This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Digital Object Identifier

Data-Driven-Based Event-Triggered Resilient Control for Cigarette Weight Control System Under Denial of Service Attacks and False Data Injection Attacks

GUOQIAN YE, LIXIANG SHEN, Yi Feng, Lifeng Fan, Chi Zhang, and Yuliang Li*
Zhejiang Hangzhou Cigarette Factory, ZJTI, Kehai Road 118, Hangzhou, China

Corresponding author: Yuliang Li (e-mail: liyuliang@zjtobacco.com).

"This work was supported in part by the Key Research and Development Project Plan of China Tobacco Corporation (Project ID: 110202102043), in part by the 2021 Technology Plan of China Tobacco Zhejiang Industrial Co., Ltd. (Project ID: ZJZY2021D014)"

ABSTRACT This article proposes an event-triggered resilient control algorithm for cigarette weight control systems to defend against denial of service attacks (DoS) attacks and false data injection (FDI) attacks. First, the mathematical model of the system is derived by considering its physical and electromagnetic characteristics. Then, an attack detection mechanism is designed to identify potential FDI attacks. A predictive compensation algorithm is also developed to mitigate the influence of these attacks, incorporating an observer to estimate unknown compensation signals. Due to limited network resources, we employ an event-based model-free adaptive control (MFAC) framework, where data is transmitted only when specific conditions are violated. Throughout the entire control process, only the input and output data of the system are used. Finally, simulation comparisons are provided to demonstrate the effectiveness and superiority of our method.

INDEX TERMS Weight control systems, DoS attacks, FDI attacks, model free adaptive control (MFAC), predictive algorithm

I. INTRODUCTION

Cyber-physical system (CPSs), integrating the physical world with information processing technology, have played a crucial role in advancing industrial automation, intelligent transportation, medical diagnosis, and other fields [1]–[3]. As a fundamental cyber-physical system, the cigarette weight control system consists of control units, actuators, various physical devices, and communication networks. Its primary function is to ensure that the weight of each cigarette remains within an acceptable range. At present, there are some studies on cigarette weight control. The authors in [4] proposed a model predictive algorithm to address the weight errors related to random tobacco density, detection lag, and uneven distribution. In [5], a double closed loop control structure is proposed to improve the control accuracy of the cigarette weight control system.

Although the incorporation of the network enhances interaction among different modules and minimizes local data storage, the system is vulnerable to network attacks due to the openness of the network. These attacks include, but are not limited to, denial of service (DoS) attacks and false data injection (FDI) attacks [6]. DoS attackers aim to prevent information transmission by locking the communication channels, causing the system to fail to operate [7]. The attacks will make the controller unable to receive the density information of tobacco, and the height of the level disc cannot be adjusted in time, affecting the normal operation of the cigarette weight control system. FDI attacks manipulate data within the system to generate misleading results or incorrect decisions, leading to unpredictable outcomes [8]. For the cigarette weight system, the injection of false data will cause the cigarette weight to deviate from the actual value, resulting in unqualified cigarettes. In [9], the authors investigate the optimal scheduling problem for wireless networked control systems under DoS attacks to maximize the impact of attacks. A resilient control method for networked cyber-physical systems is investigated in [10] to protect the system from attacks and maintain stability and robustness. [11] proposes an observer-based control method to withstand FDI attacks in the communication channels from the controller to the actuator. The authors in [12] design a robust controller against the FDI attack in the load frequency control system, so that

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

the system can maintain good performance under attacks.

On the other hand, the traditional periodic data sampling method may lead to data redundancy and increase the communication burden, especially in CPSs with limited network resources [13]. The event-based control approaches have demonstrated effectiveness in addressing these issues in networked control systems [14]–[17], where a new event-based pulse-modulated control method is investigated in [14] for stochastic systems, focusing on achieving average quadratic performance. This method allows accurate data capture and transmission at critical moments, effectively reducing the communication burden. For discrete systems, a disturbance rejection control method based on an event trigger mechanism (ETC) is designed in [18], [19], so that the controller is updated only when necessary, thus reducing computing and communication overhead. Based on singular perturbation theory and event-triggering techniques, [20] presents an event-triggered observer-based fuzzy control method for coal-fired power generation systems, achieving optimization design for both control and observer to enhance system performance.

Note that the methods mentioned above require the mathematical model of the systems in advance [21]. However, in practical application, it is difficult to obtain an accurate mathematical model and parameters because of the complexity and uncertainty of the environment. To deal with such a problem, some effective data-driven methods, including neural networks and fuzzy logic algorithms [22]–[24], have been developed, in which the parameters are updated in real-time based on actual data and feedback information without using any model information. Although the methods have received the satisfied control performance, another constrained assumption on system structure is needed. The model-free adaptive control (MFAC) algorithm, as a typical data-driven algorithm, requires less data and demonstrates better robustness in practical applications [25]–[27]. In [28], a resilient MFAC method is provided to defend against the DoS attacks in the senor-controller channel. Nevertheless, they do not take the FDI attack and limited communication resources into consideration, which motivates our work.

As a crucial component of new infrastructure development, the industrial internet breaks the isolation boundaries of industrial control systems by facilitating the integration of information technology (IT) and operational technology (OT). It transforms industrial control networks from closed and isolated systems to open, interconnected, universal, and standardized platforms [29]–[31]. With increasing demands for computing power and functionality, Windows-based industrial personal computer (IPC) control systems are gradually replacing traditional control systems in cigarette makers [32], [33]. The production network of the cigarette control system is connected to the management network. Apart from the border protection, there are almost no internal security measures within the system, which makes the IPC control system susceptible to numerous intelligent network attacks. Due to the fact that the security problems have not been addressed for the cigarette weight control system in the existing works [4], [5], we propose an event-triggered MFAC approach for cigarette weight control systems to defend against both DoS attacks and FDI attacks. The main contributions are as follows:

1) The new resilient MFAC frameworks are designed for the cigarette weight control system to defend against DoS and FDI attacks in the communication channels between sensors and controllers. The proposed approach only utilizes the input and output data of the systems.

2) A detector based on a prediction algorithm is given to detect potential attacks on the system. To defend against these attacks, a predictive compensation algorithm is designed to mitigate the impacts of DoS attacks.

3) A novel event-based transmission mechanism with the dead-zone operator is proposed to conserve communication resources, in which Zeno behaviors are executed.

The subsequent sections of this paper are organized as: Section II presents the problem formulations, while the main results are presented in Section III. Section IV provides the stability analysis. Sections V and VI contain the simulation example and conclusion, respectively.

II. PROBLEM FORMULATION

A. CIGARETTE WEIGHT CONTROL SYSTEM

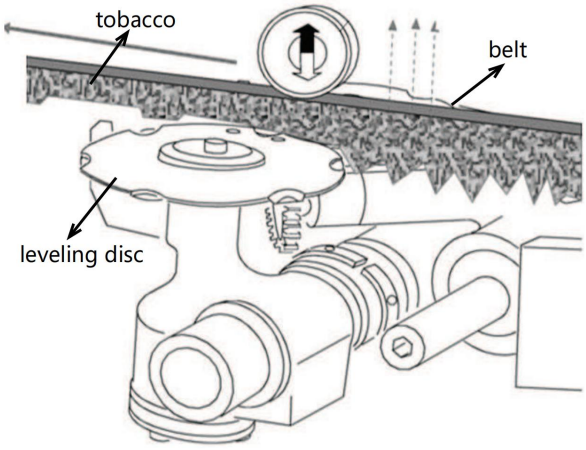

FIGURE 1. Schematic diagram of the cutting part in the cigarette weight control system

The leveling plate module in the cigarette weight control system can be regarded as a servo system. In the existing method of tobacco suction molding, as shown in Fig. 1, tobacco is attached to the belts by negative pressure and then conveyed to the leveling disc via the belts. After being cut on a flat plate, the remaining shredded tobacco is rolled into tobacco sticks. During this process, the density of the remaining shredded tobacco is measured by microwave detection devices to determine whether the current height of the leveling disc is appropriate. Specifically, the reference

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

control loop generates the online reference signal L_d for the height of the leveling disc based on the preset normal cigarette weight m^* and the detected tobacco density. Notably, the reference height L_d varies over time due to the stochastic nature of the tobacco density sucked onto the belt. Once the controller module receives data packets from the local sensor and the reference value L_d via the networks, it will generate voltage signals $V(k)$ to drive the servo motors, adjusting the leveling disc height to the reference value L_d. Since the density of the cut tobacco usually experiences slight fluctuations during two consecutive operations within the same batch, the aforementioned control process can effectively keep the cigarette weight within the required m^* range while maintaining an acceptable level of fault tolerance.

