IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 16, 2020, accepted February 25, 2020, date of publication March 2, 2020, date of current version March 13, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2977423

A Survey of Network Attacks on Cyber-Physical Systems

LIWEI CAO, XIAONING JIANG, YUMEI ZHAO, SHOUGUANG WANG, (Senior Member, IEEE), DAN YOU, (Student Member, IEEE), AND XIANLI XU

School of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

Corresponding author: Xiaoning Jiang (jiangxiaoning@zjgsu.edu.cn)

This work was supported in the part by the Zhejiang Provincial Key R&D Program of China under Grant 2018C01084, in part by the the Zhejiang Natural Science Foundation under Grant LQ20F020009, in part by the Zhejiang Gongshang University, Zhejiang Provincial Key Laboratory of New Network Standards and Technologies under Grant 2013E10012.

ABSTRACT A cyber-physical system (CPS) typically consists of the plant, sensors, actuators, the controller and a communication network. The communication network connects the individual components to achieve the computing and communication in the CPS. It also makes the CPS vulnerable to network attacks. How to deal with the network attacks in CPSs has become a research hotspot. This paper surveys the types of network attacks in CPSs, the intrusion detection methods and the attack defense strategies. The future research directions of CPSs network security are also presented.

INDEX TERMS Cyber-physical systems, network attacks, intrusion detection, defense strategies.

I. INTRODUCTION

The notion of cyber-physical systems (CPSs) was first proposed by National Aeronautics and Space Administration (NASA) in 1992, and described in detail by Baheti and Gill [1]. Nowadays, they have become the core technology of the next generation of industrial revolution [2], and many works have been done to prove their importance, such as the top of eight information technologies [3], the German Industry 4.0 [4], Industrial Internet in the U.S., [5], ARTEMIS (Advanced Research and Technology for Embedded Intelligence and Systems) [6] and CPS European Roadmap and Strategy in the European Union [7].

CPSs have been widely used in industrial control systems, advanced communications, smart power grids [8], transportation networks [9], vehicular social networks [10], [11], and many areas closely related to daily fields. A CPS integrates computation, communication and control (3C) technologies [12] to monitor and control processes [13], [14], and its overall framework is shown in Fig. 1. A CPS can be divided into three layers according to the framework: perception execution layer, data transmission layer, application control layer [15], [16]. Perception execution layer consists of physical components such as sensors and actuators. Application control layer mainly provides services for users.

The associate editor coordinating the review of this manuscript and approving it for publication was Guanjun Liu.

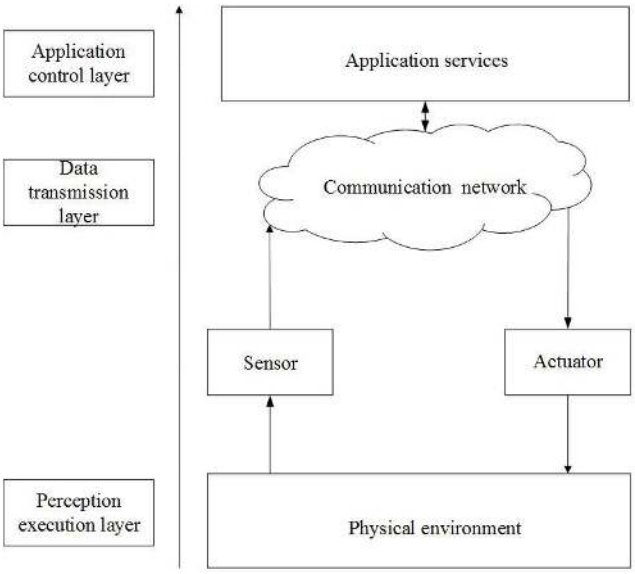

FIGURE 1. Architecture of a CPS.

Data transmission layer connects the perception execution layer and the application control layer, and is mainly used to deliver information.

The data transmission layer transmits information through the communication network, but the use of the

communication network makes CPSs more vulnerable to network attacks. Some behaviors of a CPS may be changed due to network attacks, and then the CPS will reach an unsafe state that damages the system. The unsafe state will affect production processes and pose a threat to economic and society [17]–[19].

Recently, the problem of network attacks in CPSs has become a research hotspot. The problem of intrusion detection [20]–[22] and defense strategies in CPSs are reviewed in this paper. There are many works developing intrusion detection methods and defense strategies for specific types of network attacks [20], [21], [23]–[25], such as deception attacks, covert attacks and so on. The key point of defense strategies is to detect intrusions on-line and protect the system from damages by initiating a security module once an intrusion is detected.

In this paper, we classify network attacks in CPSs and review the work on intrusion detection and defense strategies. The content of the paper is organized as follows. In section 2, we talk about the classification of network attacks in CPSs. In Section 3, the development and classification of intrusion detection technologies are introduced. In section 4, several different network attack defense strategies are summarized and section 5 concludes this paper and gives the research directions in the future work.

II. CLASSIFICATION OF NETWORK ATTACKS

Typically, there are three types of network attacks on CPSs based on the framework in Fig. 1, i.e., network attacks on the perception execution layer, network attacks on the data transmission layer, and network attacks on the application control layer [15]. We introduce them in this section one after another.

A. NETWORK ATTACKS ON THE PERCEPTION EXECUTION LAYER

Perception execution layer is composed of various nodes like sensors and actuators, where the data from the physical components are collected and the commands from the control center are communicated. Most nodes at this layer are deployed in an unsupervised environment. Thus, they are easy to be the targets of an intruder.

The research on network attacks on the perception execution layer mainly focuses on the security issues of sensors and actuators. There are basically four types of network attacks on the perceptual execution layer, i.e., Actuator Enablement attacks (AE-attacks), Actuator Disablement attacks (AD-attacks), Sensor Erasure attacks (SE-attacks), and Sensor Insertion attacks (SI-attacks) [24]. Once a sensor or an actuator is attacked, the information from the plant or the instruction to be executed on the plant may be tampered with. As a result, an unsafe state may be reached that damages the system. There are other common attacks such as deception attacks, robust pole-dynamics attacks, covert attacks and robust attacks.

