

# Relentless False Data Injection Attacks Against Kalman-Filter-Based Detection in Smart Grid

Yifa Liu  and Long Cheng , Senior Member, IEEE

**Abstract**—As one of the most dangerous cyber attacks in smart grids, the false data injection attacks pose a serious threat to power system security. To detect the false data, the traditional residual method and other improved methods, such as the Kalman-filter-based detector, have been proposed. However, these methods often have defects, especially in a very complex networked system with noises. By investigating the tolerance to the uncertainty in the residual detection method and properties of noises, the attack magnitude planning has been presented to hide the attack behind noises, which can bypass the residual detection method. As to the Kalman-filter-based detector, this article designs a specific attack strategy that can successfully deceive the Kalman-filter-based detector. Under this strategy, the false data injected at each step are used to balance the anomalies caused by previous false data, making the system look quite normal in monitoring, while deviating the system from normal operation eventually.

**Index Terms**—Attack sequence, false data injection, Kalman filter, smart grid security, state estimation.

## I. INTRODUCTION

ELECTRICITY plays an important role in the daily productions and lives of human beings, and power failure can cause serious losses these days [1]. With the advancement of various industrial developments, especially the advance of Industry 4.0, the demand for electricity has soared significantly [2]. Therefore, the requirements of the management and control for the power systems become urgent. As a result, the smart power grid has been proposed [3]. Adopting digital technology, the smart grid allows the two-way flow of information between power generators and end consumers to help improve efficiency and reliability of the power transformation and transmission. However, with the increasing growth of its scale and complexity, the smart grid has proven to be fragile and vulnerable [4],

[5]. Smart grids use historical data for the dynamic optimization of the grid operation and resource utilization. There are many meters amounted at important components, and those measurements are transmitted to the control center. Based on these measurements, the control center makes the right decision [6]. Therefore, the false data injection (FDI) attacks against the grid state estimation can cause great damage to the smart grid [7], [8].

To combat FDI attacks, the smart grid first needs to detect attacks. The traditional detection method for FDI attacks is to monitor the residual of state estimation [9]. The false data usually do not satisfy the laws of physics, such as Kirchhoff's laws. Even if these laws are satisfied, the false data often contradict the rules of the power system operation. Hence, when the power grid is under FDI attacks, the residual is increasing significantly.

However, it is indicated that the attacker can manipulate the injected false data to bypass the residual detection and introduce arbitrary errors into the state estimation [10], [11]. To be able to detect false data more accurately, many studies have taken different approaches to enhance detection capabilities. Maximum likelihood estimation was applied in [12] and [13]. In [14], an adaptive Markov strategy was utilized to change the threshold values in the detection process. A game theoretic approach was adopted to analyze the optimal detection threshold for FDI in [15]. By using the multiagent system theory, a voting protocol was proposed to evaluate the risk of each element being attacked in [16]. In [17], by examining the difference between estimations obtained from different subsets of sensors, hypothesis testing was proposed to find the attacked part. Even though many improved measures are proposed [18], these methods have a common serious defect: they are all static data-based methods, and rely entirely on the measurement data collected by the sensors. As long as the attacker has adequate knowledge of the grid structure, the well-designed false data can bypass the residual test to avoid being detected.

The defect of the static data-based detection method essentially lies in the lack of the correct reference basis. To overcome these limitations, the Kalman-filter-based detection method has been proposed, which builds a prediction of the grid state based on the grid's historical states. Therefore, this method can detect these carefully designed stealthy FDI attacks [19], [20].

Although the Kalman-filter-based detection has led to great success, many studies may have overoptimistic expectations regarding its detection ability. This is because the serious disruptive effect of noises in the detection process is not fully analyzed. Due to the existence of measurement noises, even without FDI

Manuscript received 23 August 2021; accepted 29 November 2021. Date of publication 6 January 2022; date of current version 19 September 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 61633016, Grant 61873268, Grant 62025307, and Grant U1913209 and in part by the Beijing Natural Science Foundation under Grant JQ19020. Recommended by Associate Editor Andy Sun. (Corresponding author: Long Cheng.)

The authors are with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China, and also with the School of Artificial Intelligence, University of Chinese Academy of Sciences, Beijing 100049, China (e-mail: liuyifa2018@ia.ac.cn; long.cheng@ia.ac.cn).

Digital Object Identifier 10.1109/TCNS.2022.3141026

attacks, the residual of state estimation in the detection method still exists [21]. It is noted that the Kalman-filter-based detection cannot distinguish small amounts of false data and noises [22], [23]. Based on this property, it has been proved that the attacker is able to successfully inject false data without being detected by the Kalman-filter-based detection [23]. Although the results presented in [23] make the first step against the Kalman-filter-based detection, the attack method proposed in [23] cannot cause sufficient damage to the power system. The reasons are summarized as follows.

- 1) The attack magnitude is limited. If the attack magnitude is set too high, the attack is to be detected immediately.
- 2) The attack duration is short. This attack method is based on the assumption that the power grid operates in a steady state. When the grid state is changed by the attacks, the attack method fails and can be detected by the Kalman-filter-based detection.
- 3) The states of the system after the attack have not been well analyzed, which makes it impossible to design the subsequent attack strategy.

Motivated by the aforementioned observations, in order to design a long-term continuous attack strategy to cause fatal harm to the power system, this article quantitatively analyzes the relationship between the attack magnitude and the exposure risk, as well as the conditions for relentless stealthy attacks against the Kalman-filter-based detection. It has been found that the estimations generated by the Kalman filter are based on historical measurement data whose security cannot be guaranteed either. According to this observation, this article tries to take advantage of the previous attacks and further continuously fabricate new and more violent attacks to balance the residuals caused by attacks so as to continuously attack the power grid with an increasing magnitude by theoretical analysis. The simulation results indicate that the detection result based on the Kalman filter at each step can be normal if the attack vectors are well-organized, while the attack strength can be reinforced constantly and push the smart grid to collapse step by step. In addition, the proposed method is proved to be able to avoid being detected by the residual detection method as well, which means that the proposed attack method can bypass the dominant FDI detection methods in the literature.

The contributions of this article are summarized as follows.

- 1) This article proposes a continuous false data injection attack strategy to bypass the traditional residual detection method even if the attacker does not know the precise structure information about the power grid.
- 2) This article finds out the defects of the Kalman-filter-based detection method and constructs an attack sequence of increasing magnitude to bypass the detection, which illustrates that the Kalman-filter-based detector cannot fully ensure the security of the smart grid either.

## II. PRELIMINARIES

This section gives the model of the smart grid operation and the state estimation with and without FDI attacks.

### A. Smart Grid Description

The dynamics and measurement equations of the smart grid can be described by the following state space equations:

$$\begin{aligned}\hat{X}[k+1] &= g(\hat{X}[k], \hat{U}[k]) \\ \hat{Z}[k] &= h(\hat{X}[k]) + v[k]\end{aligned}\quad (1)$$

where  $\hat{X}[k] = [\hat{x}_1[k] \ \hat{x}_2[k] \ \cdots \ \hat{x}_n[k]]^T \in \mathbb{R}^n$  is the vector of states at the  $k$ th sampling instant,  $\hat{x}_i[k]$  is the state of the  $i$ th node in the grid,  $\hat{U}[k] \in \mathbb{R}^n$  is the input vector at the  $k$ th sampling instant,  $\hat{Z}[k] = [\hat{z}_1[k] \ \hat{z}_2[k] \ \cdots \ \hat{z}_m[k]]^T \in \mathbb{R}^m$ ,  $m > n$  is the measurement vector at the  $k$ th sampling instant,  $\hat{z}_i[k]$  is the measurement of the  $i$ th meter,  $v[k] = [v_1[k] \ v_2[k] \ \cdots \ v_m[k]]^T \sim N_m(0, R)$  is the vector of measurement noises, and  $R \in \mathbb{R}^{m \times m}$  is positive definite.

In the literature, since meters are physically isolated [24], the noises  $v_1, v_2, \dots, v_m$  are assumed to be independent, i.e.,  $R = \text{diag}(\sigma_1^2, \sigma_2^2, \dots, \sigma_m^2)$ ,  $v_i \sim N(0, \sigma_i^2)$ ,  $i = 1, 2, \dots, m$ .

Similar to the one in [25], around the stable operating point  $(X_d, U_d)$ , which satisfies  $X_d = g(X_d, U_d)$ , the system model can be linearized as follows: denote  $X[k] = \hat{X}[k] - X_d = [x_1[k] \ x_2[k] \ \cdots \ x_n[k]]^T \in \mathbb{R}^n$ ,  $U[k] = \hat{U}[k] - U_d$ , and  $Z[k] = \hat{Z}[k] - HX_d = [z_1[k] \ z_2[k] \ \cdots \ z_m[k]]^T \in \mathbb{R}^m$ , then the power system defined by (1) can be simplified as

$$\begin{aligned}X[k+1] &= GX[k] + BU[k] \\ Z[k] &= HX[k] + v[k]\end{aligned}\quad (2)$$

where  $G = \frac{\partial g}{\partial X} \big|_{\substack{x=X_d \\ u=U_d}}$ ,  $B = \frac{\partial g}{\partial U} \big|_{\substack{x=X_d \\ u=U_d}}$ , and  $H = \frac{\partial h}{\partial X} \big|_{\substack{x=X_d \\ u=U_d}}$ .

