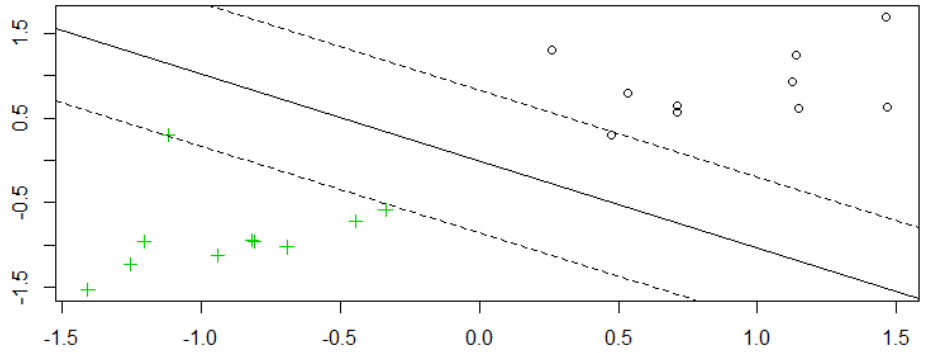

Fig. 1. The SVM boundary with margins.

The Fig. 1 illustrates how SVM algorithm operates with boundary. The circles and asterisks represent two classes in two-dimensional space. Each data point is represented by $(\bar{x},\ y)$ where $\bar{x}$ are feature values and y is a label (asterisk, circle or -1, 1). Moreover, the boundary is calculated in order to maximize the margin space. [18] The boundary is calculated according to equation (1).

$$f(\bar{x}) = \bar{w}\bar{x} + b \tag{1}$$

The main boundary is also known as hyperplane which is defined as $\bar{w}\bar{x} + b = 0$ and the margin width is defined as $\max\frac{2}{\|w\|}$. According to gutter constraint, we can set the margins on +1 and -1. The relationship is represented by equation as $\bar{w}\bar{x}_i + b = y_i$, where $\bar{x}_i \in \{-1, +1\}$. The OCSVM algorithm solves dual optimization problem in order to optimize constrained system. The final function can be seen in (2). [18]

$$L_{(\alpha)} = min\frac{1}{2}\sum_i^n \sum_j^n \alpha_i \alpha_j K(x_i x_j) \tag{2}$$

Where $0 \leq \alpha_i \leq \frac{1}{vm}$ and $\sum_i^n \alpha_i = 1$. Moreover, α_i is a Lagrange multiplier, ν is a trade-off parameter, m represents the total number of datapoints in a training dataset and $K(x_i, x_j)$ is a kernel function which is dot product in higher dimensional space. [18] There is a necessity to separate the dataset. However, the separation of the datasets are computational demanding process in most cases. The solution for this problem is the transformation of data into higher dimensional space. Thus, the kernel function K is described by the equation (3).

$$K\left(x_i, x_j\right) = \left(\emptyset(x_i), \emptyset\left(x_j\right)\right) \tag{3}$$

There are four commonly used kernels (Linear kernel, Polynomial kernel, Radial Basis Function (RBF) and Sigmoid kernel). However, we decided to use RBF which is suitable for the purpose of the research. Moreover, the kernel nonlinearly maps samples into a higher dimensional space. [19] Where γ represents Gamma parameter.

$$K(x_i, x_j) = exp\left(-\gamma \left\| x_i - x_j \right\|^2\right), \ \gamma > 0 \quad (4)$$

3.1 Gamma parameter

Gamma (γ) is the main parameters for nonlinear RBF also for SVM. The predictive model is set up for the best suited boundary in order to maximize space between margins. However, the shortage of the approach is the misclassification which can lead to poorly assembled predictive model. Therefore, Cortes and Vapnik (1995) [18] developed soft margins which allow to change or excluded data points for the purpose of minimize the number of errors. Gamma is the parameter of the nonlinear classification due to RBF kernel. Moreover, this parameter is a trade-off between error due to bias and variance of the predictive model. Therefore, there are two main problems, a problem of overfitting of the model and the boundary does not correspond with the complexity of data.