The working principle of the DC servo motor in the cigarette system is similar to that of an ordinary DC motor. The electromagnetic torque is generated by the action of armature air flow and air gap flux, which makes the servo motor rotate. The armature control method is usually used to change the speed by changing the voltage under the condition of keeping the excitation voltage unchanged. The lower the voltage, the lower the speed, and if the voltage is zero, it will stop turning. Considering the physical and electromagnetic characteristics of the servo system, it has [34], [35]

$$V(k) = R_s \cdot i_s(k) + L_s \frac{di_s(k)}{dk} + E_s(k), \tag{1}$$

where $V(k)$ represents armature voltage and $i_s(k)$ denotes armature current. L_s and R_s are the inductances and resistances of the armature windings, respectively. The back electromotive fore $E_s(k)$ can be expressed as

$$E_s(k) = P_e \cdot \omega(k), \tag{2}$$

where P_e represents motor torque constant and $\omega(k)$ is angular speed. The motor torque $T_s(k)$ satisfies the following expressions among those related to current $i_s(k)$, angular speed $\omega(k)$, and load torques $T_l(k)$ [4]

$$T_s(k) = P_m \cdot i_s(k), \tag{3}$$

$$T_s(k) = J_s \frac{d\omega(k)}{dk} + \beta\omega(k) + T_l(k), \tag{4}$$

where P_m and J_s denote load electromagnetic and torque rotational inertia, respectively. β is a viscous friction coefficient. Therefore, the mathematical expression of the system can be given as

$$\begin{cases} V(k) = R_s \cdot i_s(k) + L_s \dfrac{di_s(k)}{dk} + E_s(k), \\ E_s(k) = P_e \cdot \omega(k), \\ T_s(k) = P_m \cdot i_s(k), \\ T_s(k) = J_s \dfrac{d\omega(k)}{dk} + \beta\omega(k) + T_l(k), \end{cases} \tag{5}$$

Additionally, the angular speed $\omega(k)$ and the height $L(k)$ of the cleaver plate satisfy:

$$\begin{cases} \theta(k) = \int \omega(k)dk, \\ L(k) = n \cdot \theta(k), \end{cases} \tag{6}$$

where $\theta(k)$ denotes the rotation angles. From the (6), one can see that $\omega(k) = \frac{d\theta(k)}{dk} = \frac{1}{n}\frac{dL(k)}{dk}$. For the sampling period K, the $\omega(k)$ satisfied the discrete-time dynamics $\omega(t) = \frac{1}{n}\frac{L(t+1)-L(t)}{K}$.

B. SYSTEM ASSUMPTIONS AND ATTACK MODELS

It can be observed from (5) that the system dynamics exhibit strong nonlinearity. To facilitate analysis, the dynamics of the servo motor are reformulated into a more general discrete form

$$L(t+1) = \Psi(L(t), V(t)), \tag{7}$$

where t represents the discrete-time instant and $\Psi(\cdot)$ denotes the unknown nonlinear function related to the unknown dynamics of the system. Two following assumptions are provided for the system (7) to limit the discussed range:

Assumption 1: The partial derivatives $\Psi(\cdot)$ with respect to $V(t)$ are continuous.

Assumption 2: The systems (7) satisfy the Lipschitz condition: for $t \geq 0$, and $\Delta V(t) \neq 0$, it has

$$|\Delta L(t+1)| \leq b|\Delta V(t)|, \tag{8}$$

where $\Delta L(t+1) = L(t+1) - L(t)$, $\Delta V(t) = V(t) - V(t-1)$, $b > 0$ is a positive constant.

Lemma 1: [36] If the system (7) fulfills Assumptions 1-2 and $|\Delta V(t)| \neq 0$, there exists an unknown bounded parameter $\zeta(t)$ referred to as pseudo-partial derivative (PPD). In this context, (7) can be reformulated in the following general form:

$$\Delta L(t+1) = \zeta(t)\Delta V(t). \tag{9}$$

Remark 1: In fact, Assumptions 1-2 are acceptable for the cigarette weight control system. As a typical premise in controller design for nonlinear systems, Assumption 1 is reasonable for the dynamics (5). Assumption 2 is consistent with the behavior of the cigarette system, where a finite change in voltage corresponds to a finite change in the leveling disc height.

In an unreliable communication environment, DoS and FDI attackers launch a series of targeted attacks on the system locally or globally by monitoring and analyzing the characteristics of the network and data. It is active and premediated for the open network. The common steps of an attacker invading the IPC control system of a cigarette maker are as follows: 1) threaten infection and transmission: the threat sources that exist in the wide area network and portable devices infect and spread through phishing, U-disk ferry and so on; 2) penetrating the controller: once a computer is infected, the attack extends to threats on peripheral devices like the human-computer interface (HMI) and programmer, serving as a starting point to invade the controller; 3) implementation of attacks: after successfully invading the controller, the attacker will launch attacks on physical devices and network channels through the EtherCAT bus, IO devices, monitoring network frequency, and so on. FDI attackers send

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

false status information to the HMI and other devices during the invasion period intending to deceive on-site operators, ultimately leading to the disruption of production activities.

As pointed out in [37], a frequently used DoS technique is to launch DoS attacks on communication channels by interfering with their radio frequencies so the controller can no longer receive information from the sensor. Similar to [37]–[39], we consider a kind of random DoS attack. This attack is designed to jam the communication channels between sensors and controllers in the cigarette control system, thereby preventing information exchange among components of the system and leading to the loss of sensor data. The stochastic activities of DoS attacks on the system are described as

$$L_{\mathrm{DoS}}(t) = \sigma_1(t)\breve{L}(t), \tag{10}$$

where $\breve{L}(t)$ is the transmitted data to be given later while the stochastic variable $\sigma_1(t) \in \{0,1\}$ obeying Bernoulli distributed process

$$\begin{cases} \mathrm{Prob}\{\sigma_1(t)=1\} = E\{\sigma_1(t)\} = \vartheta, \\ \mathrm{Prob}\{\sigma_1(t)=0\} = 1 - E\{\sigma_1(t)\} = 1-\vartheta, \end{cases} \tag{11}$$

where $\vartheta \in (0,1)$. For known $\eta > 0$, it assumes that $E\left\{(\sigma_1(t)-\vartheta)^2\right\} = \eta$ holds with expectation operators E.

By identifying the current system configuration, FDI attackers can inject malicious measurements that mislead the state estimation process without being detected by inappropriate or limited measurement detection techniques. The FDI attackers inject false information randomly into the network communication channels, aiming to destabilize the system. To mitigate the impact of corrupted transmission data, we propose an attack detection mechanism based on a predictor, formulated as follows:

$$\begin{cases} \left|\breve{L}(t|t^p) - L_s(t)\right| \le \tau, \sigma_2(t) = 1, \\ \left|\breve{L}(t|t^p) - L_s(t)\right| > \tau, \sigma_2(t) = 0, \end{cases} \tag{12}$$

where the predicted output $\breve{L}(t|t^p)$ is generated by the compensator based on the transmitted trusted data. $L_s(t)$ denotes the signal received by controller. If there is no FDI attacks, $L_s(t) = \breve{L}(t)$, else, $L_s(t) = \breve{L}(t) + f(t)$. The signals under the DoS attacks and FDI attacks satisfy

$$L_{attack}(t) = \sigma_1(t)\breve{L}(t) + (1-\sigma_2(t))f(t). \tag{13}$$

Remark 2: The occurrence of attacks depends on many factors, including but not limited to unreliable network environments, attack positions, and attack strategies. So far, a variety of attack problems for the controlled systems against these attacks have been investigated in [40]–[42]. The possibility of attackers in the controlled environment is also a major concern of APT attack issues. But the essential causes are the differences among APT, FDI, and DoS attacks. Different from the FDI and DoS attacks, APT attacks aim to tamper with the information, steal data, and execute and stop a task or program [43]. According to the characteristics of three types of attacks, different defense strategies should be adopted to deal with them.

C. CONTROL OBJECTIVE

Considering the limited communications resources and complicated network environments, the main control object of this paper is to design a resilient controller based on an event-triggered mechanism such that the output $L(t)$ of cigarette weight control system can be adjusted online according to reference signals $L_d(t+1)$ under FDI attacks and DoS attacks.

III. MAIN RESULTS

A. THE DESIGN OF EVENT-BASED MFAC FRAMEWORK

In this section, we will design the event-based MFAC control algorithm based on the aforementioned strategy. At first, we construct the criterion function to obtain an estimation algorithm for the unknown PPDs

$$\begin{aligned} J(\hat{\zeta}(t)) =& |L(t) - L(t-1) - \hat{\zeta}(t)\Delta V(t-1)|^2 \\ &+ \eta(\hat{\zeta}(t) - \hat{\zeta}(t-1))^2 \\ =& \Delta L^2(t) - 2\Delta L(t)\hat{\zeta}(t)\Delta V(t-1) \\ &+ [\hat{\zeta}(t)\Delta V(t-1)]^2 + \eta(\hat{\zeta}(t) - \hat{\zeta}(t-1))^2, \end{aligned} \tag{14}$$

where the weighting factor $\eta > 0$ denotes the positive constant and $\hat{\zeta}(t)$ represents the estimation value of $\zeta(t)$.

Remark 3: The first term of the cost function (14) reflects the characteristics of dynamics (7). The second term is associated with the estimation errors of PPDs, and minimizing this term can achieve optimal estimation performance. In other words, a robust estimation algorithm can ensure minimizing the change of PPD while obeying the linear dynamics $\Delta L(t) = \hat{\zeta}(t)\Delta V(t-1)$.

