Survey of Cyber Attacks on Cyber Physical Systems Recent Advances and Challenges

Department of Computer Science and Engineering
박희지

2023.03.27

SEOULTECH 서울과학기술대학교
UCSLAB Ubiquitous Computing & Security Laboratory

CONTENTS

1. Introduction

Cyber physical system (CPS)

- CPS is a typical product of Industry 4.0, which plays an important role since a CPS is able to integrate the physical and virtual worlds by providing real-time data processing services.

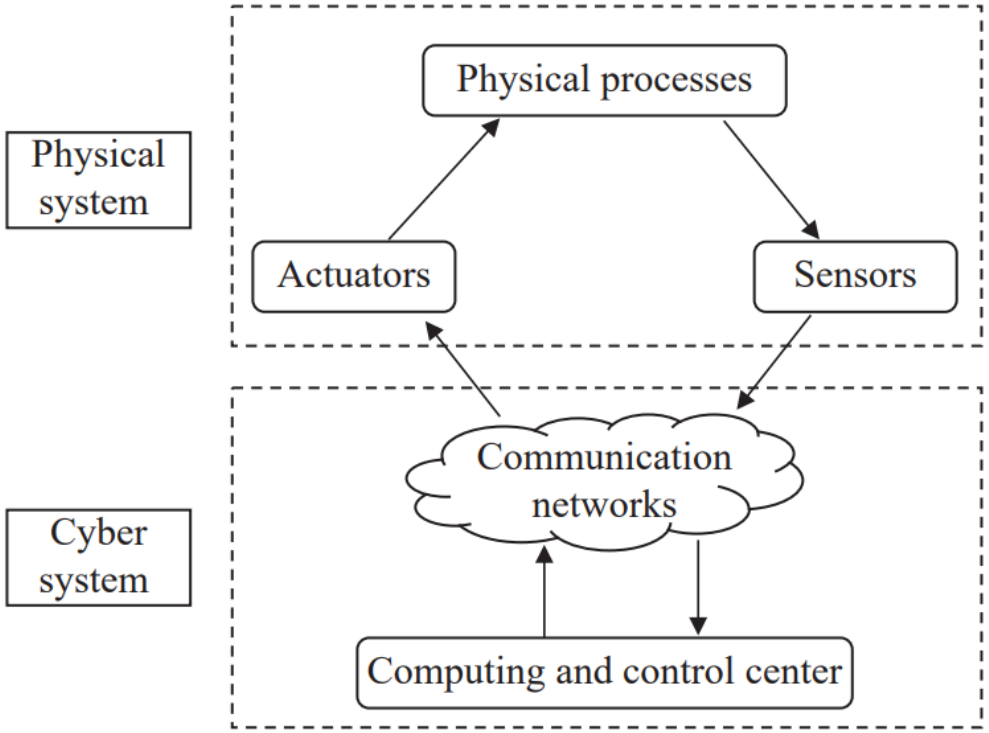
- CPS enables integration, sharing and collaboration of information, as well as real-time monitoring and global optimization of systems.

- There is a wide range of applications in modern industry based on CPSs, such as **smart grids, healthcare, aircraft, digital manufacturing and robotics**. Literature shows that CPS includes, but is not limited to, networked control systems (NCSs), wireless sensor networks, and smart grids.

1. Introduction

A cyber physical system (CPS)

- A CPS consists of a physical system and a cyber system.



1) physical system
- physical processes
- Sensors: They are used for real-time data acquisition.
- Actuator: Control commands are executed by correspon- ding actuators to realize desired physical actions.

2) cyber system
- Computing and control center: It is responsible for receiving data measured by sensors.
- Communication network: It provides a communication platform for the control center and physical system.

1. Introduction

- With the rapid development of modern industry, demands for CPS integration are growing to make up for shortcomings among networks, technologies, tools, and devices.

- The integration of systems and technologies in CPS tends to be complex and diverse, making it a compatible and open system, which unfortunately provides a platform for adversaries to exploit CPS and results in numerous security issues.

- cyber attacks
  - ① The attack on Ukrainian power grids
  - ② Healthcare organizations were threatened by cyber attacks during the coronavirus disease 2019.
  - ③ Etc.

1. Introduction

TABLE I
TYPICAL CYBER ATTACK EVENTS FROM YEARS 2010 TO PRESENT

Year	Country/Institution	Details
2010	Iran	Stuxnet attack destroying core controllers of industries
2015	Ukraine	BlackEnergy attack on power grid, leading to massive power outage
2017	Russia, Ukraine, India, China	WannaCry attack aiming to encrypt data and demand ransom payments
2020	Brno University Hospital, Czech Republic	A cyber attack that shut down IT network of a Czech hospital
2020	US Dept. Health & Human Services	Unspecified attack on servers
2021	Colonial Pipeline, US	A ransomware attack on a US fuel pipeline, leading to shutdown of a critical fuel network

1. Introduction

Cyber attacks on CPS

- The **availability attack** is the most common cyber attack. Its objective is to block the communication network by making data and information unavailable. Typical availability attacks include DoS, distributed DoS and jamming ones.

- an **integrity attack** can occur on sensors, actuators, communication networks, and computing and control centers as data and control commands can be falsified under such an attack. There are many types of integrity attacks, e.g., false data injection attacks, middlemen, sparse and replay attacks.

- **Confidentiality attacks** may occur at any part of a system since any system information may be targeted by an attacker. Attack methods include eavesdropping, and the combination of DoS and integrity attacks.

1. Introduction

TABLE II
RELATED SURVEYS ON CYBER ATTACK

(A: Availability attack; I: Integrity attack; C: Confidentiality attack; TD: Time-driven system; ED: Event-driven system; D: Detection; SC: Secure control; DES: Discrete event system)

Year	Reference	Attack types			Models		Attack strategies	Defense strategies		Main focus
		A	I	C	TD	ED		D	SC	
2018	Ding *et al.*, [10]	√	√	×	√	×	√	√	√	Attack detection and secure control
	Giraldo *et al.*, [11]	×	√	×	√	×	×	√	×	Detection mechanisms for integrity attack
2019	Mahmoud *et al.*, [12]	√	√	×	√	×	×	√	√	Modeling, detection and control of attacks
	Rashidinejad *et al.*, [13]	×	√	√	×	√	√	√	√	Attack defense based on DES
	Dibaji *et al.*, [14]	√	√	√	√	×	√	√	√	Attack defense mechanisms
2020	Singh *et al.*, [15]	√	√	√	√	×	×	√	√	Existing problems and challenges
	Cao *et al.*, [16]	√	√	×	√	√	×	√	√	Attack defense based on DES
	Tan *et al.*, [17]	√	√	×	√	×	×	√	√	Detection mechanisms
2021	Zhang *et al.*, [18]	√	√	×	√	×	×	√	√	Attack defense for industrial CPS
	Ding *et al.*, [19]	√	√	×	√	×	×	√	√	State estimation and secure control
	This study	√	√	√	√	√	√	√	√	All issues in this table

