Review of machine learning based intrusion detection approaches for industrial control systems

Jean-Marie Flaus and John Georgakis

University Grenoble Alpes, CNRS, Grenoble INP, G-SCOP, F-38000 Grenoble, France
jean-marie.flaus@univ-grenoble-alpes.fr

Abstract. In recent years, industrial control systems are more and more subject to cyberattacks and the consequences can be potentially disastrous. Intrusion detection is one of the tools used in the risk management process. Specific approaches have been developed for industrial systems. Most are designed to detect abnormalities between a reference model and the observed behavior, one of the differences with IT systems is that this model may include one of the controlled physical system. The construction of this model is a key step and the use of machine learning techniques appears as an attractive solution. This article reviews the approaches found in the literature and summarizes the main proposed ideas.

Keywords: IDS, intrusion detection system, machine learning, Industrial control, industrial cybersecurity.

Category : Protection

1 Introduction

Cyber security of industrial installations, of cyber-physical systems and more generally of Industrial IoT systems is a very important problem. Cybercrime is growing significantly in recent years and many information technology systems (IT) are the subject of attacks that can spread rapidly and have a major impact such as Wanacry. The evolution of industrial plants (OT) where there is a technological convergence with the world of traditional IT and the development of more and more interconnected systems makes them also increasingly vulnerable.

The establishment of a risk management approach is divided into several phases: identification, protection, detection, response and recovering [1]. In the detection phase, intrusion detection systems (IDS) are important. The detection of intrusion is a fairly complex problem and there is no solution that enable accurate detection: unfounded alerts can be generated and some intrusions can be undetected. Much work has taken place since the 80s ([2][3]), but this is still an active area of research especially with regard to IDS for industrial systems. One of the explored approaches for model building is to use machine learning approaches, which are part of Artificial Intelligence techniques.

This article presents a review of the approaches for intrusion detection for industrial systems and more particularly of IDS with machine learning.

The paper is organized as follows: in the first part, we present industrial control systems and their differences with traditional IT systems. The second part presents the different approaches for intrusion detection, especially for industrial systems and the third part is a review of the main research works on this topic.

2 Industrial Control System

An industrial control system (ICS) may be defined as a kind of computer system connected to a physical system with the aim of monitoring or controlling an industrial process. It consists of:

- a networked information processing system, consisting of workstations, servers, network equipment, printers, storage and backup systems,
- and a set of specific devices that can receive the measurements, act on the physical system, and interact with the operators. In this category, we find the Programmable Logical Controllers (PLC), the sensors and actuators, the safety instrumented system (SIS), and the human-machine interfaces (HMI) for control of manufacturing operations and safety actions.

Very often, these elements are operated by a specific software, such as a SCADA (Supervisory control and data acquisition) software, an historian software or programming workshops for programmable logical controller.

The Purdue model (Figure 1)[4] is used as a reference model to describe the architecture of an ICS. It introduces five levels:

- Level 0 (physical level): this level corresponds to physical systems used for production. Sensors and actuators are at this level.
- Level 1 (local control): this level includes the functions involved in the detection, monitoring and control of the physical process. They are carried out by the processing devices such as PLCs, or Remote Terminal Units. Two kinds of controllers are used: those for normal operation (BPCS, Basic Process Control Process System) and those for security actions (SIS Safety Instrumented System).
- Level 2 (Supervisory Control): it contains the human machine interfaces (HMI) systems for the control and data acquisition (SCADA) and distributed systems (DCS). The facilities of this level are usually associated with the production area.
- Level 3 (Operations Management): in the level, there is mainly the Manufacturing Execution System (MES).
- Level 4 (Enterprise Business Systems): This level includes the functions involved in managing operations of manufacturing.

Industrial control systems interact with physical systems which have specific constraints. Among those of interest in this study, it should be noted that it is not possible to suddenly stop a running program regardless of the state of the manufacturing process or equipment. This is what limits the use of Intrusion Protection System because they block the communication flow in case of the detection of an intrusion. Others specific

points are that industrial control systems have a long lifetime and that the protocols are old and unsafe.