B. NETWORK ATTACKS ON THE DATA TRANSMISSION LAYER

Data transmission layer connects the perception execution layer and the application control layer to realize the goal of conveying information between these two layers. A communication network is the core bearer network of the data transmission layer. It mainly transmits data through communication networks such as the Internet, a private network, and a local area network. The diversity of communication network access methods and the complexity of network equipment and architecture will bring certain security threats to CPSs.

The layer also has the ability to process and manage massive information. Networks may be congested with a large number of data to be transmitted in the data transmission layer and then CPSs will be vulnerable to network attacks.

Although it is the most difficult for intruders to attack data transmission layer, after data transmission layer was successfully intruded, the intruder can freely change the information transmitted in attacked network channel. The Man-in-the-Middle Attack [26], as one of the most powerful network attacks on the data transmission layer, can observe, hide, create, and even change the information transmitted from one device to another in the communication channel [20]. In other words, for the attack to send fake data to any party, and then CPS will be driven into an unsafe state that damages the system.

The denial-of-service (DoS) [27]–[29] attack is a kind of resource depletion attack, which takes the advantage of the network protocols/software defects or sends a lot of useless requests to exhaust the resources of the attacked object. Finally, it makes the server or the communication networks fail to provide services [30].

In CPSs, a DoS attack uses the malicious program to consume the communication bandwidth to prevent the interaction of information between controllers and actuators. DoS attacks are mainly caused by malicious attacks. These attacks will cut off the connection between the actuator and the controller, then the controller cannot get the feedback information in time, thus the system will be out of control. A large number of invalid service requests will occupy routing and server resources [31], finally the performance becomes bad, even collapse. During a DoS attack, no messages are sent or received on the channel.

C. NETWORK ATTACKS ON THE APPLICATION CONTROL LAYER

Application control layer is made up of controllers and user applications. After receiving the information transmitted from the data transmission layer, the application control layer generates execution control commands after judgments, and feeds back them to the underlying physical unit of the perception execution layer through the data transmission layer, and then the actuators perform related operations.

Some applications in this layer will storage a large amount of user privacy data, such as the personal information and

consumption habits of users. An intruder injects a script into the system maliciously or attacks a database, obtaining unauthorized access to the system and then making a serious impact on the application control layer. Once the application control layer is attacked, a lot of user privacy information can be leaked. At the same time, because a single defense strategy is difficult to meet requirements of multiple application systems, application control layer security faces huge challenges.

To our best knowledge, the research in the literature mainly focuses on network attacks at the perception execution layer and the data transmission layer. Thus, in the following two sections, we review intrusion detection methods and defense strategies for network attacks at the perception execution layer and the data transmission layer only.

III. INTRUSION DETECTION

Intrusion detection [32] is an important technology to guarantee the security of networks so that illegal operations launched by intruders such as attackers and hackers can be avoided via authentication identification.

The concepts of intrusion and intrusion detection were proposed by Anderson for the first time [33]. Denning [34] put forward the concept of real-time detection and a host-based intrusion detection model named Intrusion Detection Expert Systems (IDES). Lunt and Jagannathan [35] further improved the intrusion detection model proposing the idea of real-time detection independent system platform based on IDES.

Houbeilein *et al.* [36] developed a network-based intrusion detection system named Network Security Monitor (NSM), which directly used Network flows as the source of audit data for the first time. Since then, intrusion detection methods were divided into two types: host-based Intrusion Detection Systems (IDS) and network-based IDS. Some host-based IDS used the detection sequence of the server operating system as the main input source to detect intrusion behaviors; while most network-based IDS used monitoring network faults as the detection mechanism, but some used server-based detection modes and typical IDS static anomaly detection algorithm.

According to intrusion detection technology, intrusion detection can be divided into misuse detection and anomaly detection. Misuse detection includes expert systems [35], simple pattern matching [37], model checking (MC) method [38], and state transition analysis [39], etc. Anomaly detection includes statistical methods [40], profile-based method [41], neural network-based methods [40] and genetic algorithm based methods, etc.

In the following two subsections, intrusion detection methods for network attacks at the perception execution layer and the data transmission layer are introduced in detail.

A. INTRUSION DETECTION ON PERCEPTION EXECUTION LAYER

Hoehn and Zhang [42] proposed a new method to detect cover attacks and zero dynamic attacks on CPSs. The previous attack strategies were very complex and required relying on sound system knowledge. In addition, the attack signals were completely invisible in sensor readings. As a result, common fault diagnosis systems had been unable to detect such attacks and trigger alerts. Hoehn *et al.* introduced a modulation matrix to the path of the control variable. The input behavior of the system was changed by modulation matrix, so the intruder lost sound knowledge of the system, and then cover attacks and zero dynamic attacks can be detected.

Carvalho *et al.* [24] adopted a model-based approach to accurately capture the impact of vulnerabilities and attacks on control systems. The model-based approach describes the unsafe behavior that is possibly induced by attackers and the resilience that the system defender wants to achieve. This method also allows the monitoring deviations of the attacked system from the normal system conduct. Their work complements the work on anomaly/intrusion detection [43]–[46].

Teng *et al.* [47] proposed a self-adaptive collaboration intrusion detection method based on 2-class support vector machines and decision trees. The collaborative and adaptive intrusion detection model was created and implemented using the Environments-classes, agents, roles, groups, and objects (E-CARGO) model and adaptive scheduling mechanisms are developed. The feasibility and efficiency of their proposed method are validated by experimental results.

When a CPS suffers from a stealthy attack, state estimation may be changed by injecting biased values into sensor-collected measurements. Acosta *et al.* [48] presented an approach of intrusion detection to detect stealthy attacks. The approach is based on an extremely randomized tree algorithm and kernel principal component analysis. It reduces the computational cost by dimensionality reduction but guarantees the feature of high accuracy.