The minimization of the above criterion functions yields the following estimation algorithm:

$$\begin{aligned} &\frac{\partial J(\hat{\zeta}(t))}{\partial \hat{\zeta}(t)} \\ =& -2\Delta L(t)\Delta V(t-1) + 2[\hat{\zeta}(t)\Delta V(t-1)]\Delta V(t-1) \\ &+ 2\eta(\hat{\zeta}(t) - \hat{\zeta}(t-1)) \\ =& 2\left[(\hat{\zeta}(t) - \hat{\zeta}(t-1))\Delta V^2(t-1)\right] + 2\hat{\zeta}(t-1)\Delta V^2(t-1) \\ &- 2\Delta L(t)\Delta V(t-1) + 2\eta(\hat{\zeta}(t) - \hat{\zeta}(t-1)) = 0, \end{aligned} \tag{15}$$

then, it has

$$\hat{\zeta}(t) = \hat{\zeta}(t-1) + \frac{\mu\Delta V(t-1)}{\eta + \Delta V^2(t-1)}(\Delta L(t) - \hat{\zeta}(t-1)\Delta V(t-1)), \tag{16}$$

where μ is the step-size to make the algorithm more general. To achieve control objectives, the cost function of input signal

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

$V(t)$ is designed as

$$\begin{aligned} & J(V(t)) \\ =& |L_d(t+1)-L(t+1)|^2+\rho|V(t)-V(t-1)|^2 \\ =& |L_d(t+1)-L(t)-\zeta(t)\Delta V(t)|^2+\rho|V(t)-V(t-1)|^2 \\ =& [L_d(t+1)-L(t)]^2-2\left[L_d(t+1)-L(t)\right]\zeta(t)\Delta V(t) \\ & +[\zeta(t)\Delta V(t)]^2+\rho[\Delta V(t)]^2, \end{aligned} \tag{17}$$

where ρ is a positive weighting factor.

Remark 4: The first term of the function (14) represents the error tracking cost between the actual output height and the desired height. The perfect tracking performance reflects the satisfied tobacco weight in cigarettes. The second term denotes the voltage change involving motor steady operation and the power supply, and minimizing this term is to make the signal change in a gentle way.

Then, it has

$$\begin{aligned} \frac{\partial J(V(t))}{\partial V(t)} =& -2[L_d(t+1)-L(t)]\zeta(t) \\ & +2[\zeta(t)\Delta V(t)]\zeta(t)+2\rho[\Delta V(t)]=0, \end{aligned} \tag{18}$$

and we can get

$$V(t)=V(t-1)+\frac{\lambda\zeta(t)}{\rho+\zeta^2(t)}\left(L_d(t+1)-L(t)\right), \tag{19}$$

where λ is the step-size to make the algorithm more general. Since $\zeta(t)$ in (19) is unknown, we replace it with $\hat{\zeta}(t)$:

$$V(t)=V(t-1)+\frac{\lambda\hat{\zeta}(t)}{\rho+\hat{\zeta}^2(t)}\left(L_d(t+1)-L(t)\right). \tag{20}$$

In order to make the algorithms have stronger ability to track time-varying parameter, a reset estimation algorithm is adopted as

$$\hat{\zeta}(t)=\hat{\zeta}(1), \quad \text{if } \hat{\zeta}(t)\le\varpi \text{ or } |\Delta V(t-1)|\le\varpi, \tag{21}$$

where ϖ is a small positive constant, $\hat{\zeta}(1)$ is the initial estimation value of $\zeta(t)$.

Compared to periodic communication, the characteristic of ETC is that data transmission only occurs when the conditions related to the state (43) are satisfied. The main idea of designing the ETC mechanism for MFAC algorithm is that the updates of $\hat{\zeta}(t)$ and the controller occur only at triggering moments. The index operator $o(t)$ is used to indicate whether the event trigger occurs or not, which is defined as

$$o(t)=\begin{cases}1, & \text{event is triggered,}\\ 0, & \text{event is not triggered.}\end{cases} \tag{22}$$

Therefore, according to (16), and (20), the event-based MFAC algorithm for the dynamic systems (7) is developed as

$$\hat{\zeta}(t)=\hat{\zeta}(t-1)+o(t)\frac{\mu\Delta V(t-1)}{\eta+\Delta V^2(t-1)}(\Delta L(t)-\hat{\zeta}(t-1) \Delta V(t-1)), \tag{23a}$$

$$\hat{\zeta}(t)=\hat{\zeta}(1), \quad \text{if } |\hat{\zeta}(t)|\le\varpi \text{ or } |\Delta V(t-1)|\le\varpi, \text{ or } \operatorname{sign}(\hat{\zeta}(t))\ne\operatorname{sign}(\hat{\zeta}(1)), \tag{23b}$$

$$V(t)=V(t-1)+\frac{\lambda\hat{\zeta}(t)}{\rho+\hat{\zeta}^2(t)}\left(L_d(t+1)-\breve{L}(t)\right) \tag{23c}$$

where the condition $\operatorname{sign}(\hat{\zeta}(t))\ne\operatorname{sign}(\hat{\zeta}(1))$ implies that $\hat{\zeta}(t)\ge 0$ or $\hat{\zeta}(t)\le 0$ holds for all t [44]. Let $D_t=[\breve{L}(t)\quad\hat{\zeta}(t)]^T$ be the data package sent to the controller and the predictor at the triggering instant.

Remark 5: The algorithms (19)-(21) are classical MFAC algorithms first proposed in [25]. To conserve network communication resources, we introduce an event-triggered operator $o(t)$ into the update law (23a) and provide appropriate triggering conditions in (43)-(44). In light of attacks on communication channels, it has $V(t)=V(t-1)+\frac{\lambda\hat{\zeta}(t)}{\rho+\hat{\zeta}^2(t)}(L_d(t+1)-L_{attack}(t))$. To mitigate the impact of attacks, we will design a predictive compensation mechanism in which the compensated data will replace the contaminated data $L_{attack}(t)$ transmitted to the controller.

B. THE DESIGN OF PREDICTIVE COMPENSATION SIGNAL

In this section, the predictive compensation signal $\breve{L}(t\mid t^p)$ will be designed based on the algorithm (23)-(23c). When the event trigger condition given later is violated at instant t_j, the data transmitted from the event trigger module to the controller/compensator through the network is

$$\breve{L}(t)=L\left(t_j\right), \tag{24}$$

$$\zeta(t)=\zeta\left(t_j\right), \tag{25}$$

$$\Delta\breve{V}(t)=\Delta V\left(t_j\right), \tag{26}$$

for $t_j\le t<t_{j+1}$, t_j is the j-th event-triggering time-stamp packed with $\hat{\zeta}(t)$ and $\breve{L}(t)$ in D_t.

Assume that reference height sequence $\Upsilon_d(t+1)=[L_d(t+1),\ldots,L_d(t+\bar{n}+1)]^T$ can be obtained and stored in the controller and predictor in advance. Moreover, the maximum time of the predictive iteration algorithm is $\bar{n}=\bar{t}_1+\bar{t}_2-1$, where $\bar{t}_2$ is the upper bound between two consecutive event-triggering intervals, and every network attack initiated occurs at the moment when the event is triggered.

According to the successfully transmitted feedback data $\breve{L}(t)$, the iterative predictive algorithm is proposed as follows:

$$\Delta V\left(t^p\mid t^p\right)=\varsigma\left(t^p\right)\left(L_d\left(t^p+1\right)-\breve{L}\left(t^p\mid t^p\right)\right), \tag{27}$$

where t^p is a time-stamp of predictor at that the instant $\breve{L}(t)$ arrives. Correspondingly, variables at the instant t^p are defined as $\hat{\zeta}(t^p)=\hat{\zeta}(t), \varsigma\left(t^p\right)=\left(\lambda\hat{\zeta}\left(t^p\right)\right)/\left(\rho+\hat{\zeta}^2\left(t^p\right)\right)$, $\breve{V}(t^p\mid t^p)=\breve{V}\left(t^p\right)$ and $\breve{L}\left(t^p\mid t^p\right)=\breve{L}\left(t^p\right)=\breve{L}(t)$, respectively .

The predictive output increment can be calculated by the following equations:

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

$$\Delta\breve{L}\left(t^p+n\mid t^p\right)=\hat{\zeta}\left(t^p\right)\Delta\breve{V}\left(t^p+n-1\mid t^p\right), \tag{28}$$

$$\breve{L}\left(t^p+n\mid t^p\right)=\breve{L}\left(t^p+n-1\mid t^p\right)+\Delta\breve{L}\left(t^p+n\mid t^p\right), \tag{29}$$

$$\Delta\breve{V}\left(t^p+n\mid t^p\right)=\varsigma\left(t^p\right)\left(L_d\left(t^p+1\right)-\breve{L}\left(t^p+n\mid t^p\right)\right), \tag{30}$$

where $\Delta\breve{L}\left(t^p+n\mid t^p\right)$, $\breve{L}\left(t^p+n\mid t^p\right)$, and $\Delta\breve{V}\left(t^p+n\mid t^p\right)$ denote the predictive values of $\Delta\breve{L}\left(t+n\right)$, $\breve{L}\left(t+n\right)$ and $\Delta\breve{V}\left(t+n\right)$, respectively. From (19), the cumulative sum of predictive output increments based on the data received at latest transmission t^p is

$$\Delta\breve{L}_s\left(t^p+n\mid t^p\right)=\Delta\breve{L}_s\left(t^p+n-1\mid t^p\right)+\Delta\breve{L}\left(t^p+n\mid t^p\right), \tag{31}$$

with $\triangle\breve{L}_s\left(t^p+1\mid t^p\right)=\Delta\breve{L}\left(t^p+1\mid t^p\right)$.

