Research Article

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2018, Vol. 14(8)

DOI: 10.1177/1550147718794615
journals.sagepub.com/home/dsn
SAGE

A survey of intrusion detection on industrial control systems

Yan Hu[1], An Yang[2,3], Hong Li[2,3], Yuyan Sun[2,3] and Limin Sun[2,3]

Abstract

The modern industrial control systems now exhibit an increasing connectivity to the corporate Internet technology networks so as to make full use of the rich resource on the Internet. The increasing interaction between industrial control systems and the outside Internet world, however, has made them an attractive target for a variety of cyber attacks, raising a great need to secure industrial control systems. Intrusion detection technology is one of the most important security precautions for industrial control systems. It can effectively detect potential attacks against industrial control systems. In this survey, we elaborate on the characteristics and the new security requirements of industrial control systems. After that, we present a new taxonomy of intrusion detection systems for industrial control systems based on different techniques: protocol analysis based, traffic mining based, and control process analysis based. In addition, we analyze the advantages and disadvantages of different categories of intrusion detection systems and discuss some future developments of intrusion detection systems for industrial control systems, in order to promote further research on intrusion detection technology for industrial control systems.

Keywords

Industrial control systems, intrusion detection, protocol analysis, traffic mining, control process analysis

Date received: 2 March 2018; accepted: 13 July 2018

Handling Editor: Posco Fung Po Tso

Introduction

Industrial control systems (ICS)[1] is a general term that encompasses several types of control systems and associated components used for industrial process control. ICS are mainly responsible for real-time data acquisition, system monitoring and automatic control and management of industrial processes. ICS have been widely used in important fields such as finance, transportation, water treatment, manufacturing, and power generation and distribution. They play an important role in a nation's critical infrastructure and directly affect a nation's economy. With an increasing integration with the computer and Internet technology (IT), ICS are becoming more intelligent and more open.

In recent years, the security issue of ICS has aroused wide public concerns, and the number of cyber attacks against ICS are increasing quickly. In 2010, the notorious Stuxnet malware[2] attacked the industrial control program in Iran's Natanz uranium enrichment base and got the control of some core devices, and then accelerated the uranium-enriched centrifuge abnormally and eventually led to scrapping of the centrifuge. The factory was forced to shut down. In 2015, BlackEnergy 3[3] attacked the Ukraine power grid by invading the

[1]School of Computer and Communication Engineering, University of Science & Technology Beijing, Beijing, China
[2]Beijing Key Laboratory of IoT Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[3]School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

Corresponding author:
Hong Li, Beijing Key Laboratory of IoT Information Security, Institute of Information Engineering, Chinese Academy of Sciences, No. 65, Xingshikou Road, Sijiqing Town, Haidian District, Beijing 100195, P.R. China.
Email: lihong@iie.ac.cn

power grid control center through VPN and tampered with the control instructions of the relay and cut off the circuit. At the same time, the network and control softwares of the system were destroyed and a telephone DDoS attack was launched to prevent the control system from sensing the abnormal states and then recovering the power grid system. At Black Hat 2017, Dr Staggs[4] presented how to invade the wind farm control system by physically connecting unmanned wind turbines in the United States. A series of security incidents indicate that ICS have become an attractive target for hackers. How to protect the security of ICS is one of the most urgent international issues.

Intrusion detection systems (IDS)[5] are designed for the automatic detection of malicious attacks. They collect and analyze network traffic, security logs, audit data, and information from key points of a computer system, to check whether there exit security violations in the system. Intrusion detection is also one of the most important means of maintaining the security of ICS. Currently, intrusion detection technology for ICS is a research hotspot, which has drawn great attention from both academia and industry. Accordingly, a broad scope of intrusion detection techniques for ICS is developed. The purpose of this article is to summarize the existing intrusion detection techniques for ICS and propose a new classification of ICS IDS by taking the particularities of ICS into consideration, in order to promote future research on ICS IDS.

The rest of this article is organized as follows. Section "Overview of ICS" introduces the architecture and security requirements of ICS. Section "Traditional Taxonomy of ICS IDS" presents the traditional classification of ICS IDS. In section "New Taxonomy of ICS IDS," we propose a new taxonomy of ICS IDS based on different techniques. In sections "Future Developments of ICS IDS" and "Conclusion," we discuss some possible developments of ICS IDS in the future and draw a conclusion of this article.

Overview of ICS

In this section, we mainly introduce the architecture and the security requirements of ICS and discuss the necessity of protecting the security of ICS with intrusion detection technologies.

Architecture of ICS

The main difference between ICS and traditional information systems is the close relationship with the physical world. As shown in Figure 1, the architecture of a modern industrial control system mainly consists of three layers: an enterprise management layer, a supervisory layer, and a field layer. The enterprise management layer mainly includes management information systems (MIS), enterprise resource planning (ERP) systems, manufacturing execution systems (MES), and other application systems. This layer uses the network communication technology to connect with the Internet, in order to realize the real-time monitoring and management of industrial processes and furthermore assist enterprise-level intelligent decision-making. The supervisory layer consists of process monitoring systems, historical and real-time databases, and a series of operator and engineer stations. This layer is responsible for data acquisition and transmission between the enterprise management layer and the field layer, and controlling field devices based on specific control logics. The field layer includes various types of sensors, actuators, transmitters, and I/O devices. This layer is mainly responsible for the perception of field information and the manipulation of field devices, and furthermore exchanging digital or analog data between different field devices through the field bus.

Security requirements of ICS

The security requirements of ICS differ significantly from those of traditional information systems. In traditional information systems, security means that unauthorized individuals or organizations cannot disclose, modify, steal, or damage a series of private, sensitive, and valuable data. However, security in traditional enclosed ICS is mainly understood as safety, that is, avoiding adverse impacts of failures of hardwares, softwares, or systems on the production safety, personal safety, and property safety. Nowadays, with the gradual openness of ICS, their connections with the Internet become more extensive, so ICS have both safety and security requirements. Specially, the security requirements of ICS are summarized as follows:

1. *Real-time*. In ICS, the operation time of each physical device is strictly limited. A slight deviation may damage the physical device and lead to serious industrial accidents.
2. *Limited computing resources*. The field devices in ICS include a variety of sensors and actuators with limited computing and storage resources, making it difficult to support the running of security programs.
3. *Fixed business logic*. ICS should follow specific business logics, to achieve specific production goals. Breakage to business logics is likely to cause serious accidents.
4. *Legacy systems*. There exists a significant portion of legacy sub-systems in ICS, making it difficult to upgrade ICS. During the continuous operation of ICS, field devices are likely to encounter persistent security threats, which