Since it is difficult to directly measure the states  $X[k]$  during the power grid operation, the control center uses the collected measurements  $Z[k]$  to estimate the states of the smart grid. Denote  $\hat{X}[k]$  as the state estimation at the  $k$ th sampling instant, and  $r[k]$  defined below is the residual between the real state value and its estimation

$$r[k] = Z[k] - H\hat{X}[k]. \quad (3)$$

To minimize the following objective function:

$$\begin{aligned}J[k] &= (Z[k] - H\hat{X}[k])^T R^{-1} (Z[k] - H\hat{X}[k]) \\ &= [\hat{X}[k] - (H^T R^{-1} H)^{-1} H^T R^{-1} Z[k]]^T H^T R^{-1} \\ &\quad H [\hat{X}[k] - (H^T R^{-1} H)^{-1} H^T R^{-1} Z[k]] \\ &\quad + Z[k]^T [I - R^{-1} H (H^T R^{-1} H)^{-1} H^T R^{-1}] Z[k]\end{aligned}\quad (4)$$

the weighted least-square estimation  $\hat{X}[k]$  can be obtained as

$$\hat{X}[k] = (H^T R^{-1} H)^{-1} H^T R^{-1} Z[k]. \quad (5)$$

Applying the state estimation (5) into the measurement model (3), the corresponding residual can be obtained as

$$\begin{aligned}r[k] &= Z[k] - H\hat{X}[k] \\ &= (I - H(H^T R^{-1} H)^{-1} H^T R^{-1}) v[k].\end{aligned}\quad (6)$$

During the stable operation of the smart grid, the control objective is to keep the grid's state at the stable operating point

( $X_d, U_d$ ), i.e.,  $X[k] = 0$ . To this end, the linear feedback control can be employed [25]. Because the controller can only use the state estimation, the output feedback-based control law is designed as follows:

$$\begin{aligned} U[k] &= K\hat{X}[k] = K(H^T R^{-1} H)^{-1} H^T R^{-1} Z[k] \\ &= KX[k] + K(H^T R^{-1} H)^{-1} H^T R^{-1} v[k]. \end{aligned} \quad (7)$$

Then, substituting the control law (7) and the estimation (5) into (2) leads to the following closed-loop system:

$$\begin{aligned} X[k+1] &= (G+BK)X[k] + BK(H^T R^{-1} H)^{-1} H^T R^{-1} v[k] \\ Z[k] &= HX[k] + v[k]. \end{aligned} \quad (8)$$

### B. FDI Attack Description

When the attacker launches an FDI attack, some measured data are tampered with the mix of false data. The modified measurements are shown as follows:

$$Z_a[k] = Z[k] + A[k] = HX[k] + v[k] + A[k] \quad (9)$$

where  $Z_a[k]$  is the measurement vector after tampering at the  $k$ th sampling instant, and  $A[k] = [A_1[k] \ A_2[k] \ \cdots \ A_m[k]]^T \in \mathbb{R}^m$  is the malicious data added to the original measurements. In this article, both the direction and the magnitude of the FDI attacks are considered. That is:  $D[k]T[k] = A[k]$  where  $D[k] = A[k]/\|A[k]\|_2 = [D_1[k] \ D_2[k] \ \cdots \ D_m[k]]^T \in \mathbb{R}^m$  is the attack direction vector and  $T[k] \geq 0$  is the attack magnitude at  $k$ th instant.

Replacing the original measurements  $Z[k]$  with measurements after being attacked  $Z_a[k]$ , the estimation of the grid state and the corresponding residual at this time are

$$\hat{X}_a[k] = (H^T R^{-1} H)^{-1} H^T R^{-1} (Z[k] + A[k]) \quad (10)$$

$$\begin{aligned} r[k] &= Z_a[k] - H\hat{X}_a[k] \\ &= (I - H(H^T R^{-1} H)^{-1} H^T R^{-1})v[k] \\ &\quad + (I - H(H^T R^{-1} H)^{-1} H^T R^{-1})A[k] \end{aligned} \quad (11)$$

where  $\hat{X}_a$  is the estimation after being attacked.

Applying (9) and (10) into the system (8), the dynamic behavior of the attacked system is described as follows:

$$\begin{aligned} X[k+1] &= GX[k] + BK(H^T R^{-1} H)^{-1} H^T R^{-1} Z_a[k] \\ &= (G+BK)X[k] + BK(H^T R^{-1} H)^{-1} H^T R^{-1} v[k] \\ &\quad + BK(H^T R^{-1} H)^{-1} H^T R^{-1} A[k] \\ Z_a[k] &= HX[k] + v[k] + A[k]. \end{aligned} \quad (12)$$

The following sections introduce the traditional residual detection method and the Kalman-filter-based detection method against FDI attacks, and study how to design stealth attacks to bypass these two detection methods.

## III. TRADITIONAL RESIDUAL DETECTION METHOD AND CORRESPONDING ATTACK STRATEGY

This section first introduces the traditional residual detection method, then indicates its detection range and gives an attack

strategy to avoid its detection without the precise configuration information of the smart grid.

### A. Problem Formulation

When the attacker launches an FDI attack, according to (6) and (11), the residual of estimation may increase. The traditional detection method is to monitor that residual in real time, and set a prespecified threshold  $\tau$ . If the norm of the residual exceeds the threshold i.e.,  $\|r[k]\| > \tau$ , then it is believed that the data have been maliciously modified or a fault has occurred in the system. This article considers the Euclidean norm for analysis and discussion

$$\|r[k]\|_2 = \|(I - H(H^T R^{-1} H)^{-1} H^T R^{-1})(v[k] + A[k])\|_2. \quad (13)$$

However, due to the existence of noise, the threshold  $\tau$  cannot be set too low; otherwise, alarms may be triggered frequently, affecting the normal operation. It is well known that the probability that a white (Gaussian) noise is higher than any value is always not zero. Then, the residual may still exceed that threshold, regardless of how high the threshold is set.

Therefore, the significance level  $\alpha$  should be set to allow the residual norm exceeding the threshold. That is, the tolerance domain for FDI attacks satisfies the following condition:

$$P(\|r[k]\|_2 > \tau) < \alpha. \quad (14)$$

### B. Defects of the Residual Detection

It should be noted that if the attacker knows all (see [24]) or partial (see [11]) structure information of the smart grid, and chooses an appropriate attack direction to satisfy the condition  $D[k] = Hc/\|Hc\|_2$ , for any  $c \in \mathbb{R}^n$ , then residual defined by (11) at this time is

$$\begin{aligned} r[k] &= (I - H(H^T R^{-1} H)^{-1} H^T R^{-1})v[k] \\ &\quad + (I - H(H^T R^{-1} H)^{-1} H^T R^{-1})HcT[k] \\ &= (I - H(H^T R^{-1} H)^{-1} H^T R^{-1})v[k] + HcT[k] - HcT[k] \\ &= (I - H(H^T R^{-1} H)^{-1} H^T R^{-1})v[k] \end{aligned}$$

which is the same as the residual without attacks (6). In this case, no matter how strong the attack is, it can pass the residual detection. This attack strategy needs to adjust the attack vector  $A[k]$  into an appropriate direction. In the actual operation, the attacker carries out the attacks by hacking the distributed meters and modifying their measurements. The following subsection gives the fact that even if the attacker can only choose a fixed and adverse attack direction, it can still avoid the detection by continuously injecting a small amount of false data.

### C. Attack Against the Residual Detection

In this subsection, it is assumed that the attacker can only change the attack magnitude, and cannot change the attack direction, i.e.,  $D[i] = D = [D_1 \ D_2 \ \cdots \ D_m]^T$ ,  $A[i] = DT[i]$ . Denote  $\|(I - H(H^T R^{-1} H)^{-1} H^T R^{-1})\|_2 \triangleq \xi$ ,  $\rho_i = |D_i/\sigma_i|$ ,  $\sigma_{\max} = \max_{i=1,2,\dots,m}\{\sigma_i\}$ , and  $\rho_{\max} = \max_{i=1,2,\dots,m}\{\rho_i\}$ .

**Theorem 1:** When the magnitude of a single FDI attack  $T$  satisfies the following conditions, i.e.,  $A[i] = DT$ , for any  $i$ , it can bypass the residual detection defined by (14):

$$T^2 < \frac{2\xi^2\sigma_{\max}^2}{m\rho_{\max}^2(\tau^2 - \xi^2\sigma_{\max}^2)} \left[ \frac{\tau^2}{2\xi^2\sigma_{\max}^2} + \ln \alpha + \frac{1}{2} \ln \frac{\pi}{2} - \ln \left( 4 + \frac{\tau}{\xi\sigma_{\max}} \left( \frac{64}{(m-1)\pi} \right)^{\frac{m-1}{2}} \right) \right]. \quad (15)$$

**Proof:** See the proof of Theorem 1 in Appendix B. ■

Although this is a very conservative strategy, at least, the conclusion can be given that low-intensity attacks cannot be detected. Furthermore, since each test is independent, the same strategy can be adopted each time. So, the attacker can continuously launch an “imperceptible” attack and inject a small amount of false data to continuously harm the smart grid.

#### IV. KALMAN-FILTER-BASED DETECTION METHOD AND CORRESPONDING ATTACK STRATEGY

The defect of the residual detection lies in the fact that the test statistics for attack detection completely rely on the measured data that may be attacked, hence, well-designed false data can bypass the detection. If the control center can predict the operating states and compare them to measurements under attacks, regardless of how the false data are constructed, they can be found.

The Kalman filter is an efficient optimal recursive data processing algorithm that can obtain the effective and reliable prediction of the future state through the past measurements [26]. It is suitable for detecting false data attacks.

This section first introduces a Kalman-filter-based FDI attack detection method, and then, gives the analysis of its performance and weakness in the presence of attacks. Finally, an infiltrating attack strategy is proposed to bypass the detection and sabotage the grid.

##### A. Kalman-Filter-Based Attack Detector

Denote  $\hat{X}[t_1|t_2]$  as the state estimation at time  $t_1$  by using measurements up to time  $t_2$ , and let  $P[t_1|t_2]$  be the covariance of the estimation  $\hat{X}[t_1|t_2]$ .