The prediction sequence used to compensate for attacks is

$$\Delta\breve{L}_{t^*}^s=\left[\Delta\breve{L}_s\left(t^p\mid t^p\right),\Delta\breve{L}_s\left(t^p+1\mid t^p\right),\cdots,\Delta\breve{L}_s\left(t^p+\bar{n}\mid t^p\right)\right]^{\mathrm{T}}, \tag{32}$$

which is saved in the buffer with $\hat{\zeta}\left(t^p\right)=\hat{\zeta}(t)$. If the attack takes place at time $t=t^p+n$, the compensation signal of $\breve{L}\left(t^p+n\right)$ is computed by

$$\breve{L}\left(t\mid t^p\right)=\breve{L}\left(t^p+n\mid t^p\right)=\Delta\breve{L}_s\left(t\mid t^p\right)+\breve{L}\left(t^p-1\right). \tag{33}$$

Now, we start to discuss the boundedness of triggering predictive output increment $\Delta\breve{L}_s\left(t\mid t^p\right)$.

Lemma 2: Consider the given algorithm of attack predictive output (27)-(33). The increment $\Delta\breve{L}_s\left(t\mid t^p\right)$ is bounded for $t>t^p$.

Proof: The detailed proof is given in Appendix A. ■

Next, we design the event-triggering mechanism. From (33), it has

$$\begin{aligned}\breve{L}(t)&=\breve{L}\left(t^p-1\right)+\Delta\breve{L}_s\left(t^p+n-1\mid t^p\right)\\&\quad+\breve{L}\left(t\mid t^p\right)-\breve{L}\left(t^p+n-1\mid t^p\right)\\&=\breve{L}\left(t\mid t^p\right)+\Delta(t),\end{aligned} \tag{34}$$

where

$$\begin{aligned}\Delta(t)&=\breve{L}\left(t^p-1\right)-\breve{L}\left(t^p+n-1\mid t^p\right)\\&\quad+\left(1-\left(1-\hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\right)^{n-1}\right)\left(L_d^p-\breve{L}\left(t^p\mid t^p\right)\right).\end{aligned} \tag{35}$$

Notice that the output measurement value $L(t)$ is bounded, $\breve{L}\left(t^p-1\right)$ and $\breve{L}\left(t^p+n-1\mid t^p\right)$ are also bounded. In addition, we can acquire $\hat{\zeta}\left(t^p\right)\le\hat{g},0<\hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)<1$. Hence, there is an upper bound of the variable $\Delta(t)$, that is, $\Delta(t)<\bar{\Delta}$ holds for all time t.

Remark 6: As depicted in the Fig. 2, a compensator based on prediction algorithms is embedded on the controller side to defend against attacks in the sensor-controller channel. When the predictor receives $\breve{L}(t)$ and $\hat{\xi}(t)$ sent by the senor at instant t, it will be activated and mark these latest data $\breve{L}(t)$ and $\hat{\xi}(t)$ as $\breve{L}(t^p)$ and $\hat{\xi}(t^p)$, respectively. Subsequently, the predictor generates a series of predictive sequences $\Delta\breve{L}_{t^*}^s=\left[\Delta\breve{L}_s\left(t^p\mid t^p\right)\quad\Delta\breve{L}_s\left(t^p+1\mid t^p\right)\cdots\Delta\breve{L}_s\left(t^p+\bar{n}\mid t^p\right)\right]^{\mathrm{T}}$ and stores them in the buffer. Note that the predictive algorithms (27) -(30) operate along the predictive axis, and the variables $\hat{\zeta}\left(t^p\right)=\hat{\zeta}(t)$, $\varsigma\left(t^p\right)=\left(\lambda\hat{\zeta}\left(t^p\right)\right)/\left(\rho+\hat{\zeta}^2\left(t^p\right)\right)$ and the reference signal $L_d\left(t^p+1\right)$ remain same during this process. Additionally, the values of $\breve{L}(t^p)$ and $\hat{\xi}(t^p)$ will not be updated until the predictor receives the new uncontaminated data from the sensor. Once FDI or DoS attacks happen, the compensator will select the corresponding data from the buffer and send the compensation signal calculated in (33) to the controller.

C. THE DESIGN OF RESILIENT CONTROLLER

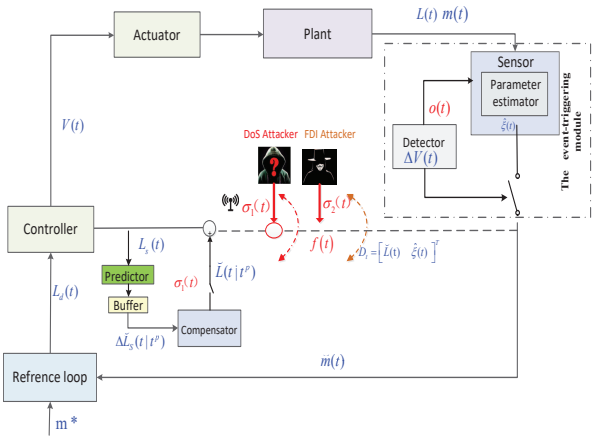

FIGURE 2. Framework of the nonlinear system against jamming attacks

In this section, we will provide the resilient controller in details. In order to mitigate the effects of attacks, as shown in Fig. 2, we provide a compensation mechanism under the assumption that the compensator of the system can supervise network attacks. Consider the situation that FDI and DoS attacks take place in the channel between controller and sensor, where two kinds of attacks are not allowed to occur at the same time. When FDI attacks or DoS attacks occur, the compensator will extract the corresponding prediction values from the buffer and send them to the controller to substitute these polluted or lost data. Therefore, the compensation signal $L_{\mathrm{A}}\left(t\right)$ is designed as

$$\begin{aligned}L_A(t)=&\sigma_2(t)[\sigma_1(t)\breve{L}(t)+(1-\sigma_2(t))f(t)]\\&+[\sigma_2(t)(1-\sigma_1(t))+(1-\sigma_2(t))]\breve{L}\left(t\mid t^p\right),\end{aligned} \tag{36}$$

where $\breve{L}\left(t\mid t^p\right)$ is predictive value of $\breve{L}\left(t\right)$ by using trusted data at instant of t^p. In view of the fact that $L_A(t)$ can not be

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

obtained by controller directly. Therefore, the the developed resilient MFAC algorithm based on observer can be further designed as follows:

$$\hat{\zeta}(t) = \hat{\zeta}(t-1) + o(t)\frac{\mu \Delta V(t-1)}{\eta + \Delta V^2(t-1)}(\Delta L(t) - \hat{\zeta}(t-1)\Delta V(t-1)), \tag{37}$$

$$\hat{\zeta}(t) = \hat{\zeta}(1) \text{ if } |\hat{\zeta}(t)| \le \theta \text{ or } |\Delta V(t-1)| \le \xi \text{ or } \operatorname{sign}(\hat{\zeta}(t)) \ne \operatorname{sign}(\hat{\zeta}(1)), \tag{38}$$

$$V(t) = V(t-1) + \frac{\lambda \hat{\zeta}(t)}{\rho + \hat{\zeta}^2(t)}\left(L_d(t+1) - \hat{L}_A(t)\right), \tag{39}$$

$$\hat{L}_A(t) = \hat{L}_A(t-1) + \hat{\zeta}(t-1)\Delta V(t-1) + \gamma\left(\hat{L}_A(t-1) - L_A(t-1)\right), \tag{40}$$

where the $\hat{L}_A(t)$ is the observer value of $L_A(t)$, and γ is the feedback gain. The observer error $e_\delta(t)$ is defined as

$$e_\delta(t) = \hat{L}_A(t) - \breve{L}(t). \tag{41}$$

According to (26), we define the input error $e_u(t)$ as

$$e_u(t) = \Delta V(t) - \Delta \breve{V}(t). \tag{42}$$

In addition, the event-triggering scheme is designed as

$$t_{j+1} = \inf\left\{ t > t_j \left| B\left(|e_u(t)|\right) \ge \sqrt{\frac{\omega\left(1 - 3(1+\gamma)^2\right)}{3\hat{g}^2}} \right| e_\delta(t) \right| \bigcup t - t_j \ge t_2 \Big\}, \tag{43}$$

where $1 < \omega < 1 - \frac{1}{(1-3(1+\gamma)^2)}$ is a constant and $B(\cdot)$ is the dead-zone operator satisfying

$$B\left(|e_u(t)|\right) = \begin{cases} |e_u(t)|, & |e_\delta(t)| \ge \sqrt{\Theta} \\ 0, & \text{otherwise} \end{cases} \tag{44}$$

where Θ will be illustrated later.

Remark 7: When the attacks happen in the transmission channel successfully, the data package D_t is lost. $L_A(t)$ in (36) will substitute the lost data $\breve{L}(t)$ to be sent to the controller. Since the parameter $\hat{\zeta}(t)$ changes very slowly in those interval, $\hat{\zeta}(t^p) = \hat{\zeta}(t)$, which is packed in the data package $D_A = \left[L_A(t) \quad \hat{\zeta}(t^p)\right]^T$, will be sent to the controller to replace $D_t = [\breve{L}(t) \quad \hat{\zeta}(t)]^T$. By establishing a reasonable condition (43) related to the error $e_\delta(t)$ and $e_u(t)$, the proposed ETM can save communication resources without affecting the stability of the system.

Remark 8: The proposed ETC mechanism has two merits. First, the introduction of the additional condition $t - t_j \ge t_2$ prevents the trigger mechanism from "sleeping" for a long time. The condition can also be utilized to judge whether the module is working properly. Second, Zeno behaviors can be effectively executed by incorporating the dead-zone operator $B(\cdot)$.

IV. STABILITY ANALYSIS

Theorem 1: Take nonlinear systems (7) with Assumptions 1-2 into account. If the event-based model-free adaptive controller (23) is designed with PCA (27)-(33) and the event-triggering conditions (43), then the error $e_\delta(t)$ is bounded in the mean-square sense.