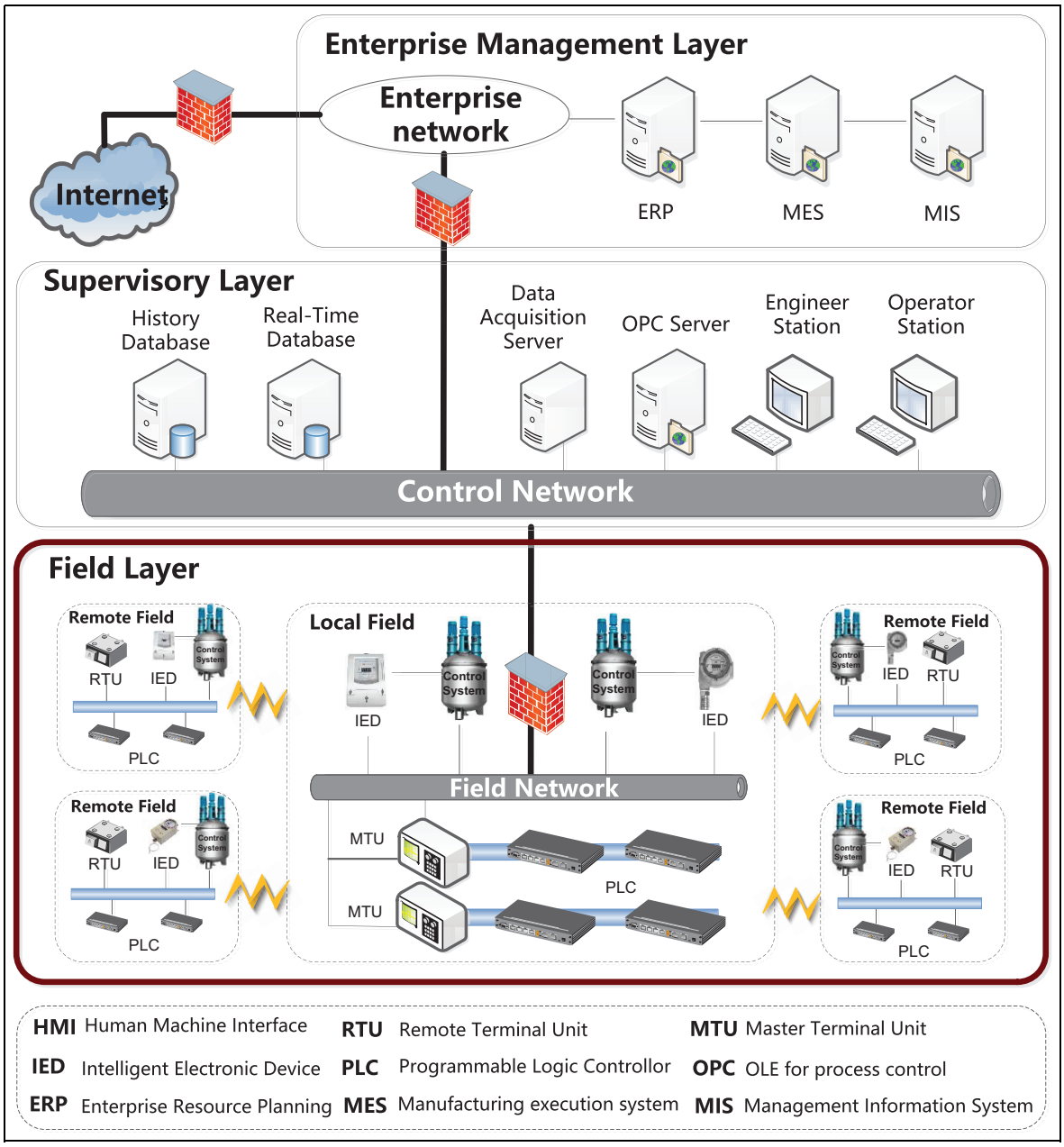

Figure 1. Architecture of industrial control system.

poses a great challenge to the current intrusion detection technology.

5. *Hard updating and restarting of industrial equipments*. To ensure the stability of ICS as well as the social and economic benefits, all equipments in ICS need to operate continuously, so it is very hard to stop the running of ICS for bug fixes or software updates.
6. *Poor security of industrial protocols*. With the introduction of Internet, industrial protocols that were originally secure in closed environments become vulnerable to cyber attacks in open environments, increasing the chance of important and even sensitive process data getting exposed to attackers.

Necessity of IDS to ICS

With the deep integration of ICS with the Internet, ICS can make full use of the universal protocols, software and hardware resources on the Internet, to achieve remote process monitoring and wide information exchange. Many emerging technologies (e.g. embedded, multi-standard network technology, and wireless technology) bring new development opportunities for traditional ICS. In spite of so many merits brought about

by modern information and communications technologies, the shift from isolated environments to open environments exposes ICS to a broad scope of malicious cyber attacks. Disruption of ICS could have a considerable negative impact on public safety or cause significant economic losses. Therefore, it is imperative and urgent to develop effective technologies for identifying malicious attacks against ICS.

IDS, a necessary complement to traditional firewall solutions, provide an effective way to detect malicious attacks against ICS. IDS can identify malicious activities violating security policies of ICS. In addition, they can provide evidences to inform the system administrator to make proper reactions to cyber attacks. Therefore, IDS can effectively keep ICS from suffering great destructions. As a result, developing effective intrusion detection technologies plays a considerably important role in protecting the security of ICS.

In the next section, we present the traditional taxonomy of ICS IDS.

Traditional taxonomy of ICS IDS

Since the occurrence of Stuxnet, the security of ICS has attracted a lot of attentions from both academia and industry. Intrusion detection technology has been widely regarded as an important means for defending the security of ICS.[6] However, intrusion detection technology designed for traditional information systems does not consider the particularity of ICS, so it still has limitations in ensuring the security of ICS. Although the research on ICS IDS develops quickly, it has not yet been clearly defined. In the following, we will try to give a reasonable definition of ICS IDS.

Mitchell and Chen[7] categorized ICS IDS according to detection techniques or data sources, as illustrated in Figure 2. Specifically, according to detection techniques, ICS IDS fall into two categories: misuse-based and anomaly-based. Misuse-based IDS mainly compare the collected system information with the known signatures in the misuse pattern database, thus to identify known intrusions effectively. The advantage of misuse-based IDS is the high detection rate of known attacks. However, they cannot detect zero-day (unknown) attacks. Anomaly-based IDS compare the current behavior of a system with its "normal behavior pattern." Once the deviation between the current behavior and the normal behavior is greater than a predefined threshold, an alert is raised. Anomaly-based IDS are capable of identifying a variety of unknown attacks, but has a relatively high false alarm rate. In addition, Mitchell and Chen summarized a new subclass of anomaly-based IDS: behavior specification-based IDS, which build the normal behavior model of a system based on industrial control protocols and system behavior specifications.

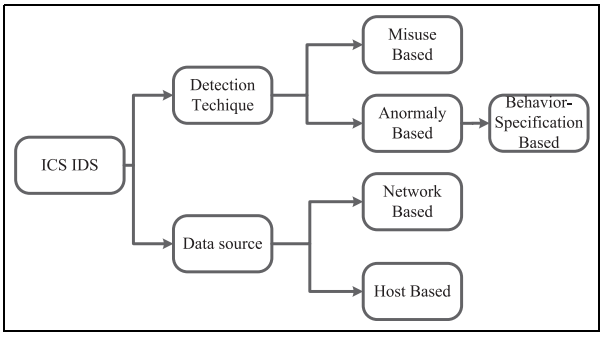

Figure 2. Traditional taxonomy of ICS IDS.[7]

On the contrary, ICS IDS can be divided into two categories according to different data sources: network-based and host-based. Network-based IDS use network adapters to collect and analyze network communication data in real time and find out the global intrusion behaviors using data analysis techniques. The disadvantage is that it cannot locate the specific node under attack. The host-based IDS mainly monitor the documents, procedures, and other information of a specific host to identify intrusion behaviors on the current node.

New taxonomy of ICS IDS

Traditional IDS are mainly designed for information systems, so the taxonomy of IDS does not pay much attention to the particularity of ICS, that is, the close relationship with the physical world. Therefore, we propose a new taxonomy of ICS IDS by taking into account both the detection techniques and the characteristics of ICS. In this article, ICS IDS are divided into three categories: protocol analysis-based, traffic mining-based, and control process analysis-based. The former two categories of technology mainly detect standard cyber attacks targeted at ICS, by analyzing the industrial protocols and traffic data generated in industrial control networks. The third category is mainly employed to detect semantic attacks, which exploit knowledge of specific control systems or physical processes to cause damage to ICS.