B. INTRUSION DETECTION ON DATA TRANSMISSION LAYER

Zhengbing *et al.* [49] proposed a lightweight intrusion detection system that can detect intrusions in real time, efficiently and effectively. In their study, behavior profiles and data mining techniques were tools to detect coordinated attacks.

Lima *et al.* [20] developed an intrusion detection module that can detect man-in-the middle attacks. This module can prevent the system from arriving in an unsafe state by forcing managers to disable all controllable events of CPS after detecting the intrusion that would definitely lead system to lose resources.

By injecting spoofed null data or a power save-poll (PS-Poll) frame to a system, attacker who launches a power save denial of service (PS-Dos) attack to 802.11 networks will gain the buffered frames of the sleeping stations. Agarwal *et al.* [50] proposed a method based on real-time discrete event systems to detect PS-Dos attacks of 802.11 networks. This method has the characteristics of high accuracy and fast detection rate and overcomes the drawbacks of 802.11 networks.

IV. DEFENSE STRATEGIES

Defense strategies are of great importance to the security of CPSs. Generally, we first detect network attacks in a CPS and then activate a corresponding defense strategy once a specific attack is detected.

The research on CPS network attacks is mostly based on the framework of discrete event systems (DESs). Some works use Petri nets to model and analyze CPSs. Petri nets as a mathematical tool has been used to handle many problems [51]–[60] in DESs. Others use finite state automata to model and analyze CPS, such as [61], [62]. Thorsley and Teneketzis [22] studied the intrusion detection of network attacks under DES framework and how to mitigate the damage caused by attacks. Attackers totally changed the set of enabled events ordered by the monitor. The main goal of the research was to design a monitor that can meet the specifications after abnormal operations and attacks.

This section introduces defense strategies against the attacks at the perception execution layer and the data transmission layer. Little research is about the defense strategies at the application control layer, which is thereby not detailed in this paper.

A. DEFENSE STRATEGIES AGAINST PERCEPTION EXECUTION LAYER ATTACKS

1) ATTACK ON SENSORS

Goes *et al.* [63] studied the security of CPSs. A general model to detect deception attacks was proposed. Deception attacks can change sensor readings and mislead the controller, with the purpose of inducing the CPS into an undesirable state. A new bipartite transfer structure was introduced, called the insertion-deletion structure (IDA), to capture the interaction between the system and the attacker. The IDA was a discrete transformation system and the foundation of the attack strategy synthesis problem. It can predict all possible actions of an attacker including some steady behaviors, and can predict which state the system will reach when the attacker toke different actions.

Meira-Goes *et al.* [64] also studied the synthesis of deception attacks by stealth sensors. The work [64] was based on the framework of a random DES, resulting in a broader class of attack strategies. Goes *et al.* studied the problem from the attacker's perspective and modeled the attack strategy as probabilistic automata. According to the possibility of the system reaching an unsafe state, they presented an optimal attack strategy.

Su [19] studied deception attacks under the framework of DES. After intercepting sensor readings from a target system, an attacker can arbitrarily alter them. The changed sensor readings would induce a given supervisor to issue an incorrect control command, which can drive the system to an undesirable state. First, a new concept of attack ability and attack under bounded sensor reading alterations (ABSRA) were presented. The system was modeled as a finite automaton. As long as the system model and a given supervisor can be modeled by a finite-state automaton, it was then shown that the optimal (or least restrictive) ABSRA existed and can be computed by a specific composition algorithm called ABSRA synthesis algorithm. Based on this algorithm, Su proposed a supervisor synthesis algorithm to ensure that the non-empty synthesized supervisor would remain ''robust'' to any ABSRA. A supervisor that is ABSRA-robust in the sense that any ABSRA will either be detectable or inflict no damage to the system.

Jeon and Eun [65] studied a sensor attack named Robust Pole-dynamics Attack (RPDA) of CPSs. The RPDA can be built with limited knowledge of a target system and can stay stealthy until the attack succeeds. Specifically, the attack manifested itself by injecting faulty data into the sensor to undermine the stability of the feedback controller. The feedback controller instability would make the system unstable. When a unique nominal model of target dynamics was known, stealth can be retained by deploying a mechanism similar to the disturbance observer (DOB), which can be designed to absorb the effects of mismatches between nominal and actual dynamics until the attack was successful. The success of the attack depended on whether the system state exceeded the threshold. Sensor attacks using the dynamics of unstable systems had been studied before, and the generation of such attacks needed an accurate understanding of the stealth of the target system, in other words, the attack must completely eliminate the effects of instability at the sensor to avoid being detected. If not, the attack would be detected anomaly detection. In their work, the DOB mechanism was used to absorb the attack mismatch and the degree of absorption was selected to delay detection until the attack was successful. Therefore, this attack posed a more serious threat to the CPS than a conventional attack.

Yin [62] considered the problem of network attacks defense under the framework of Mealy automata. Under this framework, observable events can be observed only when the relevant sensors were working normally. Without any restrictive assumptions, the problem of monitor synthesis was addressed for security and non-blocking specifications. Yin proposed an approach based on mode-transformation method, which consisted of two stages. First, a transformation algorithm was proposed that transformed the non-blocking supervisor synthesis problem of Mealy automata into a conventional supervisor synthesis problem under partial observation. Then it was proved that a comprehensive supervisor for the converting problems can indeed solve the original problem.

Wakaiki *et al.* [66] considered the supervisory control problem of DES with multiple intruders. The goal of the supervisor was to enforce a specific language on the plant without knowing which the intruder was, regardless of the behavior of the intruder. They proposed a new concept of observability under attacks, which took into account the ability of attacker to change symbols. For replacement-removal attacks, a supervisor was constructed by a robust product automaton. Product automata were also used to test the observability under replacement-removal attacks.