Proof: The proof is given in Appendix B. ■

V. SIMULATION RESULTS

A. CIGARETTE WEIGHT CONTROL SYSTEM

To demonstrate the effectiveness of the proposed resilient MFAC methods with the event-triggered mechanism in Eq. (37)-(40), several simulation tests are conducted on the cigarette weight control systems with time-varying reference signals $L_d(t+1)$. In practical scenarios, the leveling disc height $L(t)$ will be adjusted to the appropriate reference position based on the tobacco density on the belt. The relationship between L and random tobacco density ϱ is provided as follows [4]

$$\varrho = 2 \cdot \left(1 + N\left(\mu, \sigma^2\right)\right) \cdot \int_0^L f(L, D) dL, \tag{45}$$

$$f(L, D) = \frac{1}{2} \cdot K_\rho \cdot \left[-a^{-(L-L_0)} + 1\right], \quad 0 < a < 1, \tag{46}$$

where $f(L, D)$, a, K_ρ, and L_0 denote the exponential function, base number, magnification factor, and translation factor, respectively. The parameters μ and σ^2 are chosen as $\mu = 0$, $\sigma^2 = 0.02$. The standard weight of cut tobacco contained in each cigarette is set at 610 mg. According to (45)-(46), the calculated leveling disc height is chosen as the reference signal $L_d(t+1)$. Since tobacco density usually exhibits stochastic behavior, the reference height $L_d(t+1)$ fluctuates around 12 mm. The specific dynamic models of the cigarette weight control system are shown in (5)-(6), and the parameters of the system are chosen as $R_s = 0.2$, $L_a = 0.15$, $P_e = 1$, $P_m = 0.1$, $J_s = 0.02$, and $\beta = 0.05$, respectively. The parameters of the resilient controller (37)-(39) are set as $\lambda = 0.9$, $\rho = 0.1$, $\mu = 0.1$, and $\eta = 0.4$. The FDI attacks injected into the channels are modeled as $f(t) = 0.5\sin(0.5t) + 0.125\cos(t/10)$.

The activities of FDI attack and DoS attack represented by $\sigma_2(t)$ and $\sigma_1(t)$ are shown in Fig. 4. Combined with Fig. 4, one can see that only one attack occurs at each instant. The curves of the system output are plotted in Fig. 5, in which the value of the leveling disc height $L(t)$ is oscillated once the FDI attack or DoS attack is activated. This means that the attacks have an impact on the tracking performance of the cigarette weight control system. The signal $L(t)$ and reference signal $L_d(t)$ under the developed resilient control mechanism are exhibited in Fig. 6. It is obvious that $L(t)$ can closely track the time-varying signal $L_d(t+1)$, and the proposed control method can effectively mitigate the influence of attacks. The corresponding triggered interval time is depicted in Fig. 7, which implies continuous information transmission is avoided and the communication resource is saved.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

B. LOAD FREQUENCY CONTROL SYSTEM

In [28], the impact of attacks is regarded as a kind of delay, where actuator signals do not update until the latest feedback signals are received. This process will last no matter what happens during this period. To exhibit the superiority of our strategy in dealing with attacks, several simulation comparisons have been conducted on the load frequency control system using the same MFAC control framework, with our proposed compensation strategy and the one presented in [28]. First, the dynamics of the i-th area power system are provided as described in [45].

$$\begin{cases} \Delta f_i(s) = \dfrac{1}{sH_i + D_i} \\ \quad \times \left(\dfrac{1}{1+sT_{gi}} \dfrac{1}{1+sT_{ti}} \left(u_i(s) - \dfrac{1}{R_i} \Delta f_i(s) \right) \right. \\ \quad \left. -\Delta P_{di}(s) - \Delta P_{\text{tie}-i}(s) \right), \\ \Delta P_{\text{tie}-i}(s) = \dfrac{2\pi}{s} \displaystyle\sum_{j=1, j\neq i}^{n} T_{ij} \left(\Delta f_i(s) - \Delta f_i(s) \right), \\ \text{ACE}_i(s) = \beta_i \Delta f_i(s) + \Delta P_{\text{tie}-i}(s), \end{cases} \tag{47}$$

where definitions of variables and parameters are provided in Table 1. The variables u_i, Δf_i are the input and output signals of the system, respectively. The primary control objective of the i-th power system is to ensure that Δf_i can track the ideal signals Δf_d under the DoS and FDI attacks. By observing the model (47), one can know that the discrete-time dynamics of the load frequency control system follow the nonlinear dynamics (9). The selection of system parameters can be referred to [46]. The control parameters are set as $\rho = 0.3$, $\nu = 1$, $\eta = 0.25$, and $\lambda = 0.35$. The activities of attackers are shown in Fig. 9. The simulation result is given in Figs. 11, which exhibits good tracking performance among the output signals and reference signals.

TABLE 1. Parameters and signals of the i-th area system [45]

Symbol	Definition
Δf_i	frequency deviation (Hz)
$\Delta P_{\text{tie}-i}$	tie line power deviation (p.u.)
$\Delta P_{\text{m}i}$	generator output power deviation (p.u.)
$\Delta P_{\text{g}i}$	governor valve position deviation (p.u.)
M_i	inertia of generator (p.u. s)
$T_{\text{t}i}$	turbine time constants (s)
$T_{\text{g}i}$	governor time constants (s)
T_{ij}	synchronizing torque coefficient of tie-line between
ACE_i	area control error (ACE) (p.u.)
β_i	frequency bias factor (p.u./Hz)
D_i	generator unit damping coefficient (p.u./Hz)
R_i	speed droop (Hz/p.u.)

In [28], attacks are considered a form of delay, and the actuator signals will not update until the communication between the sensor and controller is restored, regardless of whether attacks occur or not during this interval. The output curves of the system with the resilient controller in [28] are depicted in Fig. 10. Compared with Fig. 11, it can be concluded that our proposed predictive compensation mechanism has better control performance under frequent attacks.

Remark 9: In [27], a model-free controller is devised for a general theoretical model to obtain better control performance and smaller tracking errors than traditional controllers. Several simulation comparisons are carried out in various systems to verify this enhancement. But this work does not take the security problems associated with systems suffering attacks into consideration. It's worth noting that the event-based MFAC algorithm proposed in this paper is given for a specific physical model, that is, the cigarette weight control system, aiming to defend against two types of network attacks. Our primary focus is on designing an effective resilient controller within the MFAC control framework. How to make the proposed resilient MFAC algorithms have better performance in reducing tracking error has not been investigated in this paper, but it is an interesting topic to be studied in the future. Therefore, similar to [28], we conduct simulations in Section V. A to demonstrate the effectiveness of our proposed attack compensation strategy in securing the cigarette weight control system. Additionally, simulation results in Section V. B of another attack compensation strategy proposed in [28] within the same MFAC framework are presented to illustrate the superiority of the devised compensation mechanism.

VI. CONCLUSION

This paper presents MFAC approaches for cigarette weight control systems to counter both DoS and FDI attacks, incorporating a novel event-triggered mechanism. The main contributions are the development of security MFAC frameworks based on neural networks, enabling defense against DoS and FDI attacks in communication channels between sensors and controllers, utilizing only input and output data for robust control. It employs an attack detector with a prediction algorithm for detecting potential attacks, using neural network control algorithms to eliminate false information and predictor values to mitigate DoS attack impacts. Additionally, a novel event-triggered mechanism with a dead-zone operator is proposed to conserve communication resources and ensure bounded tracking

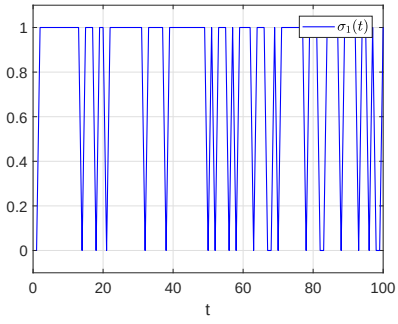

FIGURE 3. The attack variables $\sigma_1(t)$ of DoS attacks with $\vartheta = 0.7$

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

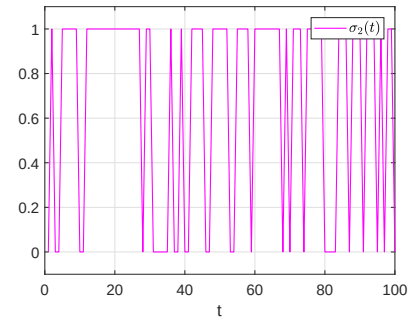

FIGURE 4. The attack variables $\sigma_2(t)$ of FDI attacks

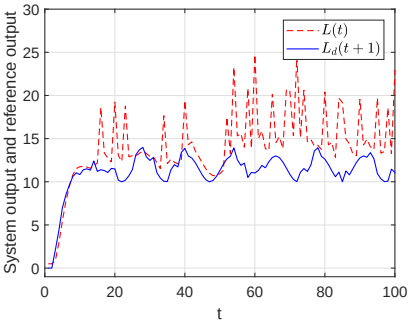

FIGURE 5. The performance of the weight control system suffering the attacks

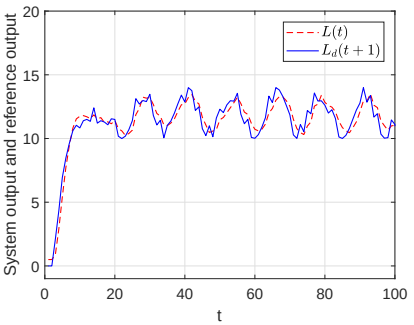

FIGURE 6. The performance of system with controller (39)