Protocol analysis–based IDS detect malicious attacks by checking whether the transmission packets in an industrial control network violate the industrial protocol specifications. This category of techniques mainly relies on the accurate definition of detection rules. Inaccurate rule definition usually results in a relatively high false alarm rate. In addition, it is time-consuming to parse every transmission packet. Traffic mining–based IDS overcome these shortcomings to some extent. This category of techniques tries to build

nonlinear and complex relationships between the network traffics and the normal/abnormal system behaviors. The two categories of technology originate from traditional information systems, but they do not take into account the close association between ICS and the physical world. This omission gives attackers chances to tamper with the industrial process data or destroy operating rules of field devices, and finally cause fatal damages to ICS. These attacks neither violate protocol specifications nor cause abnormal network traffics. As a result, control process analysis–based IDS emerged, attempting to identify this kind of semantic attacks. In general, the three categories of intrusion detection technologies constitute a relatively complete and nonoverlapping technical architecture of ICS IDS.

In the following of this section, we try to give a definition of ICS IDS and then elaborate on the new taxonomy of ICS IDS.

Definition of ICS IDS

IDS for ICS are devices or software applications or their combinations monitoring the behaviors of ICS for detecting malicious activities or policy violations by collecting and analyzing all available data (e.g. protocol specifications, system logs, host data, network traffics, sensor measurements, together with the domain-specific knowledge of industrial control). Any malicious activity should be reported to a system administrator and then remedial measures should be taken to keep ICS from suffering destructions.

Protocol analysis–based IDS

Protocol analysis–based IDS mainly use the protocol analysis technology to detect the changes of protocol format or status of data packets transmitted in the industrial control network and then identify abnormal behaviors of ICS.

Security analysis of common industrial protocols. Industrial communication protocols mainly considered the reliability and efficiency of ICS when they were designed. Traditional ICS are relatively enclosing, so the security of industrial communication protocols is rarely considered. Nowadays, with the gradual opening of ICS, common industrial protocols (e.g. MODBUS, ICCP/TASE.2, DNP3) become vulnerable to a variety of cyber attacks.

Modbus,[8] invented by Modicon (now a brand of Schneider Electric) in 1979, is the first bus protocol in the world to be actually used in industrial fields and has a wide range of applications. Modbus data communication adopts the Master/Slave mode. A Master sends a data request message to a Slave. If the Slave receives the correct message, it sends the response data to the Master. A Master can also send a message to modify the data on a Slave side, thus to achieve bidirectional data communication. Modbus communication uses the original data, without any encryption or authentication mechanisms, so attackers can parse Modbus addresses and function codes and then steal or tamper with the communication data. The lack of encryption and authentication mechanisms makes Modbus communication efficient but can also lead to serious security issues.

The Inter-Control Center Communications Protocol (ICCP) was proposed by the American Electric Power Research Institute (EPRI) in the 1990s and presented to the International Electrotechnical Commission (IEC). ICCP is mainly used for communication between different control centers of power industry. This protocol specifies that a client can communicate with multiple remote servers, and a server can also communicate with multiple remote clients. A client and a server should establish a deterministic access control bilateral table, in order to achieve reliable information exchange. ICCP makes some security improvements over Modbus, that is, the access control bilateral table defining the variable identifiers, variable types, and access permissions that the server and the client allow for communication. However, such security mechanisms still have some security risks. First, they lack data encryption and identity authentication mechanisms and are vulnerable to attacks such as theft and counterfeiting. Second, the bilateral tables are not hidden, so they can be tampered with easily.

DNP3[9] (Distributed Network Protocol) is a communication protocol between automation components. It is commonly used in industries like water treatment, power generation, and distribution. Compared to the first two protocols, DNP3 is more reliable and provides data fragmentation, data reassembly, data verification, link control, and priority control. Wide use of CRC (Cyclic Redundancy Check) checksum in the protocol ensures the data accuracy. However, enhancing the security mechanism undoubtedly increases the complexity of the protocol. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has reported several DNP3 vulnerabilities. In addition, the protocol still does not use authorization or encryption mechanisms and is vulnerable to man-in-the-middle attacks.

From the above analysis, we conclude that due to less consideration of security in the design phase, there exist a large number of security risks in industrial communication protocols. Therefore, intrusion detection technology based on protocol analysis emerges.

Public industrial communication protocol analysis–based IDS. In addition to a series of proprietary protocols,

there exist some public protocols in ICS, so researchers can easily access and analyze these protocols. A protocol specification generally defines the message formats and the communication patterns allowed by this protocol. Therefore, intrusion detection mechanisms can be designed based on protocol specifications. Any abnormal behavior violating the protocol specifications can be effectively detected. In 2007, Cheung et al.[10] proposed an intrusion detection mechanism, which used a model extracted from protocol specifications to describe the expected or acceptable behavior of a system and then detected unusual behaviors violating this model. Specifically, the technique was based on the TCP/IP field bus protocol (e.g. Modbus/TCP) and constructed a protocol specification model for the legal values of different fields and the legal relationships between different fields in a data packet. In addition, this technique built normal communication patterns based on the security requirements, the data transmission directions and the transmission ports of a specific industrial control system. The approach can effectively identify potential abnormal behaviors, but yields a higher false alarm rate since it may judge the emerging normal behaviors as anomaly.

Morris et al.[11] designed an intrusion detection technique for Modbus based on Snort (an intrusion detection software).[12] Snort rules were used to examine communication data in industrial networks and effectively detect illegal data. However, the detection accuracy of this method greatly relies on the precise definition of Snort rules. Morris improved this approach in 2013. They proposed 50 signature rules by analyzing the loopholes in the Modbus protocol and greatly improved the detection accuracy.

In order to achieve agile development, some researchers made refinements and improvements over traditional IDS, trying to make them adapted to ICS. Bro[13] is a network-based IDS developed by the University of Berkeley. It mainly collects network packets through bypass monitoring, and extracts corresponding events according to their contents. Afterward, it uses a protocol parser to parse protocols of different network layers and analyzes the above events based on policy scripts, thus to identify potential intrusions. Lin et al.[14] made some improvements over Bro, as shown in Figure 3. They designed a packet parser supporting industrial protocols like DNP3 and analyzed the legal values of different fields in a packet, thus to design security policies that match the protocol. This system can also parse other protocols used in ICS in addition to DNP3.

Proprietary industrial communication protocol analysis–based IDS. In addition to public protocols, some proprietary industrial protocols are used to develop IDS techniques in some specific industries. Hong et al.[15] analyzed automatic systems in substations of a smart grid and detected anomalies or malicious behaviors in multicast messages based on the IEC 61850 standards (e.g. Generic Object Oriented Substation Event (GOOSE) and Sample Value technology (SV)), which was issued by the IEC in 2004. This method based on proprietary protocol specifications can effectively detect malicious attacks such as Packet Tampering, Replay Attacks and Denial of Service (DoS).

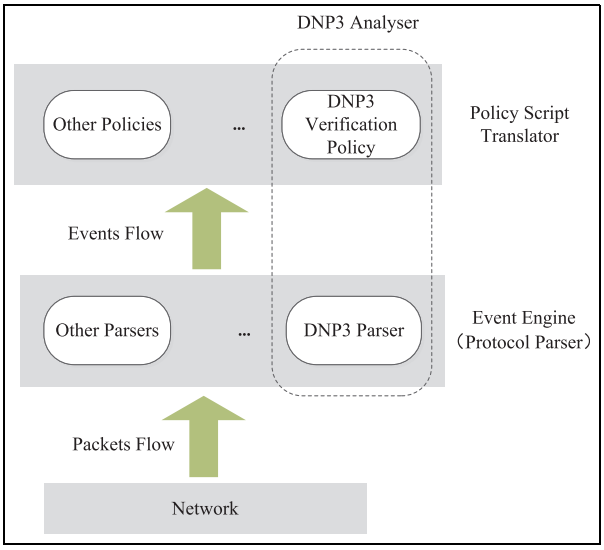

Figure 3. Bro-based ICS IDS.[14]

Optimization for protocol analysis–based IDS. Based on the above analysis, we can conclude that protocol analysis–based IDS mostly adopt the misuse-based intrusion detection techniques. In the detection process, contents of all packets should be analyzed deeply, which greatly reduces the efficiency of IDS. Therefore, researchers proposed some enhanced intrusion detection mechanisms for ICS, by combining the misuse-based and anomaly-based mechanisms.[16,17] First, the misuse-based detection technology was used to match the observed behavior of a system with the intrusion patterns in the database, in order to identify known attacks quickly. After that, the anomaly-based technology was employed to check the remaining data and recognize unknown attacks. Experimental results verified that approaches of this kind could effectively improve the detection accuracy and efficiency of ICS IDS.