The protocols and types of information exchanged at each level of the Purdue model are specific to this level or a set of levels. This is the reason why the levels may often be separated by a firewall: for example, Modbus or OPC protocol are used between level 0 and 1, between the level 1 and 2 and should not be used elsewhere. The intrusion detection must adapt to this architecture

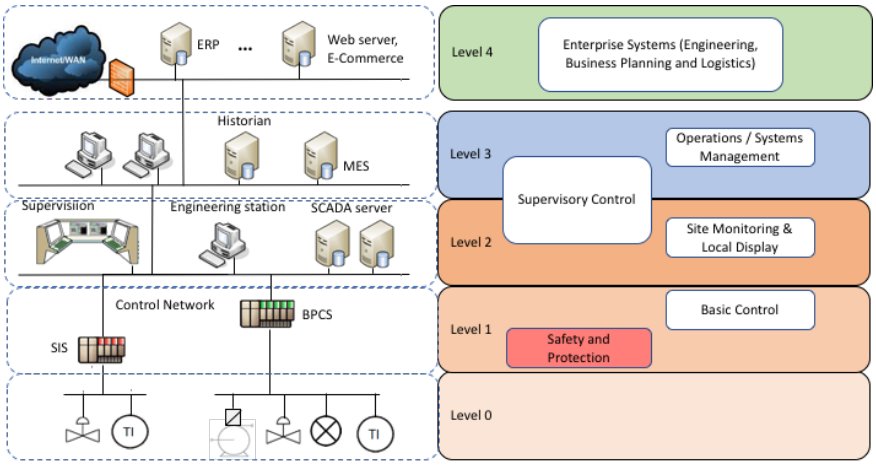


Fig. 1. Architecture of an industrial control system

The differences between an industrial control system and a classical IT system include:

1) a variety of protocols, including those known as "industrial", such as Modbus, which are poorly secured;

2) real-time constraints;

3) a part of the behavior and the evolution of the system imposed by the laws of physics;

4) a current normal behavior which is the one of the basic operating mode (BPCS) and an exceptional normal behavior which is the one the safety system, and which, in principle, is rarely activated (but which is normal).

Some of these aspects, such as the second one, are additional constraints to consider while others, such as the third one, are elements on which a detection system can rely to improve detection.

3 Intrusion Detection System

3.1 Principle

The principle of an intrusion detection system is to monitor events in a system or a computer network and to analyze them in order to detect incidents that constitute violations of some rules related to the security policy or that are the manifestation of imminent threats to the information system or to the installation.

Incidents can be caused by various sources, such as malware attempting to access unauthorized resources, malicious users accessing the system from the Internet and authorized system users who abuse their privileges or trying to get additional privileges.

Intrusion detection systems (IDS) can use the information from the network by observing flows and information from each station or devices by observing their activity to trigger alerts.

To detect incidents, IDS uses a model that can represent either normal behavior or abnormal behavior. In the first case, the algorithm tries to detect anomalies and the approach is called "anomaly based IDS". In the second case, the model describes behavior characteristics of an intrusion and the approach is called "signature based IDS". The models are constructed by human experts or using machine learning methods. There are also hybrid approaches combining the two types of models.

If the model is inadequate, for example if the signature is missing or incorrect, or if the normal behavior is not modeled properly, then the IDS may generate an alarm for a legitimate traffic or a normal action: it is called a "false positive". Similarly, hostile activity, which does not correspond to an IDS signature or is looking like a normal activity, may not be detected, this is called a false negative (false sense of security). This imperfect functioning is an important limitation to the use of IDS.