**Prediction:** At time  $k$ , according to (8), the priori estimation at time  $k+1$  and its corresponding covariance are

$$\begin{aligned} \hat{X}[k+1|k] &= (G+BK)\hat{X}[k|k] \\ &= (G+BK)(\hat{X}[k|k] - W[k]v[k]) + (G+BK)W[k]v[k] \end{aligned} \quad (16)$$

$$\begin{aligned} P[k+1|k] &= (G+BK)(P[k|k] - W[k]RW[k]^T)(G+BK)^T \\ &\quad + [BK(H^TR^{-1}H)^{-1}H^TR^{-1} + (G+BK)W[k]]R \\ &\quad \times [BK(H^TR^{-1}H)^{-1}H^TR^{-1} + (G+BK)W[k]]^T \end{aligned} \quad (17)$$

where  $W[k] \in \mathbb{R}^{n \times m}$  is the Kalman gain at time  $k$ .

**Remark 1:** Notice that  $X[k]$  and  $(\hat{X}[k|k] - W[k]v[k])$  are uncorrelated with  $v[k]$ , respectively [see (22)]. This means that the process noise and the measurement noise are correlated, therefore, this Kalman filter used in this article is slightly different from the classic Kalman filter.

**Update:** At time  $k+1$ , notice that  $v[k+1]$  is uncorrelated with the combination of  $v[1], v[2], \dots, v[k]$ . The posteriori estimation and its covariance are

$$\begin{aligned} \hat{X}[k+1|k+1] &= \hat{X}[k+1|k] + W[k+1](Z[k+1] - H\hat{X}[k+1|k]) \\ &= (I - W[k+1]H)\hat{X}[k+1|k] + W[k+1](HX[k+1] + v[k+1]) \end{aligned} \quad (18)$$

$$\begin{aligned} P[k+1|k+1] &= (I - W[k+1]H)P[k+1|k](I - W[k+1]H)^T \\ &\quad + W[k+1]RK^T[k+1]. \end{aligned} \quad (19)$$

To minimize  $P[k+1|k+1]$ ,  $W[k+1]$  should be designed as

$$W[k+1] = P[k+1|k]H^T(H^TP[k+1|k]H^T + R)^{-1}.$$

Then, the Kalman filter of (8) is described as follows:

$$\begin{aligned} \hat{X}[k+1|k] &= (G+BK)\hat{X}[k|k] \\ P[k+1|k] &= (G+BK)P[k|k](G+BK)^T \\ &\quad + BK(H^TR^{-1}H)^{-1}K^TB^T \\ &\quad + BK(H^TR^{-1}H)^{-1}H^TW[k]^T(G+BK)^T \\ &\quad + (G+BK)W[k]H(H^TR^{-1}H)^{-1}K^TB^T \\ \hat{X}[k+1|k+1] &= (I - W[k+1]H)\hat{X}[k+1|k] \\ &\quad + W[k+1]Z[k+1] \\ P[k+1|k+1] &= P[k+1|k] - W[k+1]HP^T[k+1|k] \\ W[k+1] &= P[k+1|k]H^T(H^TP[k+1|k]H^T + R)^{-1}. \end{aligned} \quad (20)$$

The residual given by the Kalman filter (20) is defined as the difference between the measurement and the prediction

$$\mathbf{r}[k] = Z[k] - H\hat{X}[k|k-1]. \quad (21)$$

The healthy grid operates normally and provides stable power supplies. It is assumed that the Kalman filter can give the accurate estimate before the system is attacked, i.e.,  $(X[t] - \hat{X}[t|t]) \sim N_m(0, P[t|t]), t < k+1$

$$\begin{aligned} \hat{X}[k|k] &= (I - W[k]H)\hat{X}[k|k-1] + W[k]Z[k] \\ &= (I - W[k]H)\hat{X}[k|k-1] + W[k]HX[k] + W[k]v[k]. \end{aligned} \quad (22)$$

It is noted that  $X[k]$  is uncorrelated with  $v[k]$ , and  $(\hat{X}[k|k] - W[k]v[k])$  is uncorrelated with  $v[k]$ . Hence,  $(X[t] - \hat{X}[t|t] + W[k]v[k]) \sim N_m(0, P[t|t] - W[k]RW[k]^T[k])$ .

If the grid suffers from an FDI attack at time  $k$  and the tampered data are the same as the one defined in (9), then the

residual becomes

$$\tau[k] = Z_a[k] - H\hat{X}[k|k-1]. \quad (23)$$

Through real-time monitoring the Euclidean norm of this residual, the presence of (some) bad measurements can be detected, if this residual is so large that its norm exceeds the threshold, i.e.,  $\|\tau[k]\|_2 > \tau$ . Similarly with (14), due to the existence of noises, the threshold still needs to be set to limit false alarms. Then, the tolerance domain for FDI attacks satisfies the following condition:

$$P(\|\tau[k]\|_2 > \tau) < \alpha. \quad (24)$$

From (23), it can be seen that regardless of how the attack direction  $D$  is designed, the attack magnitude is always reflected in the residual. It means that this Kalman-filter-based detection method can overcome the limitation of the traditional residual detection defined by (11), avoiding the harm caused by the *stealth bad data injection* [27].

However, it is noted that the effectiveness of the Kalman-filter-based detection method is entirely based on the premise that historical data are trustable. The later parts give a special way to infiltrate the smart grid with the Kalman-filter-based detector.

### B. Single Attack Case: The Preattack Strategy

Since the Kalman filter cannot fundamentally separate attacks from noises, small attacks still work. Based on this observation, this subsection discusses the possibility of a single attack by-passing the detection.

Assume the first attack occurs at time  $s$ , i.e.,  $T[j] = 0$ ,  $j < s$ .

**Theorem 2:** For a smart grid under stable operation, the first attack  $A[s]$  can avoid being detected by the Kalman filter as long as its magnitude is sufficiently small to satisfy the following condition:

$$\|A[s]\|_2^2 < \frac{2\|\Gamma\|_2^2}{md_{\min}^2(\tau^2 - \|\Gamma\|_2^2)} \left[ \frac{\tau^2}{2\|\Gamma\|_2^2} + \ln \alpha + \frac{1}{2} \ln \frac{\pi}{2} - \ln \left( 4 + \frac{\tau}{\|\Gamma\|_2} \left( \frac{64}{(m-1)\pi} \right)^{\frac{m-1}{2}} \right) \right] \quad (25)$$

where  $\Gamma\Gamma^T = R + [HBK(H^TR^{-1}H)^{-1}H^TR^{-1} - H(G+BK)W[s]]R[HBK(H^TR^{-1}H)^{-1}H^TR^{-1} - H(G+BK)W[s]]^T + H(G+BK)(P[s|s] - W[s]RW^T[s])(G+BK)^TH^T$ , and  $d_{\min}$  is the smallest absolute value of the elements of  $\Gamma^{-1}A[s]/\|A[s]\|_2$ .

**Proof:** See the proof of Theorem 2 in Appendix C. ■

**Remark 2:** If the attacker can choose  $D[s] = Hc/\|Hc\|_2$ , for any  $c \in \mathbb{R}^n$ , as the attack direction, the preattack strategy can certainly bypass the traditional residual detection as mentioned in Section III-B. Even if this condition cannot be satisfied, it only needs to let the attack magnitude satisfy both constraints given by Theorems 1 and 2, and then, the preattack strategy can bypass the traditional residual detection.

The false data injected at a single small attack have insufficient power. Hence, relentless attacks are required to cause considerable damage to the grid.

When the system with a Kalman filter (20) is injected with false data, those false data may continue to implicitly appear in subsequent residuals and affect the detection tests. Hence, the attacker can take advantage of the impact of previous attacks when developing the attack strategy.

### C. Multiple Attacks Case: The Postattack Strategy

Since the indicator of the Kalman filter relates to the past states of the grid, the tolerances for multiple attacks are time varying. First, the operating state equations of the smart grid with the Kalman filter before and after attacks are given.

Before the attacks, there is enough time for the grid and its filter to reach the steady state, and the covariance matrices of priori and posteriori estimations converge as follows:

$$\begin{cases} |t| = P[t+1|t+1] \triangleq P, t \rightarrow \infty \\ P[t+1|t] = P[t+2|t+1] \triangleq \tilde{P}, t \rightarrow \infty \\ \lim_{t \rightarrow \infty} W[t] \triangleq W_{\infty}. \end{cases} \quad (26)$$

Then, applying the steady-state covariance and the corresponding Kalman gain (26) into prediction process (16) and update process (18) leads to the following conditions:

$$\begin{cases} \tilde{P} = (G+BK)(P-W_{\infty}RW_{\infty}^T)(G+BK)^T \\ \quad + [BK(H^TR^{-1}H)^{-1}H^TR^{-1} + (G+BK)W_{\infty}]R \\ \quad \times [BK(H^TR^{-1}H)^{-1}H^TR^{-1} + (G+BK)W_{\infty}]^T \\ P = \tilde{P} - \tilde{P}H^T(H\tilde{P}H^T + R)^{-1}H\tilde{P}^T \\ W_{\infty} = \tilde{P}H^T(H\tilde{P}H^T + R)^{-1}. \end{cases} \quad (27)$$

Hence, the control center actually uses a constant Kalman gain for estimation, and the attacker can also use this gain. Then, the system (8) with a Kalman filter (20) can be simplified as follows:

$$\begin{aligned} X[k+1] &= (G+BK)X[k] \\ &\quad + BK(H^TR^{-1}H)^{-1}H^TR^{-1}v[k] \\ Z[k] &= HX[k] + v[k] \\ \hat{X}[k+1|k] &= (G+BK)\hat{X}[k|k] \\ \hat{X}[k+1|k+1] &= (I-W_{\infty}H)\hat{X}[k+1|k] + W_{\infty}Z[k+1] \\ &= (I-W_{\infty}H)(G+BK)\hat{X}[k|k] \\ &\quad + W_{\infty}(HX[k+1] + v[k+1]). \end{aligned} \quad (28)$$