Two algorithms were proposed to reconstruct state by sensor measurements. The first algorithm reconstructed the state from a batch of sensor measurements while the other was able to incorporate new measurements as they become available, in the spirit of a Luenberger observer [67]. However, these two algorithms would be damaged by noise imposed by attackers. Shoukry and Tabuada introduced the notion of sparse observability to describe how to solve this problem. An event-triggered method was used to verify timing performance of these two algorithms.

2) ATTACK ON ACTUATORS

Carvalho *et al.* [21] considered the AE-attacks. In the case of the AE-attacks, some actuators were vulnerable to attacks. The problem that the authors address was to protect a system from a predefined set of unsafe states after an attack. The specific approach was as follows: firstly, they modeled the system under AE-attacks as a deterministic finite state automaton. Next, a model-based approach was adopted to accurately capture the vulnerabilities and attacks of the control system. The unsafe behavior that an attacker was trying to induce and the resiliency that the system defender was hoping to achieve can be described by the model-based methods. In addition, the model-based methods can monitor deviations of the attacked system from normal system. Finally, based on the results of supervisory control and fault diagnosis of DES, they proposed a defense strategy that can detect attacks and disable all controllable actuator events immediately once an attack was detected. The new concept of AE-security controllability was defined, which represented the ability to use the proposed defense strategy to avoid the system entering an unsafe state after an attack, which was a variant of safe controllability in [68]. Finally, an algorithm was proposed to verify whether the system can automatically control security.

3) ATTACKS ON SENSORS AND ACTUATORS

Carvalho *et al.* [24] considered the intrusion detection and mitigation problems of supervisory control systems under AE-attacks, SE-attacks and SI-attacks. Attackers can intrude some vulnerable sensors and then erase real sensor readings or insert false ones. It may lead the system to enter an unsafe state. First, their work presented deterministic finite-state automata for these classes of attacks. Then, a defense strategy was proposed to detect such attacks online and disable all controllable events after detection. Finally, an algorithmic program was developed to verify whether the system can be protected from damages caused by attacks, where the damages were modeled as the accessibility of a predefined set of unsafe system states. The approach was similar to the work in [68], which proposed a strategy of fault detection on-line and reconfiguration of control law when faults are detected. In this case, the sufficient and necessary condition to be concerned with is ''General Form of safe controllability (GF-safe controllability)'', which was a property to be satisfied if the system was successfully satisfied to prevent damage caused by AE, SE or SI attacks and a General Form of attack (GF-attack) variant of safe controllability in [68]. At the same time, a test was developed to verify ''GF-safe controllability''.

Lima *et al.* [23] proposed a defense strategy involving security module that can prevent network attacks on sensors and/or actuators. When the system was not attacked, this strategy would not change the behavior of the closed-loop system, that is, the security module only disabled controlled events when an intrusion event caused the system to enter an unsafe state. In addition, they introduced undetectable network attack (DNA) security and detectable network attack (UNA) security to verify some properties of this strategy and gave necessary and sufficient conditions of these two definitions. For sake of implement the security module, it is necessary to ensure that it would not run counter to the designed supervisory control system. In the last, they also presented the necessary and sufficient conditions for the UNA and DNA security of the system.

Teixeira *et al.* [69] studied the typical control structure of control systems under network attacks. On this basis, a general antagonism model was discussed that was suitable for many attack scenarios, and the attack resources were mapped to the corresponding dimension of the attack space. By the detailed discussion of replay attacks, zero dynamic attacks and bias injection attacks, the concept of confrontation model and attack space were illustrated. Subsequently, the work [70] mainly considered the case where an attacker performed the zero dynamic attack on the system. Firstly, the stealth characteristics of the attack were characterized and analyzed, and then the system structure was modified to detect such attacks. Finally, the zero dynamic attack was solved by modifying the input, output and dynamic characteristics of the system.

Pasqualetti *et al.* [71] modeled CPS under attacks as a descriptor system whose constraints were unknown inputs that affected state and measurement. Firstly, based on the established model, the concepts of attack detectability and recognizability were defined by the impact of attacks on the output measurement. Then, the limitations of a class of monitors were pointed out from two aspects of system theory and graph theory. The main performance is as follows: 1) the monitor can detect the network physical attack if and only if the signal of the attacker triggers zero dynamics of the input/output system; 2) the monitor can carry out undetectable or unrecognized attacks if the monitoring signal was not clear, the monitor cannot detect or recognize attacks. Finally, a graph theory description of undetectable attack was proposed.

Park *et al.* [72] solved the problem of designing a robust attack for the opponent to break through the uncertain CPS without being detected. First they reinterpreted the zero-dynamics attack in terms of the normal representation. Then, a new zero dynamic attack method was proposed for uncertain systems [9], [70], [71]. The alternative method used a disturbance observer and did not need perfect system knowledge to stay stealthy. A robust zero-dynamics attack required a nominal model of a plant as well as the input and

output signals of the system. The presented attack illustrated how the attackers can use disclosure resources of CPSs rather than perfect model knowledge.

Hoehn and Zhang [42] inserted the modulation matrix into the actuator signal path to alter the output behavior of system and detect attacks, and Fritz and Zhang [73] extended this method to all actuator and sensor channels to detect replay attacks and covert attacks, and adapted it to meet the requirements of DES. They accomplished attack detection by comparing the received signals from the CPS with the expected behavior of the model. Fritz and Zhang mainly contributed to the attack model for covert attacks and replay attacks of CPS modeled by DES, as well as detection methods for such network attacks. On the basis of altering the input and output behavior, the proposed approach can be easily achieved by a permutation matrix. In addition, it didn't limit the vulnerability of sensor and actuator channels. Therefore, an attacker can access all sensor and actuator data, that is, all sensor and actuator signals can be observed and changed.