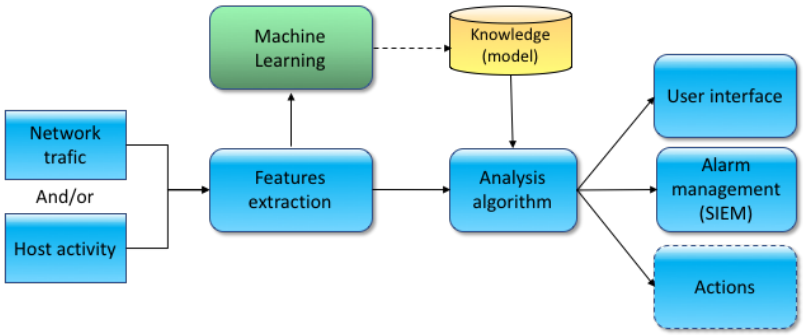


Fig. 2. Structure of an IDS

3.2 Machine Learning Methods

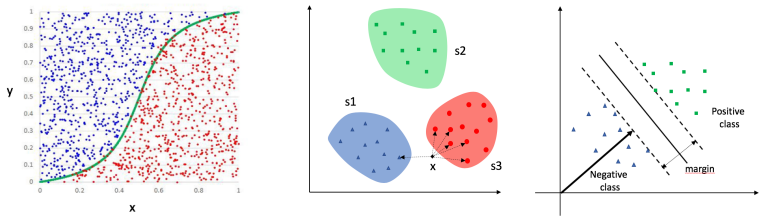
The idea of automatically building the model which is used to detect intrusions is quite old [5]. The process consists of two stages: extracting a feature vector from the observed data, and processing it with an algorithm in order to build the model which will be used to detect the intrusion.

To build the model for the IDS, many tools or techniques from the field of artificial intelligence have been used such as classification methods, statistical learning or rule-based systems [6]. Classifiers and statistical learning methods, including k-nearest neighbor (k-NN) algorithms, Bayesian classifiers, Support Vector Machines (SVM) and Artificial Neural Networks (ANN) are the most commonly found methods. More recently, deep learning approaches have also begun to be applied.

Among these approaches, some are said to be supervised, the attribute vector must be labeled as characteristic of a good or bad behavior, and others are called unsupervised because they classify feature vectors automatically.

Linear regression is the best known and the best understood algorithm in statistics and machine learning. It classifies samples into two classes. Logistic regression is an extension which is based on the logistic function (Figure 3.a).

k-NN is a learning algorithm based on the principle that elements in a data set usually exist near other elements with similar properties [7]. By labeling the instances used for learning, it is possible to classify a new instance from its distance to its nearest neighbors (Figure 3.b).



(A) logistic regression (B) k-NN neighbors (C) SVM

Fig. 3. Different classification approaches (DRAWINGS AGAIN)

The principle of Bayesian classifiers is based on Bayes theorem and the assumption of conditional independence [8]. Bayesian networks can represent more complex Bayesian interactions between a set of variables in a graph form supporting Bayesian laws.

SVM is a particular case of clustering techniques. It is a generalization of linear classifiers that separate the data with a hyperplane with a certain thickness (Figure 3.c). OCSVM (One Class) are SVM with a single class, the instances not belonging to the class are classified as being abnormal.

Artificial neural networks are excellent candidates for learning and recognition of previously learned patterns. However, it is very difficult to explain why a decision was made by such a mechanism. This approach was extended in the 2010s by using networks with many layers and using a specific learning mode (Deep Learning)[9].

In supervised mode, the principle of learning is to generate instances labeled as being benign or malicious, which are then provided to the algorithm. In the unsupervised approach, learning assumes that the majority of traffic must be normal and malicious traffic must be statistically different from benign [10].

The effectiveness of the algorithm is important, but the performance in terms of speed may also be a factor of choice [11].

Moreover, as developed in the sequel, the characteristics of the data used as input, which can measure different aspects of the behavior, are essential.

4 Intrusion detection systems for ICS

Before considering the potential benefits of AI techniques, we will introduce the principle of intrusion detection systems for industrial systems. Indeed, given the specific characteristics of cyber physical systems, learning techniques can be used differently to what we find for IT systems.