After the attacker launches the attack, at any moment  $l \geq s$ , replacing  $Z[k]$  with  $Z_a[k]$  leads to the following system equation:

$$\begin{aligned} X[l+1] &= (G+BK)X[l] \\ &\quad + BK(H^TR^{-1}H)^{-1}H^TR^{-1}v[l] \\ &\quad + BK(H^TR^{-1}H)^{-1}H^TR^{-1}A[l] \\ Z_a[l] &= HX[l] + v[l] + A[l] \\ \hat{X}[l+1|l] &= (G+BK)\hat{X}[l|l] \\ \hat{X}[l+1|l+1] &= (I-W_{\infty}H)(G+BK)\hat{X}[l|l] \\ &\quad + W_{\infty}(HX[l+1] + v[l+1] + A[l+1]). \end{aligned} \quad (29)$$

**Theorem 3:** After the first attack, if the attacker adopts the following postattack strategy, it can pass the detection using the Kalman filter defined by (29):

$$\begin{aligned}
 A[l] = & [H(G+BK)W_\infty - HBK(H^TR^{-1}H)^{-1}H^TR^{-1}]A[l-1] \\
 & - H(G+BK) \left\{ \sum_{k=0}^{l-s-2} (G+BK)^{l-s-k-2} BK \right. \\
 & \times (H^TR^{-1}H)^{-1}H^TR^{-1}A[s+k] \\
 & + \sum_{k=0}^{l-s-2} \sum_{i=k}^{l-s-2} [(I-W_\infty H)(G+BK)]^{l-s-i-2} W_\infty H \\
 & \times (G+BK)^{i-k} BK(H^TR^{-1}H)^{-1}H^TR^{-1}A[s+k] \\
 & \left. + \sum_{k=0}^{l-s-2} [(I-W_\infty H)(G+BK)]^{l-s-k-1} W_\infty A[s+k] \right\} \quad (30)
 \end{aligned}$$

where  $s < l$  is the first attack occurring time, and  $A[s]$  can be any sufficient small vector following the preattack strategy in Theorem 2.

**Proof:** See the proof of Theorem 3 in Appendix D. ■

**Theorem 4:** The postattack strategy defined by (30) in Theorem 3 can bypass the traditional residual detection completely.

**Proof:** See the proof of Theorem 4 in Appendix E. ■

After the smart grid suffers from the FDI attacks, there is a slight difference between the amount of false data contained in the estimation and that in the measurement, and this difference gradually becomes significant over time. However, on the other hand, the attacker can take advantage of this and keep generating false data in order to make the previous false data look real.

## V. NUMERICAL SIMULATION

This section illustrates the defects of two detection methods in concern (the traditional residual detection and the Kalman-filter-based detection).

Consider a 4-bus model of the distribution test feeders proposed by IEEE distribution test feeder working group [28], which is shown in Fig. 1. The admittance matrix  $Y$  of this power network is given in (31), shown at the bottom of the page.

Each distributed energy resource is connected into the smart grid at the point of common coupling, and it needs to control the voltages ( $V = [V_1 \ V_2 \ V_3 \ V_4]^T$ ) of those points of

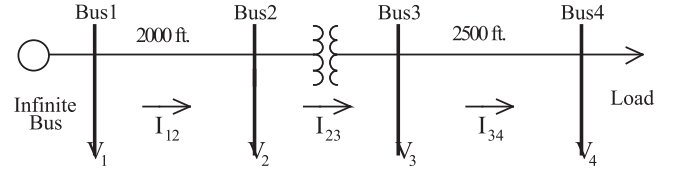


Fig. 1. Illustration of the IEEE 4-bus test feeder model.

common coupling to keep them at the reference values  $V_d = [12.470 \ 7.123 \ 2.258 \ 1.987]^T$  (kV).

To achieve that, the system state is defined as the deviation of the voltages from the reference values, i.e.,  $X = V - V_d$ . The sampling period is set to be 10 ms. From [25], the dynamics of the system can be written by

$$\begin{aligned}
 X[k+1] &= GX[k] + BU[k] \\
 U[k] &= -KX[k] \quad (32)
 \end{aligned}$$

where the state transition matrix  $G$ , input matrix  $B$ , and feedback control gain  $K$  are shown as follows:

$$\begin{aligned}
 G &= \begin{bmatrix} 2.759 & 1.768 & 5.110 & 10.360 \\ -3.500 & 1 & 0 & 0 \\ -5.442 & -4.748 & -3.088 & -8.288 \\ -1.197 & -5.546 & -9.688 & -9.775 \end{bmatrix} \\
 B &= \begin{bmatrix} 0.008 & 3.342 & 5.251 & -10.360 \\ -3.500 & 0 & 0 & 0 \\ -0.693 & -0.661 & -4.201 & -8.288 \\ -4.349 & -4.142 & -1.087 & -10.775 \end{bmatrix} \\
 K &= \begin{bmatrix} 1.0000 & -1.4286 & -0.0000 & -0.0000 \\ -0.8052 & 1.5995 & 2.4960 & 0.7234 \\ 1.5276 & 0.2175 & -0.6126 & 1.6858 \\ -0.1371 & 0.4545 & 0.0014 & 0.0878 \end{bmatrix}.
 \end{aligned}$$

The measurements are based on the sensors in branch and bus power flows, which can be derived by

$$Z[k] = HX[k] + v[k]$$

$$Y(s) = \begin{bmatrix} \frac{1}{0.1750+0.0005s} & -\frac{1}{0.1750+0.0005s} & 0 & 0 \\ -\frac{1}{0.1750+0.0005s} & \frac{1}{0.1750+0.0005s} + \frac{1}{0.1667+0.0004s} & -\frac{1}{0.1667+0.0004s} & 0 \\ 0 & -\frac{1}{0.1667+0.0004s} & \frac{1}{0.1667+0.0004s} + \frac{1}{0.2187+0.0006s} & -\frac{1}{0.2187+0.0006s} \\ 0 & 0 & -\frac{1}{0.2187+0.0006s} & \frac{1}{0.2187+0.0006s} + \frac{1}{12.3413+0.0148s} \end{bmatrix} \quad (31)$$

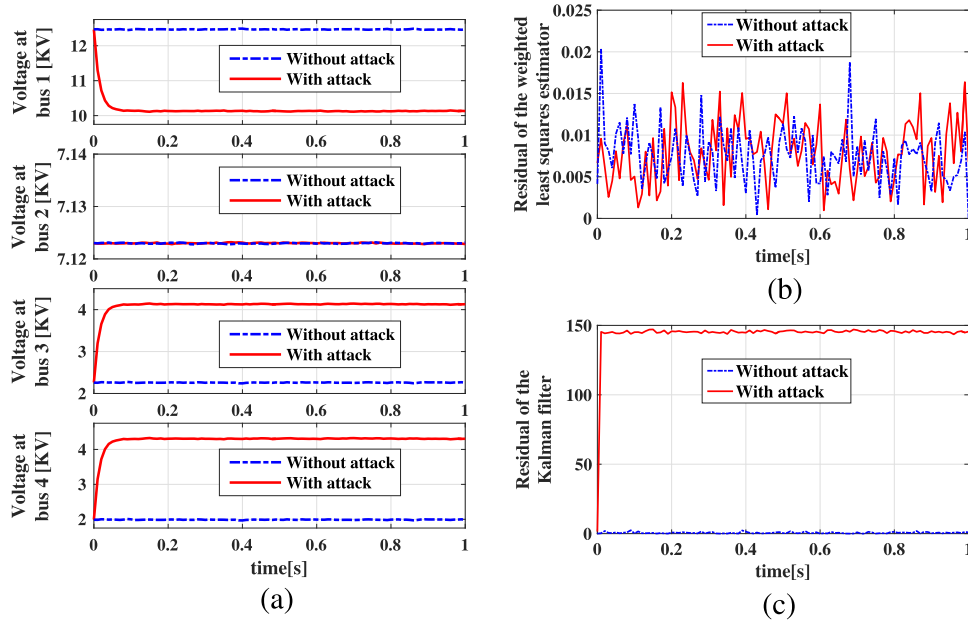


Fig. 2. Stealth false data injection attack bypasses the traditional residual detection while being detected by the Kalman-filter-based detection. (a) Voltage on each bus. (b) There is no significant difference in residuals given by the weighted least-squares estimator with and without attack. (c) Residual given by the Kalman filter with attack is significantly larger than that without attack.

where  $Z = [P_1 \ P_2 \ P_3 \ P_4 \ P_{12} \ P_{23} \ P_{34}]^T$  is the measurement vector consisting of power injections,  $v \sim N_7(0, \text{diag}(1.7050, 5.2910, 2.2502, 6.2500, 2.0610, 4.1305, 6.2500))$  is the *i.i.d* noise sequence, and the measurement matrix  $H$  is

$$H = \begin{bmatrix} 38.5002 & 67.4010 & 0 & 0 \\ -38.5002 & -80.8445 & -42.4082 & 0 \\ 0 & 13.4435 & 46.9084 & 5.1140 \\ 0 & 0 & -4.5002 & -5.1140 \\ 104.0129 & -67.4010 & 0 & 0 \\ 0 & 98.9019 & 42.4082 & 0 \\ 0 & 0 & 16.1489 & -5.1140 \end{bmatrix}.$$

#### A. Kalman-Filter-Based Detection Against the Stealth Attack

As the most common detection method against false data injection attacks, the traditional residual detection method can find many attacks, except for those carefully constructed stealth FDI. To launch a stealth attack, the attack direction is designed as  $D = [0 \ 0 \ 1 \ -1 \ 0 \ 0 \ -1]/\sqrt{3}$ , and attack magnitude  $T$  is set to 1. That is

$$A[i] = \begin{bmatrix} 0 & 0 & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & 0 & 0 & -\frac{1}{\sqrt{3}} \end{bmatrix}, \text{ for any } i. \quad (33)$$

Both the traditional residual detection and the Kalman-filter-based detection are adopted. Fig. 2 shows the evolutions of the states at normal operation and the states under attacks.