2. System Models for CPS

- A system model plays a fundamentally important role in realizing system control theory on CPS due to its ability to characterize the dynamic behavior of a CPS. Literature shows that a CPS under attack can be usually modeled as two types of systems, i.e., **time-driven** and **event-driven** ones.
- **Time-driven systems** including continuous-time and discrete- time systems have caught much attention in CPS modeling. We note that the linear time-invariant (LTI) system is the most commonly used model for both.
- LTI is modeled as (1), Based on such model, a variety of availability attack models are designed.

$$x_{k+1} = Ax_k + w_k$$
$$y_k = Cx_k + v_k \quad (1)$$

where $k \in \mathbb{N}$, x_k, $w_k \in \mathbb{R}^n$ and y_k, $v_k \in \mathbb{R}^m$, represent the system state, process noise, system measurement and measurement noise at time k, respectively. Moreover, w_k and v_k are uncorrelated zero-mean Gaussian noises with covariance Σ_w and Σ_v, respectively.

$$\eta_k = \begin{cases} 1, & S_a \text{ is injected at time } k, \\ 0, & \text{otherwise.} \end{cases} \quad (2)$$

2. System Models for CPS

- Integrity attacks target sensor measurements or control commands. Let ak be an attack vector, the actual measurement under attacks is $y_k^a = y_k + a_k$, where $y_k^a \in \mathbb{R}^m$. A similar model can be constructed for attacks on control commands, i.e., $u_k^a = u_k + a_k$, where u_k and u_k^a are control inputs when attacks are absent and present, respectively.
- In addition to conventional models, some stochastic models are proposed in the literature. A typical discrete-time stochastic model is constructed as

$$\begin{aligned} x_{k+1} &= Ax_k + g_{(Z_{k+1})}Bu_k + v_{k+1} \\ y_k &= Cx_k + w_{k+1} \end{aligned} \qquad (3)$$

- where $\gamma_{(Zk)} \in \{0, 1\}$ denotes an attack sequence that prevents the control signal from reaching the actuator and Zk corresponds to the internal state of an attacker.
- And Two typical tools to model a CPS as a DES are finite state automata and Petri nets. The former can show system states clearly, while the latter can provide a compact model.

2. System Models for CPS

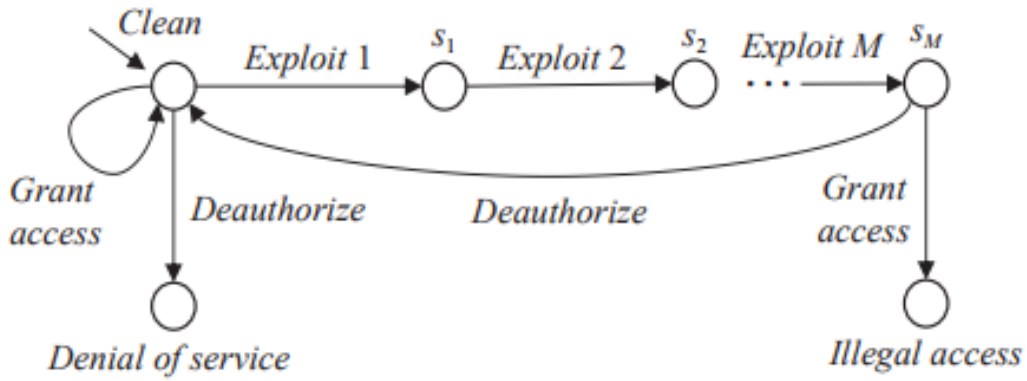


Fig. 2. An automaton G of a cyber attack on a computer system [29].

- An attacker may gain access to the system via a series of exploits to make the system reach undesirable states. The supervisor can allow or forbid the occurrence of certain events according to observed events (sensor readings), so that behaviors of a system can be controlled.
- However, such a supervisor can make wrong decisions since an integrity attacker may falsify event sequences sent to it. In [29], the attacker is assumed to be able to insert or remove event Exploit i in a sequence. Such an attack is characterized as a set A

$$A = \{A_{\emptyset}, A_{Exploit\ 1}, A_{Exploit\ 2}, \ldots, A_{Exploit\ M}\}$$

- A Petri net is another tool to model CPS. It is a 3-tuple N = (P, T, F), where P and T are the set of places and transitions, respectively. $F \subseteq (P \times T) \cup (T \times P)$ is the set of flow relations that is represented by directed arcs. Modeling CPS and attacks as Petri nets is similar to the case with automata. Related models refer to [27].

2. System Models for CPS

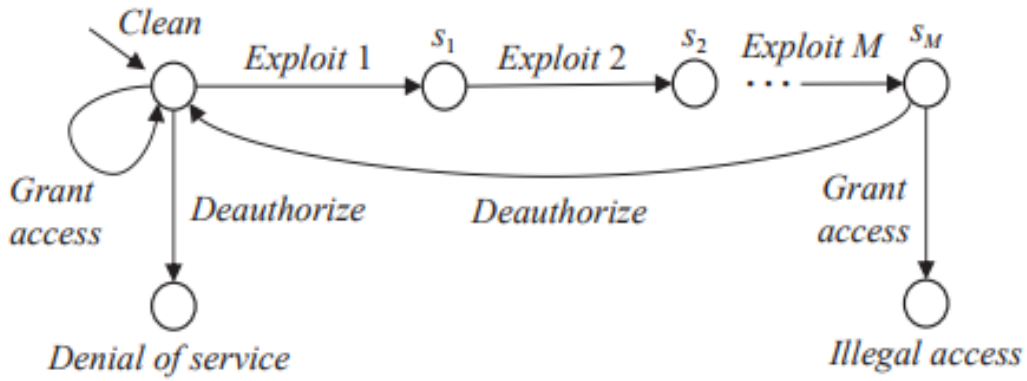


Fig. 2. An automaton G of a cyber attack on a computer system [29].