4 Methods

The purpose of the article is to create time efficient and accurate detection system in ICS environment. The OCSVM with RBF kernel is used in order to fulfill the main goal of the article and therefore develop a confidential predictive model. However, a considerable number of ICS devices which have limited computational power due to their long life cycle. Therefore, every anomaly detection system has to take into account requirements for computational power. Additionally, we can conclude that computational power is increasing due to growing Gamma value. Hence, there must be the specific equilibrium between the detection capabilities and computational complexity. The multi-criteria evaluation is one of the possible ways how to establish accurate and low computational cost detection system. The multi-criteria evaluation is based on the reference point of the multiple criteria (Accuracy, Sensitivity, Specificity, Precision, False Positive Rate (FPR) and Time).

- Accuracy - It represents the correct classification of the model. Moreover, accuracy is calculated as correct classification divided by correct and incorrect classification.
- Sensitivity - Sensitivity is also known as recall or true positive rate. Moreover, it is based on true positive condition and predicted positive condition. The criterion expresses how much relevant results are retrieved by the predictive model.
- Specificity - Specificity is also known as True negative rate. This criterion represents the measure of how correctly the negatives examples are classified.
- Precision - The criterion is also known as positive predictive value, takes into account true positive value and false positive value. The precision gives us information about how many relevant and irrelevant results give us the predictive model.

- FPR - This criterion is commonly known as false alarm rate. The predictive model improperly identifies normal harmless behavior as an anomaly which may lead to disruption of ICS. Therefore, FPR is highly important for critical infrastructure because the availability of the services is the most important criterion for ICS.
- Time - Time represents necessary time period for creation and evaluation of the predictive model.

The predictive model is based the Mississippi State University and Oak Ridge National Laboratory SCADA dataset.[20] The dataset consisting of 37 power system event scenarios. The dataset is structured as follow natural events (8), no events (1) and attack events (28). Normal operation of the system is represented by "no events". The "natural events" can be characterized as a natural fault of the system. The "attack events" can be described as the system under the cyber-attack. Furthermore, four Intelligent Electronic Devices (IED) were monitored. We investigated cyber-attack type: Data injection.

5 Results

Preprocessed dataset is divided into four subsets which representing data for each IED. We created seven hundred and fifty predictive models for each subset and different value of gamma parameter in order to evaluate the detection system. Moreover, the criteria for each predictive model are calculated (Accuracy, Sensitivity, Specificity, Precision, FPR and Time). The best fitting value of gamma parameter is determined by multi-criteria evaluation (reference point). Moreover, the weight for each criterion is selected according to its priority for ICS system. Therefore, we established three groups. The first and least important group include Accuracy and Sensitivity due to their focus only on positive classification. The second group includes Specificity, Precision and Time. The first two criteria which partially involving false positive identification, and time to build the predictive model which is very important for ICS. The last group involving false positive rate as the most important criterion due to the possible availability disruption of the ICS.

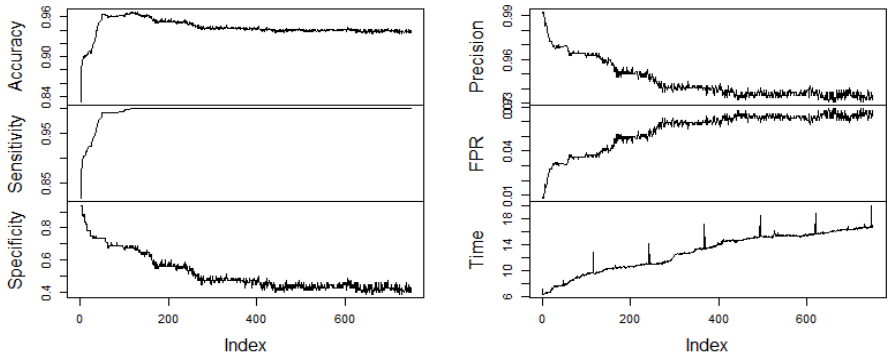

Fig. 2. The results for the first IED.