B. DEFENSE STRATEGIES AGAINST DATA TRANSMISSION LAYER ATTACKS

1) MAN-IN-THE-MIDDLE ATTACKS

Man-in-the-middle attacks are one of the most powerful network attacks of CPSs. Once a CPS suffered from a man-in-the-middle attack, the intruder can observe, hide, create or change information in the attacked sensor or control communication channel [20], [25].

Lima *et al.* [20] studied the man-in-the-middle attack. They built a deterministic model of systems under sensor channel attacks and actuator channel attacks, and proposed a defense strategy that detected intrusions and protected the system from damages caused by man-in-the-middle attacks on communication networks channels in CPS. In addition, they defined a safe controllability under network attacks, called NA-safe controllability, which can detect attacks in the network and prevented the system from reaching an unsafe state, and an algorithm was presented to verify this attribute. Finally, a kind of computing device was developed to detect the attack that led to an unsafe state, which was called intrusion detection module.

Lima *et al.* [25] extended the work [20]. First, they proved that correctness of the NA-safe controllability verification algorithm in [20]. They showed how to use a security module against attacks in the communication network channel of CPS, and finally proved that NA-safe controllability was a sufficient and necessary condition for the security module.

2) DENIAL-OF-SERVICE ATTACKS

At present, mathematical models such as Queuing model [67], Bernoulli model [74] and Markov model [75] have been applied to the study of CPSs performance under DoS attacks.

Befekadu *et al.* [75] studied a finite-horizon risk-sensitive control problem of DoS attacks under a Markov modulated model. Attackers would use a hidden Markov model, randomly injected the control packets in the system. Befekadu *et al.* introduced a new equivalent probability measure to characterize all properties of a stochastic process. Then a hidden Markov model was extended by a memoryless Bernoulli process to get a perfect risk-sensitive control strategy.

Amin *et al.* [76] studied the effects of DoS attacks on the performance of linear quadratic gaussian (LQG) control. They aimed to design a control strategy to minimize system cost function in DoS attack environment and proposed an optimal solution based on positive semidefinite programming.

Foroush and Martinez [77] presented an plant-jammer-operator control strategy for periodic DoS attacks with limited power in the control system. They proposed an event-triggering time-sequence to reduce communication. In addition, they proved this triggering time-sequence can resist DoS attack and ensure the stability of the system state under some circumstances.

De Persis and Tesi [78] presented a general DoS attack model that only constrains the attacker action in time by posing limitations on the frequency of DoS attacks and their duration. It is possible to capture many different types of DoS attacks, including trivial, periodic, random and protocol-aware jamming attacks. Later, based on the DoS attack model in [78], Feng and Tesi [79] studied maximally robust controllers under DoS attacks. They aimed to maximize frequency and continuance of DoS attacks without undamaging closed-loop stability. And Dolk *et al.* [80] studied a framework for output-based dynamic event-triggered control (ETC) systems under DoS attacks.

While advanced controllers were exchanging information, a DoS attack may analyze the transmitted information and find vulnerabilities. Once a vulnerability of system was discovered, the system can be intruded by the DoS attack, which caused a (Direct current) DC microgrid to enter an unsafe state. A framework was proposed to study the fault ride-through capability of DC microgrids in DoS attacks [81]. In the last, two simulation case studies showed the effectiveness of that framework.

V. CONCLUSION AND FUTURE WORK

With the advent of the 5G era, information systems and physical systems are undergoing tremendous changes. CPSs have become prevalent in a vast range of applications, including industrial control systems, advanced communication, smart power grids and transportation networks. However, people cannot ignore the serious threats to CPSs caused by network attacks while considering saving production costs and improving production efficiency. Therefore, it is increasingly important to improve the safety and performance of CPSs. In recent years, more and more cases of network attacks on CPSs show that the destructiveness and pertinence of network attacks have been improved than before. Attackers can use the network to launch attacks on public infrastructures such as smart grids, smart transportation, and large hydropower

stations, which have seriously threatened national security, social stability, and economic development. Therefore, it is urgent to quickly and effectively improve the CPS defense capability. This paper reviews the types of network attacks in CPS, intrusion detection methods and defense strategies in the literature.

CPSs in the future may no longer face a single attack only but face multiple attacks. It could happen that a CPS is attacked by multiple intruders at the same time or the intruder is capable of launching multiple network attacks simultaneously on the system. For example, a system may be subjected to replay attacks and covert attacks simultaneously. Obviously, the existing detection methods and defense strategies for a single attack are not enough to ensure the security of CPSs in this case. An important object of our future work is thus detecting each of the multiple attacks quickly and designing a comprehensive defense strategy to make the system run normally. Wakaiki *et al.* [66] first studied multiple attacks and Gao *et al.* [82] recently studied how to detect multiple attacks on DESs but did not provide corresponding defense strategies. In summary, the current research on intrusion detection and defense strategy design for multiple attacks is still in its infancy. How to deal with multiple network attacks in CPSs should be investigated in the future work. On the other hand, the attack issues in the future work may be studied by generalizing the problem setting on the considered CPSs. We may consider the case that we do not know for sure the initial state of the system or we can only get the partial observation of the behavior of the considered system. Besides, since almost all studies in the literature use automata to model CPSs when dealing with attack issues, we may try to use Petri nets as a modelling tool to solve the problem to see if we can gain some advantages in computational complexity.

REFERENCES

[1] R. Baheti and H. Gill, "Cyber-physical systems," *Impact Control Technol.*, vol. 12, no. 1, pp. 161–166, Mar. 2011.

[2] H. Ge, D. Yue, X. P. Xie, S. Deng, and S. L. Hu, "Analysis of cyber physical systems security issue via uncertainty approaches," in *Proc. Adv. Comput. Methods Life Syst. Model. Simulation*. Nanjing, China: Springer, 2017, ch. 6, sec. 6, pp. 421–431.

[3] L. U. Challenge, "Leadership under challenge: Information technology R&D in a competitive world, president's council of advisors on science and technology (PCAST) report," Tech. Rep., 2007.