- An attacker may gain access to the system via a series of exploits to make the system reach undesirable states. The supervisor can allow or forbid the occurrence of certain events according to observed events (sensor readings), so that behaviors of a system can be controlled.
- However, such a supervisor can make wrong decisions since an integrity attacker may falsify event sequences sent to it. In [29], the attacker is assumed to be able to insert or remove event Exploit i in a sequence. Such an attack is characterized as a set A

$$A = \{A_{\emptyset}, A_{Exploit\ 1}, A_{Exploit\ 2}, \ldots, A_{Exploit\ M}\}$$

- A Petri net is another tool to model CPS. It is a 3-tuple N = (P, T, F), where P and T are the set of places and transitions, respectively. $F \subseteq (P \times T) \cup (T \times P)$ is the set of flow relations that is represented by directed arcs. Modeling CPS and attacks as Petri nets is similar to the case with automata. Related models refer to [27].

3. Availability Attack

The purpose of an availability attack is to make data, information and resources in the system unavailable. There are several ways for attackers to implement availability attacks, such as filling buffers in a user or the kernel domain, blocking or jamming the communication among key components, and altering a routing protocol.

The most common availability attack is **DoS** one. In recent years, most studies about CPSs have concentrated on DoS. Researchers have extensively studied it based on time-driven systems, while rarely based on event-driven systems. Thus, we focus on the recent work about it in terms of time-driven systems.

A. DoS Attack Strategies Against CPS

- Need to study cyber attacks on CPS in terms of attack and defense strategies.
- In most cases, only knowing what kind of attack the system is subjected to, can we propose effective countermeasure. It is reasonable for researchers to study DoS attacks from an attacker's point of view.

3. Availability Attack

A. DoS Attack Strategies Against CPS

- Usually, DoS attacks block communication via a wireless network since its nodes' energy budget is limited [32]. Energy constraints become a tricky issue since they can impact the effectiveness of attacks. This problem is considered in recent attack strategies. They focus on allocating power and scheduling energy to gain more benefits for attackers. Consider a system modeled as (1), a DoS attack (2) is launched on the system.

$$\begin{aligned} x_{k+1} &= Ax_k + w_k \\ y_k &= Cx_k + v_k \end{aligned} \tag{1}$$

$$\eta_k = \begin{cases} 1, & S_a \text{ is injected at time } k, \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

3. Availability Attack

A. DoS Attack Strategies Against CPS

Problem 1:

$$\max_{\eta \in \Gamma} tr[J_a(\eta)] \tag{5}$$

$$\text{s.t.} \sum_{k=1}^{T} \eta_k = n \tag{6}$$

- Problem 1 is modified in [34] by replacing $J_a(\eta)$ in (5) with a Linear Quadratic Gaussian control cost function. Solution to the modified problem aims to maximize the attacking effect on a wireless NCS. It should be pointed out that strong assumptions are required in both studies [33], [34].

- It is unlikely for practical systems to work perfectly all the time. [35] focuses on a DoS attack under a scenario where packets may be lost even if no attack occurs.

3. Availability Attack

A. DoS Attack Strategies Against CPS

- By solving Problem 1, an optimal scheduling method is proposed to maximize the expected estimation error. It greatly degrades the performance of a remote estimator, thus maximizing the attack effect on the system. In addition, the proposed method handles a problem of when to launch an attack to maximize damage to the system.

- However, the effect of attack power on system performance is ignored. Such issue is considered in [36], i.e., optimal DoS attack energy management is studied while taking account of packet losses and the effect of attack power.

- As a result, two static attack power allocation policies and a dynamic one are proposed. The former aims to maximize expected terminal error and average error, while the latter considers two indexes based on a Markov decision process. They can work only if the packet transmitted from a sensor to an estimator is not lost at the initial time [35], [36].

3. Availability Attack

B. Defense Strategies Against DoS Attack

- Two strategies for defending against cyber attacks include attack detection and secure control. Advances on the former are mostly derived from computer science instead of system control theory.
- Many detection methods are designed based on artificial intelligence approaches, such as deep learning, reinforcement learning and neural network [37]−[40], which is beyond the scope of this paper. We only discuss secure control methods against DoS attacks in this section.
- Once an availability attack is successfully launched, the closed-loop stability of CPS is destroyed since certain data packets are prevented from being transmitted over communication networks.
- **Event-triggered (ET) control** has the advantage of saving network resources significantly while maintaining good closed-loop system performance. It is widely used to achieve resilient control for CPS, especially systems with limited network resources, such as NCSs and wireless networks.
- Usually, an ET scheme can be divided into ET sampling and ET transmission. The former embeds an event-generator into a sensor to select signals to be sampled, while the latter embeds it behind the sensor to determine whether the sampled signals should be released. A detailed analysis of this ET control framework is referred to [41].

3. Availability Attack

B. Defense Strategies Against DoS Attack

- Asynchronous DoS attacks are considered in [43], i.e., DoS attacks can occur on sensor-to-controller (S-C) channels and controller-to-actuator (C-A) channels. Two different ET mechanisms are designed for them, namely S-C ET and C-A ET. The former is embedded in a smart sensor system and the latter is introduced in a controller system. Under the proposed ET strategies, a closed-loop system is proved to be input-to- state stable.
- Motivated by ET transmission schemes and periodic ET control schemes in [44] and [45], Hu et al. [46] propose an observer-based resilient ET transmission scheme for NCS, where a system suffers from periodic DoS jamming attacks.
- The proposed method is effective to improve the efficiency of resource utilization and guarantee the stability of the system under the periodic DoS attack. Subsequently, Hu et al. [47] study a networked system under non-periodic DoS jamming attacks, where the attack signal is

$$S2_{\mathrm{DoS}}(t) = \begin{cases} 0, & t \in [g_{n-1}, g_{n-1} + b_{n-1}) \\ 1, & t \in [g_{n-1} + b_{n-1}, g_n) \end{cases} \tag{9}$$

- It must be noted that internal and external environments are usually complex and uncertain in practice, leading to failure of the above methods since uncertainty of system parameters is not considered. Thus, some researchers treat CPS as a stochastic system.