Data can be provided by taking the information from a host (HIDS) or at the network level (NIDS). For those using the network data, they can, in addition to the use of conventional attributes (source address, destination indicators, timing ...), be able to perform a deep analysis of the packet content using the industrial protocol (Deep Packet inspection). They can, for example, read the detail of Modbus frames. This type of IDS is named I-NIDS in the rest of the paper (Industrial-NIDS). Another category is HIDS that can be installed in industrial equipment such as a PLC, or that are able to use information from this kind of device. We call them I-HIDS (Industrial-HIDS).

Most of the Industrial IDS are able to use the state of the physical system which is available either in the device memory or can be captured in the network stream. This information allows to use a model of the physical process or of the control software in order to detect anomalies. They are called Process Aware IDS.

As said before some IDS use a model of normal behavior (anomaly), a model characterizing an intrusion (signature) or a mixed approach. However, in the case of industrial ICS, the signatures can be sought in process variables, such abnormal fluctuations of controlled variable, which can be characteristic of an attack and was the case in Stuxnet.

As for the learning method (statistics, clustering, neural network, Deep learning, ...) and the way of decision, the approaches are those used for classical IDS and some more suited to physical system modelling such as Kalman filter and autoregressive filter.

5 Machine learning based Industrial ICS

5.1 Proposed approaches

In this section, we present the main intrusion detection approaches for ICS that have been proposed in the literature. We are basically interested in the specific approaches for ICS, ie those using industrial network flows and / or using the state of the ICS or of the physical system. All the analyzed approaches are summarized in the following table. They are ordered according to their date of publication and are characterized by the type of data source and the learning method. In terms of data sources, we consider where the data is collected :

- the network flows (I-NIDS);
- the memory of the equipment (I-HIDS);
- or both (I-NHIDS);

and the nature of the information:

- the variables characterizing the evolution of the process;
- the program and the PLC configuration;
- the processing time.

Input data	Learning method	References
process variables I-NIDS	Auto Associative Kernel Regression (AAKR) model coupled with the Statistical Probability Ratio Test (SPRT)	[12]Yang, D., A. Usynin, and JW Hines. 2006 Anomaly-Based Intrusion Detection for SCADA Systems
PLC software and execution time I-HIDS	Application level instrumentation, measurement of time to execute code and monitoring, Statistics learning	[13] Zimmer C, Bhat B, Mueller F (2009) Time-Based Intrusion Detection in Cyber-Physical Systems.
Packets attributes I-NIDS	neural network	[14] Linda O (2009) Neural Network based Intrusion Detection System for critical infrastructure Neural Network Based Intrusion Detection System for Critical Infrastructure
process variables I-NHIDS	Kalman Filter	[15] Rrushi J, Kang KD (2009) Detecting defects in process control networks.
Process variables (sensors outputs) I-NIDS	Self organizing maps Kohonen networks	[16] Moya JM Araujo Á, Banković Z, et al (2009) Improving security for SCADA systems sensor networks with reputation and self-organizing maps.
process variables I-NIDS	Autoregressive model with Burg algorithm for learning	[17] Hadžiosmanovi D Sommer R, PH Hartel, 2013, Through the Eye of the PLC: Semantic Security Monitoring for Industrial Processes
KPI Characterizing the SCADA traffic I-HIDS	One Class SVM	[18] Jiang J, Yasakethu L (2013) Anomaly detection via one class SVM for protection of SCADA systems [19] Jiang J, Yasakethu L (2013) Intrusion Detection via Machine Learning for SCADA System Protection.
process variables I-NIDS	One-Class Classification SVDD	[20] Nader P (2013) Intrusion detection in scada systems using one-class classification, [21] Nader P, P Honeine, Beauseroy P (2014)
Packets attributes I-NIDS	One-Class SVM	[22] Maglaras LA, Jiang J (2014) Intrusion detection in SCADA systems using machine learning techniques.
Process variables from SCADA & RTU I-HIDS	Unsupervised method clustering	[23] Almalawi A, Yu X, Z Tari et al (2014) An unsupervised anomaly-based detection approach for integrity attacks are SCADA systems
Packets attributes State & process I-NHIDS	Hidden Markov Model Learning with Baum Welch algorithm	[24] Zhou C, Huang S, Xiong N, et al (2015) Design and Analysis of Multimodel Anomaly-Based Intrusion Detection Systems in Industrial Process Automation.