Moreover, the protocol analysis–based IDS can also be combined with traffic analysis for more effective intrusion detection. Based on communication patterns stipulated in ICS protocol specifications and specific business logics, the detection rules can be extracted and then handed over to the traffic analysis module to

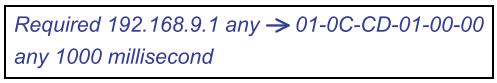

Figure 4. A comprehensive traffic model retrieved from protocol specifications.[18]

improve the accuracy of intrusion detection. Hadeli et al.[18] proposed such an intrusion detection scheme for power systems. This scheme extracts legal and illegal network traffic patterns from the predefined protocol specifications and the formal description of a system and then transforms them into comprehensive traffic models, as shown in Figure 4. This model indicates that an anomaly occurs if no GOOSE control message is sent from an IED (Intelligent Electronic Device) with IP 192.168.9.1 for more than 1000 ms, or a GOOSE control message is sent to a multicast address other than 01-0C-CD-01-00-00. The two words "any" imply that a control message can be sent to or from any port of a device. Afterward, these retrieved traffic rules are submitted to Snort and transformed into Snort rules, allowing Snort to alert on traffic that is expected but not observed.

Yusheng et al.[19] proposed a new algorithm named SD-IDS (Stereo Depth IDS), which can perform deep inspection for Modbus TCP traffic in real time. The SD-IDS algorithm consists of two parts: rule extraction and deep inspection. The rule extraction module is responsible for extracting semantic relationships among key fields in the Modbus TCP protocol. The deep inspection module performs anomaly or intrusion detection based on the extracted relationships and the real-time traffic data.

Traffic mining–based IDS

Most protocol analysis–based IDS have the following shortcomings: poor detection ability against unknown attacks and long time to parse data packets. In order to overcome these shortcomings to some extent, traffic mining–based intrusion detection techniques are developed. The advantage of this kind of technology is the ability to detect a wide range of unknown attacks.

ICS have relatively fixed operation objects and business processes, a simple and static network topology, and a small number of applications, which results in a relatively stable ICS traffic under normal conditions. Traffic data are a kind of important information reflecting the security status of ICS. This provides the possibility of traffic mining–based intrusion detection technology. Traffic mining–based IDS mainly collect traffic data from different regions in ICS and then apply data mining (e.g. neural networks (NNs), Bayesian classifiers, support vector machines (SVMs), decision trees, and other data mining algorithms) or data analysis (statistical analysis) technology to the collected data, in order to identify anomalous behaviors in industrial networks.

A traffic mining–based intrusion detection method proposed by Stavroulakis and Stamp[20] extracts five tuples (source IP address, destination IP address, transport-layer protocol, source port, destination port), the traffic duration, and the average time interval between adjacent packets from the collected traffic data. Then the data mining technology is employed to distinguish the abnormal behaviors from the normal behaviors of the system and finally detect a variety of intrusions such as Replay, Denial of Service (DoS), Man-in-the-Middle, and Packet Tampering.

Hou et al.[21] proposed an approach based on the probabilistic principal component analysis (PCA) to detect abnormal traffic in industrial networks. They concluded that random burst traffic is an important cause of false alarm. Afterward, they built a probabilistic PCA model for the traffic matrix and analyzed the impact of random burst traffic on PCA. Then, an Iterative Variational Bayesian algorithm was used to estimate the model parameters, which were further used to estimate the distribution function of the rank of the traffic matrix. Finally, the abnormal traffic of ICS was detected according to the change of the rank. Experimental results showed that this method is able to effectively suppress the interference of random burst traffic to intrusion detection.

Artificial NN is another effective data mining technique, which simulates the thinking process of human brains. It can be used to analyze large amounts of data and then identify unknown intrusions on ICS. In the process of traffic mining, NNs establish nonlinear mapping relationships between traffic features and system security states (normal/abnormal) through model training and then classify the real-time data based on trained models and finally identify abnormal traffics or malicious intrusions in ICS effectively. Vollmer and Manic[22] extracted network traffic features (e.g. packet size, ICMP protocol ID, ICMP sequence number, ICMP code, ICMP type, IP protocol ID, IP protocol option, IP survival time) to construct input vectors for NN model training. After feature normalization, the error backpropagation algorithm was used to train the NN model. During detection, the real-time network traffic features were extracted to construct input vectors, which were classified by the NN model. Accordingly, attacks like DoS and eavesdropping could be detected. In their follow-up work,[23] they also proposed a sliding window–based feature vector extraction technique which could dynamically and accurately extract 16 kinds of network features, for example, the number of IP addresses in a real packet sequence, the maximum and minimum number of packets related to a single IP, the average time interval between adjacent

data packets, the window duration, the data transmission speed, the number of protocols in the window, and the number of identification codes. In addition, they used a comprehensive method combining BP and LM to detect abnormal traffics and achieved satisfactory intrusion detection accuracy.

Ashfaq et al.[24] proposed an effective semi-supervised NN learning mechanism, which requires only a small amount of labeled data. This approach first trains a fuzzy classifier (a NN model with random weights) with a small amount of labeled data and then use it to classify the unlabeled data. The output of the classifier is a membership vector. Each entry of this vector denotes the degree the current input vector belongs to a corresponding category. In the model training process, the high-ambiguity and low-ambiguity data are combined with the original training set to retrain the fuzzy classifier.

However, training a NN model consumes a lot of time and computing resources. To overcome this shortcoming, Linda et al.[25–27] realized an intrusion detection mechanism based on fuzzy logic. Fuzzy logic is another simulation of human brain to do fuzzy reasoning and judgment. It consumes less time and computing resources when compared to NN. Linda et al.[25] used fuzzy rules to represent the normal behavior patterns of ICS. The fuzzy rules can be extracted from the network packet sequence using an adjusted online nearest neighbor clustering algorithm. This learning method requires less computing resources, so it can run on embedded sensors. During detection, the scheme computes the degree the input vectors belong to the normal behavior patterns based on the outputs of multiple fuzzy rules, thus to identify intrusions. In their follow-up work,[26] TYPE-2 fuzzy logic was integrated into the model to minimize the impacts of uncertainties on the system performance and enhancing the sensors' perception of network security status, in order to further improve the intrusion detection accuracy. Linda et al.[27] designed an IDS using the TYPE-2 fuzzy logic to encode domain knowledge in specific industrial environments and network systems and describe the relationships between the possibility of intrusion occurrence and the network communication features. According to the experimental results, the architecture can adjust the algorithm thresholds adaptively for more accurate intrusion detection.