There is no significant difference between the residuals with and without attacks in Fig. 2(b), which means that the stealth attack (33) can bypass the traditional residual detection. Fig. 2(c) shows the results of the Kalman-filter-based detection. It can be seen that the residual between the measurement and the estimation significantly soars after the attack. Once the Kalman filter is adopted, those stealth FDI attacks can be found immediately.

#### B. Specific Attack for Kalman-Filter-Based Detection

This subsection verifies the correctness of Theorems 2–4, namely, whether the relentless false data injection attacks can bypass the Kalman-filter-based detection and the traditional residual detection.

When the attacker launches a relentless false data injection attack proposed in this article, the preattack strategy is designed as  $A[1] = [1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1] \times 10^{-99}$ , which would not be caught certainly. Then, the subsequent attack vector design follows the requirement defined by (30) in Theorem 3. Fig. 3 shows the evolutions of the states of the power system with the Kalman-filter-based detection and the traditional residual detection. From Fig. 3(d), the attack magnitude increases rapidly. While from Fig. 3(b) and 3(c), the residual is quite normal and has almost no difference from the case without attack. However, this attack can eventually cause the bus voltage to significantly jump from the reference state. This can demonstrate that the attack sequence defined by (30) successfully cheats the Kalman-filter-based detector.

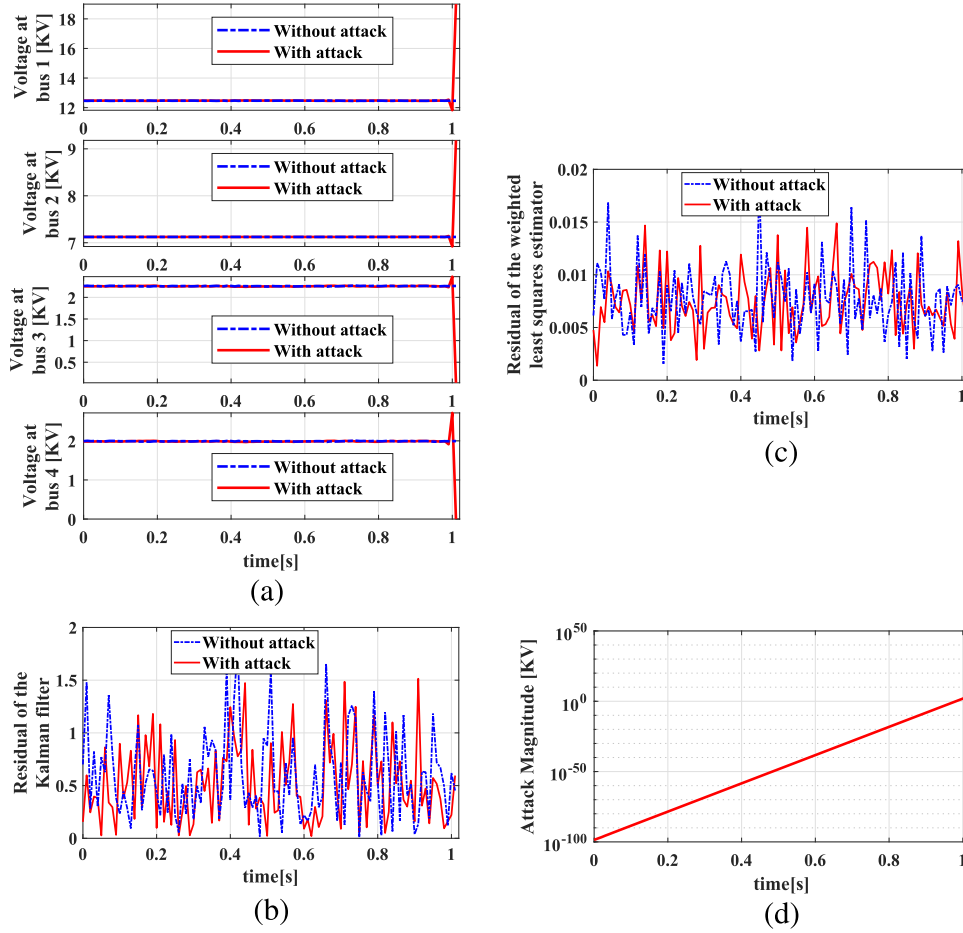


Fig. 3. Attack strategy proposed in this article bypasses the Kalman-filter-based detection. (a) Voltage on each bus. (b) There is no significant difference in residuals given by the Kalman filter with and without attack. (c) There is no significant difference in residuals given by the weighted least-squares estimator with and without attack. (d) Attack magnitude gradually increases.

## VI. CONCLUSION

This article analyzes the defects of the traditional residual detection method, and indicates the effect of the Kalman filter in the detection of stealth attacks. By predicting the real-time states of the smart grid, the Kalman filter can make up for those defects to some extent. However, the Kalman-filter-based detection method cannot solve the problem completely. This article then investigates the defects of the Kalman-filter-based detection method in detail, and proposes a specific attack strategy. Through theoretical studies, the carefully constructed attack is proved to be able to deceive the Kalman filter: estimations and residuals given by the Kalman filter behave normally as if nothing happens while the attack magnitude is gradually increasing, which finally causes the damage of the smart grid.

## APPENDIX A

**Lemma 1:** The probability of a normal random variable  $X^* \sim N(0, 1)$  being greater than a given value  $\sqrt{2K \ln \ln n}$  satisfies

$$P(X^* \geq \sqrt{2K \ln \ln n}) < 4\sqrt{\frac{K}{\pi}} (\ln n)^{-K}$$

where  $n > e = 2.718\dots$ ,  $K > 0$

$$\begin{aligned} \text{Proof: } P(X^* \geq \sqrt{2K \ln \ln n}) &= \frac{1}{\sqrt{2\pi}} \int_{x \geq \sqrt{2K \ln \ln n}} e^{-\frac{x^2}{2}} dx \\ &< \frac{1}{\sqrt{2\pi}} \sum_{r \geq n} [\sqrt{2K \ln \ln(r+1)} - \sqrt{2K \ln \ln r}] e^{-K \ln \ln r} \\ &< \sqrt{\frac{K}{\pi}} \sum_{r \geq n} \frac{\ln \ln(r+1) - \ln \ln r}{\sqrt{\ln \ln r}} (\ln r)^{-K} \\ &< \sqrt{\frac{K}{\pi}} (\ln n)^{-K} \sum_{r \geq n} \frac{\ln[\frac{1}{r \ln r} + 1]}{\sqrt{\ln \ln r}} < 4\sqrt{\frac{K}{\pi}} (\ln n)^{-K}. \end{aligned}$$

**Lemma 2:** For any  $x > 0$ , the following two inequalities hold:

$$\begin{aligned} e^x + e^{-x} &< 2e^{x^2} \\ e^x - e^{-x} &< 2xe^{x^2}. \end{aligned}$$

## APPENDIX B

### PROOF OF THEOREM 1

**Proof:** With a given attack direction  $D$ , the norm of the residual can be derived as follows:

$$\begin{aligned} \|\mathbf{r}[k]\|_2 &= \|(I - H(H^T R^{-1} H)^{-1} H^T R^{-1})(v[k] + DT[k])\|_2 \\ &< \xi \|(v[k] + DT[k])\|_2. \end{aligned} \quad (34)$$

A sufficient condition to satisfy condition (14) is

$$P(\|(v[k] + DT[k])\|_2 > \frac{\tau}{\xi}) < \alpha. \quad (35)$$

Consider the probability of the Euclidean norm of a random vector  $(v + DT)$  being greater than a given value  $\gamma$ , where  $v \sim N_m(0, R)$ ,  $D \in R^m$ ,  $\|D\|_2 = 1$ ,  $T \in R$

$$\begin{aligned} P(\|(v + DT)\|_2 > \gamma) &= P\left(\sqrt{\sum_{i=1}^m (v_i + D_i T)^2} > \gamma\right) \\ &= \int \cdots \int \prod_{i=1}^m \frac{1}{\sqrt{2\pi}\sigma_i} \exp\left(-\frac{v_i^2}{2\sigma_i^2}\right) dv_i \\ &\quad \int \cdots \int_{\sum_{i=1}^m (\sigma_i \omega_i)^2 > \gamma^2} (2\pi)^{-\frac{m}{2}} \exp\left(-\frac{1}{2} \sum_{i=1}^m \left(\omega_i - \frac{D_i T}{\sigma_i}\right)^2\right) \prod_{i=1}^m d\omega_i \\ &< \int \cdots \int_{\sum_{i=1}^m \omega_i^2 > \frac{\gamma^2}{\max_j \sigma_j^2}} (2\pi)^{-\frac{m}{2}} \exp\left(-\frac{1}{2} \sum_{i=1}^m \left(\omega_i - \max_j \left|\frac{D_j}{\sigma_j}\right| T\right)^2\right) \prod_{i=1}^m d\omega_i. \end{aligned} \quad (36)$$