Packets attributes I-NIDS	Blackbox analysis of PLC register with a single window classification and statistical analysis	[25] Erez N, A Wool (2015) Control variable classification, modeling and anomaly detection in Modbus / TCP SCADA system
process variables I-NIDS	SVM on the time window	[26] Keliris A Salehghaffari H Cairl B (2016) Machine Learning-Based Defense Against Attacks on Process-Aware Industrial Control Systems
Packets attributes I-NIDS	Statechart based approach,specific learning algorithm to learn timed DFA (Deterministic Finite Automaton)	[27] Kleinmann A, A Wool (2016) Automatic Construction of Statechart-Based Anomaly Detection Models for Multi-Threaded Industrial Control Systems. [28] Wool AK and A (2016) A Statechart-Based Anomaly Detection Model for Multi-Threaded SCADA Systems.
Packets attributes I-NIDS	One-Class Classification (OCC) algorithms. OC-OC-SVM & SVDD	[29] Da Silva EG, Da Silva AS, Wickboldt JA, et al (2016) A One-Class NIDS for SDN-Based SCADA Systems
Process variables (sensors) I-HIDS	Fault detection is based neural network Link deep learning	[30] He Y, Mendis GJ, Wei J (2016) Real-time Detection of False Data Injection Attacks in Smart Grids: A Deep Learning-Based Intelligent Mechanism.
Packets attributes & Process Variables sequences I-NIDS	Discrete Time Markov Chains (DTMCs) & statistical learning	[31] Caselli M Zambon E, F Kargl (2016) Sequence-Aware Intrusion Detection in Industrial Control Systems Sequence-Aware Intrusion Detection in Industrial Control Systems
Packets attributes I-NIDS	Hierarchical Neuron based Neural Network Architecture (HNA-NN) Technical & Intrusion Weighted Particle based Cuckoo Search Optimization (IWP-CSO) and	[32] Shitharth S, D Winston Prince (2017) An enhanced optimization based algorithm for intrusion detection in SCADA network
process variables I-NIDS	Neural networks trained with OPSO-BPNN (Particle Swarm Optimization with back-propagation algorithm)	[33] Yang H, Chen T, Guo X, et al (2018) Research on intrusion detection of industrial control system is based OPSO-BPNN algorithm
Packet attributes and process variables I-NIDS	Tools for Weka data mining Hybrid learning approach	[34] Ullah I, Mahmoud QH (2018) A hybrid model for anomaly-based intrusion detection in SCADA networks.
Packet processing time (by the PLC) I-HIDS (in the PLC)	K-Means Clustering	[35] Letters S, T Alves Das R, T Morris (2018) Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers.

5.2 Discussion

Most approaches are anomaly based IDS, except [26] which is devoted to an original approach using a model of attacks specific to ICS based on the evolution of the process control variables.

Four key elements distinguish approaches: what is modeled and is the basis for the detection of abnormality, the data used as input for detecting the abnormality by using the model, the model structure which can include more or less information about the system (e.g. by imposing a dynamical model) and the learning method for constructing the model.

Regarding the model on which is based the IDS, we found that the proposed approaches are modeling:

- changes in the process variables or measures, such as [17] ;
- the sequence of messages between the ICS devices which are exchanged on the network [35][24];
- the control software or its execution trace [13];

We can note that all the elements specific to ICS that can be modelled have been considered.

The different approaches use information input which is representative of the operation of an industrial control system. It can be classified into two categories:

- information on the process, represented by the measured values and the values sent to the actuators,
- information on industrial communication protocols and on the operation of various devices, obtained through deep packet inspection, as in [26] for example, or by thorough observations of equipment operation as in [35].

The approach in [31] proposes to combine the two types of information and obtains interesting results.