The Fig. 2 shows the results for Accuracy, Sensitivity, Specificity, Precision, False Positive Rate (FPR) and Time for the first IED. The results decompose in the interval: Accuracy from 0.832 to 0.967, Sensitivity from 0.819 to 1, Specificity from 0.382 to 0,941, Precision from 0.931 to 0.992, FPR from 0.008 to 0.069 and Time from 6.279 to 19.997 ms. Moreover, the best outcomes for each criterion according to gamma parameter is calculated as follow: Accuracy - 0.232 gamma, Sensitivity - 0.232 gamma, Specificity - 0.002 gamma, Precision - 0.008 gamma, FPR - 0.008 gamma and Time - 0.008 gamma.

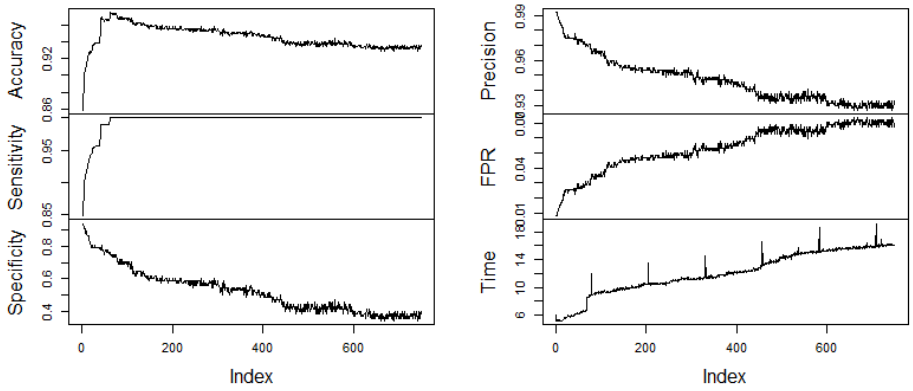

Fig. 3. The results for the second IED.

The graphs in Fig. 3 represents the results for the second IED. The results decompose in the interval: Accuracy from 0.859 to 0.975, Sensitivity from 0.849 to 1, Specificity from 0.338 to 0.941, Precision from 0.927 to 0.992, FPR from 0.008 to 0.073 and Time from 5.092 to 19.236 ms. The gamma parameter for the best outputs is as follow: Accuracy - 0.124 gamma, Sensitivity - 0.124 gamma, Specificity - 0.002 gamma, Precision - 0.006 gamma, FPR - 0.006 gamma and Time - 0.026 gamma.

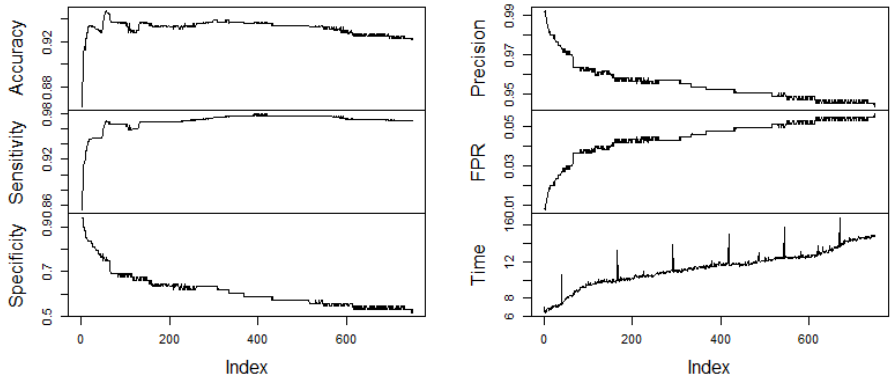

Fig. 4. The results for the third IED.

The Fig. 4 shows the results for the third IED which are decomposed in the interval: Accuracy from 0.863 to 0.947, Sensitivity from 0.854 to 0.979, Specificity from 0.515 to 0,941, Precision from 0.944 to 0.992, FPR from 0.056 to 0.008 and Time from 6.374 to 16.881 ms. The gamma parameter for the best outputs of the criteria is as follow: Accuracy - 0.116 gamma, Sensitivity - 0.814 gamma, Specificity - 0.002 gamma, Precision - 0.008 gamma, FPR - 0.008 gamma and Time - 0.008 gamma.