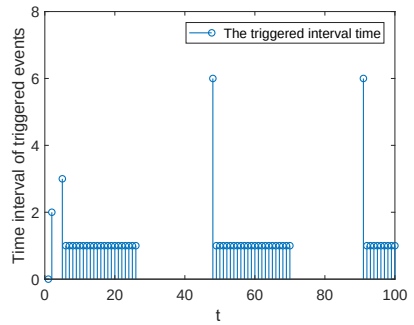

FIGURE 7. Triggering interval time of the system with controller (39)

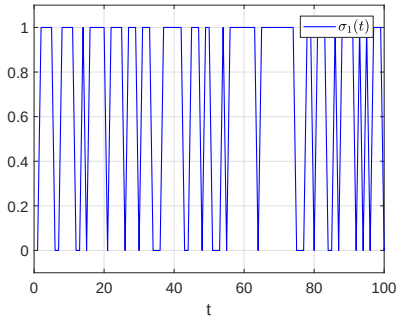

FIGURE 8. The attack variables $\sigma_1(t)$ of DoS attacks with $\vartheta = 0.65$

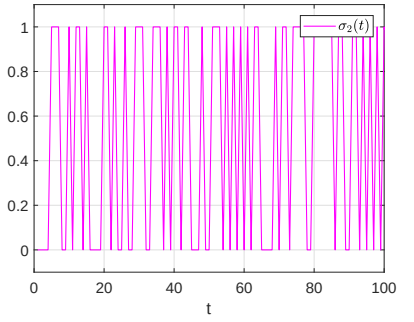

FIGURE 9. The attack variables $\sigma_2(t)$ of FDI attacks

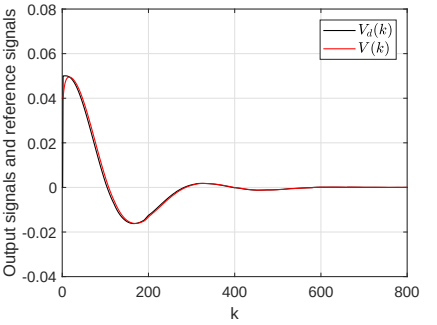

FIGURE 10. The outputs of systems with MFAC predictive compensation algorithm under attacks

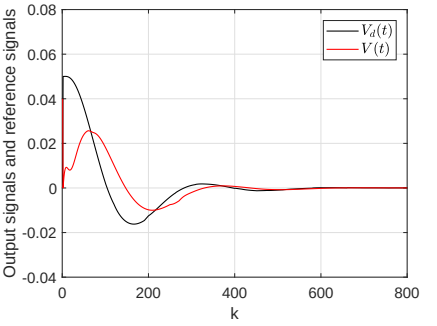

FIGURE 11. The outputs of systems with compensation mechanism in [28] under attacks

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

errors even during attacks, preventing Zeno behaviors for enhanced stability. Finally, some simulation examples show the effectiveness of the method.

Several control strategies have been employed to address the attack problem [28], [47]. These strategies utilize historical data stored in a zero-order holder to compensate for the corrupted data. Nevertheless, the controller will not be updated for a long time when the systems suffer continuous attacks, which affects control performance. Besides, the discrepancy between current data and historical data also becomes large under high-frequency attacks. Our proposed predictive compensation strategy can effectively remove this limitation. But it is worth noting that the utilization of predictors inevitably increases the computational workload and construction cost of the systems. In addition, our algorithm cannot solve the resilient control problem for some stealthy and undetectable attacks [48]. Recently, an iteration single critic learning framework was utilized in [49] for the autonomous vehicles to defend against DoS attacks and receive the satisfied control performance. How to design MFAC algorithms based on the iterative critical learning framework against attacks is an interesting issue to be studied. In the future work, we will also focus on some other factors that may affect the performance of the controller, such as stealthy FDI attacks [48], attack residence time [28], network induced delay [45], and so on.

APPENDIX A

Assume that there exist constants $\Delta L_d^* > 0$ and $\bar{r} > 0$ such that $|L_d(t+1) - L_d(t)| \leq \Delta L_d^*$ and $|L_d(t+1)| \leq \bar{r}$. Notice that $\Delta \breve{L}_s\left(t^p \mid t^p\right) = 0$, from (29) and (33), it follows:

For $t = t^p + 1$, it has

$$\begin{aligned} &\Delta \breve{L}_s\left(t \mid t^p\right) \\ &= \Delta \breve{L}_s\left(t^p+1 \mid t^p\right) \\ &= \Delta \breve{L}_s\left(t^p \mid t^p\right) + \Delta \breve{L}\left(t^p+1 \mid t^p\right) \\ &= \breve{L}\left(t^p+1 \mid t^p\right) - \breve{L}\left(t^p \mid t^p\right) \\ &= \zeta\left(t^p\right)\varsigma\left(t^p\right)\left(L_d\left(t^p+1\right) - \breve{L}\left(t^p \mid t^p\right)\right) \triangleq X. \end{aligned} \tag{48}$$

For $t = t^p + 2$, it has

$$\begin{aligned} &\Delta \breve{L}_s\left(t \mid t^p\right) \\ =&\Delta \breve{L}_s\left(t^p+2 \mid t^p\right) \\ =&\Delta \breve{L}_s\left(t^p+1 \mid t^p\right) + \Delta \breve{L}\left(t^p+2 \mid t^p\right) \\ =&X + \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\left(L_d\left(t^p+2\right) - \breve{L}\left(t^p+1 \mid t^p\right)\right) \\ =&X + \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\left(L_d\left(t^p+1\right) - \left(\Delta \breve{L}\left(t^p+1 \mid t^p\right) + \breve{L}\left(t^p \mid t^p\right)\right)\right. \\ &\left. + L_d\left(t^p+2\right) - L_d\left(t^p+1\right)\right) \\ \leq&X + \left(1 - \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\right)X + \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\Delta L_d^*. \end{aligned} \tag{49}$$

For $t = t^p + 3$, it has

$$\begin{aligned} &\Delta \breve{L}_s\left(t \mid t^p\right) \\ =&\Delta \breve{L}_s\left(t^p+3 \mid t^p\right) \\ =&\Delta \breve{L}_s\left(t^p+2 \mid t^p\right) + \Delta \breve{L}\left(t^p+3 \mid t^p\right) \\ =&\Delta \breve{L}_s\left(t^p+2 \mid t^p\right) + \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\left(L_d\left(t^p+3\right) - \breve{L}\left(t^p+2 \mid t^p\right)\right) \\ =&\Delta \breve{L}_s\left(t^p+2 \mid t^p\right) + \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right) \\ &\times \left(L_d\left(t^p+1\right) - \left(\Delta \breve{L}_s\left(t^p+2 \mid t^p\right) + \breve{L}\left(t^p \mid t^p\right)\right) + L_d\left(t^p+3\right)\right. \\ &\left. - L_d\left(t^p+1\right)\right) \\ \leq&X + \left(1 - \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\right)X + \left(1 - \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\right)^2 X \\ &+ \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\Delta L_d^* + 2\hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\Delta L_d^*. \end{aligned} \tag{50}$$

Furthermore, for $t = t^p + n$, we have

$$\begin{aligned} &\Delta \breve{L}_s\left(t \mid t^p\right) \\ =&\Delta \breve{L}_s\left(t^p+n \mid t^p\right) \\ \leq&X + \left(1 - \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\right)X + \cdots \\ &+ \left(1 - \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\right)^{n-1} X + \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\Delta L_d^* \\ &+ 2\hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\Delta L_d^* + \cdots + (n-1)\hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\Delta L_d^* \\ =&\frac{1 - \left(1 - \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\right)^n}{1 - \left(1 - \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\right)}X + \frac{n(n-1)}{2}\hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\Delta L_d^* \\ \leq&\left(1 - \left(1 - \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\right)^n\right)\left(L_d\left(t^p+1\right) - \breve{L}\left(t^p \mid t^p\right)\right) \\ &+ \frac{n^2}{2}\hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right)\Delta L_d^*. \end{aligned} \tag{51}$$

Due to $n \leq \bar{n}, 0 < \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right) < 1$ and $0 < 1 - \hat{\zeta}\left(t^p\right)\varsigma\left(t^p\right) < 1$, it can be concluded that $\Delta \breve{L}_s\left(t \mid t^p\right)$ is bounded with upper bound $\bar{r} - \breve{L}\left(t^p \mid t^p\right) + \left(\bar{n}^2\right)/(2)\Delta L_d^*$.