In addition, some researchers used SVM for intrusion detection on ICS. They mapped the linearly inseparable traffic data into a high-dimensional feature space using kernel functions and constructed a superplane to distinguish the normal and abnormal behaviors. Maglaras and Jiang[6] proposed an ICS intrusion detection algorithm based on One-Class Support Vector Machine (OCSVM), which does not require any labeled training data or prior knowledge about attack categories and can be trained offline. This method is

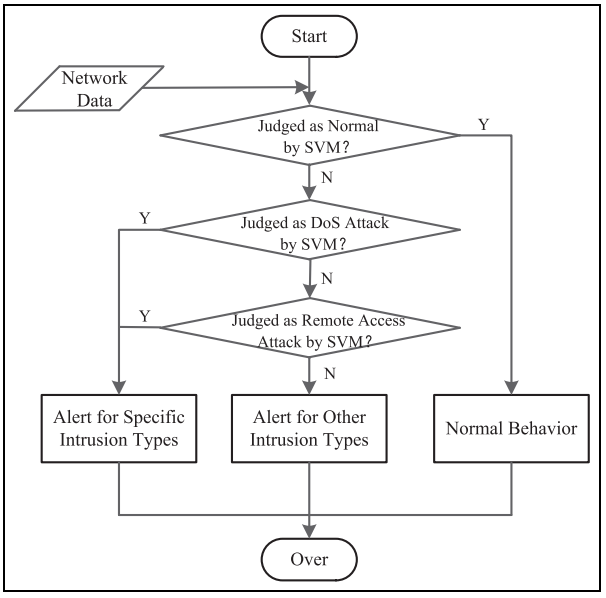

Figure 5. The hierarchical SVM-based ICS IDS.[28]

able to construct traffic models for multiple protocols that detect a variety of intrusion behaviors against ICS, for example, Man-in-the-Middle and SYNFlood. Traditional SVM is only able to distinguish the normal behaviors from the abnormal behaviors, but cannot determine the specific types of anomalies. Therefore, Luo[28] designed an intrusion detection approach based on multi-class SVM. As shown in Figure 5, multiple SVM classifiers are combined to determine the exact category of an intrusion.

Javaid et al.[29] proposed a deep learning approach to distinguish between normal and abnormal traffic data. First, this method uses a sparse auto-encoder to perform unsupervised learning. The unsupervised learning network includes an input layer, an implicit feature layer, and an output layer. By adjusting the network parameters, the output layer should reproduce the input data as accurately as possible. Next, the training process uses the learned features and the labeled training data to train the classifier and finally completes classification tasks.

Aghdam and Kabiri[30] designed an ant colony–based algorithm to automatically identify important traffic features for intrusion detection. This algorithm discards redundant or invalid features and improves the efficiency and accuracy of intrusion detection. Compared with traditional IDS, this algorithm can identify more malicious attacks and greatly reduce the computational overhead. Tsang and Kwong[31] designed a multi-agent architecture for distributed intrusion detection and defense in large switching networks. In this architecture, the authors used an efficient biological heuristic learning model named the improved ant colony clustering

model, which uses a heuristic search to obtain the optimal clusters approximately. The basic idea of the model is to perform online nearest neighbor clustering on the training data set (only the normal data), in order to get clusters and then transform them into fuzzy rules. One cluster yields one corresponding fuzzy rule. Afterward, different fuzzy rules work on the test data to determine how much the test data belong to the normal behavior. Kiss et al.[32] formalized all the data in ICS as time series and proposed an intrusion detection mechanism based on clustering algorithms to identify potential attacks against ICS.

Caselli et al.[33,34] discovered a new kind of network traffic attacks, that is, sequence attacks, which send misplaced messages in industrial communication systems to drive field devices or the whole control system to malfunction or even strike directly at physical processes. In order to detect sequence attacks, the authors proposed to transform network traffic traces into time-ordered lists of events and then used a Discrete-Time Markov Chain (DTMC) model to describe normal message sequences (communications patterns). Finally, traffic data analysis was performed based on the DTMC model to identify sequence attacks. Ferling et al.[35] held the opinion that the sequence-aware intrusion detection models are often large and difficult to handle and further result in time-consuming traffic analysis. Accordingly, they proposed a method which builds smaller traffic models by combining states in the DTMC model differing just for the range of Information Object Addresses (IOAs) used in the IEC-104 protocol. The smaller models can reduce the complexity effectively while still keeping the detection accuracy for most sequence attacks.

Marsden et al.[36] stated that the Modbus TCP protocol is usually vulnerable to cyber attacks due to its unencrypted and unauthenticated nature, so the authors proposed a probability risk identification–based intrusion detection system (PRI-IDS) based on analyzing network traffics of Modbus TCP/IP to identify replay attacks. This method marks traffic data with predefined risk values and then caches periods of traffic data and generates risk values for those cached periods. Cached periods with risk values outside of 1 standard deviation from the mean value are identified as possible replay attacks.

Dong et al.[37] proposed a traffic feature map–based intrusion detection approach for industrial networks. An information entropy–based method is employed to extract key traffic features and then construct traffic feature vectors. Afterward, a multiple correlation analysis algorithm is applied to the traffic feature vectors to build a feature relationship map. Then, the discrete cosine transform (DCT) and singular value decomposition (SVD) methods are employed to generate a perceptual hash digest database of normal and abnormal traffic feature maps. Finally, intrusion detection rules are extracted from the database. The rules are important for modeling the periodic features of industrial network traffics. This method transforms text traffic data into figure information and provides ICS IDS with new solutions.

Control process analysis–based IDS

Control process analysis–based IDS make full use of the semantic information and peculiarity of ICS to detect intrusions, which is a great difference from IDS designed for traditional IT systems. Currently, this kind of technology includes process data analysis–based, control command analysis–based, and ICS physical model–based IDS techniques.

Process data analysis–based IDS. Process data (e.g. reactor pressure, temperature, and pH level) play an important role in ICS. These data generally indicate the security status of a physical process. Unexpected change of these data usually indicates intrusion occurrence.

Krotofil et al.[38] held the opinion that the values of industrial process variables should conform to certain physical laws. The authors proposed a lightweight real-time attack algorithm that can run on the micro controllers of field devices and tamper with process data. This attack uses a technique called runs analysis to extract the noise characteristics from the original value sequence of a process variable and then gets the dynamic nature of the value sequence by using a triangle approximation technique. Based on the extracted noise characteristics and series dynamics, the attack algorithm can generate a fake but plausible value sequence to replace the true values of the process variable. Moreover, the authors proposed a detection method based on cluster entropy to check the consistency and rationality of the value sequence of a process variable. Once the consistency or rationality is violated, an intrusion behavior is detected.

Hadžiosmanović et al.[39] designed an intrusion detection method for ICS based on the sematic analysis of process variables. This method consists of three steps: (1) extracting the current values of process variables from the network traffic; (2) classifying the observed process variables into three categories according to their semantics: constants, enums, and continuous variables; and (3) constructing a behavioral model for each process variable based on their types, and then raising an alarm when the actual behavior deviates from the expected behavior predicted by the model. The model proposed in this article can effectively identify control process–oriented intrusions, but the description of feature semantics is still not thorough. The authors stated that in their future work, they would extract richer

context information to assist intrusion detection, such as more structural protocols and project configuration files.

Carcano et al.[40] used multiple process variables to describe the states of a control system by designing a formal modeling language and then proposed an intrusion detection technology based on the proximity between the current system state and the critical system states. The modeling language mainly supports the Modbus protocol and can be easily extended to other industrial protocols. In addition, it can provide a corresponding formalized virtual system similar to the real physical system for IDS to monitor. Furthermore, the language defines the critical states and different danger levels for ICS, and how to measure the distance between different system states. In the process of detection, the method calculates the proximity between the current state and the critical states. If the proximity exceeds a preset threshold, an alert is raised.

Colbert et al.[41] devised a control process–oriented intrusion detection technique for ICS. They proposed two control process–oriented detection methods to enhance the traditional ICS IDS. Unlike traditional anomaly-based IDS, this mechanism is mainly based on the key process variables defined by an ICS operator. The advantage is that the operator is more familiar with the peculiarity of ICS. The thresholds of the key process variables are determined by the network engineer and the ICS operator collaboratively. Sensors monitor the values of key process variables and raise an alarm once the values exceed their thresholds. In addition, the authors proposed an intrusion detection method based on the process network parameters, which are also determined by the both the network engineer and the ICS operator. These parameters can indicate a lack of important control components or a significant amount of unusual traffic which is not likely to occur in normal industrial environments. Although the process network parameters do not indicate severe problems as the critical process variables do, but they can still generate alerts for some potential malicious system behaviors.