3. Availability Attack

B. Defense Strategies Against DoS Attack

- Asynchronous DoS attacks are considered in [43], i.e., DoS attacks can occur on sensor-to-controller (S-C) channels and controller-to-actuator (C-A) channels. Two different ET mechanisms are designed for them, namely S-C ET and C-A ET. The former is embedded in a smart sensor system and the latter is introduced in a controller system. Under the proposed ET strategies, a closed-loop system is proved to be input-to- state stable.
- Motivated by ET transmission schemes and periodic ET control schemes in [44] and [45], Hu et al. [46] propose an observer-based resilient ET transmission scheme for NCS, where a system suffers from periodic DoS jamming attacks.
- The proposed method is effective to improve the efficiency of resource utilization and guarantee the stability of the system under the periodic DoS attack. Subsequently, Hu et al. [47] study a networked system under non-periodic DoS jamming attacks, where the attack signal is

$$S2_{\mathrm{DoS}}(t) = \begin{cases} 0, & t \in [g_{n-1}, g_{n-1} + b_{n-1}) \\ 1, & t \in [g_{n-1} + b_{n-1}, g_n) \end{cases} \tag{9}$$

- It must be noted that internal and external environments are usually complex and uncertain in practice, leading to failure of the above methods since uncertainty of system parameters is not considered. Thus, some researchers treat CPS as a stochastic system.

3. Availability Attack

B. Defense Strategies Against DoS Attack

- An important issue we should take into account is that potential faults may occur in practical systems. They degrade the reliability of systems as well as the performance of aforementioned strategies. Sathishkumar and Liu [54] propose a resilient fault-tolerant control strategy for a nonlinear NCS to deal with periodic DoS jamming attacks, actuator saturation, randomly occurring nonlinearities and actuator faults.
- In addition to an ET control framework, researchers also adopt other methodologies to realize secure control. For example, robust control for a NCS is studied in [55], where a dynamic observer-based control architecture is designed. It shows that the considered dynamic observer equipped with prediction and state resetting capabilities is applicable to a general class of DoS attacks. However, it works only if the process under control is observable.
- Yuan and Xia [57] consider DoS attacks between sensor and remote estimation. They present a multi-transmission strategy to reduce the probability of a system being attacked. Their interaction is modeled as a stochastic game, based on which, a resilient control strategy is developed.
- Zhang et al. [58] consider DoS attacks that can be random or periodic but their duration time is limited. They propose some criteria to check whether a non-periodic sampled-data control system can preserve stability under such attacks.

3. Availability Attack

B. Defense Strategies Against DoS Attack

- Apart from resilient control, stochastic control can be used to deal with DoS attacks. It often adopts a Markov process to model systems and DoS attacks to realize risk sensitive control [26], [59], [60]. After constructing a stochastic model (3), an exponential running cost is considered in [26].

$$J(u) = \left(\frac{1}{\theta}\right) E\left[\exp\left\{\left(\frac{\theta}{2}\right)\left\{\sum_{k=0}^{N-1}\left(x_k^T X x_k + \gamma_{(Z_{k+1})} u_k^T Y u_k\right) + x_N^T X_N x_N\right\}\right\}\right] \qquad (10)$$

- Using a stochastic model, Befekadu et al. [26] design an optimal control policy for a discrete-time partially observed system. Their policy is based on a chain of measure transformation techniques and dynamic programming, such that a recursive optimal control policy and the considered information-state can be transformed into a fully observable stochastic control problem.

3. Availability Attack

B. Defense Strategies Against DoS Attack

- A real CPS usually consists of multiple subsystems, which are deployed in a distributed manner. It increases attack surfaces, making it more frangible in security [61]. For example, communication channels among subsystems can suffer from different DoS attacks. The whole system can be severely affected even if only one channel is attacked. Such a security problem cannot be handled well by a centralized method since attack modes are different on each channel.
- Hence, an urgent study is demanded in order to develop distributed defense approaches for cyber attacks. Determining how to achieve a consensus for a distributed CPS under DoS attacks is handled in many studies, e.g., [62]−[64]. By introducing a k -connected graph, [62] designs a distributed event-triggered controller for a CPS under mode-switching DoS attacks.
- Yet, some negative effects may be generated on the system since the method adopts a continuous Lyapunov function, which can generate mismatched terms.
- To mitigate this problem, the controller is further combined with an extended Laplacian matrix to ensure the system consensus. A practical case is investigated in [65] that answers how to address a distributed secure platoon control issue for connected vehicles under DoS attacks.

3. Availability Attack

TABLE III
SUMMARY OF RECENT DEFENSE WORK ON DOS ATTACK

(DT: Discrete-time system; CS: Continuous-time system)

Reference	Target	Model type	Attack type	Methodologies	Advantages	Disadvantages
[42]	Multi-area power system	CS	DoS	ET transmission,load frequency control	Improving the transaction efficiency	Limited attack duration time
[43]	CPS	CS	Asynchronous DoS	ET sampling and transmission	Handling system disturbance and measurement noise	Constraints on DoS frequency and duration
[46]	NCS	CS	Periodic DoS	Observer-based ET transmission	Preserving good control performance	A uniform lower bound for the attack sleeping period
[47]	Networked system	CS	Non-periodic DoS	ET transmission,H_∞ filtering	Achieving good filter performance and reducing unnecessary resource consumption	Known sleeping and active intervals of DoS attacks
[48]	Uncertain NCS	CS	PWM DoS	ET transmission	Handling system parameter uncertainties	Full state information
[52]	Stochastic NCS	CS	Non-periodic DoS	Observer-based ET framework	Preserving stability with a L_2-gain performance level	Constraints on DoS frequency and duration
[53]	Stochastic NCS	DT	Bernoulli distributed DoS	ET sampling	Handling active, consecutive packets dropout	Specified attack location
[54]	Nonlinear NCS	CS	Periodic DoS	ET transmission	Handling fault-prone systems	A uniform lower bound for the attack sleeping period

3. Availability Attack

TABLE III
SUMMARY OF RECENT DEFENSE WORK ON DOS ATTACK

(DT: Discrete-time system; CS: Continuous-time system)

Reference	Target	Model type	Attack type	Methodologies	Advantages	Disadvantages
[55]	NCS	CS	DoS	Dynamic observer-based control	Handling general DoS attacks	Constraints on DoS frequency and duration
[56]	NCS	CS	Stochastic DoS	Markov process	Constructing stability and stabilization criterion	Sufficient knowledge on DoS attack
[57]	CPS	CS	DoS	Multi-transmission	Reducing the probability of being attacked	Full state information
[58]	NCS	CS	DoS	Sampled-data model	Handling random and periodic DoS attacks	Limited attack duration time
[26]	DT partially observed system	DT	Markov modulated DoS	Markov process	Optimal risk-sensitive control	Many assumptions
[62]	CPS	CS	Mode-switching DoS	k-connected graph, extended Laplacian matrix	A more general attack model	Negative effects on the system
[65]	Connected vehicles	CS	DoS	Graph theory, switched time-delay system	Establishing quantitative relations between platooning performance and attack parameters	A simple system structure
[66]	CPS	DT	DoS	Sliding mode control,zero-sum game	Preserving stability and reducing external disturbance	Constraints on DoS frequency and duration

4. Integrity Attack

Integrity attacks aim to destroy the data integrity of a CPS. They can be launched by altering or deleting sensor measurements and control decisions, or inserting incorrect data into them.