The third aspect concerns the structure of the model. The different publications aim:

- either to classify measured samples, using a supervised or unsupervised technique. This approach is interesting in that it requires little knowledge about the system. What is learned is relatively "black box" and it does not offer guarantees of proper functioning or explanations on the detected anomalies.[21]
- either to build a model in one form or another of the process [28] or of the controlled process [31]. In this case, knowledge is capitalized as an explicit model, such as a timed automaton describing the operation. It is easier to validate it, and an explanation of the anomaly is easier to develop.

In terms of learning technique, one can notice that the relatively simple methods yield good results, such as the one class SVM method [19] or statistical approaches[28], while more complex approaches based on neural networks training or deep learning do not offer decisive advantages [14].

However, machine learning for IDS still poses problems [36]. Relatively conventional problems arising in dynamical system identification and fault detection, such as the quality of data used for learning (adequate excitation of the system to obtain data representative of the operation, taking into account uncertainty), are not considered. Moreover, the proposed approaches do not provide performance indicator or analysis of the quality of the algorithm. They only show some test results, for which it is difficult to assess the representativeness.

Furthermore, most of the proposed techniques are anomaly based intrusion detection. It is interesting to note that these methods are those which are the subject of very active research but are quite rarely used in practice [37].

Some progresses are still needed in order to develop algorithms based on models better suited to cyber physical systems and able to capture their real characteristics. It is also necessary to provide quality indicators of the decision and the possibility to explain why an anomaly has been detected.

6 Conclusion

This review of approaches of intrusion detection systems for industrial systems shows that the identification of the design parameters (choice of attributes, behavioral modeling, detection approach) is an important step and that machine learning algorithms do not need to be complex to lead to good results. These intrusion detection systems can be an improvement for intrusion detection, but there are not mature enough and more realistic approaches able to indicate the confidence level of the alerts, and even to give an explanation of anomaly source need to be developed.

References

1. Stouffer K, Stouffer K, Abrams M Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security
2. Anderson JP (1980) Computer security threat monitoring and surveillance. Tech Rep James P Anderson Co 56
3. Denning DE (1987) An intrusion-detection model. IEEE Trans Softw Eng 222–232 .
4. Williams TJ (1994) The Purdue Entreprise Reference Architecture. Comput Ind 24:141–158
5. Javitz HS, Valdes A (1994) The NIDES statistical component: Description and justification. Contract, http://web.cs.ucdavis.edu/ ~wu/ecs236/papers/ hw2_ NIDES- STA-description .pdf

6. Buczak AL, Guven E (2016) A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications surveys & Tutorials,18:1153–1176
7. Cover T, Hart P (1967) Nearest neighbor pattern classification. IEEE Trans Inf Theory 13:21–27.
8. Mitchell TM (2005) Machine learning, 432 pages, McGraw-Hill Science/Engineering/Math
9. Skansi S (2018) Introduction to Deep Learning Algorithms. From Logical Calculus to Artificial Intelligence, Springer Berlin Heidelberg
10. L. Portnoy EE and SS (2001) Intrusion detection with unlabeled data using clustering. In: Proceedings of ACM CSS Workshop on Data Mining Applied to Security
11. Shah SAR, Issac B (2017) Performance comparison of intrusion detection systems and application of machine learning to Snort system. Futur Gener Comput Syst.
12. Yang D, Usynin A, Hines J (2005) Anomaly-based intrusion detection for SCADA systems. 5th Intl Top Meet Nucl Plant Instrumentation, Control Hum Mach Interface Technol (NPIC&HMIT 05) 12–16
13. Zimmer C, Bhat B, Mueller F (2009) Time-Based Intrusion Detection in Cyber-Physical Systems. 30th IEEE Real-Time Syst Symp 89–92
14. Linda O (2019) Neural Network based Intrusion Detection System for critical infrastructures. International Joint Conference on Neural Networks.
15. Rrushi J, Kang KD (2009) Detecting anomalies in process control networks. IFIP Adv Inf Commun Technol 311:151–165.
16. Moya JM, Araujo Á, Banković Z, et al (2009) Improving security for SCADA sensor networks with reputation systems and self-organizing maps. Sensors 9:9380–9397.
17. Hadziosmanovic D, Sommer R, Zambon E, Hartel P (2014) Through the Eye of the PLC: Towards Semantic Security Monitoring for Industrial Control Systems, ACSAC '14 Proceedings of the 30th Annual Computer Security Applications Conference
18. Jiang J, Yasakethu L (2013) Anomaly detection via one class SVM for protection of SCADA systems. Proc - 2013 Int Conf Cyber-Enabled Distrib Comput Knowl Discov CyberC 2013 82–88.
19. Yasakethu SLP, Jiang J (2013) Intrusion Detection via Machine Learning for SCADA System Protection. 1st Int Symp ICS SCADA Cyber Secur Res 101–105
20. Nader P (2013) Intrusion detection in scada systems using one-class classification, roc 21st European Signal Processing Conference (EUSIPCO 2013) 1–5
21. Nader P, Honeine P, Beauseroy P (2014) lp-norms in One-Class Classification for Intrusion Detection in SCADA Systems. Proc IEEE Transactions on Industrial Informatics, 10:4.
22. Maglaras LA, Jiang J (2014) Intrusion detection in SCADA systems using machine learning techniques. 2014 Sci Inf Conf 626–631.
23. Almalawi A, Yu X, Tari Z, et al (2014) An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. Comput Secur 46:94–110.