[4] H. Kagermann, "Change through digitization-Value creation in the age of Industry 4.0," in *Management of Permanent Change, National Academy of Science and Engineering*, Berlin, Germany: Springer, 2015, ch. 2, pp. 23–45.

[5] M. Annunziata and P. C. Evans, "The industrial Internet@ work," Gen. Electr., Boston, MA, USA, White Paper, 2013.

[6] *Advanced Research and Technology for Embedded Intelligence and Systems*, ARTEMIS Ind. Assoc., Eindhoven, The Netherlands, 2007.

[7] B. Schätz, M. Törngren, R. Passerone, H. Pfeifer, S. Bensalem, J. McDermid, A. S. Vincentelli, and M. V. Cengarle, "CyPhERS-cyber-physical European roadmap and strategy," Fortiss GmbH, Munich, Germany, Tech. Rep. 611430, 2015.

[8] M. M. Rana, L. Li, and S. W. Su, "Cyber attack protection and control of microgrids," *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 2, pp. 602–609, Mar. 2018.

[9] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, Jan. 2015.

[10] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, Y. Zhang, F. R. Yu, and B. Hu, "Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1314–1345, 2nd Quart., 2019.

[11] Y. Xie, L. Liu, R. Li, J. Hu, Y. Han, and X. Peng, "Security-aware signal packing algorithm for CAN-based automotive cyber-physical systems," *IEEE/CAA J. Automatica Sinica*, vol. 2, no. 4, pp. 422–430, Oct. 2015.

[12] E. A. Lee, "Cyber physical systems: Design challenges," in *Proc. 11th IEEE Int. Symp. Object Compon.-Oriented Real-Time Distrib. Comput. (ISORC)*, Orlando, FL, USA, May 2008, pp. 363–369.

[13] J. Shi, J. Wan, H. Yan, and H. Suo, "A survey of cyber-physical systems," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2011, pp. 1–6.

[14] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[15] T. Lu, B. Xu, X. Guo, L. Zhao, and F. Xie, "A new multilevel framework for cyber-physical system security," in *Proc. 1st Int. Workshop Swarm Edge Cloud*, 2013, pp. 1–2.

[16] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA J. Autom. Sinica*, vol. 4, no. 1, pp. 27–40, Jan. 2017.

[17] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2016.

[18] N. Evancich and J. Li, "Attacks on industrial control systems," in *Cyber-Security of SCADA and Other Industrial Control Systems*. Springer, 2016, ch. 6, pp. 95–110, doi: 10.1007/978-3-319-32125-7_6.

[19] R. Su, "Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations," *Automatica*, vol. 94, pp. 35–44, Aug. 2018.

[20] P. M. Lima, M. V. S. Alves, L. K. Carvalho, and M. V. Moreira, "Security against network attacks in supervisory control systems," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 12333–12338, Jul. 2017.

[21] L. K. Carvalho, Y.-C. Wu, R. Kwong, and S. Lafortune, "Detection and prevention of actuator enablement attacks in supervisory control systems," in *Proc. 13th Int. Workshop Discrete Event Syst. (WODES)*, Xi'an, China, May 2016, pp. 298–305.

[22] D. Thorsley and D. Teneketzis, "Intrusion detection in controlled discrete event systems," in *Proc. 45th IEEE Conf. Decis. Control*, San Diego, CA, USA, Dec. 2006, pp. 6047–6054.

[23] P. M. Lima, L. K. Carvalho, and M. V. Moreira, "Detectable and undetectable network attack security of cyber-physical systems," *IFAC-PapersOnLine*, vol. 51, no. 7, pp. 179–185, 2018.

[24] L. K. Carvalho, Y.-C. Wu, R. Kwong, and S. Lafortune, "Detection and mitigation of classes of attacks in supervisory control systems," *Automatica*, vol. 97, pp. 121–133, Nov. 2018.

[25] P. M. Lima, M. V. S. Alves, L. K. Carvalho, and M. V. Moreira, "Security against communication network attacks of cyber-physical systems," *J. Control, Autom. Electr. Syst.*, vol. 30, no. 1, pp. 125–135, Feb. 2019.

[26] D. E. Comer and R. E. Droms, *Computer Networks and Internets*. Upper Saddle River, NJ, USA: Prentice-Hall, 2003. [Online]. Available: https://dl.acm.org/doi/book/10.5555/861590

[27] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[28] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[29] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-Service (dos) attacks on load frequency control in smart grids," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Feb. 2013, pp. 1–6.

[30] P. Srikantha and D. Kundur, "Denial of service attacks and mitigation for stability in cyber-enabled power grid," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Feb. 2015, pp. 1–5.

[31] J. Zhang, R. S. Blum, L. M. Kaplan, and X. Lu, "Functional forms of optimum spoofing attacks for vector parameter estimation in quantized sensor networks," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 705–720, Feb. 2017.

[32] S. Teng, N. Wu, W. Zhang, and X. Fu, "Cooperative intrusion detection based on object monitoring," *Acta Sci. Nat. Univ. Sunyatseni*, vol. 47, no. 6, pp. 76–81, 2008.

[33] J. P. Anderson, "Computer security threat monitoring and surveillance," James P. Anderson Company, Philadelphia, PA, USA, Tech. Rep. 79F296400, Apr. 1980.