In general, they are more subtle and difficult to be detected than availability attacks. The reason is that falsified data spreads through a sensor network in an epidemic way, leading to negative effects on systems.

A. Integrity Attack Strategies Against CPS

1) Time-Driven System-Based Attack Strategies

- Section II shows that a CPS is often modeled as an LTI system. For instance, Wu et al. [68] model a CPS as a continuous-time LTI system and design two optimal location switching strategies to implement false data injection attacks.
- However, their methods are limited by strong assumptions. For example, an attacker should have perfect knowledge about system parameters and state information, and the communication channel is perfect without any noise.

4. Integrity Attack

A. Integrity Attack Strategies Against CPS

1) Time-Driven System-Based Attack Strategies

- Both types of attacks in [73] are stealthy, but random attacks are subject to a strong assumption, namely, measurements are protected in the system.
- Guo et al. [74] study a linear integrity attack on remote state estimation. They propose a new attack strategy as

$$c_k^a = T_k c_k + b_k \qquad (15)$$

- such a strategy is restricted by the linear form and faces two problems. One is that a linear attack framework cannot cover the general form of possible attacks. Another is that a more general attack model exists and is able to cause a worse damage to the system. To solve them, Wu et al. [75] find a worst-case integrity attack. They extend the linear attack in [74] to a general form based on an innovation.

$$c_k^a = f_k(c_k) \qquad (16)$$

4. Integrity Attack

A. Integrity Attack Strategies Against CPS

2) Event-Driven System-Based Attack Strategies

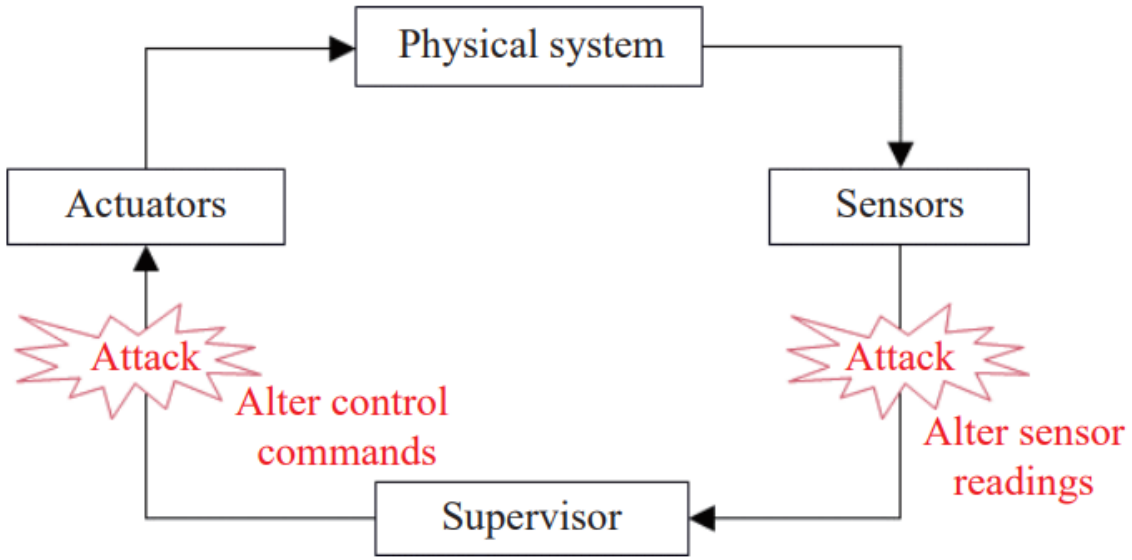


Fig. 3. A closed-loop supervisory control system under attacks.

- A CPS can be characterized as a closed-loop supervisory control system as shown in Fig. 3 . Integrity attacks against a DES are divided into three classes, i.e., sensor, actuator, and general attacks. Sensor and actuator attacks are injected via sensor and actuator channels, respectively, while general ones are injected via both channels.
- Now, we consider an automaton G in Fig. 2 .
- An event sequence is captured by sensors and sent to the supervisor. During this period, A intercepts it and removes event Exploit 3

4. Integrity Attack

A. Integrity Attack Strategies Against CPS

2) Event-Driven System-Based Attack Strategies

- In [82], a structure called insertion-deletion attack (IDA) is established by modeling game-like interactions between a supervisor and the environment. IDA embeds all possible cases that some sensor events are modified by attackers without being noticed by a supervisor, thus realizing a stealthy attack. It is worth noting that system models used in [82] and [81] are automata.

- Based on DES, another tool is also commonly used to study attacks, i.e., Petri nets. Li et al. [83] model a smart grid as a stochastic Petri net, where a smart grid is threatened by topology attacks and equipped with defense strategies. Topology attacks are coordinated attacks evolved from false data injection attacks. Li et al. [83] define two successful topology attacks and utilize Petri nets to capture behaviors of systems and such attacks.

4. Integrity Attack

B. Time-Driven System-Based Defense Strategies

1) Attack Detection

- Attack detection is an efficient way to protect CPS from serious damage. A detection method can identify occurrences of attacks such that warnings can be sent to an operator to take appropriate measures. Many methodologies are adopted to develop detection methods, such as state estimation, $\chi 2$ -detector, fault detection, and watermarking-based methods.
- State estimation is crucial to control systems and to defend from integrity attacks. Although many studies address integrity issues based on state estimation, most of them require such strong assumptions that their proposed methods cannot be put into practical use.
- They propose a least-budget defense strategy based on a measurement residual-based estimator to address false data injection attacks on a power system. However, their method is applicable to a specific known attack only. It becomes ineffective if an attack is unknown. Thus, Ge et al. [25] design distributed estimators based on Krein space to provide suitable residuals for attack detection. Then, a two-stage attack detection framework is developed to ensure that unknown attacks can be detected and identified by each estimator.