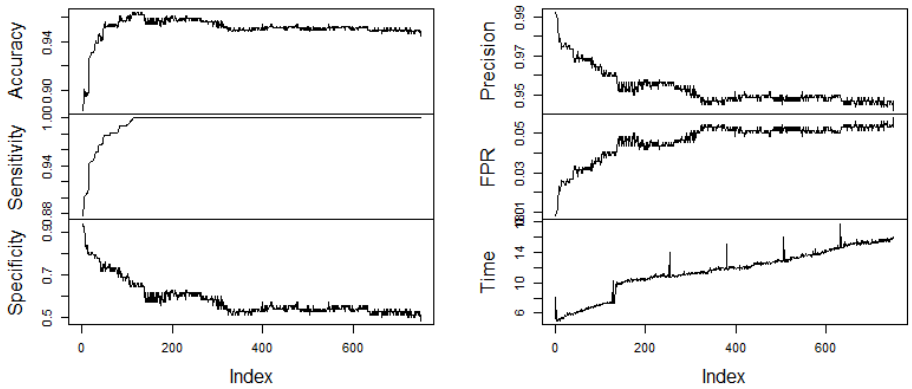

Fig. 5. The results for the fourth IED

The last results are shown in Fig. 5. The results for each criterion is spread as follow: Accuracy from 0.884 to 0.964, Sensitivity from 0.877 to 1, Specificity from 0.485 to 0,941, Precision from 0.942 to 0.992, FPR from 0.008 to 0.058 and Time from 4.954 to 12.758 ms. The gamma parameter for the best outputs of each criterion is as follow: Accuracy - 0.25 gamma, Sensitivity - 0.266 gamma, Specificity - 0.002 gamma, Precision - 0.004 gamma, FPR - 0.004 gamma and Time - 0.01 gamma.

Table 1. The overall results for the computed gamma parameters

	Accuracy	Sensitivity	Specificity	Precision	FPR	Time (ms)	Gamma
IED 1	0.892	0.891	0.897	0.986	0.014	6.491	0.01
IED 2	0.906	0.905	0.912	0.989	0.012	5.235	0.014
IED 3	0.898	0.893	0.941	0.992	0.008	6.374	0.008
IED 4	0.901	0.9	0.911	0.988	0.012	5.179	0.012

In Tab. 1 can be seen all values for selected criteria according to chosen Gamma parameter. The parameter Gamma was computed for each IED according to the Reference point. Moreover, it calculates the best choice for each criterion and compares it to the actual state of the criteria according to their weights. At the end of the multi-step procedure, the results are fused into one via Majority vote technique. The final results affected by fusion are as follows: Accuracy - 0.898, Sensitivity - 0.888, Specificity - 0.985, Precision - 0.998, FPR - 0.002.

6 Discussions

The presented paper is focused on improvement of detection capabilities of predictive models via choosing an appropriate value of the Gamma parameter. The Gamma parameter is one of the determining parameters for Radial kernel of the SVM. We established novelty detection system based on one-class SVM. Moreover, four IED under cyber-attack were used in order to create and evaluate the proposed solution. Furthermore, seven hundred and fifty predictive models with a different value of Gamma parameter were used.

The results presented in figures 2, 3, 4, 5 are assigned to four IED. The overall results indicate relatively high values for Accuracy, Sensitivity, Specificity, Precision and low values for FPR and Time especially for the low value of Gamma parameter. Moreover, the progress of graphs for is similar within a group of IED. The most significant results are situated in the first quarter of each graph (Fig. 2. Fig. 3, Fig. 4, Fig. 5) as result of high FPR and Time parameter in the rest of the data. Therefore, it is important to note that every miscalculation of Gamma parameter could have the serious impact on ICS. All relevant criteria achieve relatively high values in case of Accuracy, Sensitivity, Specificity, Precision and contrary FPR, Time criteria achieve considerably low values. The results for all predictive models show the best results for the relatively low value of Gamma parameter. Thus, proposed system based on multi-criteria evaluation calculated low values of Gamma parameter (0.01, 0.014, 0.008, 0.012). Moreover, the classifier fusion of the subsets resulted in improvement of detection capabilities of the detection system, especially for FPR parameter.