[34] D. E. Denning, "An intrusion-detection model," *IEEE Trans. Softw. Eng.*, vol. SE-13, no. 2, pp. 222–232, Feb. 1987.
[35] T. F. Lunt and R. Jagannathan, "A prototype real-time intrusion-detection expert system," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, Apr. 1988, pp. 59–66.
[36] L. T. Heberlein, G. V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, and D. Wolber, "A network security monitor," Dept. Elect. Eng. Comput. Sci., Lawrence Livermore Nat. Lab., California Univ., Davis, CA, USA, Tech. Rep. UCRL-CR-105095 and DE91007139, 1989.
[37] M. Roesch, "Lightweight intrusion detection for networks," in *Proc. LISA*, 2005, pp. 229–238.
[38] W. Zhu, M. Deng, and Q. Zhou, "An intrusion detection algorithm for wireless networks based on ASDL," *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 1, pp. 92–107, Jan. 2018.
[39] K. Ilgun, R. A. Kemmerer, and P. A. Porras, "State transition analysis: A rule-based intrusion detection approach," *IEEE Trans. Softw. Eng.*, vol. 21, no. 3, pp. 181–199, Mar. 1995.
[40] M. Markou and S. Singh, "Novelty detection: A review-part 1: Statistical approaches," *Signal Process.*, vol. 83, no. 12, pp. 2481–2497, Dec. 2003.
[41] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," Nat. Inst. Standards Technol., Gaithersburg, MA, USA, Tech. Rep. NIST SP 800-94, 2012.
[42] A. Hoehn and P. Zhang, "Detection of covert attacks and zero dynamics attacks in cyber-physical systems," in *Proc. Amer. Control Conf. (ACC)*, Boston, MA, USA, Jul. 2016, pp. 302–307.
[43] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Comput. Surv.*, vol. 42, no. 1, pp. 1–31, Dec. 2009.
[44] A. Lazarevic, V. Kumar, and J. Srivastava, "Intrusion detection: A survey," in *Managing Cyber Threats*. Springer, 2005, ch. 1, sec. 2, pp. 19–78. [Online]. Available: https://link.springer.com/chapter/10.1007/0-387-24230-9_2
[45] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 42–57, Jan. 2013.
[46] C. V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection," *Comput. Secur.*, vol. 29, no. 1, pp. 124–140, Feb. 2010.
[47] S. Teng, N. Wu, H. Zhu, L. Teng, and W. Zhang, "SVM-DT-based adaptive and collaborative intrusion detection," *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 1, pp. 108–118, Jan. 2018.
[48] M. R. C. Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks," *IEEE Access*, vol. 8, pp. 19921–19933, 2020.
[49] H. Zhengbing, S. Jun, and V. P. Shirochin, "An intelligent lightweight intrusion detection system with forensics technique," in *Proc. 4th IEEE Workshop Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl.*, Dortmund, Germany, Sep. 2007, pp. 647–651.
[50] M. Agarwal, S. Purwar, S. Biswas, and S. Nandi, "Intrusion detection system for PS-poll DoS attack in 802.11 networks using real time discrete event system," *IEEE/CAA J. Automat. Sinica*, vol. 4, no. 4, pp. 792–808, Oct. 2017.
[51] X. Guo, S. Wang, D. You, Z. Li, and X. Jiang, "A siphon-based deadlock prevention strategy for S3PR," *IEEE Access*, vol. 7, pp. 86863–86873, 2019.
[52] S. Wang, D. You, and M. Zhou, "A necessary and sufficient condition for a resource subset to generate a strict minimal siphon in s 4PR," *IEEE Trans. Autom. Control*, vol. 62, no. 8, pp. 4173–4179, Aug. 2017.
[53] Y. Teng, Y. Du, L. Qi, and W. Luan, "A logic Petri net-based method for repairing process models with concurrent blocks," *IEEE Access*, vol. 7, pp. 8266–8282, 2019.
[54] W. Duo, X. Jiang, O. Karoui, X. Guo, D. You, S. Wang, and Y. Ruan, "A deadlock prevention policy for a class of multithreaded software," *IEEE Access*, vol. 8, pp. 16676–16688, 2020, doi: 10.1109/ACCESS.2020.2964312.
[55] S. Wang, D. You, and C. Seatzu, "A novel approach for constraint transformation in Petri nets with uncontrollable transitions," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 8, pp. 1403–1410, Aug. 2018.
[56] S. Wang, C. Wang, M. Zhou, and Z. Li, "A method to compute strict minimal siphons in a class of Petri nets based on loop resource subsets," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 42, no. 1, pp. 226–237, Jan. 2012.
[57] G. Liu, "Complexity of the deadlock problem for Petri nets modeling resource allocation systems," *Inf. Sci.*, vol. 363, pp. 190–197, Oct. 2016.
[58] G. Liu, C. Jiang, and M. Zhou, "Two simple deadlock prevention policies for S^3PR based on key-resource/operation-place pairs," *IEEE Trans. Autom. Sci. Eng.*, vol. 7, no. 4, pp. 945–957, Oct. 2010.
[59] G. J. Liu, C. J. Jiang, and M. C. Zhou, "Improved sufficient condition for the controllability of dependent siphons in system of simple sequential processes with resources," *IET Control Theory Appl.*, vol. 5, no. 9, pp. 1059–1068, Jun. 2011.
[60] Y. Wang, H. Liu, W. Zheng, Y. Xia, Y. Li, P. Chen, K. Guo, and H. Xie, "Multi-objective workflow scheduling with deep-Q-network-based multi-agent reinforcement learning," *IEEE Access*, vol. 7, pp. 39974–39982, 2019.
[61] F. G. Cabral, M. V. Moreira, O. Diene, and J. C. Basilio, "A Petri net diagnoser for discrete event systems modeled by finite state automata," *IEEE Trans. Autom. Control*, vol. 60, no. 1, pp. 59–71, Jan. 2015.
[62] X. Yin, "Supervisor synthesis for mealy automata with output functions: A model transformation approach," *IEEE Trans. Autom. Control*, vol. 62, no. 5, pp. 2576–2581, May 2017.
[63] R. M. Goes, E. Kang, R. Kwong, and S. Lafortune, "Stealthy deception attacks for cyber-physical systems," in *Proc. IEEE 56th Annu. Conf. Decis. Control (CDC)*, Melbourne, VIC, Australia, Dec. 2017, pp. 4224–4230.
[64] R. Meira-Goes, R. Kwong, and S. Lafortune, "Synthesis of sensor deception attacks for systems modeled as probabilistic automata," in *Proc. Amer. Control Conf. (ACC)*, Philadelphia, PA, USA, Jul. 2019, pp. 5620–5626.
[65] H. Jeon and Y. Eun, "A stealthy sensor attack for uncertain cyber-physical systems," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6345–6352, Aug. 2019.
[66] M. Wakaiki, P. Tabuada, and J. P. Hespanha, "Supervisory control of discrete-event systems under attacks," *Dyn. Games Appl.*, vol. 9, no. 4, pp. 965–983, Sep. 2018.
[67] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor Noise/Attacks," *IEEE Trans. Autom. Control*, vol. 61, no. 8, pp. 2079–2091, Aug. 2016.
[68] A. Paoli, M. Sartini, and S. Lafortune, "Active fault tolerant control of discrete event systems using online diagnostics," *Automatica*, vol. 47, no. 4, pp. 639–649, Apr. 2011.
[69] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proc. 1st Int. Conf. High Confidence Netw. Syst. (HiCoNS)*, Montreal, QC, Canada, 2012, pp. 55–64.
[70] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Revealing stealthy attacks in control systems," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Monticello, IL, USA, Oct. 2012, pp. 1806–1813.
[71] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.
[72] G. Park, H. Shim, C. Lee, Y. Eun, and K. H. Johansson, "When adversary encounters uncertain cyber-physical systems: Robust zero-dynamics attack with disclosure resources," in *Proc. IEEE 55th Conf. Decis. Control (CDC)*, Las Vegas, NV, USA, Dec. 2016, pp. 5085–5090.
[73] R. Fritz and P. Zhang, "Modeling and detection of cyber attacks on discrete event systems," *IFAC-PapersOnLine*, vol. 51, no. 7, pp. 285–290, May 2018.
[74] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186–192, Jan. 2013.
[75] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under Markov modulated Denial-of-Service (DoS) attack strategies," *IEEE Trans. Autom. Control*, vol. 60, no. 12, pp. 3299–3304, Dec. 2015.
[76] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proc. Int. Workshop Hybrid Syst., Comput. Control*, San Francisco, CA, USA, 2009, pp. 31–45.
[77] H. S. Foroush and S. Martinez, "On event-triggered control of linear systems under periodic denial-of-service jamming attacks," in *Proc. IEEE 51st IEEE Conf. Decis. Control (CDC)*, Dec. 2012, pp. 2551–2556.
[78] C. De Persis and P. Tesi, "Input-to-State stabilizing control under Denial-of-Service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.
[79] S. Feng and P. Tesi, "Resilient control under Denial-of-service: Robust design," *Automatica*, vol. 79, pp. 42–51, May 2017.
[80] V. S. Dolk, P. Tesi, C. De Persis, and W. P. M. H. Heemels, "Event-triggered control systems under Denial-of-Service attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 93–105, Mar. 2017.