4. Integrity Attack

B. Time-Driven System-Based Defense Strategies

1) Attack Detection

- Attack detection is an efficient way to protect CPS from serious damage. A detection method can identify occurrences of attacks such that warnings can be sent to an operator to take appropriate measures. Many methodologies are adopted to develop detection methods, such as state estimation, $\chi 2$ -detector, fault detection, and watermarking-based methods.
- State estimation is crucial to control systems and to defend from integrity attacks. Although many studies address integrity issues based on state estimation, most of them require such strong assumptions that their proposed methods cannot be put into practical use.
- They propose a least-budget defense strategy based on a measurement residual-based estimator to address false data injection attacks on a power system. However, their method is applicable to a specific known attack only. It becomes ineffective if an attack is unknown. Thus, Ge et al. [25] design distributed estimators based on Krein space to provide suitable residuals for attack detection. Then, a two-stage attack detection framework is developed to ensure that unknown attacks can be detected and identified by each estimator.

4. Integrity Attack

B. Time-Driven System-Based Defense Strategies

1) Attack Detection

- Fault detection and isolation (FDI) focuses on determining whether the behavior of an underlying process is correct or not. Since attacks often incur erroneous system behaviors, an FDI technique is widely used and extended to confirm the occurrence of an integrity attack. In general, the design of an FDI-based method involves two steps, state estimation and threshold design. The first issue is often addressed by introducing observers, such as unknown input observers (UIOs) [100], [101]. Based on state estimation, a residual is generated to compare a measurement with its estimate.
- It is used to design detection thresholds. In [100] and [101], a false data injection attack can be identified if a component of a set of residuals exceeds a predefined threshold. It should be pointed out that [101] adopts an adaptive threshold to improve the detection performance.
- However, this method may miss attacks since it is too difficult to compute such a threshold in practice. Thus, Wang et al. [102] design a novel approach based on a nonlinear interval observer. Their approach mitigates the computation of this threshold. To be precise, interval residuals are adopted as a detection criterion rather than the traditional residual evaluation function and threshold.

4. Integrity Attack

B. Time-Driven System-Based Defense Strategies

1) Attack Detection

- Combining watermarking techniques with existing detectors emerges to be a novel idea to identify integrity attacks. A watermarking is useful to protect data transmitted through a communication network by encrypting and decrypting it. Each innovation sequence ck is first processed at the sending side

$$g_k = ac_k + m_k \qquad (19)$$

- In addition to watermarking-based methods, new detection methods have been proposed. For instance, in [107], a finite- time memory fault detection filter is presented for randomly occurring integrity attacks in a nonlinear discrete system.
- Attack detection for a distributed CPS is considered in [108], where a new detector is proposed based on the latest updated data. The computational burden of this detector does not depend on the size of CPS. Thus, it has high scalability.

4. Integrity Attack

B. Time-Driven System-Based Defense Strategies

2) Secure Control

- Usually, a detector just sends a warning to an operator once an attack is identified. The attack can still damage a system if the operator has no countermeasures or does not handle it in time. Secure control is required to guarantee the stability and safety of a system under attack.
- The secure estimation and control problems for a discrete- time linear system are studied in [109]. Xie and Yang [110] focus on false data injection attacks on communication channels from a controller to an actuator.
- They first design a switched attack- resilient observer and then present a supervisory switching strategy to guarantee attack-resilient performance. Such a method is effective to control a CPS under false data injection attacks.
- However, it may suffer from high computational complexity since it requires accurate state estimation.

4. Integrity Attack

B. Time-Driven System-Based Defense Strategies

2) Secure Control

- In addition to false data injection attacks, a class of sparse attacks is studied in the work [111], [112]. Sparse sensor attack is able to tamper measurements of a subset of sensors in a feedback control loop.
- In [113], an event-triggered secure observer-based control scheme is proposed for a continuous- time CPS under actuator and sparse sensor attacks. It requires that the set of attacked channels remains unchanged.
- It is nontrivial to consider distributed secure control for a real industrial CPS, such as unmanned vehicle systems and power systems [114], [115].
- For example, an attack-resilient cooperative control policy is developed in [116] for a power system to regulate the active power at a specific command.
- To enhance the resilience of an islanded microgrid to false data injection attacks, Bidram et al. [117] propose a control scheme based on a weighted mean subsequence reduced algorithm, which allows each distributed energy resource to neglect information altered by attackers. Such a mechanism is also employed in [118].

4. Integrity Attack

B. Time-Driven System-Based Defense Strategies

2) Secure Control

- Different from [117], [118] considers a multi-microgrid system as a multi-agent one, which is modeled as a weighted directed graph.
- A distributed resilient control approach is presented in [119] for multiple energy storage systems in an islanded microgrid, which is inspired by the adaptive resilient control of multiagent systems in [120], [121].
- By introducing the adaptive technique, negative effects caused by attacks and faults can be compensated. Additionally, distributed state estimation and control problems are discussed in [122] for an interconnected CPS with sensor attacks.
- The first issue is addressed by designing a distributed preselectors and an observer, while the second one is resolved based on secure state estimation and a virtual fractional dynamic surface.

4. Integrity Attack

C. Event-Driven System-Based Defense Strategies

- Similar to time-driven system-based methods, defense strategies based on DES can be classified into two categories: attack detection and secure control.

1) Attack Detection

- Attack detection in DES is an intrusion detection module. A detection module is connected with the supervisor. It can observe same events as the supervisor does. Once an attack is detected, the module sends information to the supervisor, such that the system can be prevented from entering an unsafe state before the attack causes damage.
- The problem of intrusion detection and prevention is studied in [123] for supervisory control systems. This work is further extended in [124], where both attacks on sensors and actuators are considered, including actuator enablement attacks, disablement ones, sensor erasure attacks and insertion ones.
- However, the methods in [123] and [124] disable all controllable events once an attack is detected, which may lead to unnecessary loss of resources.

4. Integrity Attack

C. Event-Driven System-Based Defense Strategies

2) Secure Control

- As attackers induce the system into an undesirable state, a general idea to implement secure control is to model a CPS as a DES first. Then, we design a control specification to disable all the undesirable states. Finally, a corresponding supervisor is obtained to prevent them from being reachable under attacks.
- As mentioned before, On the basis of the knowledge for ABSRA model, Su [81] proposes an integrity attack model, called ABSRA. Note that the work [81] is motivated by that in [124].
- The difference between them is that the former aims to detect attacks online, thereby requiring real-time fault diagnosis, while the latter does not require real-time detection but a prior knowledge of attack models.
- Meira-Góes et al. [128] model an underlying uncontrollable system as a discrete transition system. control specification in [128] focuses on preventing certain bad states from being reachable. Thus, the problem of defending integrity attacks can be converted into a DES supervisory control problem.