APPENDIX B

Case 1: When $\sigma_2(t) = 1$, we can derive $L_A(t) = \sigma_1(t)\breve{L}(t) + [1 - \sigma_1(t)]\breve{L}\left(t \mid t^p\right)$. According to (34), we further obtain

$$L_A(t) = \breve{L}(t) - (1 - \sigma_1(t))\Delta(t), \tag{52}$$

and

$$\breve{L}(t+1) = \breve{L}(t) + \hat{\zeta}(t)\Delta \breve{V}(t). \tag{53}$$

From (9), (37)- (41), (52) and (53), we get

$$\begin{aligned} e_\delta(t+1) &= \hat{L}_A(t+1) - \breve{L}(t+1) \\ &= \hat{L}_A(t) + \hat{\zeta}(t)\Delta V(t) + \gamma\left(\hat{L}_A(t) - L_A(t)\right) \\ &\quad - \breve{L}(t) - \hat{\zeta}(t)\Delta \breve{V}(t) \\ &= e_\delta(t) + \hat{\zeta}(t)(\Delta V(t) - \Delta \breve{V}(t)) \\ &\quad + \gamma\left(\hat{L}_A(t) - \breve{L}(t) + \breve{L}(t) - L_A(t)\right) \end{aligned} \tag{54}$$

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

$$
\begin{aligned}
&= (1+\gamma)e_\delta(t) + \hat{\zeta}(t)e_u(t) + \gamma\left(\breve{L}(t) - L_A(t)\right)\\
&= (1+\gamma)e_\delta(t) + \hat{\zeta}(t)e_u(t) + \gamma\left(1-\sigma_1(t)\right)\Delta(t)\\
&= (1+\gamma)e_\delta(t) + \hat{\zeta}(t)e_u(t) + \gamma\left(\vartheta-\sigma_1(t)\right)\Delta(t)\\
&\quad + \gamma(1-\vartheta)\Delta(t).
\end{aligned}
$$

Consider the following Lyapunov functional candidate

$$\nu(t) = e_\delta^2(t). \tag{55}$$

At the triggering instant $t = t_j$, $e_u(t) = \Delta V(t) - \Delta\breve{V}(t) = 0$. Then, (54) can be rewritten as

$$
\begin{aligned}
e_\delta(t+1) =&(1+\gamma)e_\delta(t) + \gamma\left(\vartheta-\sigma_1(t)\right)\Delta(t)\\
&+ \gamma\left(1-\vartheta\right)\Delta(t).
\end{aligned} \tag{56}
$$

From (11), taking the conditional expectation of the difference $\nu(t)$ yields

$$
\begin{aligned}
&E\{\Delta\nu(t+1)\}\\
&= E\left\{\nu(t+1) - \nu(t) \mid e_\delta(t)\right\}\\
&= E\left\{e_\delta^2(t+1) - e_\delta^2(t) \mid e_\delta(t)\right\}\\
&= E\Big\{(1+\gamma)^2 e_\delta^2(t) + \gamma^2\left(\vartheta-\sigma_1(t)\right)^2\Delta^2(t)\\
&\quad + \gamma^2(1-\vartheta)^2\Delta^2(t) + 2(1+\gamma)e_\delta(t)\gamma\left(\vartheta-\sigma_1(t)\right)\Delta(t)\\
&\quad + 2\gamma^2\left(\vartheta-\sigma_1(t)\right)\Delta(t)(1-\vartheta)\Delta(t)\\
&\quad + 2(1+\gamma)e_\delta(t)\gamma(1-\vartheta)\Delta(t) - e_\delta^2(t) \mid e_\delta(t)\Big\}\\
&\le E\Big\{2(1+\gamma)^2 e_\delta^2(t) + 2\gamma^2(1-\vartheta)^2\Delta^2(t)\\
&\quad + \gamma^2\left(\vartheta-\sigma_1(t)\right)^2\Delta^2(t) - e_\delta^2(t) \mid e_\delta(t)\Big\}\\
&\le -\left(1-2(1+\gamma)^2\right)|e_\delta(t)|^2 + 2\gamma^2(1-\vartheta)^2\bar{\Delta}^2\\
&\quad + \gamma^2\eta\bar{\Delta}^2,
\end{aligned} \tag{57}
$$

then, $E\{\Delta\nu(t+1)\} < 0$ holds if $|e_\delta(t)|^2 > (\eta + 2(1-\vartheta)^2)\gamma^2\bar{\Delta}^2)/(1-2(1+\gamma)^2 = \Theta$. And $E\{\nu(t+1)\} = E\left\{\sum_{i=2}^{t+1}\Delta\nu(i) + \nu(1)\right\} < E\{\nu(1)\}$ implies that $e_\delta(t)$ is bounded in the mean-square sense.

During the interval time, $t_j < t < t_{j+1}$. In this situation, $\Delta\breve{V}(t) \neq \Delta V(t)$. It has

$$
\begin{aligned}
&E\{\Delta\nu(t)\}\\
&\le E\Big\{3(1+\gamma)^2 e_\delta^2(t) + 3\gamma^2(1-\vartheta)^2\Delta^2(t)\\
&\quad + 3\hat{\zeta}^2(t)e_u^2(t) + \gamma^2\left(\vartheta-\sigma_1(t)\right)^2\Delta^2(t) - e_\delta^2(t) \mid e_\delta(t)\Big\}\\
&\le -\left(1-3(1+\gamma)^2\right)e_\delta^2(t) + 3\gamma^2(1-\vartheta)^2\bar{\Delta}^2 + 3\hat{g}^2 e_u^2(t)\\
&\quad + \gamma^2\eta\bar{\Delta}^2.
\end{aligned} \tag{58}
$$

From (43), we have $3\hat{g}^2 e_u^2(t) \le \omega\left(1-3(1+\gamma)^2\right)e_\delta^2(t)$. Then, it yields

$$E\{\Delta\nu(t)\} \le -(1-\omega)\left(1-3(1+\gamma)^2\right)e_\delta^2(t) + \Omega, \tag{59}$$

where $\Omega = \left(\eta + 3\left(1-\vartheta\right)^2\right)\gamma^2\bar{\Delta}^2$. Define $\chi = 1-(1-\omega)(1-3(1+\gamma)^2$, due to $1 < \omega < 1 - \frac{1}{(1-3(1+\gamma)^2)}$, it has $0 < \chi < 1$. And it is not difficult to obtain:

$$
\begin{aligned}
E\{\nu(t+1)\} &\le E\{\chi\nu(t) + \Omega\}\\
&\le \cdots\\
&\le \chi^t\nu(1) + \frac{\Omega\left(1-\chi^t\right)}{1-\chi},
\end{aligned} \tag{60}
$$

which implies the boundedness of the tracking error $e_\delta(t)$.

Case 2: When $\sigma_2(t) = 0$, from(34) and (36), it has $L_A(t) = \breve{L}\left(t \mid t^p\right) = \breve{L}(t) - \Delta(t)$. During the interval time $t_j < t < t_{j+1}$, there is $\Delta\breve{V}(t) \neq \Delta V(t)$ and it is easy to obtain

$$
\begin{aligned}
e_\delta(t+1) &= \hat{L}_A(t+1) - \breve{L}(t+1)\\
&= \hat{L}_A(t) + \hat{\zeta}(t)\Delta V(t) + \gamma\left(\hat{L}_A(t) - L_A(t)\right)\\
&\quad - \breve{L}(t) - \hat{\zeta}(t)\Delta\breve{V}(t)\\
&= e_e(t) + \hat{\zeta}(t)(\Delta V(t) - \Delta\breve{V}(t))\\
&\quad + \gamma\left(\hat{L}_A(t) - \breve{L}(t) + \breve{L}(t) - L_A(t)\right)\\
&= (1+\gamma)e_\delta(t) + \hat{\zeta}(t)e_u(t) + \gamma\left(\breve{L}(t) - L_A(t)\right)\\
&= (1+\gamma)e_\delta(t) + \hat{\zeta}(t)e_u(t) + \gamma\Delta(t).
\end{aligned} \tag{61}
$$

At the instant $t = t_j$, $e_u(t) = \Delta\breve{V}(t) - \Delta V(t) = 0$. In this situation, we have $e_\delta(t+1) = (1+\gamma)e_\delta(t) + \gamma\Delta(t)$. The stability analysis of this case is similarly to the Case 1. Due to the limitation of space, the proof process is omitted. This completes the proof.

REFERENCES

[1] S. S. Xu, H. Huang, Y. Kung, and S. Lin, "Collision-free fuzzy formation control of swarm robotic cyber-physical systems using a robust orthogonal firefly algorithm," *IEEE Access*, vol. 7, pp. 9205–9214, 2019.

[2] M. Henshaw, "Research challenges and transatlantic collaboration on transportation cyber-physical systems," *Transportation Cyber-Physical Systems*, pp. 247–265, 2018.

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

[4] X. Zhang, X. Qiu, W. Meng, Y. Li, and L. Zhang, "An event-triggered predictive control for weight control system," in *2022 12th International Conference on Information Science and Technology (ICIST)*, pp. 171–177, 2022.

[5] Y. Li, X. Zhou, and L. Zhang, "Design and application of double closed loop weight control system for cigarette maker," in *Journal of Physics: Conference Series*, pp. 048–052, 2020.

[6] N. He, K. Ma, and H. Li, "Resilient predictive control strategy of cyber–physical systems against FDI attack," *IET Control Theory & Applications*, vol. 16, no. 11, pp. 1098–1109, 2022.

[7] V. S. Dolk, P. Tesi, C. De Persis, and W. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 93–105, 2016.

[8] G. Morgenstern and T. Routtenberg, "Structural-constrained methods for the identification of false data injection attacks in power systems," *IEEE Access*, vol. 10, pp. 94169–94185, 2022.

[9] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS attack scheduling in wireless networked control system," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 3, pp. 843–852, 2015.

[10] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Başar, "Resilient control of cyber-physical systems against denial-of-service attacks," in *2013 6th International Symposium on Resilient Control Systems (ISRCS)*, pp. 54–59, 2013.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

[11] C. Xie and G. Yang, "Observer-based attack-resilient control for linear systems against FDI attacks on communication links from controller to actuators," *International Journal of Robust and Nonlinear Control*, vol. 28, no. 15, pp. 4382–4403, 2018.