Kiss et al.[42] proposed a Gaussian Mixture Model (GMM) to detect cyber attacks against measurement data sent to controllers (e.g. PLC). In this scheme, the GMM performs soft clustering on the measurement data. The training process is based on the Expectation-Maximization (EM) algorithm. Finally, the best classification of each measurement is obtained. Observations outside the normal clusters are judged as outliers. The data densities of abnormal clusters are usually significantly lower than those of normal clusters. The GMM is an unsupervised soft-classification model and can give the confidence level that each measurement belongs to a given cluster. The experimental results showed that the GMM has a better intrusion detection performance on ICS than the traditional k-means clustering algorithms.

Gao et al.[43] presented three attacks in ICS: command injection, response injection, and Denial of Service. A behavior monitoring method based on an artificial NN model, which leverages knowledge of the physical properties of the controlled system, was proposed to detect the response injection attacks. IDS results showed that NN is a promising mechanism for detecting response injection attacks.

Moya et al.[44] presented a kind of highly threatening attacks against ICS, that is, Monitoring-Control Attacks (MCAs) in which attackers manipulate control signals by fabricating sensor measurements in a feedback loop. MCAs are likely to occur due to low cost and able to inflict severe consequences upon ICS. However, it is hard to detect MCAs since they usually hide in normal sensor measurements. To detect MCAs, a semantic analysis framework for IDS in power grids was designed in this article. The framework is composed of two modules running in parallel: a Correlation Index Generator (CIG) and a Correlation Knowledge Base (CKB). The former is mainly used to index correlated MCAs and the latter is updated aperiodically according to the change of attacks' Correlation Indices (CI). The framework has the ability to detect MCAs with satisfying detection accuracy and estimate attack consequences in real time.

Control command analysis–based IDS. Control commands are also an important part in ICS. Adversaries sometime manipulate the control commands to achieve attack goals. Therefore, analyzing control commands can help to find out a portion of intrusion behaviors against ICS.

Carcano et al.[45] proposed a novel IDS technology, which designs a new language to describe the control commands involved in power grids and provides a semantic description for detection features. Then, the method uses two strategies to analyze Modbus packets. One is the single packet signature–based strategy, which detects illegal packets sent by PLCs or RTUs by making semantic analysis on control commands. The other is the state-based strategy, since invalid control commands usually drive the system into a critical state, so the strategy detects intrusions by tracking the states of ICS.

Similarly, Lin et al.[46] proposed a semantic analysis technique for control commands, on the basis of distributed ICS. This technique can forecast the consequences of control commands based on the prior knowledge about the network and the physical facilities in power grids and then reveal the intention of attackers. The semantic analysis framework includes: (1) analyzing network packets of ICS by Bro to obtain control

commands; (2) monitoring and storing the sensor measurements from the links between the control center and each substation; and (3) triggering the anomaly analysis module to predict possible consequences of control commands. This article evaluated the proposed scheme on the IEEE 30 bus system and the results showed that (1) by opening three outgoing lines, an attacker can bypass the traditional IDS and steer the system to a critical state and (2) semantic analysis of control commands spends less time and can achieve reliable intrusion detection results.

ICS physical model–based IDS. A reasonable physical model is able to accurately describe the evolution of an industrial control system. The future expected outputs of a system can be predicted by a physical model together with appropriate prediction mechanisms. Then, the observed outputs of the system can be compared with the expected values and yield a residual series. Performing statistical analysis on the residual series can realize intrusion detection. When the system operates normally, the residuals are close to zero. Once the system is attacked, the observed outputs deviate significantly from the expected outputs. In other words, the residuals deviate significantly from zero.[47]

Cárdenas et al.[48] constructed an approximately linear state-space model for ICS to describe the system behavior. The model indicates that the current state of a system depends on its previous states and the control inputs. The constructed state-space model can be used to forecast sensor measurements in real time. Then, the observed sensor measurements are compared with the forecasts. The residuals are utilized to detect malicious attacks against ICS. The authors also presented two intrusion detection methods: sequence-based detection and change-based detection. The purpose of the sequence-based detection is to detect anomalies as quickly as possible, so the detection problem is regarded as the optimal stopping problem in sequence analysis theory, that is, determining a sequence of the minimum length based on which a judgment can be made. The purpose of the change-based detection is to detect possible changes at an uncertain time point. For example, a transition from a normal state to an abnormal state is detected based on whether a residual or an accumulated residual exceeds a predefined threshold.

Edelmayer et al.[49] constructed an equivalent linear time-invariant representation of the original linear time-varying control system and then built a detection filter based on the linear time-invariant system. The detection filter can achieve similar detection accuracy on the original system. Sridhar and Govindarasu[50] built an intrusion detection and mitigation mechanism for smart grids based on the knowledge of power systems and detected attacks such as malicious data injection by predicting future generation load.

Liu et al.[51] discovered a new kind of data injection attacks against state estimation in power networks in 2011. This attack injects erroneous data into the system persistently until the system crashes, but keeps the residual magnitude at each step below the threshold, thus to bypass the stateless intrusion detection scheme. This is the first stealthy attack against ICS. Since then, stealthy attacks have emerged in a variety of industrial control scenarios (e.g. chemical process control[48] and industrial waste water treatment[52]).

However, until 2016, Urbina et al.[53] stated that existing intrusion detection technology still cannot detect stealthy attacks effectively. In this article, the authors studied how to limit the impacts of stealthy attacks. Although this kind of stealthy attacks cannot be detected, their impacts can be limited to some extent by properly configuring different detection schemes and metrics. The authors proposed a novel metric to measure the impacts of stealthy attacks. The horizontal axis denotes the expected time interval between two adjacent false alarms, and the vertical axis denotes the maximum deviation that a stealthy attack can achieve per unit time. Through theoretical analysis and experimental verification, it was proved that based on this new metric and a reasonable configuration of different detection schemes, the negative impacts of stealthy attacks can be effectively limited. After that, some researchers conducted further research on stealthy attacks, but they mainly focused on how to perform stealthy attacks on specific ICS[54] or exploring the impacts of stealthy attacks on some more complex systems.[55] As a result, detecting stealthy attacks against ICS becomes an urgent issue in the future research.

Tian et al.[56] considered a stronger false data injection (FDI) attack scenario against the state model estimation of smart grids, in which the adversary can also attempt to detect the use of moving target defense (MTD) against FDI before they launch FDI. This kind of advanced FDI attacks was called the Parameter Confirming-First (PCF) FDI attack in this article. Therefore, in order to enhance the stealthiness of MTD, the authors designed a hidden MTD approach able to make itself invisible to attackers. In addition, the hidden MTD is capable of inducing adversaries to launch useless attacks and increase their probability of getting exposed. Finally, the hidden MTD was demonstrated to be equal to the traditional MTD in maintaining the power flows of the whole grid.

Myers et al.[57] argued that ICS usually define the number and order of task executions strictly. Each control system has a unique task flow. Therefore, the authors proposed an ICS attack detection method based on process mining. This method extracted a

control process model for ICS by monitoring and analyzing the log files of control devices and then used the consistency detection method to identify the abnormal system behavior that did not conform to the constructed process model.

Future developments of ICS IDS

Although the intrusion detection technology for ICS develops quickly, there is still a big room for the improvement of ICS IDS. For example, in specific ICS environments, it is necessary to develop a scientific and accurate evaluation system for the performance of IDS, which is also an important research area in the future. In addition, ICS are large and complex and consist of widely distributed sub-systems. As a result, there is a great need to develop distributed and collaborative IDS. The distributed and parallel architecture of ICS IDS are expected to effectively mitigate the negative impacts brought about by limited computing resources in ICS, thus to improve the efficiency of IDS. However, how to measure or mine spatial and temporal correlations between distributed IDS, based on which to fuse a set of distributed and maybe conflicting detection results and thus to get accurate and real-time comprehensive detection results, is a new and interesting issue.