Find a rotation matrix  $T \in \mathbb{R}^{m \times m}$  whose first row is  $[\frac{1}{\sqrt{m}} \ \frac{1}{\sqrt{m}} \ \cdots \ \frac{1}{\sqrt{m}}]$  such that  $T[\omega_1 \ \omega_2 \ \cdots \ \omega_m]^T = [\varpi_1 \ \varpi_2 \ \cdots \ \varpi_m]^T$ , where  $\varpi_1 = \frac{1}{\sqrt{m}} \sum_{i=1}^m \omega_i$ ,  $\sum_{i=1}^m \omega_i^2 = \sum_{i=1}^m \varpi_i^2$ , and  $\prod_{i=1}^m d\omega_i = \prod_{i=1}^m d\varpi_i$ ,  $\varpi_i \sim N(0, 1)$ ,  $i = 1, 2, \dots, m$ . The rotation matrix  $T$  is not unique. Then, (36) can be transformed into the following integral:

$$\begin{aligned} P(\|(v + DT)\|_2 > \gamma) &< \int \cdots \int_{\sum_{i=1}^m \omega_i^2 > \frac{\gamma^2}{\max_j \sigma_j^2}} (2\pi)^{-\frac{m}{2}} \exp\left(-\frac{1}{2} \sum_{i=1}^m (\omega_i - \rho_{\max} T)^2\right) \prod_{i=1}^m d\omega_i \\ &= \int \cdots \int_{\sum_{i=1}^m \varpi_i^2 > \frac{\gamma^2}{\max_j \sigma_j^2}} (2\pi)^{-\frac{m}{2}} \exp\left(-\frac{1}{2} (\varpi_1 - \sqrt{m} \rho_{\max} T)^2\right) \\ &\quad \exp\left(-\frac{1}{2} \sum_{i=2}^m \varpi_i^2\right) \prod_{i=1}^m d\varpi_i \\ &< P\left(\varpi_1 > \frac{\gamma}{\sigma_{\max}} + \sqrt{m} \rho_{\max} T\right) + P\left(\varpi_1 > \frac{\gamma}{\sigma_{\max}} - \sqrt{m} \rho_{\max} T\right) \\ &\quad + \int_{\varpi_1 = -\frac{\gamma}{\sigma_{\max}}}^{\frac{\gamma}{\sigma_{\max}}} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{1}{2} (\varpi_1 - \sqrt{m} \rho_{\max} T)^2\right) d\varpi_1 \end{aligned}$$

$$\times \int \cdots \int_{\sum_{i=2}^m \varpi_i^2 > \frac{\gamma^2}{\sigma_{\max}^2} - \varpi_1^2} \prod_{i=2}^m \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{\varpi_i^2}{2}\right) d\varpi_i. \quad (37)$$

According to Lemma 1, it can be calculated that the probability  $P(\varpi_2 > \sqrt{2Kn}) < 4\sqrt{K}e^{-nK}/\sqrt{\pi}$ . Then, let  $K = 1/(m-1)$  and  $n = \gamma^2/2\sigma_{\max}^2 - \varpi_1^2/2$ , it can be obtained that

$$\begin{aligned} P\left(\varpi_2 > \frac{1}{\sqrt{m-1}} \sqrt{\frac{\gamma^2}{\sigma_{\max}^2} - \varpi_1^2}\right) &< 4\sqrt{\frac{1}{(m-1)\pi}} \exp\left(-\frac{1}{m-1} \left(\frac{\gamma^2}{2\sigma_{\max}^2} - \frac{\varpi_1^2}{2}\right)\right). \end{aligned} \quad (38)$$

And let  $K = 1/2$  and  $n = \frac{\gamma}{\sigma_{\max}} \pm \sqrt{m} \rho_{\max} T$ , it can be obtained that

$$\begin{aligned} P\left(\varpi_1 > \sqrt{2\frac{1}{2}} \left(\frac{\gamma}{\sigma_{\max}} \pm \sqrt{m} \rho_{\max} T\right)^2\right) &< 4\sqrt{\frac{1}{2\pi}} \exp\left(-\frac{1}{2} \left(\frac{\gamma}{\sigma_{\max}} \pm \sqrt{m} \rho_{\max} T\right)^2\right). \end{aligned} \quad (39)$$

Then, applying (38) and (39) into (37), we can have that

$$\begin{aligned} P\left(\sqrt{\sum_{i=1}^m (v_i + D_i T)^2} > \gamma\right) &< 4\sqrt{\frac{1}{2\pi}} \exp\left(-\frac{1}{2} \left(\frac{\gamma}{\sigma_{\max}} + \sqrt{m} \rho_{\max} T\right)^2\right) \\ &\quad + 4\sqrt{\frac{1}{2\pi}} \exp\left(-\frac{1}{2} \left(\frac{\gamma}{\sigma_{\max}} - \sqrt{m} \rho_{\max} T\right)^2\right) \\ &\quad + \left(8\sqrt{\frac{1}{(m-1)\pi}}\right)^{m-1} \exp\left(-\frac{\gamma^2}{2\sigma_{\max}^2} + \frac{\varpi_1^2}{2}\right) \\ &\quad \times \frac{1}{\sqrt{2\pi}} \int_{\varpi_1 = -\frac{\gamma}{\sigma_{\max}}}^{\frac{\gamma}{\sigma_{\max}}} \exp\left(-\frac{1}{2} \varpi_1^2 - \frac{1}{2} m \rho_{\max}^2 T^2\right. \\ &\quad \left.+ \sqrt{m} \rho_{\max} T \varpi_1\right) d\varpi_1 \\ &< \sqrt{\frac{8}{\pi}} \exp\left(-\frac{\gamma^2}{2\sigma_{\max}^2} - \frac{1}{2} m \rho_{\max}^2 T^2\right) \\ &\quad \times \left[\exp\left(\frac{\gamma \sqrt{m} \rho_{\max} T}{\sigma_{\max}}\right) + \exp\left(-\frac{\gamma \sqrt{m} \rho_{\max} T}{\sigma_{\max}}\right)\right] \\ &\quad + \frac{1}{\sqrt{2\pi m} \rho_{\max} T} \left(\frac{64}{(m-1)\pi}\right)^{\frac{m-1}{2}} \\ &\quad \times \exp\left(-\frac{\gamma^2}{2\sigma_{\max}^2} - \frac{1}{2} m \rho_{\max}^2 T^2\right) \\ &\quad \times \left[\exp\left(\frac{\gamma \sqrt{m} \rho_{\max} T}{\sigma_{\max}}\right) - \exp\left(-\frac{\gamma \sqrt{m} \rho_{\max} T}{\sigma_{\max}}\right)\right]. \end{aligned} \quad (40)$$

According to Lemma 2

$$\exp\left(\frac{\gamma\sqrt{m}\rho_{\max}T}{\sigma_{\max}}\right) + \exp\left(-\frac{\gamma\sqrt{m}\rho_{\max}T}{\sigma_{\max}}\right) < 2 \exp\left(\left[\frac{\gamma\sqrt{m}\rho_{\max}T}{\sigma_{\max}}\right]^2\right) \quad (41)$$

$$\exp\left(\frac{\gamma\sqrt{m}\rho_{\max}T}{\sigma_{\max}}\right) - \exp\left(-\frac{\gamma\sqrt{m}\rho_{\max}T}{\sigma_{\max}}\right) < 2 \frac{\gamma\sqrt{m}\rho_{\max}T}{\sigma_{\max}} \exp\left(\left[\frac{\gamma\sqrt{m}\rho_{\max}T}{\sigma_{\max}}\right]^2\right). \quad (42)$$

Furthermore, applying (41) and (42) into (40) leads to the following equation:

$$\begin{aligned} & P\left(\sqrt{\sum_{i=1}^m (v_i + D_i T)^2} > \gamma\right) \\ & < \sqrt{\frac{32}{\pi}} \exp\left(-\frac{\gamma^2}{2\sigma_{\max}^2} - \frac{1}{2}m\rho_{\max}^2 T^2 + \frac{m\gamma^2\rho_{\max}^2 T^2}{\sigma_{\max}^2}\right) \\ & \quad + \sqrt{\frac{2}{\pi}} \frac{\gamma}{\sigma_{\max}} \left(\frac{64}{(m-1)\pi}\right)^{\frac{m-1}{2}} \\ & \quad \times \exp\left(-\frac{\gamma^2}{2\sigma_{\max}^2} - \frac{1}{2}m\rho_{\max}^2 T^2 + \frac{m\gamma^2\rho_{\max}^2 T^2}{\sigma_{\max}^2}\right) \\ & = \left[\sqrt{\frac{32}{\pi}} + \sqrt{\frac{2}{\pi}} \frac{\gamma}{\sigma_{\max}} \left(\frac{64}{(m-1)\pi}\right)^{\frac{m-1}{2}}\right] \\ & \quad \times \exp\left(-\frac{\gamma^2}{2\sigma_{\max}^2} - \frac{1}{2}m\rho_{\max}^2 T^2 + \frac{m\gamma^2\rho_{\max}^2 T^2}{\sigma_{\max}^2}\right). \quad (43) \end{aligned}$$

According to (43), let

$$\begin{aligned} & P\left(\sqrt{\sum_{i=1}^m (v_i[k] + D_i T[k])^2} > \frac{\tau}{\xi}\right) \\ & < \left[\sqrt{\frac{32}{\pi}} + \sqrt{\frac{2}{\pi}} \frac{\tau}{\xi\sigma_{\max}} \left(\frac{64}{(m-1)\pi}\right)^{\frac{m-1}{2}}\right] \exp\left(-\frac{\tau^2}{2\xi^2\sigma_{\max}^2}\right) \\ & \quad \times \exp\left(\left[\frac{m\tau^2\rho_{\max}^2}{\xi^2\sigma_{\max}^2} - \frac{1}{2}m\rho_{\max}^2\right] T[k]^2\right) < \alpha \end{aligned}$$

then it can be obtained that

$$\begin{aligned} T[k]^2 & < \frac{2\xi^2\sigma_{\max}^2}{m\rho_{\max}^2(\tau^2 - \xi^2\sigma_{\max}^2)} \left[ \frac{\tau^2}{2\xi^2\sigma_{\max}^2} + \ln \alpha + \frac{1}{2} \ln \frac{\pi}{2} \right. \\ & \quad \left. - \ln \left( 4 + \frac{\tau}{\xi\sigma_{\max}} \left(\frac{64}{(m-1)\pi}\right)^{\frac{m-1}{2}} \right) \right]. \quad (44) \end{aligned}$$

Since each test is independent of each other, every attack can effectively bypass the detection as long as its magnitude satisfies condition (15).