[12] A. Abbaspour, A. Sargolzaei, P. Forouzannezhad, K. K. Yen, and A. I. Sarwat, "Resilient control design for load frequency control system under false data injection attacks," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 9, pp. 7951–7962, 2019.

[13] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li, and J. Zhang, "A FDI attack-resilient distributed secondary control strategy for islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1929–1938, 2020.

[14] B. Wang, X. Meng, and T. Chen, "Event based pulse-modulated control of linear stochastic systems," *IEEE Transactions on Automatic Control*, vol. 59, no. 8, pp. 2144–2150, 2014.

[15] Y. Wang, W. X. Zheng, and H. Zhang, "Dynamic event-based control of nonlinear stochastic systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 12, pp. 6544–6551, 2017.

[16] Q. Zhu, "Stabilization of stochastic nonlinear delay systems with exogenous disturbances and the event-triggered feedback control," *IEEE Transactions on Automatic Control*, vol. 64, no. 9, pp. 3764–3771, 2019.

[17] S. Luo and F. Deng, "On event-triggered control of nonlinear stochastic systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 1, pp. 369–375, 2020.

[18] D. Lehmann, E. Henriksson, and K. H. Johansson, "Event-triggered model predictive control of discrete-time linear systems subject to disturbances," in *2013 European control conference (ECC)*, pp. 1156–1161, 2013.

[19] P. Cheng, Y. Yin, Y. Liu, S. Wang, and F. Pan, "Event-triggered disturbance rejection control of discrete systems," *IEEE Access*, vol. 8, pp. 77934–77939, 2020.

[20] Y. Yan, C. Yang, and X. Ma, "Event-triggered observer-based fuzzy control for coal-fired power generation systems based on singularly perturbed theory," *IEEE Access*, vol. 8, pp. 133283–133294, 2020.

[21] X. Qiu, Y. Wang, X. Xie, and H. Zhang, "Resilient model-free adaptive control for cyber-physical systems against jamming attack," *Neurocomputing*, vol. 413, pp. 422–430, 2020.

[22] Y. Wang, J. Zhang, H. Zhang, and X. Xie, "Adaptive fuzzy output-constrained control for nonlinear stochastic systems with input delay and unknown control coefficients," *IEEE Transactions on Cybernetics*, vol. 51, no. 11, pp. 5279–5290, 2021.

[23] L. Wang, M. Wang, and W. Meng, "System transformation-based event-triggered fuzzy control for state constrained nonlinear systems with unknown control directions," *IEEE Transactions on Fuzzy Systems*, vol. 31, no. 7, pp. 2331–2344, 2023.

[24] B. Rezaee and M. F. Zarandi, "Data-driven fuzzy modeling for takagi–sugeno–kang fuzzy system," *Information Sciences*, vol. 180, no. 2, pp. 241–255, 2010.

[25] Z. Hou and W. Huang, "The model-free learning adaptive control of a class of SISO nonlinear systems," in *Proceedings of the 1997 American Control Conference (Cat. No. 97CH36041)*, vol. 1, pp. 343–344, IEEE, 1997.

[26] X. Bu, Z. Hou, F. Yu, and F. Wang, "Robust model free adaptive control with measurement disturbance," *IET Control Theory & Applications*, vol. 6, no. 9, pp. 1288–1296, 2012.

[27] A. Safaei and M. N. Mahyuddin, "Adaptive model-free control based on an ultra-local model with model-free parameter estimations for a generic SISO system," *IEEE Access*, vol. 6, pp. 4266–4275, 2018.

[28] Y. Ma, W. Che, C. Deng, and Z. Wu, "Distributed model-free adaptive control for learning nonlinear mass under DoS attacks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 3, pp. 1146–1155, 2023.

[29] W. Chen, G. Chen, Y. Zhao, and J. Zhang, "Security vulnerability and encryption technology of computer information technology data under big data environment," in *Journal of Physics: Conference Series*, 2021.

[30] X. Cheng and P. Zhang, "Information security and adoptable solutions in the implementation of industry 4.0 strategy for the fourth-generation industrial revolution," in *Journal of Physics: Conference Series*, 2020.

[31] Y. Jiang, L. Wang, and X. Zhang, "Tobacco system industrial control system security," in *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, pp. 693–696, 2019.

[32] S. Wen and R. Wang, "Comprehensive experimental design of network attack and defensebased on IPC pipeline," *Experiment Science and Technology*, vol. 16, no. 5, pp. 109–113, 2018.

[33] X. Ni, J. Li, Y. Li, D. Wen, X. Jiang, Y. Zhang, L. Wei, and X. Zhang, "Configuration of network security monitoring model for IPC control system of filtered cigarette maker," *Tobacco Science & Technology*, vol. 55, no. 1, 2022.

[34] M. S. Qureshi, P. Swarnkar, and S. Gupta, "Assessment of dc servo motor with sliding mode control approach," in *2016 IEEE First International Conference on Control, Measurement and Instrumentation (CMI)*, pp. 351–355, 2016.

[35] D. K. Meena and S. Chahar, "Speed control of DC servo motor using genetic algorithm," in *2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC)*, pp. 1–7, 2017.

[36] X. Bu, W. Yu, L. Cui, Z. Hou, and Z. Chen, "Event-triggered data-driven load frequency control for multiarea power systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 5982–5991, 2021.

[37] Y. Guan and X. Ge, "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 48–59, 2017.

[38] Z. Lian, F. Guo, C. Wen, C. Deng, and P. Lin, "Distributed resilient optimal current sharing control for an islanded DC microgrid under DoS attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4494–4505, 2021.

[39] Y. Li, W. Meng, B. Fan, S. Zhao, and Q. Yang, "Distributed aperiodic control of multibus DC microgrids with DoS attack resilience," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4815–4827, 2022.

[40] E. N. Yılmaz and S. Gönen, "Attack detection/prevention system against cyber attack in industrial control systems," *Computers & Security*, vol. 77, pp. 94–105, 2018.

[41] D. Zhou, Q. Zhang, F. Guo, Z. Lian, J. Qi, and W. Zhou, "Distributed resilient secondary control for islanded DC microgrids considering unbounded FDI attacks," *IEEE Transactions on Smart Grid*, 2023.

[42] B. Zhao, A. J. Lamadrid, R. S. Blum, and S. Kishore, "A coordinated scheme of electricity-gas systems and impacts of a gas system FDI attacks on electricity system," *International Journal of Electrical Power & Energy Systems*, vol. 131, 2021.

[43] M. Li, W. Huang, Y. Wang, W. Fan, and J. Li, "The study of APT attack stage model," in *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*, pp. 1–5, 2016.

[44] Z. Hou and W. Huang, "The model-free learning adaptive control of a class of SISO nonlinear systems," in *Proceedings of the 1997 American Control Conference (Cat. No.97CH36041)*, vol. 1, pp. 343–344, 1997.

[45] C. Peng, J. Zhang, and H. Yan, "Adaptive event-triggering H_∞ load frequency control for network-based power systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 2, pp. 1685–1694, 2018.

[46] Y. Wang, Z. Wang, J. Gan, H. Zhang, and R. Wang, "Switched observer-based adaptive event-triggered load frequency control for networked power systems under aperiodic DoS attacks," *IEEE Transactions on Smart Grid*, vol. 14, no. 6, pp. 4816–4826, 2023.

[47] L. Schenato, "To zero or to hold control inputs with lossy links," *IEEE Transactions on Automatic Control*.

[48] J. Shi, S. Liu, B. Chen, and L. Yu, "Distributed data-driven intrusion detection for sparse stealthy FDI attacks in smart grids," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 3, pp. 993–997, 2021.

[49] K. Zhang, R. Su, H. Zhang, and Y. Tian, "Adaptive resilient event-triggered control design of autonomous vehicles with an iterative single critic learning framework," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 12, pp. 5502–5511, 2021.

GUOQIAN YE graduated from Zhejiang University of Mechanical Engineering in 1992 with a major in Mechanical Manufacturing. Currently, he is a technical administrator for cigarette equipment at China Tobacco Zhejiang industrial Co., Ltd. His research interests include industrial automation control technology, predictive control, and model free adaptive control.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2024.3384413

LIXIANG SHEN graduated from Zhejiang University of Technology in 2011, majoring in Computer Science and Technology. Currently, he is employed Hangzhou Cigarette Factory of Zhejiang China Tobacco Industry Co., Ltd. as an electrical administrator. His research interests include weight control, security control, and multi-agent systems.

YI FENG graduated from Zhejiang University of Technology in 2008, majoring in Computer-Aided Design. Currently, he is employed at China Tobacco Zhejiang industrial Co., Ltd. His research interests include industrial automation control technology, resilient control, and distributed systems.

LIFENG FAN was born in Zhejiang, China, in 1984. He graduated from Tianjin Engineering Normal University with a major in automation. Currently, he is the chief expert in the field of equipment maintenance at China Tobacco Zhejiang Industrial Co., Ltd. His research interests include automatic control and detection technology for tobacco machinery equipment.

CHI ZHANG as born in Zhejiang, China, in 1987. He graduated from Central South University. Currently, he is employed at China Tobacco Zhejiang Industrial Co., Ltd. His research interests include industrial automation control technology, predictive control, and neural network.

YULIANG LI graduated from Zhejiang University of Technology in 2005, majoring in automation. Currently, he is employed at China Tobacco Zhejiang Industrial Co., Ltd. His research interests include cigarette weight control systems and distributed systems.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/