[81] J. Liu, X. Lu, and J. Wang, "Resilience analysis of DC microgrids under denial of service threats," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3199–3208, Jul. 2019.
[82] C. Gao, C. Seatzu, Z. Li, and A. Giua, "Multiple attacks detection on discrete event systems," in *Proc. IEEE Int. Conf. Syst., Man Cybern. (SMC)*, Bari, Italy, Oct. 2019, pp. 2352–2357.

LIWEI CAO received the B.S. degree from the School of Information and Electronic Engineering, Zhejiang Gongshang University, China, in 2018, where she is currently pursuing the M.S. degree. Her main interests include supervisory control of discrete event systems and Petri net theory and application.

XIAONING JIANG received the M.E. degree in electronic engineering from Hangzhou Dianzi University, Hangzhou, China, in 1993, and the Ph.D. degree in computer science and technology from Zhejiang University, Hangzhou, in 2000. He is currently an Associate Professor and a Senior Engineer with Zhejiang Gongshang University, where he is also the Vice Dean of the IoT Research Institute. He has published more than 30 research articles and ten invention patents. His research interests include applied information systems, network and information security, the industrial IoT, visual analytic, and Fin-tech.

YUMEI ZHAO received the B.S. degree from the School of Information and Electronic Engineering, Zhejiang Gongshang University, China, in 2019, where she is currently pursuing the M.S. degree. Her main interests include supervisory control of discrete event systems and Petri net theory and application.

SHOUGUANG WANG (Senior Member, IEEE) received the B.S. degree in computer science from the Changsha University of Science and Technology, Changsha, China, in 2000, and the Ph.D. degree in electrical engineering from Zhejiang University, Hangzhou, China, in 2005.

In 2005, he joined Zhejiang Gongshang University, where he is currently a Professor with the School of Information and Electronic Engineering, the Director of the Discrete-Event Systems Group, and the Dean of the System Modeling and Control Research Institute. He was a Visiting Professor with the Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ, USA, from 2011 to 2012, and the Electrical and Electronic Engineering Department, University of Cagliari, Cagliari, Italy, from 2014 to 2015. He was the Dean of the Department of Measuring and Control Technology and Instrument, from 2011 to 2014. He is currently an Associate Editor of IEEE Access and the IEEE/CAA Journal of Automatica Sinica.

DAN YOU (Student Member, IEEE) received the B.S. and M.S. degrees from the School of Information and Electronic Engineering, Zhejiang Gongshang University, China, in 2014 and 2017, respectively. Her research interests include supervisory control of discrete event systems, fault prediction, and deadlock control and siphon computation in Petri nets.

XIANLI XU received the B.S. and master's degrees in automatic control and Computer Engineering from Zhejiang University, China, in 1994 and 2002, respectively. His research directions are automatic control, communication technology, image processing, artificial intelligence, and block chain application. He has presided over 3D drawing of the global lighting graphics accelerated rendering research, the Zhejiang Province Science and Technology Department project, Ei published in the Journal of Electronics and Informatics in Multichannel 3D ink rendering model for contour optimization.