Another biggest challenge for future ICS IDS is the problem of how to respond to alarms. In some control systems, simply reporting the alert to administrators can be considered enough. However, it is necessary for us to consider automated response mechanisms in order to guarantee the safety and security of ICS. In addition, there is little research focusing on whether and how the control algorithms (e.g. P, PI and proportional–integral–derivative (PID) control) can be utilized to correct or mitigate the harmful impacts of attacks until now, which is also a promising solution.

Another important issue is how to optimize intrusion detection algorithms automatically during running. ICS generally need to work continuously and the system parameters (e.g. steady system states, security requirements, and system constrains) of a target ICS may change with time, so the intrusion detection algorithm need to optimize themselves automatically based on perceptions of changing contexts in order to maintain a satisfying detection accuracy.

Conclusion

Nowadays, ICS have become more and more open, and the security issue of ICS also becomes prominent. Due to the particularity of ICS, traditional IDS designed for IT systems cannot work very well on ICS. In recent years, the intrusion detection technology for ICS has been developed quickly. It can help ICS to detect a variety of intrusions and reduce the incidence of industrial accidents brought about by malicious attacks. According to the different techniques used by ICS IDS, we classified ICS IDS into three categories—protocol analysis–based IDS, traffic mining–based IDS, and control process analysis–based IDS—and analyzed different categories of ICS IDS comprehensively, trying to promote the future research on ICS IDS.

Acknowledgements

The authors appreciate the reviewers for their helpful comments and suggestions for the improvement of this paper.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work is supported by the Fundamental Research Funds for the Central Universities (FRF-TP-17-058A1), the National Natural Science Foundation of China (61702506, 61503365 and 61502466), and the National Social Science Foundation of China (17ZDA331).

References

1. Stouffer K, Falco J and Scarfone K. *Guide to industrial control systems (ICS) security*. NIST special publication 800-82, 2011, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r1.pdf
2. Langner R. Stuxnet: dissecting a cyberwarfare weapon. *IEEE Secur Priv* 2011; 9(3): 49–51.
3. Lee RM, Assante MJ and Conway T. *Analysis of the cyber attack on the Ukrainian power grid*. Washington, DC: Electricity Information Sharing and Analysis Center (E-ISAC), 2016.
4. Staggs J. *Adventures in attacking wind farm control networks*. San Francisco, CA: black hat, 2017.
5. Yang D, Usynin A and Hines J. Anomaly-based intrusion detection for scada systems. In: *Proceedings of the 2006 5th international topical meeting on nuclear plant instrumentation controls, and human machine interface technology*, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.1649&rep=rep1&type=pdf
6. Maglaras LA and Jiang J. Intrusion detection in SCADA systems using machine learning techniques. In: *Proceedings of 2014 science and information conference*, London, UK, 27–29 August 2014, pp.626–631. New York: IEEE.
7. Mitchell R and Chen IR. A survey of intrusion detection techniques for cyber-physical systems. *ACM Comput Surv* 2014; 46(4): 55.
8. Modbus-IDA. *Modbus application protocol specification V1.1a*. North Grafton, MA, 2004, www.modbus.org/specs.php

9. Curtis K. *A DNP3 protocol primer. DNP User Group*, 2005, https://www.dnp.org/AboutUs/DNP3%20Primer%20Rev%20A.pdf
10. Cheung S, Dutertre B, Fong M, et al. Using model-based intrusion detection for scada networks. In: *Proceedings of the 2007 SCADA security scientific symposium*, vol. 46, pp.1–12, http://www.csl.sri.com/users/cheung/SCADA-IDS-S4-2007.pdf
11. Morris T, Vaughn R and Dandass Y. A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems. In: *Proceedings of the 2012 45th Hawaii international conference on system science (HICSS)*, Maui, HI, 4–7 January 2012, pp.2338–2345. New York: IEEE.
12. Roesch M. Snort—lightweight intrusion detection for networks. In: *Proceedings of the 1999 13th systems administration conference (LISA)*, vol. 99, pp.229–238, https://www.usenix.org/legacy/event/lisa99/full_papers/roesch/roesch.pdf
13. Paxson V. Bro: a system for detecting network intruders in real-time. *Comput Netw* 1999; 31(23–24): 2435–2463.
14. Lin H, Slagell A, Di Martino C, et al. Adapting bro into SCADA: building a specification-based intrusion detection system for the DNP3 protocol. In: *Proceedings of the 2013 eighth annual cyber security and information intelligence research workshop*, p.5, http://publish.illinois.edu/science-of-security-lablet/files/2014/06/Adapting-Bro-into-SCADA-Building-a-Specification-based-Intrusion-Detection-System-for-the-DNP3-Protocol.pdf
15. Hong J, Liu CC and Govindarasu M. Detection of cyber intrusions using network-based multicast messages for substation automation. In: *Proceedings of the 2014 IEEE PES conference on innovative smart grid technologies conference (ISGT)*, Washington, DC, 19–22 November 2014, pp.1–5. New York: IEEE.
16. Yang Y, McLaughlin K, Littler T, et al. Rule-based intrusion detection system for SCADA networks. In: *Proceedings of the 2013 2nd IET renewable power generation conference (RPG)*, Beijing, China, 9–11 September 2013. New York: IEEE.
17. Yang Y, McLaughlin K, Littler T, et al. Intrusion detection system for IEC 60870-5-104 based SCADA networks. In: *Proceedings of the 2013 IEEE power and energy society general meeting (PES)*, Vancouver, BC, Canada, 21–25 July 2013, pp. 1–5. New York: IEEE.
18. Hadeli H, Schierholz R, Braendle M, et al. Leveraging determinism in industrial control systems for advanced anomaly detection and reliable security configuration. In: *Proceedings of the 2009 IEEE conference on emerging technologies & factory automation (ETFA)*, Mallorca, 22–25 September 2009, pp.1–8. New York: IEEE.
19. Yusheng W, Kefeng F, Yingxu L, et al. Intrusion detection of industrial control system based on Modbus TCP protocol. In: *Proceedings Proceeding of the 2017 IEEE 13th international symposium on autonomous decentralized system (ISADS)*, Bangkok, Thailand, 22–24 March 2017, pp.156–162. New York: IEEE.
20. Stavroulakis P and Stamp M. *Handbook of information and communication security*. Berlin: Springer, 2010.
21. Hou C, Jiang H, Rui W, et al. A probabilistic principal component analysis approach for detecting traffic anomaly in industrial networks. *J Xi'an Jiaotong Univ* 2012; 46: 70–75.
22. Vollmer T and Manic M. Computationally efficient neural network intrusion security awareness. In: *Proceedings of the 2009 2nd international symposium on resilient control systems (ISRCS)*, Idaho Falls, ID, 11–13 August 2009, pp.25–30. New York: IEEE.
23. Linda O, Vollmer T and Manic M. Neural network based intrusion detection system for critical infrastructures. In: *Proceedings of the 2009 international joint conference on neural networks (IJCNN)*, Atlanta, GA, 14–19 June 2009, pp.1827–1834. New York: IEEE.
24. Ashfaq RAR, Wang XZ, Huang JZ, et al. Fuzziness based semi-supervised learning approach for intrusion detection system. *Inform Sci* 2017; 378: 484–497.
25. Linda O, Manic M, Vollmer T, et al. Fuzzy logic based anomaly detection for embedded network security cyber sensor. In: *Proceedings of the 2011 IEEE symposium on computational intelligence in cyber security (CICS)*, Paris, 11–15 April 2011, pp.202–209. New York: IEEE.
26. Linda O, Manic M, Alves-Foss J, et al. Towards resilient critical infrastructures: application of type-2 fuzzy logic in embedded network security cyber sensor. In: *Proceedings of the 2011 4th international symposium on resilient control systems (ISRCS)*, Boise, ID, 9–11 August 2011, pp.26–32. New York: IEEE.
27. Linda O, Manic M and Vollmer T. Improving cybersecurity of smart grid systems via anomaly detection and linguistic domain knowledge. In: *Proceedings of the 2012 5th international symposium on resilient control systems (ISRCS)*, Salt Lake City, UT, 14–16 August 2012, pp.48–54. New York: IEEE.
28. Luo Y. *Research and design on intrusion detection methods for industrial control system*. PhD Thesis, Zhejiang University, Hangzhou, China, 2013.
29. Javaid A, Niyaz Q, Sun W, et al. A deep learning approach for network intrusion detection system. In: *Proceedings Proceedings of the 2016 9th EAI international conference on bio-inspired information and communications technologies (formerly BIONETICS)*, pp.21–26, http://eudl.eu/pdf/10.4108/eai.3-12-2015.2262516
30. Aghdam MH and Kabiri P. Feature selection for intrusion detection system using ant colony optimization. *Int J Netw Secur* 2016; 18(3): 420–432.
31. Tsang CH and Kwong S. Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction. In: *Proceedings of the 2005 IEEE international conference on industrial technology (ICIT)*, Hong Kong, China, 14–17 December 2005, pp.51–56. New York: IEEE.
32. Kiss I, Genge B, Haller P, et al. Data clustering-based anomaly detection in industrial control systems. In: *Proceedings of the 2014 IEEE international conference on intelligent computer communication and processing (ICCP)*, Cluj Napoca, 4–6 September 2014, pp.275–281. New York: IEEE.
33. Caselli M, Zambon E, Petit J, et al. Modeling message sequences for intrusion detection in industrial control systems. In: *Proceedings of the 2015 international conference on critical infrastructure protection*, Arlington, VA, 16–18 March 2015, pp.49–71. Berlin: Springer.