Acknowledgments This work was funded by the Internal Grant Agency (IGA/FAI/2018/003) and supported by the project ev. no. VI20152019049 "RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems", supported by the Ministry of the Interior of the Czech Republic in the years 2015-2019 and also supported by the research project VI20172019054 "An analytical software module for the real-time resilience evaluation from point of the converged security ", supported by the Ministry of the Interior of the Czech Republic in the years 2017-2019. Moreover, this work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Programme project No. LO1303 (MSMT-7778/2014) and also by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089. Finally, we thank our colleagues from Mississippi State University and Oak Ridge National Laboratory which provides SCADA datasets.

References

1. Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2015). Guide to industrial control systems (ICS) security. NIST special publication, 800(82) R2, 16-16.

2. Macaulay, Tyson a Bryan Singer. Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS. Boca Raton, FL: CRC Press, c2012, x, 193 p. ISBN 14-398-0196-7.
3. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 15.
4. Dewa, Z., & Maglaras, L. A. (2016). Data Mining and Intrusion Detection Systems. International Journal of Advanced Computer Science and Applications, 7(1).
5. Pathan, A. S. K. (2014). The state of the art in intrusion prevention and detection. Auerbach Publications.
6. Goldstein, M., & Uchida, S. (2016). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PloS one, 11(4), e0152173.
7. Ebrahimi, M., Suen, C. Y., Ormandjieva, O., & Krzyzak, A. (2016). Recognizing predatory chat documents using semi-supervised anomaly detection. Electronic Imaging, 2016(17), 1-9.
8. Sharma, V., & Suryawanshi, V. (2017) Network Anomaly Detection Through Hybrid Algorithm. International Journal of Computer Science Trends and Technology (IJCST), Vol. 5.
9. Akoglu, L., Tong, H., & Koutra, D. (2015). Graph based anomaly detection and description: a survey. Data Mining and Knowledge Discovery, 29(3), 626-688.
10. Pollet, J., SCADA 2017: The Future of SCADA Security. [Online]. 8th annual ICS & SCADA security summit, SANS, February 12-13, 2013, Available at: https://files.sans.org/summit/euscada12/PDFs/RedTigerSecurity_SCADA_2017.pdf
11. Horkan, M. Challenges for IDS/IPS Deployment in Industrial Control Systems. SANS Institute, 2015, Available at: https://www.sans.org/reading-room/whitepapers/ICS/challenges-ids-ips-deployment-industrial-control-systems-36127.
12. Verba, J., Milvich, M. Idaho national laboratory supervisory control and data acquisition intrusion detection system (SCADA IDS). In Technologies for Homeland Security, 2008 IEEE Conference on (pp. 469-473). IEEE, 2008
13. Zhu, B., Sastry, S. Intrusion Detection and Resilient Control for SCADA Systems. Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection: Approaches for Threat Protection, 352, 2012
14. Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Wang, H. F. Rule-based intrusion detection system for SCADA networks. In Renewable power generation conference (RPG 2013), 2nd IET (pp. 1-4). IET, 2013
15. Maglaras, L. A., Jiang, J.: Intrusion detection in scada systems using machine learning techniques. In Science and Information Conference (SAI), 2014 (pp. 626-631). IEEE, 2014
16. Pathan, A. S. K. (2014). The state of the art in intrusion prevention and detection. Auerbach Publications.
17. Knapp, E. Industrial network security: securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems. Waltham, MA: Syngress, c2011, xvii, 341 p. ISBN 15-974-9645-6.
18. Cortes, C., & Vapnik, V. (1995). Support-vector networks. Machine learning, 20(3), 273-297.
19. Hsu, C. W., Chang, C. C., & Lin, C. J. (2003). A practical guide to support vector classification.
20. Hink, R. C. B., Beaver, J. M., Buckner, M. A., Morris, T., Adhikari, U., & Pan, S. (2014, August). Machine learning for power system disturbance and cyber-attack discrimination. In Resilient Control Systems (ISRCS), 2014 7th International Symposium on (pp. 1-8). IEEE.