## APPENDIX C PROOF OF THEOREM 2

Applying the Kalman filter (20) into (23), the norm of the residual can be derived by the following equation:

$$\begin{aligned} \|\mathbf{r}[s+1]\|_2 &= \|Z_a[s+1] - H\hat{X}[s+1|s]\|_2 \\ &= \|HX[s+1] + v[s+1] + A[s+1] - H(G+BK)\hat{X}[s|s]\|_2 \\ &= \|HBK(H^TR^{-1}H)^{-1}H^TR^{-1}v[s] + v[s+1] \\ & \quad + H(G+BK)(X[s] - \hat{X}[s|s] + W[s]v[s]) \\ & \quad - H(G+BK)W[s]v[s] + A[s+1]\|_2. \quad (45) \end{aligned}$$

Notice that  $(v[s+1] + (HBK(H^TR^{-1}H)^{-1}H^TR^{-1} - H(G+BK)W[s])v[s] + H(G+BK)(X[s] - \hat{X}[s|s] + W[s]v[s])) \sim N_m(0, \Gamma\Gamma^T)$ . Let  $w[i] \sim N_m(0, I)$ ,  $i = 1, 2, \dots$ , be a series of independent zero-mean random vectors following Gaussian distribution,  $\Gamma w[s+1] \sim N_m(0, \Gamma\Gamma^T)$ , and then, it can be obtained that

$$\|\mathbf{r}[s+1]\|_2 = \|\Gamma w[s+1] + A[s+1]\|_2. \quad (46)$$

Because  $R$  is a positive definite matrix and  $(P[s|s] - W[s]RW^T[s])$  is the covariance matrix of  $(X[t] - \hat{X}[t|t] + W[s]v[s])$ , which is positive semidefinite,  $\text{Rank}(\Gamma\Gamma^T) = \text{Rank}(\Gamma) = m$ . Therefore,  $\Gamma$  is invertible.

When the first attack occurs, to be not detected, it must satisfy the condition (24), i.e.,

$$\begin{aligned} \alpha &> P(\|\mathbf{r}[s]\|_2 > \tau) = P(\|\Gamma w[s] + A[s]\|_2 > \tau) \\ &> P(\|\Gamma\|_2 \cdot \|w[s] + \Gamma^{-1}A[s]\|_2 > \tau) \\ &= P\left(\|w[s] + \Gamma^{-1} \frac{A[s]}{\|A[s]\|_2} \|A[s]\|_2\|_2 > \frac{\tau}{\|\Gamma\|_2}\right). \quad (47) \end{aligned}$$

By applying Theorem 1, it can be calculated that

$$\begin{aligned} & P\left(\|w[s] + \Gamma^{-1} \frac{A[s]}{\|A[s]\|_2} \|A[s]\|_2\|_2 > \frac{\tau}{\|\Gamma\|_2}\right) \\ & < \left[\sqrt{\frac{32}{\pi}} + \sqrt{\frac{2}{\pi}} \frac{\tau}{\|\Gamma\|_2} \left(\frac{64}{(m-1)\pi}\right)^{\frac{m-1}{2}}\right] \exp\left(-\frac{\tau^2}{2\|\Gamma\|_2^2}\right) \\ & \quad \times \exp\left(\left[\frac{m\tau^2 d_{\min}^2}{\|\Gamma\|_2^2} - \frac{1}{2}md_{\min}^2\right] \|A[s]\|_2^2\right). \quad (48) \end{aligned}$$

Combining (47) and (48), it can be obtained that the magnitude of the attack should satisfy the following condition:

$$\begin{aligned} \|A[s]\|_2^2 &< \frac{2\|\Gamma\|_2^2}{md_{\min}^2(\tau^2 - \|\Gamma\|_2^2)} \left[ \frac{\tau^2}{2\|\Gamma\|_2^2} + \ln \alpha + \frac{1}{2} \ln \frac{\pi}{2} \right. \\ & \quad \left. - \ln \left( 4 + \frac{\tau}{\|\Gamma\|_2} \left(\frac{64}{(m-1)\pi}\right)^{\frac{m-1}{2}} \right) \right]. \quad (49) \end{aligned}$$

As long as the magnitude of the attack is small enough, this condition can be satisfied.

### APPENDIX D PROOF OF THEOREM 3

**Proof:** By applying (22) and (26) into (21), the residuals in the case that the system has reached steady state and is not attacked can be derived by

$$\begin{aligned}
 & \tau[k+1] \\
 &= Z[k+1] - H\hat{X}[k+1|k] \\
 &= H(G+BK)(X[l] - \hat{X}[l|l] + W_\infty v[l]) + v[l+1] \\
 &\quad + HBK(H^T R^{-1} H)^{-1} H^T R^{-1} v[l] - H(G+BK)W_\infty v[l] \\
 &\sim N_m(0, R + [HBK(H^T R^{-1} H)^{-1} H^T R^{-1} - H(G+BK)W_\infty] \\
 &\quad \times R[HBK(H^T R^{-1} H)^{-1} H^T R^{-1} - H(G+BK)W_\infty]^T \\
 &\quad + H(G+BK)(P - W_\infty R W_\infty^T)(G+BK)^T H^T). \quad (50)
 \end{aligned}$$

Denote  $(I - W_\infty H)(G+BK) \triangleq \Psi$ , the states of (29) and the estimation given by the Kalman filter at each time after attacks are calculated as follows:

$$\begin{aligned}
 X[l] &= (G+BK)X[l-1] \\
 &\quad + BK(H^T R^{-1} H)^{-1} H^T R^{-1} (v[l-1] + A[l-1]) \\
 &= (G+BK)^{l-s+1} X[s-1] \\
 &\quad + \sum_{k=0}^{l-s-1} (G+BK)^{l-s-k-1} BK(H^T R^{-1} H)^{-1} \\
 &\quad \times H^T R^{-1} (v[s+k] + A[s+k]) \quad (51)
 \end{aligned}$$

$$\begin{aligned}
 \hat{X}[l|l] &= \Psi \hat{X}[l-1|l-1] + W_\infty (HX[l] + v[l] + A[l]) \\
 &= \Psi^{l-s+1} \hat{X}[s-1|s-1] \\
 &\quad + \sum_{k=0}^{l-s} \Psi^{l-s-k} W_\infty H(G+BK)^{k+1} X[s-1] \\
 &\quad + \sum_{k=0}^{l-s} \Psi^{l-s-k} W_\infty H \sum_{i=0}^{k-1} (G+BK)^{k-i-1} BK \\
 &\quad \times (H^T R^{-1} H)^{-1} H^T R^{-1} (v[s+i] + A[s+i]) \\
 &\quad + \sum_{k=0}^{l-s} \Psi^{l-s-k} W_\infty (v[s+k] + A[s+k]). \quad (52)
 \end{aligned}$$

Before the attack beginning, for any time  $j$ ,  $f < j < s$ , where  $f$  is a large time when the system has already reached steady state, by the properties of the Kalman filter, it can be obtained that  $X[j] - \hat{X}[j|j] \sim N_m(0, P)$ . Then, if there was no attack, the Kalman filter would get an accurate estimate. Namely, if we replace  $A[k]$  with zero vector in (51) and (52), the difference between state and estimate  $X[l] - \hat{X}[l|l]$  follows a multivariate normal distribution  $N_m(0, P)$ .

Similar with Remark 1,  $X[l]$  and  $(\hat{X}[l|l] - W_\infty v[l])$  are both uncorrelated with  $v[l]$  in (51) and (52). Then

$$X[l]|_{A[k]=0} - (\hat{X}[l|l]|_{A[k]=0} - W_\infty v[l])$$

$$\begin{aligned}
 &= \left\{ (G+BK)^{l-s+1} X[s-1] + \sum_{k=0}^{l-s-1} (G+BK)^{l-s-k-1} BK \right. \\
 &\quad \times (H^T R^{-1} H)^{-1} H^T R^{-1} v[s+k] - \Psi^{l-s+1} \hat{X}[s-1|s-1] \\
 &\quad - \sum_{k=0}^{l-s} \Psi^{l-s-k} W_\infty H(G+BK)^{k+1} X[s-1] \\
 &\quad - \sum_{k=0}^{l-s} \Psi^{l-s-k} W_\infty \sum_{i=0}^{k-1} (G+BK)^{k-i-1} \\
 &\quad \times BK(H^T R^{-1} H)^{-1} H^T R^{-1} v[s+i] \\
 &\quad \left. - \sum_{k=0}^{l-s} \Psi^{l-s-k} W_\infty v[s+k] + W_\infty v[l] \right\} \\
 &\sim N_m(0, P - W_\infty R W_\infty^T). \quad (53)
 \end{aligned}$$

Now with attacks, by combining (51)–(53), and together with  $A[s-1] = \mathbf{0}$ , we can have the following equation:

$$\begin{aligned}
 X[l] - \hat{X}[l|l] + W_\infty v[l] \\
 &\sim N_m \left( \sum_{k=0}^{l-s-1} (G+BK)^{l-s-k-1} BK \right. \\
 &\quad \times (H^T R^{-1} H)^{-1} H^T R^{-1} A[s+k] \\
 &\quad - \sum_{k=0}^{l-s-1} \sum_{i=k}^{l-s-1} \Psi^{l-s-i-1} W_\infty H(G+BK)^{i-k} \\
 &\quad \times BK(H^T R^{-1} H)^{-1} H^T R^{-1} A[s+k] \\
 &\quad \left. - \sum_{k=0}^{l-s} \Psi^{l-s-k} W_\infty A[s+k], P - W_\infty R W_\infty^T \right). \quad (54)
 \end{aligned}$$