24. Zhou C, Huang S, Xiong N, et al (2015) Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation. IEEE Trans Syst Man, Cybern Syst 45:1345–1360 .
25. Erez N, Wool A (2015) Control variable classification , modeling and anomaly detection in Modbus / TCP SCADA systems. Int J Crit Infrastruct Prot 10:59–70.
26. Keliris A, Salehghaffari H, Cairl B et al (2016) Machine Learning-based Defense Against Process- Aware Attacks on Industrial Control Systems. 2016 IEEE International Test Conference (ITC).
27. Kleinmann A, Wool A (2016) Automatic Construction of Statechart-Based Anomaly Detection Models for Multi-Threaded Industrial Control Systems. ACM Transactions on Intelligent Systems and Technology 8(4)
28. Wool AK and A (2016) A Statechart-Based Anomaly Detection Model for Multi-Threaded SCADA Systems. Critical Information Infrastructures Security, 9578:132–144 .
29. Da Silva EG, Da Silva AS, Wickboldt JA, et al (2016) A One-Class NIDS for SDN-Based SCADA Systems. Proc - Int Comput Softw Appl Conf 1:303–312 .
30. He Y, Mendis GJ, Wei J (2016) Real-time Detection of False Data Injection Attacks in Smart Grids: A Deep Learning-Based Intelligent Mechanism. IEEE Trans Smart Grid 3053:1–12 .
31. Caselli M, Zambon E, Kargl F (2016) Sequence-aware Intrusion Detection in Industrial Control Systems Sequence-aware Intrusion Detection in Industrial Control Systems CPSS 2015 - Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Part of ASIACCS 2015. 13-24.
32. Shitharth S, Prince Winston D (2017) An enhanced optimization based algorithm for intrusion detection in SCADA network. Comput Secur 70:16–26 .
33. Yang H, Chen T, Guo X, et al (2018) Research on intrusion detection of industrial control system based on OPSO-BPNN algorithm. Proc 2017 IEEE 2nd Inf Technol Networking, Electron Autom Control Conf ITNEC 2017 2018–Janua:957–961.
34. Ullah I, Mahmoud QH (2018) A hybrid model for anomaly-based intrusion detection in SCADA networks. Proc - 2017 IEEE Int Conf Big Data, Big Data 2017 2018–Janua:2160–2167 .
35. Alves T, Das R, Morris T (2018) Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers. IEEE Embedded Systems Letters, 10:3.
36. Catania CA, García C (2012) Automatic network intrusion detection : Current techniques and open issues q. Comput Electr Eng 38:1062–1072 .
37. Sommer R, Paxson V (2010) Outside the closed world: On using machine learning for network intrusion detection. Proc - IEEE Symp Secur Priv 305–316.