4. Integrity Attack

C. Event-Driven System-Based Defense Strategies

2) Secure Control

- A common limitation of above methods [29], [81], [128] is that only one robust supervisor can be provided each time for a specific attack. It affects their efficiency in handling real-life applications where multiple attacks appear. Hence, a framework is proposed in [129] to improve their efficiency, where robust supervisors are synthesized for general sensor attacks based on automaton and game theory.
- Note that the modeling tool utilized in the aforementioned methods [29], [81], [128], [129] is automata. Apart from automata, some approaches are developed based on Petri nets. For instance, You et al. [130] study sensor attacks based on Petri nets by considering a special property, i.e., liveness.
- The four types of attacks in [124], i.e., actuator enablement attacks, disablement ones, sensor erasure attacks and insertion ones, are studied in [27] based on labeled Petri nets. They design different supervisors for sensor and actuator attacks under different premises.

4. Integrity Attack

C. Event-Driven System-Based Defense Strategies

2) Secure Control

- A common limitation of above methods [29], [81], [128] is that only one robust supervisor can be provided each time for a specific attack. It affects their efficiency in handling real-life applications where multiple attacks appear. Hence, a framework is proposed in [129] to improve their efficiency, where robust supervisors are synthesized for general sensor attacks based on automaton and game theory.
- Note that the modeling tool utilized in the aforementioned methods [29], [81], [128], [129] is automata. Apart from automata, some approaches are developed based on Petri nets. For instance, You et al. [130] study sensor attacks based on Petri nets by considering a special property, i.e., liveness.
- The four types of attacks in [124], i.e., actuator enablement attacks, disablement ones, sensor erasure attacks and insertion ones, are studied in [27] based on labeled Petri nets. They design different supervisors for sensor and actuator attacks under different premises.

4. Integrity Attack

C. Event-Driven System-Based Defense Strategies

2) Secure Control

- DES-based methods have the advantage of intuitiveness, stability and robustness. However, most of them assume that an attack model is given or we have prior knowledge about it. In addition, most methods suffer from high computational complexity. For example, supervisor synthesis [81] is NP-hard and algorithms in [27], [29], [128] and [130] are of exponential complexity.
- Table IV is provided to summarize recent advances on defense strategies in terms of references, target systems, model types, attack types, strategies, methodologies, pros and cons. It is worth noting that pros and cons of each method in Tables III and IV are derived from its unique feature or application scope rather than experimental results. In fact, it remains difficult and challenging to evaluate existing methods in a uniform framework due to different assumptions and configurations needed by them.

4. Integrity Attack

TABLE IV
SUMMARY OF RECENT DEFENSE WORK ON INTEGRITY ATTACK

(DT: Discrete-time system; CS: Continuous-time system; PF: Power flow model; DES: Discrete event system; CG: Communication graph)

Refe-rence	Target	Model type	Attack types	Strategy	Methodologies	Advantages	Disadvantages
[25]	Wireless sensor network	DT	False data injection	Detection	State estimation, Krein space	Handling unknown attacks	Unstable detection efficiency
[87]	Smart grid	PF	False data injection	Detection	State estimation, mixed integer nonlinear programming	Least budget	Many assumptions on attack model
[93]	Noisy linear dynamic system	CS	Sensor	Detection	State estimation	Optimal state estimation	Many assumptions
[98]	Smart grid	PF	False data injection, replay	Detection	χ^2 detector, cosine similarity matching	Good detection performance	Specific attack models
[99]	Stochastic linear dynamic system	DT	Bias injection	Detection	State estimation, χ^2 detector	Mitigating attack impacts	High computational expense for large-scale system
[100]	DC microgrid	CS	False data injection	Detection	Unknown Input Observer	Requiring limited system information	Specified attack models
[101]	Smart grid	CS	False data injection	Detection	Unknown Input Observer	Good detection performance	Difficulty to compute adaptive threshold
[102]	Smart grid	CS	False data injection	Detection	Nonlinear interval observer	Good detection performance	State estimation accuracy to be improved
[104]	CPS	DT	Middleman	Detection	Watermarking, state estimation	Improving χ^2 detector performance	Possibility to compromise data confidentiality
[105]	CPS	DT	Linear	Detection	Watermarking, K-L divergence	Mitigating attack impacts	Restricted to linear attacks
[107]	Nonlinear discrete system	DT	Integrity	Detection	Memory fault detection filter	Good detection performance	High computational complexity

4. Integrity Attack

TABLE IV
SUMMARY OF RECENT DEFENSE WORK ON INTEGRITY ATTACK

(DT: Discrete-time system; CS: Continuous-time system; PF: Power flow model; DES: Discrete event system; CG: Communication graph)

Refe-rence	Target	Model type	Attack types	Strategy	Methodologies	Advantages	Disadvantages
[108]	Distributed CPS	DT	Integrity	Detection	State estimation, distributed filtering	Good scalability	Inapplicable to stealthy attacks
[110]	CPS	CS	False data injection	Secure control	Observer-based control	Good system resilience	High computational complexity
[113]	CPS	CS	Sparse sensor, actuator attack	Secure control	ET control, observer-based control	Good state estimation	Unchanged attack channels
[117]	Microgrids	CG	False data injection	Secure control	Weighted mean subsequence reduced technique	Allowing to discard attacked information	Possibility to affect system performance
[118]	Microgrids	CG	False data injection	Secure control	Weighted mean subsequence reduced technique	Recovering system while isolating attacks	Performance on asynchronous system to be improved
[122]	CPS	CS	Sensor	Secure control	Distributed observer, virtual fractional dynamic surface	Obtaining exact system state	Complicated parameter design
[125], [127]	Close-loop control system	DES	Middleman	Detection	Automaton, supervisory control theory	Taking proper actions under attacks	Unnecessary loss of resources
[124]	Close-loop control system	DES	Actuator, sensor	Detection	Automaton, supervisory control theory	Handling multiple integrity attacks	Unnecessary loss of resources
[81], [128]	Close-loop control system	DES	Sensor	Secure control	Automaton, supervisory control theory	Being robust to many attacks	Exponential computational complexity
[29]	Close-loop control system	DES	Sensor	Secure control	Supervisory control theory, game theory	Handling unknown attacks	Exponential computational complexity
[130]	Close-loop control system	DES	Sensor	Secure control	Petri nets, supervisory control theory	Compact model	Exponential computational complexity
[27]	Closed-loop control system	DES	Sensor, actuator	Secure control	Petri nets, supervisory control theory	Compact model	Known attack structures