34. Caselli M, Zambon E and Kargl F. Sequence-aware intrusion detection in industrial control systems. In: *Proceedings of the 2015 1st ACM workshop on cyber-physical system security*, Singapore, 14 April, pp.13–24. New York: ACM.
35. Ferling B, Chromik J, Caselli M, et al. Intrusion detection for sequence-based attacks with reduced traffic models. In: *Proceedings of the 2018 international conference on measurement, modelling and evaluation of computing systems*, Erlangen, 26–28 February 2018, pp.53–67. Berlin: Springer.
36. Marsden T, Moustafa N, Sitnikova E, et al. Probability risk identification based intrusion detection system for SCADA systems. In: *Proceedings of 2017 international conference on mobile networks and management*, Melbourne, 13–15 December 2017, pp.353–363. Cham: Springer.
37. Dong RH, Wu DF, Zhang QY, et al. Traffic characteristic map-based intrusion detection model for industrial internet. *Int J Netw Secur* 2018; 20(2): 359–370.
38. Krotofil M, Larsen J and Gollmann D. The process matters: ensuring data veracity in cyber-physical systems. In: *Proceedings of the 2015 10th ACM symposium on information, computer and communications security*, pp.133–144. New York: ACM, http://www.cse.chalmers.se/edu/course/DAT300/2016%20SLIDESNOTES/[DAT300]Group8PaperPresentation.pdf
39. Hadžiosmanović D, Sommer R, Zambon E, et al. Through the eye of the PLC: semantic security monitoring for industrial processes. In: *Proceedings of the 2014 30th annual computer security applications conference*, pp.126–135. New York: ACM, http://www.icir.org/robin/papers/acsac14-ics.pdf
40. Carcano A, Coletta A, Guglielmi M, et al. A multidimensional critical state analysis for detecting intrusions in SCADA systems. *IEEE T Indus Inform* 2011; 7(2): 179–186.
41. Colbert E, Sullivan D, Hutchinson S, et al. A process-oriented intrusion detection method for industrial control systems. In: *Proceedings of the 2016 international conference on cyber warfare and security*, Boston, MA, 17–18 March 2016, p.497. Sonning Common: Academic Conferences International Limited.
42. Kiss I, Genge B and Haller P. A clustering-based approach to detect cyber attacks in process control systems. In: *Proceedings of the 2015 IEEE 13th international conference on industrial informatics (INDIN)*, Cambridge, 22–24 July 2015, pp.142–148. New York: IEEE.
43. Gao W, Morris T, Reaves B, et al. On SCADA control system command and response injection and intrusion detection. In: *Proceedings of the eCrime researchers summit (eCrime)*, Dallas, TX, 18–20 October 2010, pp.1–9. New York: IEEE.
44. Moya C, Hong J and Wang J. *Application of correlation indices on intrusion detection systems: protecting the power grid against coordinated attacks* (arXiv preprint arXiv:1806.03544), 2018.
45. Carcano A, Fovino IN, Masera M, et al. State-based network intrusion detection systems for scada protocols: a proof of concept. In: *Proceedings of the 2009 international workshop on critical information infrastructures security*, Bonn, 30 September–2 October 2009, pp.138–150. Berlin: Springer.
46. Lin H, Slagell A, Kalbarczyk Z, et al. Semantic security analysis of scada networks to detect malicious control commands in power grids. In: *Proceedings of the 2013 first ACM workshop on smart energy grid security*, Berlin, 8 November 2013, pp. 29–34. New York: ACM.
47. Patton RJ. Robustness in model-based fault diagnosis: the 1995 situation. *Ann Rev Contr* 1997; 21: 103–123.
48. Cárdenas AA, Amin S, Lin ZS, et al. Attacks against process control systems: risk assessment, detection, and response. In: *Proceedings of the 2011 6th ACM symposium on information, computer and communications security*, pp.355–366. New York: ACM, https://pdfs.semanticscholar.org/ee2e/e3dca15c4836b07c7a0e2c265329a9298901.pdf
49. Edelmayer A, Bokor J, Szigeti F, et al. Robust detection filter design in the presence of time-varying system perturbations. *Automatica* 1997; 33(3): 471–475.
50. Sridhar S and Govindarasu M. Model-based attack detection and mitigation for automatic generation control. *IEEE T Smart Grid* 2014; 5(2): 580–591.
51. Liu Y, Ning P and Reiter MK. False data injection attacks against state estimation in electric power grids. *ACM T Inform Syst Secur* 2011; 14(1): 13.
52. Amin S, Litrico X, Sastry S, et al. Cyber security of water SCADA systems—part I: analysis and experimentation of stealthy deception attacks. *IEEE T Contr Syst Technol* 2013; 21(5): 1963–1970.
53. Urbina DI, Giraldo JA, Cardenas AA, et al. Limiting the impact of stealthy attacks on industrial control systems. In: *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, Vienna, 24–28 October 2016, pp.1092–1105. New York: ACM.
54. Kleinmann A, Amichay O, Wool A, et al. Stealthy deception attacks against SCADA systems. In: Katsikas SK, Cuppens F, Cuppens N, et al. *Computer security*. Berlin: Springer, 2017, pp.93–109.
55. Kung E, Dey S and Shi L. The performance and limitations of -stealthy attacks on higher order systems. *IEEE T Automat Contr* 2017; 62(2): 941–947.
56. Tian J, Tan R, Guan X, et al. Enhanced hidden moving target defense in smart grids. *IEEE T Smart Grid* 2018; 1(1): 1–15.
57. Myers D, Radke K, Suriadi S, et al. Process discovery for industrial control system cyber attack detection. In: *Proceedings of the 2017 IFIP international conference on ICT systems security and privacy protection*, Rome, 29–30 May 2017, pp.61–75. Berlin: Springer.