Then, applying (54) into (23), the residual can be obtained as follows:

$$\begin{aligned}
 \tau[l+1] &= Z_a[l+1] - H\hat{X}[l+1|l] \\
 &= H(G+BK)(X[l] - \hat{X}[l|l] + W_\infty v[l]) + v[l+1] \\
 &\quad + A[l+1] + HBK(H^T R^{-1} H)^{-1} H^T R^{-1} (v[l] + A[l]) \\
 &\quad - H(G+BK)W_\infty v[l] \\
 &\sim N_m(A[l+1] + [-H(G+BK)W_\infty \\
 &\quad + HBK(H^T R^{-1} H)^{-1} H^T R^{-1}]A[l] \\
 &\quad + H(G+BK) \left\{ \sum_{k=0}^{l-s-1} (G+BK)^{l-s-k-1} \right. \\
 &\quad \times BK(H^T R^{-1} H)^{-1} H^T R^{-1} A[s+k] \\
 &\quad - \sum_{k=0}^{l-s-1} \sum_{i=k}^{l-s-1} \Psi^{l-s-i-1} W_\infty H(G+BK)^{i-k} \\
 &\quad \times BK(H^T R^{-1} H)^{-1} H^T R^{-1} A[s+k]
 \end{aligned}$$

$$\begin{aligned}
& - \sum_{k=0}^{l-s-1} \Psi^{l-s-k} W_{\infty} A[s+k] \Big\} \\
& R[HBK(H^T R^{-1} H)^{-1} H^T R^{-1} - H(G+BK)W_{\infty}] \\
& \times R[HBK(H^T R^{-1} H)^{-1} H^T R^{-1} - H(G+BK)W_{\infty}]^T \\
& + H(G+BK)(P - W_{\infty} R W_{\infty}^T)(G+BK)^T H^T). \quad (55)
\end{aligned}$$

Comparing (50) with (55), it can be seen that the residuals before and after attacks have the same covariance when the system reaches steady state, namely attacks do not change the spread of residuals. Therefore, in order to prevent the attacks from being detected, it only need to ensure that the expectation of the residual after attacks does not change. From (55), it can be found that the expectation of the residual after attacks  $\tau[i]$  is only dependent on the historical attack data. Therefore, what the attacker needs to do is just to make sure that  $E(\tau[i]) = 0$  based on the previous attacks in each step, and doing so can bypass the detection effectively. Hence, the attack vector at each step should be organized as follows:

$$\begin{aligned}
A[l] = & [H(G+BK)W_{\infty} - HBK(H^T R^{-1} H)^{-1} H^T R^{-1}] A[l-1] \\
& - H(G+BK) \left\{ \sum_{k=0}^{l-s-2} (G+BK)^{l-s-k-2} BK \right. \\
& \times (H^T R^{-1} H)^{-1} H^T R^{-1} A[s+k] \\
& + \sum_{k=0}^{l-s-2} \sum_{i=k}^{l-s-2} [(I - W_{\infty} H)(G+BK)]^{l-s-i-2} W_{\infty} H \\
& \times (G+BK)^{i-k} BK (H^T R^{-1} H)^{-1} H^T R^{-1} A[s+k] \\
& \left. + \sum_{k=0}^{l-s-2} [(I - W_{\infty} H)(G+BK)]^{l-s-k-1} W_{\infty} A[s+k] \right\}.
\end{aligned}$$

#### APPENDIX E PROOF OF THEOREM 4

**Proof:**

$$\begin{aligned}
A[l] = & H \times \left\{ [(G+BK)W_{\infty} - HBK(H^T R^{-1} H)^{-1} H^T R^{-1}] \right. \\
& \times A[l-1] - (G+BK) \left\{ \sum_{k=0}^{l-s-2} (G+BK)^{l-s-k-2} \right. \\
& \times BK (H^T R^{-1} H)^{-1} H^T R^{-1} A[s+k] \\
& + \sum_{k=0}^{l-s-2} \sum_{i=k}^{l-s-2} [(I - W_{\infty} H)(G+BK)]^{l-s-i-2} W_{\infty} H \\
& \times (G+BK)^{i-k} BK (H^T R^{-1} H)^{-1} H^T R^{-1} \\
& \left. \times A[s+k] + \sum_{k=0}^{l-s-2} [(I - W_{\infty} H)(G+BK)]^{l-s-k-1} \right.
\end{aligned}$$

$$\begin{aligned}
& \times W_{\infty} A[s+k] \Big\} \Big\} \\
& \triangleq H \times \mathcal{X}[l].
\end{aligned}$$

Applying this formula to the traditional residual detection (11) leads to the residual under the attack

$$\begin{aligned}
r[l]|_{A[l]} = & (I - H(H^T R^{-1} H)^{-1} H^T R^{-1}) v[k] \\
& + (I - H(H^T R^{-1} H)^{-1} H^T R^{-1}) A[l] \\
= & (I - H(H^T R^{-1} H)^{-1} H^T R^{-1}) v[k] \\
& + (I - H(H^T R^{-1} H)^{-1} H^T R^{-1}) H \mathcal{X}[l] \\
= & (I - H(H^T R^{-1} H)^{-1} H^T R^{-1}) v[k] \\
& + (H \mathcal{X}[l] - H \mathcal{X}[l]) \\
= & (I - H(H^T R^{-1} H)^{-1} H^T R^{-1}) v[k]
\end{aligned}$$

which is same as the residual without attacks (6). Therefore, the postattack strategy can bypass the traditional residual detection.

#### REFERENCES

- [1] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.
- [2] U. S. Energy Information Administration Office of Energy Analysis, *Annual energy outlook 2020 with projections to 2050*, 2020. [Online]. Available: <https://www.eia.gov/outlooks/aeo/pdf/AEO2020%20Full%20Report.pdf>
- [3] G. Lu, D. De, and W. Song, "SmartGridLab: A laboratory-based smart grid testbed," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Gaithersburg, MD, USA, 2010, pp. 143–148.
- [4] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures," *IEEE Trans. Ind. Inform.*, vol. 15, no. 12, pp. 6522–6530, Dec. 2019.
- [5] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Elect. Power Syst. Res.*, vol. 81, no. 7, pp. 1334–1340, 2011.
- [6] P. Braun, L. Grüne, C. M. Kellett, S. R. Weller, and K. Worthmann, "A distributed optimization algorithm for the predictive control of smart grids," *IEEE Trans. Autom. Control*, vol. 61, no. 12, pp. 3898–3911, Dec. 2016.
- [7] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–169, Mar. 2013.
- [8] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Worst-case stealthy innovation-based linear attack on remote state estimation," *Automatica*, vol. 89, pp. 117–124, 2018.
- [9] H. Yi *et al.*, "Bad data injection in smart grid: Attack and defense mechanisms," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 27–33, Jan. 2013.
- [10] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.
- [11] R. Deng and H. Liang, "False data injection attacks with limited susceptibility information and new countermeasures in smart grid," *IEEE Trans. Ind. Inform.*, vol. 15, no. 3, pp. 1619–1628, Mar. 2019.
- [12] R. Moslemi, A. Mesbahi, and J. M. Velni, "A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4930–4941, Sep. 2018.
- [13] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, Jun. 2016.
- [14] J. Hao *et al.*, "An adaptive Markov strategy for defending smart grid false data injection from malicious attackers," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2398–2408, Jul. 2018.

- [15] R. Zhang and P. Venkatasubramanian, "False data injection and detection in LQG systems: A game theoretic approach," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 1, pp. 338–348, Mar. 2020.
- [16] T. R. B. Kushal, K. Lai, and M. S. Illindala, "Risk-based mitigation of load curtailment cyber attack using intelligent agents in a shipboard power system," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 4741–4750, Sep. 2019.
- [17] A. Chattopadhyay and U. Mitra, "Security against false data-injection attack in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 2, pp. 1015–1027, Jun. 2020.
- [18] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.
- [19] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.
- [20] M. H. Basiri, J. G. Thistle, J. W. Simpson-Porco, and S. Fischmeister, "Kalman filter based secure state estimation and individual attacked sensor detection in cyber-physical systems," in *Proc. Amer. Control Conf.*, Philadelphia, PA, USA, 2019, pp. 3841–3848.
- [21] J. Zhao *et al.*, "Power system dynamic state estimation: Motivations, definitions, methodologies, and future work," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3188–3198, Jul. 2019.
- [22] M. Choraria, A. Chattopadhyay, U. Mitra, and E. Strom, "Optimal deception attack on networked vehicular cyber physical systems," in *Proc. 53rd Asilomar Conf. Signals, Syst., Comput.*, 2019, pp. 1131–1135.
- [23] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 4–13, Mar. 2017.
- [24] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, p. 13, 2011.
- [25] H. Li, L. Lai, and H. V. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1097–1107, Jul. 2012.
- [26] R. E. Kalman, "A new approach to linear filtering and prediction problems," *J. Basic Eng.*, vol. 82, pp. 35–45, 1960.
- [27] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, Gaithersburg, MD, USA, 2009, pp. 21–30.
- [28] IEEE PES AMPS DSAS Test Feeder Working Group, [Online]. Available: <https://cmte.ieee.org/pes-testfeeders/resources/>



**Yifa Liu** received the B.E. degree in automation from Nankai University, Tianjin, China, in 2018. He is currently working toward the Ph.D. degree in control theory and control engineering with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China.

His current research interests include distributed control, optimization, and multiagent systems.



**Long Cheng** (Senior Member, IEEE) received the B.S. (Hons.) degree in control engineering from Nankai University, Tianjin, China, in 2004, and the Ph.D. (Hons.) degree in control theory and control engineering from the Institute of Automation, Chinese Academy of Sciences, Beijing, China, in 2009.

He is currently a Full Professor with the Institute of Automation, Chinese Academy of Sciences. He is also an adjunct Professor with the University of Chinese Academy of Sciences. He has authored and co-authored more than 100 technical papers in peer-reviewed journals and prestigious conference proceedings. His current research interests include the rehabilitation robot, intelligent control, and neural networks.

Dr. Cheng was the recipient of the IEEE TRANSACTIONS ON NEURAL NETWORKS Outstanding Paper Award from IEEE Computational Intelligence Society, the Aharon Katzir Young Investigator Award from International Neural Networks Society, and the Young Researcher Award from Asian Pacific Neural Networks Society. He is currently serving as an Associate Editor for IEEE TRANSACTIONS ON CYBERNETICS, IEEE TRANSACTIONS ON AUTOMATION SCIENCE AND ENGINEERING, *Neurocomputing*, *International Journal of Systems Science*, and *Acta Automatica Sinica*.