5. Confidentiality Attack

- In this section, we introduce relevant work about confidentiality attacks on CPS, which relates to falsification and theft of secret information.
- However, little research has been performed to address this issue. A main reason is that confidentiality attacks are rather complicated and often involve availability and integrity attacks. For example, a secret key of confidential information can be inferred by a fault injection attack. Jiang et al. [30] focus on a distributed CPS under fault injection attacks and study fault detection design problem to meet the confidentiality-critical and real-time requirements.
- A secondary reason is that availability and integrity attacks belong to active attacks while confidentiality ones are more like passive attacks [13]. To be precise, availability and integrity attacks aim at damaging a system directly while confidentiality ones aim at stealing system information. The latter are more benign than the former.
- A typical confidentiality attack is eavesdropping. Confidential information can be stolen by eavesdropping on communications between sensors and controllers. Many methodologies have been adopted to protect CPS under eavesdropping attacks, such as data encryption [133]−[135], transmission strategy [136], and observer-based method [137]−[139].

5. Confidentiality Attack

- A concept, named opacity, has attracted researcher's attention recently [140]−[142]. Opacity is a cyber-security property related to the confidentiality and privacy of a CPS. A system is said to be opaque if attackers cannot infer the secret of a system based on their observations, where attackers are often assumed to have full information about the system structure but just partial observability. Opacity can be used to verify the security of a CPS.
- For example, Yin and Li [143] consider confidentiality of a networked supervisory control system with insecure control channels, i.e., control decisions sent by supervisors can be eavesdropped by an attacker.
- They consider two transmission mechanisms, event-based trans- mission and decision-based transmission. The former means that a supervisor always sends the latest control decision once a new event is observed, while the latter sends a new decision when it is different from the previous one. Two types of opacities are developed in [143] for the two transmission mechanisms. They both require that for two strings that one reaches a secret state and another reaches a non-secret one, the supervisor can generate a same decision history for them.
- Therefore, secret states cannot be inferred by an attacker.

6. Conclusion and Future Research

We provide some open issues and challenges as follows.

1) Determining How to Defend Against Advanced Attacks

- Cyber attacks are evolving rapidly with updating technologies. Attackers tend to launch advanced attacks to increase their success rate. For example, both DoS and integrity attacks can be launched on a CPS in a random way to enable stealthiness and avoid detection. Although some researchers have noticed this issue [146]−[148], the research results are relatively few.
- In addition, Table I shows some attack events in recent years, one of which we should pay attention to is ransomware attack. It is an attack that prevents or limits users from accessing their files and systems [149], [150]. Such attacks not only damage availability and confidentiality of a system, but also cause significant economic losses.
- Especially during COVID-19, many medical CPS and factories are attacked by ransomware, resulting in serious consequences.
- Therefore, effectively defending advanced attacks on CPS is a challenging but practical issue that deserves more attention.

6. Conclusion and Future Research

We provide some open issues and challenges as follows.

1) Determining How to Defend Against Advanced Attacks

- Cyber attacks are evolving rapidly with updating technologies. Attackers tend to launch advanced attacks to increase their success rate. For example, both DoS and integrity attacks can be launched on a CPS in a random way to enable stealthiness and avoid detection. Although some researchers have noticed this issue [146]−[148], the research results are relatively few.
- In addition, Table I shows some attack events in recent years, one of which we should pay attention to is ransomware attack. It is an attack that prevents or limits users from accessing their files and systems [149], [150]. Such attacks not only damage availability and confidentiality of a system, but also cause significant economic losses.
- Especially during COVID-19, many medical CPS and factories are attacked by ransomware, resulting in serious consequences.
- Therefore, effectively defending advanced attacks on CPS is a challenging but practical issue that deserves more attention.

6. Conclusion and Future Research

This paper provide some open issues and challenges as follows.

2) Determining How to Defend Against Stealthy Attacks

- In Section IV, we introduce the work on stealthy attacks since it is a current trend to study cyber attack. It is easy to find that these efforts focus on designing stealthy attacks rather than preventing them. They provide us with insight into possible attacks while also facilitate attackers. If a stealthy attack strategy is implemented on a system while we have no countermeasures, it can cause a worse consequence since it cannot be detected.

3) Determining How to Defend Against Confidentiality Attacks

- Compared with availability and integrity attacks, fewer studies have been presented for confidentiality attacks on CPS. There remains much room to study this topic since privacy safety and protection have attracted much attention in recent years.

6. Conclusion and Future Research

This paper provide some open issues and challenges as follows.

4) Determining How to Resolve a Partial Issue

- "Partial issue", namely, partial information, knowledge or observa- bility, has always been a challenging problem in this field. In most literature, attack strategies are developed on a premise that an attacker has full knowledge or observability about a system. The same is true for defense strategies, i.e., full information about system states or attack models is required.

5) Determining How to Conduct Appropriate Parameter Design and Performance Evaluation

- Performance of most methods is dependent on key parameters, such as detection thresholds and control parameters. However, a perfect parameter value does not exist in most cases. For a parameter, a value that maximizes one performance may degrade another.
- We lack a tool to indicate their strengths and weaknesses. Hence, providing an appropriate performance analysis for existing methods is a considerable issue.

6. Conclusion and Future Research

This paper provide some open issues and challenges as follows.

6) Determining How to Realize Practical Applications

- The applications of existing theory and model-based methods remain a challenging issue. To mitigate this, technical factors and barriers are discussed in several studies [117], while concrete engineering implementations are still missing.
- Moreover, studies on industrial CPSs are not sufficient. Although many methods are proposed for power systems and microgrids, most of them require too-strong assumptions,
- e.g., system dynamics should be simple and systems should work perfectly, which are unlikely for most real-world industrial CPSs. Only little work has been done for complex or fault- prone systems. It should be pointed out that there remains a deep gap between theoretical results and practical applications.
- To fill it, many researchers try to combine model-based methods with computer science, such as the work in [151]. It indicates a promising trend to realize highly desired practical applications.

7. Opinion on this paper

Existing studies show that security studies on cps continue, but there are still many issues to be solved.
It seems that this paper was able to think about supplementation and countermeasures for the Chen problem in this paper and consider whether it can be applied to future research.

THANK YOU